Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE
Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil

Expression des Besoins et Identification des Objectifs de Sécurité

EBIOS®

Abschnitt 5

MITTEL FÜR DIE BEHANDLUNG VON IT-RISIKEN

Version 2 – 5. Februar 2004

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01 71 75 84 15 - Fax 01 71 75 84 00

Dieses Dokument wurde vom Beratungsbüro der DCSSI
(SGDN / DCSSI / SDO / BCS)
in Zusammenarbeit mit dem EBIOS-Club erstellt.

Kommentare und Anmerkungen werden gerne unter Einsendung an folgende Adresse entgegengenommen:

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP
FRANCE

ebios.dcssi@sgdn.pm.gouv.fr

Änderungsprotokoll

Version	Gegenstand der Änderung	Stand
02/1997 (1.1)	Veröffentlichung des Leitfadens "Formalisierung von Bedürfnissen und Identifizierung von Sicherheitszielen" (EBIOS – Expression des besoins et d'identification des objectifs de sécurité).	Genehmigt
23/01/2004	Generalüberarbeitung: - Erläuterungen und Anpassung an die Internationalen Normen über Sicherheit und Risikomanagement - Hervorhebung der Basisverordnungen zur Unterscheidung von allen übrigen zu berücksichtigenden Anforderungen. - Integrierung der Konzepte "Hypothese" und "Sicherheitsvorschriften" (ISO/IEC 15408) - Übernahme der ausgewählten wesentlichen Elemente in die Zielsystemstudie - Verbesserungen bei der Festlegung der Bedarfsskala: Werte, die von der Organisation, bezogen auf ihre unmittelbaren Auswirkungen, als akzeptable Grenzen eingestuft werden. - Integrierung der für jedes Element formalisierten Bedarfe bezogen auf die nachfolgende Aktivität. - Integrierung der Bestimmung des Betriebsmodus' in die Hypothesen. - Anpassung der Konzepte an ISO/IEC 15408: Analysiert wird der Ursprung der Bedrohungen, d. h. die Angriffsmethoden und die bedrohenden Elemente, sowie deren Charakterisierung nach Art (natürlich bedingt, menschlich bedingt, umgebungsbedingt), Ursache (unbeabsichtigt, vorsätzlich bei weiterer Aufsplitterung nach Exposition, verfügbare Ressourcen, Fachkenntnissen und Motivation) und Angriffspotential. - Hervorhebung der nicht berücksichtigten Angriffsmethoden - Formalisierung der Bedrohungen im Sinne von ISO/IEC 15408 (bedrohendes Element, Angriff und Wert bezogen auf die Entitäten), bevor diese dem Sicherheitsbedarf gegenübergestellt werden. - Änderung bezüglich der Gegenüberstellung von Bedrohungen und Bedürfnissen zur Identifizierung von Risiken - Hervorhebung der nicht berücksichtigten Risiken - Integrierung der Festlegung minimaler Sicherheitsziele für die Aktivitäten "Formalisierung von Sicherheitszielen" und "Bestimmung von funktionellen Anforderungen" - Änderung bezüglich der Festlegung von Sicherheitszielen, bei der die Hypothesen, die aus der Sicherheits-Policy erwachsenen Vorschriften, die Zwänge, Basisverordnungen und Risiken berücksichtigt werden - Hinzufügen der Bestimmung von Sicherheitsniveaus, wodurch das Niveau der Sicherheitsziele bestimmt (z. B. unter Berücksichtigung des Angriffspotentials) und ein Gewährleistungsniveau ausgewählt werden kann. - Hinzufügen der Bestimmung funktioneller Sicherheitsanforderungen; dadurch können funktionelle Anforderungen bezogen auf die Sicherheitsziele bestimmt und diese Entsprechung dargestellt werden - Hinzufügen der Bestimmung von Sicherheitsgewährleistungsanforderungen, mit denen eventuelle Gewährleistungsanforderungen festgelegt werden können. Verbesserungen hinsichtlich Form, Anpassungen und geringfügiger Korrekturen (Grammatik, Rechtschreibung, Formulierungen, Gestaltung, Kohärenz usw.)	vom EBIOS-Club genehmigt
05/02/2004	Veröffentlichung der Version 2 des EBIOS-Leitfadens	Genehmigt

Inhaltsverzeichnis

1 Einführung

Die EBIOS[1] –Methode besteht aus fünf sich ergänzenden Abschnitten.

- Abschnitt 1 - Einführung
  In diesem Abschnitt werden der Kontext, der Nutzen und der Stellenwert der EBIOS-Methodik vorgestellt. Vervollständigt wird dieser Abschnitt durch ein Literaturverzeichnis, ein Glossar und ein Abkürzungsverzeichnis.

- Abschnitt 2 - Methodik
  Dieser Abschnitt beschreibt den Ablauf der verschiedenen Aktivitäten der Methode.

- Abschnitt 3 - Techniken
  In diesem Abschnitt werden Mittel zur Realisierung der Aktivitäten der Methode angeboten. Es ist ratsam, diese Techniken den Anforderungen und Praktiken der jeweiligen Institution anzupassen.

- Abschnitt 4 – Mittel zur IT-Risikobewertung
  Dieser Abschnitt entspricht dem ersten Teil der Wissensdatenbanken der EBIOS-Methode (Entitätstypen, Angriffsmethoden, Schwachstellen)

- Abschnitt 5 – Mittel zur Behandlung von IT-Risiken
  Dieser Abschnitt entspricht dem zweiten Teil der Wissensdatenbanken der EBIOS-Methode (Sicherheitsziele, Sicherheitsanforderungen, Tabellen zur Festlegung der funktionellen Sicherheitsziele und –anforderungen).

Das vorliegende Dokument entspricht dem fünften Abschnitt der Methode.

Es beinhaltet:
- Eine Datenbank mit den Sicherheitszielen,
- eine Datenbank mit den Sicherheitsanforderungen,
- Tabellen, über die die Sicherheitsziele in Abhängigkeit von den Angriffsmethoden und Schwachstellen bestimmt werden können
- Tabellen, über die die Sicherheitsanforderungen bestimmt werden können, die in der Lage sind, den Sicherheitszielen zu genügen.

[1] EBIOS ist eine Schutzmarke des Generalsekretariats der Nationalen Verteidigung in Frankreich.

2 Allgemeine Sicherheitsziele

Die Sicherheitsziele werden nach Entitätstypen sortiert. Sie werden mit einem Code und einem Namen versehen. Für den Entitätstyp SYS (System) werden die Sicherheitsziele der anderen Entitätstypen benutzt.
Obwohl die Summe aller Sicherheitsziele sicher nicht vollständig ist, ist doch sichergestellt, dass ein Grossteil aller die IT-Sicherheit betreffenden Themen abgedeckt wird.
Die Sicherheitsziele müssen weiter verfeinert werden, um sie dem besonderen Kontext der EBIOS-Studie anpassen zu können.

2.1 MAT : Hardware

MAT_01	
Inhalt	Für den Fall eines Geräteausfalls muss ein Vorrat an Ersatz-Betriebsmitteln bereit gehalten werden

MAT_02	
Inhalt	Im Schadensfall, bei Ausfall oder Nachlässigkeit muss es möglich sein, Systeme, Anwendungen, Datenmengen oder Protokollaufzeichnungen ganz oder teilweise wiederherzustellen

MAT_03	
Inhalt	Gemäßigte Änderungen der Umgebungsbedingungen (Temperatur, Feuchtigkeit, Luftzusammensetzung) dürfen kein anomales Verhalten der elektronischen Einrichtungen und Datenträger hervorrufen

MAT_04	
Inhalt	Während der gesamten Aufbewahrungsdauer muss eine einwandfreie Lesbarkeit der archivierten Datenträger garantiert werden

MAT_05	
Inhalt	Betriebsmittel und Datenträger müssen jederzeit und bedingungslos wieder in Betrieb gesetzt werden können, selbst in Ausnahmesituationen

MAT_06	
Inhalt	Die Beschreibung der gesamten IT-Ausstattung sowie deren Lokalisierung müssen sichergestellt sein

MAT_07	
Inhalt	Die IT-Ausstattung einschließlich Datenträger (Speicherkassetten, Festplatten, Laptops) muss gegen Diebstahl gesichert werden

MAT_08	
Inhalt	Von einem Datenträger zu löschende sensitive Informationen dürfen nicht rekonstruiert werden können

MAT_09	
Inhalt	Die Betriebsmittel müssen entsprechend den zu erbringenden Dienstleistungen dimensioniert werden, wobei eventuelle Überlastungsperioden zu berücksichtigen sind

MAT_10	
Inhalt	Die Systeme, die die Betriebsmittel betreiben, müssen gegen eine Benutzung durch unbefugte Benutzer geschützt werden

MAT_11	
Inhalt	Bei der Wahl der Betriebsmittel, Datenträger und Softwareprogramme müssen Ergonomie und Wartungsfreundlichkeit berücksichtigt werden

MAT_12	
Inhalt	Die Betriebsmittel müssen den im Unternehmen geltenden Hygiene- und

	Sicherheitsvorschriften entsprechen
MAT_13	
Inhalt	Die Kontrolle und Instandhaltung der Betriebsmittel muss jederzeit gewährleistet sein, auch während der Ferienzeit, an Feiertagen und außerhalb der Öffnungszeiten
MAT_14	
Inhalt	Die Einhaltung der Sicherheitsanforderungen muss für die Installation, den Betrieb und die Instandhaltung der Betriebsmittel garantiert werden
MAT_15	
Inhalt	Bei der Wahl der Betriebsmittel, Softwareprogramme und Datenträger muss die Zuverlässigkeit berücksichtigt werden

2.2 LOG : Software

LOG_01	
Inhalt	Die Integrität der Programme und Daten muss garantiert werden
LOG_02	
Inhalt	Die Aktualisierung von Softwareprogrammen darf weder die Sicherheit, noch die Funktionalitäten früherer Versionen beeinträchtigen
LOG_03	
Inhalt	Sämtliche Operationen zur Aktualisierung der Softwareprogramme müssen identifiziert und gerechtfertigt werden können
LOG_04	
Inhalt	Die Konfiguration der Systeme und Anwendungen muss mit den Anforderungen der Sicherheitspolitik übereinstimmen
LOG_05	
Inhalt	Auf den sensitiven Anwendungen und den zugehörenden Systemen lastende böse Absichten oder Nachlässigkeiten müssen detektiert werden
LOG_06	
Inhalt	Vor Inbetriebnahme eines neuen Tools muss die Konformität mit den Anforderungen der Sicherheitspolitik garantiert werden können
LOG_07	
Inhalt	Die Verwaltung der Lizenzen, deren Eintragung und Aufbewahrung muss sichergestellt sein
LOG_08	
Inhalt	Die Institution muss eine Liste über die auf den Geräten installierten Konfigurationen führen und die Konformität mit dieser Liste jederzeit garantieren können
LOG_09	
Inhalt	Die Software muss unter Beachtung der Sicherheitsanforderungen installiert und zur Gewährleistung ihrer Beständigkeit instand gehalten werden
LOG_10	
Inhalt	Die Protokolle über Eingriffe müssen ausgewertet werden können, auch wenn sie von verschiedenen Systemen generiert wurden (Möglichkeit zur Rekonstruktion der zeitlichen Abfolge von Ereignissen)
LOG_11	
Inhalt	Innerhalb der Informationsverarbeitungssysteme muss eine aktive Verwaltung der Ermächtigungen unter Berücksichtigung von Informationsansprüchen und Änderungsberechtigungen sichergestellt werden

LOG_12	
Inhalt	Da die Benutzung von Kommunikations- bzw. Gruppenarbeitsmitteln nicht den Anforderungen der Sicherheitspolitik unterliegt, muss sie durch besondere Bedingungen und Vorschriften geregelt werden

LOG_13	
Inhalt	Jeder Systemzugriff muss durch eine Einrichtung zur Authentifizierung und Identifikation geschützt werden

LOG_14	
Inhalt	Ausfälle oder Leistungsabweichungen der Systeme müssen gemeldet werden

LOG_15	
Inhalt	Für jedes System muss die Möglichkeit bestehen, ein unnormales Verhalten in Echtzeit oder im Nachhinein zu erkennen, die durchgeführten Aktionen nachzuvollziehen und die Autoren zu identifizieren

LOG_16	
Inhalt	Die Anzeige sensitiver Daten darf keine Sicherheitsschwachstelle für die Vertraulichkeit der Daten darstellen

LOG_17	
Inhalt	Die Softwareprogramme müssen so entworfen werden, dass Bedienungsfehler eingeschränkt werden

2.3 RES : Netzwerk

RES_01	
Inhalt	Die Zugänge zu Kommunikationsschnittstellen müssen gegen Missbrauch und Benutzung in böser Absicht geschützt werden

RES_02	
Inhalt	Die Kommunikationsschnittstellen müssen die Übertragungen im Hinblick auf die Vertraulichkeit, Integrität und Verfügbarkeit schützen

RES_03	
Inhalt	Gegebenenfalls muss die Authentifizierung und Nichtabstreitbarkeit von Kommunikationen aktiviert werden können

RES_04	
Inhalt	Die Kompatibilität zwischen den angeschlossenen Elementen muss gewährleistet sein (Sprachen, Zeitzonen, Normen usw.)

RES_05	
Inhalt	Es muss einen klaren und aktuellen Routenplan geben

RES_06	
Inhalt	Die Netzzugänge müssen bereitgestellt und kontrolliert werden

2.4 PER : Personal

PER_01	
Inhalt	Das Personal muss die Betriebsmittel und Datenträger außerhalb der Räumlichkeiten gegen Diebstahl und Intrusion schützen

PER_02	
Inhalt	Personal mit Zugang zu sensitiven Informationen muss entsprechend sensibilisiert und identifiziert werden

PER_03	
Inhalt	Das Personal muss einen sachgerechten Umgang mit den Betriebs- und

	Kommunikationsmitteln und eine pflegliche Behandlung der Datenträger sowie die Sicherheitsvorschriften bezüglich der Klassifizierung von Informationen einhalten
PER_04	
Inhalt	Zur Gewährleistung der Kontinuität der Aufgaben bei Abwesenheit muss eine Personalreserve bereitgehalten werden
PER_05	
Inhalt	Das Personal muss der Sicherheitsmethodik anhängen, und die Rollen und Verantwortungen müssen klar definiert und bekannt sein
PER_06	
Inhalt	Neue Mitarbeiter oder Aushilfskräfte müssen ihre Aufgaben in Einklang mit der Sicherheitspolitik erledigen können
PER_07	
Inhalt	Es muss eine Trennung zwischen der entscheidenden, ausführenden und kontrollierenden Gewalt geben
PER_08	
Inhalt	Das Personal muss in die Verantwortung einbezogen und über eventuelle Sanktionen aufgeklärt werden
PER_09	
Inhalt	Das Personal muss für die Wahrung des Berufsgeheimnisses und der Zurückhaltung sensibilisiert werden
PER_10	
Inhalt	Das Personal muss für die Einhaltung der Normen der Institution sensibilisiert und entsprechend geschult werden
PER_11	
Inhalt	Das Personal muss bei einem Zwischenfall die anzuwendenden Reflexe kennen (Unterrichtungspflicht, Mittel zur Weitergabe von Informationen usw.)
PER_12	
Inhalt	Das Personal muss für die Benutzung der zur Ausübung seiner Tätigkeit notwendigen Hard- und Softwaremittel ausgebildet sein
PER_13	
Inhalt	Die Einbindung der Direktion in die Sicherheitsmethodik muss reell und sichtbar sein

2.5 PHY : Standort

PHY_01	
Inhalt	Die Erbringung der zum Betrieb der Betriebsmittel wesentlichen Dienste (z. B. Elektrizität, Kommunikation, Klimatisierung usw.) muss sichergestellt, guter Qualität und durch die Institution kontrolliert sein
PHY_02	
Inhalt	Der Standort darf keine Beobachtung vertraulicher Informationen von außen ermöglichen
PHY_03	
Inhalt	Standort und Räumlichkeiten müssen die Betriebsmittel gegen Aggressionen, Brand, Überschwemmung, elektromagnetische Störungen usw. schützen
PHY_04	
Inhalt	Die Wahl des Standorts muss helfen, die Risiken einzuschränken (Schwierigkeiten bei der Zugänglichkeit zum Standort, Überschwemmung, Brand, Verschmutzung, Erdbeben, Unwetter usw.), wobei diese in die Vorüberlegungen

	zur Konstruktion einzubeziehen sind
PHY_05	
Inhalt	Kompromittierende elektromagnetische Emissionen dürfen außerhalb sensitiver Bereiche nicht auswertbar sein
PHY_06	
Inhalt	Die Lagerung von und der Umgang mit potentiell gefährlichen Stoffen oder Materialien darf für das Informationssystem kein Risiko darstellen
PHY_07	
Inhalt	Der Standort muss mit den Sicherheitsnormen der Institution konform sein
PHY_08	
Inhalt	Rauchen, Essen und Trinken muss in Räumlichkeiten mit IT-Material verboten sein
PHY_09	
Inhalt	Die Räumlichkeiten müssen gegen Feuer und Ausbreitung von Bränden geschützt werden
PHY_10	
Inhalt	Die Installation und Benutzung von Betriebsmitteln muss den geltenden Standards und Normen entsprechen (Empfehlung des Herstellers, Vorschriften der PSSI, Sicherheitsnormen usw.)
PHY_11	
Inhalt	Die Installation von Betriebsmitteln muss geplant und kontrolliert werden
PHY_12	
Inhalt	Die Räumlichkeiten müssen einschließlich der Einrichtung den Aufgaben der Institution angepasst werden

2.6 ORG : Organisation

ORG_01	
Inhalt	Die Organisation muss die Betriebsmittel und Datenträger gegen den physischen Zugang durch Unbefugte schützen
ORG_02	
Inhalt	Die Ein- und Ausgangsprozeduren sollen gegen den Diebstahl von Betriebsmitteln ankämpfen
ORG_03	
Inhalt	Die (jeweiligen) Übertragungsmittel und ihr Betrieb müssen den Schutz ihres Inhalts gegen Risiken wie Verbreitung, Diebstahl, Manipulation, Abstreitbarkeit und Verlust garantieren
ORG_04	
Inhalt	Die Organisation muss die Anforderungen der Sicherheitspolitik bei der Entwicklung, Nutzung und beim Betrieb der Systeme durchsetzen (Hardware und Software)
ORG_05	
Inhalt	Die Politik zur Wiederherstellung von Daten muss die integrale Wiederherstellung von Sicherungskopien garantieren, auch nach Weiterentwicklung der Systeme (Hardware und Software)
ORG_06	
Inhalt	Die Antiviruspolitik muss die Einschleusung und Verbreitung maligner Codes in den Systemen verhindern
ORG_07	

Inhalt	Die Archivierpolitik muss die integrale Wiedergewinnung von Daten während der gesamten festgelegten Aufbewahrungsdauer garantieren
ORG_08	
Inhalt	Die Organisation muss sich davon vergewissern, dass alle Daten in angemessenen Abständen gespeichert werden (einschließlich der nicht zentralisierten Daten)
ORG_09	
Inhalt	Die Organisation muss eine vorbeugende Politik gegen Überlastung und Ausfall der Betriebsmittel einbeziehen (Informatik, Klimatisierung, Energie, Kommunikation)
ORG_10	
Inhalt	Die Organisation muss sich der ordnungsgemäßen Verwaltung und Benutzung ausreichend robuster Passwörter vergewissern
ORG_11	
Inhalt	Die Politik zur Verarbeitung maschinenlesbarer Protokolldaten muss mit den geltenden Vorschriften übereinstimmen
ORG_12	
Inhalt	Die Organisation muss gegen den Empfang nicht erbetener Nachrichten (Spam) und gegen Fehlinformationen bei Nutzung interner Kommunikationsmittel ankämpfen
ORG_13	
Inhalt	Die Organisation muss sich der Beständigkeit der Lösungen im Hinblick auf die Regeln der Kunst und die Weiterentwicklung des Informationssystems vergewissern
ORG_14	
Inhalt	Jede Rolle, die an die Sicherheit des Informationssystems gebunden ist, muss immer (auch bei Abwesenheit des Amtsinhabers) der Verantwortung von mindestens einer Person unterstehen, die die erforderlichen Kompetenzen besitzt oder die Möglichkeit hat, entsprechende Unterlagen zu Rate zu ziehen
ORG_15	
Inhalt	Die Organisation muss sich der Kennzeichnung des vertraulichen Charakters der jeweiligen Information vergewissern und sicherstellen, dass die entsprechenden Schutzvorschriften Anwendung finden
ORG_16	
Inhalt	Die Organisation muss sicherstellen, dass die Ersatzmittel für Notfälle betriebsbereit sind und wenn möglich die Kontinuität der Dienste sensitiver Aktivitäten der Institution bei Ausfall, Schadensfall oder schwerwiegender böser Absicht aufrechterhalten
ORG_17	
Inhalt	Die Organisation muss sich vergewissern, dass die Sicherheitsanweisungen bei einem Zwischenfall oder böser Absicht eingehalten werden
ORG_18	
Inhalt	Die Organisation muss garantieren, dass die minimalen Sicherheitsanforderungen der Informationssysteme von allen eingehalten werden
ORG_19	
Inhalt	Die Organisation muss gegen die Anwesenheit unbefugter Personen am Standort ankämpfen
ORG_20	
Inhalt	Die Organisation muss die Integrität und Authentizität von Lieferungen kontrollieren (Hardware und Software)

ORG_21	
Inhalt	Die Organisation muss die Bearbeitung und Weiterverfolgung eines jeden die Sicherheit betreffenden Zwischenfalls gewährleisten, der innerhalb der Institution aufgedeckt wurde

ORG_22	
Inhalt	Die Organisation muss die Kontrolle der Sicherheitsmaßnahmen sowie deren Entsprechung im Hinblick auf die Sicherheitsziele garantieren

ORG_23	
Inhalt	Die Organisation muss sich der Konformität aller Räumlichkeiten mit der Sicherheitspolitik vergewissern (Einrichtung einer technischen oder einer IT-Plattform, Zugangseinrichtungen zum Standort, Überwachung der Räumlichkeiten, Feuerdetektion und Brandschutz usw.)

ORG_24	
Inhalt	Die Organisation muss im Krisenfall eine schnelle und wirksame Reaktion garantieren und gleichzeitig eine Einschränkung potentieller Auswirkungen und die Kontinuität wesentlicher Aktivitäten gewährleisten: Ausfall, Schadensfall, Intrusion größeren Ausmaßes, sonstige böse Absicht

ORG_25	
Inhalt	Die Organisation muss sich vergewissern, dass die Eingriffe durch externe Personen (Leistungserbringer, Lieferanten usw.) keine Gefahrenquellen für das Informationssystem darstellen

ORG_26	
Inhalt	Die Organisation muss die Einhaltung der Sicherheitspolitik bei der Einrichtung sensitiver Systeme (Hardware oder Software) garantieren

ORG_27	
Inhalt	Die Organisation muss sich der Instandhaltung der Hardware und Software vergewissern

ORG_28	
Inhalt	Die Organisation muss sich der Verfügbarkeit der aktuellen technischen Unterlagen aller Hardware-, Software- und Infrastrukturkomponenten vergewissern

ORG_29	
Inhalt	Die Organisation muss in Einklang mit den geltenden Normen ein tätigkeitsspezifisches Qualitätsmanagement einbeziehen

ORG_30	
Inhalt	Die Organisation muss gegen unzulässigen Zugriff auf Informationen und Datenverarbeitungen ankämpfen

ORG_31	
Inhalt	Die Organisation der Sicherheit des Informationssystems muss den lokalen Umgebungskontext berücksichtigen (wirtschaftlicher, sozialer, politischer, gesetzgebender Kontext)

ORG_32	
Inhalt	Die Organisation muss die Berücksichtigung der Sicherheitsbedürfnisse und Betriebszwänge im Vorfeld und während der gesamten Entwicklung garantieren

ORG_33	
Inhalt	Die Organisation muss die Möglichkeit eines Missbrauchs von Rechten und Zugriffsprivilegien auf die Systeme einschränken

ORG_34	
Inhalt	Die Organisation muss den Zugang des Personals zu neuen Technologien gewährleisten (Schulung, Zusammenarbeit usw.)

ORG_35	
Inhalt	Die Organisation muss sich der Einrichtung einer Sicherheitspolitik zum Schutz und zur Überwachung der Informationen vergewissern

ORG_36	
Inhalt	Die Organisation muss sich vergewissern, dass die festgelegten Prozeduren für die Anwendung ausreichend anpassungsfähig sind

ORG_37	
Inhalt	Die Organisation muss gerechte und dem Kontext angepasste Sanktionen bei Nicht-Einhaltung der Sicherheitspolitik vorsehen, sofern dadurch die Sicherheit des Informationssystems in Frage gestellt würde

ORG_38	
Inhalt	Die Organisation muss sich vergewissern, dass die Unterauftragnehmer/Leistungserbringer/Lieferanten/Industrielle/ Tochterorganisationen/Standorte während ihrer Einsätze die Sicherheitspolitik beachten (Arbeiten, Entwicklungen, Wartung usw.)

ORG_39	
Inhalt	Die Organisation muss sich vergewissern, dass die Protokolldaten und Beweiselemente in Einklang mit der Sicherheitspolitik ausgewertet und geschützt werden

ORG_40	
Inhalt	Die Organisation muss sich vergewissern, dass alle geltenden Gesetze und Vorschriften bei der Sicherheitspolitik berücksichtigt werden

ORG_41	
Inhalt	Die Organisation muss sich vergewissern, dass alle anwendbaren Vorschriften und Prozeduren auf neuestem Stand und den betroffenen Personen mühelos zugänglich sind

ORG_42	
Inhalt	Die Organisation muss sich vergewissern, dass die Verwaltung des Informationssystems so einfach wie möglich ausgelegt ist

ORG_43	
Inhalt	Die Ausführung sensitiver Operationen muss überprüft werden (Durchführung der Operationen von mehr als einer Person, Validierung, systematische Protokolldatenauswertung usw.)

ORG_44	
Inhalt	Die akzeptierten Restrisiken müssen Gegenstand gesonderter Studien sein und für jedes identifizierte tatsächliche Restrisiko ist, wenn möglich und für den Fall einer Konkretisierung, ein Aktionsplan auszuarbeiten

ORG_45	
Inhalt	Die Organisation muss sich vergewissern, dass die Arbeitsbedingungen zufrieden stellend sind

3 Allgemeine funktionelle Sicherheitsanforderungen

Die in diesem Teil formulierten allgemeinen funktionellen Sicherheitsanforderungen wurden unter Bezugnahme auf folgende Regelwerke erstellt :

- [ISO 15408]
- [ISO 17799]
- Sonstige Quellen (EBIOS v1, [PSSI], Best Practices usw.).

Sie werden nach "Klassen", "Familien" und eventuell "Unterfamilien" eingeteilt und mit einem Code und einem Namen versehen.
Obwohl die Summe all dieser Anforderungen sicher nicht vollständig ist, ist doch sichergestellt, dass ein Grossteil aller die IT-Sicherheit betreffenden Themen abgedeckt wird.
Diese Anforderungen müssen weiter verfeinert werden, um sie dem besonderen Kontext der EBIOS-Studie anpassen zu können.

3.1 Aus ISO 15408 hervorgehende Anforderungen

3.1.1 FAU : Sicherheitsaudit

FAU_ARP: Automatische Reaktion des Sicherheitsaudits	
Sicherheitsalarme	Hierarchisch gebunden an: Keine weitere Komponente. FAU_ARP.1.1 Die TSF muss bereits bei Erkennung einer potentiellen Verletzung der Sicherheit mit [Zuweisung: Liste der am wenigsten störenden Aktionen] beginnen. Verwandte Themen: FAU_SAA.1 Analyse von potentiellen Verletzungen Beispiele Sobald eine potentielle Verletzung der Sicherheit erkannt wird, muss mit den Aktionen zur Unterbindung der Verletzung und zur Eingrenzung der Auswirkungen begonnen werden
FAU_GEN: Generierung der Daten des Sicherheitsaudits	
Generierung der Auditdaten	Hierarchisch gebunden an: Keine weitere Komponente. FAU_GEN.1.1 Die TSF muss eine Auditaufzeichnung folgender auditierbarerer Ereignisse generieren können: a) Beginn und Ende der Auditfunktionen; b) alle auditierbaren Ereignisse für das Auditniveau [Zuweisung: Minimal, elementar, detailliert, nicht angegeben]; c) und [Zuweisung: Sonstige, speziell definierte auditierbare Ereignisse]. Verwandte Themen: FPT_STM.1 Zuverlässige Zeitangabe Beispiele Auditaufzeichnungen müssen für zuvor definierte Ereignisse generiert werden können
Generierung der Auditdaten	Hierarchisch gebunden an: Keine weitere Komponente. FAU_GEN.1.2 Die TSF muss in jeder Auditaufzeichnung mindestens folgende Informationen aufzeichnen: a) Datum und Uhrzeit des Ereignisses, Ereignistyp, Identität des Subjekts sowie das Ergebnis (Erfolg oder Misserfolg) des Ereignisses; b) und, für jeden Audit-Ereignistyp, basierend auf den in den funktionellen Komponenten im Schutzprofil (PP) oder den Sicherheitsvorgaben (ST) enthaltenen Definitionen auditierbarer Ereignisse [Zuweisung: Sonstige relevante

	Auditinformationen]. Verwandte Themen: FPT_STM.1 Zuverlässige Zeitangabe Beispiele Die Auditaufzeichnungen müssen mindestens das Datum, die Uhrzeit, den Ereignistyp, die Identität des Subjekts, das Ergebnis (Erfolg oder Misserfolg) des Ereignisses sowie jede sonstige zusätzlich erforderliche und zuvor definierte Information enthalten.
Verbindung mit der Benutzeraudität	Hierarchisch gebunden an: Keine weitere Komponente. FAU_GEN.2.1 Die TSF muss jedes auditierbare Ereignis der Identität desjenigen Benutzers zuordnen können, der dieses Ereignis ausgelöst hat. Verwandte Themen: FAU_GEN.1 Generierung der Auditdaten FIA_UID.1 Programmierung der Identifikation Beispiele Jedes auditierbare Ereignis muss eindeutig der Identität desjenigen Benutzers, der das Ereignis ausgelöst hat, zugeordnet werden können
FAU_SAA: Analyse des Sicherheitsaudits	
Analyse von potentiellen Verletzungen	Hierarchisch gebunden an: Keine weitere Komponente. FAU_SAA.1.1 Die TSF muss bei gleichzeitiger Überwachung der auditierten Ereignisse eine Anzahl von Vorschriften anwenden und auf Grundlage dieser Vorschriften eine potentielle Verletzung der TSP anzeigen können. Verwandte Themen: FAU_GEN.1 Generierung der Auditdaten Beispiele Die Vorschriften sollen der Analyse der auditierten Ereignisse dienen, um potentielle Verletzungen der Sicherheit aufdecken zu können.
Analyse von potentiellen Verletzungen	Hierarchisch gebunden an: Keine weitere Komponente. FAU_SAA.1.2 Zur Überwachung der auditierten Ergebnisse muss die TSF folgende Vorschriften anwenden: a) Ansammlung oder Kombination bekannter [Zuweisung: Teilmenge von definierten auditierbaren Ereignissen] zur Anzeige einer potentiellen Verletzung der Sicherheit; b) [Zuweisung : Beliebige sonstige Vorschriften]. Verwandte Themen: FAU_GEN.1 Generierung der Auditdaten Beispiele Auditierbare Ereignisse, die eine potentielle Verletzung der Sicherheit anzeigen, müssen als solche identifiziert werden.
Erkennung einer Anomalie auf Grund eines Profils	Hierarchisch gebunden an: FAU_SAA.1 FAU_SAA.2.1 Die TSF muss Systemnutzungsprofile bereithalten können, wobei ein einzelnes Profil die früheren Verhaltensmodelle eines oder mehrerer Mitglieder der [Zuweisung: Zielgruppe des Profils] wiedergibt. Verwandte Themen: FIA_UID.1 Programmierung der Identifikation Beispiele Typische Systemnutzungsprofile, die die früheren Verhaltensmodelle einer

	Benutzergruppe wiedergeben, müssen eingerichtet und auf neuestem Stand gehalten werden
Erkennung einer Anomalie auf Grund eines Profils	Hierarchisch gebunden an: FAU_SAA.1 FAU_SAA.2.2 Die TSF muss einen Repräsentanzindex bereithalten können, der jedem Benutzer zugeordnet wird, dessen Aktivität in einem Profil aufgezeichnet wird, wobei der Repräsentanzindex den Grad angibt, um den sich die augenblickliche Aktivität des Benutzers als abweichend von den ermittelten, im Profil dargestellten Nutzungsmodellen erweist. Verwandte Themen: FIA_UID.1 Programmierung der Identifikation Beispiele Jedem Benutzer eines typischen Nutzungsprofils muss ein aktueller Repräsentanzindex zugeordnet werden; dieser muss den Grad angeben, um den die augenblickliche Aktivität des Benutzers von den definierten, im Profil dargestellten Nutzungsmodellen abweicht
Erkennung einer Anomalie auf Grund eines Profils	Hierarchisch gebunden an: FAU_SAA.1 FAU_SAA.2.3. Die TSF muss in der Lage sein, eine drohende Verletzung der TSP anzuzeigen, sobald der Repräsentanzindex eines Benutzers die folgenden Grenzbedingungen [Zuweisung: Bedingungen, unter denen eine abweichende Aktivität durch die TSF angezeigt wird] überschreitet. Verwandte Themen: FIA_UID.1 Programmierung der Identifikation Beispiele Es müssen Vorschriften zur Analyse der Repräsentanzindexe definiert werden, damit drohende potentielle Verletzungen der Sicherheitspolitik erkannt werden können
Heuristische Vorhersage einfacher Attacken	Hierarchisch gebunden an: FAU_SAA.1 FAU_SAA.3.1 Die TSF muss eine interne Darstellung folgender charakteristischer Ereignisse [Zuweisung: Teilmenge von Systemereignissen] bereithalten können, die eine Verletzung der TSP anzeigen können. Verwandte Themen: Keine verwandten Themen Beispiele Eine interne Darstellung charakteristischer Ereignisse, die eine Verletzung der Sicherheitspolitik anzeigen können, muss bereitgehalten werden.
Heuristische Vorhersage einfacher Attacken	Hierarchisch gebunden an: FAU_SAA.1 FAU_SAA.3.2 Die TSF muss die charakteristischen Ereignisse mit der Aufzeichnung der Systemaktivitäten vergleichen können, die bei der Prüfung der [Zuweisung: Heranzuziehende Informationen zur Feststellung von Systemaktivitäten] erkannt werden können. Verwandte Themen: Keine verwandten Themen Beispiele Zur Bestimmung der Systemaktivitäten muss eine Anzahl von heranzuziehenden Informationen identifiziert und mit den charakteristischen Ereignissen, die eine Verletzung der Sicherheitspolitik anzeigen können, verglichen werden
Heuristische Vorhersage einfacher	Hierarchisch gebunden an: FAU_SAA.1 FAU_SAA.3.3 Die TSF muss in der Lage sein, eine drohende Verletzung der

Attacken	TSP anzuzeigen, wenn sich herausstellt, dass ein Systemereignis mit einem charakteristischen Ereignis, das eine potentielle Verletzung der TSP anzeigt, übereinstimmt. Verwandte Themen: Keine verwandten Themen Beispiele Es müssen Alarmmechanismen eingerichtet werden, die eine drohende Verletzung der Sicherheitspolitik anzeigen, sobald sich ein Systemereignis als übereinstimmend mit einem charakteristischen Ereignis, das eine potentielle Verletzung anzeigt, herausstellt.
Heuristische Vorhersage komplexer Attacken	Hierarchisch gebunden an: FAU_SAA.3 FAU_SAA.4.1 Die TSF muss eine interne Darstellung von Ereignisabfolgen bereithalten können, die Bestandteil folgender bekannter Intrusionsszenarien [Zuweisung: Liste der Systemereignisabfolgen, die eine repräsentative Zusammenstellung bekannter Eindringszenarien darstellen] und folgender charakteristischer Ereignisse [Zuweisung: Teilmenge von Systemereignissen] sind, die eine potentielle Verletzung der TSP anzeigen können. Verwandte Themen: Keine verwandten Themen Beispiele Es muss eine interne Darstellung von Ereignisabfolgen bereitgehalten werden, die Bestandteile bekannter Intrusionsszenarien und charakteristischer Ereignisse sind
Heuristische Vorhersage komplexer Attacken	Hierarchisch gebunden an: FAU_SAA.3 FAU_SAA.4.2 Die TSF muss die charakteristischen Ereignisse und Ereignisabfolgen mit der Aufzeichnung der Systemaktivitäten vergleichen können, die bei der Prüfung der [Zuweisung: Heranzuziehende Informationen zur Bestimmung der Systemaktivitäten] erkannt werden können. Verwandte Themen: Keine verwandten Themen Beispiele Die Informationen, die zur Bestimmung der Systemaktivitäten herangezogen werden, müssen mit den charakteristischen Ereignissen und den Ereignisabfolgen verglichen werden
Heuristische Vorhersage komplexer Attacken	Hierarchisch gebunden an: FAU_SAA.3 FAU_SAA.4.3 Die TSF muss in der Lage sein, eine drohende Verletzung der TSP anzuzeigen, wenn sich herausstellt, dass die Systemaktivität mit einem charakteristischen Ereignis oder einer Ereignisabfolge übereinstimmt, das bzw. die eine potentielle Verletzung der TSP anzeigt. Verwandte Themen: Keine verwandten Themen Beispiele Es müssen Alarmmechanismen eingerichtet werden, die eine drohende Verletzung der Sicherheitspolitik anzeigen, sobald sich Systemereignisse als übereinstimmend mit einer Ereignisabfolge, die eine potentielle Verletzung anzeigt, herausstellen
FAU_SAR: Review des Sicherheitsaudits	
Audit-Review	Die vorliegende Komponente bietet den dazu befugten Benutzern die Möglichkeit, Informationen zu erhalten und zu interpretieren. Wenn es sich um menschliche Benutzer (um Personen) handelt, müssen die Informationen in einer

	ihnen verständlichen Form präsentiert werden. Wenn es sich um externe IT-Einheiten handelt, müssen die Informationen unzweideutig in einem elektronischen Format präsentiert werden. Hierarchisch gebunden an: Keine weitere Komponente. FAU_SAR.1.1 Die TSF muss den [Zuweisung: Befugte Benutzer] die Möglichkeit bieten, über die Audit-Aufzeichnungen die [Zuweisung: Liste der Audit-Informationen] zu lesen. Verwandte Themen: FAU_GEN.1 Generierung der Auditdaten Beispiele Die dazu befugten Benutzer müssen die Möglichkeit haben, über die Audit-Aufzeichnungen die Audit-Informationen zu lesen.
Audit-Review	Die vorliegende Komponente bietet den dazu befugten Benutzern die Möglichkeit, Informationen zu erhalten und zu interpretieren. Wenn es sich um menschliche Benutzer (um Personen) handelt, müssen die Informationen in einer ihnen verständlichen Form präsentiert werden. Wenn es sich um externe IT-Einheiten handelt, müssen die Informationen unzweideutig in einem elektronischen Format präsentiert werden. Hierarchisch gebunden an: Keine weitere Komponente. FAU_SAR.1.2 Die TSF muss die Audit-Aufzeichnungen in einer Form darstellen, die dem Benutzer die Möglichkeit bietet, sie zu interpretieren. Verwandte Themen: FAU_GEN.1 Generierung der Auditdaten Beispiele Die Audit-Aufzeichnungen müssen so dargestellt werden, dass der Benutzer sie interpretieren kann
Eingeschränktes Audit-Review	Hierarchisch gebunden an: Keine weitere Komponente. FAU_SAR.2.1 Die TSF muss allen Benutzern den Lesezugriff auf die Audit-Aufzeichnungen verweigern, mit Ausnahme der Benutzer, denen ausdrücklich ein Lesezugriff gewährt wurde. Verwandte Themen: FAU_SAR.1 Audit-Review Beispiele Allen Benutzern muss das Recht auf Lesezugriff auf die Audit-Aufzeichnungen verweigert werden, mit Ausnahme der Benutzer, denen ausdrücklich ein Lesezugriff gewährt wurde
Selektives Audit-Review	Hierarchisch gebunden an: Keine weitere Komponente. FAU_SAR.3.1 Die TSF muss die Möglichkeit bieten, je nach [Zuweisung: Logisch zusammenhängende Kriterien] Auditdaten zu [Auswahl: Suchen, Sortieren, Ordnen]. Verwandte Themen: FAU_SAR.1 Audit-Review Beispiele Bezüglich der Auditdaten müssen logisch zusammenhängende Kriterien definiert werden, damit mit den Auditdaten Operationen wie Suchen, Sortieren und Ordnen durchgeführt werden können
FAU_SEL: Auswahl von Ereignissen des Sicherheitsaudits	

Selektives Audit	Hierarchisch gebunden an: Keine weitere Komponente. FAU_SEL.1.1 Die TSF muss auditierbare Ereignisse bezogen auf die Gesamtheit aller auditierten Ereignisse ein- bzw. ausschließen können, und zwar in Abhängigkeit folgender Attribute: a) [Auswahl: Identität des Objekts, Identität des Benutzers, Identität des Subjekts, Identität des Hostrechners, Ereignistyp] b) [Zuweisung : Liste zusätzlicher Attribute, auf deren Basis die Auswahl der Audits erfolgt]. Verwandte Themen: FAU_GEN.1 Generierung der Auditdaten FMT_MTD.1 Administration der TSF-Daten Beispiele Je nach Identität des Objekts, des Benutzers, des Subjekts oder des Hostrechners, des Ereignistyps oder sonstiger Attribute, auf deren Basis die Auswahl der Audits erfolgt, müssen auditierbare Ereignisse von den auditierten Ereignissen ausgeschlossen werden können
FAU_STG: Speicherung von Ereignissen des Sicherheitsaudits	
Geschützte Speicherung von Protokollen	Hierarchisch gebunden an: Keine weitere Komponente. FAU_STG.1.1 Die TSF muss gespeicherte Audit-Aufzeichnungen gegen unerlaubtes Löschen schützen. Verwandte Themen: FAU_GEN.1 Generierung der Auditdaten Beispiele Gespeicherte Audit-Aufzeichnungen müssen gegen unerlaubtes Löschen geschützt werden
Geschützte Speicherung von Protokollen	Hierarchisch gebunden an: Keine weitere Komponente. FAU_STG.1.2 Die TSF muss an den Audit-Aufzeichnungen vorgenommene Änderungen [Auswahl: Verhindern, Erkennen] können. Verwandte Themen: FAU_GEN.1 Generierung der Auditdaten Beispiele An den Audit-Aufzeichnungen vorgenommene Änderungen müssen erkannt und/oder verhindert werden können
Garantie der Verfügbarkeit von Auditdaten	Hierarchisch gebunden an: FAU_STG.1 FAU_STG.2.1 Die TSF muss gespeicherte Audit-Aufzeichnungen gegen unerlaubtes Löschen schützen. FAU_STG.2.2 Die TSF muss an den Audit-Aufzeichnungen vorgenommene Änderungen [Auswahl: Verhindern, Erkennen] können. FAU_STG.2.3 Die TSF muss garantieren, dass die [Zuweisung: Maß für die Speicherung der Audit-Aufzeichnungen] der Audit-Aufzeichnungen beibehalten wird, wenn eine der folgenden Bedingungen eintritt: [Auswahl: Audit-Speicherkapazität erschöpft, Ausfall, Attacke]. Verwandte Themen: FAU_GEN.1 Generierung der Auditdaten Beispiele Ein (zu definierender) Prozentsatz der Audit-Aufzeichnungen muss bei erschöpfter Speicherkapazität der Auditdaten, bei Ausfall oder bei Attacke

	erhalten werden
Aktion bei eventuellem Verlust von Auditdaten	Hierarchisch gebunden an: Keine weitere Komponente. FAU_STG.3.1 Die TSF muss [Zuweisung: Vorzunehmende Aktionen bei möglichem Ausfall der Auditspeicherung] vornehmen, wenn das Protokoll [Zuweisung: zuvor definierte Grenze] überschreitet. Verwandte Themen: FAU_STG.1 Geschützte Speicherung von Protokollen Beispiele Bestimmte Aktionen sind vorzunehmen, wenn das Protokoll einen zuvor definierten (noch zu definierenden) Grenzumfang überschreitet
Vorbeugung gegen Verlust von Auditdaten	Hierarchisch gebunden an: FAU_STG.3 FAU_STG.4.1 Wenn das Protokoll voll ist, muss die TSF [Zuweisung: "Die auditierbaren Ereignisse ignorieren", "Auditierbare Ereignisse, die nicht von einem befugten Benutzer mit Sonderrechten herbeigeführt wurden, verhindern", "die ältesten gespeicherten Aufzeichnungen überschreiben"] und [Zuweisung: Sonstige durchzuführende Aktionen bei Ausfall der Auditspeicherung]. Verwandte Themen: : FAU_STG.1 Geschützte Speicherung von Protokollen Beispiele Für den Fall des Erreichens der maximalen Kapazität zur Speicherung von Auditdaten müssen entsprechende Maßnahmen definiert werden (z. B. auditierbare Ereignisse ignorieren oder die ältesten Aufzeichnungen überschreiben)

3.1.2 FCO : Kommunikation

FCO_NRO: Nichtabstreitbarkeit der gesendeten Nachricht	
Selektiver Herkunftsnachweis	Hierarchisch gebunden an: Keine weitere Komponente. FCO_NRO.1.1 Die TSF muss auf Anfrage des [Auswahl: Absenders, Empfängers, [Zuweisung: Liste dritter Parteien]] Nachweise über die Herkunft übertragener [Zuweisung: Liste der Informationstypen] generieren können. Verwandte Themen: FIA_UID.1 Programmierung der Identifikation Beispiele Der Nachweis der Herkunft übertragener Informationen muss auf Anfrage des Absenders, Empfängers oder (zu definierender) dritter Parteien generiert werden können.
Selektiver Herkunftsnachweis	Hierarchisch gebunden an: Keine weitere Komponente. FCO_NRO.1.2 Die TSF muss die [Zuweisung: Liste der Attribute] des Absenders der Informationen den [Zuweisung: Liste der Informationsfelder] der Informationen, auf die sich der Nachweis bezieht, zuordnen können. Verwandte Themen: FIA_UID.1 Programmierung der Identifikation Beispiele Die Attribute des Absenders der Informationen muss den Informationsfeldern der Informationen, auf die sich der Nachweis bezieht, zugeordnet werden können.
Selektiver	Hierarchisch gebunden an: Keine weitere Komponente.

Herkunftsnachweis	FCO_NRO.1.3 Die TSF muss dem [Auswahl: Absender, Empfänger, [Zuweisung: Liste dritter Parteien]] die Möglichkeit geben, den Nachweis über die Herkunft von Informationen zu überprüfen, unter Vorgabe von [Zuweisung: Begrenzungen des Herkunftsnachweises]. Verwandte Themen: FIA_UID.1 Programmierung der Identifikation Beispiele Der Absender, der Empfänger oder (zu definierende) dritte Parteien müssen die Möglichkeit haben, unter Vorgabe der Begrenzungen des Herkunftsnachweises den Nachweis der Herkunft von Informationen überprüfen zu können
Systematischer Herkunftsnachweis	Hierarchisch gebunden an: FCO_NRO.1 FCO_NRO.2.1 Die TSF muss die Generierung des Herkunftsnachweises jederzeit für übertragene [Zuweisung: Liste der Informationstypen] sicherstellen können. FCO_NRO.2.2 Die TSF muss die [Zuweisung: Liste der Attribute] des Absenders der Informationen den [Zuweisung: Liste der Informationsfelder] der Informationen, auf die sich der Nachweis bezieht, zuordnen können. FCO_NRO.2.3 Die TSF muss dem [Auswahl: Absender, Empfänger, [Zuweisung: Liste dritter Parteien]] die Möglichkeit geben, den Nachweis über die Herkunft von Informationen zu überprüfen, unter Vorgabe von [Zuweisung: Begrenzungen des Herkunftsnachweises]. Verwandte Themen: FIA_UID.1 Programmierung der Identifikation Beispiele Der Herkunftsnachweis muss für bestimmte (zu definierende) Informationstypen jederzeit generiert werden können
FCO_NRR: Nichtabstreitbarkeit der empfangenen Nachricht	
Selektiver Empfangsnachweis	Hierarchisch gebunden an: Keine weitere Komponente. FCO_NRR.1.1 Die TSF muss auf Anfrage des [Auswahl: Absenders, Empfängers, [Zuweisung: Liste dritter Parteien]] Nachweise über den Empfang der [Zuweisung: Liste mit Informationstypen] generieren können. Verwandte Themen: FIA_UID.1 Programmierung der Identifikation Beispiele Der Nachweis des Empfangs übertragener Informationen muss auf Anfrage des Absenders, Empfängers oder (zu definierender) dritter Parteien generiert werden können
Selektiver Empfangsnachweis	Hierarchisch gebunden an: Keine weitere Komponente. FCO_NRR.1.2 Die TSF muss die [Zuweisung: Liste der Attribute] des Empfängers der Informationen den [Zuweisung: Liste der Informationsfelder] der Informationen, auf die sich der Nachweis bezieht, zuordnen können. Verwandte Themen: FIA_UID.1 Programmierung der Identifikation Beispiele Die Attribute des Empfängers der Informationen muss den Informationsfeldern der Informationen, auf die sich der Nachweis bezieht, zugeordnet werden können.

Selektiver Empfangsnachweis	Hierarchisch gebunden an: Keine weitere Komponente. FCO_NRR.1.3 Die TSF muss dem [Auswahl: Absender, Empfänger, [Zuweisung: Liste dritter Parteien]] die Möglichkeit geben, den Nachweis über den Empfang von Informationen zu überprüfen, unter Vorgabe von [Zuweisung: Begrenzungen des Empfangsnachweises]. Verwandte Themen: FIA_UID.1 Programmierung der Identifikation Beispiele Der Absender, der Empfänger oder (zu definierende) dritte Parteien müssen die Möglichkeit haben, unter Vorgabe der Begrenzungen des Empfangsnachweises den Nachweis des Empfangs von Informationen überprüfen zu können.
Systematischer Empfangsnachweis	Hierarchisch gebunden an: FCO_NRR.1 FCO_NRR.2.1 Die TSF muss die Generierung des Empfangsnachweises für die empfangenen [Zuweisung: Liste der Informationstypen] sicherstellen. FCO_NRR.2.2 Die TSF muss die [Zuweisung: Liste der Attribute] des Empfängers der Informationen den [Zuweisung: Liste der Informationsfelder] der Informationen, auf die sich der Nachweis bezieht, zuordnen können. FCO_NRR.2.3 Die TSF muss dem [Auswahl: Absender, Empfänger, [Zuweisung: Liste dritter Parteien]] die Möglichkeit geben, den Nachweis über den Empfang von Informationen zu überprüfen, unter Vorgabe von [Zuweisung: Begrenzungen des Empfangsnachweises]. Verwandte Themen: FIA_UID.1 Programmierung der Identifikation Beispiele Der Empfangsnachweis muss für bestimmte (zu definierende) übertragene Informationstypen jederzeit generiert werden können.

3.1.3 FCS : Kryptografische Unterstützung

FCS_CKM: Management der kryptografischen Schlüssel	
Generierung kryptografischer Schlüssel	Hierarchisch gebunden an: Keine weitere Komponente. FCS_CKM.1.1 Die TSF muss die kryptografischen Schlüssel gemäß eines spezifizierten Algorithmus zur Generierung kryptografischer Schlüssel [Zuweisung: Algorithmus zur Generierung kryptorgrafischer Schlüssel] und entsprechend den spezifizierten kryptografischen Schlüssellängen [Zuweisung: Länge der kryptografischen Schlüssel] generieren, wobei folgende [Zuweisung: Liste der Normen] zu beachten sind. Verwandte Themen: [FCS_CKM.2 Verteilung kryptografischer Schlüssel oder FCS_COP.1 Kryptografische Operation] FCS_CKM.4 Vernichtung von kryptografischen Schlüsseln FMT_MSA.2 Sichere Sicherheitsattribute Beispiele Die kryptografischen Schlüssel müssen gemäß eines Algorithmus zur Generierung von (zu definierenden) spezifischen kryptografischen Schlüsseln und in den (zu definierenden) spezifizierten kryptografischen Schlüssellängen, die den benannten (zu definierenden) Normen entsprechen, generiert werden
Verteilung kryptografischer Schlüssel	Hierarchisch gebunden an: Keine weitere Komponente. FCS_CKM.2.1 Die TSF muss die kryptografischen Schlüssel gemäß einer

	spezifizierten Methode zur Verteilung von kryptografischen Schlüsseln [Zuweisung: Algorithmus zur Verteilung von kryptorgrafischen Schlüsseln] verteilen, wobei folgende [Zuweisung: Liste der Normen] zu beachten sind . Verwandte Themen: [FDP_ITC.1 Import von Benutzerdaten ohne Sicherheitsattribute oder FCS_CKM.1 Generierung kryptografischer Schlüssel] FCS_CKM.4 Vernichtung von kryptografischen Schlüsseln FMT_MSA.2 Sichere Sicherheitsattribute Beispiele Die kryptografischen Schlüssel müssen gemäß einer (zu definierenden) spezifizierten Methode zur Verteilung kryptografischer Schlüssel verteilt werden, die den (zu definierenden) benannten Normen entspricht
Zugriff auf kryptografische Schlüssel	Hierarchisch gebunden an: Keine weitere Komponente. FCS_CKM.3.1 Die TSF muss einen [Zuweisung: Zugangstyp für den Zugriff auf kryptografische Schlüssel] gemäß einer spezifizierten Methode für den Zugriff auf kryptografische Schlüssel [Zuweisung: Methode für den Zugriff auf kryptografische Schlüssel] realisieren, wobei folgende [Zuweisung: Liste der Normen] zu beachten sind. Verwandte Themen: [FDP_ITC.1 Import von Benutzerdaten ohne Sicherheitsattribute oder FCS_CKM.1 Generierung kryptografischer Schlüssel] FCS_CKM.4 Vernichtung von kryptografischen Schlüsseln FMT_MSA.2 Sichere Sicherheitsattribute Beispiele Die Zugangstypen für den Zugriff auf die kryptografischen Schlüssel müssen mit einer (zu definierenden) spezifizierten Methode für den Zugriff auf kryptografische Schlüssel konform sein, die den (zu definierenden) benannten Normen entsprechen
Vernichtung von kryptografischen Schlüssel	Hierarchisch gebunden an: Keine weitere Komponente. FCS_CKM.4.1 Die TSF muss die kryptografischen Schlüssel gemäß einer spezifizierten Methode zur Vernichtung von kryptografischen Schlüsseln [Zuweisung: Algorithmus zur Vernichtung von kryptorgrafischen Schlüsseln] vernichten, wobei folgende [Zuweisung: Liste der Normen] zu beachten sind. Verwandte Themen: [FDP_ITC.1 Import von Benutzerdaten ohne Sicherheitsattribute oder FCS_CKM.1 Generierung kryptografischer Schlüssel] FMT_MSA.2 Sichere Sicherheitsattribute Beispiele Die kryptografischen Schlüssel müssen gemäß einer (zu definierenden) spezifizierten Methode zur Vernichtung von kryptografischen Schlüsseln vernichtet werden, die den (zu definierenden) benannten Normen entspricht
FCS_COP: Kryptografische Operation	
Kryptografische Operation	Hierarchisch gebunden an: Keine weitere Komponente. FCS_COP.1.1 Die TSF muss die [Zuweisung: Liste der kryptografischen Operationen] gemäß eines spezifizierten kryptografischen Algorithmus [Zuweisung: kryptografischer Algorithmus] und entsprechend den spezifizierten kryptografischen Schlüssellängen [Zuweisung: Länge der kryptografischen Schlüssel] ausführen, wobei folgende [Zuweisung: Liste der Normen] zu beachten sind. Verwandte Themen: [FDP_ITC.1 Import von Benutzerdaten ohne Sicherheitsattribute oder FCS_CKM.1 Generierung kryptografischer Schlüssel]

	FCS_CKM.4 Vernichtung von kryptografischen Schlüsseln FMT_MSA.2 Sichere Sicherheitsattribute Beispiele Die kryptografischen Operationen müssen gemäß eines (zu definierenden) kryptografischen Algorithmus und in den (zu definierenden) spezifizierten kryptografischen Schlüssellängen ausgeführt werden, die den (zu definierenden) benannten Normen entsprechen

3.1.4 FDP : Schutz der Benutzerdaten

FDP_ACC: Zugriffskontrollpolitik	
Teilweise Zugriffskontrolle	Hierarchisch gebunden an: Keine weitere Komponente. FDP_ACC.1.1 Die TSF muss die [Zuweisung: SFP für Zugriffskontrolle] für [Zuweisung: Liste der Subjekte, Objekte und der durch die SFP abgedeckten Operationen] anwenden. Verwandte Themen: FDP_ACF.1 Zugriffskontrolle basierend auf Sicherheitsattributen Beispiele Bei einer teilweisen Zugriffskontrolle muss die Sicherheitspolitik für die Zugriffskontrolle für (zu definierende) identifizierte Subjekte, Objekte und durch die Sicherheitspolitik abgedeckte Operationen zwischen Subjekten und Objekten angewendet werden
Umfassende Zugriffskontrolle	Hierarchisch gebunden an: FDP_ACC.1 FDP_ACC.2.1 Die TSF muss die [Zuweisung: SFP für Zugriffskontrolle] für [Zuweisung: Liste der Subjekte, Objekte] und alle durch die SFP abgedeckten Operationen zwischen den Subjekten und Objekten anwenden. Verwandte Themen: FDP_ACF.1 Zugriffskontrolle basierend auf Sicherheitsattributen Beispiele Bei einer umfassenden Zugriffskontrolle muss die Sicherheitspolitik für die Zugriffskontrolle für (zu definierende) identifizierte Subjekte und Objekte und für alle durch die Sicherheitspolitik abgedeckten Operationen zwischen den Subjekten und Objekten angewendet werden
Umfassende Zugriffskontrolle	Hierarchisch gebunden an: FDP_ACC.1 FDP_ACC.2.2 Die TSF muss sicherstellen, dass alle Operationen zwischen jedem Subjekt im TSC und jedem Objekt im TSC durch eine SFP für Zugriffskontrollen abgedeckt sind. Verwandte Themen: FDP_ACF.1 Zugriffskontrolle basierend auf Sicherheitsattributen Beispiele Bei einer umfassenden Zugriffskontrolle sind alle Operationen zwischen jedem Subjekt und jedem Objekt des Ziels durch die Sicherheitspolitik für Zugriffskontrollen abgedeckt.
FDP_ACF: Zugriffskontrollfunktionen	
Zugriffskontrolle	Hierarchisch gebunden an: Keine weitere Komponente.

basierend auf Sicherheitsattributen	FDP_ACF.1.1 Die TSF muss die [Zuweisung: SFP für Zugriffskontrolle] für Objekte, die auf [Zuweisung: Sicherheitsattribute, bestimmte Gruppen von Sicherheitsattributen] basieren, anwenden. Verwandte Themen: FDP_ACC.1 Teilweise Zugriffskontrolle FMT_MSA.3 Initialisierung statischer Attribute Beispiele Bei einer auf Sicherheitsattributen basierenden Zugriffskontrolle muss die Sicherheitspolitik für Zugriffskontrollen für Objekte, die auf (zu definierenden) Sicherheitsattributen oder Gruppen von Sicherheitsattributen basieren, angewendet werden
Zugriffskontrolle basierend auf Sicherheitsattributen	Hierarchisch gebunden an: Keine weitere Komponente. FDP_ACF.1.2 Die TSF muss folgende Vorschriften anwenden, um festzustellen, ob eine Operation zwischen kontrollierten Subjekten und kontrollierten Objekten zulässig ist: [Zuweisung: Vorschriften zur Regelung der Zugriffe zwischen den kontrollierten Subjekten und den kontrollierten Objekten mittels kontrollierter Operationen an kontrollierten Objekten]. Verwandte Themen: FDP_ACC.1 Teilweise Zugriffskontrolle FMT_MSA.3 Initialisierung statischer Attribute Beispiele Bei einer auf Sicherheitsattributen basierenden Zugriffskontrolle müssen stets die Vorschriften zur Regelung des Zugriffs zwischen kontrollierten Subjekten und kontrollierten Objekten mittels kontrollierter Operationen an kontrollierten Objekten angewendet werden
Zugriffskontrolle basierend auf Sicherheitsattributen	Hierarchisch gebunden an: Keine weitere Komponente. FDP_ACF.1.3 Die TSF muss den Zugriff von Subjekten auf Objekte unter Beachtung der folgenden zusätzlichen Vorschriften ausdrücklich zulassen: [Zuweisung: Auf Sicherheitsattributen basierende Vorschriften, die ausdrücklich den Zugriff von Subjekten auf Objekte zulassen]. Verwandte Themen: FDP_ACC.1 Teilweise Zugriffskontrolle FMT_MSA.3 Initialisierung statischer Attribute Beispiele Bei einer auf Sicherheitsattributen basierenden Zugriffskontrolle muss der Zugriff der Subjekte auf die Objekte unter Beachtung der zusätzlichen Vorschriften, die ausdrücklich diese (zu definierenden) Zugriffe zulassen, ausdrücklich autorisiert werden
Zugriffskontrolle basierend auf Sicherheitsattributen	Hierarchisch gebunden an: Keine weitere Komponente. FDP_ACF.1.4 Die TSF muss den Zugriff von Subjekten auf Objekte unter Beachtung der [Zuweisung: Auf Sicherheitsattributen basierende Vorschriften, die ausdrücklich den Zugriff von Subjekten auf Objekte verweigern] ausdrücklich verweigern. Verwandte Themen: FDP_ACC.1 Teilweise Zugriffskontrolle FMT_MSA.3 Initialisierung statischer Attribute Beispiele Bei einer auf Sicherheitsattributen basierenden Zugriffskontrolle muss

	der Zugriff der Subjekte auf die Objekte unter Beachtung der zusätzlichen Vorschriften, die ausdrücklich diese (zu definierenden) Zugriffe verweigern, ausdrücklich untersagt werden
FDP_DAU: Datenauthentifizierung	
Elementare Datenauthentifizierung	Hierarchisch gebunden an: Keine weitere Komponente. FDP_DAU.1.1 Die TSF muss die Möglichkeit zur Generierung von Nachweisen als Gültigkeitsgarantie von [Zuweisung: Liste der Objekte oder Informationstypen] bieten. Verwandte Themen: Keine verwandten Themen Beispiele (Zu definierende) identifizierte Subjekte müssen die Möglichkeit haben, den Nachweis über die Gültigkeit der (zu definierenden) angegebenen Informationen zu überprüfen
Elementare Datenauthentifizierung	Hierarchisch gebunden an: Keine weitere Komponente. FDP_DAU.1.1 Die TSF muss die Möglichkeit zur Generierung von Nachweisen als Gültigkeitsgarantie von [Zuweisung: Liste der Objekte oder Informationstypen] bieten. Verwandte Themen: Keine verwandten Themen Beispiele Es muss die Möglichkeit bestehen, einen Nachweis zu generieren, der als Garantie für die Gültigkeit von (zu definierenden) Objekten oder Informationstypen herangezogen werden kann
Datenauthentifizierung mit Identität des Garanten	Hierarchisch gebunden an: FDP_DAU.1 FDP_DAU.2.2 Die TSF muss den [Zuweisung: Liste der Subjekte] die Möglichkeit bieten, den Nachweis über die Gültigkeit der angegebenen Informationen und die Identität des Benutzers, der den Nachweis generiert hat, zu überprüfen. Verwandte Themen: FIA_UID.1 Programmierung der Identifikation Beispiele Bei einer Authentifizierung mit Identität des Garanten müssen (zu definierende) identifizierte Subjekte die Möglichkeit haben, den Nachweis über die Gültigkeit der (zu definierenden) angegebenen Informationen und die Identität des Benutzers, der den Nachweis generiert hat, zu überprüfen
FDP_ETC: Export in einen Bereich außerhalb der TSF-Kontrolle	
Export von Benutzerdaten ohne Sicherheitsattribute	Hierarchisch gebunden an: Keine weitere Komponente. FDP_ETC.1.1 Die TSF muss die [Zuweisung: SFP für Zugriffskontrolle oder SFP für Informationsflusskontrolle] beim Export von durch die SFP(s) kontrollierten Benutzerdaten in einen Bereich außerhalb des TSC anwenden. FDP_ETC.1.2 Die TSF muss die Benutzerdaten ohne die an diese Daten gebundenen Sicherheitsattribute exportieren. Verwandte Themen: [FDP_ACC.1 Teilweise Zugriffskontrolle oder FDP_IFC.1 Teilweise Informationsflusskontrolle]

	Beispiele Bei einem Datenexport ohne Sicherheitsattribute müssen die Benutzerdaten ohne die an diese Daten gebundenen Sicherheitsattribute exportiert werden
Export von Benutzerdaten ohne Sicherheitsattribute	Hierarchisch gebunden an: Keine weitere Komponente. FDP_ETC.1.1 Die TSF muss die [Zuweisung: SFP für Zugriffskontrolle oder SFP für Informationsflusskontrolle] beim Export von durch die SFP(s) kontrollierten Benutzerdaten in einen Bereich außerhalb des TSC anwenden. FDP_ETC.1.2 Die TSF muss die Benutzerdaten ohne die an diese Daten gebundenen Sicherheitsattribute exportieren. Verwandte Themen: [FDP_ACC.1 Teilweise Zugriffskontrolle oder FDP_IFC.1 Teilweise Informationsflusskontrolle] Beispiele Beim Export von durch die Sicherheitspolitik kontrollierten Benutzerdaten in einen Bereich außerhalb des Sicherheitsbereichs müssen die Sicherheitspolitik für die Zugriffskontrollen und die Sicherheitspolitik für die Informationsflusskontrollen angewendet werden
Export von Benutzerdaten mit Sicherheitsattributen	Hierarchisch gebunden an: Keine weitere Komponente. FDP_ETC.2.1 Die TSF muss die SFP(s) [Zuweisung: SFP für Zugriffskontrolle oder SFP für Informationsflusskontrolle] beim Export von durch die SFP(s) kontrollierten Benutzerdaten in einen Bereich außerhalb des TSC anwenden. FDP_ETC.2.2 Die TSF muss die Benutzerdaten mit den ihnen verbundenen Sicherheitsattributen exportieren. Verwandte Themen: [FDP_ACC.1 Teilweise Zugriffskontrolle oder FDP_IFC.1 Teilweise Informationsflusskontrolle] Beispiele Bei einem Datenexport mit Sicherheitsattributen müssen die Benutzerdaten mit den ihnen verbundenen Sicherheitsattributen exportiert werden
Export von Benutzerdaten mit Sicherheitsattributen	Hierarchisch gebunden an: Keine weitere Komponente. FDP_ETC.2.3 Die TSF muss sicherstellen, dass die Sicherheitsattribute beim Export in einen Bereich außerhalb der TSC unzweideutig mit den exportierten Benutzerdaten verbunden werden. Verwandte Themen: [FDP_ACC.1 Teilweise Zugriffskontrolle oder FDP_IFC.1 Teilweise Informationsflusskontrolle] Beispiele Eine unzweideutige Verbindung der Sicherheitsattribute mit den Benutzerdaten muss garantiert werden, wenn diese exportiert werden
Export von Benutzerdaten mit Sicherheitsattributen	Hierarchisch gebunden an: Keine weitere Komponente. FDP_ETC.2.4 Die TSF muss beim Export von Benutzerdaten aus dem TSC folgende Vorschriften anwenden [Zuweisung: Zusätzliche Vorschriften zur Exportkontrolle].

	Verwandte Themen: [FDP_ACC.1 Teilweise Zugriffskontrolle oder FDP_IFC.1 Teilweise Informationsflusskontrolle] Beispiele Beim Export von Benutzerdaten in einen Bereich außerhalb des Sicherheitsbereichs müssen zusätzliche (zu definierende) Vorschriften zur Exportkontrolle angewendet werden
FDP_IFC: Politik zur Informationsflusskontrolle	
Teilweise Informationsflusskontrolle	Hierarchisch zu: keiner anderen Komponente. FDP_IFC.1.1 Die TSF muss die [Zuweisung: SFP für Informationsflusskontrolle] auf [Zuweisung: Liste der Subjekte, Informationen und der durch die SFP abgedeckten Operationen, die einen Fluss von kontrollierten Informationen zu und von kontrollierten Subjekten bewirken] durchsetzen. Verwandte Themen: FDP_IFF.1 Einfache Sicherheitsattribute Beispiele Für eine teilweise Informationsflusskontrolle ist die Sicherheitspolitik zur Informationsflusskontrolle auf die Subjekte, Informationen und Operationen durchzusetzen, die einen Fluss zu und von kontrollierten Subjekten bewirken
Vollständige Informationsflusskontrolle	Hierarchisch zu: FDP_IFC.1 FDP_IFC.2.1 Die TSF muss die [Zuweisung: SFP für Informationsflusskontrolle] auf [Zuweisung: Liste von Subjekten und Informationen] und alle von der SFP abgedeckten Operationen, die einen Fluss dieser Informationen zu und von Subjekten bewirken, durchsetzen. Verwandte Themen: FDP_IFF.1 Einfache Sicherheitsattribute Beispiele Für eine vollständige Informationsflusskontrolle ist die Sicherheitspolitik zur Informationsflusskontrolle auf Subjekte, Informationen und alle Operationen durchzusetzen, die einen Fluss zu und von kontrollierten Subjekten bewirken
Vollständige Informationsflusskontrolle	Hierarchisch zu: FDP_IFC.1 FDP_IFC.2.2 Die TSF muss sicherstellen, dass alle Operationen, die einen Fluss einer beliebigen Information des TSC zu und von jedem Subjekt des TSC bewirken, von einer SFP für Informationsflusskontrolle abgedeckt werden. Verwandte Themen: FDP_IFF.1 Einfache Sicherheitsattribute Beispiele Für eine vollständige Informationsflusskontrolle müssen alle Operationen, die einen Fluss von Informationen zu und von jedwedem Subjekt des Sicherheitsbereichs bewirken, von einer Sicherheitspolitik zur Informationsflusskontrolle abgedeckt werden
FDP_IFF: Funktionen zur Informationsflusskontrolle	
Einfache Sicherheitsattribute	Hierarchisch zu: keiner anderen Komponente. FDP_IFF.1.1 Die TSF muss die [Zuweisung: SFP für

	Informationsflusskontrolle] auf Grundlage folgender Arten von Subjekt- und Informations-Sicherheitsattributen durchsetzen: [Zuweisung: Mindestanzahl und Arten der Sicherheitsattribute]. FDP_IFF.1.2 Die TSF muss einen über eine kontrollierte Operation erfolgenden Informationsfluss zwischen einem kontrollierten Subjekt und den kontrollierten Informationen erlauben, wenn die folgenden Regeln zutreffen: [Zuweisung: für jede Operation die geforderte auf Sicherheitsattributen basierende Beziehung zwischen Subjekt und Informations-Sicherheitsattributen]. FDP_IFF.1.3 Die TSF muss die [Zuweisung: zusätzliche SFP-Regeln für Informationsflusskontrolle] durchsetzen. FDP_IFF.1.4 Die TSF muss liefern, was folgt [Zuweisung: Liste zusätzlicher SFP-Fähigkeiten]. FDP_IFF.1.5 Die TSF muss einen Informationsfluss auf Grundlage folgender Regeln explizit autorisieren: [Zuweisung: auf Sicherheitsattributen basierende Regeln, die Informationsflüsse explizit autorisieren]. FDP_IFF.1.6 Die TSF muss einen Informationsfluss auf Grundlage folgender Regeln explizit verweigern: [Zuweisung: auf Sicherheitsattributen basierende Regeln, die Informationsflüsse explizit verweigern]. Verwandte Themen: FDP_IFC.1 Teilweise Informationsflusskontrolle FMT_MSA.3 Initialisierung statischer Attribute Beispiele Für einfache Sicherheitsattribute ist ein Informationsfluss zwischen einem kontrollierten Subjekt und Informationen, die über eine kontrollierte Operation kontrolliert wurden, auf Grundlage sicherheitsattributbasierter Regeln (zu definieren) zu erlauben
Einfache Sicherheitsattribute	Hierarchisch zu: keiner anderen Komponente. FDP_IFF.1.1 Die TSF muss die [Zuweisung: SFP für Informationsflusskontrolle] auf Grundlage folgender Arten von Subjekt- und Informations-Sicherheitsattributen durchsetzen: [Zuweisung: Mindestanzahl und Arten der Sicherheitsattribute]. FDP_IFF.1.2 Die TSF muss einen über eine kontrollierte Operation erfolgenden Informationsfluss zwischen einem kontrollierten Subjekt und den kontrollierten Informationen erlauben, wenn die folgenden Regeln zutreffen: [Zuweisung: für jede Operation die geforderte auf Sicherheitsattributen basierende Beziehung zwischen Subjekt und Informations-Sicherheitsattributen]. FDP_IFF.1.3 Die TSF muss die [Zuweisung: zusätzliche SFP-Regeln für Informationsflusskontrolle] durchsetzen. FDP_IFF.1.4 Die TSF muss liefern, was folgt [Zuweisung: Liste zusätzlicher SFP-Fähigkeiten]. FDP_IFF.1.5 Die TSF muss einen Informationsfluss auf Grundlage folgender Regeln explizit autorisieren: [Zuweisung: auf Sicherheitsattributen basierende Regeln, die Informationsflüsse explizit autorisieren]. FDP_IFF.1.6 Die TSF muss einen Informationsfluss auf Grundlage

	folgender Regeln explizit verweigern: [Zuweisung: auf Sicherheitsattributen basierende Regeln, die Informationsflüsse explizit verweigern]. Verwandte Themen: FDP_IFC.1 Teilweise Informationsflusskontrolle FMT_MSA.3 Initialisierung statischer Attribute Beispiele Die Sicherheitspolitik zur Informationsflusskontrolle ist auf Grundlage einer Mindestanzahl von identifizierten Sicherheitsattributen durchzusetzen (zu definieren)
Einfache Sicherheitsattribute	Hierarchisch zu: keiner anderen Komponente. FDP_IFF.1.1 Die TSF muss die [Zuweisung: SFP für Informationsflusskontrolle] auf Grundlage folgender Arten von Subjekt- und Informations-Sicherheitsattributen durchsetzen: [Zuweisung: Mindestanzahl und Arten der Sicherheitsattribute]. FDP_IFF.1.2 Die TSF muss einen über eine kontrollierte Operation erfolgenden Informationsfluss zwischen einem kontrollierten Subjekt und den kontrollierten Informationen erlauben, wenn die folgenden Regeln zutreffen: [Zuweisung: für jede Operation die geforderte auf Sicherheitsattributen basierende Beziehung zwischen Subjekt und Informations-Sicherheitsattributen]. FDP_IFF.1.3 Die TSF muss die [Zuweisung: zusätzliche SFP-Regeln für Informationsflusskontrolle] durchsetzen. FDP_IFF.1.4 Die TSF muss liefern, was folgt [Zuweisung: Liste zusätzlicher SFP-Fähigkeiten]. FDP_IFF.1.5 Die TSF muss einen Informationsfluss auf Grundlage folgender Regeln explizit autorisieren: [Zuweisung: auf Sicherheitsattributen basierende Regeln, die Informationsflüsse explizit autorisieren]. FDP_IFF.1.6 Die TSF muss einen Informationsfluss auf Grundlage folgender Regeln explizit verweigern: [Zuweisung: auf Sicherheitsattributen basierende Regeln, die Informationsflüsse explizit verweigern]. Verwandte Themen: FDP_IFC.1 Teilweise Informationsflusskontrolle FMT_MSA.3 Initialisierung statischer Attribute Beispiele Es sind die zusätzlichen Regeln der Sicherheitspolitik zur Informationsflusskontrolle (zu definieren) durchzusetzen
Einfache Sicherheitsattribute	Hierarchisch zu: keiner anderen Komponente. FDP_IFF.1.1 Die TSF muss die [Zuweisung: SFP für Informationsflusskontrolle] auf Grundlage folgender Arten von Subjekt- und Informations-Sicherheitsattributen durchsetzen: [Zuweisung: Mindestanzahl und Arten der Sicherheitsattribute]. FDP_IFF.1.2 Die TSF muss einen über eine kontrollierte Operation erfolgenden Informationsfluss zwischen einem kontrollierten Subjekt und den kontrollierten Informationen erlauben, wenn die folgenden Regeln zutreffen: [Zuweisung: für jede Operation die geforderte auf Sicherheitsattributen basierende Beziehung zwischen Subjekt und Informations-Sicherheitsattributen].

	FDP_IFF.1.3 Die TSF muss die [Zuweisung: zusätzliche SFP-Regeln für Informationsflusskontrolle] durchsetzen. FDP_IFF.1.4 Die TSF muss liefern, was folgt [Zuweisung: Liste zusätzlicher SFP-Fähigkeiten]. FDP_IFF.1.5 Die TSF muss einen Informationsfluss auf Grundlage folgender Regeln explizit autorisieren: [Zuweisung: auf Sicherheitsattributen basierende Regeln, die Informationsflüsse explizit autorisieren]. FDP_IFF.1.6 Die TSF muss einen Informationsfluss auf Grundlage folgender Regeln explizit verweigern: [Zuweisung: auf Sicherheitsattributen basierende Regeln, die Informationsflüsse explizit verweigern]. Verwandte Themen: FDP_IFC.1 Teilweise Informationsflusskontrolle FMT_MSA.3 Initialisierung statischer Attribute Beispiele Es ist eine Liste der ergänzenden Fähigkeiten der Sicherheitspolitik (zu definieren) zu liefern
Einfache Sicherheitsattribute	Hierarchisch zu: keiner anderen Komponente. FDP_IFF.1.1 Die TSF muss die [Zuweisung: SFP für Informationsflusskontrolle] auf Grundlage folgender Arten von Subjekt- und Informations-Sicherheitsattributen durchsetzen: [Zuweisung: Mindestanzahl und Arten der Sicherheitsattribute]. FDP_IFF.1.2 Die TSF muss einen über eine kontrollierte Operation erfolgenden Informationsfluss zwischen einem kontrollierten Subjekt und den kontrollierten Informationen erlauben, wenn die folgenden Regeln zutreffen: [Zuweisung: für jede Operation die geforderte auf Sicherheitsattributen basierende Beziehung zwischen Subjekt und Informations-Sicherheitsattributen]. FDP_IFF.1.3 Die TSF muss die [Zuweisung: zusätzliche SFP-Regeln für Informationsflusskontrolle] durchsetzen. FDP_IFF.1.4 Die TSF muss liefern, was folgt [Zuweisung: Liste zusätzlicher SFP-Fähigkeiten]. FDP_IFF.1.5 Die TSF muss einen Informationsfluss auf Grundlage folgender Regeln explizit autorisieren: [Zuweisung: auf Sicherheitsattributen basierende Regeln, die Informationsflüsse explizit autorisieren]. FDP_IFF.1.6 Die TSF muss einen Informationsfluss auf Grundlage folgender Regeln explizit verweigern: [Zuweisung: auf Sicherheitsattributen basierende Regeln, die Informationsflüsse explizit verweigern]. Verwandte Themen: FDP_IFC.1 Teilweise Informationsflusskontrolle FMT_MSA.3 Initialisierung statischer Attribute Beispiele Ein Informationsfluss ist auf der Grundlage sicherheitsattributbasierter Regeln, die die Informationsflüsse (zu definieren) explizit autorisieren, zu autorisieren

Einfache Sicherheitsattribute	Hierarchisch zu: keiner anderen Komponente. FDP_IFF.1.1 Die TSF muss die [Zuweisung: SFP für Informationsflusskontrolle] auf Grundlage folgender Arten von Subjekt- und Informations-Sicherheitsattributen durchsetzen: [Zuweisung: Mindestanzahl und Arten der Sicherheitsattribute]. FDP_IFF.1.2 Die TSF muss einen über eine kontrollierte Operation erfolgenden Informationsfluss zwischen einem kontrollierten Subjekt und den kontrollierten Informationen erlauben, wenn die folgenden Regeln zutreffen: [Zuweisung: für jede Operation die geforderte auf Sicherheitsattributen basierende Beziehung zwischen Subjekt und Informations-Sicherheitsattributen]. FDP_IFF.1.3 Die TSF muss die [Zuweisung: zusätzliche SFP-Regeln für Informationsflusskontrolle] durchsetzen. FDP_IFF.1.4 Die TSF muss liefern, was folgt [Zuweisung: Liste zusätzlicher SFP-Fähigkeiten]. FDP_IFF.1.5 Die TSF muss einen Informationsfluss auf Grundlage folgender Regeln explizit autorisieren: [Zuweisung: auf Sicherheitsattributen basierende Regeln, die Informationsflüsse explizit autorisieren]. FDP_IFF.1.6 Die TSF muss einen Informationsfluss auf Grundlage folgender Regeln explizit verweigern: [Zuweisung: auf Sicherheitsattributen basierende Regeln, die Informationsflüsse explizit verweigern]. Verwandte Themen: FDP_IFC.1 Teilweise Informationsflusskontrolle FMT_MSA.3 Initialisierung statischer Attribute Beispiele Ein Informationsfluss ist auf Grundlage von sicherheitsattributbasierten Regeln, die die Informationsflüsse (zu definieren) explizit verweigern, zu verweigern
Hierarchische Sicherheitsattribute	Hierarchisch zu: FDP_IFF.1 FDP_IFF.2.1 Die TSF muss die [Zuweisung: SFP für Informationsflusskontrolle] auf der Grundlage der folgenden Arten von Sicherheitsattributen von Subjekten und Informationen durchsetzen: [Zuweisung: die Mindestanzahl und die Art der Sicherheitsattribute]. FDP_IFF.2.2 Die TSF muss einen Informationsfluss zwischen einem kontrollierten Subjekt und kontrollierten Informationen über eine kontrollierte Operation erlauben, wenn die folgenden Regeln, die auf geordneten Beziehungen zwischen den Sicherheitsattributen basieren, angewendet werden: [Zuweisung: für jede Operation die geforderte auf Sicherheitsattributen basierende Beziehung zwischen Subjekt und Informations-Sicherheitsattributen]. FDP_IFF.2.3 Die TSF muss die [Zuweisung: zusätzliche SFP-Regeln für Informationsflusskontrolle] durchsetzen. FDP_IFF.2.4 Die TSF muss die [Zuweisung: Liste zusätzlicher SFP-Fähigkeiten] liefern. FDP_IFF.2.5 Die TSF muss einen Informationsfluss auf Grundlage folgender Regeln explizit autorisieren: [Zuweisung: auf Sicherheitsattributen basierende Regeln, die Informationsflüsse explizit

	autorisieren]. FDP_IFF.2.6 Die TSF muss einen Informationsfluss auf Grundlage folgender Regeln explizit verweigern: [Zuweisung: auf Sicherheitsattributen basierende Regeln, die Informationsflüsse explizit verweigern]. FDP_IFF.2.7 Die TSF muss die folgenden Beziehungen auf jedes gültige Sicherheitsattributpaar zur Informationsflusskontrolle durchsetzen: a) es gibt eine Steuerungsfunktion, die bei Vorhandensein von zwei gültigen Sicherheitsattributen bestimmt, ob die Sicherheitsattribute identisch sind, ob ein Attribut über dem anderen steht oder ob die Sicherheitsattribute nicht vergleichbar sind; und b) es gibt unter allen Sicherheitsattributen eine 'kleinste obere Schranke', so dass es bei Gültigkeit eines beliebigen Sicherheitsattributpaars ein Sicherheitsattribut gibt, das über den beiden gültigen Sicherheitsattributen steht oder diesen entspricht; und c) es gibt unter allen Sicherheitsattributen eine 'kleinste untere Schranke', so dass es bei Gültigkeit eines beliebigen Sicherheitsattributpaars ein Sicherheitsattribut gibt, das nicht über den beiden gültigen Sicherheitsattributen steht. Verwandte Themen: FDP_IFC.1 Teilweise Informationsflusskontrolle FMT_MSA.3 Initialisierung statischer Attribute Beispiele Für hierarchische Sicherheitsattribute ist ein Informationsfluss zwischen einem Subjekt und Informationen, die über eine kontrollierte Operation kontrolliert wurden, gemäß den Regeln zu erlauben, die sich auf geordnete Beziehungen zwischen Sicherheitsattributen (definieren) stützen
Hierarchische Sicherheitsattribute	Hierarchisch zu: FDP_IFF.1 FDP_IFF.2.1 Die TSF muss die [Zuweisung: SFP für Informationsflusskontrolle] auf der Grundlage der folgenden Arten von Sicherheitsattributen von Subjekten und Informationen durchsetzen: [Zuweisung: die Mindestanzahl und die Art der Sicherheitsattribute]. FDP_IFF.2.2 Die TSF muss einen Informationsfluss zwischen einem kontrollierten Subjekt und kontrollierten Informationen über eine kontrollierte Operation erlauben, wenn die folgenden Regeln, die auf geordneten Beziehungen zwischen den Sicherheitsattributen basieren, angewendet werden: [Zuweisung: für jede Operation die geforderte auf Sicherheitsattributen basierende Beziehung zwischen Subjekt und Informations-Sicherheitsattributen]. FDP_IFF.2.3 Die TSF muss die [Zuweisung: zusätzliche SFP-Regeln für Informationsflusskontrolle] durchsetzen. FDP_IFF.2.4 Die TSF muss die [Zuweisung: Liste zusätzlicher SFP-Fähigkeiten] liefern. FDP_IFF.2.5 Die TSF muss einen Informationsfluss auf Grundlage folgender Regeln explizit autorisieren: [Zuweisung: auf Sicherheitsattributen basierende Regeln, die Informationsflüsse explizit autorisieren]. FDP_IFF.2.6 Die TSF muss einen Informationsfluss auf Grundlage folgender Regeln explizit verweigern: [Zuweisung: auf

	Sicherheitsattributen basierende Regeln, die Informationsflüsse explizit verweigern]. FDP_IFF.2.7 Die TSF muss die folgenden Beziehungen auf jedes gültige Sicherheitsattributpaar zur Informationsflusskontrolle durchsetzen: a) es gibt eine Steuerungsfunktion, die bei Vorhandensein von zwei gültigen Sicherheitsattributen bestimmt, ob die Sicherheitsattribute identisch sind, ob ein Attribut über dem anderen steht oder ob die Sicherheitsattribute nicht vergleichbar sind; und b) es gibt unter allen Sicherheitsattributen eine 'kleinste obere Schranke', so dass es bei Gültigkeit eines beliebigen Sicherheitsattributpaars ein Sicherheitsattribut gibt, das über den beiden gültigen Sicherheitsattributen steht oder diesen entspricht; und c) es gibt unter allen Sicherheitsattributen eine 'kleinste untere Schranke', so dass es bei Gültigkeit eines beliebigen Sicherheitsattributpaars ein Sicherheitsattribut gibt, das nicht über den beiden gültigen Sicherheitsattributen steht. Verwandte Themen: FDP_IFC.1 Teilweise Informationsflusskontrolle FMT_MSA.3 Initialisierung statischer Attribute Beispiele Für hierarchische Sicherheitsattribute muss es eine Steuerungsfunktion geben, die bei zwei gültigen Sicherheitsattributen bestimmt, ob diese identisch sind, ob ein Attribut über dem anderen steht oder ob diese nicht vergleichbar sind
Hierarchische Sicherheitsattribute	Hierarchisch zu: FDP_IFF.1 FDP_IFF.2.1 Die TSF muss die [Zuweisung: SFP für Informationsflusskontrolle] auf der Grundlage der folgenden Arten von Sicherheitsattributen von Subjekten und Informationen durchsetzen: [Zuweisung: die Mindestanzahl und die Art der Sicherheitsattribute]. FDP_IFF.2.2 Die TSF muss einen Informationsfluss zwischen einem kontrollierten Subjekt und kontrollierten Informationen über eine kontrollierte Operation erlauben, wenn die folgenden Regeln, die auf geordneten Beziehungen zwischen den Sicherheitsattributen basieren, angewendet werden: [Zuweisung: für jede Operation die geforderte auf Sicherheitsattributen basierende Beziehung zwischen Subjekt und Informations-Sicherheitsattributen]. FDP_IFF.2.3 Die TSF muss die [Zuweisung: zusätzliche SFP-Regeln für Informationsflusskontrolle] durchsetzen. FDP_IFF.2.4 Die TSF muss die [Zuweisung: Liste zusätzlicher SFP-Fähigkeiten] liefern. FDP_IFF.2.5 Die TSF muss einen Informationsfluss auf Grundlage folgender Regeln explizit autorisieren: [Zuweisung: auf Sicherheitsattributen basierende Regeln, die Informationsflüsse explizit autorisieren]. FDP_IFF.2.6 Die TSF muss einen Informationsfluss auf Grundlage folgender Regeln explizit verweigern: [Zuweisung: auf Sicherheitsattributen basierende Regeln, die Informationsflüsse explizit verweigern]. FDP_IFF.2.7 Die TSF muss die folgenden Beziehungen auf jedes gültige Sicherheitsattributpaar zur Informationsflusskontrolle durchsetzen:

	a) es gibt eine Steuerungsfunktion, die bei Vorhandensein von zwei gültigen Sicherheitsattributen bestimmt, ob die Sicherheitsattribute identisch sind, ob ein Attribut über dem anderen steht oder ob die Sicherheitsattribute nicht vergleichbar sind; und b) es gibt unter allen Sicherheitsattributen eine 'kleinste obere Schranke', so dass es bei Gültigkeit eines beliebigen Sicherheitsattributpaars ein Sicherheitsattribut gibt, das über den beiden gültigen Sicherheitsattributen steht oder diesen entspricht; und c) es gibt unter allen Sicherheitsattributen eine 'kleinste untere Schranke', so dass es bei Gültigkeit eines beliebigen Sicherheitsattributpaars ein Sicherheitsattribut gibt, das nicht über den beiden gültigen Sicherheitsattributen steht. Verwandte Themen: FDP_IFC.1 Teilweise Informationsflusskontrolle FMT_MSA.3 Initialisierung statischer Attribute Beispiele Für hierarchische Sicherheitsattribute muss es eine 'kleinste obere Schranke' geben, so dass es bei Vorhandensein eines beliebigen gültigen Sicherheitsattributpaars ein Sicherheitsattribut gibt, das über den beiden gültigen Sicherheitsattributen steht oder diesen entspricht
Hierarchische Sicherheitsattribute	Hierarchisch zu: FDP_IFF.1 FDP_IFF.2.1 Die TSF muss die [Zuweisung: SFP für Informationsflusskontrolle] auf der Grundlage der folgenden Arten von Sicherheitsattributen von Subjekten und Informationen durchsetzen: [Zuweisung: die Mindestanzahl und die Art der Sicherheitsattribute]. FDP_IFF.2.2 Die TSF muss einen Informationsfluss zwischen einem kontrollierten Subjekt und kontrollierten Informationen über eine kontrollierte Operation erlauben, wenn die folgenden Regeln, die auf geordneten Beziehungen zwischen den Sicherheitsattributen basieren, angewendet werden: [Zuweisung: für jede Operation die geforderte auf Sicherheitsattributen basierende Beziehung zwischen Subjekt und Informations-Sicherheitsattributen]. FDP_IFF.2.3 Die TSF muss die [Zuweisung: zusätzliche SFP-Regeln für Informationsflusskontrolle] durchsetzen. FDP_IFF.2.4 Die TSF muss die [Zuweisung: Liste zusätzlicher SFP-Fähigkeiten] liefern. FDP_IFF.2.5 Die TSF muss einen Informationsfluss auf Grundlage folgender Regeln explizit autorisieren: [Zuweisung: auf Sicherheitsattributen basierende Regeln, die Informationsflüsse explizit autorisieren]. FDP_IFF.2.6 Die TSF muss einen Informationsfluss auf Grundlage folgender Regeln explizit verweigern: [Zuweisung: auf Sicherheitsattributen basierende Regeln, die Informationsflüsse explizit verweigern]. FDP_IFF.2.7 Die TSF muss die folgenden Beziehungen auf jedes gültige Sicherheitsattributpaar zur Informationsflusskontrolle durchsetzen: a) es gibt eine Steuerungsfunktion, die bei Vorhandensein von zwei gültigen Sicherheitsattributen bestimmt, ob die Sicherheitsattribute identisch sind, ob ein Attribut über dem anderen steht oder ob die Sicherheitsattribute nicht vergleichbar sind; und b) es gibt unter allen Sicherheitsattributen eine 'kleinste obere Schranke', so dass es bei Gültigkeit eines beliebigen

	Sicherheitsattributpaars ein Sicherheitsattribut gibt, das über den beiden gültigen Sicherheitsattributen steht oder diesen entspricht; und c) es gibt unter allen Sicherheitsattributen eine 'kleinste untere Schranke', so dass es bei Gültigkeit eines beliebigen Sicherheitsattributpaars ein Sicherheitsattribut gibt, das nicht über den beiden gültigen Sicherheitsattributen steht. Verwandte Themen: FDP_IFC.1 Teilweise Informationsflusskontrolle FMT_MSA.3 Initialisierung statischer Attribute Beispiele Für hierarchische Sicherheitsattribute muss es eine 'kleinste untere Schranke' geben, so dass es bei Vorhandensein eines beliebigen gültigen Sicherheitsattributpaars ein Sicherheitsattribut gibt, das nicht über den beiden Sicherheitsattributen steht
Beschränkt unzulässiger Informationsfluss	Hierarchisch zu: keiner anderen Komponente. FDP_IFF.3.1 Die TSF muss die [Zuweisung: SFP für Informationsflusskontrolle] durchsetzen, um die Kapazität von [Zuweisung: Arten unzulässiger Informationsflüsse] auf [Zuweisung: maximale Kapazität] zu beschränken. Verwandte Themen: AVA_CCA.1 Analyse versteckter Kanäle FDP_IFC.1 Teilweise Informationsflusskontrolle Beispiele Die Anwendung der Sicherheitspolitik zur Informationsflusskontrolle muss die Kapazität unzulässiger Informationsflussarten (definieren) maximal beschränken können (definieren)
Teilweise Ausschaltung unzulässiger Informationsflüsse	Hierarchisch zu: FDP_IFF.3 FDP_IFF.4.1 Die TSF muss die [Zuweisung: SFP für Informationsflusskontrolle] durchsetzen, um die Kapazität von [Zuweisung: Arten unzulässiger Informationsflüsse] auf [Zuweisung: maximale Kapazität] zu beschränken. FDP_IFF.4.2 Die TSF muss verhindern [Zuweisung: Arten unzulässiger Informationsflüsse]. Verwandte Themen: AVA_CCA.1 Analyse versteckter Kanäle FDP_IFC.1 Teilweise Informationsflusskontrolle Beispiele Zur teilweisen Ausschaltung unzulässiger Informationsflüsse muss die Anwendung der Sicherheitspolitik zur Informationsflusskontrolle bestimmte identifizierte Arten unzulässiger Informationsflüsse verhindern (definieren)
Kein unzulässiger Informationsfluss	Hierarchisch zu: FDP_IFF.4 FDP_IFF.5.1 Die TSF muss sicherstellen, dass es keinen unzulässigen Informationsfluss gibt, um zu umgehen [Zuweisung: Name der SFP für Informationsflusskontrolle]. Verwandte Themen: AVA_CCA.3 Umfassende Analyse versteckter Kanäle FDP_IFC.1 Teilweise Informationsflusskontrolle Beispiele

	Um unzulässige Informationsflüsse vollständig auszuschalten, muss die Anwendung der Sicherheitspolitik zur Informationsflusskontrolle sicherstellen, dass es keinen unzulässigen Informationsfluss gibt, der die Einrichtungen zur Kontrolle der Informationsflüsse umgeht
Kontrolle unzulässiger Informationsflüsse	Hierarchisch zu: keiner anderen Komponente. FDP_IFF.6.1 Die TSF muss die [Zuweisung: SFP für Informationsflusskontrolle] durchsetzen, um [Zuweisung: Arten unzulässiger Informationsflüsse] zu kontrollieren, wenn die [Zuweisung: maximale Kapazität] überschritten wird. Verwandte Themen: AVA_CCA.1 Analyse versteckter Kanäle FDP_IFC.1 Teilweise Informationsflusskontrolle Beispiele Mit der Sicherheitspolitik zur Informationsflusskontrolle müssen die Arten unzulässiger Informationsflüsse (definieren) kontrolliert werden können, wenn diese eine maximale Kapazität überschreiten (definieren)
FDP_ITC: Import aus einer Zone, die nicht von der TSF kontrolliert wird	
Import von Benutzerdaten ohne Sicherheitsattribute	Hierarchisch zu: keiner anderen Komponente. FDP_ITC.1.1 Die TSF muss die [Zuweisung: SFP für Zugriffskontrolle oder Informationsflusskontrolle] beim Import von unter Kontrolle der SFP stehenden Benutzerdaten von außerhalb des TSC durchsetzen. FDP_ITC.1.2 Die TSF muss die mit den Benutzerdaten verknüpften Sicherheitsattribute ignorieren, wenn diese von außerhalb des TSC importiert werden. Verwandte Themen: [FDP_ACC.1 Teilweise Zugriffskontrolle, oder FDP_IFC.1 Teilweise Informationsflusskontrolle] FMT_MSA.3 Initialisierung statischer Attribute Beispiele Bei einem Import ohne Sicherheitsattribut sind alle Sicherheitsattribute, die mit Benutzerdaten verknüpft sind, bei einem Import von außen zu ignorieren
Import von Benutzerdaten ohne Sicherheitsattribute	Hierarchisch zu: keiner anderen Komponente. FDP_ITC.1.3 Die TSF muss die folgenden Regeln beim Import unter Kontrolle der SFP stehender Benutzerdaten von außerhalb des TSC durchsetzen: [Zuweisung: zusätzliche Importkontrollregeln]. Verwandte Themen: [FDP_ACC.1 Teilweise Zugriffskontrolle, oder FDP_IFC.1 Teilweise Informationsflusskontrolle] FMT_MSA.3 Initialisierung statischer Attribute Beispiele Es sind die zusätzlichen Regeln der Sicherheitspolitik zur Importkontrolle durchzusetzen (definieren)
Import von Benutzerdaten ohne Sicherheitsattribute	Hierarchisch zu: keiner anderen Komponente. FDP_ITC.1.1 Die TSF muss die [Zuweisung: SFP für Zugriffskontrolle oder Informationsflusskontrolle] beim Import von unter Kontrolle der SFP stehenden Benutzerdaten von außerhalb des TSC durchsetzen. FDP_ITC.1.2 Die TSF muss die mit den Benutzerdaten verknüpften

	Sicherheitsattribute ignorieren, wenn diese von außerhalb des TSC importiert werden. Verwandte Themen: [FDP_ACC.1 Teilweise Zugriffskontrolle, oder FDP_IFC.1 Teilweise Informationsflusskontrolle] FMT_MSA.3 Initialisierung statischer Attribute Beispiele Beim Import von Daten von außerhalb des Sicherheitsbereichs ist die Sicherheitspolitik zur Zugriffskontrolle oder zur Informationsflusskontrolle durchzusetzen
Import von Benutzerdaten mit Sicherheitsattributen	Hierarchisch zu: keiner anderen Komponente. FDP_ITC.2.1 Die TSF muss die [Zuweisung: SFP für Zugriffskontrolle oder Informationsflusskontrolle] beim Import von unter Kontrolle der SFP stehenden Benutzerdaten von außerhalb des TSC durchsetzen. FDP_ITC.2.2 Die TSF muss die Sicherheitsattribute verwenden, die mit den importierten Benutzerdaten verknüpft sind. FDP_ITC.2.3 Die TSF muss sicherstellen, dass mit dem verwendeten Protokoll die Sicherheitsattribute mit den empfangenen Benutzerdaten unzweideutig verknüpft werden können. FDP_ITC.2.4 Die TSF muss sicherstellen, dass die Sicherheitsattribute der importierten Benutzerdaten so wie vom Sender der Benutzerdaten vorgesehen interpretiert werden. FDP_ITC.2.5 Die TSF muss beim Import von Benutzerdaten von außerhalb des TSC die folgenden Regeln durchsetzen, die von der TSC kontrolliert werden: [Zuweisung: zusätzliche Importkontrollregeln]. Verwandte Themen: [FDP_ACC.1 Teilweise Zugriffskontrolle, oder FDP_IFC.1 Teilweise Informationsflusskontrolle] [FTP_ITC.1 TSF-übergreifender gesicherter Kanal, oder FTP_TRP.1 Gesicherter Pfad] FPT_TDC.1 Elementare Konsistenz von TSF-übergreifenden TSF-Daten Beispiele Bei einem Import mit Sicherheitsattributen sind die Sicherheitsattribute, die mit den importierten Benutzerdaten verknüpft sind, zu verwenden
Import von Benutzerdaten mit Sicherheitsattributen	Hierarchisch zu: keiner anderen Komponente. FDP_ITC.2.1 Die TSF muss die [Zuweisung: SFP für Zugriffskontrolle oder Informationsflusskontrolle] beim Import von unter Kontrolle der SFP stehenden Benutzerdaten von außerhalb des TSC durchsetzen. FDP_ITC.2.2 Die TSF muss die Sicherheitsattribute verwenden, die mit den importierten Benutzerdaten verknüpft sind. FDP_ITC.2.3 Die TSF muss sicherstellen, dass mit dem verwendeten Protokoll die Sicherheitsattribute mit den empfangenen Benutzerdaten unzweideutig verknüpft werden können. FDP_ITC.2.4 Die TSF muss sicherstellen, dass die Sicherheitsattribute der importierten Benutzerdaten so wie vom Sender der Benutzerdaten vorgesehen interpretiert werden. FDP_ITC.2.5 Die TSF muss beim Import von Benutzerdaten von außerhalb des TSC die folgenden Regeln durchsetzen, die von der SFP

	kontrolliert werden: [Zuweisung: zusätzliche Importkontrollregeln]. Verwandte Themen: [FDP_ACC.1 Teilweise Zugriffskontrolle, oder FDP_IFC.1 Teilweise Informationsflusskontrolle] [FTP_ITC.1 TSF-übergreifender gesicherter Kanal, oder FTP_TRP.1 Gesicherter Pfad] FPT_TDC.1 Elementare Konsistenz von TSF-übergreifenden TSF-Daten Beispiele Bei einem Import mit Sicherheitsattributen müssen mit dem verwendeten Protokoll die Sicherheitsattribute mit den empfangenen Benutzerdaten unzweideutig verknüpft werden können
Import von Benutzerdaten mit Sicherheitsattributen	Hierarchisch zu: keiner anderen Komponente. FDP_ITC.2.1 Die TSF muss die [Zuweisung: SFP für Zugriffskontrolle oder Informationsflusskontrolle] beim Import von unter Kontrolle der SFP stehenden Benutzerdaten von außerhalb des TSC durchsetzen. FDP_ITC.2.2 Die TSF muss die Sicherheitsattribute verwenden, die mit den importierten Benutzerdaten verknüpft sind. FDP_ITC.2.3 Die TSF muss sicherstellen, dass mit dem verwendeten Protokoll die Sicherheitsattribute mit den empfangenen Benutzerdaten unzweideutig verknüpft werden können. FDP_ITC.2.4 Die TSF muss sicherstellen, dass die Sicherheitsattribute der importierten Benutzerdaten so wie vom Sender der Benutzerdaten vorgesehen interpretiert werden. FDP_ITC.2.5 Die TSF muss beim Import von Benutzerdaten von außerhalb des TSC die folgenden Regeln durchsetzen, die von der SFP kontrolliert werden: [Zuweisung: zusätzliche Importkontrollregeln]. Verwandte Themen: [FDP_ACC.1 Teilweise Zugriffskontrolle, oder FDP_IFC.1 Teilweise Informationsflusskontrolle] [FTP_ITC.1 TSF-übergreifender gesicherter Kanal, oder FTP_TRP.1 Gesicherter Pfad] FPT_TDC.1 Elementare Konsistenz von TSF-übergreifenden TSF-Daten Beispiele Bei einem Import mit Sicherheitsattributen sind die Sicherheitsattribute der importierten Benutzerdaten so wie vom Sender der Benutzerdaten vorgesehen zu interpretieren
FDP_ITT: TOE (EVG)-interner Datenfluss	
Elementarer Schutz eines internen Datenflusses	Hierarchisch zu: keiner anderen Komponente. FDP_ITT.1.1 Die TSF muss die [Zuweisung: SFP für Zugriffskontrolle oder Informationsflusskontrolle] durchsetzen, um die [Auswahl: Preisgabe, Modifizierung oder Verwendungsverlust] von Benutzerdaten bei ihrer Übertragung zwischen physisch separierten Teilen des TOE (EVG) zu verhindern. Verwandte Themen: [FDP_ACC.1 Teilweise Zugriffskontrolle, oder FDP_IFC.1 Teilweise Informationsflusskontrolle] Beispiele Die Sicherheitspolitik zur Zugriffskontrolle oder zur Informationsflusskontrolle muss Preisgabe, Modifizierung oder

	Verwendungsverlust von Daten bei ihrer Übertragung zwischen physisch separierten Teilen des Sicherheitsbereichs verhindern
Datenseparierung bei einem Datenfluss auf Grundlage von Attributen	Hierarchisch zu: FDP_ITT.1 FDP_ITT.2.1 Die TSF muss die [Zuweisung: SFP für Zugriffskontrolle oder Informationsflusskontrolle] durchsetzen, um die [Auswahl: Preisgabe, Modifizierung oder Verwendungsverlust] von Benutzerdaten bei ihrer Übertragung zwischen physisch separierten Teilen des TOE (EVG) zu verhindern. FDP_ITT.2.2 Die TSF muss die von der oder den SFP bei ihrer Übertragung zwischen physisch separierten Teilen des TOE (EVG) kontrollierten Daten auf Grundlage des folgenden Werts: [Zuweisung: Sicherheitsattribute, die eine Separierung erfordern] separieren. Verwandte Themen: [FDP_ACC.1 Teilweise Zugriffskontrolle, oder FDP_IFC.1 Teilweise Informationsflusskontrolle] Beispiele Bei einer Separierung von Daten, die auf Grundlage von Attributen übertragen wurden, sind die kontrollierten Daten, die zwischen physisch separierten Teilen des Sicherheitsbereichs übertragen werden, in Abgängigkeit der Sicherheitsattribute zu separieren, die eine Separierung erfordern
Integritätskontrolle	Hierarchisch zu: keiner anderen Komponente. FDP_ITT.3.1 Die TSF muss die [Zuweisung: SFP für Zugriffskontrolle oder Informationsflusskontrolle] durchsetzen, um die Benutzerdaten bei ihrer Übertragung zwischen physisch separierten Teilen des TOE (EVG) zu kontrollieren, um die folgenden Fehler zu erkennen: [Zuweisung: Integritätsfehler]. FDP_ITT.3.2 Bei Erkennung eines Daten-Integritätsfehlers muss die TSF [Zuweisung: die im Fall eines Integritätsfehlers einzuleitende Aktion spezifizieren]. Verwandte Themen: [FDP_ACC.1 Teilweise Zugriffskontrolle, oder FDP_IFC.1 Teilweise Informationsflusskontrolle] FDP_ITT.1 Elementarer Schutz einer internen Übertragung Beispiele Integritätsfehler sind bei der Übertragung von Benutzerdaten zwischen physisch separierten Teilen des Sicherheitsbereichs zu erkennen
Integritätskontrolle	Hierarchisch zu: keiner anderen Komponente. FDP_ITT.3.1 Die TSF muss die [Zuweisung: SFP für Zugriffskontrolle oder Informationsflusskontrolle] durchsetzen, um die Benutzerdaten bei ihrer Übertragung zwischen physisch separierten Teilen des TOE (EVG) zu kontrollieren, um die folgenden Fehler zu erkennen: [Zuweisung: Integritätsfehler]. FDP_ITT.3.2 Bei Erkennung eines Daten-Integritätsfehlers muss die TSF [Zuweisung: die im Fall eines Integritätsfehlers einzuleitende Aktion spezifizieren]. Verwandte Themen: [FDP_ACC.1 Teilweise Zugriffskontrolle, oder FDP_IFC.1 Teilweise Informationsflusskontrolle] FDP_ITT.1 Elementarer Schutz einer internen Übertragung

	Beispiele Werden Integritätsfehler erkannt, sind spezielle Aktionen (definieren) einzuleiten
Integritätskontrolle auf Grundlage von Attributen	Hierarchisch zu: FDP_ITT.3 FDP_ITT.4.1 Die TSF muss die [Zuweisung: SFP für Zugriffskontrolle oder Informationsflusskontrolle] durchsetzen, um die Benutzerdaten bei ihrer Übertragung zwischen physisch separierten Teilen des TOE (EVG) zu kontrollieren, um die folgenden Fehler [Zuweisung: Integritätsfehler] auf Grundlage der folgenden Attribute: [Zuweisung: Sicherheitsattribute, die getrennte Übertragungskanäle erfordern] zu erkennen. FDP_ITT.4.2 Bei Erkennung eines Daten-Integritätsfehlers muss die TSF [Zuweisung: die im Fall eines Integritätsfehlers einzuleitende Aktion spezifizieren]. Verwandte Themen: [FDP_ACC.1 Teilweise Zugriffskontrolle, oder FDP_IFC.1 Teilweise Informationsflusskontrolle] FDP_ITT.2 Separierung von Daten bei einem attributabhängigen Datenfluss Beispiele FDP_ITT.3.1: Integritätskontrolle auf Grundlage von Sicherheitsattributen, die separate Datenflusskanäle erfordern
FDP_RIP: Schutz der Restinformationen	
Teilweiser Schutz der Restinformationen	Hierarchisch zu: keiner anderen Komponente. FDP_RIP.1.1 Die TSF muss sicherstellen, dass die Bereitstellung aller Informationen, die vorher in einer Ressource enthalten waren, bei [Auswahl: Bereitstellung der Ressource an, Beendigung der Bereitstellung der Ressource der] folgende/n Objekte aufgehoben wird: [Zuweisung: Objektliste]. Verwandte Themen: Keine verwandten Themen BeispieleFür einen teilweisen Schutz der Restinformationen ist die Verfügbarkeit aller Informationen, die vorher in einer Ressource enthalten waren, bei der Bereitstellung oder Beendigung der Bereitstellung der Objektressource (definieren) aufzuheben
Vollständiger Schutz der Restinformationen	FDP_RIP.2.1 Die TSF muss sicherstellen, dass die Verfügbarkeit aller Informationen, die vorher in einer Ressource enthalten waren, bei [Auswahl: Bereitstellung der Ressource an, Beendigung der Bereitstellung der Ressource von] alle/n Objekten aufgehoben wird. Verwandte Themen: Keine verwandten Themen Beispiele Für einen vollständigen Schutz der Restinformationen ist die Verfügbarkeit aller Information, die vorher in einer Ressource enthalten war, bei der Bereitstellung oder Beendigung der Bereitstellung aller Objektressourcen aufzuheben
FDP_ROL: Annullierung	
Elementare Annullierung	Hierarchisch zu: keiner anderen Komponente. FDP_ITC.1.1 Die TSF muss die [Zuweisung: SFP für Zugriffskontrolle oder Informationsflusskontrolle] durchsetzen, um die Annullierung der [Zuweisung: Operationsliste] auf die [Zuweisung: Objektliste] zu

	erlauben. FDP_ROL.1.2 Die TSF muss die Annullierung der Operationen in den [Zuweisung: Grenzen, in denen die Annullierung durchgeführt werden kann] erlauben. Verwandte Themen: [FDP_ACC.1 Teilweise Zugriffskontrolle, oder FDP_IFC.1 Teilweise Informationsflusskontrolle] Beispiele Für elementare Annullierungen muss die Annullierung von Operationen (definieren) auf identifizierte Objekte (definieren) erlaubt sein
Elementare Annullierung	Hierarchisch zu: keiner anderen Komponente. FDP_ITC.1.1 Die TSF muss die [Zuweisung: SFP für Zugriffskontrolle oder Informationsflusskontrolle] durchsetzen, um die Annullierung der [Zuweisung: Operationsliste] auf die [Zuweisung: Objektliste] zu erlauben. FDP_ROL.1.2 Die TSF muss die Annullierung der Operationen in den [Zuweisung: Grenzen, in denen die Annullierung durchgeführt werden kann] erlauben. Verwandte Themen: [FDP_ACC.1 Teilweise Zugriffskontrolle, oder FDP_IFC.1 Teilweise Informationsflusskontrolle] Beispiele Bei elementaren Annullierungen muss die Annullierung der Operationen in den Grenzen erlaubt werden, in denen die Annullierung durchgeführt werden kann (definieren)
Fortgeschrittene Annullierung	Hierarchisch zu: FDP_ROL.1 FDP_ROL.2.1 Die TSF muss die [Zuweisung: SFP für Zugriffskontrolle oder Informationsflusskontrolle] durchsetzen, um die Annullierung aller Operationen auf die [Zuweisung: Objektliste] zu erlauben. FDP_ROL.2.2 Die TSF muss die Annullierung für die Operationen in den [Zuweisung: Grenzen, in denen die Annullierung durchgeführt werden kann] erlauben. Verwandte Themen: [FDP_ACC.1 Teilweise Zugriffskontrolle, oder FDP_IFC.1 Teilweise Informationsflusskontrolle] Beispiele Für fortgeschrittene Annullierungen müssen alle Operationen auf identifizierte Objekte (definieren) annulliert werden können
FDP_SDI: Integrität der gespeicherten Daten	
Kontrolle der Integrität der gespeicherten Daten	Hierarchisch zu: keiner anderen Komponente. FDP_SDI.1.1 Die TSF muss die innerhalb des TSC gespeicherten Benutzerdaten bei der Suche von [Zuweisung: Integritätsfehler] auf alle Objekte auf Grundlage der folgenden Attribute [Zuweisung: Attribute der Benutzerdaten] kontrollieren. Verwandte Themen: Keine Abhängigkeit Beispiele

	Die gespeicherten Benutzerdaten sind bei der Suche von Integritätsfehlern auf alle Objekte auf Grundlage der Attribute der Benutzerdaten (definieren) zu kontrollieren
Kontrolle der Integrität der gespeicherten Daten und einzuleitende Aktionen	Hierarchisch zu: FDP_SDI.1 FDP_SDI.2.1 Die TSF muss die innerhalb der TSC gespeicherten Benutzerdaten bei der Suche von [Zuweisung: Integritätsfehler] auf alle Objekte auf Grundlage der folgenden Attribute [Zuweisung: Attribute der Benutzerdaten] kontrollieren. FDP_SDI.2.2 Wird ein Integritätsfehler erkannt, muss die TSF [Zuweisung: einzuleitende Aktionen] Verwandte Themen: Keine Abhängigkeit Beispiele Wird ein Integritätsfehler erkannt, sind spezielle Aktionen (definieren) einzuleiten
FDP_UCT: Schutz der Vertraulichkeit der Benutzerdaten bei einem TSF-übergreifenden Datenfluss	
Elementare Vertraulichkeit bei einem Datenaustausch	Hierarchisch zu: keiner anderen Komponente. FDP_UTC.1.1 Die TSF muss die [Zuweisung: SFP für Zugriffskontrolle oder Informationsflusskontrolle] durchsetzen, um Objekte so [Auswahl: übertragen, empfangen] zu können, dass sie vor einer unerlaubten Preisgabe geschützt sind. Verwandte Themen: [FTP_ITC.1 TSF-übergreifender gesicherter Kanal, oder FTP_TRP.1 Gesicherter Pfad] [FDP_ACC.1 Teilweise Zugriffskontrolle, oder FDP_IFC.1 Teilweise Informationsflusskontrolle] Beispiele Die Objekte sind so zu übertragen und zu empfangen, dass sie vor unerlaubter Preisgabe geschützt sind
FDP_UIT: Schutz der Integrität der Benutzerdaten bei einer TSF-übergreifenden Übertragung	
Integrität bei einem Datenaustausch	Hierarchisch zu: keiner anderen Komponente. FDP_UIT.1.1 Die TSF muss die [Zuweisung: SFP für Zugriffskontrolle oder Informationsflusskontrolle] durchsetzen, um Benutzerdaten so [Auswahl: übertragen, erhalten] zu können, dass sie vor Fehlern bei der [Auswahl: Änderung, Löschung, Einfügung, Playback] geschützt sind. Verwandte Themen: [FDP_ACC.1 Teilweise Zugriffskontrolle, oder FDP_IFC.1 Teilweise Informationsflusskontrolle] [FTP_ITC.1 TSF-übergreifender gesicherter Kanal, oder FTP_TRP.1 Gesicherter Pfad] Beispiele Die Benutzerdaten sind so zu übertragen und zu empfangen, dass sie vor Änderungen, Löschungen, Einfügungen oder Playback geschützt sind
Integrität bei einem Datenaustausch	Hiérarchique à : aucun autre composant. FDP_UIT.1.2 La TSF doit pouvoir déterminer lors de la réception des données de l'utilisateur si [sélection : une modification, une suppression, une insertion, un rejeu] a eu lieu.

	Dépendances : [FDP_ACC.1 Contrôle d'accès partiel, ou FDP_IFC.1 Contrôle de flux d'information partiel] [FTP_ITC.1 Canal de confiance inter-TSF, ou FTP_TRP.1 Chemin de confiance] Exemples Lors de la réception des données de l'utilisateur, il doit être possible de déterminer si une modification, une suppression, une insertion ou un rejeu a eu lieu Hierarchisch zu: keiner anderen Komponente. FDP_UIT.1.2 Die TSF muss beim Empfang von Benutzerdaten feststellen können, ob [Auswahl: eine Änderung, eine Löschung, eine Einfügung, ein Playback] stattgefunden hat. Verwandte Themen: [FDP_ACC.1 Teilweise Zugriffskontrolle, oder FDP_IFC.1 Teilweise Informationsflusskontrolle] [FTP_ITC.1 TSF-übergreifender gesicherter Kanal, oder FTP_TRP.1 Gesicherter Pfad] Beispiele Beim Empfang von Benutzerdaten muss es möglich sein festzustellen, ob eine Änderung, eine Löschung, eine Einfügung oder ein Playback stattgefunden hat
Senderbedingte Wiederherstellung bei einem Datenaustausch	Hierarchisch zu: keiner anderen Komponente. FDP_UIT.2.1 Die TSF muss die [Zuweisung: SFP für Zugriffskontrolle oder Informationsflusskontrolle] durchsetzen, um die Daten ausgehend von [Auswahl: Liste wiederherstellungskompatibler Fehler] mit Hilfe des gesicherten IT-Produkts am Ausgangspunkt der Sendung wiederherstellen zu können. Verwandte Themen: [FDP_ACC.1 Teilweise Zugriffskontrolle, oder FDP_IFC.1 Teilweise Informationsflusskontrolle] FDP_UIT.1 Integrität bei einem Datenaustausch FTP_ITC.1 TSF-übergreifender gesicherter Kanal Beispiele Bei einer Wiederherstellung durch den Sender müssen die Daten ausgehend von wiederherstellungskompatiblen Fehlern (definieren) mit Hilfe des gesicherten Systems am Ausgangspunkt der Sendung wiederhergestellt werden können
Empfängerbedingte Wiederherstellung bei einem Datenaustausch	Hierarchisch zu: FDP_UIT.2 FDP_UIT.3.1 Die TSF muss die [Zuweisung: SFP für Zugriffskontrolle oder Informationsflusskontrolle] durchsetzen, um die Daten ausgehend von [Zuweisung: Fehlerliste, die eine Wiederherstellung erlaubt] ohne jedwede Hilfe des gesicherten IT-Produkts am Ausgangspunkt der Sendung wiederherstellen zu können. Verwandte Themen: [FDP_ACC.1 Teilweise Zugriffskontrolle, oder FDP_IFC.1 Teilweise Informationsflusskontrolle] FDP_UIT.1 Integrität bei einem Datenaustausch FTP_ITC.1 TSF-übergreifender gesicherter Kanal Beispiele

	Bei einer Wiederherstellung durch den Empfänger müssen die Daten ausgehend von Fehlern, die eine Wiederherstellung erlauben (definieren), ohne jedwede Hilfe des gesicherten Systems am Ausgangspunkt der Sendung wiederhergestellt werden können

3.1.5 FIA : Identifikation und Authentisierung

FIA_AFL: Erfolglose Authentisierungen	
Management einer Authentisierungsstörung	Hierarchisch zu: keiner anderen Komponente. FIA_AFL.1.1 Die TSF muss erkennen, wenn [Zuweisung: Anzahl] erfolglose Authentisierungsversuche im Zusammenhang mit [Zuweisung: Liste von Ereignissen, die mit der Authentisierung verbunden sind] stattgefunden haben. Verwandte Themen: FIA_UAU.1 Zeitpunkt der Authentisierung Beispiele Das System muss erkennen, wenn eine Anzahl (definieren) erfolgloser Authentisierungsversuche im Zusammenhang mit Ereignissen, die mit der Authentisierung verbunden sind (definieren), stattgefunden haben
Management einer Authentisierungsstörung	Hierarchisch zu: keiner anderen Komponente. FIA_AFL.1.2 Wenn die festgelegte Anzahl erfolgloser Identifikationsversuche erreicht oder überschritten ist, muss die TSF [Zuweisung: Aktionsliste]. Verwandte Themen: FIA_UAU.1 Zeitpunkt der Authentisierung Beispiele Wenn die festgelegte Anzahl erfolgloser Authentisierungsversuche erreicht oder überschritten ist, sind spezielle Aktionen (definieren) einzuleiten
FIA_ATD: Definition der Benutzerattribute	
Definition der Attribute eines Benutzers	Hierarchisch zu: keiner anderen Komponente. FIA_ATD.1.1 Die TSF muss die folgende Liste mit Sicherheitsattributen, die zu individuellen Benutzern gehören [Zuweisung: Liste der Sicherheitsattribute], pflegen. Verwandte Themen: Keine Keine verwandten Themen Beispiele Es ist eine Liste mit Sicherheitsattributen, die zu individuellen Benutzern gehören, zu pflegen (definieren)
FIA_SOS: Spezifikation von Geheimnissen	
Prüfung von Geheimnissen	Hierarchisch zu: keiner anderen Komponente. FIA_SOS.1.1 Die TSF muss einen Mechanismus anbieten, um Geheimnisse zu generieren, die [Zuweisung: eine Metrik einer bestimmten Qualität] entsprechen. Verwandte Themen: Keine verwandten Themen Beispiele

	Es muss ein Mechanismus zur Verfügung stehen, um Geheimnisse zu generieren, die einer Metrik einer bestimmten Qualität (definieren) entsprechen
Generierung von Geheimnissen durch die TSF	Hierarchisch zu: keiner anderen Komponente. FIA_SOS.2.1 Die TSF muss einen Mechanismus anbieten, um Geheimnisse zu generieren, die einer [Zuweisung: eine Metrik einer bestimmten Qualität] entsprechen. Verwandte Themen: Keine verwandten Themen Beispiele Es muss ein Mechanismus zur Verfügung stehen, um Geheimnisse zu generieren, die einer Metrik einer bestimmten Qualität (definieren) entsprechen
Generierung von Geheimnissen durch die TSF	Hierarchisch zu: keiner anderen Komponente. FIA_SOS.2.2 Die TSF muss in der Lage sein, die Verwendung der von ihr generierten Geheimnisse für [Zuweisung: Liste der Funktionen der TSF] zur Pflicht zu machen. Verwandte Themen: Keine verwandten Themen Beispiele Die Verwendung von im Rahmen von FIA_SOS.2.1 generierten Geheimnissen muss für identifizierte Funktionen (definieren) zur Pflicht gemacht werden können
FIA_UAU: Authentisierung des Benutzers	
Zeitpunkt der Authentisierung	Hierarchisch zu: keiner anderen Komponente. FIA_UAU.1.1 Die TSF muss die Ausführung von [Zuweisung: Liste der von der TSF vermittelten Aktionen] für den Benutzer erlauben, bevor er authentisiert wird. Verwandte Themen: FIA_UID.1 Zeitpunkt der Identifikation Beispiele Bestimmte, vom System für den Benutzer vermittelte Aktionen (definieren) müssen erlaubt werden, bevor eine Authentisierung des Benutzers erfolgt
Zeitpunkt der Authentisierung	Hierarchisch zu: keiner anderen Komponente. FIA_UAU.1.2 Die TSF muss erfordern, dass jeder Benutzer erfolgreich authentisiert wird, bevor diesem jegliche andere TSF-vermittelte Aktion erlaubt wird. Verwandte Themen: FIA_UID.1 Zeitpunkt der Identifikation Beispiele Jeder Benutzer ist erfolgreich zu authentisieren, bevor diesem andere vom System vermittelte Aktionen erlaubt werden, wobei die von FIA_UAU.1.1 definierten Aktionen ausgenommen sind
Fälschungssichere Authentisierung	Hierarchisch zu: keiner anderen Komponente. FIA_UAU.3.1 Die TSF muss die Verwendung von Authentisierungsdaten [Auswahl: erkennen, verhindern], die von einem beliebigen Benutzer der TSF gefälscht wurden.

	Verwandte Themen: Keine verwandten Themen Beispiele Die Verwendung von Authentisierungsdaten, die von einem beliebigen Benutzer gefälscht wurden, ist zu erkennen und zu verhindern
Fälschungssichere Authentisierung	Hierarchisch zu: keiner anderen Komponente. FIA_UAU.3.2 Die TSF muss die Verwendung von Authentisierungsdaten [Auswahl: erkennen, verhindern], die von jedem anderen Benutzer der TSF kopiert wurden. Verwandte Themen: Keine verwandten Themen Beispiele Die Verwendung von Authentisierungsdaten, die von einem anderen Benutzer als demjenigen, dem diese zugewiesen sind, kopiert wurden, ist zu erkennen und zu verhindern
Mechanismen zur einmaligen Authentisierung	Hierarchisch zu: keiner anderen Komponente. FIA_UAU.4.1 Die TSF muss die Wiederverwendung von Authentisierungsdaten verhindern, die mit [Zuweisung: identifizierter/n Authentisierungsmechanismus/en] verbunden sind. Verwandte Themen: Keine verwandten Themen Beispiele Bei einer einmaligen Authentisierung ist die Wiederverwendung der Authentisierungsdaten, die mit identifizierten Authentisierungsmechanismen (definieren) verbunden sind, zu verhindern
Mechanismen zur mehrmaligen Authentisierung	Hierarchisch zu: keiner anderen Komponente. FIA_UAU.5.1 Die TSF muss [Zuweisung: Liste der Mechanismen zur mehrmaligen Authentisierung] liefern, um zur Authentisierung des Benutzers beizutragen. Verwandte Themen: Keine verwandten Themen Beispiele Bei Mechanismen zur mehrmaligen Authentisierung sind Mechanismen zur mehrmaligen Authentisierung (definieren) bereitzustellen, um zur Authentisierung des Benutzers beizutragen
Mechanismen zur mehrmaligen Authentisierung	Hierarchisch zu: keiner anderen Komponente. FIA_UAU.5.2 Die TSF muss die angekündigte Identität jedes Benutzers gemäß [Zuweisung: Regeln, die beschreiben, wie Mechanismen zur mehrmaligen Authentisierung die Authentisierung bereitstellen] authentisieren. Verwandte Themen: Keine verwandten Themen Beispiele Bei Mechanismen zur mehrmaligen Authentisierung ist die angekündigte Identität jedes Benutzers gemäß den Regeln zu authentisieren, die beschreiben, wie die Mechanismen zur mehrmaligen Authentisierung die Authentisierung (definieren) bereitstellen

Erneute Authentisierung	Hierarchisch zu: keiner anderen Komponente. FIA_UAU.6.1 Die TSF muss den Benutzer unter den folgenden Bedingungen erneut authentisieren [Zuweisung: Liste der Bedingungen, für die eine erneute Authentisierung gefordert wird]. Verwandte Themen: Keine verwandten Themen Beispiele Der Benutzer muss unter den speziellen Bedingungen erneut authentisiert werden, für die eine erneute Authentisierung gefordert wird (definieren)
Authentisierung mit geschützten Feed-back	Hierarchisch zu: keiner anderen Komponente. FIA_UAU.7.1 Die TSF darf dem Benutzer [Zuweisung: Liste der zurückgesendeten Informationen] nur dann liefern, wenn die Authentisierung läuft. Verwandte Themen: FIA_UAU.1 Zeitpunkt der Authentisierung Beispiele Dem Benutzer können bei laufender Authentisierung nur bestimmte spezielle Informationen (definieren) geliefert werden
FIA_UID: Benutzeridentifikation	
Zeitpunkt der Identifikation	Hierarchisch zu: keiner anderen Komponente. FIA_UID.1.1 Die TSF muss die Ausführung von [Zuweisung: Liste der von der TSF vermittelten Aktionen] für den Benutzer erlauben, bevor dieser identifiziert wird. Verwandte Themen: Keine verwandten Themen Beispiele Bestimmte, vom System für den Benutzer vermittelte Aktionen (definieren) müssen erlaubt werden, bevor eine Identifikation des Benutzers erfolgt
Zeitpunkt der Identifikation	Hierarchisch zu: keiner anderen Komponente. FIA_UID.1.2 Die TSF muss erfordern, dass jeder Benutzer erfolgreich identifiziert wurde, bevor für diesen jegliche andere TSF-vermittelte Aktion erlaubt werden. Verwandte Themen: Keine verwandten Themen Beispiele Jeder Benutzer ist erfolgreich zu identifizieren, bevor diesem jegliche andere vom System vermittelte Aktion erlaubt wird, wobei die von FIA_UID.1.1 definierten Aktionen davon ausgenommen sind
FIA_USB: Verbindung Benutzer-Subjekt	
Verbindungen Benutzer-Subjekt	Hierarchisch zu: keiner anderen Komponente. FIA_USB.1.1 Die TSF muss die geeigneten Sicherheitsattribute des Benutzers mit Subjekten verbinden, die für diesen Benutzer handeln. Verwandte Themen: FIA_ATD.1 Definition der Benutzerattribute Beispiele

	Die geeigneten Sicherheitsattribute des Benutzers sind mit Subjekten zu verbinden, die für diesen Benutzer handeln

3.1.6 FMT : Sicherheitsmanagement

FMT_MOF: Management des Verhaltens der Sicherheitsfunktionen	
Management des Verhaltens der Sicherheitsfunktionen	Hierarchisch zu: keiner anderen Komponente. FMT_MOF.1.1 Die TSF muss die Fähigkeit zum [Auswahl: Feststellen des Verhaltens von, Deaktivieren, Aktivieren, Modifizieren des Verhaltens] der Funktionen [Zuweisung: Liste der Funktionen] auf [Zuweisung: die autorisierten identifizierten Rollen] beschränken. Verwandte Themen: FMT_SMR.1 Sicherheitsrollen Beispiele Die Fähigkeit zur Feststellung des Verhaltens, Deaktivieren, Aktivieren oder Modifizieren des Verhaltens identifizierter Funktionen (definieren) ist auf die autorisierten identifizierten Rollen zu beschränken (definieren)
FMT_MSA: Management der Sicherheitsattribute	
Management der Sicherheitsattribute	Hierarchisch zu: keiner anderen Komponente. FMT_MSA.1.1 Die TSF muss die [Zuweisung: SFP für Zugriffskontrolle, SFP für Informationsflusskontrolle] zur Beschränkung der Fähigkeit [Auswahl: Standardvorgabe ändern, Abfragen, Modifizieren, Löschen, [Zuweisung: andere Operationen]] des Sicherheitsattributs [Zuweisung: Liste der Sicherheitsattribute] auf [Zuweisung: die autorisierten identifizierte Rollen] durchsetzen. Verwandte Themen: [FDP_ACC.1 Teilweise Zugriffskontrolle, oder FDP_IFC.1 Teilweise Informationsflusskontrolle] FMT_SMR.1 Sicherheitsrollen Beispiele Die Fähigkeit, die Standardvorgabe zu ändern, abzufragen, zu modifizieren, zu löschen und andere identifizierte Operationen (definieren) bestimmter Sicherheitsattribute (definieren) durchzuführen, muss auf die autorisierten identifizierten Rollen (definieren) beschränkt bleiben
Sichere Sicherheitsattribute	Hierarchisch zu: keiner anderen Komponente. FMT_MSA.2.1 Die TSF muss sicherstellen, dass nur sichere Werte für Sicherheitsattribute akzeptiert werden. Verwandte Themen: ADV_SPM.1 Informelles EVG-Sicherheitsmodell [FDP_ACC.1 Teilweise Zugriffskontrolle, oder FDP_IFC.1 Teilweise Informationsflusskontrolle] FMT_MSA.1 Management der Sicherheitsattribute FMT_SMR.1 Sicherheitsrollen Beispiele Für die Sicherheitsattribute dürfen nur sichere Werte akzeptiert werden
Initialisierung statischer Attribute	Hierarchisch zu: keiner anderen Komponente. FDP_MSA.3.1 Die TSF muss die [Zuweisung: SFP für Zugriffskontrolle, SFP für Informationsflusskontrolle] zur Bereitstellung von vorgegebenen Standardwerten mit [Auswahl: einschränkenden, freizügigen, anderen Eigenschaften] Eigenschaften für Sicherheitsattribute, die zur Durchsetzung

	der SFP benutzt werden, durchsetzen. Verwandte Themen: FMT_MSA.1 Management der Sicherheitsattribute FMT_SMR.1 Sicherheitsrollen Beispiele Für Sicherheitsattribute, die zur Durchsetzung der Sicherheitspolitik verwendet werden, sind einschränkende, freizügige oder andere Eigenschaften (definieren) betreffende Standardwerte zu liefern
Initialisierung statischer Attribute	Hierarchisch zu: keiner anderen Komponente. FMT_MSA.3.2 Die TSF muss [Zuweisung: autorisierte identifizierte Rollen] gestatten, bei der Erzeugung eines Objekts oder von Informationen alternative Anfangswerte zu spezifizieren, die die vorgegebenen Standardwerte ersetzen. Verwandte Themen: FMT_MSA.1 Management der Sicherheitsattribute FMT_SMR.1 Sicherheitsrollen Beispiele Die autorisierten identifizierten Rollen (definieren) müssen als Ersatz von Standardwerten alternative Anfangswerte spezifizieren können, wenn ein Objekt oder eine Information geschaffen wird
FMT_MTD: Management der TSF-Daten	
Management der TSF-Daten	Hierarchisch zu: keiner anderen Komponente. FMT_MTD.1.1 Die TSF muss die Fähigkeit zum [Auswahl: Standardvorgabe ändern, Abfragen, Modifizieren, Löschen, Zurücksetzen [Zuweisung: andere Operationen]] von [Zuweisung: Liste von TSF-Daten] auf [Zuweisung: die autorisierten identifizierten Rollen] beschränken. Verwandte Themen: FMT_SMR.1 Sicherheitsrollen Beispiele Die Fähigkeit, den Standardwert zu ändern, abzufragen, zu modifizieren, zu löschen, zurückzusetzen und andere identifizierte Operationen (definieren) bestimmter identifizierter Daten (definieren) durchzuführen, muss auf autorisierte Rollen (definieren) beschränkt bleiben
Management der Grenzwerte der TSF-Daten	Hierarchisch zu: keiner anderen Komponente. FMT_MTD.2.1 Die TSF muss die Spezifikation der Grenzwerte der [Zuweisung: Datenliste der TSF] auf [Zuweisung: die autorisierten identifizierten Rollen] beschränken. Verwandte Themen: FMT_MTD.1 Management der TSF-Daten FMT_SMR.1 Sicherheitsrollen Beispiele Die Spezifikation von Grenzwerten bestimmter Daten (definieren) ist auf die autorisierten identifizierten Rollen (definieren) zu beschränken
Management der Grenzwerte der TSF-Daten	Hierarchisch zu: keiner anderen Komponente. FMT_MTD.2.2 Die TSF muss die folgenden Aktionen einleiten, wenn die TSF-Daten die angegebenen Grenzwerte erreichen oder diese überschreiten [Zuweisung: einzuleitende Aktionen]. Verwandte Themen: FMT_MTD.1 Management der TSF-Daten

	FMT_SMR.1 Sicherheitsrollen Beispiele Wenn die Daten die von FMT_MTD.2.2 angegebenen Grenzwerte erreichen oder überschreiten, sind spezielle Aktionen (definieren) einzuleiten
Sichere TSF-Daten	Hierarchisch zu: keiner anderen Komponente. FMT_MTD.3.1 Die TSF muss sicherstellen, dass nur sichere Werte für TSF-Daten akzeptiert werden. Verwandte Themen: ADV_SPM.1 Informelles EVG-Sicherheitsmodell FMT_MTD.1 Mangement der TSF-Daten Beispiele Als Systemdaten dürfen nur sichere Werte akzeptiert werden
FMT_REV: Widerruf	
Widerruf	Hierarchisch zu: keiner anderen Komponente. FMT_REV.1.1 Die TSF muss die Fähigkeit, Sicherheitsattribute zu widerrufen, die mit [Auswahl: Benutzer, Subjekte, Objekte, andere ergänzende Ressourcen] innerhalb des TSC verknüpft sind, auf [Zuweisung: die autorisierten identifizierten Rollen] beschränken Verwandte Themen: FMT_SMR.1 Sicherheitsrollen Beispiele Nur die autorisierten identifizierten Rollen (definieren) dürfen die Fähigkeit haben, Sicherheitsattribute, die mit Benutzern, Subjekten, Objekten und anderen ergänzenden Ressourcen (definieren) innerhalb des Systems verknüpft sind, zu widerrufen
Widerruf	Hierarchisch zu: keiner anderen Komponente. FMT_REV.1.2 Die TSF muss die Regeln [Zuweisung: Spezifikation der Widerrufsregeln] umsetzen. Verwandte Themen: FMT_SMR.1 Sicherheitsrollen Beispiele Es sind spezielle Widerrufsregeln (definieren) umzusetzen
FMT_SAE: Ablauf der Sicherheitsattribute	
Zeitlich beschränkte Autorisierung	Hierarchisch zu: keiner anderen Komponente. FMT_SAE.1.1 Die TSF muss die Fähigkeit, ein Ablaufdatum für [Zuweisung: Liste der Sicherheitsattribute, für die das Ablaufdatum durchzusetzen ist] zu spezifizieren, auf [Zuweisung: die autorisierten identifizierten Rollen] beschränken. Verwandte Themen: FMT_SMR.1 Sicherheitsrollen FPT_STM.1 Zuverlässige Tag- und Zeiteinstellung Beispiele Nur die autorisierten identifizierten Rollen (definieren) dürfen die Fähigkeit haben, für bestimmte Sicherheitsattribute, die ein Ablaufdatum (definieren) benötigen, ein Ablaufdatum zu spezifizieren
Zeitlich beschränkte	Hierarchisch zu: keiner anderen Komponente.

Autorisierung	FMT_SAE.1.2 Die TSF muss für jedes dieser Sicherheitsattribute in der Lage sein, [Zuweisung: Liste der für jedes Sicherheitsattribut einzuleitenden Aktionen], nachdem das Ablaufdatum des Sicherheitsattributs überschritten ist. Verwandte Themen: FMT_SMR.1 Sicherheitsrollen FPT_STM.1 Zuverlässige Tag- und Zeiteinstellung Beispiele Nach Überschreitung des Ablaufdatums des Sicherheitsattributs müssen bestimmte spezielle Aktionen (für jedes von FMT_SAE.1.1 identifizierte Attribut zu definieren) eingeleitet werden können
FMT_SMR: Rollen für das Sicherheitsmanagement	
Sicherheitsrollen	Hierarchisch zu: keiner anderen Komponente. FMT_SMR.1.1 Die TSF muss die Rollen [Zuweisung: die autorisierten identifizierten Rollen] auf dem neuesten Stand halten. FMT_SMR.1.2 Die TSF muss Benutzer mit Rollen verknüpfen können. Verwandte Themen: FIA_UID.1 Zeitpunkt der Identifikation Beispiele Die identifizieren erlaubten Rollen (definieren) sind auf dem neuesten Stand zu halten
Sicherheitsrollen	Hierarchisch zu: keiner anderen Komponente. FMT_SMR.1.1 Die TSF muss die Rollen [Zuweisung: die autorisierten identifizierten Rollen] auf dem neuesten Stand halten. FMT_SMR.1.2 Die TSF muss Benutzer mit Rollen verknüpfen können. Verwandte Themen: FIA_UID.1 Zeitpunkt der Identifikation Beispiele Es muss möglich sein, Benutzern mit Rollen verknüpfen zu können
Einschränkungen bei Sicherheitsrollen	Hierarchisch zu: FMT_SMR.1 FMT_SMR.2.1 Die TSF muss die Rollen [Zuweisung: die autorisierten identifizierten Rollen] erhalten. FMT_SMR.2.2 Die TSF muss Benutzer mit Rollen verknüpfen können. FMT_SMR.2.3 Die TSF muss sicherstellen, dass die Bedingungen [Zuweisung: Bedingungen für die verschiedenen Rollen] erfüllt werden. Verwandte Themen: FIA_UID.1 Zeitpunkt der Identifikation Beispiele Bei Einschränkungen bei den Sicherheitsrollen sind die mit den verschiedenen Rollen (definieren) verknüpften Bedingungen zu erfüllen
Annahme von Rollen	Hierarchisch zu: keiner anderen Komponente. FMT_SMR.3.1 Die TSF muss für die Übernahme der folgenden Rollen [Zuweisung: Rollen] eine ausdrückliche Anforderung anfordern.

	Verwandte Themen: FMT_SMR.1 Sicherheitsrollen Beispiele Die Übernahme bestimmter identifizierter Rollen (definieren) muss Gegenstand einer ausdrücklichen Anforderung sein

3.1.7 FPR : Schutz der Privatsphäre

FPR_ANO: Anonymität	
Anonymität	Hierarchisch zu: keiner anderen Komponente. FPR_ANO.1.1 Die TSF muss sicherstellen, dass [Zuweisung: alle Benutzer oder Subjekte] den richtigen Namen des Benutzers, der der [Zuweisung: Liste der Subjekte, Operationen oder Objekte] zugeordnet ist, nicht bestimmen können. Verwandte Themen: Keine verwandten Themen Beispiele Benutzer oder Subjekte (definieren) dürfen den richtigen Namen des Benutzers nicht bestimmen können, der Subjekten, Operationen oder identifizierten Objekten (definieren) zugeordnet ist
Anonymität ohne Informationsanforderung	Hierarchisch zu: FPR_ANO.1 FPR_ANO.2.1 Die TSF muss sicherstellen, dass [Zuweisung: alle Benutzer oder Subjekte] den richtigen Namen des Benutzers, der der [Zuweisung: Liste der Subjekte, Operationen oder Objekte] zugeordnet ist, nicht bestimmen können. FIA_ANO.2.2 Die TSF muss [Zuweisung: Liste der Dienste] an [Zuweisung: Liste der Subjekte] liefern, ohne einen beliebigen Bezug auf den richtigen Namen des Benutzers zu beanspruchen. Verwandte Themen: Keine verwandten Themen Beispiele Für Anonymität ohne Anforderung einer Information müssen bestimmten Dienste (definieren) bestimmte Subjekte (definieren) liefern, ohne einen Bezug auf den richtigen Namen des Benutzers zu beanspruchen
FPR_PSE: Möglichkeit, unter einem Pseudonym zu handeln	
Möglichkeit, unter einem Pseudonym zu handeln	Hierarchisch zu: keiner anderen Komponente. FPR_PSE.1.1 Die TSF muss sicherstellen, dass [Zuweisung: alle Benutzer oder Subjekte] den richtigen Namen des Benutzers, der der [Zuweisung: Liste der Subjekte, Operationen oder Objekte] zugeordnet ist, nicht bestimmen können. FPR_PSE.1.2 Die TSF muss in der Lage sein, den Decknamen des richtigen Namens des Benutzers an [Zuweisung: Liste der Subjekte] zu liefern [Zuweisung: Anzahl der Decknamen]. FPR_PSE.1.3 Die TSF muss [Auswahl: einen Decknamen für einen Benutzer bestimmen, den Decknamen für den Benutzer akzeptieren] und kontrollieren, dass er mit der [Zuweisung: decknamenrelevante Metrik] übereinstimmt. Verwandte Themen: Keine verwandten Themen

	Beispiele Die Benutzer oder Subjekte (definieren) dürfen den richtigen Namen des Benutzers nicht bestimmen können, der Subjekten, Operationen oder identifizierten Objekten (definieren) zugeordnet ist
Möglichkeit, unter einem Pseudonym zu handeln	Hierarchisch zu: keiner anderen Komponente. FPR_PSE.1.1 Die TSF muss sicherstellen, dass [Zuweisung: alle Benutzer oder Subjekte] nicht in der Lage sind, den richtigen Namen des Benutzers zu bestimmen, der der [Zuweisung: Liste der Subjekte, Operationen oder Objekte] zugeordnet ist. FPR_PSE.1.2 Die TSF muss in der Lage sein, den Decknamen des richtigen Namens des Benutzers an [Zuweisung: Liste der Subjekte] zu liefern [Zuweisung: Anzahl der Decknamen] FPR_PSE.1.3 Die TSF muss [Auswahl: einen Decknamen für einen Benutzer bestimmen, den Decknamen für den Benutzer akzeptieren] und kontrollieren, dass er mit der [Zuweisung: decknamenrelevante Metrik] übereinstimmt. Verwandte Themen: Keine verwandten Themen Beispiele Es muss möglich sein, eine bestimmte Anzahl von Decknamen (definieren) des richtigen Namens des Benutzers an identifizierte Subjekte (definieren) zu liefern
Möglichkeit, unter einem Pseudonym zu handeln	Hierarchisch zu: keiner anderen Komponente. FPR_PSE.1.1 Die TSF muss sicherstellen, dass [Zuweisung: alle Benutzer oder Subjekte] nicht in der Lage sind, den richtigen Namen des Benutzers zu bestimmen, der der [Zuweisung: Liste der Subjekte, Operationen oder Objekte] zugeordnet ist. FPR_PSE.1.2 Die TSF muss in der Lage sein, den Decknamen des richtigen Namens des Benutzers an [Zuweisung: Liste der Subjekte] zu liefern [Zuweisung: Anzahl der Decknamen] FPR_PSE.1.3 Die TSF muss [Auswahl: einen Decknamen für einen Benutzer bestimmen, den Decknamen für den Benutzer akzeptieren] und kontrollieren, dass er mit der [Zuweisung: decknamenrelevante Metrik] übereinstimmt. Verwandte Themen: Keine verwandten Themen Beispiele Das System muss einen Decknamen für einen Benutzer bestimmen, den Decknamen des Benutzers akzeptieren und kontrollieren, dass der Deckname mit der decknamenrelevanten Metrik übereinstimmt (definieren)
Reversible Verwendung von Pseudonymen	Hierarchisch zu: FPR_PSE.1 FPR_PSE.2.1 Die TSF muss sicherstellen, dass [Zuweisung: alle Benutzer oder Subjekte] nicht in de Lage sind, den richtigen Namen des Benutzers zu bestimmen, der der [Zuweisung: Liste der Subjekte, Operationen oder Objekte] zugeordnet ist. FPR_PSE.2.2 Die TSF muss in der Lage sein, den Decknamen des

	richtigen Namens des Benutzers an [Zuweisung: Liste der Subjekte] zu liefern [Zuweisung: Anzahl der Decknamen]. FPR_PSE.2.3 Die TSF muss [Auswahl: einen Decknamen für einen Benutzer bestimmen, den Decknamen für den Benutzer akzeptieren] und kontrollieren, dass er mit der [Zuweisung: decknamenrelevante Metrik] übereinstimmt. FPR_PSE.2.4 Die TSF muss [Auswahl: ein autorisierter Benutzer, [Zuweisung: Liste der gesicherten Subjekte]] befähigen, die Identität des Benutzers auf der Grundlage des gelieferten Decknamens zu bestimmen, aber nur unter den folgenden Bedingungen [Zuweisung: Liste der Bedingungen]. Verwandte Themen: FIA_UID.1 Zeitpunkt der Identifikation Beispiele Bei einer reversiblen Verwendung von Pseudonymen müssen erlaubte Benutzer und gesicherte Subjekte (definieren) in der Lage sein, die Identität des Benutzers auf der Grundlage des gelieferten Decknamens zu bestimmen, aber nur unter bestimmten Bedingungen (definieren)
Möglichkeit, bei Verwendung eines Decknamens unter einem Pseudonym zu handeln	Hierarchisch zu: FPR_PSE.1 FPR_PSE.3.1 Die TSF muss sicherstellen, dass [Zuweisung: alle Benutzer oder Subjekte] nicht in der Lage sind, den richtigen Namen des Benutzers zu bestimmen, der der [Zuweisung: Liste der Subjekte, Operationen oder Objekte] zugeordnet ist. FPR_PSE.3.2 Die TSF muss in der Lage sein, den Decknamen des richtigen Namens des Benutzers an [Zuweisung: Liste der Subjekte] zu liefern [Zuweisung: Anzahl der Decknamen] FPR_PSE.3.3 Die TSF muss [Auswahl: einen Decknamen für einen Benutzer bestimmen, den Decknamen für den Benutzer akzeptieren] und kontrollieren, dass er mit der [Zuweisung: decknamenrelevante Metrik] übereinstimmt. FPR_PSE.3.4 Die TSF muss einen Decknamen für den richtigen Namen des Benutzers liefern, der mit einem Decknamen übereinstimmt, der zuvor unter den folgenden Bedingungen [Zuweisung: Liste der Bedingungen] geliefert wurde; im gegenteiligen Fall darf der gelieferte Decknamen in keinerlei Beziehung mit den zuvor gelieferten Decknamen stehen. Verwandte Themen: Keine verwandten Themen Beispiele Für die Möglichkeit, unter einem Pseudonym bei Verwendung eines Decknamens zu handeln, muss der für den richtigen Namen des Benutzers gelieferte Deckname nach Möglichkeiten mit einem Decknamen übereinstimmen, der zuvor unter bestimmten Bedingungen (definieren) geliefert wurde
Möglichkeit, bei Verwendung eines Decknamens unter einem Pseudonym zu handeln	Hierarchisch zu: FPR_PSE.1 FPR_PSE.3.1 Die TSF muss sicherstellen, dass [Zuweisung: alle Benutzer oder Subjekte] nicht in der Lage sind, den richtigen Namen des Benutzers zu bestimmen, der der [Zuweisung: Liste der Subjekte, Operationen oder Objekte] zugeordnet ist. FPR_PSE.3.2 Die TSF muss in der Lage sein, den Decknamen des richtigen Namens des Benutzers an [Zuweisung: Liste der Subjekte] zu

	liefern [Zuweisung: Anzahl der Decknamen] FPR_PSE.2.3 Die TSF muss [Auswahl: einen Decknamen für einen Benutzer bestimmen, den Decknamen für den Benutzer akzeptieren] und kontrollieren, dass er mit der [Zuweisung: decknamenrelevante Metrik] übereinstimmt. FPR_PSE.3.4 Die TSF muss einen Decknamen für den richtigen Namen des Benutzers liefern, der mit einem Decknamen übereinstimmt, der zuvor unter den folgenden Bedingungen [Zuweisung: Liste der Bedingungen] geliefert wurde; im gegenteiligen Fall darf der gelieferte Decknamen in keinerlei Beziehung mit den zuvor gelieferten Decknamen stehen. Verwandte Themen: Keine verwandten Themen Beispiele Besteht die Möglichkeit, unter einem Pseudonym bei Verwendung eines Decknamens zu handeln, darf der gelieferte Deckname nicht mit den zuvor gelieferten Decknamen in Beziehung stehen, wenn FPR_PSE.3.4.1 nicht eingehalten werden kann
FPR_UNL: Unmöglichkeit der Herstellung einer Verbindung	
Unmöglichkeit der Herstellung einer Verbindung	Hierarchisch zu: keiner anderen Komponente. FPR_UNL.1.1 Die TSF muss sicherstellen, dass [Zuweisung: alle Benutzer oder Subjekte] zu keiner Bestimmung in der Lage sind, wenn [Zuweisung: Liste der Operationen] [Auswahl: vom gleichen Benutzer ausgelöst wurden, wie folgt verbunden sind [Zuweisung: Liste der Beziehungen]]. Verwandte Themen: Keine verwandten Themen Beispiele Benutzer oder Subjekte (definieren) dürfen nicht in der Lage sein zu bestimmen, ob bestimmte Beziehungen (definieren) vom gleichen Benutzer ausgelöst wurden oder in Übereinstimmung mit identifizierten Beziehungen (definieren) verbunden sind
FPR_UNO: Nicht-Beobachtbarkeit	
Nicht-Beobachtbarkeit	Hierarchisch zu: keiner anderen Komponente. FPR_UNO.1.1 Die TSF muss sicherstellen, dass [Zuweisung: Liste der Benutzer oder Subjekte] die Durchführung von [Zuweisung: Liste der Operationen] auf [Zuweisung: Liste der Objekte] durch [Zuweisung: Liste der geschützte Benutzer oder Subjekte] nicht beobachten können. Verwandte Themen: Keine verwandten Themen Beispiele Identifizierte Benutzer und Subjekte (definieren) dürfen die Durchführung bestimmter Operationen (definieren) auf Objekte (definieren) durch bestimmte geschützte Benutzer und Subjekte (definieren) nicht beobachten können
Bereitstellung von Informationen, die auf die Nicht-Beobachtbarkeit Einfluss haben	Hierarchisch zu: FPR_UNO.1 FPR_UNO.2.1 Die TSF muss sicherstellen, dass [Zuweisung: Liste der Benutzer oder Subjekte] die Durchführung von [Zuweisung: Liste der Operationen] auf [Zuweisung: Liste der Objekte] durch [Zuweisung: Liste der geschützte Benutzer oder Subjekte] nicht beobachten können.

	FPR_UNO.2.2 Die TSF muss verschiedenen Teilen des TOE (EVG) [Zuweisung: Informationen in bezug auf die Nicht-Beobachtbarkeit] so gewähren, dass die folgenden Bedingungen während der Lebensdauer der Informationen [Zuweisung: Liste der Bedingungen] erfüllt werden. Verwandte Themen: Keine verwandten Themen Beispiele Zur Bereitstellung von Informationen, die Einfluss auf die Nicht-Beobachtbarkeit haben, müssen den verschiedenen Teilen des Systems die mit der Nicht-Beobachtbarkeit (definieren) im Zusammenhang stehenden Informationen gewährt werden, um bestimmte Bedingungen (definieren) einzuhalten
Nicht-Beobachtbarkeit ohne Beanspruchung von Informationen	Hierarchisch zu: keiner anderen Komponente. FIA_UNO.3.1 Die TSF muss [Zuweisung: Liste der Dienste] an [Zuweisung: Liste der Subjekte] liefern, ohne einen beliebigen Bezug auf [Zuweisung: Informationen über die Privatsphäre] zu beanspruchen. Verwandte Themen: FPR_UNO.1 Nicht-Beobachtbarkeit Beispiele Identifizierte Subjekte (definieren) müssen bestimmte Dienste (definieren) liefern, ohne einen irgend einen Bezug auf Informationen über die Privatphäre (definieren) zu beanspruchen
Beobachtbarkeit für einen erlaubten Benutzer	Hierarchisch zu: keiner anderen Komponente. FPR_UNO.4.1 Die TSF muss [Zuweisung: alle erlaubte Benutzer] die Fähigkeit verleihen, die Verwendung von [Zuweisung: Liste der Ressourcen oder Dienste] zu beobachten. Verwandte Themen: Keine verwandten Themen Beispiele Erlaubte Benutzer (definieren) müssen die Fähigkeit haben, die Verwendung von identifizierten Ressourcen oder Diensten (definieren) zu beobachten

3.1.8 FPT : Schutz der TSF

FPT_AMT: Test der unterliegenden abstrakten Maschine	
Test der abstrakten Maschine	Hierarchisch zu: keiner anderen Komponente. FPT_AMT.1.1 Die TSF muss eine Testfolge [Auswahl: beim Erststart, periodisch bei normalem Betrieb, auf Anforderung eines erlaubten Benutzers, andere Bedingungen] durchführen, um nachzuweisen, dass die Sicherheitshypothesen, die von der unterliegenden abstrakten Maschine an die TSF geliefert wurden, korrekt arbeiten. Verwandte Themen: Keine verwandten Themen Beispiele Beim Erststart sind Tests durchzuführen, um nachzuweisen, dass die Sicherheitshypothesen, die von den für die Sicherheit zuständigen Systeme geliefert wurden, korrekt arbeiten
Test der abstrakten Maschine	Hierarchisch zu: keiner anderen Komponente.

	FPT_AMT.1.1 Die TSF muss eine Testfolge [Auswahl: beim Erststart, periodisch bei normalem Betrieb, auf Anforderung eines erlaubten Benutzers, andere Bedingungen] durchführen, um nachzuweisen, dass die Sicherheitshypothesen, die von der unterliegenden abstrakten Maschine an die TSF geliefert wurden, korrekt arbeiten. Verwandte Themen: Keine verwandten Themen Beispiele Im normalen Betrieb sind Tests durchzuführen um nachzuweisen, dass die Sicherheitshypothesen, die von den für die Sicherheit zuständigen Systeme geliefert wurden, korrekt arbeiten
Test der abstrakten Maschine	Hierarchisch zu: keiner anderen Komponente. FPT_AMT.1.1 Die TSF muss eine Testfolge [Auswahl: beim Erststart, periodisch bei normalem Betrieb, auf Anforderung eines erlaubten Benutzers, andere Bedingungen] durchführen um nachzuweisen, dass die Sicherheitshypothesen, die von der unterliegenden abstrakten Maschine an die TSF geliefert wurden, korrekt arbeiten. Verwandte Themen: Keine verwandten Themen Beispiele Auf Anforderung eines erlaubten Benutzers sind Tests durchzuführen um nachzuweisen, dass die Sicherheitshypothesen, die von den für die Sicherheit zuständigen Systeme geliefert wurden, korrekt arbeiten
Test der abstrakten Maschine	Hierarchisch zu: keiner anderen Komponente. FPT_AMT.1.1 Die TSF muss eine Testfolge [Auswahl: beim Erststart, periodisch bei normalem Betrieb, auf Anforderung eines erlaubten Benutzers, andere Bedingungen] durchführen, um nachzuweisen, dass die Sicherheitshypothesen, die von der unterliegenden abstrakten Maschine an die TSF geliefert wurden, korrekt arbeiten. Verwandte Themen: Keine verwandten Themen Beispiele Unter bestimmten ergänzenden Bedingungen (definieren) sind Tests durchzuführen um nachzuweisen, dass die Sicherheitshypothesen, die von den für die Sicherheit zuständigen Systeme geliefert wurden, korrekt arbeiten
FPT_FLS: Sicherer Modus nach Störung	
Störung mit Aufrechterhaltung eines sicheren Zustands	Hierarchisch zu: keiner anderen Komponente. FPT_FLS.1.1 Die TSF muss einen sicheren Zustand aufrechterhalten, wenn die folgenden Störfallarten auftreten: [Zuweisung: Liste der Störfallarten der TSF]. Verwandte Themen: ADV_SPM.1 Informelles EVG-Sicherheitsmodell Beispiele Die für die Sicherheit zuständigen Systeme müssen einen sicheren Zustand aufrechterhalten, wenn Störungen (definieren) auftreten
FPT_ITA: Verfügbarkeit exportierter TSF-Daten	
TSF-übergreifende Verfügbarkeit im Rahmen einer	Hiérarchique à : aucun autre composant. FPT_ITA.1.1 La TSF doit garantir la disponibilité [affectation : liste des types

Verfügbarkeitsmetrik	de données de la TSF] fournies à un produit TI de confiance distant dans le cadre de [affectation : une métrique de disponibilité définie] étant donné les conditions suivantes [affectation : conditions pour garantir la disponibilité]. Dépendances : Pas de dépendance Exemples La disponibilité de certaines données de sécurité (d finir) fournies un syst me de confiance distant dans le cadre d'une métrique de disponibilité spécifique (d finir) étant données des conditions (d finir) pour garantir la disponibilité[GRL1] Hierarchisch zu: keiner anderen Komponente. FPT_ITA.1.1 Die TSF muss die Verfügbarkeit [Zuweisung: Liste der Datenarten der TSF], die einem dezentalen gesicherten IT-Produkt im Rahmen von [Zuweisung: eine definierte Verfügbarkeitsmetrik] geliefert werden, sicherstellen, sofern die folgenden Bedingungen [Zuweisung: Bedingungen zur Gewährleistung der Verfügbarkeit] gegeben sind. Verwandte Themen: Keine verwandten Themen Beispiele Die Verfügbarkeit bestimmter gelieferter Sicherheitsdaten (definieren) ein dezentral gesichertes System im Rahmen einer speziellen Verfügbarkeitsmetrik (definieren) bei gegebenen Bedingungen (definieren), um Verfürgbarkeit zu gewährleisten [GRL1].
FPT_ITC: Verfügbarkeit exportierter TSF-Daten	
TSF-übergreifende Vertraulichkeit bei einer Übertragung	Hierarchisch zu: keiner anderen Komponente. FPT_ITC.1.1 Die TSF muss alle TSF-Daten , die von der TSF an ein dezentrales gesichertes IT-Produkt übertragen werden, bei ihrer Übertragung vor einer nicht erlaubten Preisgabe schützen. Verwandte Themen: Keine verwandten Themen Beispiele Alle Sicherheitsdaten, die von einem für die Sicherheit verantwortlichen System an ein dezentrales gesichertes System übertragen werden, sind bei ihrer Übertragung vor einer nicht erlaubten Preisgabe zu schützen
FPT_ITI: Integrität von exportierten TSF-Daten	
Détection d'une modification inter-TSF	Hierarchisch zu: keiner anderen Komponente. FPT_ITI.1.1 Die TSF muss eine Änderung aller TSF-Daten bei ihrer Übertragung zwischen der TSF und einem dezentralen gesicherten IT-Produkt im Rahmen der folgenden Metrik [Zuweisung: eine definierte Änderungsmetrik] erkennen können. FPT_ITI.1.2 Die TSF muss die Integrität aller TSF-Daten, die zwischen der TSF und einem dezentralen gesicherten IT-Produkt übertragen werden, kontrollieren können und [Zuweisung: einzuleitende Aktion] durchführen, wenn Änderungen erkannt werden. Verwandte Themen: Keine verwandten Themen Beispiele Jede Änderung von Sicherheitsdaten bei ihrer Übertragung zwischen einem

	für die Sicherheit verantwortlichen System und einem dezentralen gesicherten System muss innerhalb der Grenzen einer speziellen Änderungsmetrik (definieren) erkannt werden
Erkennen einer TSF-übergreifenden Änderung	Hierarchisch zu: keiner anderen Komponente. FPT_ITI.1.1 Die TSF muss eine Änderung aller TSF-Daten bei ihrer Übertragung zwischen der TSF und einem dezentralen gesicherten IT-Produkt im Rahmen der folgenden Metrik [Zuweisung: eine definierte Änderungsmetrik] erkennen können. FPT_ITI.1.2 Die TSF muss die Integrität aller TSF-Daten, die zwischen der TSF und einem dezentralen gesicherten IT-Produkt übertragen werden, kontrollieren können und [Zuweisung: einzuleitende Aktion] durchführen, wenn Änderungen erkannt werden. Verwandte Themen: Keine verwandten Themen Beispiele Die Integrität aller Sicherheitsdaten, die zwischen einem für die Sicherheit verantwortlichen System und einem dezentralen gesicherten System übertragen werden, ist zu kontrollieren und es sind Aktionen (definieren) einzuleiten, wenn Änderungen erkannt werden
Erkennen und Korrektur einer TSF-übergreifenden Änderung	Hierarchisch zu: FPT_ITI.1 FPT_ITI.2.1 Die TSF muss eine Änderung aller TSF-Daten bei ihrer Übertragung zwischen der TSF und einem dezentralen gesicherten IT-Produkt im Rahmen der folgenden Metrik [Zuweisung: eine definierte Änderungsmetrik] erkennen können. FPT_ITI.2.2 Die TSF muss die Integrität aller TSF-Daten, die zwischen der TSF und einem dezentralen gesicherten IT-Produkt übertragen werden, kontrollieren können und [Zuweisung: einzuleitende Aktion] durchführen, wenn Änderungen erkannt werden. FPT_ITI.2.3 Die TSF muss alle TSF-Daten, die zwischen der TSF und einem dezentralen gesicherten IT-Produkt übertragen werden, korrigieren können [Zuweisung: Art der Änderung]. Verwandte Themen: Keine verwandten Themen Beispiele Bei einer systemübergreifenden Korrektur einer Änderungen müssen Arten von Änderungen (definieren) aller Sicherheitsdaten, die zwischen einem für die Sicherheit verantwortlichen System und einem dezentralen gesicherten System übertragen werden, korrigiert werden können
FPT_ITT: Fluss von TSF-Daten innerhalb des TOE (EVG)	
Einfacher Schutz bei internem TSF-Datenaustausch	Hierarchisch zu: keiner anderen Komponente. FPT_ITT.1.1 Die TSF muss die TSF-Daten vor [Auswahl: Preisgabe, Modifizierung] schützen, wenn sie zwischen separaten Teilen des TOE (EVG) übertragen werden. Verwandte Themen: Keine verwandten Themen Beispiele Sicherheitsdaten sind vor Preisgabe und Modifizierung zu schützen, wenn sie zwischen separaten Teilen des Systems übertragen werden
Separierung von	Hierarchisch zu: FPT_ITT.1

TSF-Daten bei einer Übertragung	FPT_ITT.2.1 Die TSF muss die TSF-Daten vor [Auswahl: Preisgabe, Modifizierung] schützen, wenn sie zwischen separaten Teilen des TOE (EVG) übertragen werden. FPT_ITT.2.2 Die TSF muss die Daten des Benutzers von TSF-Daten separieren, wenn solche Daten zwischen separaten Teilen des TOE (EVG) übertragen werden. Verwandte Themen: Keine verwandten Themen Beispiele Die Benutzerdaten sind von Sicherheitsdaten zu separieren, wenn derartige Daten zwischen separaten Teilen des Systems übertragen werden
Integritätskontrolle der TSF-Daten	Hierarchisch zu: keiner anderen Komponente. FPT_ITT.3.1 Die TSF muss [Auswahl: die Änderung von Daten, das Vertauschen von Daten, die Umprogrammierung von Daten, die Unterdrückung von Daten, [Zuweisung: andere Integritätsfehler]] für die TSF-Daten erkennen können, die zwischen separaten Teilen des TOE (EVG) übertragen werden. Verwandte Themen: FPT_ITT.1 Einfacher Schutz bei internem TSF-Datenaustausch Beispiele Änderung, Austausch, Umprogrammierung, Unterdrückung oder andere Integritätsfehler (definieren) bei Sicherheitsdaten, die zwischen separaten Teilen des Systems übertragen werden, müssen erkannt werden
Kontrolle der Integrität der TSF-Daten	Hierarchisch zu: keiner anderen Komponente. FPT_ITT.3.2 Die TSF muss die folgenden Aktionen [Zuweisung: einzuleitende Aktion spezifizieren] durchführen, sobald bei den Daten ein Integritätsfehler erkannt wurde. Verwandte Themen: FPT_ITT.1 Einfacher Schutz bei internem TSF-Datenaustausch Beispiele Wird ein Daten-Integritätsfehler erkannt, sind spezielle Aktionen (definieren) einzuleiten
FPT_PHP: Physischer Schutz der TSF	
Passives Erkennen eines physischen Angriffs	Hierarchisch zu: keiner anderen Komponente. FPT_PHP.1.1 Die TSF muss ein physisches Eindringen, das der TSF Schaden zufügen könnte, eindeutig erkennen. FPT_PHP.1.2 Die TSF muss bestimmen können, ob ein physisches Eindringen in die Einrichtungen oder Elemente der TSF stattgefunden hat. Verwandte Themen: FMT_MOF.1 Management des Verhaltens der Sicherheitsfunktionen Beispiele Jedes physische Eindringen, das der Sicherheit des Systems Schaden zufügen könnte, ist eindeutig zu erkennen
Passives Erkennen	Hierarchisch zu: keiner anderen Komponente.

eines physischen Angriffs	FPT_PHP.1.1 Die TSF muss ein physisches Eindringen, das der TSF Schaden zufügen könnte, eindeutig erkennen. FPT_PHP.1.2 Die TSF bestimmen können, ob ein physisches Eindringen in die Einrichtungen oder Elemente der TSF stattgefunden hat. Verwandte Themen: FMT_MOF.1 Management des Verhaltens der Sicherheitsfunktionen Beispiele Es muss möglich sein zu bestimmen, ob ein physisches Eindringen in die Sicherheitseinrichtungen oder -elemente stattgefunden hat
Anzeige eines physischen Angriffs	Hierarchisch zu: FPT_PHP.1 FPT_PHP.2.1 Die TSF muss ein physisches Eindringen, das der TSF Schaden zufügen könnte, eindeutig erkennen. FPT_PHP.2.2 Die TSF bestimmen können, ob ein physisches Eindringen in die Einrichtungen oder Elemente der TSF stattgefunden hat. FPT_PHP.2.3 Die TSF muss für [Zuweisung: Liste der Einrichtungen oder Elemente der TSF, für die ein aktives Erkennen erforderlich ist] die Einrichtungen und Elemente kontrollieren und einem/r [Zuweisung: ein Benutzer oder eine besonders geeignete Rolle] anzeigen, wenn ein physisches Eindringen in die Einrichtungen oder Elemente der TSF stattgefunden hat. Verwandte Themen: FMT_MOF.1 Management des Verhaltens der Sicherheitsfunktionen Beispiele Bestimmte Sicherheitseinrichtungen und elemente (definieren) sind zu kontrollieren; jedwedes physische Eindringen in diese Einrichtungen und Elemente ist einem speziellen Benutzer oder einer besonders geeigneten Rolle (definieren) anzuzeigen
Widerstand gegenüber einem physischen Angriff	Hierarchisch zu: keiner anderen Komponente. FPT_PHP.3.1 Die TSF muss [Zuweisung: Szenarien physischen Eindringens] in die [Zuweisung: Liste der Einrichtungen oder Elemente der TSF] widerstehen, indem automatisch so geantwortet wird, dass die TSP nicht verletzt wird. Verwandte Themen: Keine verwandten Themen Beispiele Das System muss Szenarien physischen Eindringens (definieren) in die Sicherheitseinrichtungen oder -elemente widerstehen, indem automatisch so geantwortet wird, dass die Sicherheitspolitik nicht verletzt wird
FPT_RCV: Sicherer Restart	
Manueller Restart	Hierarchisch zu: keiner anderen Komponente. FPT_RCV.1.1 Nach einer Störung oder einer Unterbrechung des Dienstes muss die TSF in einen Wartungsmodus übergehen, in dem die Wiedereinsetzung des TOE (EVG) in einen sicheren Zustand angeboten wird. Verwandte Themen: FPT_TST.1 Test der TSF AGD_ADM.1 Administratorleitfaden

	ADV_SPM.1 Informelles EVG-Sicherheitsmodell Beispiele Nach einer Störung oder einer Unterbrechung des Dienstes müssen die für die Sicherheit zuständigen Systeme in einen Wartungsmodus übergehen, in dem die Wiedereinsetzung des TOE (EVG) in einen sicheren Zustand angeboten wird
Automatischer Restart	Hierarchisch zu: FPT_RCV.1 FPT_RCV.2.1 Wenn ein automatischer Restart nach einer Störung oder einer Unterbrechung des Dienstes nicht möglich ist, muss die TSF in einen Wartungsmodus übergehen, in dem die Wiedereinsetzung des TOE (EVG) in einen sicheren Zustand angeboten wird. FPT_RCV.2.2 Die TSF muss für [Zuweisung: Liste der Störfälle oder Dienstunterbrechungen] die Rückkehr des TOE (EVG) in einen sicheren Zustand bei Verwendung automatischer Verfahren sicherstellen. Verwandte Themen: FPT_TST.1 Test der TSF AGD_ADM.1 Administratorleitfaden ADV_SPM.1 Informelles EVG-Sicherheitsmodell Beispiele Wenn ein automatischer Restart nach einer Störung oder einer Unterbrechung nicht möglich ist, müssen die für die Sicherheit zuständigen Systeme in einen Wartungsmodus übergehen, in dem die Wiedereinsetzung des Systems in einen sicheren Zustand angeboten wird
Automatischer Restart	Hierarchisch zu: FPT_RCV.1 FPT_RCV.2.1 Wenn ein automatischer Restart nach einer Störung oder einer Unterbrechung des Dienstes nicht möglich ist, muss die TSF in einen Wartungsmodus übergehen, in dem die Wiedereinsetzung des TOE (EVG) in einen sicheren Zustand angeboten wird. FPT_RCV.2.2 Die TSF muss für [Zuweisung: Liste der Störfälle oder Dienstunterbrechungen] die Rückkehr des TOE (EVG) in einen sicheren Zustand bei Verwendung automatischer Verfahren sicherstellen. Verwandte Themen: FPT_TST.1 Test der TSF AGD_ADM.1 Administratorleitfaden ADV_SPM.1 Informelles EVG-Sicherheitsmodell Beispiele Bei bestimmten Störungen oder einer Dienstunterbrechungen (definieren) ist die Rückkehr des Systems in einen sicheren Zustand bei Verwendung automatischer Verfahren sicherzustellen
Unkritischer automatischer Restart	Hierarchisch zu: FPT_RCV.2 FPT_RCV.3.1 Wenn ein automatischer Restart nach einer Störung oder einer Unterbrechung des Dienstes nicht möglich ist, muss die TSF in einen Wartungsmodus übergehen, in dem die Wiedereinsetzung des TOE (EVG) in einen sicheren Zustand angeboten wird. FPT_RCV.3.2 Die TSF muss für [Zuweisung: Liste der Störfälle oder Dienstunterbrechungen] die Rückkehr des TOE (EVG) in einen sicheren Zustand bei Verwendung automatischer Verfahren sicherstellen. FPT_RCV.3.3 Die von der TSF für einen Restart nach einer Störung oder

	einer Unterbrechung des Dienstes gelieferten Funktionen müssen sicherstellen, dass der sichere Anfangszustand wiederhergestellt wird, ohne [Zuweisung: Quantifizierung] Datenverluste der TSF oder von Objekten im TSC zu überschreiten. FPT_RCV.3.4 Die TSF muss die Möglichkeit bieten, die Objekte bestimmen zu können, die wiederhergestellt oder nicht wiederhergestellt werden konnten. Verwandte Themen: FPT_TST.1 Test der TSF AGD_ADM.1 Administratorleitfaden ADV_SPM.1 Informelles EVG-Sicherheitsmodell Beispiele Bei einem unkritischen automatischen Restart müssen die Funktionen für einen Restart nach einer Störung oder Dienstunterbrechung sicherstellen, dass der sichere Anfangszustand wiederhergestellt wird, ohne dass ein bestimmtes Volumen an Datenverlust (definieren) überschritten wird
Unkritischer automatischer Restart	Hierarchisch zu: FPT_RCV.2 FPT_RCV.3.1 Wenn ein automatischer Restart nach einer Störung oder einer Unterbrechung des Dienstes nicht möglich ist, muss die TSF in einen Wartungsmodus übergehen, in dem die Wiedereinsetzung des TOE (EVG) in einen sicheren Zustand angeboten wird. FPT_RCV.3.2 Die TSF muss für [Zuweisung: Liste der Störfälle oder Dienstunterbrechungen] die Rückkehr des TOE (EVG) in einen sicheren Zustand bei Verwendung automatischer Verfahren sicherstellen. FPT_RCV.3.3 Die von der TSF für einen Restart nach einer Störung oder einer Dienstunterbrechung gelieferten Funktionen müssen sicherstellen, dass der sichere Anfangszustand wiederhergestellt wird, ohne [Zuweisung: Quantifizierung] Datenverluste der TSF oder von Objekten im TSC zu überschreiten. FPT_RCV.3.4 Die TSF muss die Möglichkeit bieten, die Objekte bestimmen zu können, die wiederhergestellt oder nicht wiederhergestellt werden konnten. Verwandte Themen: FPT_TST.1 Test der TSF AGD_ADM.1 Administratorleitfaden ADV_SPM.1 Informelles EVG-Sicherheitsmodell Beispiele Es muss möglich sein, die Objekte zu bestimmen, die wiederhergestellt oder nicht wiederhergestellt werden konnten
Funktions-Restart	Hierarchisch zu: keiner anderen Komponente. FPT_RCV.4.1 Die TSF muss sicherstellen, dass [Zuweisung: Liste der Sicherheitsfunktionen und Störfallszenarien] ein Merkmal besitzt, mit dem die Sicherheitsfunktion entweder ihre Aufgabe erfolgreich erfüllt oder ihren Betrieb für die genannten Störfallszenarien in einem konsistenten und sicheren Zustand neu startet. Verwandte Themen: ADV_SPM.1 Informelles EVG-Sicherheitsmodell Beispiele Bei identifizierten Störfallszenarien (definieren) müssen die Sicherheitsfunktionen entweder ihre Aufgabe erfolgreich erfüllen oder ihren Betrieb in einem konsistenten und sicheren Zustand neu starten

FPT_RPL: Erkennen von Play-back	
Erkennen von Play-back	Hierarchisch zu: keiner anderen Komponente. FPT_RPL.1.1 Die TSF muss für die folgenden Einheiten Play-back erkennen: [Zuweisung: Liste der identifizierten Einheiten]. Verwandte Themen: Keine verwandten Themen Beispiele Für einige identifizierte Einheiten (definieren) ist Play-back zu erkennen
Erkennen von Play-back	Hierarchisch zu: keiner anderen Komponente. FPT_RPL.1.2 Die TSF muss [Zuweisung: Liste der speziellen Aktionen] durchführen, wenn Play-back erkannt wird. Verwandte Themen: Keine verwandten Themen Beispiele Es sind spezielle Aktionen durchzuführen, sobald Play-back erkannt wird
FPT_RVM: Nichtumgehbarkeit des Referenzmonitors	
Fähigkeit der TSP, nicht kurzgeschlossen werden zu können	Hierarchisch zu: keiner anderen Komponente. FPT_RVM.1.1 Die TSF muss sicherstellen, dass TSP-Funktionen zur Durchsetzung aktiv und erfolgreich sind, bevor den Funktionen innerhalb des TSC die Ausführung gestattet wird. Verwandte Themen: Keine verwandten Themen Beispiele Funktionen, die die Sicherheitspolitik umsetzen, müssen aufgerufen und erfolgreich ausgeführt werden, bevor einer beliebigen Funktion des Systems die Ausführung gestattet wird
FPT_SEP: Separierung von Bereichen	
Separierung von Bereichen für die TSF	Hierarchisch zu: keiner anderen Komponente. FPT_SEP.1.1 Die TSF muss einen Sicherheitsbereich für ihre eigene Ausführung aufrecht erhalten, der sie vor Interferenzen und Eindringen nicht sicherer Subjekte schützt. FPT_SEP.1.2 Die TSF muss eine Separierung zwischen den Sicherheitsbereichen von Subjekten im TSC durchsetzen. Verwandte Themen: Keine verwandten Themen Beispiele Die für die Sicherheit zuständigen Systeme müssen für ihre eigene Ausführung einen Sicherheitsbereich aufrecht erhalten, der sie vor Interferenzen und Eindringen nicht sicherer Subjekte schützt
Separierung von Bereichen für die TSF	Hierarchisch zu: keiner anderen Komponente. FPT_SEP.1.1 Die TSF muss einen Sicherheitsbereich für ihre eigene Ausführung aufrecht erhalten, der sie vor Interferenzen und Eindringen nicht sicherer Subjekte schützt.F PT_SEP.1.2 Die TSF muss eine Separierung zwischen den Sicherheitsbereichen von Subjekten im TSC durchsetzen.

	Verwandte Themen: Keine verwandten Themen Beispiele Im System ist eine Separierung zwischen den Sicherheitsbereichen von Subjekten durchzusetzen
Separierung von Bereichen für die SFP	Hierarchisch zu: FPT_SEP.1 FPT_SEP.2.1 Der nicht isolierte Teil der TSF muss für seine eigene Ausführung einen Sicherheitsbereich aufrecht erhalten, der ihn vor Interferenzen und Eindringen nicht sicherer Subjekte schützt. FPT_SEP.2.2 Die TSF muss eine Separierung zwischen den Sicherheitsbereichen von Subjekten im TSC durchsetzen. FPT_SEP.2.3 Die TSF muss den Teil der TSF, der mit [Zuweisung: Liste der SFP für Zugriffskontrolle oder der SFP für Informationsflusskontrolle] verbunden ist, in einem Sicherheitsbereich für ihre eigene Ausführung aufrecht erhalten, der sie in bezug auf diese SFP vor Interferenzen und Eindringen aus den übrigen Teilen der TSF und nicht sicheren Subjekten schützt. Verwandte Themen: Keine verwandten Themen Beispiele Die für die Kontrolle von Zugriffen oder Informationsflüssen zuständigen Systeme sind für ihre eigene Ausführung in einem Sicherheitsbereich, der sie vor Interferenzen, Eindringen und nicht sicheren Subjekten schützt, aufrecht zu erhalten
Separierung von Bereichen für die SFP	Hierarchisch zu: FPT_SEP.1 FPT_SEP.2.1 Der nicht isolierte Teil der TSF muss für seine eigene Ausführung einen Sicherheitsbereich aufrecht erhalten, der ihn vor Interferenzen und Eindringen nicht sicherer Subjekte schützt. FPT_SEP.2.2 Die TSF muss eine Separierung zwischen den Sicherheitsbereichen von Subjekten im TSC durchsetzen. FPT_SEP.2.3 Die TSF muss den Teil der TSF, der mit [Zuweisung: Liste der SFP für Zugriffskontrolle oder der SFP für Informationsflusskontrolle] verbunden ist, in einem Sicherheitsbereich für ihre eigene Ausführung aufrecht erhalten, der sie in bezug auf diese SFP vor Interferenzen und Eindringen aus den übrigen Teilen der TSF und nicht sicheren Subjekten schützt. Verwandte Themen: Keine verwandten Themen Beispiele Der nicht isolierte Teil eines für die Sicherheit zuständigen Systems muss für seine eigene Ausführung einen Sicherheitsbereich aufrecht erhalten, der ihn vor Interferenzen und Eindringen nicht sicherer Subjekte schützt
Vollständiger Referenzmonitor	Hierarchisch zu: FPT_SEP.2 FPT_SEP.3.1 Der nicht isolierte Teil der TSF muss für seine eigene Ausführung einen Sicherheitsbereich aufrecht erhalten, der ihn vor Interferenzen und Eindringen nicht sicherer Subjekte schützt. FPT_SEP.3.2 Die TSF muss eine Separierung zwischen den Sicherheitsbereichen von Subjekten im TSC durchsetzen.

	FPT_SEP.3.3 Die TSF muss den Teil der TSF, der die SFP für Zugriffskontrolle oder die SFP für Informationsflusskontrolle für ihre eigene Ausführung in einem Sicherheitsbereich umsetzt, aufrecht erhalten der sie in bezug auf die TSP vor Interferenzen und Eindringen aus den übrigen Teilen der TSF und nicht sicheren Subjekten schützt. Verwandte Themen: Keine verwandten Themen Beispiele Die für die Kontrolle von Zugriffen oder Informationsflüssen zuständigen Teile der Sicherheitssysteme sind für ihre eigene Ausführung in einem Sicherheitsbereich aufrecht zu erhalten, der sie vor Interferenzen, Eindringen und nicht sicheren Subjekten schützt
FPT_SSP: Zustandssynchronisations-Protokoll	
Einfache gesicherte Quittung	Hierarchisch zu: keiner anderen Komponente. FPT_SSP.1.1 Die TSF muss eine änderungsfreie TSF-Datenübertragung quittieren, wenn das von einem anderen Teil der TSF gefordert wird. Verwandte Themen: FPT_ITT.1 Einfacher Schutz bei internem TSF-Datenaustausch Beispiele Ein für die Sicherheit zuständiges System muss eine änderungsfreie Übertragung von Sicherheitsdaten quittieren, wenn das von einem anderen System, das für die Sicherheit zuständig ist, gefordert wird
Gegenseitig gesicherte Quittung	Hierarchisch zu: FPT_SSP.1 FPT_SSP.2.1 Die TSF muss eine änderungsfreie TSF-Datenübertragung quittieren, wenn das von einem anderen Teil der TSF gefordert wird. FPT_SSP.2.2 Die TSF muss anhand von Quittungen sicherstellen, dass die betreffenden Teile der TSF den exakten Status der zwischen ihren verschiedenen Teilen übertragenen Daten kennen. Verwandte Themen: FPT_ITT.1 Einfacher Schutz bei internem TSF-Datenaustausch Beispiele Für eine gegenseitig gesicherte Quittung müssen die betreffenden für die Sicherheit zuständigen Systeme den exakten Status der zwischen ihren verschiedenen Teilen übertragenen Daten anhand von Quittungen kennen
FPT_STM: Tag- und Zeiteinstellung	
Zuverlässige Tag- und Zeiteinstellung	Hierarchisch zu: keiner anderen Komponente. FPT_STM.1.1 Die TSF muss für ihren eigenen Gebrauch eine zuverlässige Tag- und Zeiteinstellung liefern können. Verwandte Themen: Keine verwandten Themen Beispiele Ein für die Sicherheit zuständiges System muss eine zuverlässige Tag- und Zeiteinstellung für seinen eigenen Gebrauch liefern können
FPT_TDC: TSF-übergreifende Konsistenz von TSF-Daten	
Elementare Konsistenz der TSF-	Hierarchisch zu: keiner anderen Komponente.

Daten zwischen den TSFs	FPT_TDC.1.1 Die TSF muss [Zuweisung: Liste der Arten der TSF-Daten] konsistent interpretieren können, wenn diese von der TSF und einem anderen gesicherten IT-Produkt geteilt werden. Verwandte Themen: Keine verwandten Themen Beispiele Bestimmte Arten von Sicherheitsdaten (definieren) müssen konsistent interpretiert werden können, wenn sie von einem für die Sicherheit zuständigen System und einem gesicherten System geteilt werden
Elementare Konsistenz der TSF-Daten zwischen den TSFs	Hierarchisch zu: keiner anderen Komponente. FPT_TDC.1.2 Die TSF muss [Zuweisung: Liste der Interpretationsregeln, die von der TSF durchzusetzen sind] verwenden, um die TSF-Daten eines anderen gesicherten IT-Produkts interpretieren zu können. Verwandte Themen: Keine verwandten Themen Beispiele Von den für die Sicherheit zuständigen Systemen sind Interpretationsregeln (definieren) zu verwenden, um Sicherheitsdaten eines anderen gesicherten Systems zu interpretieren
FPT_TRC: Konsistenz der Reproduktion der TSF-Daten innerhalb des TOE (EVG)	
Interne Konsistenz der TSF	Hierarchisch zu: keiner anderen Komponente. FPT_TRC.1.1 Die TSF muss sicherstellen, dass die TSF-Daten konsistent sind, wenn sie zwischen Teilen des TOE (EVG) reproduziert werden. Verwandte Themen: FPT_ITT.1 Einfacher Schutz bei internem TSF-Datenaustausch Beispiele Die Sicherheitsdaten müssen konsistent sein, wenn sie zwischen Teilen des Systems reproduziert werden
Interne Konsistenz der TSF	Hierarchisch zu: keiner anderen Komponente. FPT_TRC.1.2 Die TSF muss, wenn Teile des TOE (EVG), die reproduzierte TSF-Daten enthalten, getrennt werden, die Konsistenz dieser Daten bei Wiederverbindung sicherstellen, bevor andere Anforderungen für [Zuweisung: SF-Liste, die von der Konsistenz der Reproduktion von TSF-Daten abhängt] verarbeitet werden. Verwandte Themen: FPT_ITT.1 Einfacher Schutz bei internem TSF-Datenaustausch Beispiele Werden Teile des Systems, die reproduzierte Sicherheitsdaten enthalten, getrennt, ist bei Wiederverbindung die Konsistenz der Daten sicherzustellen, bevor eine beliebige Sicherheitsfunktion, die diese Daten benötigt, durchgeführt wird
FPT_TST: TSF-Selbsttest	
TSF-Test	Hierarchisch zu: keiner anderen Komponente. FPT_TST.1.1 Die TSF muss eine Selbsttestfolge [Auswahl: beim Erststart, periodisch bei normalem Betrieb, auf Anforderung eines erlaubten Benutzers, unter den Bedingungen [Zuweisung: Bedingungen, unter denen der Selbsttest

	durchzuführen ist] durchführen um nachzuweisen, dass die TSF korrekt arbeitet. Verwandte Themen: FPT_AMT.1 Test der abstrakten Maschine Beispiele Ein für die Sicherheit zuständiges System muss beim Erststart eine Selbsttestfolge durchführen um nachzuweisen, dass es korrekt arbeitet
TSF-Test	Hierarchisch zu: keiner anderen Komponente. FPT_TST.1.1 Die TSF muss eine Selbsttestfolge [Auswahl: beim Erststart, periodisch bei normalem Betrieb, auf Anforderung eines erlaubten Benutzers, unter den Bedingungen [Zuweisung: Bedingungen, unter denen der Selbsttest durchzuführen ist] durchführen um nachzuweisen, dass die TSF korrekt arbeitet. Verwandte Themen: FPT_AMT.1 Test der abstrakten Maschine Beispiele Ein für die Sicherheit zuständiges System muss beim normalen Betrieb in periodischen Abständen eine Selbsttestfolge durchführen um nachzuweisen, dass es korrekt arbeitet
TSF-Test	Hierarchisch zu: keiner anderen Komponente. FPT_TST.1.1 Die TSF muss eine Selbsttestfolge [Auswahl: beim Erststart, periodisch bei normalem Betrieb, auf Anforderung eines erlaubten Benutzers, unter den Bedingungen [Zuweisung: Bedingungen, unter denen der Selbsttest durchzuführen ist] durchführen um nachzuweisen, dass die TSF korrekt arbeitet. Verwandte Themen: FPT_AMT.1 Test der abstrakten Maschine Beispiele Ein für die Sicherheit zuständiges System muss auf Anforderung des rechtmäßigen Benutzers eine Selbsttestfolge durchführen um nachzuweisen, dass es korrekt arbeitet
TSF-Test	Hierarchisch zu: keiner anderen Komponente. FPT_TST.1.1 Die TSF muss eine Selbsttestfolge [Auswahl: beim Erststart, periodisch bei normalem Betrieb, auf Anforderung eines erlaubten Benutzers, unter den Bedingungen [Zuweisung: Bedingungen, unter denen der Selbsttest durchzuführen ist] durchführen um nachzuweisen, dass die TSF korrekt arbeitet. Verwandte Themen: FPT_AMT.1 Test der abstrakten Maschine Beispiele Ein für die Sicherheit zuständiges System muss unter speziellen Bedingungen (definieren) eine Selbsttestfolge durchführen um nachzuweisen, dass es korrekt arbeitet
TSF-Test	Hierarchisch zu: keiner anderen Komponente. FPT_TST.1.2 Die TSF muss autorisierte Benutzer befähigen, die Integrität der TSF-Daten zu kontrollieren. Verwandte Themen: FPT_AMT.1 Test der abstrakten Maschine

	Beispiele Die rechtmäßigen Benutzer müssen die Integrität der Sicherheitsdaten kontrollieren können
TSF-Test	Hierarchisch zu: keiner anderen Komponente. FPT_TST.1.3 Die TSF muss autorisierte Benutzer befähigen, die Integrität des ausführbaren Codes der gespeicherten TSF zu überprüfen. Verwandte Themen: FPT_AMT.1 Test der abstrakten Maschine Beispiele Die rechtmäßigen Benutzer müssen die Integrität des ausführbaren Codes, der in einem für die Sicherheit verantwortlichen System gespeichert ist, kontrollieren können

3.1.9 FRU : Verwendung der Ressourcen

FRU_FLT: Pannen-Toleranz	
Fehlertoleranz mit Ausfallsicherung	Hierarchisch zu: keiner anderen Komponente. FRU_FLT.1.1 Die TSF muss die Funktionsweise von [Zuweisung: Liste der Fähigkeiten des TOE (EVG)] sicherstellen, wenn die folgenden Störungen auftreten: [Zuweisung: Liste der Störfallarten]. Verwandte Themen: FPT_FLS.1 Störung mit Aufrechterhaltung eines sicheren Zustands Beispiele Bei einer Pannentoleranz mit Ausfallsicherung sind bestimmte Fähigkeiten des Systems (definieren) sicherzustellen, wenn bestimmte Störungen (definieren) auftreten
Auf bestimmte Störungen beschränkte Fehlertoleranz	Hierarchisch zu: FRU_FLT.1 FRU_FLT.2.1 Die TSF muss sicherstellen, dass der TOE (EVG) voll arbeitet, wenn die folgenden Störungen auftreten: [Zuweisung: Liste der Störfallarten]. Verwandte Themen: FPT_FLS.1 Störung mit Aufrechterhaltung eines sicheren Zustands Beispiele Für eine beschränkte Pannentoleranz müssen alle Fähigkeiten des Systems gewährleistet sein, wenn bestimmte Störungen (definieren) auftreten
FRU_PRS: Dienstpriorität	
Beschränkte Dienstpriorität	Hierarchisch zu: keiner anderen Komponente. FRU_PRS.1.1 Die TSF muss jedem Subjekt der TSF eine Priorität zuweisen. FRU_PRS.1.2 Die TSF muss sicherstellen, dass jeder Zugriff auf [Zuweisung: kontrollierte Ressourcen] auf der Grundlage der Priorität erlaubt werden muss, die den Subjekten gewährt wurde. Verwandte Themen: Keine verwandten Themen Beispiele Für eine beschränkte Dienstpriorität ist jeder Zugriff auf kontrollierte Ressourcen

	auf der Grundlage der Priorität zu erlauben, die den Subjekten gewährt wurde
Beschränkte Dienstpriorität	Hierarchisch zu: keiner anderen Komponente. FRU_PRS.1.1 Die TSF muss jedem Subjekt der TSF eine Priorität zuweisen. FRU_PRS.1.2 Die TSF muss sicherstellen, dass jeder Zugriff auf [Zuweisung: kontrollierte Ressourcen] auf der Grundlage der Priorität erlaubt werden muss, die den Subjekten gewährt wurde. Verwandte Themen: Keine verwandten Themen Beispiele Jedem Subjekt ist eine Priorität zuzuweisen
FRU_RSA: Gewährung von Ressourcen	
Maximale Quoten	Hierarchisch zu: keiner anderen Komponente. FRU_RSA.1.1 Die TSF muss maximale Quoten auf die folgenden Ressourcen durchsetzen: [Zuweisung: kontrollierte Ressourcen], die [Auswahl: ein einzelner Benutzer, eine bestimmte Benutzergruppe, Subjekte] [Auswahl: gleichzeitig, während eines bestimmten Zeitabschnitts] verwenden können. Verwandte Themen: Keine verwandten Themen Beispiele Für identifizierte kontrollierte Ressourcen (definieren), die einzelne Benutzer, Benutzergruppen oder Subjekte (definieren) gleichzeitig oder während eines bestimmten Zeitabschnitts verwenden können, sind maximale Quoten durchzusetzen
Minimale und maximale Quoten	Hierarchisch zu: FRU_RSA.1 FRU_RSA.2.1 Die TSF muss maximale Quoten auf die folgenden Ressourcen durchsetzen: [Zuweisung: kontrollierte Ressourcen], die [Auswahl: ein einzelner Benutzer, eine bestimmte Benutzergruppe, Subjekte] [Auswahl: gleichzeitig, während eines bestimmten Zeitabschnitts] verwenden können. FRU_RSA.2.2 Die TSF muss sicherstellen, dass eine Mindestmenge jeder [Zuweisung: kontrollierte Ressource], die für eine [Auswahl: gleichzeitig, während eines bestimmten Zeitabschnitts] Verwendung durch [Auswahl: ein einzelner Benutzer, eine bestimmte Benutzergruppe, Subjekte] verfügbar ist, geliefert wird. Verwandte Themen: Keine verwandten Themen Beispiele Bei Mindestquoten muss eine Mindestmenge jeder identifizierten kontrollierten Ressource (definieren) für eine gleichzeitige Verwendung oder eine Verwendung während eines bestimmten Zeitabschnitts durch einen einzelnen Benutzer, eine bestimmte Benutzergruppe oder Subjekte verfügbar sein

3.1.10 FTA : Zugriff auf den TOE (EVG)

FTA_LSA: Beschränkung des Gültigkeitsbereichs der selektierbaren Attribute	
Beschränkung des Bereichs der selektierbaren Attribute	Hierarchisch zu: keiner anderen Komponente. FTA_LSA.1.1 Die TSF muss den Gültigkeitsbereich der Sitzungs-Sicherheitsattribute [Zuweisung: Sitzungs-Sicherheitsattribute] auf Grundlage von [Zuweisung: Attribute] beschränken.

	Verwandte Themen: Keine verwandten Themen Beispiele Der Gültigkeitsbereich der Sitzungs-Sicherheitsattribute (definieren) ist auf Grundlage bestimmter Attribute (definieren) zu beschränken
FTA_MCS: Beschränkung der Anzahl von Parallelsitzungen	
Elementare Beschränkung der Anzahl von Parallelsitzungen	Hierarchisch zu: keiner anderen Komponente. FTA_MCS.1.1 Die TSF muss die maximale Anzahl von Parallelsitzungen des gleichen Benutzers beschränken. FTA_MCS.1.2 Die TSF muss standardmäßig eine Beschränkung von [Zuweisung: standardmäßige Anzahl] Sitzungen pro Benutzer durchsetzen. Verwandte Themen: FIA_UID.1 Zeitpunkt der Identifikation Beispiele Die maximale Anzahl von Parallelsitzungen des gleichen Benutzers ist zu beschränken
Elementare Beschränkung der Anzahl von Parallelsitzungen	Hierarchisch zu: keiner anderen Komponente. FTA_MCS.1.1 Die TSF muss die maximale Anzahl von Parallelsitzungen des gleichen Benutzers beschränken. FTA_MCS.1.2 Die TSF muss standardmäßig eine Beschränkung von [Zuweisung: standardmäßige Anzahl] Sitzungen pro Benutzer durchsetzen. Verwandte Themen: FIA_UID.1 Zeitpunkt der Identifikation Beispiele Eine Beschränkung der Anzahl der Sitzungen pro Benutzer (definieren) ist standardmäßig durchzusetzen
Beschränkung der Anzahl der Parallelsitzungen durch Benutzerattribute	Hierarchisch zu: FTA_MCS.1 FTA_MCS.2.1 Die TSF muss die maximale Anzahl von Parallelsitzungen des gleichen Benutzers gemäß den Regeln [Zuweisung: Regeln für die maximale Anzahl von Parallelsitzungen] beschränken. FTA_MCS.2.2 Die TSF muss standardmäßig eine Beschränkung von [Zuweisung: standardmäßige Anzahl] Sitzungen pro Benutzer durchsetzen. Verwandte Themen: FIA_UID.1 Zeitpunkt der Identifikation Beispiele Für eine Beschränkung der Anzahl der Parallelsitzungen durch die Benutzerattribute ist die maximale Anzahl von Parallelsitzungen für den gleichen Benutzer gemäß den Regeln (definieren) zu beschränken, die sich auf die Benutzerattribute stützen
FTA_SSL: Sperren einer Sitzung	
Sperren einer Sitzung auf Veranlassung der TSF	Hierarchisch zu: keiner anderen Komponente. FTA_SSL.1.1 Die TSF muss eine interaktive Sitzung sperren nach [Zuweisung: Dauer der Inaktivität eines Benutzers]: a) durch Löschen oder Vernichten des Inhalts der Anzeigebildschirme, wodurch diese unleserlich werden; b) durch Deaktivieren aller Mittel, die Zugriff auf die Daten des Benutzers oder

	ihre Anzeige gewähren, ausgenommen zum Entsperren der Sitzung. FTA_SSL.1.2 Die TSF muss erfordern, dass vor dem Entsperren der Sitzung die folgenden Ereignisse stattfinden: [Zuweisung: Ereignisse, die stattfinden müssen]. Verwandte Themen: FIA_UAU.1 Zeitpunkt der Authentisierung Beispiele Nach einer bestimmten Inaktivitätsdauer eines Benutzers (definieren) ist eine interaktive Sitzung zu sperren, indem der Inhalt der Anzeigebildschirme unleserlich gemacht und jedwedes Mittel für den Zugriff auf Daten deaktiviert wird, außer für das Entsperren der Sitzung
Sperren einer Sitzung auf Veranlassung der TSF	Hierarchisch zu: keiner anderen Komponente. FTA_SSL.1.1 Die TSF muss eine interaktive Sitzung sperren nach [Zuweisung: Dauer der Inaktivität eines Benutzers]: a) durch Löschen oder Vernichten des Inhalts der Anzeigebildschirme, wodurch diese unleserlich werden; b) durch Deaktivieren aller Mittel, die Zugriff auf die Daten des Benutzers oder ihre Anzeige gewähren, ausgenommen zum Entsperren der Sitzung. FTA_SSL.1.2 Die TSF muss erfordern, dass vor dem Entsperren der Sitzung die folgenden Ereignisse stattfinden: [Zuweisung: Ereignisse, die stattfinden müssen]. Verwandte Themen: FIA_UAU.1 Zeitpunkt der Authentisierung Beispiele Vor dem Entsperren der Sitzung müssen bestimmte Ereignisse (definieren) stattfinden
Sperren einer Sitzung auf Initiative des Benutzers	Hierarchisch zu: keiner anderen Komponente. FTA_SSL.2.1 Die TSF muss dem Benutzer erlauben, seine eigene interaktive Sitzung zu sperren: a) durch Löschen oder Vernichten des Inhalts der Anzeigebildschirme, wodurch diese unleserlich werden; b) durch Deaktivieren aller Mittel, die Zugriff auf die Daten des Benutzers oder ihre Anzeige gewähren, ausgenommen zum Entsperren der Sitzung. FTA_SSL.2.2 Die TSF muss erfordern, dass vor dem Entsperren der Sitzung die folgenden Ereignisse stattfinden: [Zuweisung: Ereignisse, die stattfinden müssen]. Verwandte Themen: FIA_UAU.1 Zeitpunkt der Authentisierung Beispiele Der Benutzer muss seine eigene interaktive Sitzung sperren können, indem er den Inhalt der Anzeigebildschirme unleserlich macht und jedwedes Mittel zum Zugriff auf die Daten deaktiviert, außer zum Entsperren der Sitzung
Schließen einer Sitzung auf Veranlassung der TSF	Hierarchisch zu: keiner anderen Komponente. FTA_SSL.3.1 Die TSF muss eine interaktive Sitzung beenden nach [Zuweisung: Zeitraum der Inaktivität eines Benutzers]. Verwandte Themen: Keine verwandten Themen Beispiele

	Nach einer Inaktivitätszeit eines Benutzers (definieren) ist eine interaktive Sitzung zu beenden
FTA_TAB: TOE(EVG)-Zugriffsnachricht	
TOE(EVG)-Standard-Zugriffsnachrichten	Hierarchisch zu: keiner anderen Komponente. FTA_TAB.1.1 Vor Aufbau einer Benutzersitzung muss die TSF eine informative Warnmeldung bezüglich der nicht erlaubten Benutzung des TOE (EVG) anzeigen. Verwandte Themen: Keine verwandten Themen Beispiele Vor Aufbau einer Benutzersitzung muss eine informative Warnmeldung bezüglich der nicht erlaubten Benutzung des Systems angezeigt werden
FTA_TAH: TOE(EVG)-Zugriffschronologie	
TOE(EVG)-Zugriffschronologie	Hierarchisch zu: keiner anderen Komponente. FTA_TAH.1.1 Gleich nach dem erfolgreichen Aufbau einer Sitzung muss die TSF dem Benutzer [Auswahl: das Datum, die Stunde, die Methode, der Ort] des letzten erfolgreichen Aufbaus einer Sitzung anzeigen. Verwandte Themen: Keine verwandten Themen Beispiele Gleich nach dem erfolgreichen Aufbau einer Sitzung sind dem Benutzer das Datum, die Stunde, die Methode und der Ort des letzten erfolgreichen Aufbaus einer Sitzung anzuzeigen
TOE(EVG)-Zugriffschronologie	Hierarchisch zu: keiner anderen Komponente. FTA_TAH.1.2 Gleich nach dem erfolgreichen Aufbau einer Sitzung muss die TSF [Auswahl: das Datum, die Stunde, die Methode, der Ort] den letzten erfolglosen Versuch zum Aufbau einer Sitzung und die Anzahl erfolgloser Versuche seit dem letzten erfolgreichen Aufbau einer Sitzung anzeigen. Verwandte Themen: Keine verwandten Themen Beispiele Gleich nach dem erfolgreichen Aufbau einer Sitzung sind das Datum, die Stunde, die Methode und der Ort des letzten erfolglosen Versuchs zum Aufbau einer Sitzung und die Anzahl erfolgloser Versuche seit dem letzten erfolgreichen Aufbau einer Sitzung anzuzeigen
TOE(EVG)-Zugriffschronologie	Hierarchisch zu: keiner anderen Komponente. FTA_TAH.1.3 Die TSF darf die Informationen über die Zugriffschronologie der Benutzerschnittstelle nicht löschen, ohne dem Benutzer die Möglichkeit zu bieten, diese Informationen wiederzusehen. Verwandte Themen: Keine verwandten Themen Beispiele Die Informationen über die Zugriffschronologie dürfen nicht aus der Benutzerschnittstelle gelöscht werden, ohne dem Benutzer die Möglichkeit zu bieten, diese Informationen wiederzusehen
FTA_TSE: Aufbau einer TOE(EVG)-Sitzung	

Aufbau einer TOE(EVG)-Sitzung	Hierarchisch zu: keiner anderen Komponente. FTA_TSE.1.1 Die TSF muss den Aufbau auf Grundlage von [Zuweisung: Attribute] verweigern können. Verwandte Themen: Keine verwandten Themen Beispiele Der Aufbau einer Sitzung muss auf Grundlage bestimmter Attribute (definieren) verweigert werden können

3.1.11 FTP : Gesicherte Kanäle und Pfade

FTP_ITC: TSF-übergreifender gesicherter Kanal	
TSF-übergreifender gesicherter Kanal	Hierarchisch zu: keiner anderen Komponente. FTP_ITC.1.1 Die TSF muss einen Kanal zur Kommunikation zwischen ihr selbst und einem dezentralen gesicherten IT-Produkt liefern, der sich logisch von den anderen Kommunikationskanälen unterscheidet und der die Identifikation seiner äußeren Enden und den Schutz der Daten, die den Kanal durchqueren, vor Änderung oder Preisgabe gewährleistet. Verwandte Themen: Keine verwandten Themen Beispiele Mit jedem gesicherten System ist ein Kommunikationskanal zu liefern, der sich logisch von den anderen Kanälen unterscheidet und der die Identifikation seiner äußeren Enden und den Schutz der durchquerenden Daten vor Änderung oder Preisgabe gewährleistet
TSF-übergreifender gesicherter Kanal	Hierarchisch zu: keiner anderen Komponente. FTP_ITC.1.2 Die TSF muss [Auswahl: die TSF, das dezentrale gesicherte IT-Produkt] ermöglichen, die Kommunikation über den gesicherten Kanal zu veranlassen. Verwandte Themen: Keine verwandten Themen Beispiele Die Kommunikation über einen gesicherten Kanal muss vom System oder vom betreffenden gesicherten System veranlasst werden können
TSF-übergreifender gesicherter Kanal	Hierarchisch zu: keiner anderen Komponente. FTP_ITC.1.3 Die TSF muss die Kommunikation über den gesicherten Kanal für [Zuweisung: Liste der Funktionen, für die ein gesicherter Kanal gefordert wird] veranlassen. Verwandte Themen: Keine verwandten Themen Beispiele Das System muss die Kommunikation über den gesicherten Kanal für Funktionen veranlassen, für die ein gesicherter Kanal gefordert wird (definieren)
FTP_TRP: Gesicherter Pfad	
Gesicherter Pfad	Hierarchisch zu: keiner anderen Komponente. FTP_TRP.1.1 Die TSF muss einen Pfad zur Kommunikation zwischen ihr selbst und Benutzern [Auswahl: dezentral, lokal] liefern, der sich logisch von den

	anderen Kommunikationspfaden unterscheidet und der die Identifikation seiner äußeren Enden und den Schutz der übertragenen Daten vor Änderung oder Preisgabe gewährleistet. Verwandte Themen: Keine verwandten Themen Beispiele Zwischen dem System und einem Benutzer ist ein Kommunikationspfad zu liefern, der sich logisch von den anderen Pfaden unterscheidet und der die Identifikation seiner äußeren Enden und den Schutz der durchquerenden Daten vor Änderung oder Preisgabe gewährleistet
Gesicherter Pfad	Hierarchisch zu: keiner anderen Komponente. FTP_ITC.1.2 Die TSF muss [Auswahl: die TSF, lokale Benutzer, dezentale Benutzer] ermöglichen, eine Kommunikation über den gesicherten Pfad zu veranlassen. Verwandte Themen: Keine verwandten Themen Beispiele Die Kommunikation über einen gesicherten Pfad muss vom System, von lokalen Benutzern oder von dezentralen Benutzern veranlasst werden können
Gesicherter Pfad	Hierarchisch zu: keiner anderen Komponente. FTP_TRP.1.3 Die TSF muss die Verwendung des gesicherten Pfads für [Auswahl: erstmalige Authentisierung eines Benutzers [Zuweisung: andere Dienste, für die ein gesicherter Pfad gefordert wird]] fordern. Verwandte Themen: Keine verwandten Themen Beispiele Zur erstmaligen Authentisierung eines Benutzers und für andere Dienste (definieren) muss die Verwendung eines gesicherten Pfades gefordert werden

3.2 Aus ISO 17799 hervorgehende Anforderungen

3.2.1 BPS : Sicherheitspolitik (Kapitel 3)

BPS_PSI: Sicherheitspolitik der Information (§3.1)	
BPS_PSI.1.1	Von der Leitung ist eine Dokumentation zur Sicherheitspolitik zu erarbeiten und genehmigen
BPS_PSI.1.2	Die Sicherheitspolitik ist an alle Mitarbeiter zu verteilen
BPS_PSI.1.3	Die Sicherheitspolitik muss die Definition der allgemeinen und speziellen Verantwortlichkeiten einschließen
BPS_PSI.1.4	Die Sicherheitspolitik muss klare und anwendbare Sicherheitsregeln definieren, die alle Sicherheitsaspekte abdecken
BPS_PSI.1.5	Die Sicherheitspolitik muss Regeln zur Klassifizierung der Information enthalten
BPS_PSI.2.1.1	Die Sicherheitspolitik muss regelmäßig überprüft werden und bei Änderungen, die sie beeinflussen, sind Maßnahmen zu treffen, damit sie weiterhin geeignet bleibt
BPS_PSI.2.1.2	Die Aktualisierung der Sicherheitspolitik fällt in den Verantwortungsbereich einer Prüf-Gruppe oder eines Ausschusses, deren bzw. dessen Mitglieder identifiziert sind
BPS_PSI.2.1.3	Die Gruppe oder der Ausschuss zur Prüfung der Sicherheitspolitik muss sich auf die Arbeiten der Sicherheitsmanagement-Gruppe stützen (s. BOS_ISI.1.2)
BPS_PSI.2.2	Vor der Freigabe neuer Dienste des Informationssystems ist die Konformität der Informationssysteme mit der Sicherheitspolitik zu prüfen
BPS_PSI.2.3	Es muss ein Verfahren zur Infragestellung der Sicherheitspolitik bzw. der Sicherheitsregeln auf Grundlage der Informationen geben, die über angezeigte Sicherheitszwischenfälle (Art, Häufigkeit, verbundene Kosten...) gesammelt wurden
BPS_PSI.2.4	Die Angemessenheit der Sicherheitspolitik in bezug auf die Anforderungen der Tätigkeit ist regelmäßig zu überprüfen (z. B. im Rahmen einer globalen Auditpolitik)

3.2.2 BOS : Organisatorische Sicherheit (Kapitel 4)

BOS_ISI: Infrastruktur der Informationssicherheit (§4.1)	
BOS_ISI.1.1	Es ist eine Sicherheitsmanagement-Gruppe zu bilden, die die Leitung bei Sicherheitsinitiativen klar orientiert und wirksam unterstützt
BOS_ISI.1.2	Die Sicherheitsmanagement-Gruppe hat sich auf periodische Zustandsfeststellungen der Sicherheit der Informationssysteme (festgestellte Zwischenfälle, Fortschritte bei der Erfüllung von Aktionsplänen, neue Dienste…) zu stützen
BOS_ISI.2.1	Die Koordinierung der Umsetzung von Maßnahmen zur Beherrschung der Informationssicherheit ist nach Möglichkeit von einer Managementgruppe zu übernehmen, deren Mitglieder verschiedene Funktionen in den betroffenen Abteilungen der Organisation innehaben
BOS_ISI.3.1	Die Verantwortlichkeiten in bezug auf den Schutz des individuellen Kapitals und der Informationen sowie auf die Durchführung von speziellen Sicherheitsverfahren sind klar zu definieren
BOS_ISI.3.2	Die Sicherheitspolitik hat allgemeine Richtlinien für die Zuweisung von Sicherheitsverantwortung zu geben
BOS_ISI.3.3	Die Richtlinien der Sicherheitspolitik für die Zuweisung von Sicherheitsverantwortung können durch detailliertere ergänzende Dokumente für Standorte, Systeme oder spezielle Dienste ergänzt werden
BOS_ISI.4.1	Für neue Infrastrukturen zur Informationsverarbeitung ist ein Verfahren für die

	Genehmigung durch die Leitung zu erarbeiten
BOS_ISI.5.1	Die Organisation muss über eine technologische Kontrolle verfügen, die ihrer Umgebung und ihren Anforderungen angepasst ist (z. B. Kontrolle von Schwachstellen und Korrekturmaßnahmen)
BOS_ISI.5.2	Es muss möglich sein, interne oder externe Spezialisten zu Fragen der Informationssicherheit zu Rate zu ziehen (inkl. nationale Organisationen, die für die Sicherheit von Informationssystemen spezialisiert sind, wie z. B. die DCSSI oder die CNIL)
BOS_ISI.5.3	Die Ratschläge dieser Spezialisten sind innerhalb der gesamten Organisation zu kommunizieren
BOS_ISI.6.1	Es sind geeignete Kontakte mit den rechtmäßigen Behörden, Vorschriften erlassenden Organisationen, Erbringern von IT-Dienstleistungen und Betreibern von Telekommunikationsdiensten zu pflegen
BOS_ISI.6.2	Bei Sicherheitszwischenfällen muss auf die unter BOS_ISI.6.1 aufgeführten Kontakte zurückgegriffen werden können, um schnell und richtig reagieren zu können (Rückgriff auf Beratungsleistungen, Aktion von Partnern...)
BOS_ISI.6.3	Der Austausch mit den unter BOS_ISI.6.1 aufgeführten Kontakten darf für den Schutz der Sicherheitsinformationen keine Gefährdung darstellen
BOS_ISI.7.1	Die Anwendung der Politik zur Informationssicherheit ist von unabhängiger Seite zu überprüfen (z. B. von einer internen oder externen Organisation, die im Sicherheitsbereich keine weitere operative Verantwortung trägt)
BOS_SAT: Sicherheit des Zugriffs durch Dritte (§4.2)	
BOS_SAT.1.1	Die Zugriffsarten auf das Informationssystem durch Dritte (logischer und physischer Zugriff) sind in einem Bestandsverzeichnis zu erfassen, und es ist für alle aufgeführten Zugriffsarten eine Risikoanalyse durchzuführen
BOS_SAT.1.2	Zur Beherrschung der Sicherheit von Zugriffen auf das Informationssystem durch Dritte sind geeignete Maßnahmen umzusetzen
BOS_SAT.1.3	Immer, wenn ein Dritter in das Informationssystem eingreifen muss, muss ein Verantwortlicher der Organisation über Mittel zur Kontrolle der durchgeführten Operationen verfügen
BOS_SAT.1.4	Der Zugriff Dritter auf das Informationssystem muss durch ein funktionales Bedürfnis begründet sein
BOS_SAT.1.5	Der Zugriff Dritter auf das Informationssystem vor Ort darf erst dann stattfinden, nachdem geeignete Mechanismen zur Kontrolle umgesetzt und ein Vertrag unterzeichnet wurde, der die Bedingungen des Zugriffs definiert
BOS_SAT.2.1	Die Bestimmungen, die den Zugriff Dritter auf die Infrastrukturen zur Informationsverarbeitung der Organisation beinhalten, müssen sich auf einen ordnungsgemäßen Vertrag stützen, der alle notwendigen Sicherheitsanforderungen enthält
BOS_SOT: Subunternehmen (§4.3)	
BOS_SOT.1.1	Die Sicherheitsanforderungen einer Organisation, die Management und Beherrschung der Gesamtheit oder eines Teils ihrer IT-Systeme, Netzwerke und/oder ihrer bürotechnischen Umgebung Dritten anvertraut, sind in einem Vertrag zwischen den Parteien zu behandeln
BOS_SOT.1.2	Verträge über ausgelagerte Serviceleistungen müssen die Verantwortlichkeiten der Vertragspartner und mögliche Sanktionen im Falle von Nichterfüllung dieses Vertrages definieren

3.2.3 BCM : Klassifizierung und Kontrolle der Werte (Kapitel 5)

BCM_RLC: Mit Werten verbundene Verantwortung (§5.1)	
BCM_RLC.1.1	Es ist ein globales Bestandsverzeichnis über Güter und Ressourcen (inkl. verbundene Lizenzen) aufzustellen, mit dem zumindest sensible und lebenswichtige Elemente identifiziert werden können
BCM_CLI: Klassifizierung der Information (§5.2)	

BCM_CLI.1.1	Klassifizierungen und verbundene Schutzmaßnahmen, die zu der Information in Beziehung stehen, müssen die Bedürfnisse des Unternehmens nach Teilung oder Beschränkung der Information und geschäftliche Einflüsse, die mit diesen Bedürfnissen in Beziehung stehen, berücksichtigen
BCM_CLI.1.2	Die Verantwortung für die Klassifizierung einer Information und die periodische Überprüfung dieser Klassifikation obliegt nach Möglichkeit dem Absender der Information oder ihrem beauftragten Eigentümer
BCM_CLI.2.1	Für die Etikettierung und die Verarbeitung von Informationen gemäß dem von der Organisation angenommenen Klassifizierungssystems ist ein Bündel von Verfahren zu definieren

3.2.4 BSP : Personelle Sicherheit (Kapitel 6)

BSP_SPR: Sicherheit bei der Definition von Arbeitsplätzen und Ressourcen (§6.1)	
BSP_SPR.1.1	In den Stellenbeschreibungen sind Rollen und Verantwortung auf dem Gebiet der Sicherheit, so wie in der Sicherheitspolitik der Organisation beschrieben, den Möglichkeiten entsprechend zu dokumentieren
BSP_SPR.2.1	Ständige Mitarbeiter sind bei ihrer Bewerbung zu überprüfen
BSP_SPR.3.1	Die Angestellten müssen eine Vertraulichkeitsvereinbarung unterschreiben, die Bestandteil ihrer Einstellungsbedingungen ist
BSP_SPR.4.1	Die Einstellungsbedingungen müssen die Verantwortung des Angestellten auf dem Gebiet der Sicherheit festlegen
BSP_FOU: Schulung der Benutzer (§6.2)	
BSP_FOU.1.1	Alle Angestellten der Organisation und ggf. organisationsexterne Benutzer sind entsprechend zu schulen und müssen regelmäßig über die Sicherheitspolitik und die Verfahren der Organisation auf dem laufenden gehalten werden
BSP_FOU.2.1	Alle Angestellten der Organisation und ggf. organisationsexterne Benutzer sind für den Einsatz von Tools entsprechend zu schulen (vor allem bei der Indienststellung neuer Tools)
BSP_RIS: Reaktion auf Sicherheitszwischenfälle und Funktionsstörungen (§6.3)	
BSP_RIS.1.1	Sicherheitszwischenfälle sind nach ihrer Feststellung so schnell wie möglich über geeignete Managementwege zu melden
BSP_RIS.2.1	Die Benutzer von Informationsdiensten müssen alle in den Systemen oder Diensten beobachteten oder vermuteten Sicherheitsabnormitäten bzw. jedwede Bedrohung, der diese ausgesetzt sein könnten, aufzeichnen und melden
BSP_RIS.3.1	Es sind Verfahren zur Meldung von Funktionsstörungen der Software zu erarbeiten und kontrollieren
BSP_RIS.4.1	Es sind Mechanismen zur Quantifizierung und Kontrolle von Art, Volumen und Kosten von Zwischenfällen und Funktionsstörungen zu erarbeiten
BSP_RIS.5.1	Verstöße gegen die Sicherheitspolitik und Sicherheitsverfahren der Organisation durch die Angestellten sind im Rahmen von Disziplinarmaßnahmen zu ahnden
BSP_RIS.5.2	Die bei Verstößen gegen die Sicherheitspolitik und die Sicherheitsverfahren zu erwartenden Disziplinarmaßnahmen sind allen Angestellten zu kommunizieren

3.2.5 BPE : Physische Sicherheit und Sicherheit der Umgebung (Kapitel 7)

BPE_ZOS: Sicherheitszonen (§7.1)	
BPE_ZOS.1.1	Die Organisationen müssen zum Schutz der Zonen, die Infrastrukturen zur Informationsverarbeitung enthalten, Sicherheitsgürtel nutzen
BPE_ZOS.2.1	Die Sicherheitszonen sind an ihren Eingängen durch geeignete Aufsichtsmaßnahmen zu schützen, so dass nur rechtmäßige Mitarbeiter zu diesen Zutritt haben
BPE_ZOS.3.1	Es sind Sicherheitszonen zu bilden, um Büros, Räume und Infrastrukturen mit speziellen Sicherheitsanforderungen zu schützen

BPE_ZOS.4.1	Für die Arbeit in den Sicherheitszonen sind Aufsichtsmaßnahmen und zusätzliche Richtlinien zu verwenden, um die von den physischen Aufsichtsmaßnahmen zum Schutz der Sicherheitszonen gelieferte Sicherheit zu erhöhen
BPE_ZOS.5.1	Liefer- und Ladezonen sind zu beaufsichtigen und nach Möglichkeit von den Infrastrukturen zur Informationsverarbeitung zu isolieren, um jedweden unerlaubten Zugriff zu verhindern
BPE_SEM: Sicherheit der Hardware (§7.2)	
BPE_SEM.1.1	IT-Hardware ist so zu platzieren und zu schützen, dass Risiken durch Bedrohung, Gefahren aus der Umgebung sowie Gelegenheiten für unrechtmäßigen Zugriff reduziert werden
BPE_SEM.2.1	Die Hardware ist vor Stromausfall oder anderen elektrischen Anomalien zu schützen
BPE_SEM.3.1	Elektrische und Telekommunikationskabel, die Daten übertragen oder Informationsdiensten dienen, sind vor Abhören zu schützen
BPE_SEM.3.2	Elektrische und Telekommunikationskabel, die Daten übertragen oder Informationsdiensten dienen, sind vor Beschädigung zu schützen
BPE_SEM.4.1	Die Hardware ist gemäß den Anweisungen des Herstellers und/oder dokumentierten Verfahren zu warten, um ihre kontinuierliche Verfügbarkeit und Integrität sicherzustellen
BPE_SEM.5.1	Es sind Sicherheitsaufsichts-Verfahren und Maßnahmen durchzusetzen, um Hardware, die außerhalb der Räumlichkeiten einer Organisation verwendet wird, zu sichern
BPE_SEM.6.1	In einer Hardware enthaltene Informationen sind vor Aussonderung oder Wiederverwendung dieser Hardware zu löschen
BPE_MMG: Allgemeine Kontrollmaßnahmen (§7.3)	
BPE_MMG.1.1	Die Organisationen müssen für übersichtliche Büros und Bildschirme sorgen, um die Risiken eines unrechtmäßigen Zugriffs, von Informationsverlust und Schäden an den Informationen zu vermindern
BPE_MMG.2.1	Keine Hardware, keine Information und keine Software darf ohne Genehmigung entfernt werden

3.2.6 BGC : Mangement der Kommunikation und des Betriebs (Kapitel 8)

BGC_PRE: Operative Verfahren und Verantwortlichkeiten (§8.1)	
BGC_PRE.1.1	Operative Verfahren sind zu dokumentieren und zu pflegen
BGC_PRE.2.1	Änderungen an Infrastrukturen zur Informationsverarbeitung und an Informationssystemen sind von den Verantwortlichen für die betreffenden Infrastrukturen zu kontrollieren
BGC_PRE.2.2	Änderungen an Infrastrukturen zur Informationsverarbeitung und an Informationssystemen sind zu dokumentieren
BGC_PRE.3.1	Verantwortlichkeiten und Verfahren für das Management von Zwischenfällen sind so zu gestalten, dass eine schnelle, effektive und geordnete Reaktion auf Sicherheitszwischenfälle gewährleistet ist
BGC_PRE.4.1	Verantwortlichkeiten und Verantwortlichkeitszonen sind so aufzuteilen, dass die Möglichkeiten unrechtmäßiger Änderungen oder des Missbrauchs von Informationen oder Diensten reduziert werden
BGC_PRE.5.1	Infrastrukturen für Entwicklung und Tests sind von operativen Infrastrukturen zu trennen
BGC_PRE.6.1	Vor einem Rückgriff auf externe Dienste zur Verwaltung von Infrastrukturen sind die damit verbundenen Risiken zu identifizieren, und mit dem Lieferanten sind geeignete Aufsichtsmaßnahmen zu vereinbaren und vertraglich zu fixieren
BGC_PRS: Systemplanung und akzeptanz (§8.2)	
BGC_PRS.1.1	Kapazitätsanträge sind zu kontrollieren und zukünftiger Kapazitätsbedarf ist zu

	prognostizieren, um die Verfügbarkeit entsprechender Verarbeitungs- und Speicherleistungen sicherzustellen
BGC_PRS.2.1	Es sind Akzeptanzkriterien für neue Informationssysteme, Aktualisierungen und neue Versionen zu erarbeiten, und es müssen entsprechende Systemversuche vor deren Akzeptanz durchgeführt werden
BGC_PLM: Schutz vor böswilliger Software (§8.3)	
BGC_PLM.1.1	Um vor böswilliger Software zu schützen, sind Maßnahmen zur Beaufsichtigung, Erkennung und Vorbeugung sowie geeignete Maßnahmen zur Sensibilisierung der Benutzer umzusetzen
BGC_INT: Verwaltung (§8.4)	
BGC_INT.1.1	Von geschäftsbezogenen Informationen und wichtiger Software sind in regelmäßigen Abständen Sicherungskopien anzufertigen
BGC_INT.2.1	Operativen Mitarbeiter müssen über ihre Tätigkeit Buch führen
BGC_INT.3.1	Fehler sind anzuzeigen, und es sind Korrekturmaßnahmen einzuleiten
BGC_GER: Netzwerkverwaltung (§8.5)	
BGC_GER.1.1	Zum Erhalt und zur Pflege von Sicherheit in den Netzwerken ist ein Bündel von Aufsichtsmaßnahmen umzusetzen
BGC_MSS: Umgang mit Datenträgern und Datenträgersicherheit (§8.6)	
BGC_MSS.1.1	Das Management beweglicher Datenträger wie z. B. von Bändern, Disketten, Kassetten und gedruckten Berichten ist zu beaufsichtigen
BGC_MSS.2.1	Sind Datenträger nutzlos geworden, müssen sie auf sichere Weise ausgesondert werden
BGC_MSS.3.1	Es sind Verfahren für den Umgang mit und das Lagern von Informationen zu erarbeiten, um diese Informationen vor jeder unrechtmäßigen Preisgabe oder Missbrauch zu schützen
BGC_MSS.4.1	Die Systemdokumentation ist vor unrechtmäßigen Zugriffen zu schützen
BGC_EIL: Austausch von Informationen und Software (§8.7)	
BGC_EIL.1.1	Für den Austausch von Informationen und Software zwischen Organisationen sind Verträge zu erarbeiten, von denen einige offiziell sein können
BGC_EIL.2.1	Im Transit befindliche Datenträger sind vor jedwede unrechtmäßigen Zugriff, vor jeder missbräuchlichen Verwendung oder jeder Minderung zu schützen
BGC_EIL.3.1	Der elektronische Handel ist vor betrügerischen Aktivitäten, vertraglichen Unstimmigkeiten und vor Preisgabe oder Änderung der Information zu schützen
BGC_EIL.4.1	Für die Verwendung von elektronischer Post ist eine Politik zu erarbeiten und es sind Aufsichtsmaßnahmen einzuführen, um die von elektronischer Post hervorgerufenen Sicherheitsrisiken zu vermindern
BGC_EIL.5.1	Um die Risiken des Geschäfts und der Sicherheit, die mit bürotechnischen Systemen verbunden sind, zu beherrschen, sind Politiken und Hinweise zu erarbeiten und umzusetzen
BGC_EIL.6.1	Bevor Informationen der Öffentlichkeit zur Verfügung gestellt werden, muss es ein offizielles Genehmigungsverfahren geben, und die Integrität dieser Informationen ist vor jedweder unrechtmäßigen Änderung zu schützen
BGC_EIL.7.1	Sprachkommunikation, über Telekopie und Video zu schützen, müssen Verfahren und Aufsichtsmaßnahmen zu dessen Schutz vorhanden sein

3.2.7 BMA : Zugriffskontrolle (Kapitel 9)

BMA_EMA: Anforderungen des Unternehmens an die Zugriffskontrolle (§9.1)	
BMA_EMA.1.1	Die geschäftlichen Anforderungen an die Zugriffskontrolle sind zu definieren und zu dokumentieren, und der Zugriff ist darauf zu beschränken, was in der Politik der Zugriffskontrolle definiert wurde
BMA_GAU: Management des Zugriffs der Benutzer (§9.2)	

BMA_GAU.1.1	Es muss für alle Systeme und IT-Dienste, die von mehreren Benutzern genutzt werden, für die Gewährung von Zugriff zu diesen ein offizielles Verfahren zur Eintragung und Austragung von Benutzern geben
BMA_GAU.2.1	Die Zuweisung und Nutzung von Sonderrechten ist zu beschränken und zu beaufsichtigen
BMA_GAU.3.1	Die Zuweisung von Passwörtern hat nach einem offiziellen Managementverfahren zu erfolgen
BMA_GAU.4.1	Die Zugriffsrechte der Benutzer sind in regelmäßigen Abständen durch ein offizielles Verfahren zu überprüfen
BMA_REU: Verantwortung der Benutzer (§9.3)	
BMA_REU.1.1	Die Benutzer müssen bei der Auswahl und Verwendung von Passwörtern Best Practice-Regeln einhalten
BMA_REU.2.1	Die Benutzer haben darauf zu achten, dass Hardware ohne Aufsicht durch geeignete Maßnahmen gesichert ist
BMA_MAR: Zugriffskontrolle auf Netzwerke (§9.4)	
BMA_MAR.1.1	Die Benutzer dürfen nur auf die speziellen Dienste direkten Zugriff haben, zu deren Nutzung sie berechtigt sind
BMA_MAR.2.1	Der Weg zwischen der Benutzerstation und dem IT-Dienst ist zu beaufsichtigen
BMA_MAR.3.1	Entfernte Benutzer müssen sich authentisieren
BMA_MAR.4.1	Verbindungen mit dezentralen IT-Systemen sind zu authentisieren
BMA_MAR.5.1	Der Zugriff auf Diagnoseports muss sicher beherrscht werden
BMA_MAR.6.1	In die Netzwerke sind Aufsichtsmaßnahmen zu integrieren, um Gruppen von IT-Diensten, Benutzergruppen und IT-Systemgruppen zu isolieren
BMA_MAR.7.1	Die Fähigkeit von Benutzern, in Bündelnetzwerken Verbindungen herzustellen, ist Übereinstimmung mit der Politik der Zugriffskontrolle zu beschränken (s. BMA_EMA.1.1)
BMA_MAR.8.1	Für Bündelnetzwerke sind Maßnahmen zur Beaufsichtigung der Datenverteilung zu treffen, um sicherzustellen, dass die PC-Verbindungen und die Informationsflüsse nicht gegen die BMA_EMA.1.1 verstoßen
BMA_MAR.9.1	Die Sicherheitseigenschaften aller von der Organisation verwendeten Dienste sind eindeutig zu beschreiben
BMA_MAS: Zugriffskontrolle auf Betriebssysteme (§9.5)	
BMA_MAS.1.1	Zur Authentisierung von Verbindungen mit speziellen Standorten und tragbarer Hardware ist die Benutzerstation automatisch zu identifizieren
BMA_MAS.2.1	Der Zugriff auf Informationsdienste hat über ein sicheres Verbindungsverfahren zu erfolgen
BMA_MAS.3.1	Alle Benutzer müssen über einen eigenen Identifier (Benutzer-Identifikationscode) verfügen, den nur sie benutzen, so dass Aktivitäten rückwirkend der entsprechenden Person zugeordnet werden können
BMA_MAS.4.1	Die Systeme zur Passwortverwaltung müssen eine wirksame interaktive Funktion zur Verfügung stellen, die die Qualität der Passwörter gewährleistet (keine zu kurzen oder zu einfachen Passwörter, keine Wiederverwendung alter Passwörter...)
BMA_MAS.5.1	Die Verwendung von Utility-Programmen ist zu beschränken und streng zu beaufsichtigen
BMA_MAS.6.1	Benutzern, die eventuell Gegenstand von Nötigung sein könnten, ist eine persönlicher Nötigungsalarm zur Verfügung zu stellen
BMA_MAS.7.1	Nicht verwendete Benutzerstationen, die sich in Zonen mit einem hohen Risiko befinden oder Systeme mit hohem Risiko versorgen, müssen sich nach einer bestimmten Inaktivitätsperiode automatisch ausschalten, um den Zugriff von nicht berechtigten Personen zu verhindern
BMA_MAS.8.1	Die Verbindungszeit ist zu beschränken, um Applikationen mit hohen Risiken zusätzlich abzusichern

BMA_MAA: Zugriffskontrolle auf Applikationen (§9.6)	
BMA_MAA.1.1	Zugriffe auf die Information und auf Funktionen der Applikationssysteme sind in Übereinstimmung mit der Politik der Zugriffskontrolle nach BMA_EMA.1.1 zu beschränken
BMA_MAA.2.1	Kritische Systeme müssen eine besondere (isolierte) IT-Umgebung haben
BMA_SAS: Zugriffskontrolle auf Systeme und deren Verwendung (§9.7)	
BMA_SAS.1.1	Es sind Auditberichte anzufertigen, in denen Ausnahmen und andere sicherheitsrelevante Ereignisse aufzuzeichnen sind, die für einen vereinbarten Zeitraum gelten, um zukünftige Erhebungen und die Kontrolle von Maßnahmen zur Zugriffskontrolle zu erleichtern
BMA_SAS.2.1	Es sind Verfahren zur Kontrolle der Verwendung von Infrastrukturen zur Informationsverarbeitung zu erarbeiten, und das Ergebnis dieser Kontrollaktivitäten ist regelmäßig zu prüfen
BMA_SAS.3.1	Die Uhren der Computers sind zu synchronisieren, um exakte Aufzeichnungen zu erhalten
BMA_IMT: Transportable IT-Einheiten und Telearbeit (§9.8)	
BMA_IMT.1.1	Um vor Risiken, die von der Arbeit mit mobilen IT-Einheiten ausgehen, zu schützen, ist eine offizielle Politik zu erarbeiten und es sind geeignete Aufsichtsmaßnahmen zu treffen
BMA_IMT.2.1	Zur Genehmigung und Beaufsichtigung von Aktivitäten im Rahmen von Telearbeit sind eine Politik und Verfahren zu erarbeiten

3.2.8 BDM : Systementwicklung und wartung (Kapitel 10)

BDM_ESS: Sicherheitsanforderungen von Systemen (§10.1)	
BDM_ESS.1.1	Die Anforderungen des Unternehmens an neue Systeme oder Verbesserungen bestehender Systeme müssen die Anforderungen an Aufsichtsmaßnahmen spezifizieren
BDM_SSA: Sicherheit von Applikationssystemen (§10.2)	
BDM_SSA.1.1	Daten, die in Applikationssysteme eingegeben werden, sind zu bestätigen um sicherzustellen, dass diese korrekt und geeignet ist
BDM_SSA.2.1	In die Systeme sind Gültigkeitsprüfungen zu integrieren, um jedwede Minderung der verarbeiteten Daten zu erkennen
BDM_SSA.3.1	Bei Applikationen, bei denen der Schutz des Inhalts der Nachrichten eine Sicherheitsanforderung darstellt, ist auf die Authentisierung von Nachrichten zurückzugreifen
BDM_SSA.4.1	Daten, die aus Applikationssystemen ausgegeben werden, sind zu bestätigen um sicherzustellen, dass die Verarbeitung der gespeicherten Informationen korrekt und den Umständen entsprechend erfolgt
BDM_COC: Chiffriermaßnahmen (§10.3)	
BDM_COC.1.1	Für den Informationsschutz ist eine Politik für den Einsatz von Chiffrierbefehlen zu erarbeiten und durchzusetzen
BDM_COC.2.1	Vertrauliche oder entscheidende Informationen sind zu ihrem Schutz zu chiffrieren
BDM_COC.3.1	Um die Authentizität und Integrität elektronischer Informationen zu schützen, sind digitale Signaturen zu verwenden
BDM_COC.4.1	Um Unstimmigkeiten darüber beizulegen, ob ein Ereigniss oder eine Aktion stattgefunden hat oder nicht, sind Dienste einzusetzen, die Daten auf Integrität und Ursprung prüfen
BDM_COC.5.1	Es ist ein Managementsystem einzusetzen, das sich auf ein vereinbartes Bündel von Standards, Verfahren und Methoden stützt, damit die Organisation zwei Arten von Chiffriertechniken zu verwenden kann
BDM_SFS: Sicherheit von Systemdateien (§10.4)	

BDM_SFS.1.1	Die Implantation von Software in operative Systeme ist zu beaufsichtigen
BDM_SFS.2.1	Testdaten sind zu schützen und zu beaufsichtigen
BDM_SFS.3.1	Der Zugriff auf Bibliotheken von Quellprogrammen ist streng zu beaufsichtigen
BDM_SED: Sicherheit der Entwicklungs- und Support-Umgebung (§10.5)	
BDM_SED.1.1	Die Anwendung von Änderungen ist anhand von Verfahren zur Beaufsichtigung von Änderungen streng zu kontrollieren, um die Beeinträchtigung von Informationssystemen zu minimieren
BDM_SED.2.1	Wurden Änderungen durchgeführt, sind die Applikationssysteme zu überprüfen und zu testen
BDM_SED.3.1	Die Möglichkeiten, Software-Pakete zu verändern, sind ungünstig zu gestalten, und wichtige Änderungen müssen streng beaufsichtigt werden
BDM_SED.4.1	Der Erwerb, die Verwendung und die Änderung von Software sind streng zu beaufsichtigen und zu kontrollieren, um diese vor der Möglichkeit der Einrichtung verdeckter Kanäle und der Einschleusung Trojanischer Pferde zu schützen
BDM_SED.5.1	Um die Entwicklung von Software durch Subunternehmen abzusichern, sind Aufsichtsmaßnahmen durchzusetzen

3.2.9 BCA : Management des kontinuierlichen Geschäftsbetriebs (Kapitel 11)

BCA_AGC: Aspekte des Managements des kontinuierlichen Geschäftsbetriebs (§ 11.1)	
BCA_AGC.1.1	Um die Kontinuität des Geschäftsbetriebs zu entwickeln und pflegen, ist für die gesamte Organisation ein entsprechendes Verfahren einzuführen
BCA_AGC.2.1	Zur Bestimmung der globalen Herangehensweise an die Kontinuität des Geschäftsbetriebs ist ein strategischer Plan auf der Grundlage einer entsprechenden Risikobewertung zu erarbeiten
BCA_AGC.3.1	Zur Aufrechterhaltung oder Wiederherstellung des Geschäftsbetriebs in den erforderlichen Fristen nach einer Unterbrechung oder einer Störung wichtiger Geschäftsverfahren sind Pläne zu erarbeiten
BCA_AGC.4.1	Um eine Konsistenz aller Pläne zu erreichen und Prioritäten für Tests und Wartung zu identifizieren, ist ein einziger Rahmen zur Planung der Kontinuität des Geschäftsbetriebs aufrecht zu erhalten
BCA_AGC.5.1	Pläne zur Kontinuität des Geschäftsbetriebs sind in regelmäßigen Abständen zu testen und durch regelmäßige Überprüfungen zu waren, um sich zu vergewissern, dass diese auf dem neuesten Stand und wirksam sind

3.2.10 BCO : Einhaltung der Verpflichtungen (Kapitel 12)

BCO_CEL: Einhaltung der gesetzlichen Verpflichtungen (§12.1)	
BCO_CEL.1.1	Für jedes IT-System sind alle gesetzlichen, verordnungsrechtlichen und vertraglichen Anforderungen ausdrücklich zu definieren und zu dokumentieren
BCO_CEL.2.1	Um die Einhaltung gesetzlicher Anforderungen an die Verwendung von Produkten, die durch gewerbliche Eigentumsrechte geschützt sind, und an die Verwendung von Eigentumssoftware sicherzustellen, sind geeignete Verfahren durchzusetzen
BCO_CEL.3.1	Wichtige Register der Organisation sind vor jedwedem Verlust, vor Vernichtung und Fälschung zu schützen
BCO_CEL.4.1	Um personengebundene Informationen so zu schützen, wie es von den entsprechenden Gesetzen verlangt wird, sind Aufsichtsmaßnahmen durchzusetzen
BCO_CEL.5.1	Die Leitung muss die Verwendung von Infrastrukturen zur Informationsverarbeitung erlauben, und es sind Aufsichtsmaßnahmen durchzusetzen, um die missbräuchliche Verwendung dieser Infrastrukturen zu verhindern

BCO_CEL.6.1	Um die Einhaltung von Übereinkommen, Gesetzen, nationalen Vorschriften oder anderen Instrumenten, deren Ziel darin besteht, den Zugriff auf Chiffrierbefehle oder ihre Verwendung zu kontrollieren, sicherzustellen, sind Aufsichtsmaßnahmen zu treffen
BCO_CEL.7.1	Wenn eine Aktion gegen eine Person zivil- oder strafrechtliche Verfolgung impliziert, müssen die vorgelegten Beweise den Regeln entsprechen, die in dem entsprechenden Gesetz oder den Vorschriften des entsprechenden zuständigen Gerichts vorgesehen sind
BCO_CEL.7.2	Wenn eine Aktion gegen eine Person zivil- oder strafrechtliche Verfolgung impliziert, müssen die vorgelegten Beweise allen Standards bzw. allen für die Vorlage zulässiger Beweise bekannten Best Practice-Bestimmungen entsprechen
BCO_RPS: Überprüfung der Sicherheitspolitik und der technischen Konformität (§12.2)	
BCO_RPS.1.1	Die Verantwortlichen haben darauf zu achten, dass in ihrem Verantwortungsbereich alle Sicherheitsverfahren korrekt eingehalten werden
BCO_RPS.1.2	Alle Bereiche innerhalb der Organisation sind regelmäßig zu überprüfen, um ihre Konformität mit der Sicherheitspolitik und ihren Standards sicherzustellen
BCO_RPS.2.1	IT-Systeme sind regelmäßig auf ihre Übereinstimmung mit den geltenden Sicherheitsstandards zu überprüfen
BCO_CAS: Hinweise zu Systemaudits (§12.3)	
BCO_CAS.1.1	Audits operativer Systeme sind so zu planen und durchzuführen, dass Risiken einer Störung des Geschäftsbetriebs minimiert werden
BCO_CAS.2.1	Der Zugriff auf die Tools zur Auditierung der Systeme ist zu schützen, um jedwede Verletzung oder jeden eventuellen Missbrauch zu verhindern

3.3 Sicherheits-Policyen der Informationssysteme (PSSI)

3.3.1 PSI : Politique de sécurité

PSI-01: Weiterentwicklungen der PSSI

Eine Organisation kann sich im Laufe der Zeit verändern (Organisation, Aufgaben, Umkreis, strategische Leitlinien, Werte). Demzufolge unterliegt ihr Informationssystem häufigen Änderungen, so wie auch die Bedrohungen und Verwundbarkeiten, denen es ausgesetzt ist. Aus diesem Grund ist die PSSI erneut zu überprüfen:

- bei jeder wichtigen Weiterentwicklung des Kontextes oder des Informationssystems;

- bei einer Weiterentwicklung der Bedrohung;

- bei einer Weiterentwicklung der Sicherheitsbedürfnisse;

- im Ergebnis eines Audits;- im Ergebnis eines Sicherheitszwischenfalls;

- systematisch in festgelegten Intervallen;

auf Anforderung einer Autorität (Sicherheitsverantwortlicher, Leitung...) im Rahmen eines Verfahrens, dass in der PSSI festzulegen ist.

PSI-02: Verteilung der PSSI

Die PSSI sowie ihre operativen Ableitungen sind einwandfrei zu dokumentieren. Zu den aktualisierten Referenzversionen müssen allen Mitarbeitern der Organisation problemlos Zugriff haben.

Die PSSI muss allen internen Akteuren sowie ggf. allen Personen, die auf das Informationssystem der Organisation zugreifen (Subunternehmen, Dienstleister, Praktikanten...), bekannt sein.

Da sie aber auch vertrauliche Informationen beinhalten kann, können die Mitarbeiter der Organisation in Abhängigkeit ihrer Aufgaben in unterschiedlichem Maße betroffen sein. Aus diesem Grund empfiehlt es sich, ggf. Zusammenfassungen zu erarbeiten und zu verteilen, die bezüglich der Informationen, die für die jeweiligen Leser besonders zutreffend sind, detailliertere Auszüge enthalten. Ziel dieser Zusammenfassungen ist es, jeden in Abhängigkeit seiner Bedürfnisse mit den Anforderungen und den Sicherheitsregeln bekannt zu machen.

PSI-03: Überprüfung der Anwendung der PSSI

Es empfiehlt sich, Verfahren und Mittel zur internen Kontrolle der Anwendung der PSSI einzurichten und diese durch Verfahren und externe Audits zu ergänzen. Der Erlass von Regeln ist nur dann sinnvoll, wenn auch Mittel vorhanden sind, um deren Einhaltung zu kontrollieren, insbesondere auf dem Gebiet der Sicherheit. Alles andere wäre inakzeptabel.

PSI-04: Schutz der Organisation anvertrauten Informationen

Dieses Prinzip erlaubt, sich von der Vollständigkeit der gesetzlichen Referenzen zu überzeugen.

Informationen, die sich vorübergehend im Besitz der Organisation befinden und die von ihrem Eigentümer klassifiziert oder mit einem besonderen Vermerk versehen wurden, sind unter Anwendung der gleichen Maßnahmen streng zu schützen, wie es bei der Ausgangsorganisation der Fall wäre. Diese Maßnahmen können sich aus der Anwendung von

Gesetzestexten (Gesetz Nr. 78-17 vom 6. Januar 1978 über Informatik, Dateien und Freiheiten [französisches Datenschutzgesetz - Anm. d. Üb.], interministeriellen Anweisungen wie z. B. solchen Anweisungen, die die Einhaltung der Klassifikation von Informationen erfordern, die mit dem Verteidigungsgeheimnis verbunden sind [IGI 900], Anweisungen über den Schutz von Informationen des nationalen Erbes [II 486] oder über die Errichtung eines Verteidigungsmarktes [II 2000] ergeben.

Sollten sich diese Regeln nicht aus gemeinsamen gesetzlichen Vorschriften ergeben, sind die Verpflichtungen der Parteien gegenüber den ausgetauschten Informationen vertraglich zu fixieren.

PSI-05: Annahme einer Bedürfnisskala

Die objektive Klassifizierung der wesentlichen Elemente der Organisation (Informationen und Funktionen) kann mit einer verschiedene Sicherheitskriterien (Verfügbarkeit, Integrität, Vertraulichkeit...) widerspiegelnde Bedürfnisskala erleichtert werden.

Ansatzpunkte zur Ausarbeitung einer Bedürfnisskala werden mit der Methodologie des PSSI-Leitfadens vorgeschlagen. Es wird ausgeführt, dass für jedes Sicherheitskriterium eine Wichtung und Referenzwerte zu erarbeiten sind. Die Referenzwerte müssen objektiv, organisationsspezifisch und mit ihrer strategischen Ausrichtung verbunden sein.

Im übrigen empfiehlt der im PSSI-Leitfaden angebotene typisierte Plan die Aufnahme dieser Skala in die PSSI.

PSI-06: Kriterien zur Bestimmung der Sicherheitsbedürfnisse

Mit der Methodologie des PSSI-Leitfadens werden Ansatzpunkte zur Ausarbeitung einer Bedürfnisskala vorgeschlagen, um die Sicherheitsbedürfnisse (im Hinblick auf Verfügbarkeit, Integrität, Vertraulichkeit...) der wesentlichen Elemente (Informationen und Funktionen) gemäß einer geeigneten Bedürfnisskala zu bestimmen.

Für die identifizierten wesentlichen Elemente bieten sich zwei Möglichkeiten an:

- direkte Verwendung dieser Bedürfnisskala für nicht klassifizierte Elemente;

- Elemente, die bereits klassifiziert wurden (z. B. sensible, lebenswichtige oder solche Informationen, die mit dem Verteidigungsgeheimnis im Zusammenhang stehen...), werden mit dieser Bedürfnisskala in Beziehung gesetzt.

Im wesentlichen werden Sicherheitsbedürfnisse von Informationen, wenn man von Informationen, die mit dem Verteidigungsgeheimnis im Zusammenhang stehen und personenbezogenen Informationen, für die die geltenden Gesetze anzuwenden sind, einmal absieht, nach ihrem Ursprung, der Bewertung ihres Interesses und ihrer Gültigkeit in bezug auf ihren Lebenszyklus im operativen Produktionsprozess bestimmt:

- die Überprüfung des Ursprungs der Informationen (Ausland, Gemeingut, Kunde, Lieferant...) ist für die Sicherheit besonders wichtig; in Abhängigkeit der Herkunft können spezielle Kriterien angewendet werden, um eine

eventuelle Verletzung der Vertraulichkeit vor ihrem Sammeln, ihre Exaktheit, Gültigkeit und ihrer korrekten Präsentation für das System beurteilen zu können;

- die Bewertung des Interesses und der Gültigkeit der zusammengetragenen Informationen erfolgt durch Anwendung eindeutiger Kriterien, die von der Leitung der Organisation bestimmt wurden und die sich auf einen bestimmten Bereich (F&E, Qualitätszirkel, Erfassung technologischer Entwicklungen..) beziehen können.

Hinweis in bezug auf sensible Informationen:

Sensibel sind solche Informationen, deren Preisgabe oder Minderung die Interessen des Staates oder der Organisation, für die ein finanzieller Schaden z. B. den Ruin bedeuten würde, beschädigen könnten. Folglich ist deren Vertraulichkeit immer zu schützen, wobei sehr oft einem großen Integritätsbedürfnis Rechnung zu tragen ist.

Zu dieser Kategorie gehören die folgenden Informationen:

- einerseits Informationen, die mit dem Verteidigungsgeheimnis lt. Art. 5 [IGI 900] im Zusammenhang stehen; die Organisation ist demnach verpflichtet, die gesetzlich vorgeschriebenen Klassifizierungsregeln einzuhalten; weiterhin ist die Organisation verpflichtet, Mittel einzusetzen, um mit diesen Gesetzen konform zu sein;

- andererseits Informationen, die sensibel, aber lt. Art. 4 [REC 901] keine Verteidigungsinformationen sind, d. h. mit der Aufgabe oder der Aktivität der Organisation verbundene Informationen (z. B. über technisches Know-how oder Informationen, die unter das Berufsgeheimnis fallen), Informationen, die sich auf kommerzielle Angebote beziehen oder Auskunft geben über den Sicherheitszustand (z. B. Ergebnisse von internen Audits).

Ziel der Klassifizierung ist es vor allem, den Benutzer über die Sensibilität der vom ihm verarbeiteten Informationen zu informieren, die Kontrolle zu erleichtern und, was sich daraus ergibt, den Schutz sensibler Informationen zu verbessern. Für Informationen, die nicht unter die [IGI 900] fallen, ist die gewählte Klassifizierung von der Organisation zu genehmigen.

Hinweis in bezug auf lebenswichtige Informationen:

Als ,,lebenswichtig" gelten solche Informationen, deren Vorhandensein zum ordnungsgemäßen Betrieb der Organisation notwendig ist. Deren Verfügbarkeit immer zu schützen, wobei sehr oft einem großen Integritätsbedürfnis Rechnung zu tragen ist.

Folgende Informationen können als lebenswichtig erkannt werden:

- einerseits Informationen, die mit dem Verteidigungsgeheimnis lt. Art. 6 [IGI 900] im Zusammenhang stehen,

- andererseits Informationen, die lt. Art. 5 [REC 901] nicht unter das Verteidigungsgeheimnis fallen, aber für den Betrieb des Systems notwendig sind, sowie solche Informationen, die nicht von Art. 5 erfasst werden (z. B.

Artikelnomenklaturen für eine Produktionseinheit).

Ziel der Klassifizierung ist es vor allem, den Benutzer über die Sensibilität der vom ihm verarbeiteten Informationen zu informieren, die Kontrolle zu erleichtern und, was sich daraus ergibt, den Schutz lebenswichtiger Informationen zu verbessern. Für Informationen, die nicht unter die [IGI 900] fallen, ist die gewählte Klassifizierung von der Organisation zu genehmigen. Insbesondere kann eine Mindest-Verfügbarkeitsschwelle für lebenswichtige Informationen (verarbeitete oder verarbeitende) festgelegt werden, unterhalb derer das Informationssystem als nicht einsatzfähig gilt .

Hinweis in bezug auf strategische Informationen:

Als strategisch gelten die Informationen, deren Kenntnis notwendig ist, um die Ziele zu erreichen, die der strategischen Ausrichtung der Organisation entsprechen. Sie können durch Gesetze geschützt werden, aber auch Gegenstand von Verträgen, Übereinkommen oder Absichtserklärungen, die vom BGB geschützt werden, sein.

Ziel der Klassifizierung ist es vor allem, den Benutzer über die Sensibilität der vom ihm verarbeiteten Informationen zu informieren, die Kontrolle zu erleichtern und, was sich daraus ergibt, den Schutz strategischer Informationen zu verbessern; die Klassifizierung kann sich auf organisationsspezifische Kriterien, wie z. B. einen bestimmten Bereich (Forschung, Innovationen, Märkte...), das genehmigte Wertniveau und die Gültigkeitsdauer, stützen.

Hinweis in bezug auf personenbezogene Informationen:

Art. 4 des Gesetzes ,,Informatik und Freiheiten" [französisches Datenschutzgesetz - Anm. d. Üb.] den Begriff personenbezogene Information wie folgt: ,,Personenbezogene Informationen sind solche, anhand derer, gleich welcher Form auch immer, direkt oder indirekt natürliche Personen, auf die sie sich beziehen, identifiziert werden können, unabhängig davon, ob die Verarbeitung durch eine natürliche oder juristische Person erfolgt."

Ziel der Klassifizierung ist es vor allem, die Kontrolle zu erleichtern und, was sich daraus ergibt, den Schutz personenbezogener Informationen lt. Gesetz zu verbessern; die Klassifizierung kann sich auf organisationseigene Kriterien, wie z. B. einen bestimmten Bereich (medizinisch, Personalmanagement...), die Art der Umfrage oder Untersuchung, den Ort der Verarbeitung oder Speicherung, stützen.

Hinweis in bezug auf kostenintensive Informationen:

Kostenintensive Informationen sind solche, die Bestandteil des Vermögens der Organisation sind und deren Sammlung, Verarbeitung, Speicherung

	oder Übertragung längere Fristen in Anspruch nehmen oder erhöhte Gestellungskosten verursachen. Für die Kategorie kostenintensive Informationen können die unter strategische Informationen genannten Gesetze angewendet werden. Ziel der Klassifizierung ist es vor allem, den Benutzer über die Sensibilität der vom ihm verarbeiteten Informationen zu informieren, die Kontrolle zu erleichtern und, was sich daraus ergibt, den Schutz strategischer Informationen zu verbessern; die Klassifizierung kann sich auf organisationsspezifische Kriterien, wie z. B. einen bestimmten Bereich (Forschung, Innovationen, Märkte...), das genehmigte Wertniveau und die Gültigkeitsdauer, stützen.
PSI-07: „Deklassifizierung" von Informationen	Manchmal werden Informationen zeitlich begrenzt klassifiziert. Diese Mindestzeiträume sind je nach Art der Informationen durch Regeln zu bestimmen.
PPSI-08: „Überklassifizierung" von Informationen	Der Schutzgrad muss sich proportional zur Klassifizierung von Informationen und Systemen verhalten. Auch wenn eine höhere Klassifizierung besseren Schutz verspricht, so besteht doch die Gefahr, dass das Vertrauen in die Klassifizierungsmethode durch eine systematische Überklassifizierung beschädigt wird. Um dies zu vermeiden, ist: - von einer Überklassifizierung der Information abzusehen, - die zugewiesene Klassifizierung in regelmäßigen Abständen zu überprüfen.
PSI-09: Identifikation und Geltungsbereich der Klassifizierung einer Information	Die Identifikation der Klassifikation muss klar, allen bekannt und sofort erkennbar sein. Für Dokumente ist sie in die Grafikcharta zu integrieren, für Disketten und andere Medien in die Verfahren zur Verwaltung dieser Medien, für Dateien in die Verfahren zur Organisation der IT-Ressourcen. Maschinen, die zu einem Netzwerk gehören, das vertrauliche Informationen verarbeitet oder beherbergt, sind ebenfalls zu identifizieren. Die Mitarbeiter müssen sich dessen bewusst sein, dass die Klassifikation ihrer Organisation einer Klassifikation von Informationen, die von anderen Organisationen kommen, nicht entsprechen muss. Umgekehrt ist die für die Organisation definierte Klassifizierung nur im Umkreis der PSSI sinnvoll.
PSI-10: Definition und Kontrolle von Berechtigungen	Die Organisation, die Eigentümerin der Informationen ist, muss in der Lage sein, Berechtigungen, die mit der Verwendung von Informationen verbunden sind, zuzuweisen. Weiterhin hat sie die Aufgabe, Regeln für das Management dieser Berechtigungen zu bestimmen und entsprechende Kontrollen durchzuführen. Die Organisation kann zu einem bestimmten Augenblick Verwahrerin von Informationen sein, ohne dass sie ihr notwendigerweise auch gehören. In diesem Fall hat sie keine Entscheidungsbefugnis im Hinblick auf die verarbeiteten Informationen, sondern muss die vom Eigentümer (Kunden, Subunternehmen...) zu ihrer Verwaltung definierten Regeln auf Grundlage der zugewiesenen Klassifizierung einhalten.
PSI-11: Kriterien für	Um Indiskretionen und Schwund zu vermeiden, dürfen Informationen und im

die interne Verteilung von Informationen

allgemeinen die damit verbundenen Medien nur in einer Umgebung verwendet werden, die den von der Organisation definierten Sicherheitsanforderungen entspricht.

Ziel der Kontrolle der internen Verteilung ist es, sich darüber zu vergewissern, dass die Informationen ausschließlich den Personen zur Verfügung stehen, die diese im Rahmen ihrer Arbeitsaufgaben kennen müssen. Mit einer Kontrolle wird ebenfalls überprüft, dass das Kopieren von Informationen in Übereinstimmung mit den gesetzlichen Befugnissen (Autorenrechte, Copyright), der Gesetzgebung (Verteidigungsgeheimnis) und den speziellen Zwängen der Organisation erfolgt.

Das Bedürfnis der Kenntnis (für die Vertraulichkeit) kann auf das Bedürfnis der Änderung (für die Integrität), der Verwendung (für die Disponibilität)... ausgeweitet werden.

PSI-12: Kriterien für die externe Verteilung von Informationen

Durch nicht kontrollierte Zurverfügungstellung von schutzbedürftigen Informationen kann der Organisation Schaden zugefügt werden (z. B. Verlust an Glaubwürdigkeit oder Ansehen, Aneignung von Know-how...).

Durch die Schaffung von Kriterien wird abgesichert, dass Informationen, die eine Organisation verlassen, zu einer vorherigen Überprüfung der Berechtigung des Empfängers zwingen, wenn es sich um vertrauliche Informationen handelt, oder einer vertraglichen Klausel, die die betreffenden Organisationen bindet; bei personengebundenen Informationen hat die Kommunikation gemäß den geltenden Gesetzen zu erfolgen.

Im übrigen kann im Rahmen dieses Prinzips in Erwägung gezogen werden, dass die externe Verteilung von Informationen von berechtigten Mitarbeitern vorgenommen wird sowie nach einem vorherigen Genehmigungsverfahren.

3.3.2 ORG : Organisatorische Sicherheit

ORG-01: Allgemeine Verantwortlichkeiten für die Sicherheit des Informationssystems der Organisation

Um die globale Verantwortung für die Errichtung, die Umsetzung und den Betrieb eines SIS-Managements in der Organisation abzusichern, ist ein Verantwortlicher für die Sicherheit der Informationssysteme (Sicherheitsverantwortlicher o. ä.) zu benennen. Dieser Sicherheitsverantwortliche (dieser Begriff wird im weiteren angewendet werden) ist auf allen Ebenen und in allen Bereichen der Organisation für die Einhaltung der PSSI verantwortlich.

Er untersteht der Leitung der Organisation, muss in der Lage sein, Sicherheitsaspekte gegen Partikularinteressen durchzusetzen und Sicherheit in alle Projekte integrieren, die die Informationssysteme berühren.

Die Besetzung dieser Funktion ist ein starkes Signal, das notwendig ist, um zu unterstreichen, dass die Organisation ihrer PSSI eine große Bedeutung beimisst.

Bei Verwaltungen wird diese Verantwortung durch SIS-Funktionsstrukturen abgedeckt.

ORG-02: Verantwortlichkeiten für die Erarbeitung und

Die PSSI betrifft alle lebenswichtigen Funktionen einer Organisation. Im allgemeinen kann eine längere Störung ihres oder ihrer Informationssysteme von dieser nicht hingenommen werden. Aus diesem

Umsetzung einer PSSI

Grund ist die PSSI von strategischem Interesse: Es muss eine Regel geben, die die Verantwortlichkeiten für ihre Erarbeitung als auch ihre unausweichlichen Weiterentwicklungen, z. B. im Rahmen eines Lenkungsausschusses, definiert.

Außerdem definiert die Regel in der Phase der Umsetzung der PSSI die Verantwortung der qualifizierten Autoritäten bei der Einführung und Kontrolle der Sicherheitshinweise für die Installation und den Betrieb der Mittel, die das Informationssystem bilden.

Sie unterstreicht vor allem die Notwendigkeit der Integration des Sicherheitsgedankens in die Planung und Entwicklung neuer Projekte, die mit dem Informationssystem in Beziehung stehen, und zwar von Anfang an. Weiterhin weist die PSSI darauf hin, dass die Sicherheit des Informationssystems nicht auf Aspekte und Weiterentwicklungen auf dem Gebiet der Technik beschränkt ist, sondern alle Weiterentwicklungen oder Änderungen der Organisation, ihrer Aufgaben usw. einschließt.

ORG-03: Wahrnehmung der Verantwortlichkeiten

Das allgemeine Prinzip zur Sensibilisierung der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung OECD lautet: ,,Die Zuweisungen und Verantwortlichkeiten von Eigentümern, Lieferanten und Benutzern eines Informationssystems und der anderen Parteien, die von der Sicherheit der Informationssysteme betroffen sind, sind klar zum Ausdruck zu bringen."

Es ist von grundlegender Bedeutung, dass für alle sicherheitsrelevanten Bereiche (Sicherheit der Infrastruktur, Sicherheit in den Projekten und Applikationsfamilien, Sicherheit der Räumlichkeiten, Sicherheitsdokumentation...) ein Verantwortlicher benannt wird, und dass alle sicherheitsrelevanten Aufgaben zugewiesen sind.

Die organisatorische Sicherheit muss in jedem der genannten Bereiche strategische, Lenkungs- und operative Ebenen einschließen.

Vor allem muss klar und eindeutig identifiziert werden können, wer für die Sicherheit in Verbindung mit Netzwerken oder transversalen Systemen, wie z. B. dem Bürotechnik-Netzwerk oder den Einrichtungen für den Zugriff auf externe Netzwerke, verantwortlich ist.

ORG-04: Verantwortlichkeiten auf Entscheiderebene

Es fällt in den Zuständigkeitsbereich der Entscheiderebene, sämtliche Vorkehrungen dafür zu treffen, dass Sicherheit in Übereinstimmung mit den Bedürfnissen und Zielen der Organisation geplant und umgesetzt sowie zu überprüfen, dass die Sicherheitspolitik der Informationssysteme (PSSI) eingehalten wird.

(1) Bei einem Ministerium wird diese Ebene von einem hohen Beamten der Verteidigung wahrgenommen, der dafür vom Minister beauftragt wurde. Er ist für die Anwendung aller für die Sicherheit der Verteidigung relevanten Bestimmungen, den Geheimnisschutz und die Sicherheit der Informationssysteme verantwortlich.

Bei der Erfüllung seiner Aufgaben kann er von einem für die Sicherheit der Informationssysteme zuständigen Beamten unterstützt werden, zu dessen wichtigsten Aufgaben gehören ([IGI 900], Art. 19 und [REC 901], Art. 18):

- die Bedingungen für die Anwendung der interministeriellen Anweisungen zu präziseren;

- Anweisungen, die speziell für sein Ministerium gelten, zu erarbeiten und deren Anwendung zu kontrollieren;

- die Sensibilisierung der Behörden zu organisieren;

- die Verbindung zu den interministeriellen Spezialausschüssen sicherzustellen.

(2) Bei einer öffentlichen oder privaten Organisation entspricht dieses Niveau einem hohen Sicherheitsverantwortlichen, der von der Geschäftsleitung beauftragt wurde. Dieser wird bei der Erfüllung seiner Aufgaben von einem Sicherheitsausschuss unterstützt.

Die Geschäftsleitung legt auf der Grundlage von Vorschlägen des hohen Sicherheitsverantwortlichen sowie in Übereinstimmung mit den Zielen der Organisation und der verschiedenen umgesetzten Politiken (Politik des Personalmanagements, Budget- und Produktionspolitik...) die wichtigsten Leitlinien auf dem Gebiet der SIS fest. Sie kann im übrigen die Instanz sein, die die Sicherheitspolitik der Informationssysteme (PSSI) bestätigt.

Die Anwendung der Sicherheitspolitik der Informationssysteme (PSSI) wird vom hohen Sicherheitsverantwortlichen kontrolliert. Dieser nimmt an den Beratungen der Geschäftsleitung teil und berät diese in allen sicherheitsrelevanten Fragen, wie z. B. bei der Definition von Zielen, der Bereitstellung von Ressourcen und von Personal.

Der Sicherheitsausschuss, dem der hohe Sicherheitsverantwortliche vorsitzt, versammelt die Sicherheitsverantwortlichen der verschiedenen Funktionen der Organisation. Er kontrolliert die koordinierte Umsetzung der PSSI. Insbesondere überprüft er, dass die Sicherheitsregeln konsistent sind und entscheidet bei Konflikten mit anderen Regeln und Praktiken, die innerhalb der Organisation Anwendung finden.

(3) Für die Sicherheit der Informationssysteme kann ein Team gebildet werden, das dem hohen Verteidigungsbeamten (oder dem hohen Sicherheitsverantwortlichen) zur Verfügung steht, insofern sich eine derartige Maßnahme aufgrund der Bedürfnisse der Organisation als notwendig erweist. Dieses Team führt Spezialisten auf den Gebieten Informatik und Telekommunikationsnetzwerktechnik zusammen, aber auch andere Spezialisten, die für nicht technologische Aspekte der Informationssysteme verantwortlich sind und eine Sicherheitsausbildung absolviert haben. Ihre Hauptaufgaben sind:

- Vorbereitung und Koordinierung von Sicherheitsaktivitäten;

- periodische Bewertung von Schwachstellen;

- Suche technischer Lösungen und Erarbeitung von Verfahren;

- Einführung von Sensibilisierungs- und Schulungsprogrammen;

- Sicherheitsgutachten (auf Anforderung der Geschäftsleitung).

Das Sicherheitsteam kann aus ständigen Mitarbeitern zusammengesetzt sein, wobei auf Grundlage der Bedürfnisse (bei größeren Projekten, deren Ziel eine erhebliche Weiterentwicklung des Informationssystems ist) zeitweilig Spezialisten oder Fachleute der betroffenen Bereiche hinzugezogen werden können.

ORG-05: Verantwortlichkeiten auf Lenkungsebene

Wenn es die Größe einer Organisation rechtfertigt, sind Untereinheiten (Standorte, Teile des Informationssystems, Abteilungen...) mit Verantwortlichen ,,vor Ort", klar definierten Verantwortlichkeiten und einer effektiven Koordination mit der zentralen Struktur zu identifizieren.

Bei einer ministeriellen Organisation entspricht diese Ebene qualifizierten Beamten, die für die Sicherheit der Informationssysteme, für die sie zuständig sind, die Verantwortung tragen ([IGI 900], Art. 20 und [REC 901], Art. 19).

Bei einer privaten Organisation entspricht diese Ebene einem vor Ort tätigen Sicherheitsbetreuer, der für die Sicherheit der Informationssysteme Verantwortung trägt und dem vom Sicherheitsverantwortlichen geleiteten Team angehört.

Ihre Aufgabe besteht darin, die Umsetzung der PSSI auf ihrer jeweiligen Ebene (Leitung, Dienst, Einrichtung...) zu lenken und insbesondere folgendes zu tun:

- sich zu vergewissern, dass die vertraglichen und gesetzlichen Bestimmungen eingehalten werden;

- interne Hinweise und Richtlinien auszuarbeiten;

- sich zu vergewissern, dass interne Sicherheitskontrollen korrekt durchgeführt werden;

- die Sensibilisierung der Mitarbeiter zu organisieren;

Diese Autoritäten können sich auf die Kompetenzen des Sicherheitsteams stützen.

Um Lenkungsaufgaben der SIS zu erfüllen, ist es manchmal notwendig, Lenkungsausschüsse zu bilden, die zuständig sind für:

- die Kontrolle der Anwendung der PSSI;

- die Verarbeitung von Krisen, die mit der Sicherheit des Informationssystems verbunden sind;

- die technologische Kontrolle, die Kontrolle der Bedürfnisse der SIS der Organisation und die Weiterentwicklung der PSSI.

ORG-06: Verantwortlichkeiten auf operativer Ebene

Die hierarchischen Autoritäten sind auf allen Ebenen persönlich für die Anwendung der Maßnahmen verantwortlich, die von qualifizierten Autoritäten zur Gewährleistung der Sicherheit der Informationssysteme definiert wurden ([IGI 900], Art. 20 und [REC 901], Art. 19).

Alle Personen, die zu der Organisation gehören oder in diese eingreifen, sind in die SIS einbezogen und tragen Verantwortung. Diese ist klar zu

formalisieren und jedem zur Kenntnis zu bringen.

Die Verantwortlichkeiten und Verpflichtungen dieses Personenkreises betreffen vor allem (s. auch Sicherheitsprinzipien in bezug auf vertragliche Verpflichtungen):

- die Einhaltung von Gesetzen und Vorschriften,

- die Einhaltung der Politik und spezieller Regeln (die mit einem Projekt, einer Einrichtung, einer besonderen Funktion verbunden sind),

- den Zugriff auf ein Netzwerk oder auf Räumlichkeiten in einer anderen Organisation.

Diese Verantwortlichkeiten können auf Grundlage ihrer Funktionen und Berechtigungen verstärkt werden (s. Sicherheitsprinzipien in bezug auf Berechtigungen). So tragen z. B. Administratoren von Informationssystemen, Geheimnisträger und Benutzer sensibler Funktionen von Sicherheitssystemen im Bereich SIS eine besondere Verantwortung.

Andererseits müssen die Verantwortlichkeiten der Mitarbeiter der Organisation auch den Fall berücksichtigen, wenn sie in ein anderes Sicherheitssystem als das ihrer eigenen Organisation (Kunden, Partner...) eingreifen.

ORG-07: Andere Verantwortliche der Organisation, die bei der SIS eine Rolle spielen

Es gibt andere Funktionen, die keine Sicherheitsfunktionen sind, mit denen aber trotzdem besondere Rollen wahrgenommen werden, die für die Sicherheit der Informationssysteme unverzichtbar sind.

Diese Funktionen sind vor allem:

- Sicherheitsmitarbeiter oder -betreuer

Damit jeder Standort, Dienst bzw. jede Einheit die Hinweise und Verfahren umsetzen kann, greifen die hierarchisch übergeordneten Autoritäten auf einen oder mehrere Sicherheitsmitarbeiter zurück, die im wesentlichen die Funktion einer Schnittstelle zwischen den Benutzern des Informationssystems und den Verantwortlichen für die Kontrolle der SIS erfüllen.

Damit werden zwei Ziele verfolgt:

o die Verteilung von sicherheitsrelevanten Informationen und Anwendungsregeln für den richtigen Gebrauch wird erleichtert;

o die Weiterleitung von Informationen von den Benutzern zu den zentralen Stellen, die für die Kontrolle der Sicherheit zuständig sind, ist gewährleistet.

Diese Aufgabe ist von solchen Mitarbeitern wahrzunehmen, die sowohl geografisch als auch im Hinblick auf ihre Tätigkeit nahe am Benutzer sind.

Diese Mitarbeiter sind die bevorzugten Ansprechpartner des Sicherheitsteams.

Sie können ebenfalls für Ressourcen, die mehreren operativen Einheiten gemeinsam sind, zuständig sein. Ihre Aufgabe besteht also darin, Schutzmaßnahmen, die mit den Zielen der Einheiten kompatibel sind, umzusetzen, und Sicherheitsprobleme vor Ort zu lösen. Fehlen derartige Maßnahmen, könnten sich daraus Schwierigkeiten bei der Abgrenzung

funktionaler Aufgaben von Sicherheitsaktionen ergeben.

- Juristen der Organisation

Juristen spielen im Bereich SIS der Organisation eine unverzichtbare Rolle. Auf Initiative des Sicherheitsverantwortlichen nehmen sie teil an:

o der Erarbeitung von Sicherheitsklauseln und SIS-Verpflichtungen in kommerziellen und Arbeitsverträgen;

o Klagen und Geschäftsanweisungen;

o der Integration von SIS-Regeln in die verschiedenen Bestimmungen und Chartas der Organisation;

o der Bestimmung der Beziehungen zu den Subunternehmen,

o der Bestimmung der Verantwortung der Auditoren.

Zusätzlich zu ihren operativen Kontrollfunktionen erfüllen Auditoren die folgenden Rollen:

o Definition der Auditstrategie, vor allem bei SIS-Audits;

o Durchführung von SIS-Audits, oder Veranlassung von deren Durchführung, gemäß Auditplan oder auf Anforderung der Leitungen in Abstimmung mit dem Sicherheitsverantwortlichen;

o Information des Auftraggebers und der auditierten Einheiten gemäß ihres Kenntnisbedarfs und Information des Sicherheitsverantwortlichen über die Aufdeckung eventueller SIS-Zwischenfälle oder -Anomalien.

o andere Verantwortungen, die bei der Durchführung spezieller Sicherheitsaktionen, z. B. im Rahmen von Plänen zur Verbesserung der Sicherheit, bei der Migration von Applikationen, notwendig werden können.

ORG-08: Spezielle Einheiten zur Management und Lenkung der Sicherheit

Es können weitere Spezialeinheiten geschaffen werden. Dazu können insbesondere gehören:

- ein Sicherheitsausschuss, der für die Pflege der PSSI und die Kontrolle der Anwendung des prioritären Aktionsplans verantwortlich ist. Dieser Ausschuss ist ebenfalls dafür zuständig, die Gesamtleitung über die Effektivität der durchgeführten Politik auf dem laufenden zu halten.

- ein Krisenteam, das ggf. mit der Umsetzung eines Notfallverfahrens beauftragt wird, um Notfällen zu begegnen;

- ein Team zur technologischen Kontrolle, das für die Kontrolle von Sicherheitswarnungen und ihre Bearbeitung je nach Dringlichkeit zuständig ist;

- ein Auditstab, der für die Durchführung von Audits des Informationssystems zuständig ist.

ORG-09: Anwendung des Begriffs der Inhaberverantwortung

Der Begriff der Inhaberverantwortung betrifft, so wie unter ORG-05 (Verantwortlichkeiten auf Lenkungsebene) definiert, den in der Hierarchie einer organisatorischen Einheit (Einrichtung, Dienst, Verantwortungs- oder Profit-Center) Verantwortlichen oder die qualifizierte Autorität, der bzw. die

	zur Erfüllung seiner/ihrer Aufgaben über eigene Mitarbeiter und materielle Ressourcen verfügt. Der Begriff der Inhaberschaft findet Anwendung auf den Informations- und Softwarebestand sowie auf die Hardware, die Bestandteil des Informationssystems ist. Er umfasst die Verpflichtung zur Einhaltung der Gesetze, Vorschriften und Regeln, die für die Organisation gelten. Die betreffenden Informationen, Hard- und Software können der Organisation gehören oder dieser von Dritten (Kunden, Partner, Leistungserbringer...) anvertraut worden sein.Der verantwortliche Inhaber bestimmt die akzeptablen Risikoebenen sowie die Bedingungen für den Zugriff auf Dateien, für die Aktualisierung von Informationen (in Übereinstimmung mit den innerhalb der Organisation geltenden Klassifizierungsregeln) oder für Änderungen an der ihm zur Verfügung stehenden Hard- und Software.
ORG-10: Anwendung des Begriffs der Verwahrerverantwortung	Der verantwortliche Inhaber beauftragt den verantwortlichen Verwahrer, beim Sammeln, bei der Verarbeitung, der Verteilung und der Speicherung zum Schutz der Informationen, Hard- und Software geltenten Gesetze, Vorschriften und Regeln anzuwenden. Der verantwortliche Verwahrer kann z. B. ein Informatiker des Betriebsteams, ein Dokumentar, ein Sekretär usw. sein. Er ist der Hüter eines Teils des Vermögens der Organisation und deswegen insbesondere dazu verpflichtet, das Gesetz, das sich auf den rechtlichen Schutz der ihm anvertrauten Software bezieht (Raubkopien), einzuhalten.
ORG-11: Management der Beziehungen mit anderen Beteiligten im Rahmen der SIS	Die PSSI muss die Art der Beziehungen formalisieren, Hinweise geben und sachdienliche Kontakte mit Drittorganisationen identifizieren, die im Rahmen der Kontrolle und der Pflege der SIS eine Rolle spielen (oder eine Rolle spielen könnten). Zu diesen Organisationen können gehören: - in der Kategorie Autoritäten und Partner: o Organisationen, mit denen beim Erkennen einer böswilligen Handlung im Rahmen des Informationssystems Kontakt aufzunehmen ist; o Organisationen zur Kontrolle und Warnung; o Auditorganisationen; - in der Kategorie der Leistungserbringer: o Erbringer von Telekommunikationsleistungen; o Erbringer von Leistungen innerhalb der Organisation; o Leistungserbringer, die Subunternehmer sind und/oder für einen Teil des Betriebs des Sicherheitssystems zuständig sind; o spezialisierte Leistungserbringer im Rahmen der Sicherheit; o externe Auditorganisationen. Von wesentlicher Bedeutung ist es, den Zugriff zu beherrschen, unabhängig davon, ob es sich dabei um den Zugriff auf das Informationssystem oder auf sensible Informationen handelt, die das Informationssystem oder seine

Sicherheit betreffen. Sobald Dritte aufgrund von Servicenotwendigkeiten diese Art von Zugriff haben müssen, muss man sich vergewissern, dass die gleichen Sicherheitsregeln, die auch für interne Mitarbeiter gelten, anwendbar sind (Dokumentation und vertragliche Aspekte) und von den betreffenden Akteuren angewendet werden.

ORG-12: Vertraglicher Rahmen für den Austausch gesicherter Daten

Mit der Möglichkeit des Zugriffs interner oder externe Dienste oder telematischer Applikationen auf die Organisation stellt sich das Problem der Kooperation zwischen den verschiedenen Informationssystemen. Ziel dieser Regel ist es, Datenverlust, Datenänderung und Datenmissbrauch vorzubeugen.

Folglich sind Verantwortlichkeiten und durch Verträge untersetzte Verpflichtungen der verschiedenen Beteiligten sowohl auf Ebene der Datenübertragung als auch der sie umfassenden Applikationen vorzusehen. Der gesicherte Datenaustausch findet im Rahmen von Übertragungen wie oben definiert statt. Unter vertraglicher Rahmen sind Vereinbarungen zwischen mehreren Parteien für den Datenaustausch zu verstehen, unabhängig davon, ob dieser von Informationstechnologien gestützt wird oder nicht. Diese Regel bezieht sich auch auf den Austausch von IT-Daten.

Die von der Organisation mit allen Benutzern des Informationssystems abgeschlossenen Vereinbarungen oder Verträge beinhalten Kontrollklauseln, die z. B. präzisieren:

- die Verantwortung für das Management der ausgetauschten Datenflüsse;
- die Sicherheitsverfahren, die für diese Verfahren anzuwenden sind;
- die Standards zur Strukturierung der Daten;
- die Verantwortlichkeiten bei Informationsverlust;
- spezielle Maßnahmen zum Schutz von Chiffrierschlüsseln.

ORG-13: Bedingungen für die Verwendung von organisationsexternen Telekommunikationsnetzen

Durch Verwendung organisationsexterner Telekommunikationsnetze werden Benutzer miteinander in Beziehung gebracht, die à priori nicht die gleichen Sicherheitsanforderungen haben und die überdies nicht überwachbar sind.

Die Bedingungen zur gesicherten Nutzung organisationsexterner Telekommunikationsnetze beziehen sich vor allem auf die Kontrolle der Mittel, die eventuell vom zentralisierten Management des Informationssystems nicht erfasst werden, wie z. B. installierte Modems oder Minitel-Geräte. Für den Spezialfall E-Mail sind Maßnahmen zu treffen, deren Ziel darin besteht, den Versand von Nachrichten, die abgefangen und unerlaubt geändert werden könnten und deswegen Schwachstellen sind, zu kontrollieren, sowie im Hinblick auf gesetzliche Erwägungen in bezug auf Integrität und Ursprung der Daten.

Mitarbeiter der Organisation, die von zu Hause aus tätig sind (Telearbeit), befinden sich in einer privaten Umgebung, über das die Organisation keinerlei Kontrolle hat. Aus diesem Grund muss sie besondere technische Regeln bezüglich der Zugriffsrechte erlassen, aber auch den Benutzer sensibilisieren, indem sie ihn über seine Verantwortung gegenüber den Informationen, die ihm das Unternehmen anvertraut, aufklärt.

	Bei externen Netzwerke finden die Seiten der OSI-Architektur Anwendung.
ORG-14: Spezielle Informationsschutzklauseln	Ist ein Austausch mit Dritten vorgesehen, können in die Verträge spezielle Klauseln eingearbeitet werden, die bestimmen, in welchem Rahmen dieser Austausch stattfindet. Diese Klauseln beziehen sich auf solche Mittel wie z. B.: - die Kontrolle der Abwesenheit böswilliger Codes; - intern angewendete Schutzregeln (Definition einer Tabelle mit sich überschneidenden Klassifizierungen); - das Medium, über das der Austausch stattfindet, und die Mittel zum Schutz vor Preisgabe, zur Bewahrung der Integrität und von Integrität und Ursprung der Daten... Wenn sich die Organisation verpflichtet hat, Klauseln von Dritten einzuhalten, hat sie darüber ihre Mitarbeiter zu informieren bzw. diese sogar in ihre PSSI aufzunehmen.
ORG-15: Auswahl, Koordination und Einsatz von Chiffriermitteln	Aufgrund des Anforderungsprofils ist die Auswahl der Mittel (z. B. einzusetzende Software oder Chiffrierwerkzeuge) und in einem noch stärkeren Maße der externen Dienstleister (z. B. Zertifizierer, Erbringer vertraulicher Leistungen) von der Sicherheitsstruktur der Organisation zu bestätigen und zu genehmigen, wenn dieser Auswahl nicht direkt von dieser Struktur vorgenommen wird. Zu den wesentlichen Elementen, die in bezug auf Vertraulichkeit zu berücksichtigen sind, gehört die Entscheidung, ob von den Mitarbeitern chiffrierte Dokumente von der Organisation überschrieben werden müssen oder nicht. Hier sind Lösungen auf Ebene des Schlüsselmanagements (z. B. Einsetzen eines Schlüsselverwahrers) bzw. von Funktionen und Utility-Programmen (systematische Einrichtung von Feldern für Überschreiben) denkbar. Für jede dieser Basisfunktionen (Vertraulichkeit, Authentisierung, Sende- und Empfangsbeweis) sind Regeln zu erarbeiten, die die einzuhaltenden Mindestanforderungen (sowohl prinzipielle als auch operative) festlegen. Die Auswahl externer Leistungserbringer (z. B. Zertifizierungsbehörde oder Zertifizierungsdienstleister) ist eine Entscheidung, die die Struktur betrifft und von der Sicherheitsstruktur zu genehmigen und von der Gesamtleitung zu bestätigen ist. Es ist darauf zu achten, dass in jedem Vertrag mit diesen Leistungserbringern entsprechende Schutz-, Sicherheits- und Garantieklauseln wirklich vorhanden sind.
ORG-16: Einrichtung einer Organisation zur Kontrolle und Vorbeugung	Es ist eine Organisation zu definieren, die die Liste der wichtigsten Risiken, die auf dem Informationssystem lasten (neue Bedrohungen, neue Sicherheitsbedürfnisse, bedeutendere Weiterentwicklung des Informationssystems...) kontrolliert und pflegt. Diese Organisation muss über Kompetenzen interner oder externer Spezialisten verfügen sowie über ausreichende Mittel, um Informationen zu sammeln und zu qualifizieren (Kontakte, Abonnements bei speziellen Organisationen, s. ORG-12, Management der Beziehungen mit anderen Beteiligten im Rahmen der SIS).

Weiterhin muss sie über kontrollierte Mittel sowie über Mittel zur Verteilung relevanter Sicherheitsinformationen zu vorbeugenden Zwecken verfügen.Diese Kontrolle kann ausgelagert oder in Verbindung mit Organisationen wie z. B. dem CERTA durchgeführt werden, das französische Verwaltungen regelmäßig mit Hinweisen, Warnungen oder Empfehlungen versorgt.

Allerdings ist auch ein bestehendes Kontrollsystem auf die Beachtung von Empfehlungen zu kontrollieren. Die Kontrolle ist kein Selbstzweck, und auch die Umsetzung der Empfehlungen, die sich aus der Kontrolle ergeben haben, ist zu kontrollieren.

ORG-17: Organisation von Krisenstäben

Das Prinzip besteht darin, vorsorglich eine Organisation zu definieren (Verantwortlichkeiten, Funktionsweise und Mittel), die in der Lage ist, auf größere Zwischenfälle zu reagieren, denen das Informationssystem ausgesetzt sein kann. Zu diesem Zweck sind Climbing-Verfahren zu erarbeiten, zu testen und Mitarbeiter für deren Durchführung zu schulen.

Am wichtigsten ist es, Akteure auf der richtigen hierarchischen Ebene zu identifizieren, um in der Lage zu sein, so schnell Entscheidungen zu treffen, wie es die Situation verlangt.

Weiterhin sind Mittel und Verfahren zu erarbeiten, die in der Lage sind:

- die Warmeldung zu verbreiten;

- Informationen zu sammeln;

- einen Krisenstab zu bilden;

- über konservierende Maßnahmen zu entscheiden;

- einen Aktionsplan mit Korrekturmaßnahmen zu erarbeiten.

3.3.3 GER : SIS-Risikomanagement

GER-01: Definition des Rahmens des SIS-Risikomanagements

Das SIS-Risikomanagement ist ein kontinuierlicher Prozess, dessen Rahmen (Ressourcen, Mittel, Verantwortung...) für jeden seiner Aspekte präzise beschrieben werden muss:

- Sicherheitsbewertung: Analyse und Bewertung des SIS-Risikos durch Vergleich des Risikoniveaus mit vorher definierten Risikokriterien;

- Risikobehandlung: Verminderung, Übertragung oder Annahme des vermittels der vorhergehenden Aufgabe bewerteten Risikos;

- Risikoakzeptanz: Akzeptanz des verarbeiteten Risikos und ggf. des Restrisikos;

- Risiko-Kommunikation: Austausch oder Vermittlung von Informationen über das Risiko.

GER-02: Identifikation der Sicherheitsziele

Die Identifikation der Sicherheitsziele dient der Definition des tatsächlichen SIS-Sicherheitsbedürfnisses der Organisation. Dieses SIS-Lastenheft kann unter Einhaltung der folgenden Schritte und unter Berücksichtigung der Aufgaben oder der Geschäftstätigkeit der Organisation wie folgt formalisiert werden:

- Zusammenstellung der strategischen Elemente (Zwänge, Anforderungen, strategische Ausrichtung, Bezugssystem...),

- Ausdruck der Sicherheitsbedürfnisse der wesentlichen Elemente (Informationen und Funktionen) im Hinblick auf Verfügbarkeit, Integrität, Vertraulichkeit... und gemäß einer objektiven Bedürfnisskala,

- Untersuchung der Bedrohungen, die auf der Organisation lasten (Charakterisierung der bedrohlichen Elemente, Untersuchung der Verwundbarkeiten...),

- Identifikation der tatsächlichen Risiken für die Organisation.

Die Sicherheitsziele müssen alle identifizierten Risiken abdecken.

Mit der Definition der Sicherheitsbedürfnisse können die Sensibilitätsniveaus (im Hinblick auf Vertraulichkeit, Integrität, Verfügbarkeit...), die den Bestandteilen eines Informationssystems garantiert werden müssen, eindeutig beschrieben werden.

Die vom Informationssystem erwartete Sicherheit ist in seinen Spezifikationen zu beschreiben, da sie wie seine Leistungsfähigkeit oder die von ihm zu erbringenden Dienste eine wesentliche Dimension dieses Systems darstellt. Der Ausdruck der Sicherheitsbedürfnisse ist methodisch und global einer tiefgreifenden Prüfung zu unterziehen. Wird diese Analyse methodisch durchgeführt, können eine homogene Gesamtsicht auf die SIS-Problematik gewahrt, ein vollständiges Sicherheits-Bezugssystem erstellt und die meisten Risiken, denen das System ausgesetzt ist, erfasst werden.

Auch sind durch eine Risikobewertung in diesem Stadium die Verwundbarkeiten des Systems und eventuelle Folgen für seine Sicherheit zu ermitteln, so dass die Einführung bestimmter Abwehrmittel, deren Kosten-Effektivitäts-Verhältnis abgewogen wurde, begründet werden kann. So können z. B. die Ergebnisse einer Risikobewertung dazu führen, dass auf Sicherungssysteme zurückgegriffen wird, um Kompetenz- oder Geldmangel auszugleichen.

Die Entscheidung, Risiken zu berücksichtigen oder nicht, kann auf der Grundlage dieser Analysen getroffen werden.

GER-03: Umstände, die eine Neubewertung der Sicherheit des Informationssystems rechtfertigen

Die OECD-Leitlinien über die Neubewertung der Sicherheit von Informationssystemen und netzwerken legt fest:

,,Alle beteiligten Parteien müssen die Sicherheit von Informationssystemen und netzwerken prüfen und neu bewerten und ihre Sicherheitspolitiken, praktiken, maßnahmen und verfahren entsprechend ändern. Neue oder sich entwickelnde Verwundbarkeiten und Bedrohungen sind ständig zu ermitteln. Alle beteiligten Parteien müssen alle Sicherheitsaspekte kontinuierlich überprüfen, neu bewerten und ändern, um diesen sich entwickelnden Risiken zu begegnen."

	Wurde ein System einer Bewertung unterzogen, wäre es irrig anzunehmen, dass es fehlerfrei oder nicht änderbar sei, ganz im Gegenteil: Es muss neuen Anforderungen genügen, die in Änderungen an der Hardware, Software und Dokumentation ihren Ausdruck finden. Außerdem können sich neue Sicherheitsbedürfnisse und Risiken manifestieren, die zu bewerten und zu bearbeiten sind. So gesehen liegt es auf der Hand, dass bestimmte Änderungen, wie z. B. die Umstrukturierung des Kernbereichs eines Betriebssystems, eine Neubewertung erforderlich machen, in die Teilergebnisse der vorherigen Bewertung einfließen können. Im Gegensatz dazu können andere Änderungen neubewertungsneutral sein, insofern sie nur die Teile des Informationssystems berühren, die von Sicherheitskomponenten getrennt sind und diese nicht beeinflussen. Diese Überlegungen können zu einer Neubewertung des Systems oder lediglich zu einer Änderung einzelner Regeln führen.
GER-04: Perspektivische Untersuchung der SIS-Weiterentwicklung	Mit einer perspektivischen Untersuchung der SIS-Weiterentwicklung kann mittelfristigen Bedürfnissen der Organisation vorgegriffen werden, und es können neue sicherheitsrelevante Ziele, Software, Hardware oder andere Mechanismen integriert werden. Diese perspektivische Untersuchung ist untrennbar mit den strategischen Ausrichtungen (oder einem Leitschema für Informationssysteme) verbunden, das sich auf die neuen Informationstechnologien, die von der Organisation ausgewählt werden könnten, bezieht. Weiterhin zielt diese Regel darauf ab zu überprüfen, dass jedwede Weiterentwicklung des Informationssystems mit den in der Organisation geltenden Sicherheitsprinzipien übereinstimmt. Sollte dies nicht der Fall sein, kann mit Hilfe der perspektivischen Untersuchung gemessen werden, welche Auswirkungen auf die Sicherheit des Systems zu erwarten sind, und es können Einrichtungen technischer oder organisatorischer Art vorgeschlagen werden, die eventuell zu einer Änderung der Prinzipien und Regeln der PSSI der Organisation führen.
GER-05: Beaufsichtigung und Kontrolle einiger spezieller Informationsflüsse	Erlaubt die Kommunikation Austausch zwischen innen und außen des Informationssystems sowie innerhalb des Informationssystems oder sogar zwischen voneinander abgeschirmten Bereichen, kann sich die Einführung von speziellen Regeln und Mitteln zur Kontrolle dieser Informationsflüsse als notwendig erweisen. Das Interesse an der Durchführung einer methodischen Risikoanalyse wird insbesondere hier deutlich, da mit ihr alle Informationsflüsse, die vom Sicherheitssystem ausgetauscht werden, sowie die Gefahren, die auf ihnen lasten, klar identifiziert werden können. Das hat z. B. Einfluss auf die Regeln für den E-Mail-Austausch mit der Außenwelt, wobei Vorrichtungen deren Umsetzung in bezug auf die Größe der ausgetauschten Nachrichten, die Art der Anhänge (Akzeptanz aktiver Inhalte oder keine Akzeptanz), die Überprüfung auf Viren und böswillige Codes ermöglichen. Diese verschiedenen Maßnahmen müssen mit der Sicherheitscharta und den Vorschriften für die ordnungsgemäße Nutzung von IT-Ressourcen übereinstimmen, die jeder Benutzer unterschreiben muss. Diese dienen nicht nur seiner Information, sondern es kommen überdies andere Aspekte (Pflicht zur Mitarbeiterinformation, Achtung der

Privatsphäre) ins Spiel.

Ein anderes Beispiel ist der ausgehende http-Fluss (Konsultation externer Web-Server von Stellen im Informationssystem), der von Einrichtungen wie z. B. Ausgangsidentifikation, Aufzeichnung des Verbindungsverlaufs durch einen Ausgabeproxy... begleitet wird.

Es ist kein Ziel dieser Ausführung, alle Umstände zu beleuchten oder für alles und jeden geeignete Regeln und Mittel anzubieten. Vielmehr soll allgemein darauf aufmerksam gemacht werden, dass diese Informationsflüsse im Hinblick auf ihre Sicherheitsrelevanz zu identifizieren und zu analysieren sind sowie im Interesse der Gewährleistung von Sicherheit Anlass für die Einrichtung spezieller Lösungen sein können oder müssen.

GER-06: Identifikation von Diensten und Mitteln, die Chiffrierung rechtfertigen

Unter Berücksichtigung von Folgen sowohl technischer als auch gesetzlicher Natur sind die Applikationen und Dienste zu identifizieren, auf die Chiffriermittel angewendet werden müssen. Für jede Applikation oder jeden Dienst sind Chiffrierlösungen zu identifizieren. Die Auswahl hat in Abhängigkeit von der Art der verarbeiteten Informationen und vom gesetzlichen Rahmen zu erfolgen. So dürfen z. B. bei einem Informationssystem, das verteidigungsrelevante Informationen verarbeitet, nur speziell zugelassene Chiffriermittel eingesetzt werden. Auch hier bestimmt die Risikoabschätzung, welche gesetzlichen Zwänge auf diesem Gebiet zu berücksichtigen sind, sowie die Bedürfnisse der Benutzer.

3.3.4 CDV : Sicherheit und Lebenszyklus

CDV-01: Projektintegration der SIS

Die PSSI hat eine Organisation zu planen, die gewährleistet, dass über den gesamten Lebenszyklus eines Projekts (Untersuchung von Zweckmäßigkeit, Machbarkeit, des allgemeinen und detaillierten Konzepts bis hin zur Aussonderung) Sicherheitsaspekte Berücksichtigung finden. Diese Organisation muss, trotz ihrer Projektautonomie, in enger Beziehung mit den für Lenkung und Koordinierung der allgemeinen SIS in der Organisation Verantwortlichen stehen.

Insbesondere muss die Organisation die Bereiche und Projekte identifizieren, bei denen die Mitwirkung anerkannte Experten erforderlich ist.

CDV-02: Bedingungen für die Inbetriebnahme neuer Bestandteile des Informationssystems

Diese Regel zielt darauf ab, Risiken zu reduzieren, die auf mangelnde Zusammenarbeit mit den anderen Bestandteilen der Umgebung auf dem Gebiet der Sicherheit oder mangelnde Eignung der geltenden Hinweise für Technik und menschliches Verhalten zurückzuführen sind, die Ursache für Betriebsfehler sein können.

Neue Bestandteile des Informationssystems (Hard- oder Software) sind, auch wenn sie als effektiv und mit den Herstellungsspezifikationen übereinstimmend gelten, in ihrer neuen Umgebung Integrationstests zu unterziehen.

Gemäß den aus dieser Regel ableitbaren Bedingungen ist z. B. eine vollständige Akzeptanz des Bestandteils im Hinblick auf die Identifikation der durchzuführenden technischen und prozedualen Änderungen denkbar sowie die Möglichkeit, im Falle eines Scheiterns die technische Umgebung

	in den alten Zustand vor Inbetriebnahme dieses Bestandteils zurückzuführen.
CDV-03: Überprüfung der Software vor ihrer Inbetriebnahme	Softwareüberprüfungen vor ihrer Inbetriebnahme dienen insbesondere dazu, die Bedrohung durch Virusinfektion, andere böswillige Codes und nicht konforme Software zu bekämpfen. Viren oder andere böswillige Codes stellen für die Sicherheit von Systemen ein immer schwerwiegenderes Problem dar. Sie bedrohen alle Organisationen und Institutionen, unabhängig von deren Verwundbarkeitsniveau. Dabei sind die Organisationen, die der Öffentlichkeit am breitesten zugänglich sind, IT-Piraterie am meisten ausgesetzt, bei der oft genug technisches Geschick und Medienwirksamkeit im Vordergrund stehen. Das Risiko der Nicht-Konformität von Software betrifft sensible Organisationen, die, greifen sie bei der Softwareentwicklung auf Dienstleistungserbringer zurück, Exaktheit und Konformität der Codeprogrammierung überprüfen müssen, um sich davon zu überzeugen, dass das Programm nur das macht, wofür es entwickelt wurde und dass es keine versteckten Pforten gibt, über die Programmfunktionen später unberechtigterweise geändert werden können. Um das Eindringen schädigender Software (Viren, Würmer, Trojaner, logische Bomben) zu vermeiden und zu erkennen, können Vorsichtsmaßnahmen ergriffen werden. Alle IT-Speichermedien, deren Herkunft außerhalb der Organisation liegt und vor allem Medien unbekannter Herkunft, sind zu überprüfen. Eine Gegenmaßnahme, um dieser Bedrohung zu begegnen, ist die Installation von Mitteln für eine systematische Erkennung.
CDV-04: Bedingungen für die Umsetzung von Sicherheitsmaßnahmen	Der Sicherheitsverantwortliche überprüft, ob die Hardwareprogramme seiner Organisation mit den Sicherheitsleitlinien und der strategischen Ausrichtung der Organisation übereinstimmen und in bezug dazu gültig sind.Weitere Kontrollen werden im Rahmen von Untersuchungen, die von ihm ausgelöst werden, vom Sicherheitsteam durchgeführt. Diese Kontrollen zeichnen sich durch ihre Tragweite und Tiefe aus, wobei: - ihre Tragweite mit der Definition des Detailniveaus im Zusammenhang steht (vertikale Komponente); - ihre Tiefe mit den verschiedenen Elementen, die bei der Kontrolle Berücksichtigung finden, im Zusammenhang steht (horizontale Komponente). Für ein vertrauensvolles Klima innerhalb des Personals und einen ordnungsgemäßen Ablauf der Geschäftstätigkeit der Organisation spielt eine Abstufung der Sicherheitskontrollen eine wichtige Rolle. Die die Abstufung bestimmenden Umstände sind vom Entscheiderniveau klar festzulegen. Die Kontrollen selbst sind außerhalb eines möglichen juristischen oder disziplinarischen Rahmens mit kommunikativen und personalvorbereitenden Mitteln zu begleiten.
CDV-05: Bedingungen	Die Verwundbarkeit der Einheiten (Hardware, Software, Netzwerke,

für die Sicherheitsüberprüfungen durch die Lenkungsebene

Räumlichkeiten, Organisationen, Mitarbeiter) durch Bedrohungen (zufällige oder absichtliche, natürliche, durch Menschen oder die Umgebung) und deren Angriffsmethoden ist in periodischen Abständen neu zu bewerten, um das Sicherheitsniveau des Informationssystems einschätzen zu können.

Die für die Sicherheit notwendigen technischen Bedingungen, Methoden und Tools werden dabei von qualifizierten Autoritäten festgelegt, die vom Sicherheitsteam der Organisation unterstützt werden. Diese überprüfen auch deren ordnungsgemäße Anwendung und Effektivität auf der Grundlage von auf Entscheiderebene gefassten Kriterien.

Diese Überprüfungen, die im Rahmen geplanter Sicherheitsinspektionen oder audits stattfinden, erstrecken sich auf die verschiedenen sicherheitsrelevanten Einheiten des Informationssystems (Hardware, Software, Netzwerke, Räumlichkeiten, Organisationen, Mitarbeiter).

Kontrollen, für die auf das operative Personal sowie technische Ressourcen zurückgegriffen werden muss, sind von der Lenkungsebene zu planen, damit sie den ordnungsgemäßen Geschäftsbetrieb der Organisation nicht behindern.

CDV-06: Kontinuität der Sicherheitsüberprüfungen durch die operative Ebene

Die Sicherheitsmitarbeiter führen durch Anwendung der von der qualifizierten Autorität vorgegebenen Sicherheitsschwellen die Kontrollen durch, für die sie zuständig sind. Werden wiederholt Abweichungen festgestellt, die z. B. mit Erfordernissen des Betriebs oder einer Zustandsänderung des Informationssystems verbunden sind, kann das Lenkungsniveau diese Schwellen ändern.

Ihre Kontrolltätigkeiten sind eng mit der Erfüllung operativer Aufgaben verbunden und beziehen sich auf ([IGI 900], Art. 20, [REC 901], Art. 19):

- den Schutz von Personen und betreffen z. B. die ständige Aktualisierung der Liste der Festangestellten und derjenigen, die ggf. Informationen verarbeiten,

- den Schutz von Informationen und betreffen z. B. die Überprüfung der Vernichtung klassifizierter Informationen, die aus dem System entfernt werden müssen,

- den Schutz von Systemen und Netzwerken und betreffen z. B. die Kontrolle der Verteilung von Authentisierungselementen für klassifizierte Applikationen an Benutzer.

Diese Kontrollen ergänzen die den Ingenieuren anvertrauten Kontrollmaßnahmen, die auch die Auditberichte auswerten.

CDV-07: Ständige Kontrolle der Schutzmittel

Ein anderer wichtiger Sicherheitsaspekt ist die Überprüfung von Integrität und Verfügbarkeit der Schutzmittel. Diese Regel bezieht sich auf Sicherheitsvorrichtungen, denen vertraut wird, um den Schutz der Informationsverarbeitung sicherzustellen. Hierbei handelt es sich um Ausrüstungen, Mechanismen (Hard- und Software) und ihre Dokumentation, wie in Art. 10 [IGI 900], ,,Kontrollierte Sicherheitsartikel der Informationssysteme" (ACSSI) genannt, oder Art. 9 [REC 901].

Die Gewährung dieses Vertrauens rechtfertigt eine Überprüfung von

	Integrität und Verfügbarkeit dieser Mittel, die einen Lebenszyklus haben: Sie wurden entworfen, durchgeführt, verwendet, repariert und dann ausgesondert oder vernichtet. Ihre Integrität und Verfügbarkeit sind die Basis für eine effektive Sicherheit und werden durch die Umsetzung spezieller Managementmaßnahmen gewährleistet, zu denen ein möglichst proaktives Wartungsprogramm gehört.
CDV-08: Anwendung von Codekontrolle und Akzeptanzverfahren	Um die Einschleusung böswilliger Funktionen zu bekämpfen, können Verfahren zur Überprüfung der Entwicklung durchgeführt werden (z. B. gegenseitige Codeüberprüfung, Versiegelung des Codes unter Verantwortung des Entwicklers, Überprüfung durch Musterentnahme...). Bei jeder Codeentwicklung oder änderung ist dieser vor seiner Inbetriebnahme Akzeptanz-, Integrations- und Qualifikationsverfahren zu unterziehen. Dabei ist der Überprüfung von Werten und Grenzen eine besondere Aufmerksamkeit zu schenken.
CDV-09: Andere Arten notwendiger Kontrollen	Hier einige Beispiele für Kontrolle, die durchzuführen sind: - Kontrolle, ob die PSSI-Normen in den Projekten Anwendung finden; - Kontrolle, ob die PSSI in bezug auf die Weiterentwicklung der Anforderungen des Informationssystems alles abdeckt; - Kontrolle, ob die Regeln für das Zugriffs- und Berechtigungsmanagement richtig angewendet werden; - Kontrolle, ob die Sicherheitsregeln von Dritten (Outsourcing von Diensten, IT-Outsourcing-Verträge) eingehalten werden; - Kontrolle der Zwischenfall-Basis und der Vollständigkeit der Verarbeitungen; - Kontrolle der Einhaltung der Regeln für den physischen Zugriff; - regelmäßige Kontrolle von Aktivitätsverläufen, insbesondere der Konten, die über weitreichende Privilegien innerhalb des Systems verfügen oder Zugriff auf sensible/lebenswichtige Informationen oder Funktionen haben; - Kontrolle, ob alle Lieferantenverträge Sicherheitsklauseln enthalten; - Kontrolle der Wirksamkeit von Schutzmaßnahmen des öffentlichen Netzwerks; - Kontrolle, ob vor der Inbetriebnahme eines neuen Informationssystems oder einer größeren Weiterentwicklung Akzeptanzverfahren durchgeführt wurden; - Kontrolle der Einhaltung von Gesetzen, Vorschriften u. a. Praktiken;
CDV-10: Die Kontrollverfahren dürfen die Arbeit der Informationssysteme nicht beeinträchtigen	Kontrollverfahren müssen klar definiert sein. Für Tests und Kontrollen des Informationssystems notwendige Zugriffe und Privilegien sind in Raum und Zeit zu beaufsichtigen. Dabei ist vor allem darauf zu achten, dass die Ausführung dieser Verfahren den Betrieb des Informationssystems nicht wesentlich beeinträchtigt.
CDV-11: Durchführung	Die Wirksamkeit von Sicherheitsmitteln kann nur dann aufrecht erhalten

eines Sicherheitsaudits

werden, wenn sie regelmäßig unter Einsatz greifbarer Elemente überprüft wird. Dazu sind von qualifizierten und berechtigten Personen in Übereinstimmung mit Verfahren, die nach präzisen, abgestimmten Verfahren zu definieren sind, Sicherheitsaudits des Informationssystems durchzuführen, um sich von der richtigen Anwendung von Sicherheitsverfahren, Verfahren für den operativen Betrieb, der Konsistenz dieser Verfahren, der vorhandenen Mittel sowie davon zu überzeugen, dass der gesamte, ins Auge gefasste Prozess von diesen Mitteln berücksichtigt wird unter Einschluss von Weiterentwicklungen.

Die Ergebnisse dieser Audits werden dem Auftraggeber sowie den Personen, bei denen diesbezüglicher Kenntnisbedarf besteht, mitgeteilt. Über Sicherheitszwischenfälle oder schwachstellen des Informationssystems ist dem Sicherheitsverantwortlichen Bericht zu erstatten.

Externe Sicherheitsaudits des Informationssystems bedürfen des vorherigen Einverständnisses des Sicherheitsverantwortlichen. Für diesen Audittyp ist ein strenger Rahmen vorgesehen, in dem die Verantwortung jedes Akteurs definiert ist (Tiefe der Untersuchung, Verbreitung der Ergebnisse).

In Ergänzung dieser Tests können Eindringversuche durchgeführt werden. Diese Tests sind zu definieren und begleiten (Auswahl eines Leistungserbringers, Vertraulichkeitsverpflichtung, Speicherverfahren und Plan zur Ingangsetzung...).

3.3.5 ACR : Sicherung und Zertifizierung

ACR-01: Minimalanforderungen an die im Informationssystem verwendete Anwendersoftware

Diese Anforderungen sind klar zu formulieren und beziehen sich im wesentlichen auf:

- den Schutz der Konfigurations- bzw. Parametrierdaten: Diese werden zu oft vergessen, obwohl sie zu den Mitteln gehören, die allzu oft übersehen werden und mit denen eine Anwendersoftware am leichtesten umgedreht werden kann.

- die Validierung und eventuelle Filtrierung eingegebener Daten vor ihrer Verarbeitung: Diese Validierung ist planmäßig und systematisch durchzuführen, bezieht sich aber vor allem auf ,,Eingaben" durch Benutzer (Risiko von Fehlern oder böswilligen Absichten) und Daten von außen.

- die Validerung ausgehender Daten: Hierbei handelt es sich um das Gegenstück zu Vorherigem mit Bezug auf:

- den Schutz der Eingaben vor der darauffolgenden Verarbeitung innerhalb einer Anwendersoftwarekette,

- und/oder die Zuverlässigkeit der Ergebnisse am Kettenende;

- Risiken einer Veränderung der Daten oder von Datenkorruption durch die Anwendersoftware selbst: Diese Probleme sind sehr häufig auf Konzeptionsfehler oder noch häufiger auf Implementierungsfehler (Bugs) zurückzuführen, die dann von böswilligen Benutzern genutzt werden können.

	- das Vorhandensein und die Relevanz von Mechanismen zur Selbstkontrolle, die in der Anwendersoftware selbst vorhanden sind, und ihre Fähigkeit, bei abnormem oder ganz einfach unvorhergesehenem Verhalten Warnmeldungen zu generieren; - das Vorhandensein und die Relevanz der Mechanismen für Ablaufverfolgung und Journalschreibung, die je nach Bedarf verfügbar und konfigurierbar sind.
ACR-02: Erarbeitung eines Sicherheitsziels	Das Sicherheitsziel spezifiziert das Systems auf dem Gebiet der Sicherheit. Dieser Schritt ist sehr wichtig, da damit sowohl das zu erreichende Ziel, als auch seine Mittel festgelegt werden. Zunächst einmal dienen die tieferen Überlegungen im Rahmen der Untersuchung der Sicherheitsbedürfnisse und Risikoanalyse dazu festzulegen, was letztendlich geschützt werden soll, wobei präzisiert wird, gegen wen und gegen was. Die Sicherheitsziele des Systems sind eine Zusammenfassung dieser Überlegungen. Diese Ziele sind ab der Spezifikationsphase klar definiert, damit sie erreichbar werden und abgeschätzt werden kann, ob die Systemsicherheit in der Lage ist, diese zu erfüllen. Aus diesen Sicherheitszielen werden die einzuleitenden technischen und nicht technischen Maßnahmen abgeleitet. Nicht technische Maßnahmen sind Verfahren und Regeln zur Umsetzung, zum Management und zur Organisation, zur Berechtigung von Personen, zum Schutz des Systemumfelds und alle Vorkehrungen verordnungsrechtlicher Art. Technische Maßnahmen sind die Sicherheitsfunktionen des Systemkonzepts, um die Ziele zu erreichen. Diese Funktionen werden anhand von Sicherheitsmechanismen durchgeführt, die in das System integriert werden. Ziele und Funktionen bilden das Wesen des Sicherheitsziels. In der Konzeption des Informationssystems ist das Sicherheitsziel die Basis für Sicherheit. Jedoch müssen, damit man sicher sein kann, dass die Ziele erfüllt werden, einerseits diese Funktionen und Mechanismen auch wirklich vorhanden sein, und andererseits muss ihnen ausreichend vertraut werden können.
ACR-03: Einhaltung der Sicherheitsanforderungen vor der operativen Inbetriebnahme	Die Überprüfung der Einhaltung der Anforderungen muss umfassen: - deren Anwendung bei der Auswahl (Kaufsoftware) oder Spezifizierung (Entwicklungssoftware) um sicherzustellen, dass die Eigenschaften der Software ausreichend sind, um eine vom Sicherheitsstandpunkt aus akzeptable Umsetzung zu ermöglichen, einerseits; - und anderseits unter betriebsvorbereitenden Bedingungen durchgeführt werden, um das Sicherheitsniveau zu den tatsächlichen Bedingungen des Betriebs (Umgebung, Parametrierung..) sicherzustellen.
ACR-04: Periodische Überprüfung der	Um sich vor Abdriften im Laufe der Zeit zu schützen, sind Verfahren einzuführen, anhand derer regelmäßig und periodisch überprüft wird, ob

Einhaltung der Sicherheitsanforderungen an die Anwendersoftware

die Sicherheitsanforderungen im Hinblick auf Eigenschaften und Funktionen der Anwendersoftware eingehalten werden. Ein Teil dieser Kontrolle kann intern erfolgen.

ACR-05: Bewertung des Vertrauensniveaus des Informationssystems: Bewertung und Zertifizierung

Die Konzipierung des Systems erfolgt auf der Grundlage einer konsistenten Herangehensweise, die zur Erfüllung der Sicherheitsziele führt. Die Sicherheitsfunktionen werden mit dem Ziel ausgewählt, dass diese Ziele erfüllt werden können. Sobald das System entwickelt und in den Dienst gestellt wurde, muss festgestellt werden, wie weit man ihm dauerhaft im Hinblick auf die ordnungsgemäße Erfüllung des Sicherheitsziels vertrauen kann.

Einerseits hängt dieses Vertrauen von der Auswahl und Effektivität der Funktionen sowie der Qualität ihrer Entwicklung ab, andererseits aber auch von der Art, in der das System installiert, in Dienst genommen und betrieben wird.

Durch die Untersuchung der o. g. Gesichtspunkte kann begründetes Vertrauen in die Umsetzung des Sicherheitsziels entwickelt werden. Darin besteht das Ziel der Bewertung. Ein nach o. g. Prinzipien entwickeltes System kann bewertet werden, und man hat dann die Bestätigung, dass man ihm im Hinblick auf die Sicherheit, das es den ihm anvertrauten Informationen gewährt, und den von ihnen verwendeten Verfahren vertrauen kann.

Die Bewertung trägt signifikant dazu bei, Risiken eines unerwünschten Verhaltens einer Applikation zu reduzieren. Dabei werden Eigenschaften eines Systems oder Produkts in bezug auf standardisierte Sicherheitskriterien, z. B. Gemeinsame Kriterien, einer Bewertung unterzogen.

Diese Bewertung ist nach einer abgestimmten Methode, die definierten Regeln gehorcht, durchzuführen. Die Ergebnisse dieser Bewertung und die Tatsache, dass die verwendeten Bewertungskriterien korrekt angewendet wurden, werden mit einer formalen Erklärung - Zertifikat genannt - bestätigt.

Diese Zertifizierung ist jedoch nicht obligatorisch. Es obliegt dem Auftraggeber der Bewertung zu beurteilen, ob eine Zertifizierung notwendig ist.

ACR-06: Kriterien für Erwerb und Anwendung von Software-Paketen

Kriterien, die für den Kauf von Softwarepaketen sprechen, sind im wesentlichen wirtschaftlicher und operativer Natur (sofortige Verfügbarkeit des Produkts, vernünftige Kosten, technische Wartung und Support). Allerdings besteht bei gekaufter Software im Hinblick auf ihre Integrität und Verwendung innerhalb der Organisation ein Sicherheitsproblem.

Aus diesem Grund muss es eine Regel geben, anhand derer Kriterien bestimmt werden kann, ob die gekauften Softwarepakete und ihre Nutzungsbedingungen u. a. die folgenden Bedingungen erfüllen:

- Einhaltung der innerhalb der Organisation geltenden Sicherheitsprinzipien (vor der Kaufentscheidung zu bestimmen);

- Konformität und Integrität (vor der Indienststellung dieser

	Softwarepakete durch Tests nachzuweisen); - Nutzungsbeschränkungen auf Grundlage der Sensibilität der Arbeitsplätze.
ACR-07: Annahme von Entwicklungsmethoden und tools	Durch die Annahme von Entwicklungsmethoden und tools nach der Konzeption des Informationssystems bringt die Organisation ihren Willen zum Ausdruck, Sicherheit gewährleisten zu wollen. Die Anwendung dieser Regel rechtfertigt das Vertrauen in Konzeption und Umsetzung des Sicherheitsziels. Sie trägt zur Einführung homogener, konsistenter Schutzmaßnahmen bei, die auch die Gewähr dafür bieten, dass eine eventuelle Evaluierung des Informationssystems erfolgreich verläuft. Dabei ist jedoch zu berücksichtigen, dass diese Regel nicht meint, dass zur Entwicklung des Informationssystems nur eine Methode anzuwenden ist, sondern vielmehr darauf hinweist, dass auf die notwendige Konsistenz zwischen den verschiedenen, von der Organisation verwendeten Methoden zu achten ist.
ACR-08: Annahme eines Standards für Programmierung und Datencodierung	Die Annahme eines Programmierstandards bezieht sich auf alle IT-Anwendungsentwicklungen, darunter auch auf die Teile der Software, die in diversen Hardwarekomponenten oder Vorrichtungen des Informationssystems enthalten sein können. Für die Annahme eines Programmierstandards empfiehlt es sich zunächst, die Hard- und Softwarekonfigurationen, die für die Entwicklung verwendet werden sollten, zu bestimmen. Danach sind eine Darstellung und Programmstruktur zu wählen. Dadurch werden einheitliche, von allen anerkannte Bezüge hergestellt, die die Wartung der Software und die Pflege der technischen Dokumentation erleichtern. Die Datencodierung betrifft die Formatierung und Darstellung der Datenfelder, für die aus ähnlichen Gründen wie für die Programmstruktur ein Standard anzunehmen ist. Die verschiedenen Datenausgabezustände erfolgen ebenfalls nach Darstellungsstandards, die die funktionalen Besonderheiten der Benutzer der Organisation berücksichtigen. Für die richtige Definition der Daten und die Struktur von Dateien und Datenbanken ist der Datenadministrator verantwortlich.
ACR-09: Abnahme des Informationssystems	Mit der Sicherheitsabnahme wird nach Einsicht in die Abnahmeunterlagen durch die (regierungsamtlichen oder organisationsspezifischen) Abnahmebehörde festgestellt, dass das betreffende Informationssystem in der Lage ist, Informationen auf einem bestimmten Sensibilitäts- oder Klassifizierungsniveau zu verarbeiten, und dass die ihm innewohnenden Sicherheits-Restrisiken akzeptiert und beherrscht werden. Um eine Abnahme erfolgreich durchzuführen, wird im allgemeinen ein Lenkungsausschuss mit der Projektbetreuung beauftragt. Dieser Lenkungsausschuss betreut die Erstellung der Abnahmeunterlagen, die

	der Abnahmeautorität zur Bestätigung vorgelegt werden. Die Sicherheitsabnahme ist so lange gültig, wie das Informationssystem unter den von der Abnahmebehörde bestätigten Bedingungen arbeitet. Sie ist Ausdruck für die Akzeptanz des im Hinblick auf Vertraulichkeit, Verfügbarkeit, Authentizität sowie Datenintegrität- und Ursprung qualifizierten und quantifizierten Restrisikoniveaus.
ACR-10: Zulassung des Informationssystems	Die Bewertung und Zertifizierung als Bestätigung der Ergebnisse dieser Bewertung sind lediglich eine Bestätigung dessen, dass das Sicherheitsziel erreicht ist. Das ist aber nur ein Aspekt, um zu beurteilen, ob das System oder ein in seiner Umgebung befindliches Produkt mit Hilfe nicht technischer Sicherheitsmaßnahmen (insbesondere den tatsächlich eingeführten Betriebsmaßnahmen) den Schutz bietet, der der Sensibilität der ihnen anvertrauten Ressourcen sowie den Gefahren, die sie abwehren müssen, angemessen ist. Darüber hinaus ist das Sicherheitsziel auch gegenüber der tatsächlichen Betriebsumgebung des Systems auf seine Relevanz zu beurteilen. Diese Aufgabe wird von der Zulassung erfüllt. Sie erkennt formal an, dass das evaluierte Produkt oder System in der Lage sind, die Informationen unter bestimmten Anwendungsbedingungen bis zu einem bestimmten Niveau zu schützen.
ACR-11: Management der Sicherheitsdokumentation	Das Management der Sicherheitsdokumentation besteht aus Führung, Aktualisierung, Reproduktion und Vernichtung: - das Management der Sicherheitsdokumentation beruht auf einer präzisen, effektiven Führung, deren Kernelement ein stets aktuelles Bestandsverzeichnis ist, - da sich das Informationssystem ständig weiterentwickelt, ist die Sicherheitsdokumentation regelmäßig zu aktualisieren, - Reproduktion und Vernichtung der Dokumentation erfolgen auf Anordnung des Sicherheitsverantwortlichen. Dieser überprüft, dass alle bezeichneten Dokumente und nur auf diese von obigen Vorgängen erfasst werden.
ACR-12: Annahme eines Standards zur Erarbeitung der Sicherheitsdokumentation	Aufgrund der Unterschiedlichkeit von Hard- und Software sowie der Verfahren ist ein Standard zur Erarbeitung der Sicherheitsdokumentation notwendig. Dieser Standard bezieht sich vor allem auf die Art und Weise der Darstellung und den Inhalt der Dokumentation: Alle Sicherheitsbestandteile sind unter Einhaltung derselben Formensprache zu beschreiben, dem berechtigten Personal Betriebs- und Wartungseingriffe zu erleichtern. Der Standard bezieht sich in zweiter Linie aber auch auf die Art und Weise, in der die Dokumentation ,,durchgeführt" wird, d. h. verfasst, gedruckt sowie die Klassifizierung der Dokumente. Außerdem sind alle Elemente, die zur Erarbeitung der Dokumentation herangezogen wurden, ebenso und unter denselben Bedingungen zu handhaben und zu schützen, wie die auf deren Grundlage erarbeiteten

	Sicherheitsdokumente selbst.
ACR-13: Produktion von Dokumenten durch die Organisation	Alle Dokumente, die von der Organisation produziert werden, müssen der Grafikcharta und ihrer Qualitätssicherungspolitik entsprechen. Insbesondere ist jedem Dokument eine bestimmte Referenz zuzuordnen, anhand derer es möglich ist, den Autor, das Datum der Erstellung des Dokuments, alle Elemente für das Versionsmanagement sowie den Klassifizierungsvermerk für dieses Dokument zu identifizieren. Diese Referenz muss im Dokument deutlich erkennbar sein. Die Sicherheit einer Information wird ab Veröffentlichung eines Dokuments zugewiesen. Der Verfasser des Dokuments ist standardmäßig der Eigentümer. Damit ist er für seine Klassifizierung verantwortlich. Das Medium wird auf Grundlage der Klassifizierung seiner Informationen entsprechend geschützt. Spezielle Sicherheitsregeln sind auf Grundlage der Klassifizierung anzuwenden.
ACR-14: Pflege der Sicherheitsdokumentation	Es sind eine Organisation und Regeln zu erarbeiten, nach denen die Sicherheitsdokumentation zu aktualisieren ist, wenn Änderungen vollzogen wurden (vgl. Dokumentenmanagement). Gleichzeitig ist sicherzustellen, dass die alte Dokumentation archiviert oder ausgesondert wird.

3.3.6 ASH : Menschliche Aspekte

ASH-01: Begriff der Anerkennung von Verantwortung	Für Arbeitsplätze, die Informationen enthalten, die sich auf das Verteidigungsgeheimnis beziehen, bedeutet Bescheinigung der Anerkennung von Verantwortung, dass sich eine Person verpflichtet, die Gesetze, Vorschriften und Sicherheitsregeln des Informationssystems einzuhalten. Diese ist Gegenstand einer schriftlichen, lt. IGI 1300 unterzeichneten Erklärung. Art. 16 bestimmt vor allem: ,,...diese Bescheinigung bedeutet, dass der Inhaber der Zulassung anerkennt, die besonderen Verpflichtungen und die Sanktionen lt. Art. 70 bis 85 und R. 24 des Strafgesetzbuchs [Code pénal] zu kennen, die für jeden Verwahrer oder Besitzer von Informationen, die für die Sicherheit der Nation und des Staates relevant sind, gelten [...] Es obliegt dem Direktor der Organisation oder dem hierarchisch Zuständigen, den Betreffenden über den Geltungsbereich dieser Bescheinigung aufzuklären." Für Arbeitsplätze, die nicht in diese Kategorie fallen, können spezielle Vertraulichkeitsklauseln, Klauseln, die bei Beendigung des Arbeitsvertrages aufleben oder Wettbewerbsverbotsklauseln in den Arbeitsvertrag aufgenommen werden, sofern Bedarf besteht. Bei Informationen, die nicht der [IGI 1300] unterliegen, werden derartige Fragen von der [REC 600] behandelt, die insbesondere präzisiert: ,,Alle Mitarbeiter der Kategorien, die Zugriff auf IT-Ressourcen des Unternehmens haben müssen, müssen zuvor ein Dokument unterschreiben, mit dem sie die Übernahme von Verantwortung erklären

	(vgl. Abschnitt 1.). Dieses Dokument kann für jede dieser Mitarbeiterkategorien spezielle Elemente enthalten." Diese im wesentlichen auf Abschreckung beruhende Maßnahme kann durch die Androhung von Sanktionen verstärkt werden. Auswirkungen auf disziplinarischer Ebene bei Nichteinhaltung dieser internen Sicherheitsregeln sind in diesen Fällen den neu eingestellten Mitarbeitern bei Übernahme ihrer Funktionen zu erläutern.
ASH-02: Sicherheitsklauseln in Arbeitsverträgen	Arbeitsverträge von Mitarbeitern müssen: - entweder ausdrückliche Klauseln über die Sicherheit des Informationssystems beinhalten: o Verbote, o Pflicht zur Anzeige einer Anomalie oder einer Sicherheits-Schwachstelle, o Pflicht zur Zurückhaltung, o Vertraulichkeitsklauseln, o Verantwortung für die Einhaltung der Regeln, die für den Schutz des Vermögens der Organisation gelten; - oder sich ausdrücklich auf die verschiedenen Vorschriften beziehen, die in diesem Bereich durchzusetzen sind (vgl. Kapitel, das die gesetzlichen und verordnungsrechtlichen Verpflichtungen behandelt), wie zum Beispiel: o die PSSI, o die Gesetze, die sich auf die Ethik des jeweiligen Berufs beziehen, o die für die Organisation geltenden Vorschriften (Chartas, interne Vorschriften...). Diese Elemente müssen Sanktionen bzw. Maßnahmen behandeln, die im Falle einer Nicht-Einhaltung dieser Verpflichtungen angewendet werden. Dieses Prinzip hat auch für jeden Praktikanten oder Zeitarbeiter zu gelten.Mitarbeiter, die Verantwortung tragen oder mit sensiblen Aufgaben betraut sind (Sicherheitsmanagement, Inspektion...) müssen besondere Verpflichtungserklärungen unterschreiben, die mit ihrer zukünftigen Funktion verbunden sind. Die verschiedenen Verpflichtungen müssen, auch wenn sie nicht direkt Bestandteil des Arbeitsvertrags sind, von der Rechtsabteilung der Organisation zu prüfen und zu bestätigen (vgl. vorhergehendes Kapitel über die Verantwortlichkeiten). (Vgl. Berechtigungsprinzipien und Gesetzliche und verordnungsrechtliche Verpflichtungen)
ASH-03: Annahme von Auswahlkriterien für Mitarbeiter, die mit sensiblen	Diese Regel betrifft alle Kategorien von Mitarbeitern, die an sensiblen Informationssystemen arbeiten. Sie legt fest, welchen Auswahlmodus die Organisation für Stellen, die auf die Funktionsweise und die Verwendung des Systems Einfluss haben, bei der Einstellung von Personal

Informationssystemen arbeiten	anzuwenden hat, und insbesondere die für jeden Arbeitsplatz erforderlichen Sicherheitskriterien. Zum Beispiel kann im Einstellungsverfahren die Anforderung nach Arbeitszeugnissen über die Tätigkeit in sensiblen Bereichen berücksichtigt werden.Diese Regel schließt die Möglichkeit der Überprüfung von Arbeitszeugnisses eines Stellenbewerbers ein sowie derjenigen von Personen, denen zeitweilig eine Tätigkeit übertragen wurde, welche die Notwendigkeit der Verwendung des Informationssystems beinhaltet.
ASH-04: Allgemeine Berechtigungskriterien	Auf das Informationssystem dürfen nur namentlich berechtigte Personen physisch und logisch Zugriff haben. Damit findet die Bestimmung von Zugriffsbeschränkungen auf Systeme und Informationen in Übereinstimmung mit deren Sensibilität (vgl. Klassifizierung) und der Kritizität der für diese Daten und Ressourcen erlaubten Aktionen statt. Berechtigungen werden einer physischen Person erteilt und sind nicht übertragbar. Über die Gewährung von Berechtigungen für ein System oder eine Information wird von deren Eigentümern entschieden.Bei der Definition der Berechtigungen ist das Prinzip des Kenntnisbedarfs zu berücksichtigen: Jeder Akteur hat nur auf die Informationen Zugriff, die er für die Erfüllung seiner Aufgabe benötigt. Es wird empfohlen, bei Eröffnung / Indienststellung neuer Systeme das Prinzip der geringsten Zugriffsrechte (Standardberechtigung Null) anzuwenden.
ASH-05: Berechtigungskategorien	Die Berechtigungskategorien sind bei Einstellungsverfahren von Mitarbeitern oder bei der Auswahl von Lieferanten, die einem Berechtigungsverfahren unterliegen, zu berücksichtigen. Die Anforderungen an das Personal müssen den Berechtigungen entsprechen, wie z. B. durchzuführende Überprüfungen und Kontrollen (Identität, Kompetenz), Unterzeichnung spezieller Verpflichtungserklärungen...
ASH-06: Regeln für Zuweisung und Verpflichtung (Verantwortlichkeiten)	Über die Zuweisung von Berechtigungen wird bei Einstellung des Mitarbeiters bestimmt. Sie ist zeitlich und räumlich festzulegen.Die Person, der die Berechtigung erteilt wird, hat ihre Kenntnis über die Verantwortung, die sich aus der ihr gewährten Berechtigung ergibt, förmlich zu bestätigen.Jedwede Befugnis für einen Bereich oder ein Projekt des Informationssystems ist förmlich durch seinen Eigentümer (Verantwortlicher für den Schutz der Verarbeitung und der vom Sicherheitssystem verarbeiteten Informationen) zu autorisieren.
ASH-07: Personalreserve	Es können organisatorische Maßnahmen getroffen werden, um an einem lebenswichtigen Arbeitsplatz Vakanzen, auch zeitlich beschränkte (Urlaub...), zu vermeiden. Die Organisation hat für alle lebenswichtigen Arbeitsplätze eine ausreichende und erfahrene Personalreserve vorzuhalten. Für jeden Mitarbeiter, der einen lebenswichtigen Arbeitsplatz besetzt, muss ein Ersatzmitarbeiter vorhanden sein, der die gleichen Kompetenzen und den gleichen Kenntnisstand über den Vorgang hat.
ASH-08 : Procédure	Die Sensibilität eines Arbeitsplatzes steht mit seinem Bedürfnis an

d'habilitation pour les postes de travail sensibles

Vertraulichkeit, Verfügbarkeit und Integrität im Zusammenhang, denen Informationen, Hard- und Software, die ihn bilden, unterliegen. Die Sensibilität wird nach Klassifizierungskriterien bestimmt (vgl. Kapitel, das die Sicherheit von Informationen behandelt), kann aber auch von dem Ort abhängen, an dem sich der Arbeitsplatz befindet: So kann auch ein Arbeitsplatz eines Verantwortlichen für menschliche Beziehungen in einer Region mit einem hohen sozialen Risiko als sensibler Arbeitsplatz betrachtet werden.Für einen Arbeitsplatz, der Umgang mit Informationen umfasst, die sich auf das Verteidigungsgeheimnis beziehen, werden die Berechtigungen der Mitarbeiter von Art. 3 [IGI 1300] bestimmt:

,,Das Berechtigungsverfahren besteht darin zu überprüfen, dass ein Mitarbeiter ohne Gefahr für die nationale Verteidigung, die Sicherheit des Staates bzw. für seine eigene Sicherheit im Rahmen der Ausübung seiner Tätigkeit von Informationen Kenntnis erlangen kann, die auf einer bestimmten Ebene angesiedelt sind. Nach Abschluss des Berechtigungsverfahrens entscheidet die zuständige Stelle, ob der betreffende Mitarbeiter zugelassen wird, von Informationen Kenntnis zu erlangen, die auf der geforderten Ebene eingestuft wurden."

Für sensible Arbeitsplätze, die keine Informationen nutzen, die für das Verteidigungsgeheimnis relevant sind, kann ein Berechtigungsverfahren angewendet werden, das sich auf das Modell der Verfahren stützt, das im Rahmen des Verteidigungsmarkts Anwendung findet. In diesem Fall kann auf [REC 600] Bezug genommen werden.

ASH-09: Abschirmung sensibler Arbeitsplätze

Le cloisonnement des postes de travail sensibles vise à lutter contre la fuite des informations représentant un enjeu pour les intérêts de l'État ou de l'organisme.

Pour la préservation des intérêts de l'État et, tout particulièrement dans le cadre de la protection du secret de défense, les décisions d'admission ou d'agrément aux informations classifiées d'un niveau donné, telles que définies dans les articles 10 à 12 de l'[IGI n°1300], n'autorisent pas pour autant le bénéficiaire à accéder à toutes les informations relevant de ce niveau ; le besoin de connaître ces informations reste fonction de l'activité de la personne ou des dossiers particuliers qui lui sont confiés.

D'une manière identique, pour la préservation des intérêts propres à un organisme dont les informations ne relèvent pas du secret de défense, la connaissance des besoins en information pour l'accomplissement de la mission ou du métier permet la mise en place d'un cloisonnement efficace des postes de travail.

Die Abschirmung sensibler Arbeitsplätze dient der Bekämpfung des Abflusses von Informationen, die für den Staat oder die Organisation von besonderem Interesse sind.

Zum Schutz der Interessen des Staates und insbesondere im Rahmen des Schutzes des Verteidigungsgeheimnisses ist der Begünstigte durch Entscheidungen, die ihn zu Informationen zulassen, die auf einer bestimmten Ebene angesiedelt sind, so wie in Art. 10 bis 12 IGI 1300

	bestimmt, jedoch nicht berechtigt, Zugriff auf alle Informationen auf dieser Ebene zu haben; das Bedürfnis, diese Informationen zu kennen, hängt auch in diesem Fall von der Tätigkeit dieses Mitarbeiters ab bzw. von den besonderen Vorgängen, die ihm anvertraut wurden. Gleichermaßen wird durch die Kenntnis der Informationsbedürfnisse zur Erfüllung der Aufgabe oder des Berufs auch Organisationen, deren Informationen für das Verteidigungsgeheimnis keine Relevanz haben, eine wirksame Arbeitsplatzabschirmung zum Schutz ihrer eigenen Interessen ermöglicht.
ASH-10: Beauftragung	Die Eigentümer oder Besitzer der Information können Mitarbeiter der Organisation mit der Durchführung von Schutzmitteln beauftragen. Jedoch sind sie weiterhin für die Sicherheit verantwortlich. Aus diesem Grund müssen sie über Mittel verfügen, um die Einhaltung der Sicherheitsregeln zu kontrollieren. Die Berechtigungen werden einer physischen Person erteilt und sind nicht übertragbar.

3.3.7 PSS : Planung der Kontinuität der Aktivitäten

PSS-01: Definition der Grenzen des Kontinuitätsplans	Der Rahmen des Kontinuitätsplans (Ressourcen, Verantwortlichkeiten, Periodizität der Tests...) ist insgesamt für jeden der folgenden Aspekte genau zu definieren: - die Installationen, Hardware und IT-Netzwerke; - die Software und Daten; - die Benutzer des Informationssystems. Eine Analyse der SIS-Risiken stellt die Elemente zur Verfügung, anhand derer eine Entscheidung über die für die Organisation notwendigen Pläne getroffen werden kann. Diese Pläne verursachen erhebliche Kosten, die nachzuweisen sind.
PSS-02: Berücksichtigung ausgelagerter Dienste	Das Management von Kontinuitätsplänen, die externe Partner einbeziehen, ist zu vertiefen, insbesondere bei der Festlegung der vertraglichen Verpflichtungen. Es muss Elemente umfassen, die sich auf Übungen beziehen, deren Ziel die regelmäßige Überprüfung der ordnungsgemäßen Funktionsweise der Pläne ist.
PSS-03: Erarbeitung eines Restartplans	Um kritische operative Aufgaben des Informationssystems vor den wichtigsten Störfällen, menschlichen Fehlern, Naturkatastrophen oder vorsätzlichen Angriffen zu schützen, ist ein IT-Restartplan (bzw. Aktivitäts-Restartplan) notwendig. Sein Ziel besteht darin, Beeinträchtigungen der Sicherheit nach größeren Zwischenfällen zu beschränken und das Informationssystem wieder in den ursprünglichen Betriebszustand zu versetzen. Im Aktivitäts-Restartplan sind alle operativen Anforderungen des Informationssystems zu berücksichtigen, um eine Rückkehr zu einem normalen Betrieb sicherzustellen. Bei Beschädigung oder bei einer Störung einer Ausrüstung bieten die sich aus diesem Plan ergebenden Verfahren Alternativen und zeitlich begrenzte Mittel an, um die Kontinuität

des Dienstes sicherzustellen.

Dabei ist die Untersuchung der Verfügbarkeit des Informationssystems für die Erarbeitung eines Aktivitäts-Restartplans ein wesentliches Element, da die Schwere der verursachten Schäden im allgemeinen von der Dauer der Nichtverfügbarkeit abhängt. Ziel der Verfügbarkeitsuntersuchung ist es demnach, die Zeitabschnitte zu definieren, in denen der Schaden in Übereinstimmung mit der Ebene des Notfallverfahrens des Aktivitäts-Restartplans als auf einer bestimmten Ebene befindlich betrachtet wird.

PSS-04: Positionierung von Applikationen in den Kontinuitätsplan

Jede Applikation ist auf Grundlage der Risikoanalyse der Organisation im Hinblick auf ihre Restartpriorität zu beurteilen. Diese Beurteilung entspricht der Auswirkung, die die Nichtverfügbarkeit der Applikation auf den Geschäftsbetrieb hätte.

PSS-05: Einrichtung von Sicherungsverfahren

Es ist ein Sicherungsplan zu erarbeiten. Dieser Sicherungsplan hat die Anforderungen an die Frist zur Wiederherstellung der Informationen je nach Art der Aktivität oder des Verfahrens zu berücksichtigen. Dabei ist zwischen Wiederherstellungen von Anwendungs- und Datensystemen zu unterscheiden.

Der Sicherungsplan ist regelmäßig zu testen, um nachzuweisen, dass eine höhere Vertrauensebene gerechtfertigt ist. Das Verfahren regelmäßiger Sicherungen lebenswichtiger Daten und Programme ist eine grundlegende Maßnahme. Klassischerweise wird eine minimale Anzahl von Informationssicherungen an einem entfernten Ort gespeichert, der ausreichend weit entfernt ist, um bei einem Schadenfall am Hauptstandort unbeeinträchtigt zu bleiben; die physischen Schutzmaßnahmen für die Sicherungskopien haben das gleiche Niveau wie die Standards, die am Hauptstandort angewendet werden. Es sind Mittel zur Kontrolle der Konsistenz und der Integrität der gesicherten Informationen einzuführen und zu verwalten.

PSS-06: Regelmäßige Tests der Pläne

Um nachzuweisen, dass eine höhere Vertrauensebene gerechtfertigt ist, sind der Kontinuitätsplan und die verbundenen Pläne regelmäßig zu testen. Nach Abschluss dieser Übungen wird eine Gruppe ,,Erfahrungsrücklauf" eingesetzt, die die Pläne aktualisiert, nachdem Fehlfunktionen oder Funktionsverzögerungen analysiert wurden.

3.3.8 INC : Management von Zwischenfällen

INC-01: Definition vorstellbarer abnormer Situationen

Potentiell abnorme Situationen sind u. a.:

- Funktionspannen oder -anomalien der Hardware,

- Funktionspannen oder -anomalien der Software und der Anwendungen,

- Probleme im Zusammenhang mit eingegebenen Daten, die nicht vorhanden, unvollständig oder abnorm sind,

- Produktion von keinen, unvollständigen oder abnormen Ergebnissen,

- ...

Elemente, die bei der Auswahl weiterzuleitender Warnmeldungen zu berücksichtigen sind, werden von der Risikoanalyse geliefert. Diese

	Auswahl hängt insbesondere von den definierten Sicherheitszielen ab.
INC-02: Einrichtung eines Netzwerks zum Erkennen von und zur Warnung vor Sicherheits-Zwischenfällen	Zweckbestimmung eines Warnnetzwerks ist es, nach Erkennen eines Zwischenfalls so schnell wie möglich einen Eingriff zu veranlassen, um dadurch die Folgen eines Stillstands des Informationssystems zu beschränken, oder Verfahren infolge des Eintretens des Zwischenfalls zu aktivieren. Glieder dieses Warnnetzwerks sind alle Benutzer, vor allem diejenigen, die sensible Arbeitsplätze innehaben. Die Benutzer sind zu befähigen, ihre Hardware zu schützen und Hinweise auf missbräuchliche Manipulationen oder ungewöhnliche Aktivitäten zu erkennen. Die Effektivität eines Warnnetzwerks ist von der Struktur seiner Organisation und vor allem von den Sicherheitsmitarbeitern abhängig. Sie hängt vom technischen Niveau der Mittel zum Erkennen und vom Mobilisierungsgrad der Benutzer des Informationssystems ab: Der daraus resultierende Eingriff wird um so wirksamer sein, wenn die richtigen Mittel im richtigen Augenblick eingesetzt werden. Sollten Informationen bloßgestellt werden, die dem Verteidigungsgeheimnis unterliegen, hat die Organisation vor allem schnell zu reagieren: ,,Wird die Sicherheit einer Information gefährdet oder anscheinend gefährdet, auf welche Weise auch immer, sind Geschwindigkeit und Diskretion des Eingriffs besonders wichtig, um Folgeschäden zu begrenzen; dabei ist ein unbegründeter, fehlerhafter Bericht einem verzögerter Eingriff immer vorzuziehen."
INC-03: Beherrschung von Sicherheits-Zwischenfällen	Sicherheits-Zwischenfälle zu beherrschen bedeutet, sich zu vergewissern, dass nach einem Eingriff nach einer Warnung ein sicherer Zustand wiederhergestellt wurde: Die Hinzuziehung von Experten von außen und die Verpflichtung, ihnen den Zugang zum Standort und den Zugriff auf das Informationssystem zu erleichtern, bedeutet nicht, dass die Mitarbeiter der Organisation von der Anwendung der Sicherheitsregeln befreit sind. Sicherheitszwischenfällen können beherrscht werden, wenn vorher dementsprechende Verfahren festgelegt wurden und eingehalten werden. Verschiedene Notfallarten können verschiedene Aktionen notwendig machen: - bei Notfällen aufgrund physischer Unfälle, die die Infrastruktur oder das Informationssystem einer sensiblen Zone beeinträchtigen und keine feindseligen Aktionen nach sich ziehen, die darauf abzielen, Bestandteile des Informationssystems in fremde Gewalt zu bringen, besteht die Aktion folglich darin, die Hard- und Software sowie die Dokumente während des Eingriffs, wie z. B. Verlagerung von Ausrüstungen in einen Reinraum oder das Herunterfahren der Sicherheitsmechanismen in den Notbetriebs-Modus bis zur Wiederherstellung des Normalbetriebmodus des Informationssystems, zu kontrollieren, - bei Notfällen aufgrund feindseliger Aktionen, die darauf abzielen, Bestandteile des Informationssystems in fremde Gewalt zu bringen, kann in bestimmen Fällen ein unkompliziert durchzuführender und praktischer Zerstörungsplan das einzige Mittel sein, um eine schwerwiegende Bloßstellung zu verhindern.

INC-04: Kontrolle von Sicherheits-Zwischenfällen

Eine Organisation, die auf Kontrolle von Sicherheits-Zwischenfällen verzichtet, setzt sich der Gefahr aus, die Verwundbarkeit ihres Informationssystems zu verkennen und unfähig zu sein, wirksam auf wiederholte Schadenfälle gleicher Art reagieren zu können.

Aus diesem Grund sind Verantwortlichkeiten für die Kontrolle von Zwischenfällen und Verfahren festzulegen, wobei die Verfahren alle Arten potentieller Vorkommnisse abdecken müssen, inkl. Störfälle des Systems oder Dienstausfälle, Fehler, die aus falschen oder inadäquaten Daten resultieren, Schwachstellen bei Vertraulichkeiten.

Um diese Anforderung erfüllen zu können, stützt sich die Kontrolle von Sicherheits-Zwischenfällen auf das Berichtswesen, d. h. Berichte nach Soforteingriffen und Fehlfunktionslisten der verschiedenen Aktionen, und in beiden Fällen auf die Analyse und Identifikation der Ursachen des Schadenfalls sowie Statistiken über die Vorkommenshäufigkeit.Zu den Maßnahmen, die darauf abzielen, das genannte Warnverfahren zu vereinheitlichen und verpflichtend zu machen, gehört die Annahme eines Berichtsstandards und von Richtlinien zu seiner Nutzung.

Über Zwischenfälle jedweder Art, die z. B. in der Betriebsphase festgestellt werden, ist dem Sicherheitsverantwortlichen so schnell wie möglich zu berichten.

Fehlfunktionen und Schwächen des Informationssystems sind aufzuzeichnen und zu korrigieren. Dabei ist vor allem notwendig, Fehlfunktionen zu kontrollieren um sich zu vergewissern, dass die notwendigen Korrekturmaßnahmen wirklich durchgeführt wurden und autorisierten Aktionen entsprechen.

Voraussetzung für die Analyse und Identifikation der Ursachen des Vorkommnisses ist, dass das Sammeln der Auditberichte, die Durchführung von Schutzmaßnahmen und die Kommunikation mit den Benutzern, die von dem Zwischenfall beeinträchtigt wurden, nach einem Plan erfolgen.

INC-05: Mittel zum Erkennen eines Eindringens oder missbräuchlicher Verwendung

Es wird empfohlen, dass Vorrichtungen und/oder Verfahren Versuche eines Eindringens oder einer missbräuchlichen Verwendung erkennen können, wodurch als als Reaktion darauf die notwendigen Maßnahmen ergriffen werden können, um diese Versuche scheitern zu lassen.

Aus diesem Grund sind für jede Komponente bzw. jede sensible Anwendung des Sicherheitssystems Ad-hoc-Mittel zu bestimmen und einzurichten, die von einem konfigurierten Kontrollmechanismus bis hin zu speziellen Tools, wie Systemen zum Erkennen eines Eindringens, reichen können.

INC-06: Umsetzung eines wirksamen Warndienstes

Das Prinzip besteht darin, Ereignisse oder Zwischenfälle, die Hinweise auf einen Angriff enthalten (oder enthalten könnten) oder denen eine Feindseligkeit zugrunde liegt, so schnell wie möglich festzustellen.

Der Warndienst hat die Weiterleitung und Zentralisierung erkannter Zwischenfälle über einfache Informationsprozesse (vgl. Funktion der Rollen) zu organisieren und muss die Benutzer und Betreiber dahingehend sensibilisieren, dass sie jedwede Anomalie anzuzeigen haben. Es sind mehrere Warnebenen vorzusehen. Diese verschiedenen

Ebenen müssen von den Benutzern erkennbar sein, d. h. jeder muss wissen, auf welcher Ebene sich das Informationssystem zu einem gegebenen Augenblick befindet.

INC-07: Planung von Reflexreaktionen bei Notfallsituationen

Das Prinzip besteht darin, typische Schadenfallszenarien auszuwählen und die besten Reaktionen im Hinblick auf erhaltende Maßnahmen zu formalisieren, um die Weiterverbreitung der Auswirkungen des Zwischenfalls oder des Angriffs zu beschränken oder sogar zu verhindern, ggf. als interne und externe Entscheidungs- und Informationsbefugnis. Damit wird vermieden, dass sich Zwischenfälle als Schadenfälle mit ärgerlichen oder unerträglichen Folgen für die Organisation entwickeln.

Jeder Warnebene entspricht eine klare Verfahrensanweisungen für die durchzuführenden Aktionen. Diese Verfahrensanweisungen stützen sich auf das Prinzip der tiefgestaffelten Verteidigung, was auf Grundlage der jeweiligen Warnmeldung die Errichtung unabhängiger Schutzbarrieren erlaubt.

3.3.9 FOR : Sensibilisierung und Schulung

FOR-01: Dokumentation der Verantwortung

Alle SIS-Verantwortlichkeiten sind unzweideutig zu verfassen und den Mitarbeitern, die dafür verantwortlich sind, zur Kenntnis zu bringen. Die Beschreibung dieser Verantwortlichkeiten muss die Beschränkungen enthalten, die mit jedem zeitlich und räumlich verknüpft sind.

Weiterhin haben sich alle betroffenen Akteure formal zu verpflichten, diese Verantwortlichkeiten zur Kenntnis zu nehmen und zu akzeptieren.

FOR-02: Allgemeine Sensibilisierung für Sicherheit

Die Sensibilisierung zielt darauf ab, jedem Benutzer bewusst zu machen, dass er bei der Bekämpfung von Feindseligkeiten ein wichtiges Stück Verantwortung trägt.

Die Definition der Ziele dieser Sensibilisierung ist eng mit der Aufgabe oder Tätigkeit der Organisation, mit der Sensibilität des Informationsbestands und der physischen Güter sowie den bekannten Bedrohungen verbunden. Diese können z. B. das Streben nach Verbundenheit der Mitarbeiter im Hinblick auf den Schutz der Güter der Organisation sein oder auch die Einrichtung und Effektivität eines Warnnetzwerks, das alle Benutzer des Informationssystems einschließt.

Sensibilisierungsaktionen ohne klar definierte Ziele spiegeln lediglich vor, dass Mitarbeiter in der Lage seien, bei einem Angriff auf das Informationssystem effektiv zu reagieren.

Sensibilisierungsprogramme sind regelmäßig vom SIS-Verantwortlichen zu planen und zu leiten. Ziel dieses Programms ist es, die wichtigsten Inhalte der PSSI der Organisation ins Gedächtnis zu rufen und jeden Mitarbeiter zu informieren über:

- die Sicherheitsanforderungen;

- die wichtigsten Bedrohungen;

- Gesetze, Vorschriften und Chartas;

- die organisatorische Sicherheit;

	- die Sicherheitsprinzipien und regeln der Organisation; - das an den Tag zu legende Verhalten; - spezielle Regeln (wechselnde Arbeitsplätze, Teleaktionen...).
FOR-03: Kommunikation über die SIS	Informationen über die Organisation und die allgemeinen Anforderungen der SIS sind innerhalb der Organisation so weit wie möglich zu verbreiten. Aus diesem Grund ist ein Mittel zur Verbreitung festzulegen und allen zur Kenntnis zu bringen. Dieses Mittel (Verfahrensanweisung, Vertrag...) muss sicherstellen, dass dort alle für die Organisation relevanten SIS-Informationen auffindbar sind. Ein Mittel kann z. B. die Einrichtung eines Sicherheitsbereichs im Intranet der Organisation sein. Die allgemeine PSSI muss allen Mitarbeitern der Organisation bekannt sein, spezielle PSSIs sind den Mitarbeitern zur Kenntnis zu bringen, die mit diesen speziellen Systemen arbeiten. Die Bekanntmachung eines Teils oder der gesamten PSSI gegenüber externen Mitarbeitern, die in das Informationssystem eingreifen sollen, hat auf Grundlage ihres Kenntnisbedarfs zu erfolgen und ist in allen Fällen von der Organisation, die für die SIS verantwortlich ist, zu bestätigen (vgl. ORG). Es ist ein Eingangsbuch anzulegen, um sicherzustellen, dass jeder neue Mitarbeiter, der in das Informationssystem eingreift, über die Organisation, die Sicherheitsregeln und seine Pflichten informiert ist. Analog dazu ist ein Ausgangsbuch anzulegen, um die Mitarbeiter, die die Organisation verlassen, über die einzuhaltenden Verfahren und Regeln zu informieren.
FOR-04: Anwendung für den rechtlichen Schutz der Informationen der Organisation	Diese Regel zielt darauf ab, die Mitarbeiter dafür zu sensibilisieren, dass sie von Rechts wegen verpflichtet sind, die von ihnen verwendeten oder ihnen anvertrauten Informationen zu schützen, um das Risiko einer Veruntreuung oder Aneignung durch Dritte zu verringern. Die Anwendungsrichtlinien beziehen sich teilweise auf das Prinzip der Verantwortung der Mitarbeiter und vor allem auf die Regel in bezug auf den Begriff der Inhaberverantwortung (vgl. ORG-Verantwortung).
FOR-05: Anpassung der Sensibilisierung an die verschiedenen Benutzerklassen	Auf dem Gebiet der Sicherheit unterscheiden sich die Verantwortungsebenen erheblich je nachdem, ob es sich um leitende oder ausführende Mitarbeiter handelt. Die Sensibilisierung ist folglich an die verschiedenen Verantwortungsebenen und die Besonderheiten der jeweiligen Arbeitsplätze anzupassen. Die betroffenen Mitarbeiter gehören drei Hauptkategorien an: - Kategorie, die mit leitenden, betreuenden, verwaltenden sowie mit der Pflege von Außenbeziehungen verbunden ist, - Kategorie, die mit Tätigkeiten am Informationssystem (Ingenieure und Techniker, Benutzer der Bürotechnik...) verbunden ist, - Kategorie, die mit der Sicherheit von Informationssystemen (Ingenieure und Techniker des Sicherheitssystems, Sicherheitsmitarbeiter usw., die eine besondere Ausbildung benötigen) verbunden ist. Eine Sensibilisierung, die die operativen Besonderheiten jeder Benutzerklasse und die Anforderungen, die mehr oder weniger stark mit

	der Verantwortung oder Arbeitsplätzen in Beziehung steht, nicht berücksichtigt, erreicht nicht die gestellten Ziele und lässt Sicherheit im Hinblick auf den Aspekt Produktivität des Arbeitsplatzes wie eine zusätzliche Belastung ohne Wertschöpfung erscheinen.
FOR-06: Regelmäßige Sensibilisierung der Mitarbeiter für die SIS	Durch ständige Information der Mitarbeiter soll konstante Wachsamkeit erzeugt werden. Diese Information bezieht sich insbesondere auf die Weiterentwicklung der PSSI und der Bedrohungen. Durch ständige Information kann die Information aktualisiert werden, es können neue Informationen gegeben und an Regeln oder Hinweise erinnert werden, die nicht korrekt angewendet werden. Weiterhin ist jedwede Weiterentwicklung bezüglich der Organisation und der allgemeinen Anforderungen der SIS zu verbreiten.
FOR-07: Sensibilisierung für die Verarbeitung von Zwischenfällen	Die betreffenden Mitarbeiter sind über die einfache Funktionsweise hinaus auf einer Ebene zu sensibilisieren und auszubilden, die den Sicherheitsaspekten entspricht, für die sie verantwortlich sind. Ein wesentlicher Punkt der Sicherheitsverpflichtungen, die beim Betrieb zu beachten sind, betrifft die Einhaltung der folgenden Anforderungen: - Aufzeichnung von Zwischenfällen in einer Kladde, - Anzeige/Warnung durch den, dem dies zukommt (vgl. Fortsetzung).
FOR-08: Vorbereitung und Training für das Management von Krisensituationen	Das betreffende Personal ist nicht nur auf die Möglichkeiten und die Verarbeitung (Verfahren) von abnormen Situationen und Zwischenfällen einzustellen (FOR-07), sondern auch vorzubereiten und zu trainieren, was vor allem umfasst: - die Vorstellung von Ad-hoc-Plänen (Rettungspläne, Kontinuitätsplane, Restartpläne...), - Training der Mitarbeiter anhand von Simulationen (Übungen, die mit den Zwischenfallübungen vergleichbar sind). (Vgl. Krisenmanagement) Für jedes Mitarbeiterprofil muss ein spezielles Schulungsprogramm vorhanden sein, um bei einem Zwischenfall oder einer Sicherheitswarnung die richtigen reflexartigen Reaktionen sicherzustellen.
FOR-09: Sensibilisierung der Mitarbeiter für die Verwendung von IKT	Um vor Gefahren einer externen Preisgabe (beabsichtigt oder nicht), die mit der Verwendung von Medien der Informations- und Kommunikationstechnologie (IKT) wie z. B. Video, Telefon, Fax, Voice... verbunden ist, zu warnen, ist eine Aktionen zur Sensibilisierung der Mitarbeiter durchzuführen. Das bezieht sich insbesondere auf die Kontrolle der Empfänger, heimliches Abhören und Personen in der näheren Umgebung.
FOR-10: Mitarbeiterschulung zur Anwendung von IKT	Aufgabe dieser Schulung ist es, jedem im Bereich Informatik und Kommunikation (Informations- und Kommunikationstechnologien... IKT) Tätigen zu erläutern, welche Verantwortung er trägt, und jeden Benutzer für den Einsatz der IT- und Kommunikationsmittel sowie der ihm zur Verfügung gestellten Schutzmittel zu schulen.
FOR-11:	Der Einsatz technischer Mittel zur Feststellung von IT-Feindseligkeiten

Sensibilisierung der Benutzer für Beaufsichtigungsmittel

oder zur Pflege der Systeme verpflichtet die Organisation:

- die Informationsflüsse zu kontrollieren,

- auf ,,persönliche" Ressourcen zuzugreifen,- Austausch und Übertragung zu steuern (Netzwerk, Mailsystem, Internet),

- Beweismittel aufzubewahren.

Im Interesse der Ausgewogenheit zwischen Kontrolle und Respekt der Privatsphäre des Einzelnen, der Vermeidung von Zwischenfällen und um eine Beschädigung des Ansehens der Organisation zu vermeiden, sind die Akteure des Informationssystems über Informationsmaßnahmen zu informieren.

So empfiehlt es sich, eine Charta zu verfassen, die diesbezügliche Vorschriften enthält und das Ziel, die Mittel zur Kontrolle und zum Sammeln von IT-Beweisen erläutert.

3.3.10 EXP : Betrieb

EXP-01: Dokumentation von Verfahren und Regeln des Betriebs

Es sind alle Aktivitäten des Betriebs, eventuell nach Gruppen geordnet, zu identifizieren. Für jede dieser Aktivitäten sind die Betriebsverfahren und regeln präzise zu dokumentieren. Auf der Grundlage dieser Dokumentation können je nach Bedarf weitere Dokumente erarbeitet werden, die sich auf Grundlage von Rollen, Verantwortung und Kenntnisbedarf der Akteure an eine bestimmte Kategorie von ihnen richten. Sie ist auf einem aktuellen Stand zu halten.

EXP-02: Integration der SIS in die Verfahren und Regeln des Betriebs

Alle Dokumente für den Betrieb müssen einen Abschnitt Sicherheit enthalten, die von der Sicherheitsstruktur der Organisation bestätigt wurde.

EXP-03: Separierung der Entwicklung und der Operationen oder der Produktion

Durch Separierung von Aufgaben und Entwicklungsumgebungen, von Freigabe und anderen Aktivitäten, die mit der Arbeit des Informationssystems (Betrieb, System- und Netzwerkverwaltung, Datenerfassung, Datenpflege, Sicherheitsaudit...) verbunden sind, wird das Risiko eines beabsichtigten oder zufälligen Missbrauchs der Systemressourcen vermindert.

Diese Regel hat Einfluss auf das Sicherheitsniveau und die Effektivität bei der Verteilung von Aufgaben und Verantwortung. Sie ermöglicht:

- aufgrund der Separierung von Aufgaben, die den operativen Betrieb des Informationssystems kennzeichnen und unterschiedliche Ressourcen und Zugriffsprivilegien zu sicherheitskritischen Maschineninstruktionen benötigen, die Sicherheit zu erhöhen und gleichzeitig das Risiko böswilliger oder zufälliger Programmänderungen zu vermindern,

- dadurch die Effektivität zu erhöhen, dass sich ein Informatiker einer Betriebseinheit durch Funktionshäufung veranlasst sehen könnte, eine Software unter Missachtung der Programmierregeln, auf die in der obigen Regel hingewiesen wird (z. B. Fehlen von Kommentaren in den geänderten Codezeilen) ad hoc zu reparieren.

Mit dieser Funktionsseparierung geht eine bessere Abgrenzung der

	Verantwortung bei einem Zwischenfall einher.
EXP-04: Bedingungen für die Nutzung von IT-Outsourcing	Es wird zwischen verschiedenen IT-Outsourcingarten unterschieden: Leistungserbringung außerhalb der Organisation, Teleservice (u. a. auch Telewartung), Leistungserbringung externer Dienstleister am Standort... Die Bedingungen für die Nutzung von IT-Outsourcing sind streng und ggf. auf der Grundlage einer speziellen Sicherheitsanalyse festzulegen. So können z. B. durch den generellen Zugriff auf Telewartung Kosten durch Verringerung der Reisetätigkeit der Mitarbeiter optimiert werden. Andererseits nehmen die Risiken eines Angriffs auf das Informationssystem durch Installation einer Kommunikationsleitung zwischen dem Informationssystem und der Wartungsorganisation und die damit verbundene Notwendigkeit, Zugriffsrechte auf hohem Niveau zu gewähren, zu. (Vgl. Teleaktions-Operationen)
EXP-05: Sicherheitsbedingungen für die Wartung von Bestandteilen des Informationssystems	Die Nichteinhaltung von Hinweisen zur Vorbereitung eines Bestandteils auf Wartungsmaßnahmen kann die Organisation zu Zugeständnissen bezüglich des ordnungsgemäßen Betriebs ihres Informationssystems veranlassen bzw. zu Beeinträchtigungen führen. Die Konditionierung besteht darin, das Bestandteil im Hinblick auf seine Reparatur vorzubereiten, d. h. die folgenden Punkte zu überprüfen: - Entfernung des Permanentspeichermediums, das klassifizierte oder vertrauliche Informationen enthält, - Überschreiben des restlichen Speichers, um jedwede Möglichkeit zur Auswertung vorheriger Aufzeichnungen auszuschließen, - Überprüfung der externen Wartungsinstallationen, die den Normen für materielle und personelle Sicherheit entsprechen müssen, die auch in den Einsatzbereichen der zu reparierenden Bestandteile gelten. Sollte es aus technischen Gründen nicht möglich sein, das Permanentspeichermedium zu entfernen, können sich Wartungsmaßnahmen an dem entsprechenden Bestandteil vor Ort als notwendig erweisen, die von einem Personal vorgenommen werden, das über die entsprechende Berechtigung verfügt. Ein weiterer wesentlicher Punkt ist die Wartung der Sicherheitskomponenten.
EXP-06: Sicherheitsbedingungen für Restart nach Wartung	Die Sicherheitsbedingungen für den Restart von Bestandteilen nach Wartung zielen darauf ab, eventuelle Fangvorrichtungen oder Fehlfunktionen zu ermitteln. Folglich hängen die Bedingungen, unter denen der Betrieb wiederhergestellt wird, z. B. ab: - von den Bedingungen vor Ort, der Bewertung der Bedrohung und, bei Computern, von der Sensibilität der gespeicherten Informationen, weswegen das Bestandteil vor seinem Wiedereinbau in die

	Sicherheitszone zu prüfen ist, - im besonderen Fall von Hardware, die der TEMPEST-Norm entspricht, ist diese nach jedweder Änderung erneut auf ihre abstrahlungsverhindernden Fähigkeiten zu überprüfen.
EXP-07: Kontrolle von Operationen zur Wartung von Bestandteilen des Informationssystems	Diese Regel, die für alle Bestandteile des Informationssystems (Hard- und Software) gilt, ist bei Bestandteilen, die Sicherheitsfunktionen erfüllen, besonders wichtig. Nichtkontrolle von Wartungsoperationen führt zu Unkenntnis darüber, inwieweit die Bestandteile in der Lage sind, erneut ihre Funktionen zu erfüllen, d. h. ihnen kann im Sicherheitsbereich ungerechtfertigt vertraut werden. Zur Kontrolle von Wartungsoperationen ist ein vollständiges und detailliertes Register über alle Eingriffe an den Bestandteilen anzulegen, um die Mitarbeiter über die neuen Konfigurationen zu informieren und sie zu befähigen, die richtigen Verfahren anzuwenden. Sollte die Organisation ein Infocenter unterhalten, dessen Hauptaufgabe darin besteht, Supportleistungen für die Benutzer zu erbringen, ist darauf zu achten, dass dieses Infocenter bei Eingriffen, für die es verantwortlich ist, die gleichen Regeln anwendet, was insbesondere dann gilt, wenn es auch für die Installation von Softwarepaketen oder elektronischen Karten, die von den Benutzern verlangt werden, auf den Maschinen der Organisation zuständig ist.
EXP-08: Verwaltung der Leistungen externer Dienstleister	Das Hinzuziehen von Leistungen externer Dienstleister (mit ordnungsgemäßer Zulassung für die Verteidigungsmärkte) zur Entwicklung des Informationssystems setzt die strenge Anwendung der o. g. Regeln und eine verstärkte Kontrolle der ihnen zur Verfügung gestellten Ressourcen (sensible Applikationen und Dateien, Compiler, Editoren, technische Dokumentation...) voraus. Die Entscheidung, sensible Ressourcen zur Verfügung zu stellen, ist in bezug auf die operativen Anforderungen an die Verfügbarkeit des Informationssystems zu treffen. Um eventuelle Zwischenfälle zuordnen zu können, sind Verantwortung und Verfahren zwischen Organisation und Dienstleister klar zu definieren. Sollte die Sicherheit eines Informationssystems für die Interessen des Staates oder der Organisation von besonderer Bedeutung sein, darf die Hinzuziehung von Dienstleistungen nie in Richtung Unterbeauftragung des Facility Managements ausarten. (Vgl. Outsourcing von Diensten)
EXP-09: Integration der SIS in IT-Outsourcing-Verträge	IT-Outsourcing-Verträge und ihre Anlagen müssen einen SIS-Abschnitt enthalten, der die Verpflichtungen des Dienstleisters und jedes seiner Mitarbeiter klar spezifiziert. Sie müssen insbesondere sehr präzise spezifizieren: - die Sicherheitsanforderungen, zu deren Einhaltung sich der Dienstleister verpflichtet (die nicht unter dem Anforderungsniveau eventueller interner Anforderungen liegen dürfen);

- die Verfahren zur Kontrolle der Einhaltung dieser Anforderungen;

- die Zuweisung spezieller Verantwortlichkeiten für eine effektive Koordinierung im Falle von Zwischenfällen oder Anomalien;

die Möglichkeit der Weiterentwicklung dieser Anforderungen und Verfahren usw. in Übereinstimmung mit der Weiterentwicklung der PSSI oder ihren operativen Ableitungen und die Verpflichtung für den Dienstleister, sich diesen Weiterentwicklungen anzupassen.

EXP-10: Sicherheit bei externen Dienstleistern

Die Entscheidung, auf externe Dienstleister zurückzugreifen, und diese vertraglich zu binden, ist durch eine Analyse der Risiken und Anforderungen für die Organisation vorzubereiten, wobei die nachfolgend genannten Probleme ebenfalls Berücksichtigung finden müssen:

- die Verantwortungsbereiche der Organisation und der Erbringer externer Dienstleistungen sind klar zu definieren und vertraglich festzulegen;

- das Zusammenlegen von Dienstleister-Ressourcen, um den Bedürfnissen mehrerer Kunden zu entsprechen, kann den Sicherheitszielen nicht entsprechen;

- die Mittel des Dienstleisters, die dieser an den Informationssystemen anwendet, um mit dem Informationssystem der Organisation einen Schnittstelle zu bilden, sind an die umgesetzten Sicherheitsmitteln nicht notwendigerweise angepasst und zu diesen weder konsistent noch kompatibel;

- die Möglichkeiten und Bedingungen zur Kontrolle und Auditierung von Seiten des Auftraggebers sind oft begrenzt, insbesondere aufgrund starrer Vertragsbedingungen bzw. der herrschenden Bedingungen für einen Eingriff durch den Auftraggeber;

- die Personen, die das Informationssystem nutzen und bedienen, sind der Organisation nicht immer bekannt, wobei diese Personen übrigens gleichzeitig in Kontakt mit Daten oder Leitern von eventuell konkurrierenden Unternehmen stehen können;

- auf technischem Gebiet genießen die Dienstleister zur Erfüllung ihrer Aufgabe in punkto Sicherheit (vgl. Schutz des Zugriffs auf Wartung) im Allgemeinen recht großzügige Privilegien und können benutzt werden, um in das Informationssystem einzudringen.

Aus diesem Grund ist eine Risikoanalyse durchzuführen, die sich auf diese Probleme bezieht, um die Sicherheitsziele und maßnahmen festzulegen, die die identifizierten Risiken abdecken, vor allem auf Ebene von vertraglichen Klauseln, der Rückverfolgbarkeit oder der Kontrolle durchgeführter Operationen.

EXP-11: Antivirus-Überprüfung von Software und Daten vor ihrer Inbetriebnahme

Überprüfungen von Software und Datendateien vor ihrer Inbetriebnahme dienen insbesondere dazu, die Bedrohung durch Virusinfektion zu bekämpfen.

Um das Eindringen schädigender Software (Viren, Würmer, Trojaner, logische Bomben) zu vermeiden und zu erkennen, können Vorsichtsmaßnahmen ergriffen werden. Alle Medien, deren Herkunft außerhalb der Organisation liegt und vor allem Medien unbekannter

	Herkunft sind zu überprüfen. Eine Gegenmaßnahme, um dieser Bedrohung zu begegnen, ist die Installation von Mitteln für eine systematische Erkennung. Diese Mittel müssen so installiert werden, dass die Kontrolle aller Eingänge des Informationssystems (Internet, Netzwerk, Server, Arbeitsplätze) gewährleistet ist. Weiterhin sind auch die Elemente des Systems, die einem hohen Sicherheitsbedürfnis unterliegen, und Kontaminationspfade zu identifizieren und zu schützen. Dabei sind die zahlreichen Möglichkeiten, in den Besitz von Dateien zu gelangen (Disketten, CD-Rom, chiffrierte E-Mail-Anhänge), zu berücksichtigen. Weiterhin sind die Benutzer deutlich darauf hinzuweisen, dass sie an ihrem Arbeitsplatz keine Software zu installieren haben.
EXP-12: Sicherheitskontrollen des Informationssystems in der Betriebsphase	Durch Sicherheitskontrollen in der Betriebsphase werden die Risiken einer Beeinträchtigung von Verfügbarkeit und Integrität von Informationen und Daten vermindert. Diese Kontrollen finden z. B. in Form einer Überprüfung der Nutzung von zur Verarbeitung erlaubten Ressourcen statt. Der erste Aspekt dieser Kontrollen zielt auf die Benutzer des Informationssystems. Sie sind von den System- und Netzwerkingenieuren durchzuführen, die anhand von Mitteln zur Visualisierung eine direkte Kontrolle sicherstellen, , indem sie laufenden Transaktionen, Online-Dateien, Versuche, eine Verbindung aufzubauen usw. prüfen. Der zweite Aspekt dieser Kontrollen besteht darin, dass die Informatiker die ordnungsgemäße Anwendung der Sicherheitsverfahren überprüfen, so z. B.: - die Einhaltung der Reihenfolge der geplanten Operationen, - die korrekte Bedienung von Dateien, - die Nutzung erlaubter Makrobefehle, - die Einhaltung von Anweisungen, die für die Fehlerkorrektur oder außergewöhnliche Ereignisse gelten.
EXP-13: Reduzierung von Verwundbarkeiten	Das Dienstangebot von Bürokommunikationsnetzwerken steigt ständig. Dabei werden Informationen aller Art transportiert, deren Sicherheitsbedürfnisse sehr heterogen sind.Aus diesem Grund ist eine Politik der ständigen Sicherheitskontrolle notwendig, die dem Stand der Technik auf diesem Gebiet folgt und auf signifikante Verwundbarkeiten der Systeme und Standard-Applikationen des Informationssystems entsprechend reagieren kann. Die Kontrolle bezieht sich auf Angriffsmethoden, Verwundbarkeiten und Sicherheitslösungen.
EXP-14: Verfahren zur gesicherten Nutzung von Informationen und Daten	Daten und deren Trägermedien sind auf der gleichen Ebene zu schützen wie die Informationen, die zu ihrer Erstellung führten. Informationen und Daten sind auf Grundlage ihrer Klassifizierung Gegenstand einer speziellen Nutzung. So kann die Nutzung lebenswichtiger oder sensibler Daten besondere technische (z. B. Einsatz von Systemen mit Fehlertoleranz oder von Sicherungsdisketten) oder organisatorische Maßnahmen (z. B. Abschirmung sensibler Arbeitsplätze) notwendig machen, um Zwischenfälle in der Verarbeitungsphase zu

	vermeiden. Auch sind namentliche Informationen den gesetzlichen Anforderungen entsprechend zu schützen. Die vorliegende Regel bezieht sich auf gesicherte Betriebsverfahren. Sie ist aufgrund der Verwundbarkeit der Daten gerechtfertigt, die daraus resultiert, dass diese verschiedene Stadien durchlaufen (Verarbeitung, Sicherung und Übertragung auf Trägermedien, Lagerung, Vernichtung...). : So tragen auch die Verfahren zur Gewährleistung von Sicherheit und deren Kontrolle dazu bei, die Kontinuität des Schutzes zu diesen verschieden Betriebsstadien zu garantieren. Von allen Verfahren haben Verfahren zur Datensicherung und Vernichtung klassifizierter Medien eine besondere Sicherheitsrelevanz. - Die Datensicherung hat die Pflege ihrer Integrität und Verfügbarkeit zum Ziel. Sie ist regelmäßig durchzuführen, und die Sicherungsmedien sind an vom Verarbeitungsbereich entfernten Orten zu lagern, die das gleiche Schutzniveau bieten. Die Kontinuität des Dienstes wird durch Datensicherungs-Integritätstests garantiert. - Auf klassifizierten Medien (Magnetbänder, Disketten, transportable oder fest eingebaute Disks, Magnetplattenspeicher...) gespeicherte Daten sind vor Vernichtung ihres Trägermediums zu löschen oder zu überschreiben. - Daten, die für das Verteidigungsgeheimnis relevant sind, können in Übereinstimmung mit den geltenden Gesetzen chiffriert werden, wodurch die entsprechenden Medien bei diskontinuierlicher Verarbeitung zwischengelagert werden können.
EXP-15: Einrichtung einer Organisation zur Bekämpfung von böswilligen Codes	Durch Einführung einer Organisation und PSSI gegen die Bedrohung durch Viren kann das Risiko eines Integritäts-, Verfügbarkeits- und Vertraulichkeitsverlustes der Information verringert werden. Diese Organisation muss über die folgenden Einheiten verfügen: - Antivirus-Team (Administrator, Betreiber, Aktualisierung...); - Medienteam; - Krisenmanagement; - Organisation der Kontrolle. Bei der Bekämpfung böswilliger Codes kommt der Definition der Beziehungen zwischen den verschiedenen Beteiligten, insbesondere auf den Gebieten Kontrolle, Krisenmanagement sowie Aktualisierung von Tools und Verfahren, eine besondere Bedeutung zu.Bei der Definition einer Sicherheitsorganisation zum Schutz vor böswilligen Codes sind insbesondere die einzuführende Organisation sowie Rollen und Verantwortung jedes Akteurs festzulegen. Weiterhin ist eine technische Schutzarchitektur zur Virenabwehr zu erreichten, die alle Komponenten des Informationssystems (Arbeitsplätze, Mailserver, Internetserver, Speicherserver, Datenserver usw.) schützt.
EXP-16: Sicherheitshinweise in bezug auf Teleaktion	Teleaktion umfasst alle Betriebsoperationen des Netzwerks und der Arbeitsplätze, die dezentral durchgeführt werden: Speicherung, dezentrale Übernahme, dezentrale Applikationsinstallation, dezentrale Verarbeitung einer Anomalie, dezentrale Wartungsmaßnahme...

	Teleaktions-Zugriffe sind etwas Besonderes, wenn sie auf Arbeitsplätzen angewendet werden müssen, die Benutzern zugewiesen wurden. Dabei ist sicherzustellen, dass der Benutzer seine Umgebung beherrscht und dass kein Eingriff auf seine Dateien oder Arbeitssitzung ohne seine vorherige Genehmigung erfolgt. Damit wird ein Beitrag zur Aufrechterhaltung einer vertrauensvollen Beziehung zwischen den Netzwerkbetreibern und den Benutzern geleistet.
EXP-17: Schutz und Verwendung des Mailsystems	Um das Vertrauen in die Verwendung des elektronischen Mailsystems sicherzustellen, sind klare und einfache Regeln zu erarbeiten. So ist eine Liste technischer und nicht technischer Maßnahmen zu erstellen, um zu bekämpfen: - die Weiterverbreitung und Ausführung böswilliger Codes; - das Abfangen sensibler Informationen, die unverschlüsselt per E-Mail versandt werden; - Desinformation bzw. Spams; - die Veröffentlichung illegaler, diffamierender oder belästigender Informationen; Weiterhin sind Regeln zu erarbeiten, die sich beziehen auf: - die Aufbewahrung von Nachweisen für E-Mail-Austausch; - die Verwendung von Sicherheitsmitteln (Authentisierung, Chiffrierung der Signatur); - Verwendung des Mailsystems außerhalb der Organisation (vgl. dezentraler Zugriff); - die Überlastung des Mailsystems.
EXP-18: Spezielle Regeln für die Zugriffsfiltrierung	Router, Firewalls und E-Mail-Server können mit Filtern versehen werden, um nur den Zugriff auf bestimmte identifizierte Server zu erlauben. Alles, was nicht ausdrücklich erlaubt ist, müsste durch Zugriffsfilterung verboten werden. Dieses Prinzip ist auch intern gültig.
EXP-19: Normen für die Aufbewahrung und Vernichtung schützenswerter Informationen	Einige Kategorien von Informationen müssen unter bestimmten Bedingungen aufbewahrt und vernichtet werden. Für Informationen, die dem Verteidigungsgeheimnis unterliegen, präzisiert das Gesetz, welche Maßnahmen je nach ihrer Klassifikationsebene zu ergreifen sind. Für die anderen Kategorien sind die Maßnahmen an die Umgebung der Organisation anzupassen und müssen untereinander konsistent bleiben. Insbesondere sind, wenn die Information auf der Grundlage von Verträgen einer Organisation zur Aufbewahrung anvertraut wird, diese Aufbewahrungsbedingungen vorher auf ihre Ordnungsmäßigkeit zu prüfen. Für einige Organisationen kann in Ausnahmesituationen (Aufruhr, Bürgerkrieg...) die Notfall-Vernichtung eine besondere Bedeutung haben. Für die sich jedoch häufiger als notwendig erweisende Vernichtung von verfallenen Informationen, die eine bestimmte Rest-Vertraulichkeit haben, können präzise Normen zu deren Vernichtung erarbeitet werden.

	Außerdem unterliegt die Archivierung magnetischer Dokumente je nach Art der betreffenden Informationen (buchhalterische oder steuerliche Informationen, Mitarbeiterinformationen...) im Hinblick auf Aufbewahrungsdauer und Schutz der Medien rechtlichen Verpflichtungen.
EXP-20: Überprüfung beweglicher Medien vor ihrer Inbetriebnahme	Diese Regel, die sich auf die Kontrolle beweglicher Medien bezieht, zielt im wesentlichen auf Informationen mit vertraulichem Charakter ab und ist für Organisationen relevant, die sensible, mit dem Verteidigungsgeheimnis in Beziehung stehende Informationen oder Informationen, die als strategisch für ihre Aktivitäten beurteilt werden, verarbeiten. Eine grundlegende Maßnahme, die vor der Überprüfung und Wiederverwendung beweglicher Träger in einer anderen geschützten Installation stattzufinden hat, ist, dass alle auf ihnen gespeicherten Informationen durch vollständiges Überschreiben mit numerischen oder alphanumerischen Zeichen zu löschen sind. Enthalten diese Träger Informationen, die für das Verteidigungsgeheimnis relevant sind, ist für diese nach wie vor die höchste Daten-Klassifikationskategorie zutreffend, für die sie von Anfang an verwendet wurden (außer, sie wurden deklassiert). Dieses Prinzip kann auf nicht klassifizierte, besonders sensible Informationen angewendet werden.
EXP-21: Medien als Infektionsquelle und Preisgabesrisiko	Obwohl Organisationen für die Sicherheit von Systemen sensibilisiert sind, wird der Schutz beweglicher Träger (Disketten, Sicherungsbänder, Listen, Berichte...) oft vernachlässigt, obwohl diese Informationen der Organisation enthalten. Unter Träger versteht man jedes Mittel, das Informationen enthält, vor allem jedoch Datenträger, Papierträger (Listen, Dokumentation, Ausdrucken von Berichten...). Die Träger müssen gemäß den Regeln, die der Klassifizierung der Informationen entsprechen, die sie tragen, geschützt werden. Aus diesem Grund muss es auf Grundlage der Klassifikation Sicherheitsregeln geben, die sich auf die Verwaltung, die Überprüfung, die Lagerung (zur Vermeidung von Diebstahl und Vernichtung), den Transport und die Aussonderung beziehen. Obwohl heute die größte Virenbedrohung (böswillige Codes) im wesentlichen von öffentlichen Netzwerken ausgeht, ist das Problem der Einschleusung von Viren durch Datenträger immer noch erheblich (vgl. Bekämpfung von Viren). Für den Eingang/Ausgang von Datenträgern in/aus klassifizierte/n Zone/n gibt es spezielle Regeln (Registrierung der Medien, ihres Inhalts...) (vgl. Kontinuität beim Schutz von Informationen).
EXP-22: Aussonderung von Datenträgern oder Ausgang von Hardware	Hardware enthält Datenträger der Organisation. Deswegen sind der Eingang und insbesondere der Ausgang dieser organisationseigenen Medien zu kontrollieren. Diese Daten sind, ebenso wie die Daten, die auf anderen Trägern der Organisation gespeichert sind, zu vernichten, bevor etwas weitergegeben oder ausgesondert wird, und zwar entweder durch physische Vernichtung

	des Trägers oder durch gesichertes logisches Löschen (mehrfaches Überschreiben). Aus diesem Grund muss die Organisation für jede Medienart Regeln für deren Vernichtung erarbeiten, ggf. auch nach Klassifikationsniveau. Für Papierträger kann die Organisation entweder Aktenvernichter aufstellen oder die zu vernichtenden Träger zentralisieren und einer Fachfirma übergeben (mit der Verpflichtung, diese zu vernichten). In beiden Fällen sind die gelagerten Träger vor ihrer Vernichtung besonders zu schützen.
EXP-23: Fotokopieren von Dokumenten	Um das Fotokopieren auf Grundlage der Klassifizierung der Dokumente zu regeln, sind Sicherheitsrichtlinien zu erarbeiten. Diese Richtlinien sind unter Berücksichtigung der gesetzlichen Bestimmungen über das Fotokopieren zu verfassen.
EXP-24: Lagerung von Informationen durch die Organisation	Für die Lagerung von Informationen sind Sicherheitsregeln zu erarbeiten. Diese sind von allen Mitarbeitern klassifizierungsgemäß anzuwenden. Das Ziel dieser Regeln besteht vor allem darin, Informationen vor Preisgabe, Diebstahl oder auch Minderung zu schützen.
EXP-25: Anschluss wechselnder Arbeitsplätze und von PDAs	Es sind Sicherheitsregeln zu erarbeiten, die festlegen, welche Art von Informationen auf diesen Einheiten gespeichert werden dürfen. Es sind Schutz- und/oder Beaufsichtigungsmittel einzuführen, um die Einhaltung dieser Regeln sicherzustellen. Werden diese Mittel an das Informationssystem der Organisation angeschlossen, darf das nur bei Vorliegen einer Genehmigung erfolgen und unter Einhaltung seiner PSSI. Dabei ist besonders darauf zu achten, dass diese Ausrüstungen keine Brücke zwischen dem Informationssystem und einem öffentlichen Netzwerk bilden.

3.3.11 ENV : Physische Aspekte und Umgebung

ENV-01: Kontinuität bei der Verwaltung physischer Güter	Physische Güter sind während ihres gesamten Lebenszyklus - bei Zuweisung, Installation, im Betrieb, bei Wartung, Aussonderung und Vernichtung - zu verwalten. Diese Güter können ebenfalls wechselnden Eigentümern oder Verantwortlichen, Umgebungen oder Nutzungen unterworfen sein (Verleih von Material für eine Ausstellung, Neuzuweisung eines Materials im Rahmen eines neuen Projekts). Die Regel sieht vor, dass die gewählten Maßnahmen kontinuierlichen Schutz bieten, unabhängig von den Weiterentwicklungen oder Nutzungsänderungen, die die physischen Güter erfahren. Diese Kontinuität beruht auf der Annahme einer Klassifizierung (ggf. inkl. der Verteidigungsklassifizierung im Sinne von [IGI 900], die sich auf die Kontrolle physischer Güter ab ihrer Inbetriebnahme und über ihre Weiterentwicklung bis zu ihrer Ersetzung bezieht. Die wichtigsten Maßnahmen, die sich aus

dieser Regel ergeben, beziehen sich auf die Erfassung und die Markierung der Güter und spezielle Maßnahmen zu deren physischem Schutz ihrem Zustand entsprechend (Verleih, Wartung...), oder auf ihre Klassifizierung:

- durch die Erfassung werden die physischen Güter identifiziert, die schutzbedürftig sind,

- durch die Markierung wird die Wiedererkennung der Zugehörigkeit eines Elements zu einer bestimmten Klasse konkret materialisiert,

- durch die speziellen Maßnahmen zum physischen Schutz werden Hinweise auf die Aktionen gegeben, die gemäß der gewählten Klassifizierung durchzuführen sind. So darf sich z. B. ein Rechner mit der Aufschrift ,,Vertraulich'' in einer physischen Umgebung befinden, die diesem Schutzniveau angepasst ist, und in der physischen Umgebung einer ,,reservierten Zone''.

ENV-02: Berücksichtigung organisatorischer Zwänge der Organisation

Mittel und Maßnahmen zur physischen Sicherheit, die ohne Rücksicht auf die Zwänge der Organisation getroffen werden, können die ordnungsgemäße Abwicklung operativer Aufgaben behindern und dazu führen, dass sie von den Mitarbeitern abgelehnt werden.

Aus diesem Grund ist es notwendig, bei der Einführung von Mitteln und Verfahren zur physischen Sicherheit die operativen Zwänge der Organisation zu berücksichtigen.

ENV-03: Vollständigkeit der physischen Sicherheitsmaßnahmen

Es sind die verschiedenen Arten der folgenden Maßnahmen zu berücksichtigen.

Maßnahmen zum Schutz physischer Güter haben zum Ziel, das Ausmaß von Beeinträchtigungen zu vermindern, insbesondere im Bereich der Verfügbarkeit, der Integrität und der Vertraulichkeit.

Da es keine Universallösungen für alle Bedrohungsformen gibt, ist die Organisation verpflichtet, ein Bündel von vorbeugenden, erkennenden, reagierenden und veranlassenden Maßnahmen zu ergreifen, die in der Lage sind, einen Angriff in seinem Verlauf zu vereiteln und die verursachten Schäden zu reparieren.

Vorbeugende Maßnahmen sind auf die Verringerung der Wahrscheinlichkeit gerichtet, dass ein Schadenfall eintritt. Sie bestehen z. B. darin, im Hinblick auf das Risiko eines Brandes oder einer Überschwemmung auf die Lokalisierung bestimmter Räume (wie z. B. Bandarchive, Archive, Kanalisationen, Räume zur Aufbewahrung von Gefahrgütern) zu achten oder die Konformität der Verwendung von Materialien zu kontrollieren.

Erkennende Maßnahmen sind auf die Ausgabe einer Warnmeldung bei einem Eindringversuch oder bei der Auslösung eines Schadenfalls im Umkreis des Informationssystems gerichtet.

	Sie müssen die Lokalisierung dieser Warnung ermöglichen. Diese Maßnahmen werden durch die Installation von erkennenden oder Warnmitteln an kritischen Stellen realisiert, wie z. B. von Wärmefühlern oder Überwachungskameras. Reagierende Maßnahmen sind auf die Bekämpfung eines angezeigten Schadenfalls gerichtet, um dessen Auswirkungen zu vermindern. Diese Maßnahmen werden durch das Auslösen eingreifender Mittel, die von der Organisation vorgesehen wurden, realisiert, wie z. B. eines Brandbekämpfungsdienstes. Veranlassende Maßnahmen sind auf die Begrenzung der Folgen eines Schadenfalls gerichtet und sollen die Rückkehr des Informationssystems zum normalen Betrieb erleichtern. Sie können in der Aktivierung von Rettungsmitteln oder in der Deaktivierung von Sicherheitsfunktionen bestehen, so kann z. B. das physische Zugriffskontrollsystem im Rahmen eines Sicherheitsbetriebs im Notbetriebsmodus zeitweilig außer Kraft gesetzt werden. Die gewählten Maßnahmen müssen in Übereinstimmung mit allen von der Organisation befürchteten Schadenfällen abgestuft sein, um sicherzustellen, dass diese ausreichen, um einen Angriff zu vereiteln oder abzuschwächen.
ENV-04: Isolierung sensibler oder lebenswichtiger Systeme	Durch Isolation sensibler oder lebenswichtiger Systeme wird die Gefahrenexposition von Gütern vermindert. Das Risiko ist damit reduziert. Außerdem besteht damit die Möglichkeit zu einer bestmöglichen Proportionierung der Sicherheitsmaßnahmen bei Reduzierung der Kosten gegenüber einem alles umfassenden Schutz.
ENV-05: Äquivalenz von physischen Sicherheitsmaßnahmen und Güterarten	Die physischen Sicherheitsmaßnahmen sind in allen Räumlichkeiten durchzusetzen. Sie dienen zunächst dem Schutz der Mitarbeiter und tragen außerdem dazu bei, Risiken einer Zerstörung oder Preisgabe, die direkt oder indirekt die lebenswichtigen Interessen des Unternehmens oder der Organisation beeinträchtigen könnten, zu vermindern.Diese Regel besagt, dass die in der obiger Regel genannten Maßnahmen an die drei Kategorien physischer Güter - Infrastruktur, Hardware und unterstützende Ausrüstungen - angepasst werden können
ENV-06: Schutz vor Unfällen und Pannen	In Räumlichkeiten, in denen sich für das Informationssystem lebenswichtige Ausrüstungen befinden (inkl. Komponenten für die Netzwerkinfrastruktur), sind unter Berücksichtigung der Bedrohungen der näheren Umgebung die folgenden Maßnahmen zu treffen: - gegen Beschädigung durch Wasser; Erkennen und Reaktion - (Ausrüstungen sollten nicht in Risikoräumen untergebracht

	werden, durch die z. B. Wasserleitungen führen oder die überschwemmt werden könnten); - zur Branderkennung und zum Brandlöschen; - zur Kontrolle und Sicherstellung der elektrischen Versorgung und Notfallversorgung (wobei zumindest die Schutzelemente eine Mindest-Versorgungsdauer sicherstellen müssen, um die notwendigen Rettungsmaßnahmen durchführen zu können); - zur Notfallversorgung der Telekommunikationsnetzwerke (wobei besonders den Verfahren zum Umschalten auf Notfallversorgungsleitungen im Falle einer Leitungsunterbrechung zu achten ist); - zur Klimatisierung und Luftkonditionierung (an die Belieferung mit Verbrauchsmaterialien wie Wasser, Gas und Filter denken, sowie an Maßnahmen der Staubbekämpfung); - formalisierte Verfahren, wie bei Schadenfällen oder Pannen zu reagieren ist (inkl. außerhalb der Arbeitszeit); - Notfallmaßnahmen. Bei der Kontrolle der Umgebung sind Temperatur, Feuchtigkeit, Staub und Vibrationen zu berücksichtigen. Weiterhin ist für nicht beherrschbare Schadenfälle ein Notfallplan zu erarbeiten. (Vgl. Krisenmanagement) Alle installierten Schutzausrüstungen sind regelmäßig zu überprüfen. Überprüfungen (insbesondere von Brandschutzmaßnahmen) sind gesetzlich vorgeschrieben. Es wird dringend geraten, auch Ausrüstungen zu überprüfen, deren Überprüfung nicht vorgeschrieben ist (z. B. um Wassereinbrüche zu erkennen).
ENV-07: Physischer Schutz von Kabeln und Telekommunikationsnetzwerken	Telekom- und Informatikkabel müssen so gut wie möglich vor jedwedem böswilligen Zugriff geschützt werden, der zu Abhören führen könnte (Erdkabel, verdeckte Kabel...). Datenübertragungs- und Verteilungsausrüstungen sind vor Zugriff zu schützen. Der Schutz des Zugriffs auf Kabel und andere Netzwerkkomponenten (unabhängig davon, ob der Zugriff auf diese genehmigungspflichtig ist oder nicht) bewirkt nicht nur, dass passives (und manchmal auch aktives) Abhören verhindert wird, sondern auch zufällige Beschädigung.
ENV-08: Einteilung der Infrastruktur in Sicherheitszonen	Standorte, Gebäude und Räume, die materielle oder immaterielle Güter (Informationen und ihre jeweiligen Medien, Hardware, die zum Informationssystem gehört) enthalten oder in denen sicherheitsrelevante Aktivitäten stattfinden, sind einer besonderen Zugriffskontrolle zu unterziehen. Eine Sicherheitszone ist eine Zone, in der ständig Vorkehrungen

	zur Kontrolle der Bewegungen der Mitarbeiter und der Hardware sowie zum Erkennen und Verhindern von Abhören getroffen werden. Durch Einteilung der Infrastruktur in Sicherheitszonen wird die Einrichtung entsprechender Vorrichtungen erleichtert, was insbesondere auf die Kontrolle von Personalbewegungen durch Zuweisung spezieller Zugangsrechte zu den Zonen zutrifft. Diese Rechte können an Arbeitsplätze und Verantwortungsebenen gebunden werden.
ENV-09: Anwendung der Bedingungen für den Besucherempfang und -verkehr	Die Bedingungen für den Besucherempfang und - verkehr werden im allgemeinen von allgemeinen Sicherheitsdienst festgelegt. Außerdem ist jeder Benutzer des Informationssystems verpflichtet, für die Anwendung dieser Regel in seinem eigenen Arbeitsbereich oder in der Nähe seines Arbeitsplatzes Verantwortung zu übernehmen, was keine Überschneidung mit Obigem bedeutet. Der verantwortliche Verwahrer ist nämlich derjenige, der am besten die Unversehrtheit des ihm anvertrauten Informationsbestandes überprüfen kann. Diese Regel ist mit der Regel über die Einteilung der Infrastruktur in Sicherheitszonen zu harmonisieren, wodurch die Kontrolle der Besucher erheblich erleichtert wird.
ENV-10: Spezielle Verwaltung schutzbedürftiger physischer Güter	Zur Verwaltung schutzbedürftiger physischer Güter sind eine Klassifizierung oder Typologie, Maßnahmen zur Verwaltung dieser Güter und Maßnahmen zu ihrem lebenslangen Schutz zu erarbeiten. Dabei müssen sowohl die Mittel zum physischen Schutz als auch alle anderen Sicherheitsmaßnahmen dem Wert der zu schützenden Güter entsprechen und sich in Übereinstimmung mit den anderen angewendeten Sicherheitsmaßnahmen befinden. Dazu legt Art. 10 [IGI 900] fest: "Alle Dokumente, Hard- und Software, die wegen ihrer Integrität oder Vertraulichkeit zur Sicherheit eines Informationssystems beitragen, werden mit dem Hinweis ACSSI gekennzeichnet. ACSSI macht darauf aufmerksam, dass Verwaltung und Schutz dieser Mittel in Übereinstimmung mit den Vorschriften der ministeriellen Anweisung zu erfolgen haben, die sich auf die Artikel über die Kontrolle der Sicherheit von Informationssystemen beziehen." Physische Güter, die nicht als verteidigungsrelevant eingestuft werden, können anhand einer Typologie ihrer Art und Zuweisung entsprechend zusammengefasst werden. Auf Grundlage des Sicherheitsanforderungsniveaus werden Schutzklassen, d. h. Vertraulichkeits-, Integritäts- und Verfügbarkeitskriterien für diese Güter, erarbeitet, um ihre kontinuierliche Kontrolle sicherzustellen. Die angenommene Typologie entspricht den organisationseigenen Aufgaben oder Berufen, ihrer Kultur und ihren Zwängen.
ENV-11: Verfahren zur gesicherten Nutzung	Dezentrale Mittel, die zur Nutzung außerhalb ihrer Sicherheitszone vorgesehen oder aus dieser Zone verbracht

dezentraler Mittel	werden (PCs, tragbare Hardware, Drucker, Fotokopierer, Faxgeräte...), sind oft durch kleine Benutzerteams, ja sogar Einzelbenutzer, gekennzeichnet. Da diese ohne die Möglichkeit zur sofortigen Unterstützung und ohne Zugriff auf den physischen Schutz einer Sicherheitszone agieren, ist die Wahrscheinlichkeit eines Zwischenfalls oder einer Beeinträchtigung der Sicherheit dieser Güter sehr hoch, denn dort, wo eine Überprüfung schwierig ist, sind Indiskretion und Böswilligkeit Hauptbedrohungen. Aus diesem Grund hat das Betreiben dieser Mittel unter speziellen Bedingungen zu erfolgen, die ihrer Umgebung angepasst sind, was heißt, dass sich diese Peripherieausrüstungen nach Möglichkeit in einer kontrollierten Zone befinden sollten. Der Umgang mit tragbarer Hardware ist besonders zu untersuchen. Steigende Speicherkapazitäten und Verarbeitungsleistungen führen zu einem immer häufigeren Rückgriff auf tragbare Maschinen. Allerdings sind diese vielfältigeren Bedrohungen als fest aufgestellte Hardware ausgesetzt. Weiterhin ist die zum Schutz der Informationen notwendige Kontrolle aufgrund der Besonderheiten ihrer Verwendung viel schwieriger sicherzustellen. Da sie tragbar und klein sind, steigt die Wahrscheinlichkeit eines Verlustes oder Diebstahls erheblich. Schützenswerte Informationen sollten nach Möglichkeit nur dann auf tragbaren PCs verarbeitet werden, wenn sich diese an Orten befinden, die dem Klassifizierungsniveau dieser Informationen entsprechen. Wird diese Hardware nach außerhalb der Organisation verbracht, ist das gleiche Verfahren wie für den Ausgang klassifizierter Dokumente anzuwenden.
ENV-12: Schutz der Sicherheitsdokumentation	Die Sicherheitsdokumentation ist vor unautorisiertem Zugriff zu schützen. Ihr Schutzniveau entspricht dem Niveau der Bestandteile, auf die sie sich bezieht.Folgende Maßnahmen sind denkbar: - der verantwortliche Inhaber der Sicherheitsdokumente muss die Position der ihm anvertrauten Dokumente kennen und deren Verwendung kontrollieren; - der Umgang mit diesen Dokumenten ist nur den Mitarbeitern gestattet, die dafür eine Genehmigung haben; - die Dokumente werden an sicheren Orten aufbewahrt; - die Verteilung, die dem Sicherheitsverantwortlichen unterliegt, kann auf ein Minimum an Personen beschränkt werden.
ENV-13: Schutz der Ausrüstung vor Diebstahl	Der Mitarbeiter, dem die Ausrüstung zugewiesen wird, ist, auch wenn dies nur zeitlich vorübergehend sein sollte, ab der Zuweisung für ihren Schutz verantwortlich. Dazu sind konsistente und geeignete Mittel anzuwenden.Muss der Inhaber dieser Ausrüstung diese nach außerhalb des Standorts

	verbringen, sollten auf ihr nach Möglichkeit nur die Informationen gespeichert sein, die zur Erfüllung seiner Aufgaben außerhalb des Standorts notwendig sind. Ggf. sind die Informationen auf einem externen herausnehmbaren Medium zu transportieren. Da das Diebstahlrisiko bei tragbaren PCs auch am Standort der Organisation hoch ist, sollten diese inventarisiert und regelmäßig überprüft werden. Zur Festlegung der vom Inhaber und von der Organisation im Falle eines Diebstahls der Ausrüstung durchzuführenden Aktionen ist ein besondere Verfahrensanweisung zu erarbeiten.
ENV-14: Schutz der Sicherungsmedien	Sicherungsmedien sind vor Vernichtung, Preisgabe und Diebstahl zu schützen. Auf diese Art von Medien ist besonders zu achten, da sie aufgrund ihrer Natur einen Teil der Systeminformationen beinhalten und deswegen bevorzugtes Ziel für einen Diebstahl von Informationen sind. Ihre Nichtverfügbarkeit würde der Organisation die Fähigkeit zur Wiederherstellung der Betriebsbereitschaft nach einem Schadenfall nehmen.
ENV-15: Schutz der Systemdokumentation	Die Systemdokumentation (Netzwerkarchitektur, Bezeichnungsplan...) enthält Informationen, die, wenn sie mit anderen Informationen in Verbindung gebracht wird (Informationen über Schwachstellen...), wichtige Elemente enthalten, um einen Angriff erfolgreich durchzuführen. Ihre Preisgabe nach außen kann bestimmten Personen Möglichkeiten zur Durchführung von Eindringversuchen bieten. Aus diesem Grund sind diese Dokumentationen zu klassifizieren, und ihr Ausgang nach außen ist zu kontrollieren, was sich auch auf die Verteilung an Lieferanten bezieht.
ENV-16: Verwendung außerhalb des Standorts	Das Verbringen von IT-Ausrüstungen nach außerhalb des Standorts und ihre dortige Verwendung ist genehmigungspflichtig. Es sind Regeln zu erarbeiten, um ihre Verwendung an öffentlichen Orten oder in Verbindung mit anderen Informationssystemen zu beschränken. Werden diese Ausrüstungen an das Informationssystem eines Kunden oder Partners angeschlossen, darf das nur bei Vorliegen einer Genehmigung dieser anderen Organisation erfolgen, wobei der Eigentümer der Ausrüstung die PSSI einzuhalten hat. Um jedweden unautorisierten Zugriff auf Informationen, die sie speichern und verarbeiten, zu verhindern, sind die IT-Ausrüstungen zu schützen.

3.3.12 AUT : Identifikation / Authentisierung

AUT-01: Verwendung des gleichen Geheimworts für den Zugriff auf mehrere Dienste	Die zum Schutz von Authentisierungsgeheimnissen verwendeten Mittel bieten je nach Applikation und System ein unterschiedliches Sicherungsniveau. Aus diesem Grund müssen sich die Benutzer, wenn sie in Systemen mit konsistentem Schutz das gleiche Geheimwort verwenden möchten (Beispiel: Verwendung des gleichen Passworts, um sich

	gegenüber dem Betriebssystem und verschiedenen Applikationen zu authentisieren), darüber informieren, wie robust die Authentisierungssysteme eigentlich sind. Daraus ergibt sich, dass das gleiche Geheimwort nur für Dienste mit äquivalentem Sicherungsniveau verwendet werden darf.
AUT-02: Kombination von Authentisierungsmitteln	Der Zugriff auf das Informationssystem impliziert, dass die Benutzer zu Beginn einer Sitzung (und in gewissen Fällen auch während der Sitzung) durch Vorlage eines Authentisierungsmittels ihre Identität nachweisen. Die derzeitigen Authentisierungstechniken stützen sich auf drei Elemente: - auf das, was man weiß, z. B. Passwörter, - auf das, was man hat, z. B. Chipkarten, - auf das, was man ist, d. h. ein persönliches Merkmal (digitaler Fingerabdruck, Prüfung des Augenhintergrundes, dynamische Signatur...). Durch Zusammenführung dieser drei Elemente wird eine umfassende und wirksame Authentisierung erreicht, deren Kostenrahmen allerdings relativ hoch ist. Folglich muss der verantwortliche Inhaber mit Hilfe des Sicherheitsmitarbeiters auf der Grundlage dieser drei Konzepte bestimmen, welche Kombinationen für sein Informationssubsystem oder seine sensiblen Applikationen am besten geeignet sind. Werden mindestens zwei dieser Konzepte vereint, spricht man von einer starken Authentisierung. Eine Authentisierung, die sich lediglich darauf stützt ,,was man weiß", entspricht dem Minimal-Sicherheitsprofil eines Informationssystems. Demzufolge ist auf dynamische Mechanismen wie nur einmal verwendbare oder in der Anzahl ihre Anwendungen begrenzte Passwörter zurückzugreifen. In diesem Fall wird ein Zugriffszähler eingesetzt, auf den sich die Schutzanstrengungen zu konzentrieren haben. Generell ist festzustellen, dass die verwendeten Mittel auf Authentisierungselementen beruhen, die streng zu beaufsichtigen sind.
AUT-03: Eindeutigkeit der Benutzeridentität	Die Identität der Benutzer ist sowohl von der Systemleitung als auch vom Sicherheitsverantwortlichen eines Standorts oder einer operativen Einheit (Ebene Sicherheitsmitarbeiter) zu verwalten. Die eindeutige (unzweideutige) Identifikation des Eigentümers eines Zugangs ist zur Gewährleistung der Rückverfolgbarkeit von Operationen sowie für die Diagnose einer Sicherheitsanomalie (vgl. Kontrolle und Audit) von grundlegender Bedeutung.
AUT-04: Aushändigung und Deaktivierung von Authentisierungsmitteln	Auch bei ausgeklügeltsten Technologien zur Beaufsichtigung des Zugriffs auf ein Informationssystem bleiben die Aushändigung, die Verwendung und das Management von Authentisierungsmitteln lebenswichtige Elemente des Systems. Aus diesem Grund sind die folgenden Regeln klar zu formulieren und sorgfältig einzuhalten: - Bevor einem Benutzer ein Zugriffsmittel ausgehändigt wird, hat sich dieser durch Unterschrift formal zu verpflichten, die elementaren Regeln zum Schutz dieser Zugriffsmittel einzuhalten und seiner Benachrichtigungspflicht bei Diebstahl (oder einfachem Verdacht auf

Preisgabe des Geheimnisses) zu genügen. (vgl. Verantwortlichkeiten, vgl. Zuweisung sensibler Arbeitsplätze).

- Die Aushändigung von Zugriffsmitteln (Passwörter, Chipkarte...) hat so zu erfolgen, dass sichergestellt wird, dass nur der rechtmäßige Eigentümer dieser Mittel Kenntnis dieser Geheimnisse erlangt.

- Bei Bearbeitung einer Diebstahl- oder Verlustanzeige muss gewährleistet sein, dass die Identität des Benutzers vor Usurpation geschützt ist.

- Verlässt ein Mitarbeiter die Organisation (oder wird er umgesetzt), sind alle seine Zugriffsmittel auf das Informationssystem systematisch zu deaktivieren.

Es ist davon auszugehen, dass die Sicherheit bereits dann beeinträchtigt ist, wenn zwei oder mehr Personen z. B. das einer Benutzeridentität entsprechende Passwort kennen, es sei denn, das das im Interesse der Absicherung von Kontinuität bei den Verwaltungsfunktionen des Systems gewünscht wird.

Sollte in einigen Fällen die Teilung einer Identität und eines Authentisierungselements erlaubt werden müssen, sind besondere Maßnahmen wie versiegelte Umschläge mit Erfassung zu entwickeln, um missbräuchlicher oder fehlerhafter Benutzung vorzubeugen.

3.3.13 CAL : Kontrolle des logischen Zugriffs auf Güter

CAL-01: Vorrichtungen und Verfahren zum Schutz vor Eindringen

Die Architektur der Kommunikationsinfrastrukturen muss Einrichtungen und Verfahren beinhalten, die ein adäquates Schutzniveau vor Eindringen sicherstellen.Der Zugriff auf das Informationssystem und seine wichtigsten Ressourcen (Anwendungen) ist zu kontrollieren, um sich vor missbräuchlichem Zugriff - Eindringen - zu schützen. Dabei sind die dafür einzusetzenden Mittel je nach Sicherheitsziel unterschiedlich und können solche Maßnahmen wie Barrierevorrichtungen (Firewall) und Systeme zur Authentisierungs- und Zugriffskontrolle beinhalten.

Geeignete Defensivvorrichtungen, die die festgelegten Sicherheitsziele erfüllen, sind nach einer SIS-Risikoanalyse zu bestimmen. Diese Analyse beinhaltet die Ermittlung aller potentiellen Angriffsziele und eine Untersuchung der für die Angreifer möglichen Zugriffsmittel.

CAL-02: Netzwerkabschirmung und Informationsflusskontrolle

Die Netzwerkabschirmung hat zum Ziel:

- Erleichterung der Kontrolle des physischen Zugriffs,

- besserer Schutz vor Eindringen,

- Verhinderung von Informationsabfluss:

o in Netzwerke oder zu internen Arbeitsplätzen des Unternehmens, die von Personen besetzt werden, die diese Informationen nicht kennen sollen,

o in Netzwerke oder zu Arbeitsplätzen, die sich außerhalb des Unternehmens befinden,

o durch Herstellen einer Verbindung von außerhalb des Unternehmens bei z. B. Einsatz einer Rebound-Technik über eine Stelle, die gleichzeitig mit dem internen Netzwerk des Unternehmens und einem Modem verbunden ist.

Durch Abschirmung werden besondere Zonen bzw. Sicherheitsbereiche geschaffen, insofern diese als solche erkannt werden. Diese internen Sicherheitsgürtel sind immer dann einzurichten, wenn bei einer Analyse Untereinheiten oder sensible Applikationen festgestellt werden, die eine Sicherheitspolitik und besondere Zugriffskontrollen sowie Kommunikation erfordern.

Kommunikation zwischen innerhalb und außerhalb eines Sicherheitsgürtels hat ausschließlich über eine Einrichtung (Barrierevorrichtung) zu erfolgen, die zu Abschirmungszwecken errichtet wurde und die für die Einhaltung der besonderen Anforderungen, die an diesen Bereich gestellt werden, zuständig ist. In diesem Zusammenhang ist an der Grenze eine ,,Flussmatrix" einzurichten, die dokumentiert, welche Kommunikation von wem zu wem mit welchem Inhalt unter welchen Bedingungen stattgefunden hat.

Die Netzwerkabschirmung, anhand derer eine Informationsflusskontrolle möglich wird, stützt sich auf die Zugriffsrechte von Personen, Funktionen und Prozesse.

Eine weitere Abschirmungslösung ist der Schutz von sensiblen Informationen bei deren Übertragung.

Dabei wird überprüft, dass das für diese kommunizierten Informationen erforderliche Schutzniveau korrekt erreicht wird.

Sensible Informationen werden bei ihrer Übertragung dadurch geschützt, indem die verschiedenen Möglichkeiten, Übertragungsnetzwerke anzugreifen, so weit wie möglich ausgeschaltet werden.

Geschützt wird vor:

- Fehlleitung des Nachrichtenverkehrs auch in einer gestörten oder gesättigten Umgebung (dessen Ziel darin besteht, die Funktionsfähigkeit von Verbindungen zu verhindern oder zu stören),

- Eindringen (das zum Ziel hat, Nachrichten zu Betrugszwecken einzuschleusen oder zu verändern),

- Abfangen (d. h. des nicht erlaubten Empfangs von Sendungen),

- Nachrichtenverkehrsanalysen (aus der Untersuchung des

Nachrichtenverkehrs können Informationen abgeleitet werden).

Die klassischen Schutzmittel zur Gewährleistung von Kommunikationssicherheit sind in diesem Zusammenhang Chiffriermittel und Hardware, die keine kompromittierenden Signale aussendet.

Chiffrierung wird als Gesamtheit aller kryptografischen Mittel definiert, mit denen übertragene Informationen so geschützt werden, dass sie für all diejenigen, die nicht berechtigt sind, diese zu verstehen, unverständlich werden. Chiffriert werden entweder die Nachrichten selbst oder die Übertragungswege.

Dieses Prinzip beruht mit auf der Tatsache, dass, sollten die Sicherheitsmaßnahmen, die dem geforderten Schutzniveau entsprechen, den Einsatz von Chiffriermitteln erforderlich machen, der Einsatz dieser Mittel gesetzes- und vorschriftenkonform zu erfolgen hat und von speziellen organisatorischen Managementmaßnahmen zu begleiten ist.

CAL-03: Bedingungen für die sichere Nutzung organisationseigener Telekommunikationsnetze

Die sichere Nutzung der Telekommunikationsnetzwerke der Organisation darf nicht dazu führen, dass Sicherheitsmaßnahmen auf Ebene der Infrastruktur (z. B. die Einrichtung von Sonderzonen), der Mitarbeiter (z. B. Management des Kenntnisbedarfs), der Sicherheitsorganisation bzw. der Organisation von Hard- und Softwareressourcen in Frage gestellt werden.

Mit Zunahme der Zugriffsmöglichkeiten der Benutzer aufgrund eventueller Querverbindungen zwischen internen Netzwerken wächst die Notwendigkeit, die Bedingungen für die Nutzung der Telekommunikationsnetzwerke der Organisation zu definieren.

Um Telekommunikationsnetzwerke sicher nutzen zu können, sind Funktionen und Mechanismen einzurichten, die die Sicherheit der Daten auf ihren Übertragungswegen sicherstellen. Dafür bietet sich die folgende Aufteilung an:

- Authentisierung,
- Zugriffskontrolle,
- Vertraulichkeit der Daten,
- Integrität der Daten,
- Prüfung von Integrität und Ursprung der Daten,
- Verfügbarkeit.

Die o. g. Zugriffskontrolle beruht z. B. auf Management- und Kontrollmaßnahmen, die zeitlich unbeschränkt sind und sich beziehen auf:

- den Zugriff der Benutzer auf Dienste, für die sie eine

	Berechtigung haben, - den Anschluss isolierter oder organisationsexterner Computer an das Informationssystem, - die Aufteilung der Netzwerke in besondere Bereiche, - die Verteilung von Kommunikationen auf erlaubte Kanäle.
CAL-04: Zugriffsorganisation auf das Informationssystem	Um Kontrolle und Management von Zugriffen auf das Informationssystem sicherzustellen, muss die Organisation Regeln aufstellen und technische Normen festlegen. Diese Regeln und Normen müssen die Sicherungsebenen der Zugriffs-Beaufsichtigungsmittel definieren für: - den Zugriff auf das Unternehmensnetzwerk (Intranet) und auf transversale Dienste (im wesentlichen Mailsystem und Internetdienste), - ggf. den Zugriff auf ein gesichertes Unter-Netzwerk, - den Zugriff auf Applikationen der Organisation, - den Zugriff auf transversale Dienste des Unternehmens von außen, vor allem auf das Mailsystem, - den Zugriff auf die Hardware, die mit dem Netzwerk der Organisation verbunden ist, - den Zugriff von Arbeitsplätzen der Organisation auf andere Netzwerke vom Standort der Organisation aus und außerhalb dieses Standorts, - den Zugriff von Lieferanten auf das Informationssystem, - den öffentlichen oder ,,geladenen" Zugriff. Je nach Sicherheitsbedürfnis der Informationen und/oder der Funktionen des Informationssystems sind zu bestimmen: - die einzusetzende Technologie (Authentisierungsalgorithmus, Passwörter, die nur einmal verwendet werden können...), - Geheimnisschutz (Passwortdateien, die von Systemen oder Applikationen angelegt werden), - Bedingungen für die Zugriffszuweisung (Verpflichtung des Benutzers, die elementaren Regeln für einen geschützten Zugriff einzuhalten), - Anforderungen an die Robustheit der Zugriffsmittel und Passwörter - Konstruktionsregeln - Intervalle, in denen die Passwörter zu wechseln sind - Chronologie nicht wiederverwendbarer Passwörter, - Lebensdauer der Zugriffszuweisung, - alle Authentisierungsverfahren bei sensiblen Zugriffen oder solchen, die Medien verwenden, die als nicht vertrauenswürdig betrachtet werden (öffentliche Netzwerke) (Gewährleistung der

	Nicht-Preisgabe der Authentisierungselemente), - Verfahren bei wiederholt erfolglos verlaufenden Verbindungsversuchen, - Beschränkung der Verbindungszeiten, - Verfahren bei Anzeige des Verlusts eines Geheimworts, Bekämpfung von Identitätsusurpation, - Verfahren für Zugriffsdeaktivierung bei Ausscheiden eines Mitarbeiters oder Diebstahl von Hardware. Dezentrale Zugriffe auf das Informationssystem von außerhalb der Räumlichkeiten der Organisation (Internetzugriff, Zugriff über ein handvermitteltes Netz) sind besonders zu schützen (vor allem vor Sitzungsdiebstahl, Geheimnispreisgabe, Identitätsusurpation, absichtliche Zugriffssättigung). Für jeden dieser Zugriffe sind Verfahren zur Definition von Profilen (inkl. der Profile von Netzwerkbetreibern und Applikationen), Zuweisungen und für das Zugriffsmanagement festzulegen. Dabei empfiehlt es sich prinzipiell, nur dann einen Zugriff und Privilegien zuzuweisen, wenn diese für die Erfüllung einer Aufgabe notwendig sind. Die Sensibilisierung der Benutzer für den Schutz der ihnen anvertrauten Informationen und Mittel, die ihnen für den Zugriff auf das Informationssystem der Organisation zugewiesen wurden, spielt dabei eine besonders wichtige Rolle (die Arbeitsplätze sind die Hauptzugriffspunkte auf das Informationssystem).
CAL-05: Dateien mit Passwörtern	Ale Dateien, die Passwörter (oder Geheimwörter) enthalten, sind nach Möglichkeit auszuschließen oder zu chiffrieren (z. B. Anmeldungsskript).
CAL-06: Unterdrückung nicht kontrollierter Zugriffe auf das Informationssystem	Wichtig ist, dass alle Zugriffe auf das Informationssystem kontrolliert werden können. Aus diesem Grund sind die folgenden Zugriffe besonders zu beobachten: - von einer Ausrüstung, die mit dem Informationssystem verbunden ist und gleichzeitig über einen direkten öffentlichen Zugang verfügt (z. B. Laptop, der sowohl mit einem Modem als auch dem Unternehmensnetzwerk verbunden ist), - nicht erlaubte Verbindungen eines Arbeitsplatzes über einen physischen Netzwerkzugriff.
CAL-07: Zuweisung von Zugriffsprivilegien an Dienste	Die Zuweisung eines Zugriffs und der damit verbundenen Privilegien ist von dem oder den Eigentümer/n der Systeme, auf die der Zugriff erfolgt, zu bestätigen, damit diese/r überprüfen kann/können, ob der Zugriff mit den Berechtigungen des Benutzers übereinstimmt und ob die

	Prinzipien der Verantwortlichkeit (Separierung von Befugnissen, Privileg minderer Ordnung) eingehalten werden. Für sensible Dienste empfiehlt sich das Führen eines Verzeichnisses über erlaubte Zugriffe und Privilegien.
CAL-08: Schutz von Sonderzugriffsrechten (Wartungszugriff) auf das Informationssystem	Wartungszugriffe sind Zugriffe, die erweitere Zugriffsprivilegien auf die Systeme gewähren. Werden sie von außerhalb der Organisation ausgeführt (z. B. von Dienstleistern), sind verstärkte Mittel zum Schutz vor böswilliger Verwendung sowie Mittel zur Rückverfolgbarkeit zu definieren. In die Dienstleistungsverträge (vgl. Leistungsvertrag) sind spezielle Verpflichtungen im Hinblick auf die Übernahme von Verantwortung aufzunehmen.
CAL-09: Überprüfung der Zugriffslisten auf das Informationssystem	Zur Aufrechterhaltung der Zugriffskontrolle auf das Informationssystem sind die Listen für den Zugriff und verbundene Privilegien in regelmäßigen Abständen (auch nach dem Zufallsprinzip) zu überprüfen. Diese Kontrolle kann auf der Grundlage eines Abgleichs zwischen der Zugriffsbestandsliste, den vorhandenen, von den Benutzern unterschriebenen Verpflichtungserklärungen und der Personalliste erfolgen. Bei Zugriffen auf sensible Informationen und/oder Funktionen können sie verstärkt durchgeführt werden. Sollten Zwischenfälle festgestellt werden (z. B. unberechtigter Zugriff, zu weitreichende Privilegien...), sind die in einer Verfahrensanweisung festgelegten Aktionen durchzuführen. Bei diesen Verfahren sind die Anforderungen an das Informationssystem durch Verringerung von Privilegien zu berücksichtigen.
CAL-10: Kontrolle der Privilegien von Benutzern des Informationssystems	Es ist eine Regel zu erarbeiten, nach der die Rechte auf Privilegienbesitz überprüft werden, und zwar unabhängig von den Betriebskontrollen, die mit der Art und Weise der Nutzung der Privilegien in Beziehung stehen. Ziel dieser Kontrolle ist es, sobald ein Benutzer versucht, seine Privilegien auf eine Ressource des Informationssystems anzuwenden, diese Aktion nur dann zu erlauben, wenn sie innerhalb der in der Organisation geltenden Sicherheitsregeln stattfindet. Die aus dieser Regel ableitbaren Maßnahmen stützen sich auf: - Aktionen, für die eine Überprüfung der Privilegien stattzufinden hat, - Maßnahmen, die eingeleitet werden müssen, wenn eine Aktion versucht wird, für die das entsprechende Recht fehlt, - regelwidrige Vergünstigungen bei der Privilegienüberprüfung und ihren Gültigkeitsbedingungen.
CAL-11: Anwendung des Begriffs des	Der Begriff Informationssystembenutzerprofil beinhaltet zunächst einmal die Strukturierung von Daten (oder Objekten)

Informationssystembenutzerprofils	nach Funktionen oder Aktivitäten der Organisation, an denen der verantwortliche Inhaber ein Vorrecht hat. Die von den Benutzern verwendeten Daten sind auf Grundlage der von ihnen im Rahmen einer funktionellen Einheit (z. B. Lagerverwaltung bei einem Versorgungsdienst) verwendeten Applikationen, im Rahmen der Nutzung gemeinsamer Ressourcen (z. B. lokale Netzwerke) oder einer speziellen Aufgabe oder Aktivität, für die eine Arbeitsplatzabschirmung notwendig ist, strukturiert. Auf die gleiche Art und Weise sind auch die verschiedenen Mitarbeiter- (oder Subjekt)kategorien durch Definition von Informationssystembenutzerprofilen zu strukturieren, anhand derer Zugriffsprivilegien, die mit dem Lesen (anzeigen, ausdrucken) verbunden sind, und Verarbeitungsprivilegien, die mit dem Schreiben (anlegen, ändern, vernichten) verbunden sind, im Rahmen ihres Verantwortungsbereichs oder ihrer Aktivitäten spezifiziert werden können. Für deren Vertreter sind ebensolche Regeln zu definieren und formalisieren.
CAL-12: Verwaltung der Nutzungsprivilegien des Informationssystems	Benutzer besitzen für die Ressourcen des Informationssystems Nutzungsprivilegien, die den ihnen zugewiesenen Profilen entsprechen. Diese Privilegien sind zu verwalten, um sicherzustellen, dass die geltenden Sicherheitsregeln voll und ganz eingehalten werden. Die Kriterien für die Anwendung dieses Prinzips sind klar zu bestimmen. Sie können z. B. aus den folgenden Elementen abgeleitet werden: - den Profilen der Benutzer, deren Privilegien verwaltet werden, - den zwischen den verschiedenen Benutzerprofilen vorhandenen Privilegien, - den Personen, die berechtigt sind, diese Privilegien zu gewähren oder zu ändern, - den Bedingungen, die vor jedweder Änderung oder Gewährung von Privilegien zu erfüllen sind, - den untereinander nicht kompatiblen Benutzerprivilegien. Die Integrität der Privilegientabellen ist vom Systemverantwortlichen und dem Sicherheitsmitarbeiter besonders zu schützen und zu kontrollieren.
CAL-13: Sperren von Arbeitssitzungen	Arbeitsplätze sind die Haupteingänge in das Informationssystem. Die Benutzer müssen dafür sensibilisiert werden, dass sie, wenn sie ihren Arbeitsplatz verlassen, ihr Arbeitsumfeld unzugänglich machen (Sperren der Sitzung, Ausschalten des Arbeitsplatzes). Zur Verstärkung dieser Maßnahmen und um Fahrlässigkeit auszuschließen, werden

	Maßnahmen zum automatischen Schutz einer Arbeitssitzung nach einem bestimmten Inaktivitätszeitraum (automatisches Trennen von Verbindungen, Sperren...) empfohlen.
CAL-14: Schutz des Arbeitsumfelds	Für jedes Benutzerprofil (Administrator, Wartungspersonal, Hauptbenutzer des Arbeitsplatzes, vorübergehender Benutzer) ist eine Aktionsliste zu erstellen und durch Zugriffsrechte zu schützen.

3.3.14 JRN : Journalschreibung

JRN-01: Mittel zur Journalschreibung bei Eindringen und missbräuchlicher Verwendung	Das Informationssystem muss Mittel (Vorrichtungen und/oder Verfahren) zur Journalschreibung bei Eindringen oder missbräuchlicher Verwendung enthalten. Da es nicht immer möglich sein wird, Eindringversuche rechtzeitig zu stoppen, sind im Rahmen der Risikomanagementlogik Mechanismen zur Journalschreibung und Ablaufverfolgung vorzusehen, mit deren Hilfe bei einem erfolgreichen Eindringen oder einem Eindringversuch zur Verfügung gestellt werden können: - Elemente zur Ablaufverfolgung zur bestmöglichen Identifikation der Gründe und Ursprünge des Eindringens (Rückverfolgung des Ablaufs bis hin zu den bedrohenden Elementen), - Elemente zur Ablaufverfolgung, die ausreichend zuverlässig sind, damit diese von einem Richter bei Notwendigkeit im Fall einer Klage als Beweismittel für Eindringen (oder Eindringversuche) oder missbräuchliche Verwendung gewertet werden können. Es sind also Verfahren zur Auswertung von Abläufen und Aufzeichnungen einzurichten - mit den entsprechenden technischen und personellen Mitteln -, um - auch erfolgreiches - Eindringen feststellen und die notwendigen Beweismittel sammeln zu können. Diese Elemente sind ebenfalls erforderlich, wenn man das System in seinen Anfangszustand versetzen will.
JRN-02: Aufzeichnung der Operationen	Die Definition von Regeln zur Aufzeichnung von Abläufen auf Grundlage der gesuchten Elemente ist von entscheidender Bedeutung, wobei bei der Aufzeichnung von Sicherheitsabläufen das Prinzip von Verhältnismäßigkeit und Volumetrie zu beachten ist. Diese Regeln können von Ressourcen, die diese Abläufe sinnvoll nutzen könnten, beeinflusst werden. Für die Definition und Umsetzung von Systemen zur Journalschreibung sind die geltenden Gesetze und Vorschriften zu beachten, insbesondere bei der Verarbeitung von personengebundenen Informationen.
JRN-03: Sicherung von Beweisen	Um vor Gericht die Verwertbarkeit von Beweisen sicherzustellen, sind bei der Sicherung von IT-Beweisen die geltenden Gesetze und Praktiken einzuhalten. Dabei sind insbesondere zu beachten und sicherzustellen: - das Prinzip von Verhältnismäßigkeit und Transparenz,

	- die Zulässigkeit des Beweismittels, - Qualität und Vollständigkeit des Beweismittels, - Schutz der Privatsphäre, - Qualität der Herstellung von Beweismitteln und ihrer Lagerung bis zur Vorlage.
JRN-04: Management der Ablaufverfolgung	Das Management der Sicherheits-Ablaufverfolgung beinhaltet mehrere Aufgaben, die zu definieren und zu organisieren sind: - gesicherte Fernerfassung von Sicherheitsablaufaufzeichnungen, - Archivierung der Ablaufaufzeichnungen, - Löschen veralteter Ablaufaufzeichnungen aus den Dateien (wobei festzulegen ist, ab wann Daten veraltet und wie lange sie zu archivieren sind), - Filtrierung und Analyse der Ablaufaufzeichnungen, - Schutz der Ablaufaufzeichnungen vor Beeinträchtigung oder nicht erlaubtem Zugriff, - Warnung bei Feststellung eines wichtigen Ereignisses, - Kontrolle der Integrität der Mechanismen zur Ablaufaufzeichnung, - Verfahren zur Auswertung der Ablaufaufzeichnungen bei Separierung von Ablaufaufzeichnungen im o. g. Sinne und Ablaufaufzeichnungen zur Tätigkeit des Netzwerkadministrators, - Vernichtung von Ablaufaufzeichnungen nach Ablauf der gesetzlichen Frist.
JRN-05: Sicherheitswarnung	Es ist von der Schwere eines Sicherheitszwischenfalls abhängig, welche Maßnahmen nach dessen Feststellung zu treffen sind. So können die Methode zur Übermittlung der Warnung, die Übermittlungsgeschwindigkeit und die Art der Reaktion davon abhängen, als wie schwerwiegend der Zwischenfall eingestuft wird (vgl. Management von Zwischenfällen und Krisenmanagement). Im allgemeinen ist der Ablauf aller relevanten Sicherheitszwischenfälle aufzuzeichnen und muss auswertbar sein (Identifikation des Verursachers, von Datum, Art der Operation, Ziel...). Die Regeln für Journalschreibung und Analyse eines Zwischenfalls sind von der Einstufung des Sicherheitszwischenfalls abhängig.
JRN-06: Analyse der Aufzeichnungen Sicherheitskontrolldaten	Der gesicherte Betrieb eines Informationssystems impliziert, dass Daten zur Kontrolle der Sicherheit in einem Auditjournal aufgezeichnet werden, um überprüfen zu können, dass Sicherheit gewährleistet ist, vor allem im Hinblick auf den Zugriff auf das Informationssystem, unabhängig davon, ob dieser durch Benutzer, Techniker oder Informatiker erfolgt. Die Analyse dieser Kontrolldaten ist ein nachgelagertes Überprüfungsinstrument, kann aber auch gescheiterte Eindringversuche in das System aufdecken, oder, was verdeckter wäre, Vorbereitungen zu einem Angriff durch Einzug von Dateien oder verfallener Konten. Diese

Prüfung liefert mehr Informationen als eine direkte Kontrolle, sofern sie regelmäßig und sorgfältig durchgeführt wird.

Eine wesentliche Bedingung, um der Analyse dieser Aufzeichnungen vertrauen zu können, ist der wirksame Schutz der Mechanismen, mit denen die Kontrolldaten aufgezeichnet werden, da jeder Eindringling zunächst versuchen wird, derartige Aufzeichnungsmechanismen zu behindern, um Spuren seines Handelns zu verwischen.

Die Umsetzung von Auditjournalen kann auch in Zeiten starken Betriebs erforderlich sein, wobei man sich dabei über das Risiko für die Sicherheit bewusst sein muss, das deren Deaktivierung mit sich bringt, was sich insbesondere auf das juristische Risiko bezieht, das die Organisation eingeht, wenn sie bei einem Angriff als Rebound-Plattform dienen.

3.3.15 IGC : Infrastrukturen für das Chiffrierschlüssel-Management

IGC-01: Chiffrierschlüsselmanagementpolitik

Der Einsatz von Chiffrierschlüsseln im Rahmen einer Chiffrierschlüsselmanagementinfrastruktur macht die Umsetzung, Kontrolle und Aufrechterhaltung einer Chiffrierschlüsselmanagementpolitik erforderlich.

Diese wird im allgemeinen in Form einer Zertifizierungspolitik und einer Anzeige von Zertifizierungsverfahren, die die Anforderung an das Chiffrierschlüsselmanagement formalisieren, umgesetzt. Inhalt beider Maßnahmen ist vor allem die Bearbeitung von Lebensdauer und Austausch dieser Schlüssel.

Struktur und Inhalt dieser Dokumente sollten vorzugsweise internationale Normen (wie z. B. RFC 2527) einhalten.Hinweis: Die Erarbeitung einer Zertifizierungspolitik wird durch die vorherige Durchführung einer SIS-Risikoanalyse und das Studium anderer Zertifizierungspolitiken zu gleichen Bedürfnisarten (Server- und Personenauthentisierung, Unterschrift, Chiffrierung...) wesentlich erleichtert.

IGC-02: Schutz geheimer oder privater Schlüssel

Ob für eine Chiffrierung aus Gründen der Vertraulichkeit, zur Authentisierung oder Unterschriftsleistung - die Benutzer werden geheime oder private Schlüssel verwenden müssen. Die Sicherung von Integrität und Nicht-Preisgabe ist für die Solidität des Systems von seinem Wesen her absolut fundamental. Dieser Frage ist besondere Aufmerksamkeit zu widmen, um für jeden Einzelfall sicherzustellen, dass Auswahl und Mittel mit den Ansprüchen an den Einsatz dieser Schlüssel übereinstimmen. So kann für Dokumente, die als sensibel eingestuft wurden, gefordert werden, dass jede Chiffrierung mit einer Vorrichtung vorgenommen wird, die garantiert, dass der private Schlüssel gesichert und in einer Hardwarevorrichtung (z. B. kryptografische Chipkarte) verwendet wird, wobei für andere Einsätze auch eine Softwarelösung akzeptabel wäre.

IGC-03: Zertifizierung öffentlicher Schlüssel	Systeme mit asymmetrischer Kryptografie bergen ein Risiko der Usurpation des öffentlichen Schlüssels. Die Sicherheit des Systems beruht auf der Zuverlässigkeit der Chiffrierschlüsselmanagementinfrastruktur und dabei vor allem auf dem Zertifizierungsprozess, bei dem ein Element (Person, Server) einem öffentlichen Schlüssel zuordnet wird. Dieser Aspekt muss beherrscht werden. Dazu ist eine Zertifizierungspolitik zu verfassen.

3.3.16 SCP : Störsignale

SCP-01: Zoneneinteilung	Ein Mittel, um sich vor Störsignalen zu schützen, ist die Zoneneinteilung. Diese beinhaltet zwei Möglichkeiten: - die Einteilung von Räumlichkeiten in Zonen in Übereinstimmung mit Richtlinie 495 vom 19. September 1997, - die Einteilung von Ausrüstungen in Zonen in Übereinstimmung mit Leitfaden 430 vom 1. Juni 1999. Die Installation der Ausrüstungen hat unter Berücksichtigung der Ergebnisse der Zoneneinteilung in Übereinstimmung mit Richtlinie 485 vom 1. September 2000 zu erfolgen.
SCP-02: TEMPEST-Hardware	Ein Mittel, um sich vor Störsignalen zu schützen, ist der Einsatz von TEMPEST-Hardware (Transient ElectroMagnetic Pulse Emanations Standard). Diese Hardware, für deren Entwicklung besondere Maßnahmen gelten, um die Aussendung und Leitung von Störsignalen zu reduzieren, wird in vier Kategorien eingeteilt: - A (entspricht der Norm AMSG 720), - B (entspricht der Norm AMSG 788), - C (entspricht der Norm AMSG 784), - D (entspricht keiner der o. g Normen). Diese Hardware ist in Übereinstimmung mit Richtlinie 485 vom 1. September 2000 zu installieren. Diese Lösung ist ins Auge zu fassen, wenn die Bedürfnisse durch Zoneneinteilung nicht befriedigt werden können.
SCP-03: Faradaysche Käfige	Ein - allerdings kostspieligers - Mittel, um sich vor Störsignalen zu schützen, ist der Einsatz von Faradayschen Käfigen oder die Faradisation von Räumlichkeiten.
SCP-04: Willentliche Störsignale	Drahtlose Übertragungssysteme sind, wenn sie zur Übertragung von Informationen eingesetzt werden, potentielle Störsignalsender. Diese Signale werden als ,,willentliche Störsignale" bezeichnet und betreffen alle Drahtlossysteme wie Infrarot-, Funkfrequenz-, optische Systeme usw. Um sich vor der Abstrahlung willentlicher Störsignale zu schützen, sind die

Empfehlungen der DCSSI anzuwenden. In den meisten Fällen kann auf Chiffrierung und/oder eine Zoneneinteilung von Ausrüstungen und Räumlichkeiten zurückgegriffen werden.

Andererseits muss man sich des mit dem Einsatz derartiger Informationsübertragungsmittel verbundenen Risikos bewusst sein.

3.4 Sonstige Anforderungen

3.4.1 CCS : Sicherheitsanweisung

CCS_SIN: Anweisungen im Schadensfall	
CCS_SIN.1.1	Die Sicherheitsanweisungen im Schadensfall müssen klar und deutlich unter Berücksichtigung der gebräuchlichen Normen und Standards abgefasst werden
CCS_SIN.1.2	Die Sicherheitsanweisungen im Schadensfall müssen in Augenhöhe in frei zugänglichen Bereichen unter Berücksichtigung der gebräuchlichen Normen und Standards ausgehängt werden
CCS_SIN.1.3	Die Sicherheitsanweisungen im Schadensfall müssen an verschiedenen Orten des Standorts und vornehmlich an Orten mit Publikumsverkehr und an den von den Anweisungen betroffenen Orten ausgehängt werden (Aufzüge, Einrichtungen mit Gefahr von Wasserschäden usw.)
CCS_SIN.1.4	Die Sicherheitsanweisungen im Schadensfall müssen auf Unterlagen gedruckt werden, die den Blick anziehen
CCS_SIN.2.1	Die Prozedur zur Benachrichtigung der Rettungsdienste (Feuerwehr, Notarzt, Polizei usw.) muss ausdrücklich in den Sicherheitsanweisungen im Schadensfall vermerkt werden
CCS_SIN.2.2	Die Prozedur zur Räumung des Standorts (Fluchtwege, Sammelplatz) muss ausdrücklich in den Sicherheitsanweisungen für Schadensfälle mit Räumungspflicht vermerkt werden (Brand, Verschmutzung größeren Ausmaßes, Attentat usw.)
CCS_SIN.2.3	Die Sicherheitsanweisungen müssen Aufschluss über die angemessenen zu treffenden Maßnahmen geben (was ist bei Rauchentwicklung zu tun, Erste-Hilfe-Maßnahmen für Starkstromverletzte, Sofortmaßnahmen bei Wasserschäden, Maßnahmen zum Schutz der Systemausstattung bei Schadensfällen usw.)
CCS_SIN.3.1	Die Sicherheitsanweisungen im Schadensfall müssen regelmäßig überprüft werden, damit sie immer auf neuestem Stand sind (die Abstände der Überprüfungen bleiben zu definieren, dürfen aber keinesfalls 2 Jahre überschreiten)
CCS_SIN.3.2	Der Verantwortliche für die Überprüfung der Sicherheitsanweisungen im Schadensfall muss eindeutig identifiziert sein
CCS_SIN.3.3	Die Sicherheitsanweisungen im Schadensfall müssen regelmäßig von den betroffenen Rettungsdiensten validiert werden (Feuerwehr, Notarzt usw.)
CCS_SIN.3.4	Jede Aktualisierung der Sicherheitsanweisungen im Schadensfall muss Anlass zu einer Mitteilung an das gesamte Personal des Standorts geben
CCS_SIN.3.5	In regelmäßigen Abständen (die Abstände bleiben zu definieren, dürfen aber keinesfalls 2 Jahre überschreiten) sind Aktionen zur Sensibilisierung für die Sicherheitsanweisungen und ggf. praktische Übungen zu organisieren (Tests, Räumungsübungen, Schadensfallsimulationen usw.)
CCS_CSP: Vorbeugende Sicherheitsanweisungen	
CCS_CSP.1.1	Die vorbeugenden Sicherheitsanweisungen (z. B. Rauchverbot in der Nähe entzündbarer Materialien) müssen klar und deutlich abgefasst werden
CCS_CSP.1.2	Die vorbeugenden Sicherheitsanweisungen müssen in Augenhöhe in frei zugänglichen Bereichen ausgehängt werden.
CCS_CSP.1.3	Die vorbeugenden Sicherheitsanweisungen müssen an den von den Anweisungen betroffenen Orten ausgehängt werden
CCS_CSP.1.4	Die vorbeugenden Sicherheitsanweisungen müssen auf Unterlagen gedruckt werden, die den Blick anziehen
CCS_CSP.2.1	Die vorbeugenden Sicherheitsanweisungen müssen auf Unterlagen gedruckt werden, die den Blick anziehen (die Abstände der Überprüfungen bleiben zu definieren, dürfen aber keinesfalls 2 Jahre überschreiten)

CCS_CSP.2.2	Der Verantwortliche für die Überprüfung der vorbeugenden Sicherheitsanweisungen muss eindeutig identifiziert sein
CCS_CSP.2.3	Jede Aktualisierung der vorbeugenden Sicherheitsanweisungen muss Anlass zu einer Mitteilung an das gesamte Personal des Standorts geben
CCS_CSP.2.4	Externe Personen müssen über die vorbeugenden Sicherheitsanweisungen durch ihren jeweiligen Ansprechpartner informiert werden
CCS_SSE: Sicherheitsanweisungen für die wesentlichen Dienste	
CCS_SSE.1.1	Die Sicherheitsanweisungen für die wesentlichen Dienste müssen klar und deutlich abgefasst werden
CCS_SSE.1.2	Die Sicherheitsanweisungen für die wesentlichen Dienste müssen vorbeugende Maßnahmen unterbreiten, um den Verlust von wesentlichen Diensten zu vermeiden (z. B. Anschluss der Stationen an Wellenstrom)
CCS_SSE.1.3	Die Sicherheitsanweisungen für die wesentlichen Dienste müssen Alarmprozeduren bei Zwischenfällen unterbreiten (z. B. zu benachrichtigende Person bei Unterbrechung der Telefonleitung)
CCS_SSE.1.4	Die Sicherheitsanweisungen für die wesentlichen Dienste müssen Reaktionsmaßnahmen bei Zwischenfällen unterbreiten (z. B. Einrichten einer Ersatz-Klimaanlage)
CCS_SSE.1.5	Die Sicherheitsanweisungen für die wesentlichen Dienste müssen regelmäßig überprüft werden, damit sie immer auf neuestem Stand sind
CCS_SSE.1.6	Der Verantwortliche für die Überprüfung der Sicherheitsanweisungen für die wesentlichen Dienste muss eindeutig identifiziert sein
CCS_SSE.1.7	Jede Aktualisierung der Sicherheitsanweisungen für die wesentlichen Dienste muss Anlass zu einer Mitteilung an das gesamte Personal des Standorts geben
CCS_CSG: Allgemeine Sicherheitsanweisungen	
CCS_CSG.1.1	Es müssen Sicherheitsanweisungen zur korrekten Benutzung von Betriebsmitteln und Datenträgern erstellt und an alle potentiellen Benutzer verteilt werden
CCS_CSG.1.2	Die Sicherheitsanweisungen zur korrekten Benutzung müssen Praktiken aufzeigen, die es zu vermeiden gilt (Kein Rauchen, Essen oder Trinken in der Nähe von Betriebsmitteln, Sensibilisierung für die Sättigung von Speicherplätzen oder Datenverarbeitungsressourcen)
CCS_CSG.1.3	Die Sicherheitsanweisungen zur korrekten Benutzung müssen Aufschluss über die anzuwendenden vorbeugenden Maßnahmen geben (Schutz beim Transport, Lagerbedingungen usw.)
CCS_CSG.1.4	Die Sicherheitsanweisungen zur korrekten Benutzung müssen Aufschluss über die anzuwendenden vorbeugenden Maßnahmen geben (Schutz beim Transport, Lagerbedingungen usw.)
CCS_CSG.1.5	Die Sicherheitsanweisungen zur korrekten Benutzung müssen regelmäßig überprüft werden, damit sie immer auf neuestem Stand sind
CCS_CSG.1.6	Der Verantwortliche für die Überprüfung der Sicherheitsanweisungen zur korrekten Benutzung muss eindeutig identifiziert sein
CCS_CSG.1.7	Jede Aktualisierung der Sicherheitsanweisungen für die korrekte Benutzung muss Anlass zu einer Mitteilung an das gesamte Personal des Standorts geben
CCS_CHI: Informatik-Charta	
CCS_CHI.1.1	Die Benutzer des Informationssystems (sowohl interne als auch externe Benutzer) müssen sich durch Unterzeichnen einer Informatik-Charta bereit erklären, die Benutzungsanweisungen einzuhalten. Dabei stützt sich diese Charta auf die Sicherheitsanweisungen für die korrekte Benutzung
CCS_SRI: Sicherheit innerhalb der Betriebsordnung	
CCS_SRI.1.1	Die Verantwortungen bezüglich der Sicherheit des Informationssystems sind in der Betriebsordnung in Erinnerung zu rufen
CCS_RGI: Allgemeine Installationsvorschriften	
CCS_RGI.1.1	Zur Installation der Betriebsmittel sind allgemeine Vorschriften auszuarbeiten, die

	sich auf die Herstellerempfehlungen und identifizierten Sicherheitsbedürfnisse stützen

3.4.2 CRR : Restrisiken

CRR_ETU: Studien der Restrisiken	
CRR_ETU.1.1	Zur Feststellung der abgedeckten Risiken, der noch abzudeckenden Risiken und der verbleibenden Restrisiken muss eine Risikostudie durchgeführt und in regelmäßigen Abständen aktualisiert werden
CRR_ETU.1.2	Die identifizierten Restrisiken müssen auf ihre Durchführbarkeit / Wahrscheinlichkeit und ihre Auswirkung hin untersucht werden (finanzielle, tätigkeitsspezifische, organisatorische, personalbedingte Auswirkungen)
CRR_ETU.2.1	Für jedes Restrisiko muss ein Aktionsplan erstellt werden, um direkte Auswirkungen so weit wie möglich einzuschränken und indirekte Auswirkungen und Seiteneffekte bei Konkretisierung des Risikos bestmöglich zu vermeiden
CRR_ETU.2.2	So weit wie möglich (Vorhandensein eines angepassten Versicherungsvertrags, kontrollierte Versicherungsprämien usw.) müssen die Restrisiken durch angepasste Versicherungen abgedeckt werden
CRR_SEN: Sensibilisierung für die Restrisiken	
CRR_SEN.1.1	Das Personal der Organisation muss für die Restrisiken und die ergriffenen Maßnahmen zur Einschränkung ihrer Wahrscheinlichkeit / Durchführbarkeit und ihrer Auswirkung sensibilisiert werden
CRR_SEN.1.2	Das Personal der Organisation muss in den Aktionsplänen im Falle einer Konkretisierung eines Restrisikos geschult werden

3.4.3 CIS : Einrichten von Standorten

CIS_PSI: Kapitel über die physische Sicherheit (PSI)	
CIS_PSI.1.1	Die Sicherheitspolitik muss ein Kapitel über die physische Sicherheit von Standorten beinhalten
CIS_PSI.1.2	Das Kapitel der Sicherheitspolitik über die physische Sicherheit von Standorten muss die Normen zum Einrichten von Standorten benennen
CIS_PSI.1.3	Die Normen zum Einrichten von Standorten müssen Maßnahmen zum Schutz und zur Einschränkung von Auswirkungen im Schadensfall enthalten
CIS_CSI: Anweisungen zum Einrichten von Standorten	
CIS_CSI.1.1	Die Normen zum Einrichten von Standorten müssen auf den geltenden nationalen und/oder internationalen Normen und Standards zum Schutz gegen Schadensfälle aufbauen (Brand, Unfall, usw.)
CIS_CSI.1.2	Die Normen zum Einrichten von Standorten müssen eine Nomenklatur der physischen Zoneneinteilung zur Einschränkung von Auswirkungen im Schadensfall definieren. (z. B. Zonenisolierung durch Brandschutztüren)
CIS_CSI.1.3	Die Entsprechung der Normen zum Einrichten von Standorten mit den geltenden nationalen und/oder internationalen Normen zum Schutz gegen Schadensfälle muss regelmäßig von den Rettungsdiensten validiert werden (Feuerwehr, Notarzt usw.)
CIS_CSI.2.1	Die Räumlichkeiten (und insbesondere die veralteter Standorte) müssen regelmäßig auf ihre Konformität hin auditiert werden, um sicherzugehen, dass sie immer noch den Normen und Standards zum Einrichten von Standorten entsprechen
CIS_CSI.2.2	Die Verantwortlichen für die Evaluierung von Standorten sowie deren Vertreter müssen eindeutig identifiziert sein
CIS_CSI.2.3	Die Verantwortlichen für die Evaluierung von Standorten sowie deren Vertreter müssen für den Schutz von Standorten sensibilisiert und hinsichtlich der Normen und Standards zum Einrichten von Standorten geschult werden
CIS_CSI.2.4	Die Audits über die Konformität von Standorten müssen Anlass zur Abfassung

	eines umfassenden Abschlussberichts geben, der an die Direktion weiterzuleiten ist
CIS_CSI.2.5	Die Abschlussberichte der Audits über die Konformität von Standorten müssen genauso wie die anderen sicherheitsrelevanten Protokolldaten des Informationssystems aufbewahrt, ausgewertet und verwaltet werden
CIS_CDL: Konstruktion der Räumlichkeiten	
CIS_CDL.1.1	Bei der Konstruktion und Ausstattung der Räumlichkeiten müssen unausweichliche größere Risiken berücksichtigt werden (Unwetter, Orkane, Erdbeben, usw.)
CIS_ADL: Ausstattung der Räumlichkeiten	
CIS_ADL.1.1	Bei Gegenüber müssen die Scheiben der Räumlichkeiten getönt werden
CIS_ADL.1.2	Zur Straße zeigende Fenster dürfen keinen leichten Zugang zu den Räumlichkeiten bieten (Gitterstäbe, verstärkte Scheiben, Fenster nicht ganz zu öffnen, Alarm bei offen gelassenem Fenster außerhalb der Bürozeiten des Standorts usw.)
CIS_ADL.2.1	Bei der Innenausstattung müssen alle vorgesehenen Einrichtungselemente berücksichtigt werden (Temperaturkontrolle, Überwachung der Luftfeuchtigkeit, Filterung von Staub und sonstigen verschmutzenden Elementen usw.)
CIS_ADL.2.2	Die Betriebsmittel müssen so weit entfernt wie möglich von eventuellen Schadensquellen aufgestellt werden (Wasserleitungen, Quellen elektromagnetischer oder thermischer Strahlung usw.)
CIS_ADL.2.3	Die technischen Plattformen müssen genug Platz bieten, um eine übersichtliche Organisation der Ausstattung zu ermöglichen und den Betrieb der einzelnen Betriebsmittel nicht zu stören
CIS_ADL.3.1	Die Standardausrüstung (Netzkabel, Wasserabsperrventile, Sicherungen usw.) muss so gekennzeichnet sein, dass ihre Lokalisierung und ihre Aufgabe bekannt sind
CIS_SSI: Auswahl zur Implementierung des Standorts	
CIS_SSI.1.1	Die Nähe zu Rettungsdiensten ist bei der Auswahl zur Implementierung des Standorts ein wichtiges Kriterium
CIS_SSI.1.2	Bei der Auswahl zur Implementierung eines Standorts müssen die dem Implementierungsstandort innewohnenden Risiken berücksichtigt werden (Überschwemmungsgebiet, Nähe zu einem als riskant eingestuften Industriestandort, Verschmutzung usw.)
CIS_SSI.1.3	Bei der Auswahl zur Implementierung eines Standorts müssen die Möglichkeiten einer Zerstörung durch ein externes Ereignis berücksichtigt werden (Kollisionen, Attentate)
CIS_SSI.1.4	Bei der Auswahl zur Implementierung eines Standorts müssen die Risiken einer eingeschränkten Verfügbarkeit des Personals berücksichtigt werden (verkehrsmäßig kaum erschlossenes Gebiet, leicht zu blockierender Standort usw.)
CIS_MPP: Schutzmaßnahmen	
CIS_MPP.1.1	Die Versorgungseinrichtungen der wesentlichen Dienste müssen mit gekennzeichneten und zugänglichen Abschaltvorrichtungen (darunter ein Hauptschalter) ausgestattet sein
CIS_MPP.1.2	Die Abschaltvorrichtungen der Versorgungseinrichtungen der wesentlichen Dienste sowie alle sonstigen Elemente, die eine Unterbrechung der wesentlichen Dienste bewirken können, müssen gegen den Zugang durch Unbefugte geschützt werden
CIS_MPP.1.3	Die Elemente, die eine Unterbrechung der wesentlichen Dienste bewirken können, müssen soweit wie möglich am Standort untergebracht werden
CIS_MPP.2.1	Die Räumlichkeiten müssen mit Feuererkennungs- und Brandschutzeinrichtungen ausgerüstet werden
CIS_MPP.2.2	Die Feuererkennungs- und Brandschutzeinrichtungen müssen den Standorten

	und Implementierungszonen angepasst und entsprechend dimensioniert sein
CIS_MPP.3.1	Standorte, die eventuell bedeutende Wasserschäden zu erleiden haben, müssen mit entsprechenden Evakuationseinrichtungen ausgestattet werden (Abfallschächte, Pumpen usw.)
CIS_MPP.3.2	Gegen Wasserschäden äußerst empfindliche Zonen (elektrische Geräte, Papierarchive usw.) müssen mit angemessenen Detektoren ausgestattet werden
CIS_MPP.3.3	Kontaktflächen nach außen (Decken, Fenster u. ä.) müssen wasserbeständig sein und ihre Dichtheit muss regelmäßig überprüft werden
CIS_MPP.3.4	Spezifische Schutzvorrichtungen gegen den Wasserspiegelanstieg müssen für Standorte in Überschwemmungsgebieten vorgesehen werden
CIS_ZOS: Sicherheitszonen	
CIS_ZOS.1.1	Die Institutionen müssen zum Schutz von Zonen mit Einrichtungen zur Produktion bzw. zur Erbringung wesentlicher Dienste Schutzperimeter einrichten

3.4.4 CRI : Beziehungen zwischen den einzelnen Standorten

CRI_MOF: Kontrolle der Tochterorganisationen	
CRI_MOF.1.1	Alle Standorte einer Institution müssen sich verpflichten, die Anweisungen der Sicherheitspolitik einzuhalten
CRI_MOF.2.1	Bedeutende Änderungen an einem institutionseigenen Standort müssen Anlass zur Abfassung eines Installationsberichts geben, der an den Sicherheitsbeauftragten der Institution zu richten ist (erstmalige Einrichtung des Standorts, Änderung des Netzanschlusses usw.)

3.4.5 CET : Betreuung Dritter

CET_EGT: Allgemeine Betreuung Dritter	
CET_EGT.1.1	Externe Personen dürfen den Standort nicht betreten bzw. verlassen können, ohne sich am Empfang gemeldet zu haben
CET_EGT.1.10	Empfangsbescheinigungen oder Lieferscheine für Betriebsmittel oder Datenträger müssen beim Verlassen der betroffenen Drittperson durch den internen Ansprechpartner persönlich dem Empfang abgegeben werden
CET_EGT.1.2	Soweit wie möglich muss jeder Besuch Dritter angekündigt sein, und das Empfangspersonal muss über eine Liste verfügen, auf der die Namen aller Besucher des Tages mit voraussichtlicher Ankunftszeit und betroffenem internen Ansprechpartner verzeichnet sind
CET_EGT.1.3	Jeder Besuch muss bei Ankunft durch Vorlage eines amtlichen Ausweises authentifiziert werden; im Gegenzug zum Hinterlassen des Ausweises muss ein Besucherausweis ausgehändigt werden
CET_EGT.1.4	Bei vorgesehenem Besuch muss der Name jeden Besuchers mit der Besucherliste des jeweiligen Tages validiert werden. Nicht auf der Liste vermerkte Namen müssen hinzugefügt werden
CET_EGT.1.5	Für jeden Besucher muss die Zu- und Abgangszeit notiert werden
CET_EGT.1.6	Name, Zu- und Abgangszeit und Name des internen Ansprechpartners eines jeden Besuchers müssen genauso wie die anderen sicherheitsrelevanten Protokolldaten des Informationssystems aufbewahrt, ausgewertet und verwaltet werden
CET_EGT.1.7	Jedem Besucher, dessen Besuch nicht vorgesehen war, ist ein interner Ansprechpartner zuzuweisen, und der Besucher erhält solange keinen Zugang zu den Räumlichkeiten, bis er nicht in Begleitung seines internen Ansprechpartners ist
CET_EGT.1.8	Bringt ein Dritter Material oder Unterlagen in die Räumlichkeiten mit, muss das Material genau aufgelistet werden, die Liste ist zusammen mit dem Ausweis des Dritten aufzubewahren und das Material ist, soweit möglich, als externes Material zu kennzeichnen

CET_EGT.1.9	Ein Dritter, der Material oder Unterlagen mitgebracht hat, muss die Räumlichkeiten mit dem gleichen Material wieder verlassen oder pro weiteres bzw. fehlendes Stück eine unterzeichnete Bescheinigung vorlegen
CET_EGT.2.1	Der interne Ansprechpartner eines Besuchers muss sofort bei Ankunft des Besuchers kontaktiert werden
CET_EGT.2.2	Der interne Ansprechpartner eines Besuchers muss den Besucher ab dem Empfang betreuen
CET_EGT.2.3	Ab Übernahme der Betreuung ist der interne Ansprechpartner bis zu dessen Abreise für den Besucher verantwortlich. Er muss insbesondere sicherstellen, dass der Besuch in Einklang mit den in der Sicherheitspolitik definierten Sicherheitsgrundsätzen abläuft
CET_EGT.3.1	Zugänge zu einem Standort oder einer Zone mit besonderen Sicherheitsbedürfnissen erfordern eine Validierung der Ermächtigung der Besucher
CET_EGT.3.2	Bei einem externen Besucher muss der interne Verantwortliche des Besuchers entsprechend ermächtigt sein
CET_EGT.3.3	Bei Zugang eines institutionsinternen Mitarbeiters muss dessen Ermächtigung am Empfang des Standorts oder der Zone überprüft werden
CET_EGT.3.4	Die Validierung der Ermächtigungen kann durch eine manuelle Befragung der Ermächtigungsdatenbank nach erfolgter Authentifizierung durch Vorlage eines amtlichen Ausweises oder durch eine automatische Authentifizierungslösung erfolgen (z. B. auf Basis persönlicher Ausweise)
CET_EGT.3.5	Im Falle einer automatischen Überprüfung der Ermächtigungen müssen die Identifikationsdaten sowie Datum und Uhrzeit des Zugangs genauso wie die anderen sicherheitsrelevanten Protokolldaten des Informationssystems aufbewahrt, ausgewertet und verwaltet werden
CET_EIP: Betreuung punktueller Intervenienten	
CET_EIP.1.1	Jeder Intervenient am Informationssystem muss vor Beginn des Eingriffs über die Sicherheitsanweisungen informiert werden
CET_EIP.1.2	Der interne Ansprechpartner eines Intervenienten ist für alle Aktionen dieses Intervenienten während der gesamten Eingriffsdauer verantwortlich (technischer Eingriff, Einhalten der Anweisungen und der Sicherheitspolitik, v. a. was den Schutz der Informationen anbelangt)
CET_EIP.1.3	Ein Eingriff ist durch eine Eingriffsabnahme zu beenden, dank der die durchgeführten Operationen und die erzielten Ergebnisse überprüft werden können
CET_EIP.1.4	Im Eingriffsabnahmebericht müssen der Name des Intervenienten, dessen Firma, Tag und Uhrzeiten des Eingriffs, die durchgeführten Operationen, die erzielten Ergebnisse, eventuell aufgetretene Probleme und der Name des internen Ansprechpartners vermerkt werden
CET_EIP.1.5	Der Eingriffsabnahmebericht muss von dem oder den Intervenienten, vom internen Ansprechpartner und vom Verantwortlichen der Eingriffsabnahme unterzeichnet werden, sofern dieser nicht zugleich der interne Ansprechpartner ist
CET_EIP.1.6	Die Eingriffsabnahmeberichte müssen genauso wie die anderen sicherheitsrelevanten Protokolldaten des Informationssystems aufbewahrt, ausgewertet und verwaltet werden
CET_PLD: Betreuung bei Langzeitleistungen am Standort	
CET_PLD.1.1	Nach Beendigung der anfänglichen Empfangsprozedur muss ein Vor-Ort-Leistungserbringer wie eine Zeitarbeitskraft der Organisation behandelt werden können (Zugangsausweis, Zugriffsrechte auf das Informationssystem gemäß den zur Erbringung der Dienstleistung erforderlichen Bedürfnissen
CET_PLD.1.2	Alle einem Vor-Ort-Leistungserbringer im Rahmen seiner Mission ausgehändigten Elemente (Zugangsausweis, Benutzeridentifikation und Passwort zum Einloggen u. ä.) müssen in einer Liste über die dem

	Leistungserbringer ausgehändigten Elemente unter Angabe des Aushändigungsdatums identifiziert und registriert werden
CET_PLD.1.3	Die Liste über die dem Leistungserbringer ausgehändigten Elemente muss genauso wie die anderen sicherheitsrelevanten Protokolldaten des Informationssystems aufbewahrt, ausgewertet und verwaltet werden
CET_PLD.1.4	Jedem Vor-Ort-Leistungserbringer müssen vor Beginn der Leistungserbringung die Sicherheitsanweisungen und die Sicherheitspolitik ausgehändigt werden
CET_PLD.1.5	Vor Beginn der Leistungserbringung muss sich der Vor-Ort-Leistungserbringer verpflichten, die Sicherheitsanweisungen und die Vorschriften der Sicherheitspolitik einzuhalten
CET_PLD.1.6	Vor Beginn der Leistungserbringung muss der Vor-Ort-Leistungserbringer eine offizielle Vertraulichkeitsverpflichtung unterzeichnen
CET_PLD.2.1	Nach beendeter Leistungserbringung muss der Vor-Ort-Leistungserbringer alle physischen Elemente (z. B. den Zugangsausweis), die ihm im Rahmen seiner Mission ausgehändigt wurden, zurückgeben
CET_PLD.2.2	Die Zurückgabe der an einen Vor-Ort-Leistungserbringer ausgehändigten Elemente muss Anlass zur Abfassung eines datierten und vom Leistungserbringer und einem Organisationsverantwortlichen unterzeichneten Rückgabeberichts geben
CET_PLD.2.3	Nach beendeter Leistungserbringung vor Ort müssen alle logischen Elemente (z. B. Benutzeridentifikation und Passwort zum Einloggen), die dem Leistungserbringer im Rahmen seiner Mission zugewiesen wurden, deaktiviert oder vernichtet werden
CET_PLD.2.4	Die Deaktivierung oder Vernichtung logischer Elemente, die einem Leistungserbringer im Rahmen seiner Mission zugewiesen wurden, müssen Anlass zur Abfassung eines datierten und vom Organisationsverantwortlichen unterzeichneten Deaktivierungs- bzw. Vernichtungsberichts geben
CET_PLD.2.5	Die Abschlussbereichte am Ende einer Leistungserbringung müssen genauso wie die anderen sicherheitsrelevanten Protokolldaten des Informationssystems aufbewahrt, ausgewertet und verwaltet werden

3.4.6 CAR : Netzadministration

CAR_PAR: Schutz der Netzadministration	
CAR_PAR.1.1	Die Administrationsprogramme müssen Dienstverweigerungen (denial of service) gegenüber unempfindlich sein
CAR_AAR: Zuweisung der Netzadministration	
CAR_AAR.1.1	Die Rechneradministration muss es möglich machen, exzessiven Verbrauch von Ressourcen zu erkennen

3.4.7 CGS : Sicherheitsmanagement

CGS_GMP: Verwaltung der Passwörter	
CGS_GMP.1.1	Die Passwortpolitik muss einen regelmäßigen Wechsel vorschreiben
CGS_GMP.1.2	Die Passwörter sind vor fremden Blicken geschützt einzugeben
CGS_GMP.1.3	Die Benutzer müssen bei Auswahl und Benutzung ihrer Passwörter für ein sicherheitsgerechtes Verhalten sensibilisiert werden
CGS_SVG: Speichern	
CGS_SVG.1.1	Die Sicherheitspolitik muss eine Speicherungspolitik enthalten
CGS_SVG.1.2	Sämtliche elektronische Unterlagen müssen von der Speicherungspolitik berücksichtigt werden
CGS_SVG.1.3	Zu speichernde Daten müssen in spezifischen Speicherprozeduren identifiziert werden
CGS_SVG.1.4	Die Speicherprozeduren müssen Aufschluss über die Speichermodalitäten, die

	zu benutzenden Datenträger, die Häufigkeit der Abspeicherungen und die Prozeduren zur Verwaltung leerer und mit Speicherdaten gefüllter Datenträger geben
CGS_SVG.1.5	Die Verantwortlichen für jede Speicheroperation sowie deren Vertreter müssen eindeutig identifiziert sein
CGS_SVG.1.6	Die Verantwortlichen für die Abspeicherung sowie deren Vertreter müssen in den Techniken des Speicherns geschult sein
CGS_SVG.1.7	Die Speicherungspolitik muss regelmäßig überprüft werden, damit sie den Weiterentwicklungen des Informationssystems angepasst werden kann; die Berücksichtigung alter Speicherungen muss bewahrt werden
CGS_SVG.1.8	Die Verantwortlichen für die Überprüfung der Speicherprozeduren müssen eindeutig identifiziert sein
CGS_SVG.1.9	Jede Änderung einer Speicherprozedur muss den betroffenen Verantwortlichen für die Abspeicherung sowie deren Vertretern mitgeteilt werden
CGS_SVG.2.1	Die Abspeicherungen müssen das gleiche Schutzniveau zugebilligt bekommen wie die gespeicherten Daten
CGS_ARC: Archivierung	
CGS_ARC.1.1	Alle zu archivierenden Daten müssen Anlass zu einer Äußerung der Bedürfnisse bezüglich der Aufbewahrungsdauer und der Zuverlässigkeit der Datenträger geben
CGS_ARC.1.2	Die Maßnahmen zur Aufbewahrung zu archivierender Daten müssen den geäußerten Bedürfnissen zur Archivierung der betroffenen Daten entsprechen
CGS_ARC.1.3	Zu archivierende Daten müssen in spezifischen Archivierprozeduren identifiziert werden
CGS_ARC.1.4	Die Archivierprozeduren müssen Aufschluss über die Modalitäten zur Datenarchivierung, die zu benutzenden Datenträger, die Häufigkeit der Archivierungen und die Prozeduren zur Verwaltung leerer und mit Archivierungsdaten gefüllter Datenträger geben
CGS_ARC.1.5	Die Verantwortlichen für jede Archivieroperation sowie deren Vertreter müssen eindeutig identifiziert sein
CGS_ARC.1.6	Die Verantwortlichen für die Archivierung sowie deren Vertreter müssen in den Techniken des Archivierens geschult sein
CGS_ARC.1.7	Die Archivierprozeduren müssen regelmäßig überprüft werden, um den eventuellen Weiterentwicklungen der Bedürfnisse zur Archivierung von Daten gerecht werden zu können; die Berücksichtigung alter Archivierungen muss bewahrt werden
CGS_ARC.1.8	Die Verantwortlichen für die Überprüfung der Archivierprozeduren müssen eindeutig identifiziert sein
CGS_ARC.1.9	Jede Änderung einer Archivierprozedur muss den betroffenen Verantwortlichen für die Archivierung sowie deren Vertretern mitgeteilt werden
CGS_ARC.2.1	Die Archive müssen das gleiche Schutzniveau zugebilligt bekommen wie die archivierten Daten
CGS_PPS: Schutz der Arbeitsstationen	
CGS_PPS.1.1	Die Schutzvorkehrungen des Bios gegen einen Start über externe Datenträger müssen aktiviert sein
CGS_PPS.1.2	Alle IT-Dienste, -Funktionen und –Schnittstellen, die nicht benutzt werden, müssen deaktiviert sein
CGS_PPS.1.3	Alle Dienste, Funktionen und Schnittstellen, die nur punktuell genutzt werden, müssen deaktiviert sein, sobald sie nicht mehr benötigt werden
CGS_PPS.2.1	Nur dazu befugtes Personal darf in der Lage sein, das System bzw. die darauf installierten Softwareprogramme zu ändern
CGS_PPS.2.2	Bei der Konfiguration der Softwareprogramme ist der Aspekt der Sicherheit zu berücksichtigen

CGS_PPS.2.3	Die eingesetzten Softwareprogramme müssen gemeinhin benutzt werden oder zuvor auditiert worden sein
CGS_PPS.2.4	Die eingesetzten Softwareprogramme müssen frei von bekannten Sicherheitslücken sein
CGS_PPS.2.5	Die Integrität der Codes muss gegen unzulässige Änderungen geschützt sein
CGS_PPS.3.1	Die Betriebsmittel müssen gegen Diebstahl gesichert sein (Kabelschloss, Gravur usw.)
CGS_PPS.3.2	Externe Datenträger müssen registriert und gegen Diebstahl sowie unbenutzten Zugriff gesichert sein (Aufbewahrung in einem abschließbaren Schrank, dessen Schlüssel nur den dazu ermächtigten Personen zugänglich ist; eingeschränkte Zugangsberechtigung zu den entsprechenden Nutzungsräumen usw.)
CGS_GLI: Verwaltung der Lizenzen	
CGS_GLI.1.1	Zur Verwaltung der Lizenzen muss eine entsprechende operationelle Vorrichtung eingerichtet werden
CGS_GLI.1.2	Die Lizenznummern sich getrennt abzuspeichern
CGS_GLI.1.3	Die Lizenzverträge sind vor Brand und sonstigen Schadensfällen, die sie unbrauchbar machen könnten, geschützt aufzubewahren
CGS_GLI.1.4	Der Zugang zu den Lizenzen muss den dazu befugten Personen vorbehalten sein
CGS_GLI.2.1	Der Zugang zu den installierbaren Softwareversionen muss den dazu befugten Personen vorbehalten sein
CGS_OML: Herkunftsgarantie für Hardware und Software	
CGS_OML.1.1	Die Herkunft der Installationen (Hardware und Software) sowie deren Aktualisierungen müssen garantiert werden können
CGS_OML.1.2	Eventuelle Zertifizierungen der Installationen (Hardware und Software) sowie deren Aktualisierungen müssen kontrolliert werden
CGS_OML.1.3	Zur Garantie der Authentizität von Codes müssen entsprechende Maßnahmen ergriffen werden
CGS_GMA: Wartungsmanagement	
CGS_GMA.1.1	Die Installationen, die Hard- und Software des Informationssystems sowie alle Mittel zum Schutz des Informationssystems und zur Erbringung der wesentlichen Dienste müssen instand gehalten und regelmäßig getestet werden
CGS_GMA.1.2	Die Instandhaltungen und Funktionstests der Elemente des Informationssystems, der Sicherheitselemente und der Elemente zur Erbringung der wesentlichen Dienste müssen in Einklang mit den Herstellerempfehlungen und den geltenden Normen und Standards stehen
CGS_GMA.2.1	Bei interner Wartung müssen die Verantwortlichen für die Wartung sowie deren Vertreter in den Techniken der Instandhaltung der ihnen anvertrauten Installationen, Hardware und/oder Software geschult sein
CGS_GMA.2.2	Bei interner Wartung müssen die Technischen Unterlagen der instand zu haltenden Installationen, Hardware und/oder Software den Verantwortlichen für die Wartung sowie deren Vertretern zugänglich sein
CGS_GMA.3.1	Bei externer Wartung muss für jedes Element (Installation, Hardware, Software usw.) ein Verantwortlicher für die Kontrolle der Wartungsarbeiten benannt werden
CGS_GMA.3.2	Bei externer Wartung muss sich der Verantwortliche für die Kontrolle der Wartungsarbeiten vergewissern, dass die Wartungsoperationen in den vertraglich festgelegten Abständen durchgeführt werden
CGS_GMA.3.3	Bei externer Wartung muss sich der Verantwortliche für die Kontrolle der Wartungsarbeiten vergewissern, dass für jedes ihm anvertraute Element kontinuierlich ein entsprechender Wartungsvertrag läuft (Verlängerung oder Unterzeichnung neuer Verträge)
CGS_GMA.4.1	Die Mittel zur Instandhaltung der Systeme und Betriebsmittel müssen das gleiche

	Schutzniveau zugebilligt bekommen wie die entsprechenden Systeme und Betriebsmittel selbst
CGS_GMA.5.1	Das für die Wartung bereitgestellte Budget muss ausreichen, um eine qualitativ hochwertige Instandhaltung aller Hard- und Softwarekomponenten des Informationssystems gewährleisten zu können
CGS_GMA.6.1	Bei evolutiven Wartungsoperationen muss immer eine Rücksetzprozedur für den Fall einer Anomalie infolge einer Modifikation vorgesehen werden
CGS_GSU: Verwaltung der Unterstützung	
CGS_GSU.1.1	Für die Installationen, die Hardware und Software des Informationssystems sowie alle Mittel zum Schutz des Informationssystems muss eine Unterstützung zur Verfügung stehen
CGS_GSU.1.2	Die Prozedur zur Inanspruchnahme der Unterstützung muss entweder den Benutzern des Informationssystems oder zumindest den entsprechenden, für die Verwaltung von Zwischenfällen verantwortlichen Stellen bekannt sein
CGS_GSU.1.3	Wenn Mitarbeiter das Informationssystem außerhalb der Räumlichkeiten der Institution in Anspruch nehmen müssen, muss die Unterstützung auch außerhalb der Institution zugänglich sein, und ggf. auch von Ländern mit großem Zeitunterschied aus
CGS_GSU.2.1	Bei interner Unterstützung müssen die Verantwortlichen für die Unterstützung sowie deren Vertreter eine umfassende Ausbildung über die ihnen anvertrauten Installationen, Hardware und/oder Software erhalten haben
CGS_GSU.2.2	Bei interner Unterstützung müssen die entsprechenden Technischen Unterlagen der Installationen, Hardware und/oder Software den Verantwortlichen für die Unterstützung zur Verfügung stehen und deren Vertretern zugänglich sein
CGS_GSU.2.3	Bei interner Unterstützung kann bei einfachen Elementen die Unterstützung mit der entsprechenden Stelle zur Verwaltung von Zwischenfällen zusammengelegt werden
CGS_GSU.3.1	Bei externer Unterstützung muss für jedes Element (Installation, Hardware, Software usw.) innerhalb der jeweiligen Stelle zur Verwaltung von Zwischenfällen ein Verantwortlicher für die Kontrolle der Unterstützung benannt werden
CGS_GSU.3.2	Bei externer Unterstützung ist der Verantwortliche für die Kontrolle der Unterstützung für den Kontakt mit der externen Unterstützung gemäß den im Unterstützungsvertrag definierten Modalitäten verantwortlich
CGS_GSU.3.3	Bei externer Unterstützung muss sich der Verantwortliche für die Kontrolle der Unterstützung vergewissern, dass für jedes ihm anvertraute Element kontinuierlich ein entsprechender Unterstützungsvertrag läuft (Verlängerung oder Unterzeichnung neuer Verträge)
CGS_GDH: Verwaltung von Ermächtigungen	
CGS_GDH.1.1	Die Benutzer müssen in Abhängigkeit ihres Informationsanspruchs bzw. ihrer Änderungsberechtigung und nicht in Abhängigkeit ihrer hierarchischen Position dazu ermächtigt sein, auf Daten oder Elemente des Informationssystems zugreifen zu können und/oder diese ändern zu können
CGS_GDH.1.2	Zur Validierung des Informationsanspruchs bzw. der Änderungsberechtigung eines jeden Benutzers muss vor dessen Ermächtigung eine Benutzer-Ermächtigungsprozedur erstellt werden
CGS_GDH.1.3	Die Ermächtigungsprozedur muss so einfach und so vollständig wie möglich sein, um einen berechtigten Datenzugriff nicht zu stören und dadurch evtl. einen Verleih von Zugriffsrechten zu fördern
CGS_GDH.1.4	Die verschiedenen Ermächtigungsgrade müssen in direktem Zusammenhang mit den für die Infrastrukturen und Informationen identifizierten Sicherheitsbedürfnissen stehen
CGS_GDH.1.5	Die Verantwortlichen für die Vergabe von Ermächtigungen müssen für die Elemente, auf die sich die Ermächtigungen beziehen, eindeutig identifiziert sein
CGS_GDH.1.6	Die Ermächtigungsgrade sowie die vergebenen Ermächtigungen müssen regelmäßig kontrolliert werden, um ihre Entsprechung mit den Bedürfnissen des

	Informationssystems sicherzustellen
CGS_GDH.1.7	Die Verantwortung für die Kontrolle der Ermächtigungen darf nicht den Verantwortlichen für die Vergabe von Ermächtigungen anheim fallen
CGS_GDH.1.8	Nach beendeter Bearbeitung müssen die Ermächtigungsunterlagen (Identifikation des antragstellenden Benutzers, erteilte Ermächtigungen usw.) datiert und archiviert werden
CGS_GDH.1.9	Die archivierten Ermächtigungsunterlagen sind wie sensitive Informationen zu behandeln und zu schützen
CGS_GDH.2.1	Die jeder Ermächtigung entsprechenden Rechte müssen eindeutig definiert sein.
CGS_GDH.2.2	Sobald ein Benutzer eine Ermächtigung erhält, muss er über die damit verbundenen Rechte informiert werden
CGS_PDI: Schutz der Infrastrukturen	
CGS_PDI.1.1	Die Sicherheitspolitik muss eine Liste aufstellen, auf der alle zu realisierenden Einrichtungstypen zum Schutz der Datenverarbeitungsinfrastrukturen vermerkt sind
CGS_CIR: Klassifizierung der Information und der Verantwortung	
CGS_CIR.1.1	Die zur Klassifizierung der Information verwendeten Typen müssen in der Sicherheitspolitik beschrieben sein
CGS_CIR.1.2	Die jedem Klassifizierungstyp entsprechenden Sicherheitsvorschriften müssen in der Sicherheitspolitik beschrieben sein
CGS_CIR.1.3	Die Verantwortungen zur Anwendung der jedem Klassifizierungstyp entsprechenden Sicherheitsvorschriften, die davon abhängen, welchen Verwendungszweck die Daten haben, müssen in der Sicherheitspolitik beschrieben sein
CGS_PAI: Zugriffsprivilegien auf Informationen	
CGS_PAI.1.1	Die Verantwortlichen für die Definition, Vergabe und Kontrolle von Zugriffsrechten auf Informationen müssen eindeutig definiert sein
CGS_PAI.1.2	Die Kontrollen von Zugriffsrechten auf Informationen müssen regelmäßig überprüft werden, um sicherzustellen, dass sie immer noch den Sicherheitsbedürfnissen entsprechen
CGS_PAI.1.3	Jede Änderung der Kontrollen von Zugriffsrechten auf Informationen muss Anlass zu einer Mitteilung an alle potentiellen Benutzer der betroffenen Systeme geben
CGS_PAI.1.4	Die Prozedur zur Verwaltung der Zugriffsprivilegien muss so einfach und so vollständig wie möglich sein, um einen berechtigten Datenzugriff nicht zu stören und dadurch evtl. einen Verleih von Zugriffsmitteln zu fördern
CGS_PAI.2.1	Alle zu vergebende Benutzerrechte müssen in einer gesonderten Verordnung definiert werden
CGS_PAI.2.2	In der Verordnung zur Definition der Benutzerrechte müssen alle bestehenden Rechte eindeutig definiert sein, insbesondere die Rechte "Informationsanspruch" und "Änderungsberechtigung"
CGS_PAI.2.3	In der Verordnung zur Definition der Benutzerrechte sind Angaben über die Nutzung dieser Rechte im Hinblick auf die Zugangskontrolle und die Benutzerermächtigung zu machen
CGS_REC: Abnahme	
CGS_REC.1.1	Die Abnahmeprüfungen und Funktionstests der Softwareprogramme müssen auf allen Plattformen durchgeführt werden, auf denen sie eventuell installiert werden sollen
CGS_GPC: Verwaltung kritischer Prozesse	
CGS_GPC.1.1	Soweit wie möglich müssen kritische Prozesse auf die zentrale Institution konzentriert werden
CGS_GPC.1.2	Bei Delokalisierung eines kritischen Prozesses außerhalb der zentralen Institution müssen durch die zentrale Institution Maßnahmen zur Überwachung

	des Prozesses ergriffen werden (Aktivitätsbericht, Fernadministration usw.)
CGS_GPC.2.1	Kritische Prozesse dürfen nicht von einer einzigen Person ausgeführt werden können
CGS_GPC.2.2	Die Ergebnisse kritischer Prozesse müssen vor ihrer Anwendung validiert werden
CGS_GPC.2.3	Die Validierung kritischer Prozesse muss von mindestens zwei Verantwortlichen der Institution vorgenommen werden
CGS_GPC.2.4	Die Verantwortlichen für die Validierung kritischer Prozesse sowie deren Vertreter müssen eindeutig identifiziert sein
CGS_PEP: Schutz gemeinsam genutzter Bereiche	
CGS_PEP.1.1	Gemeinsam genutzte Bereiche oder für den Informationsaustausch vorgesehene Bereiche sind genauso wie die übrigen Bereiche des Informationssystems gegen unbefugten Zugriff zu schützen (Ermächtigung, Zugriffsrechte, Authentifizierung usw.)
CGS_OES: Organisation und Sicherheit	
CGS_OES.1.1	Die innerhalb der Institution und zwischen der Institution und ihren Partnern errichtete Organisation muss die individuelle Identifikation der Benutzer begünstigen
CGS_OES.1.2	Eventuelle Änderungen der Organisation infolge eines politischen Wechsels oder einer neuen Organisationsstrategie dürfen den Umfang abgedeckter Risiken nicht einschränken
CGS_OES.1.3	Übergangszeiten bei einer Organisationsänderung sind im Voraus zu planen und dürfen keinen Einfluss auf die Zugangsrechte und die Zuweisung von Rechten haben
CGS_HSI: Sicherheitsschutz außerhalb des Informationssystems	
CGS_HSI.1.1	Sicherheitsvorkehrungen, die nicht Gegenstand des Informationssystems sind (Rauchmelder, Detektionsmechanismen zur Vorbeugung von Wasserschäden, Blitzableiter usw.) sind genauso zu schützen wie die Einrichtungen des Informationssystems
CGS_HSI.1.2	Das mit der Organisation beauftragte Personal muss für den Schutz von Sicherheitsvorkehrungen, die nicht Bestandteil des Informationssystems sind, sensibilisiert werden
CGS_GSS: Verwaltung der Ersatzsysteme bei Notfällen	
CGS_GSS.1.1	Die Ersatzmechanismen müssen mindestens aus ausreichend dimensionierten redundanten Einrichtungen bestehen, um die als strategisch identifizierten Dienste zufrieden stellend sicherstellen zu können
CGS_GSS.1.2	Die Dimensionierung der redundanten Ersatzeinrichtungen muss regelmäßig und nach jeder größeren Weiterentwicklung des Informationssystems überprüft werden, damit ihre Angemessenheit jederzeit sichergestellt ist
CGS_GSS.1.3	Alle Ersatzeinrichtungen (ob redundant oder nicht) müssen so dimensioniert sein, dass sie eine Dienstqualität aufweisen, die den für die Notlösungen identifizierten Ziele ebenbürtig ist
CGS_GSS.1.4	Soweit wie möglich dürfen die Ersatzmittel für den Notbetrieb nicht im Nominalbetrieb eingesetzt werden, geschieht dies dennoch, muss bei ihrer Dimensionierung der voraussichtlich höhere Bedarf an Ressourcen im Falle eines Zwischenfalls berücksichtigt werden
CGS_GSS.2.1	Die Aktivierung der redundanten Ersatzmittel muss soweit wie möglich automatisch erfolgen
CGS_GSS.2.2	Bei nicht automatischer Auslösung des Notbetriebs muss die Behandlung eines Zwischenfalls mit Dienstausfall mit schnellstmöglicher Aktivierung des entsprechenden Notbetriebs beginnen
CGS_GMR: Verwaltung der Aussonderungen	
CGS_GMR.1.1	Datenträger mit institutionsinternen Informationen sind so auszusondern, dass sie der Öffentlichkeit nicht zugänglich sind

CGS_GMR.1.2	Datenträger mit vertraulichen Informationen dürfen nicht ausgesondert werden, damit sie nicht unbefugten Personen zugänglich werden können
CGS_GDA: Verwaltung der Authentifizierungen	
CGS_GDA.1.1	Ab einem bestimmten Sicherheitsniveau ist die Authentifizierung zwingend notwendig, und zwar sowohl für den Dateizugriff als auch zur Änderung von Daten
CGS_GDA.1.2	Im Rahmen des Möglichen muss die Authentifizierung zur Abfrage der Privilegien der authentifizierten Person oder Anwendung führen
CGS_GDA.1.3	Die Systemzugriffe müssen protokolliert werden, wobei die Journale möglichst und mindestens Aufschluss über die Identität des Benutzers, das betroffene System und Datum und Uhrzeit des Zugriffs geben müssen
CGS_GDA.1.4	Aus der Auswertung der Zugangseinrichtungen hervorgehende Operationen müssen genauso aufgezeichnet und protokolliert werden wie die Systemzugriffe
CGS_GDA.2.1	Die Authentifizierung einer Person muss unbedingt auf einer ihr bekannten Information beruhen (Passwort, Pincode usw.), eventuell ergänzt durch einen in ihrem Besitz befindlichen Gegenstand (Ausweis, Chipkarte usw.), durch physische Merkmale (Biometrie) oder durch beides
CGS_GDA.3.1	Die Authentifizierung einer Anwendung muss auf einem System beruhen, das sicherstellt, dass keine unbefugte Nutzung der Anwendung vorliegt (z. B. durch Signaturzertifikat)
CGS_GDA.3.2	Bestimmte (noch zu definierende) sensitive Funktionen müssen automatisch Anlass zu einer Authentifizierung geben
CGS_CSR: Konfiguration der Netzwerkdienste	
CGS_CSR.1.1	Sämtliche Netzwerkdienste sind so zu konfigurieren, dass sie nicht für andere Funktionalitäten als die ursprünglich vorgesehenen benutzt werden können
CGS_CSR.1.2	Die Verbindungen sind mit Filtern zu versehen, um einen nicht vorgesehenen Datenverkehr zu unterbinden (Ausnutzung des Asynchronbetriebs, Zugang zu nicht autorisierten Ports, Spam usw.)
CGS_CSR.1.3	Die Zugangseinrichtung muss helfen, die Möglichkeiten unzulässiger oder betrügerischer Operationen einzuschränken
CGS_CME: Konfiguration der elektronischen Nachrichtenübermittlung	
CGS_CME.1.1	Die Konfiguration der elektronischen Nachrichtenübermittlung muss eine Kontrolle der netzgenerierten Datenflüsse ermöglichen. (Einschränkung automatischer Absendungen, allgemein zugängliche Verteilungslisten usw.)
CGS_SUP: Überwachung	
CGS_SUP.1.1	Die Systemüberwachung muss so einfach und ergonomisch wie möglich gestaltet sein (klare Informationen, angepasstes und einzigartiges Tool zur Ermöglichung einer zentralen Überwachung)
CGS_GDT: Protokolldatenverwaltung	
CGS_GDT.1.1	Die Protokolldaten müssen das gleiche Schutzniveau zugebilligt bekommen wie die Operationen, aus denen sie hervorgehen und ggf. sogar ein Schutzniveau darüber, sofern es sich um personenbezogene Daten handelt

3.4.8 CDO : Unterlagen

CDO_APP: Unterlagen über die Anwendungen	
CDO_APP.1.1	Die Wartungs-, Betriebs- und Bedienungshandbücher der Anwendungen sowie eventuelle zusätzliche interne Unterlagen zum Thema müssen den betroffenen Akteuren zugänglich sein
CDO_APP.1.2	Die Wartungs-, Betriebs- und Bedienungsprozeduren der Anwendungen müssen den betroffenen Akteuren zugänglich sein
CDO_APP.1.3	Die internen Unterlagen müssen regelmäßig überprüft werden
CDO_SDC: Aktualisierung der Konfigurationen	

CDO_SDC.1.1	Für die Systeme und ihre Konfigurationen ist eine aktuelle Bestandsaufnahme durchzuführen, die bei jeder System- oder Konfigurationsänderung zu aktualisieren und an die Akteure mit Informationsanspruch weiterzugeben ist (Instandsetzer, Entwickler, interne Unterstützung usw.)
CDO_SDC.1.2	Jede Änderung der Hardware- oder Softwarekonfiguration muss die Kompatibilität mit dem übrigen Informationssystem und mit alten Datensicherungen und Archiven berücksichtigen und zudem ist eine Rücksetzprozedur für den Fall einer Anomalie vorzusehen

3.4.9 CGI : Management von Zwischenfällen

CGI_GDC: Krisenmanagement	
CGI_GDC.1.1	Potentielle Krisensituationen müssen identifiziert werden
CGI_GDC.1.2	Für jede identifizierte potentielle Krise müssen Alarmschwellen definiert werden, um zu wissen, wann eine Institution oder ein Standort in eine Krisensituation gelangt
CGI_GDC.1.3	Ein spezifisches Maß muss definiert werden, um erkennen zu können, wann die Alarmschwellen überschritten werden
CGI_GDC.1.4	Automatische Alarmweitergaben sind so einzurichten, dass bei Erreichen einer Alarmschwelle die Prozedur zum Krisenmanagement ausgelöst wird
CGI_GDC.2.1	Die Prozedur zum Krisenmanagement muss automatisch ausgelöst werden, sobald eine Alarmschwelle erreicht wird
CGI_GDC.2.2	Die Prozedur zum Krisenmanagement kann von der letzten Eskalationsstufe beim Zwischenfallmanagement vor Erreichen einer Alarmschwelle manuell ausgelöst werden
CGI_GDC.2.3	Bei fehlender letzter Eskalationsstufe muss die Verantwortung für das manuelle Auslösen der Prozedur zum Krisenmanagement einer anwesenden Person übertragen werden (Vertreter der letzten Eskalationsstufe oder speziell ernannte Person)
CGI_GDC.2.4	Die Kette der Übertragung der Verantwortung zum manuellen Auslösen der Prozedur zum Krisenmanagement muss eindeutig identifiziert sein, damit immer jemand die Verantwortung trägt, auch wenn mehrere Personen nicht zur Verfügung stehen
CGI_GDC.2.5	Alle Personen, die evtl. mit dem manuellen Auslösen der Prozedur zum Krisenmanagement beauftragt werden, müssen entsprechend sensibilisiert und im manuellen Auslösen geschult werden
CGI_GDC.2.6	Das Auslösen der Prozedur zum Krisenmanagement muss mindestens in einer raschen Kontaktaufnahme mit dem verantwortlichen Mitglied des der Situation entsprechenden Krisenstabs bestehen
CGI_GDC.3.1	Für jeden potentiellen Krisentyp muss ein Krisenstab errichtet werden (physischer Unfall, Netzattacke, Gerichtsverfahren usw.)
CGI_GDC.3.2	Ein Krisenstab muss mindestens aus einem Fachspezialisten und einem Entscheidungsträger bestehen, dessen hierarchische Position hoch genug ist, um Entscheidungen im Namen der Institution treffen zu können
CGI_GDC.3.3	Für jeden Krisenstab müssen ein Verantwortlicher sowie dessen Vertreter benannt werden
CGI_GDC.3.4	Der Verantwortliche eines Krisenstabs muss eine sofortige Sitzung des Krisenstabs einberufen, sobald eine Prozedur zum Krisenmanagement ausgelöst und er von der Krise in Kenntnis gesetzt wurde
CGI_GDC.3.5	Für jedes Mitglied eines Krisenstabs muss eine ausreichende Anzahl Vertreter vorgesehen werden
CGI_GDC.3.6	Die Mitglieder und Vertreter eines Krisenstabs müssen entsprechend sensibilisiert und im Krisenmanagement des jeweiligen Bereichs geschult werden
CGI_GDC.4.1	Ein Krisenstab muss alle notwendigen Informationen zur Eindämmung oder Lösung einer Krise erhalten

CGI_GDC.4.2	Ein Krisenstab muss alle notwendigen Entscheidungen zur Eindämmung oder Lösung einer Krise treffen können
CGI_GDC.4.3	Die vom Krisenstab getroffenen Entscheidungen sind in kürzester Zeit anzuwenden
CGI_GDC.4.4	Alle vom Krisenstab getroffenen Entscheidungen sind schriftlich festzuhalten, zu datieren und mit den Informationen zu versehen, die zum Treffen dieser Entscheidung geführt haben
CGI_GDC.4.5	Die Verantwortung zur schriftlichen Niederlegung der vom Krisenstab getroffenen Entscheidungen muss einer anderen Person als dem Leiter des Krisenstabs anvertraut werden
CGI_GDC.4.6	Die von einem Krisenstab getroffenen Entscheidungen müssen genauso wie die anderen sicherheitsrelevanten Protokolldaten des Informationssystems aufbewahrt, ausgewertet und verwaltet werden
CGI_LCI: Brandschutz	
CGI_LCI.1.1	Es muss eine Brandschutzorganisation eingerichtet werden
CGI_LCI.1.2	Die Brandschutzorganisation muss mit den geltenden Normen und Standards übereinstimmen
CGI_LCI.1.3	Die Brandschutzorganisation muss Brandschutzprofile identifizieren
CGI_LCI.1.4	Die Rolle und Verantwortungen eines jeden Brandschutzprofils müssen eindeutig definiert werden, v. a. was die Verantwortung zur Evakuierung anbelangt
CGI_LCI.1.5	Die Profile müssen identifizierten Personen der Institution zugewiesen werden
CGI_LCI.1.6	Für jedes Brandschutzprofil muss eine ausreichende Anzahl Vertreter vorgesehen werden
CGI_LCI.1.7	Die Mitglieder und Vertreter der Brandschutzprofile müssen entsprechend sensibilisiert und in ihren Aufgaben und Verantwortungen geschult werden
CGI_GIS: Management von Sicherheitszwischenfällen	
CGI_GIS.1.1	Die Stellen zum Zwischenfallmanagement müssen in der Lage sein, die meisten gängigen Zwischenfälle ihres Bereichs selbst lösen zu können
CGI_GIS.1.2	Die Stellen zum Zwischenfallmanagement müssen die Möglichkeit haben, bei Zwischenfällen, die sie nicht alleine bearbeiten können, nächst höhere Eskalationsstufen zu kontaktieren
CGI_GIS.1.3	Egal, ob sie einen Zwischenfall selbst bearbeiten oder nicht, müssen die Stellen zum Zwischenfallmanagement eine Weiterverfolgung der Zwischenfälle sicherstellen (Art des Zwischenfalls, Datum, Ansprechpartner, Ablauf der Eingriffe, Datum des Abschlusses)
CGI_GIS.1.4	Noch nicht gelöste Zwischenfälle sind regelmäßig weiterzuverfolgen, um sicherzugehen, dass die Bemühungen um eine Behebung weitergehen
CGI_GIS.1.5	Jeder behobene Zwischenfall muss mit einer Beschreibung der Symptome des Zwischenfalls, der Ursache des Zwischenfalls und der Lösung zur Behebung archiviert werden
CGI_GIS.1.6	Die Prozedur zum Bearbeiten von Sicherheitszwischenfällen muss regelmäßig überprüft werden, um sicherzugehen, dass sie immer noch dem Informationssystem und seiner Organisation entspricht
CGI_GIS.1.7	Der Verantwortliche für die Überprüfung der Prozedur zum Bearbeiten von Zwischenfällen muss eindeutig identifiziert sein
CGI_GIS.1.8	Jede Änderung der Prozedur zum Bearbeiten von Zwischenfällen muss an alle Benutzer des Informationssystems weitergegeben werden
CGI_GIS.2.1	Die Stelle, die für das Management von Sicherheitszwischenfällen im Zusammenhang mit Diebstahl zuständig ist, muss die Formalitäten zur Anzeige des Diebstahls bei den Polizeibehörden erledigen
CGI_GIS.2.2	Die Stelle, die für das Management von Sicherheitszwischenfällen im Zusammenhang mit Diebstahl zuständig ist, muss den Diebstahl vom Güterbestand der Institution abziehen

CGI_GIS.2.3	Die Stelle, die für das Management von Sicherheitszwischenfällen im Zusammenhang mit Diebstahl zuständig ist, muss sich um die Formalitäten zur Aufkündigung eventueller, auf dem gestohlenen Material vorhandener Authentifizierungselemente kümmern
CGI_GIS.2.4	Die Stelle, die für das Management von Sicherheitszwischenfällen im Zusammenhang mit Diebstahl zuständig ist, muss sich um eventuell notwendige administrative und juristische Formalitäten kümmern
CGI_GIS.2.5	Jeder Sicherheitszwischenfall im Zusammenhang mit Diebstahl muss unter Angabe von Datum, Uhrzeit und Ort sowie einer Beschreibung der Sachlage archiviert werden
CGI_GIS.3.1	Die archivierten Zwischenfälle müssen analysiert werden, um einzuschätzen, ob die Abdeckung der beim Zwischenfall ausgenutzten Schwachstelle verbessert werden kann und um eventuell weiteren Zwischenfällen vorzubeugen (z. B. bei Ausfall oder Überlastung)
CGI_GIS.3.2	Die archivierten Zwischenfälle müssen über eine Wissensdatenbank ausgewertet werden, um die Behebung künftiger Zwischenfälle der gleichen Art beschleunigen und vereinfachen zu können
CGI_GIS.3.3	Die archivierten Zwischenfälle müssen synthetisch zusammengefasst und mit den Analyseergebnissen an die identifizierten verantwortlichen Entscheidungsträger weitergegeben werden, damit sie bei der Sicherheitsstrategie der Institution berücksichtigt werden können
CGI_GIS.3.4	Die verantwortlichen Entscheidungsträger, die mit der Analyse der Zwischenfallsynthese beauftragt sind, sowie deren Vertreter, müssen eindeutig identifiziert sein
CGI_GIS.3.5	Die verantwortlichen Entscheidungsträger, die mit der Analyse der Zwischenfallsynthese beauftragt sind, sowie deren Vertreter, müssen entsprechend sensibilisiert und in dieser Art Analyse geschult werden
CGI_GIS.3.6	Die verantwortlichen Entscheidungsträger, die mit der Analyse der Zwischenfallsynthese beauftragt sind oder evtl. deren Vertreter müssen die Möglichkeit haben, Entscheidungen zu treffen, um vorhersehbare Evolutionen abwenden zu können

3.4.10 CEI : Initialstudien und Konzeption des IS

CEI_ABS: Analyse der Sicherheitsbedürfnisse	
CEI_ABS.1.1	Die Sicherung nicht gemeinsam genutzter Bereiche des Informationssystems muss in Abhängigkeit der Sicherheitsbedürfnisse der betroffenen Funktionskomponenten erfolgen
CEI_ABS.1.2	Jede Funktionskomponente muss Anlass zu einer Studie zur Feststellung der Sicherheitsbedürfnisse geben, insbesondere im Hinblick auf die Vertraulichkeit, Verfügbarkeit, Integrität und Kontrolle/Nachweis
CEI_ABS.1.3	Jedes spezifische Bedürfnis, das durch die allgemeinen Sicherheitsvorschriften des Informationssystems nicht abgedeckt wird, muss möglichst durch spezifische Vorschriften für das Funktionselement abgedeckt werden (technische Architektur, Sicherheitsprozeduren usw.)
CEI_ABS.1.4	Jedes spezifische Bedürfnis, das nicht ausreichend abgedeckt werden kann, muss Anlass zu einer Restrisikostudie geben (siehe CRR_ETU)
CEI_ABS.1.5	Die Initialstudie muss erlauben, die notwendigen Ressourcen abzuschätzen und eine erste Dimensionierung des Systems (einschließlich Spitzenzeiten und Notbetriebe) und der Arbeitsgruppen (einschließlich Vertreter) vorzunehmen, sowie die zur Entwicklung erforderlichen Ressourcen abzusehen
CEI_ABS.1.6	Die identifizierten Sicherheitsbedürfnisse müssen die absehbaren Konsequenzen sowie den lokalen Umgebungskontext berücksichtigen (wirtschaftlicher, sozialer, politischer und gesetzgebender Kontext)
CEI_ABS.1.7	Die identifizierten Sicherheitsbedürfnisse müssen die potentiellen Auswirkungen eines Zwischenfalls berücksichtigen

CEI_CDT: Auswahl der Technologien	
CEI_CDT.1.1	Bei der Auswahl der Technologien für das Informationssystem muss die Beständigkeit ein ausschlaggebender Faktor sein (Hardware, Anwendungen, Entwicklungssprachen usw.)
CEI_CDT.1.2	Veraltete Technologien müssen sobald wie möglich durch beständige Technologien ersetzt werden
CEI_CDT.2.1	Bei Auswahl der Software, Hardware und der Installationen muss die Ergonomie im Hinblick auf Benutzung und Betrieb berücksichtigt werden
CEI_CDT.2.2	Bei Auswahl der Software, Hardware und der Installationen müssen die sanitären Normen und Standards berücksichtigt werden
CEI_ERS: Untersuchung der besonderen, an die Benutzung von Hardware und Software gebundenen Risiken	
CEI_ERS.1.1	Beim Einrichten von Standorten müssen eventuelle besondere Risiken berücksichtigt werden, die an die Unterbringung von Elementen innerhalb der Institution gebunden sind (explosionsgefährdete Stoffe, brennbare Produkte, Quellen elektromagnetischer oder thermischer Strahlung usw.)

3.4.11 CPS : Sicherheitsstrategien

CPS_PPT: Strategie zum Schutz der Arbeitsstationen	
CPS_PPT.1.1	Die Sicherheitspolitik muss eine Strategie zum Schutz ortsfester und mobiler Arbeitsstationen vorsehen (Integrität, Zugangskontrolle, Kampf gegen maligne Codes usw.)
CPS_PPT.1.2	Die Strategie zum Schutz der Arbeitsstationen muss an die Sicherheitsbedürfnisse der Institution angepasst sein
CPS_PPT.1.3	Die Strategie zum Schutz der Arbeitsstationen muss regelmäßig überprüft werden, um ihre Entsprechung mit den Bedürfnissen des Informationssystems sicherzustellen
CPS_PPT.1.4	Der Verantwortliche für die Überprüfung der Strategie zum Schutz der Arbeitsstationen muss eindeutig identifiziert sein
CPS_PPT.1.5	Jede Änderung der Strategie zum Schutz der Arbeitsstationen muss Anlass zu einer Mitteilung an alle Benutzer von Arbeitsstationen geben
CPS_PAQ: Strategie zur Qualitätssicherung	
CPS_PAQ.1.1	Die am Informationssystem durchgeführten Operationen müssen durch den Qualitätssicherungsplan der Institution abgedeckt werden
CPS_PAQ.1.2	Die Vorschriften des Qualitätssicherungsplans der Institution müssen schriftlich in einem Qualitätssicherungshandbuch festgelegt werden
CPS_PAQ.1.3	Alle Mitarbeiter der Institution müssen Zugang zum Qualitätssicherungshandbuch haben
CPS_PAQ.1.4	Das Qualitätssicherungshandbuch muss regelmäßig überprüft werden, um die Entsprechung mit den Qualitätszielen der Institution sicherstellen zu können
CPS_PAQ.1.5	Der Verantwortliche für die Überprüfung des Qualitätssicherungshandbuchs muss eindeutig identifiziert sein
CPS_PAQ.1.6	Jede Änderung des Qualitätssicherungshandbuchs muss Anlass zu einer Mitteilung an alle Mitarbeiter der Institution geben
CPS_PAQ.2.1	Das Qualitätssicherheitshandbuch muss die tätigkeitsspezifischen Aspekte der Qualitätssicherung behandeln
CPS_PAQ.2.2	Alle Mitarbeiter der Institution müssen zur Annahme der Qualitätsmaßnahmen für die tätigkeitsspezifischen Qualitätsvorschriften sensibilisiert werden
CPS_PAQ.3.1	Manuelle Bearbeitungen müssen soweit wie möglich vor ihrer Realisierung zunächst von einem Verantwortlichen validiert werden
CPS_DEV: Strategie zum Schutz von Entwicklungen	
CPS_DEV.1.1	Die Entwicklung von Anwendungen für das Informationssystem muss über

	Entwicklungsvorschriften kontrolliert und eingegrenzt werden
CPS_DEV.1.2	Die Entwicklungsvorschriften müssen sich auf nationale und internationale Entwicklungsnormen und –standards stützen

3.4.12 CPD : Datenschutz

CPD_DGL: Daten der Geolokalisation	
CPD_DGL.1.1	Daten, die zur Lokalisierung einer Person oder eines Betriebsmittels genutzt werden können, müssen als sensitive Daten betrachtet und als solche im Hinblick auf die Vertraulichkeit geschützt werden
CPD_DGL.1.2	Das Institutionspersonal muss für den Schutz von Daten sensibilisiert werden, die zur Lokalisierung einer Person oder eines Betriebsmittels genutzt werden könnten
CPD_INP: Identifizierung der Schutzniveaus	
CPD_INP.1.1	Das Schutzniveau eines Systems muss physisch auf dem System und in den entsprechenden Unterlagen vermerkt werden

3.4.13 CFO : Ausbildung

CFO_SPS: Sensibilisierung für Sicherheitsprobleme	
CFO_SPS.1.1	Alle Benutzer des Informationssystems müssen für die Risiken, die auf dem Informationssystem lasten, für die Angriffsmethoden, die potentiellen Sicherheitsprobleme und die Maßnahen zur Abdeckung der Risiken bzw. zur Einschränkung der Auswirkungen sensibilisiert werden
CFO_SPS.1.2	Alle Mitarbeiter müssen dafür sensibilisiert werden, dass scheinbar harmlose Verhalten die Dienstleistungsqualität des Informationssystems beeinträchtigen können (z. B. Forward bei Hoax-Meldungen)
CFO_FRS: Ausbildung der Vertreter oder Nachfolger	
CFO_FRS.1.1	Für die wichtigen Funktionen der Organisation muss für den Fall punktueller Nichtverfügbarkeit der Amtsträger eine angemessene Anzahl Vertreter benannt werden
CFO_FRS.1.2	Die Vertreter, die zur Übernahme punktuell nicht besetzter Funktionen benannt wurden, müssen in den Aufgaben geschult werden, die im Rahmen dieser Funktionen auszuüben sind
CFO_FRS.1.3	Die Vertreter, die zur Übernahme punktuell nicht besetzter Funktionen benannt wurden, müssen über die Verantwortungen informiert werden, die im Rahmen dieser Funktionen zu übernehmen sind
CFO_FRS.1.4	Je nach zu vertretenden Funktionen kann der Vertreter teilweise oder ganz von seinen üblichen Funktionen entlastet werden
CFO_FRS.1.5	Bei einer Vertretung muss der Vertreter die gleichen Privilegien, Rechte, Zuweisungen und Verantwortung zugebilligt bekommen wie die Person, die er vertritt
CFO_FRS.2.1	Soweit wie möglich muss die Aufgabe einer Funktion durch den Amtsträger so früh wie möglich vorgesehen und vorbereitet werden
CFO_FRS.2.2	Wenn nach dem Ausscheiden eines Amtsträgers die Dimensionierung einer Arbeitsgruppe nicht mehr den ihr aufgetragenen Funktionen entspricht, muss für den ausscheidenden Amtsinhaber ein Nachfolger benannt werden
CFO_FRS.2.3	Dabei ist eine ausreichend lange Übergangszeit vorzusehen, während der der ausscheidende Amtsinhaber und sein Nachfolger die gleichen Funktionen wahrnehmen
CFO_FRS.2.4	Vor seinem Ausscheiden muss der ausscheidende Amtsinhaber seinen Nachfolger ausbilden und ihm seine üblichen Ansprechpartner vorstellen

3.4.14 CCC : Vertragsklauseln

CCC_CLR: Vertragsklauseln zur Einschränkung der Verantwortungen beider Parteien	
CCC_CLR.1.1	Die Verantwortungen, Sanktionen und Strafen, die alle unterzeichnenden Parteien eines Vertrages treffen, müssen dem Kontext angepasst und den potentiellen Auswirkungen angemessen sein (übertriebene Strafen und Sanktionen sind zu vermeiden)
CCC_CLR.1.2	Die Verantwortungen jeder unterzeichnenden Partei eines Vertrages müssen auf ein eindeutig identifiziertes Maximum beschränkt werden
CCC_RGF: Reversibilität und finanzielle Garantien	
CCC_RGF.1.1	Bei der Auswahl eines Unterauftragnehmers oder Leistungserbringers müssen Maßnahmen zur Evaluierung der finanziellen und/oder technischen Beständigkeit getroffen werden
CCC_RGF.1.2	Verträge zur Vergabe von Unteraufträgen oder Langzeit-Leistungsverträge müssen eine Reversibilitätsklausel enthalten

3.4.15 CRH : Personalwesen

CRH_DDE: Dimensionierung der Arbeitsgruppen	
CRH_DDE.1.1	Die Arbeitsgruppen sind zahlenmäßig so zu bemessen, dass sie ihren Funktionen in zufrieden stellender Art und Weise nachkommen können
CRH_DDE.1.2	Die Arbeitsgruppen sind zahlenmäßig so zu bemessen, dass die wesentlichen Funktionen bei Nichtverfügbarkeit eines Teils der Mitarbeiter sichergestellt werden können
CRH_PDP: Schutz des Personals	
CRH_PDP.1.1	Bei allgemein schwierigen Umgebungsbedingungen muss die Organisation Maßnahmen zum Schutz des Personals vorsehen (Sicherheitsdienst, Unterbringung in Standortnähe usw.)
CRH_PDP.1.2	In entfernten Standorten beschäftigtes Personal muss vorübergehend am Hauptstandort untergebracht werden können. Es muss die Möglichkeit haben, dort die wichtigsten Missionen erledigen zu können
CRH_PDP.1.3	Für den Fall schwieriger Zugänglichkeit des Standorts muss die Institution Ersatzlösungen vorsehen (Sammelbusse bei streikenden Transportunternehmen, Anmieten von Schnee-Räumfahrzeugen zur Räumung der Zufahrtstraßen zum Standort usw.)
CRH_CDT: Arbeitsbedingungen	
CRH_CDT.1.1	Die Ausstattung der Räumlichkeiten muss für die geforderte Arbeit so angemessen wie möglich sein (ausreichende Beleuchtung, angemessene Temperatur, Lärmisolierung, Aufräummöglichkeiten usw.)
CRH_CDT.1.2	Besondere Vorkehrungen sind zu treffen, um die Störungen am Arbeitsplatz soweit wie möglich einzuschränken (keine Open-Space-Besprechungen, Kaffeemaschine in ausreichender Entfernung zum Arbeitsbereich u. ä.)
CRH_QDP: Qualifikation des Personals	
CRH_QDP.1.1	Die jedem Mitarbeiter zugewiesenen Aufgaben müssen seinen Qualifikationen entsprechen

3.4.16 CDS : Dimensionierung der Systeme

CDS_DES: Dimensionierung der wesentlichen Dienste	
CDS_DES.1.1	Die wesentlichen Dienste und Ersatzdienste sind so zu bemessen, dass angemessene und qualitativ hochwertige Dienstleistungen auch während eventueller Spitzenzeiten geboten werden können
CDS_DES.1.2	Die Dimensionierung der wesentlichen Dienste muss regelmäßig und bei jeder bedeutenden Weiterentwicklung des Informationssystems oder der Standorte überprüft werden, damit die Dienste auch während eventueller Spitzenzeiten

weiterhin angemessen und qualitativ hochwertig sind

4 Vorschlag zur Abdeckung der Schwachstellen durch allgemeine Sicherheitsziele

Die Sicherheitsziele (deren Codes denen der vorhergehenden Abschnitte entsprechen) werden nach Angriffsmethode und Schwachstelle präsentiert.
Mit Hilfe der folgenden Tabellen können die allgemeinen Sicherheitsziele, die in der Lage sind, die allgemeinen Schwachstellen im Einzelnen abzudecken, problemlos bestimmt werden. Zur Bearbeitung von Schwachstellen sind sie nützlich, müssen jedoch zur umfassenden Behandlung dieser Risiken weiter vervollständigt werden, und zwar durch Ziele, die die Ursprünge und Konsequenzen der Risiken einbeziehen.

4.1.1 BRAND

Schwachstelle	Abdeckung
Einzelexemplar der Lizenzverträge	LOG_07
Intern entwickelte Einzelanwendungen	MAT_02
Benutzungsbedingungen außerhalb der tolerierten Betriebsbedingungen der Betriebsmittel	PHY_01
Fehlende Ersatz-Betriebsmittel	MAT_01
Betriebsmittel in Kontakt mit brennbaren Stoffen (z. B. stauberzeugende Massendrucker)	PHY_09
Fehlende Datensicherung auf Datenträgern	ORG_08
Original-Datenträger	MAT_02 ORG_08
Fehlender Versicherungsschutz bei schweren Schadensfällen	ORG_44
Fehlende Standorterkundung durch die Rettungsdienste (Feuerwehr)	ORG_22 ORG_25
Fehlende Normen beim Einrichten institutionseigener Standorte	ORG_23 ORG_38
Fehlende Vertragsklauseln zur Sicherstellung der Aktivitäten bei Krisensituationen beim Lieferanten	ORG_38
Fehlende Weitergabe von Sicherheitsanweisungen an externes Personal	ORG_25
Fehlende Verwaltung der Prüfberichte, die die Sicherheitsausrüstung betreffen	ORG_27
Fehlende Aushängung gültiger Anweisungen zur Benachrichtigung der Rettungsdienste	ORG_17
Fehlende Brandschutzorganisation (Festlegung der Rollen, Verantwortungen)	ORG_14 ORG_24
Fehlende Aktualisierung der Verträge zur Wartung der Brandschutzeinrichtungen	ORG_27
Fehlende Krisenmanagementorganisation	ORG_14 ORG_24
Fehlende Kenntnis der Sicherheitsmaßnahmen	PER_03 PER_11
Fehlende Tests zur Überprüfung der Reaktions- und Unterrichtungsprozeduren im Schadensfal	PER_11
Fehlende Sensibilisierung für den Schutz von Sicherheitseinrichtungen	PER_05
Konfliktgeladenes soziales Klima	
Bestehende Öffnungen zur Straße hin (Fenster)	PHY_03
Veraltete Räumlichkeiten	PHY_10
Fehlende Zugangskontrolle zum Standort oder zu den Räumlichkeiten	PHY_03
Fehlende Brandschutz-Zwischenwände	PHY_09
Während der Installationsphase, fehlende Berücksichtigung der besonderen, an die vorhandene Ausstattung gebundenen Brandrisiken	PHY_06

Fehlende, falsch dimensionierte oder unangepasste automatische Brandlöscheinrichtung	PHY_09
Fehlende Wartung der Klimatisierungssysteme	ORG_27 PHY_01

4.1.2 WASSERSCHÄDEN

Schwachstelle	Abdeckung
Einzelexemplar der Lizenzverträge	LOG_07
Intern entwickelte Einzelanwendungen	MAT_02
Fehlende Ersatz-Betriebsmittel	MAT_01
Fehlende Datensicherung auf Datenträgern	ORG_08
Original-Datenträger	MAT_02 ORG_08
Fehlender Versicherungsschutz bei schweren Schadensfällen	ORG_44
Fehlende Normen beim Einrichten institutionseigener Standorte	ORG_23 ORG_38
Fehlende Vertragsklauseln im Hinblick auf Krisensituationen bei Unterauftragnehmern oder Lieferanten	ORG_38
Fehlende Weitergabe von Sicherheitsanweisungen an externes Personal	ORG_25
Fehlende Verwaltung der Prüfberichte, die die Sicherheitsausrüstung betreffen	ORG_27
Fehlende Aushängung gültiger Anweisungen zur Benachrichtigung der Rettungsdienste	ORG_17
Fehlende Anweisungen bezüglich der Alarmierung, des Verhaltens und der Unterrichtung bei Wasserschäden (fehlende Ausweisung der Sperrventile usw.)	ORG_24 ORG_24
Fehlende Garantie für den korrekten Betrieb der Wasserdetektoren	ORG_27
Fehlende Krisenmanagementorganisation	ORG_14 ORG_24
Fehlende Tests zur Überprüfung der Reaktions- und Unterrichtungsprozeduren im Schadensfall	PER_11
Fehlende Kenntnis der Sicherheitsmaßnahmen	PER_03 PER_11
Fehlende Sensibilisierung für den Schutz von Sicherheitseinrichtungen	PER_05
Konfliktgeladenes soziales Klima	
Standort in einem Überflutungsbereich	PHY_04
Fehlende physische Zugangskontrolle zu den Räumlichkeiten	PHY_03
Undichte Öffnungen nach außen	PHY_03
Vorhandensein einer Wasserlöscheinrichtung	PHY_03
Undichte Decke oder Öffnungen nach außen	PHY_03
Fehlende Ausweisung der Wasserabsperrventile	PHY_07
Ungeschützter Zugang	PHY_03
Wasserleitung in unmittelbarer Nähe der Systemausstattung	PHY_03
Vorhandensein einer Wasserlöscheinrichtung	PHY_10
Wasserleitung in unmittelbarer Nähe der Endgeräte	PHY_03
Fehlende Abfallschächte	PHY_03
Ungeschützter Zugang zu den Räumlichkeiten, in denen sich die Einrichtungen zur Produktion bzw. zur Erbringung der wesentlichen Dienste befinden	PHY_03
Unter-Boden-Verkabelung	PHY_07
Veraltete Kühlkanäle	PHY_10
Fehlende Wartung der Klimatisierungssysteme	ORG_27

	PHY_01
Fehlendes Wasserabsperrventil	PHY_07

4.1.3 VERSCHMUTZUNG

Schwachstelle	Abdeckung
Einzelexemplar der Lizenzverträge	LOG_07
Intern entwickelte Einzelanwendungen	MAT_02
Empfindlichkeit des Datenträgers bei schlechten Aufbewahrungsbedingungen	MAT_03
Fehlende Normen beim Einrichten institutionseigener Standorte	ORG_23 ORG_38
Fehlende Aktualisierung der Wartungsverträge	ORG_27
Fehlende Maßnahmen bei Ausfall der Klimatisierungssysteme	ORG_16
Fehlende Tests zur Überprüfung der Reaktions- und Unterrichtungsprozeduren im Schadensfall	PER_11
Fehlende Kenntnis der Sicherheitsmaßnahmen	PER_03 PER_11
Fehlende Sensibilisierung für den Schutz von Sicherheitseinrichtungen	PER_05
Konfliktgeladenes soziales Klima	
Unmittelbare Nähe zu Verschmutzungsquellen (akustische Quelle, Rauch, Dampf usw.)	PHY_04
Verschmutzte Atmosphäre (Lagerhalle, Werkstatt usw.)	PHY_04
Fehlende Wartung der Klimatisierungssysteme	ORG_27 PHY_01
Fehlendes, ausreichend bemessenes redundantes Material	PHY_01
Veraltete Filter der Klimatisierungssysteme	PHY_10
Ungeschützter Zugang zur Systemausstattung	PHY_03

4.1.4 GRÖSSERER SCHADENSFALL

Schwachstelle	Abdeckung
Einzelexemplar der Lizenzverträge	LOG_07
Intern entwickelte Einzelanwendungen	MAT_02
Fehlende Ersatz-Betriebsmittel	MAT_01
Fehlende Datensicherung auf Datenträgern	ORG_08
Original-Datenträger	MAT_02 ORG_08
Fehlender Notdienst in unmittelbarer Umgebung der Institution	ORG_24
Fehlende Normen beim Einrichten institutionseigener Standorte	ORG_23 ORG_38
Fehlende Vertragsklauseln im Hinblick auf Krisensituationen bei Unterauftragnehmern oder Lieferanten	
Fehlende Aushängung gültiger Anweisungen zur Benachrichtigung der Rettungsdienste	ORG_17
Fehlender Versicherungsschutz bei schweren Schadensfällen	ORG_44
Fehlende Krisenmanagementorganisation	ORG_14 ORG_24
Fehlende Kenntnis der Sicherheitsmaßnahmen	PER_03 PER_11
Fehlende Prozeduren zum Management von Notsituationen	PER_11
Mögliche Zerstörung infolge eines externen Ereignisses (Kollisionen, Attentate)	PHY_04

Unmittelbare Nähe zu einem Gebiet mit industrieller Tätigkeit oder zu einem Risikogebiet	PHY_04
Räumlichkeiten ohne Berücksichtigung der Explosions-/Implosionsgefahr	PHY_03

4.1.5 ZERSTÖRUNG VON BETRIEBSMITTELN ODER DATENTRÄGERN

Schwachstelle	Abdeckung
Einzelexemplar der Lizenzverträge	LOG_07
Intern entwickelte Einzelanwendungen	MAT_02
Fehlende Ersatz-Betriebsmittel	MAT_01
Empfindlichkeit der Betriebsmittel	ORG_04
Zugänglichkeit der Betriebsmittel durch Fremde (Nicht-Eigentümer) (z. B. Unterbringung an einem Ort mit Publikumsverkehr)	PHY_03
Zugänglichkeit der Datenträger durch Fremde (Nicht-Eigentümer)	PHY_03
Fehlende Prozedur zur Archivierung	ORG_07
Empfindlichkeit der Datenträger	ORG_04
Fehlende Maßnahmen zur Konservierung der Archive unter Berücksichtigung der Aufbewahrungsfristen (Alterung der Bänder, Abnutzung der CD-Roms usw.)	MAT_04
Fehlende Datensicherung auf Datenträgern	ORG_08
Original-Datenträger	MAT_02 ORG_08
Fehlende Weitergabe von Sicherheitsanweisungen an externes Personal	ORG_25
Fehlender Versicherungsschutz bei Zerstörung von Betriebsmitteln	ORG_44
Fehlende Vorschriften über Gebrauch und Aufbewahrung von Betriebsmitteln und Datenträgern (Schutzmaßnahmen beim Transport, Rauchverbot usw.)	ORG_04
Fehlende Kenntnis der Sicherheitsmaßnahmen	PER_03 PER_11
Konfliktgeladenes soziales Klima	
Fehlende Sensibilisierung für den physischen Schutz der Systemausstattung	PER_01 PER_03
Fehlende Zugangskontrolle zum Standort oder zu den Räumlichkeiten oder Eindringen über indirekte Zugänge möglich	PHY_03
Ungeschützter physischer Zugang zu den Räumlichkeiten, in denen sich die Betriebsmittel oder Datenträger befinden	PHY_03
Datenträger sind unbefugten Personen zugänglich	ORG_01
Unter Boden verlegte, nicht gekennzeichnete Informationsträger	PHY_03
Zugänglichkeit der Systemausstattung durch unbefugte Personen	ORG_01
Empfindlichkeit der Systemausstattung	ORG_04

4.1.6 KLIMATISCHES PHÄNOMEN

Schwachstelle	Abdeckung
Fehlende Normen beim Einrichten institutionseigener Standorte	ORG_23 ORG_38
Fehlender Notdienst in unmittelbarer Umgebung der Institution	ORG_24
Fehlende Vertragsklauseln im Hinblick auf Krisensituationen bei Unterauftragnehmern oder Lieferanten	
Fehlende Anweisungen (hinsichtlich Alarmierung, Vorbeugung, Verhalten usw.)	ORG_24
Fehlende Kenntnis der Sicherheitsmaßnahmen	PER_03 PER_11
Fehlende Tests zur Überprüfung der Reaktions- und Unterrichtungsprozeduren im	PER_11

Schadensfall	
Fehlende Belüftungs- oder Klimatisierungsmittel bei exzessiver Sommerhitze	PHY_01
Keine Berücksichtigung der klimatischen Bedingungen bei Konstruktion der Räumlichkeiten	PHY_04
Nicht für Extrembedingungen ausgelegte Informationsträger oder Ausstattung (extreme Feuchtigkeit, Temperaturen oder physische Störungen)	MAT_03

4.1.7 SEISMISCHES PHÄNOMEN

Schwachstelle	Abdeckung
Vibrationsempfindliche Hardware	PHY_03
Fehlende Normen beim Einrichten institutionseigener Standorte	ORG_23 ORG_38
Fehlender Notdienst in unmittelbarer Umgebung der Institution	ORG_24
Fehlende Vertragsklauseln im Hinblick auf Krisensituationen bei Unterauftragnehmern oder Lieferanten	
Fehlende Anweisungen (hinsichtlich Alarmierung, Vorbeugung, Verhalten usw.)	ORG_24
Fehlende Kenntnis der Sicherheitsmaßnahmen	PER_03 PER_11
Fehlende Tests zur Überprüfung der Reaktions- und Unterrichtungsprozeduren im Schadensfall	PER_11
Keine Berücksichtigung der seismischen Risiken bei Konstruktion der Räumlichkeiten	PHY_04
Nicht für Extrembedingungen ausgelegte Informationsträger oder Ausstattung (extreme Feuchtigkeit, Temperaturen oder physische Störungen)	MAT_03

4.1.8 VULKANISCHES PHÄNOMEN

Schwachstelle	Abdeckung
Fehlende Normen beim Einrichten institutionseigener Standorte	ORG_23 ORG_38
Fehlender Notdienst in unmittelbarer Umgebung der Institution	ORG_24
Fehlende Vertragsklauseln im Hinblick auf Krisensituationen bei Unterauftragnehmern oder Lieferanten	
Fehlende Anweisungen (hinsichtlich Alarmierung, Vorbeugung, Verhalten usw.)	ORG_24
Fehlende Kenntnis der Sicherheitsmaßnahmen	PER_03 PER_11
Fehlende Tests zur Überprüfung der Reaktions- und Unterrichtungsprozeduren im Schadensfall	PER_11
Als gefährdetes Gebiet eingestufter Standort	PHY_04
Keine Berücksichtigung der seismischen Risiken bei Konstruktion der Räumlichkeiten	PHY_04
Nicht für Extrembedingungen ausgelegte Informationsträger oder Ausstattung (extreme Feuchtigkeit, Temperaturen oder physische Störungen)	MAT_03

4.1.9 METEOROLOGISCHES PHÄNOMEN

Schwachstelle	Abdeckung
Benutzungsbedingungen außerhalb der tolerierten Betriebsbedingungen der Betriebsmittel	PHY_01
Fehlender Notdienst in unmittelbarer Umgebung der Institution	ORG_24
Fehlende Normen beim Einrichten institutionseigener Standorte	ORG_23 ORG_38
Fehlende Vertragsklauseln im Hinblick auf Krisensituationen bei Unterauftragnehmern	

oder Lieferanten	
Fehlende Anweisungen (hinsichtlich Alarmierung, Vorbeugung, Verhalten usw.)	ORG_24
Fehlende Kenntnis der Sicherheitsmaßnahmen	PER_03 PER_11
Fehlende Tests zur Überprüfung der Reaktions- und Unterrichtungsprozeduren im Schadensfall	PER_11
Standort mit regelmäßigen extremen meteorologischen Phänomenen (Unwetter, Orkan, Zyklon usw.)	PHY_04
Fehlender Blitzschutz	PHY_04
Nicht für Extrembedingungen ausgelegte Informationsträger oder Ausstattung (extreme Feuchtigkeit, Temperaturen oder physische Störungen)	MAT_03

4.1.10 HOCHWASSER

Schwachstelle	Abdeckung
Fehlender Notdienst in unmittelbarer Umgebung der Institution	ORG_24
Fehlende Normen beim Einrichten institutionseigener Standorte	ORG_23 ORG_38
Fehlende Vertragsklauseln im Hinblick auf Krisensituationen bei Unterauftragnehmern oder Lieferanten	
Fehlende Anweisungen (hinsichtlich Alarmierung, Vorbeugung, Verhalten usw.)	ORG_24
Standort in einem Überflutungsbereich	PHY_04
Fehlender Schutz gegen Wasserspiegelanstieg	PHY_03
Nicht für Extrembedingungen ausgelegte Informationsträger oder Ausstattung (extreme Feuchtigkeit, Temperaturen oder physische Störungen)	MAT_03

4.1.11 AUSFALL DER KLIMATISIERUNGSSYSTEME

Schwachstelle	Abdeckung
Zu klimatisierende Betriebsmittel	MAT_03 PHY_01
Zu klimatisierende Archive	MAT_03 PHY_01
Fehlende Normen beim Einrichten institutionseigener Standorte	ORG_23 ORG_38
Fehlende Vertragsklauseln über die maximal zulässige Unterbrechungsdauer bei Erbringung eines wesentlichen Dienstes	ORG_38
Fehlende Vertragsklauseln über Schadensersatz bei Nicht-Erbringung eines wesentlichen Dienstes	ORG_38
Fehlende Anweisungen (hinsichtlich Alarmierung, Vorbeugung, Verhalten usw.)	ORG_24
Fehlende Kenntnis der Sicherheitsmaßnahmen	PER_03 PER_11
Fehlende Nachkontrolle der Klimatisierungsbedürfnisse nach Umbau oder Hinzufügung von Betriebsmitteln	PHY_01
Von Kaltwasserzufuhr oder Nahrungsmittelbelieferung abhängiges Gerät	PHY_01
Den Bedürfnissen nicht angepasste Einrichtung	PHY_01
Fehlende Wartung der Klimatisierungssysteme	ORG_27 PHY_01
Fehlendes, ausreichend bemessenes redundantes Material	PHY_01
Ungeschützter Zugang zu den Wasser- und Stromversorgungseinrichtungen	PHY_03

4.1.12 AUSFALL DER ENERGIEVERSORGUNG

Schwachstelle	Abdeckung
Störempfindliches Material (Spannungsabfälle, Überspannungen, Mikrounterbrechungen)	PHY_01
Fehlende Normen beim Einrichten institutionseigener Standorte	ORG_23 ORG_38
Fehlende Vertragsklauseln über Schadensersatz bei Nicht-Erbringung eines wesentlichen Dienstes	ORG_38
Fehlende Vertragsklauseln über die maximal zulässige Unterbrechungsdauer bei Erbringung eines wesentlichen Dienstes	ORG_38
Fehlende Anweisungen (hinsichtlich Alarmierung, Vorbeugung, Verhalten usw.)	ORG_24
Fehlende Kenntnis der Sicherheitsmaßnahmen	PER_03 PER_11
Fehlende Auskunft über die Benutzungsbedingungen der Notstrom-Versorgungspunkte	PER_11
Kommunikationsendgerät ohne Notstromversorgung	PHY_01
Keine spezielle, getrennte Unterbringung säurehaltiger Batterien, sie befinden sich in den gleichen Räumlichkeiten wie das Material, an das sie angeschlossen sind	PHY_06
Schlechte Dimensionierung der Notversorgungseinheiten (Wechselrichter, Batterien usw.)	PHY_01
Ungeschützter physischer Zugang zu den Räumlichkeiten, in denen die Einrichtungen zur Stromversorgung und Elektrizitätsverteilung untergebracht sind	PHY_03
Die Räumlichkeiten mit säurehaltigen Batterien werden weder mechanisch belüftet noch sind sie aus elektrischer Sicht explosionsgeschützt ausgelegt	PHY_06
Die verschiedenen Boden- oder Wandbeläge sind nicht antistatisch	PHY_03
Die Niederspannungsschalttafel ist nicht zugänglich	PHY_01
Die Umspannanlage Mittelspannung / Niederspannung befindet sich außerhalb des Standorts (mit Zugangskontrolle durch den Lieferanten)	PHY_01
Fehlende Notversorgungsleistungsanalyse, die bei Hinzufügen von Betriebsmitteln durchzuführen ist	PHY_01
Massen und Erdungen sind nicht vorschriftsmäßig	PHY_10

4.1.13 AUSFALL DER TELEKOMMUNIKATIONSMITTEL

Schwachstelle	Abdeckung
Über Telekommunikationsmittel ausgelagertes Material	PHY_01
Fehlende Normen beim Einrichten institutionseigener Standorte	ORG_23 ORG_38
Fehlende Vertragsklauseln über Schadensersatz bei Nicht-Erbringung eines wesentlichen Dienstes	ORG_38
Fehlende Vertragsklauseln über die maximal zulässige Unterbrechungsdauer bei Erbringung eines wesentlichen Dienstes	ORG_38
Fehlende Anweisungen (hinsichtlich Alarmierung, Vorbeugung, Verhalten usw.)	ORG_24
Fehlende Kenntnis der Sicherheitsmaßnahmen	PER_03 PER_11
Fehlende Wartung der Endgeräte und Verteilungseinrichtungen	PHY_01
Unsachgemäßer Betrieb des internen Telefonnetzes	PHY_01
Bereits festgestellte Funktionsstörung bei Erbringung des Telekommunikationsdienstes	PHY_01
Ungeschützter physischer Zugang zu den Räumlichkeiten, in denen die Einrichtungen zur Stromversorgung und Elektrizitätsverteilung bzw. die Telekommunikationsmittel untergebracht sind	PHY_03

4.1.14 ELEKTROMAGNETISCHE STRAHLUNG

Schwachstelle	Abdeckung
Elektromagnetischer oder thermischer Strahlung gegenüber empfindliche Medien und Informationsträger	PHY_03
Fehlende Vertragsklausel bezüglich der elektromagnetischen Verträglichkeit	ORG_38
Fehlende Berücksichtigung der Gefahr elektromagnetischer oder thermischer Strahlung bei der Konzeption	PHY_03
Unmittelbare Nähe zu einer Quelle elektromagnetischer oder thermischer Strahlung	PHY_03
Keine Berücksichtigung der Risiken, die mit der Nähe einer elektromagnetischen Quelle verbunden sind	PHY_03
Elektromagnetischer oder thermischer Strahlung gegenüber empfindliche Medien und Informationsträger	PHY_10

4.1.15 THERMISCHE STRAHLUNG

Schwachstelle	Abdeckung
Elektromagnetischer oder thermischer Strahlung gegenüber empfindliches Material	PHY_03
Unmittelbare Nähe zu einer Quelle elektromagnetischer oder thermischer Strahlung	PHY_03
Fehlende Berücksichtigung der Gefahr elektromagnetischer oder thermischer Strahlung bei der Konzeption	PHY_03
Keine Berücksichtigung der Risiken, die mit der Nähe einer elektromagnetischen Quelle verbunden sind	PHY_03
Elektromagnetischer oder thermischer Strahlung gegenüber empfindliche Medien und Informationsträger	PHY_10

4.1.16 ELEKTROMAGNETISCHE IMPULSE

Schwachstelle	Abdeckung
Elektromagnetischer oder thermischer Strahlung gegenüber empfindliches Material	PHY_03
Unmittelbare Nähe zu einer Quelle elektromagnetischer oder thermischer Strahlung	PHY_03
Fehlende Berücksichtigung der Gefahr elektromagnetischer oder thermischer Strahlung bei der Konzeption	PHY_03
Keine Berücksichtigung der Risiken, die mit der Nähe einer elektromagnetischen Quelle verbunden sind	PHY_03
Elektromagnetischer oder thermischer Strahlung gegenüber empfindliche Medien und Informationsträger	PHY_10

4.1.17 ABFANGEN VON KOMPROMITTIERENDEN STÖRSIGNALEN

Schwachstelle	Abdeckung
Fehlende Berücksichtigung der Installationsvorschriften	MAT_14 PHY_10
Fehlende Berücksichtigung der Zoneneinteilung des Materials	PHY_03
Material, das möglicherweise kompromittierende Störsignale aussendet	PHY_05
Die Verantwortlichen haben keinen Kontakt zu den technologischen Prüf- und Überwachungsdiensten	ORG_34
Fehlende Vorschriften über die Anwendungspflicht von Normen	ORG_04
Fehlende Vertragsklauseln über von Unterauftragnehmern und Lieferanten einzuhaltende Sicherheitsmaßnahmen	ORG_38
Fehlende Prozedur zur Überprüfung der Betriebsmittel vor dem Kauf oder nach einer Instandsetzung	ORG_20

Fehlende Kontrolle bezüglich der Anwendung der Sicherheitspolitik	ORG_22
Fehlende Datenschutzpolitik	ORG_15
Die Sicherheitspolitik wird nicht angewendet	ORG_18
Fehlende TEMPEST-Zoneneinteilung	PHY_05
Besuchereingang in unmittelbarer Gebäudenähe	PHY_05
Unmittelbare Nähe zur Straße	PHY_05
Trägermaterial fördert das Abfangen von kompromittierenden Störsignalen (elektrische Kabel, Rohrleitungen usw.)	PHY_05
Fehlender Zugangsschutz zu den Einrichtungen	PHY_03
Medien und Informationsträger senden möglicherweise kompromittierende Störsignale aus	PHY_05

4.1.18 FERN-SPIONAGE

Schwachstelle	Abdeckung
Fehlende Bildschirmschutzvorrichtungen bei Nichtbenutzung	LOG_16
Benutzung leicht zu beobachtender Passwörter für den Zugriff auf das System oder auf Systemanwendungen (Form auf einer Tastatur, kurzes Passwort)	ORG_10
Keine oder seltene Passwortänderung für den Zugriff auf das System oder die Anwendung	ORG_10
Von außen einsehbarer Bildschirm	PHY_02
Lesen von sensitiven Unterlagen in der Öffentlichkeit (Beobachten der Unterlagen durch externe Personen)	ORG_15
Fehlende Sicherheitspolitik zum Schutz der Informationsverarbeitungsinfrastruktur an den verschiedenen Standorten der Institution	ORG_02 ORG_04 ORG_27 ORG_30 ORG_33 ORG_38
Fehlende Schutzvorschriften für den Austausch vertraulich eingestufter Informationen	ORG_15
Fehlende Vertragsklauseln über von Unterauftragnehmern und Lieferanten einzuhaltende Sicherheitsmaßnahmen	ORG_38
Die Sicherheitspolitik wird nicht angewendet	ORG_18
Fehlende Identifizierung sensitiver Güter	ORG_26
Die Sicherheitsverantwortungen bezüglich der Ermächtigungsverwaltung sind nicht formalisiert	ORG_14 ORG_15
Fehlende Kontrolle bezüglich der Anwendung der Sicherheitspolitik	ORG_22
Fehlende Datenschutzpolitik	ORG_15
Fehlende Identifizierung der Sicherheitsbedürfnisse eines Projekts	ORG_32
Fehlende Kenntnis der Sicherheitsmaßnahmen	PER_03 PER_11
Geringe Sensibilisierung für den Schutz von Informationen	PER_02
Die Anwendung der Sicherheitspolitik wird durch die Direktion nicht gefördert	PER_13
Vorhandensein von Beobachtungspunkten außerhalb des Standorts	PHY_02
Zone mit Öffnungen zur Straße hin	PHY_02
Zone, die von einem Gebiet mit Publikumsverkehr aus beobachtet werden kann	PHY_07

4.1.19 PASSIVES MITHÖREN

Schwachstelle	Abdeckung
Fehlende Zugriffskontrollvorrichtung bei Nichtbenutzung	LOG_13

Möglichkeit zur Installation einer Abhörsoftware (z. B. Trojanisches Pferd)	LOG_08
Fehlender Schutz der Journale mit den Protokolldaten der jeweiligen Aktivitäten	ORG_15 ORG_39
Keine oder seltene Passwortänderung für den Zugriff auf das System oder die Anwendung	ORG_10
Fehlender Schutz gegen den Gebrauch fortgeschrittener Zugriffsprivilegien	LOG_11
Keine oder seltene Passwortänderung für den Zugriff auf die Unterstützungssoftware	ORG_10
Logischer Zugriff auf Betriebsmittel, der die Installation einer Abhörsoftware ermöglicht	MAT_10
Betriebsmittel mit abhörbarer Kommunikationsschnittstelle (Infrarot, 802.11, Bluetooth usw.)	RES_02
Fehlende Sicherheitspolitik zum Schutz der Informationsverarbeitungsinfrastruktur an den verschiedenen Standorten der Institution	ORG_02 ORG_04 ORG_27 ORG_30 ORG_33 ORG_38
Fehlende Schutzvorschriften für den Austausch vertraulich eingestufter Informationen	ORG_15
Fehlende Vertragsklauseln über von Unterauftragnehmern und Lieferanten einzuhaltende Sicherheitsmaßnahmen	ORG_38
Fehlende Kontrolle bezüglich der Anwendung der Sicherheitspolitik	ORG_22
Fehlende Identifizierung sensitiver Güter	ORG_26
Die Sicherheitsverantwortungen bezüglich der Ermächtigungsverwaltung sind nicht formalisiert	ORG_14 ORG_15
Die Sicherheitspolitik wird nicht angewendet	ORG_18
Fehlende Datenschutzpolitik	ORG_15
Fehlende Identifizierung der Sicherheitsbedürfnisse eines Projekts	ORG_32
Fehlende Ausbildung über Schutzmaßnahmen und –mittel bei externem und internem Informationsaustausch	PER_03
Manipulierbares Personal	PER_02
Die Anwendung der Sicherheitspolitik wird durch die Direktion nicht gefördert	PER_13
Geringe Sensibilisierung für einen geschützten Informationsaustausch bei vertraulichen Informationen	PER_09
Verschaffung eines Vorteils beim Abfangen einer Information	PER_08
Möglichkeit, Übertragungen außerhalb des Standorts abzufangen	PHY_05
Fehlende Zugangskontrolle zum Standort oder zu den Räumlichkeiten oder Eindringen über indirekte Zugänge möglich	PHY_03
Fehlender Zugangsschutz zu den Telekommunikationsendgeräten	RES_01
Medien und Informationsträger besitzen Eigenschaften, die ein passives Mithören erlauben (z. B. Ethernet, kabelloses Kommunikationssystem usw.)	RES_02
Informationsträger oder Kommunikationsausstattung zur Installation einer Abhöreinrichtung physisch zugänglich	ORG_01
Fehlende Authentifizierung der an das Netz angeschlossenen Betriebsmittel	RES_03
Physischer oder logischer Zugang zu einem Relais ermöglicht die Installation einer Abhöreinrichtung	PHY_03 RES_01
Kommunikation im Broadcastmodus	RES_02
Komplexe Leitweglenkung zwischen den Nebennetzen	RES_05
Schnittstelle mit Funktion, die ein Abhören ermöglicht	RES_01 RES_02
Unverschlüsselter Informationsaustausch	RES_02
Fehlende Abtrennung der Kommunikationsnetze	RES_02

Möglichkeit zum Mithören der mit den Authentifizierungsservern ausgetauschten Informationen	RES_02
Möglichkeit zum Mithören der mit den Anwendungsservern ausgetauschten Informationen	RES_02
Möglichkeit zum Einschleusen eines Abhörprogramms über die Clients	LOG_08
Möglichkeit zur Installation einer logischen Abhöreinrichtung über die Mailbox-Gateways	LOG_08
Lücken bei der Verwaltung der Zugriffsprivilegien an den Mailbox-Gateways	LOG_11

4.1.20 DIEBSTAHL VON DATENTRÄGERN ODER UNTERLAGEN

Schwachstelle	Abdeckung
Intern entwickelte Einzelanwendungen	MAT_02
Fehlende Materialbestandsaufnahme	MAT_06
Attraktive Betriebsmittel (Marktwert und technologische und strategische Werte)	MAT_07
Fehlende Diebstahlsicherung der Betriebsmittel (Kabelschloss)	MAT_07
Festplatte leicht ausbaubar	MAT_07
Betriebsmittel, das einer Gruppe von Personen frei zugänglich ist	MAT_07
Fehlender Zugangsschutz zu den Speichereinrichtungen	MAT_07
Vorhandensein eines Druckers in Bereichen mit Publikumsverkehr	ORG_01 PER_02
Datenträger allgemein zugänglich	MAT_07 ORG_15 ORG_30
Weitergabe von Datenträgern über Postdienste (externe Lieferanten, interne Post usw.)	ORG_03
Fehlender Schutz bei der Datenträgeraufbewahrung	MAT_07
Fehlende Bestandsaufnahme der benutzten Datenträger	MAT_06
Fehlende Datensicherung auf Datenträgern	ORG_08
Leicht transportierbare Datenträger (z. B. herausnehmbare Festplatte, Speicherkassette)	MAT_07
Original-Datenträger	MAT_02 ORG_08
Fehlende Datenschutz-Sicherheitspolitik an den verschiedenen Standorten der Institution	ORG_15 ORG_38
Fehlende Vertragsklauseln über von Unterauftragnehmern und Lieferanten einzuhaltende Sicherheitsmaßnahmen	ORG_38
Die Sicherheitsverantwortungen bezüglich der Klassifizierung von Informationen sind weder formalisiert noch allgemein bekannt	ORG_14 ORG_15
Die Sicherheitspolitik wird nicht angewendet	ORG_18
Fehlende Organisation zur Verwaltung von Sicherheitszwischenfällen	ORG_21
Fehlende Identifizierung sensitiver Güter	ORG_26
Fehlende Kontrolle sensitiver Güter	ORG_04 ORG_15
Fehlende Kontrolle bezüglich der Anwendung der Sicherheitspolitik	ORG_22
Fehlende Identifizierung der Sicherheitsbedürfnisse eines Projekts	ORG_32
Fehlende Datenschutzpolitik	ORG_15
Manipulierbares Personal	PER_02
Nicht-Einhalten der Vorschriften bezüglich der Klassifizierung von Informationen	PER_03
Fehlende Sensibilisierung für den Schutz vertraulicher Unterlagen bewirkt mangelnde Wachsamkeit	PER_02
Verschaffung eines Vorteils bei Verbreitung einer Information	PER_08

Die Anwendung der Sicherheitspolitik wird durch die Direktion nicht gefördert	PER_13
Fehlender persönlicher Einsatz beim Schutz vertraulicher Unterlagen	PER_05
Außerhalb des Standorts vorhandene bzw. weitergereichte Datenträger oder Unterlagen	PER_01
Fehlende Zugangskontrolle zum Standort oder zu den Räumlichkeiten oder Eindringen über indirekte Zugänge möglich	PHY_03

4.1.21 DIEBSTAHL VON BETRIEBSMITTELN

Schwachstelle	Abdeckung
Fehlende Ersatz-Betriebsmittel	MAT_01
Fehlende Materialbestandsaufnahme	MAT_06
Betriebsmittel, das einer Gruppe von Personen frei zugänglich ist	MAT_07
Attraktive Betriebsmittel (Marktwert und technologische und strategische Werte)	MAT_07
Möglichkeit zum Wiederverkauf des Gerätes (Fehlende Markierung, Benutzung ohne Passwort)	MAT_07
Leicht zerlegbares Gerät	MAT_07
Fehlende Sicherheitspolitik zum Schutz der Informationsverarbeitungsinfrastruktur an den verschiedenen Standorten der Institution	ORG_02 ORG_04 ORG_27 ORG_30 ORG_33 ORG_38
Fehlende Vertragsklauseln über von Unterauftragnehmern und Lieferanten einzuhaltende Sicherheitsmaßnahmen	ORG_38
Fehlende Organisation zur Verwaltung und Handhabung von Sicherheitszwischenfällen bei Diebstahl	ORG_21
Fehlende Kontrolle bezüglich der Anwendung der Sicherheitspolitik	ORG_22
Fehlende Kontrollvorschriften für ein- und ausgelieferte Betriebsmittel	ORG_02
Fehlende Identifizierung sensitiver Güter	ORG_26
Fehlende Identifizierung der Sicherheitsbedürfnisse eines Projekts	ORG_32
Die Anwendung der Sicherheitspolitik wird durch die Direktion nicht gefördert	PER_13
Geringe Sensibilisierung für den Schutz der Betriebsmittel außerhalb der Institution	PER_01
Manipulierbares Personal	PER_02
Nicht-Einhalten der physischen Schutzvorschriften für transportfähige Betriebsmittel	PER_01 PER_08
Verschaffung eines Vorteils bei Wiederverkauf eines Gerätes	PER_08
Benutzung von Betriebsmitteln außerhalb der Institution (am Wohnsitz der Mitarbeiter, in einer anderen Institution usw.)	PER_01
Fehlende Zugangskontrolle zum Standort oder zu den Räumlichkeiten oder Eindringen über indirekte Zugänge möglich	PHY_03

4.1.22 ÜBERNAHME RECYCELTER ODER AUSGEMUSTERTER DATENTRÄGER

Schwachstelle	Abdeckung
Vorhandensein von Restdaten der Softwareprogramme	MAT_08
Vorhandensein von Restdaten ohne Wissen des Benutzers auf weitergegebenen oder ausgemusterten Betriebsmitteln	MAT_08
Fehlende Mittel zur Vernichtung von Datenträger	MAT_08
Fehlende Identifizierung sensitiver Güter	ORG_26
Fehlende Kontrolle sensitiver Güter	ORG_04

	ORG_15
Fehlende Kontrolle bezüglich der Anwendung der Sicherheitspolitik	ORG_22
Fehlende Anwendung einer Datenschutzpolitik im Hinblick auf Recycling und Ausmusterung	ORG_15
Fehlende Vertragsklauseln über von Unterauftragnehmern und Lieferanten einzuhaltende Sicherheitsmaßnahmen	ORG_38
Manipulierbares Personal	PER_02
Nicht-Einhalten der Vorschriften zur Vernichtung von Datenträgern mit klassifizierten Informationen	PER_02
Fehlende Aufklärung und Sensibilisierung hinsichtlich der Remanenz von maschinenlesbaren Daten auf den Datenträgern	PER_02
Verschaffung eines Vorteils bei Verbreitung einer Information	PER_08
Die Anwendung der Sicherheitspolitik wird durch die Direktion nicht gefördert	PER_13
Vorhandensein ausgemusterter Datenträger außerhalb des Standorts	ORG_15
Vorhandensein ausgemusterter Datenträger in Räumlichkeiten mit Publikumsverkehr	ORG_15
Vorhandensein ausgemusterter Datenträger in Zonen, die dienstlich nicht betroffenen Personen zugänglich sind	ORG_15

4.1.23 VERBREITUNG

Schwachstelle	Abdeckung
Fehlende Überprüfung der bewilligten Mehrbenutzerzugriffe	LOG_13 MAT_10
Verfahren zur Verwaltung der Zugriffsprivilegien zu schwerfällig zu handhaben	ORG_36
Funktionen zur Verwaltung der Benutzerrechte zu kompliziert in der Anwendung; mögliche Quelle von Fehlern	MAT_11
Vorhandensein eines gemeinsamen Verzeichnisses zur Datenspeicherung	MAT_10
Datenträger zum Austausch sensitiver Informationen befähigt	MAT_10
Fehlen einer verantwortlichen Organisation zur Definition, Vergabe und Kontrolle von Zugriffsprivilegien	ORG_14 ORG_30
Fehlende Identifizierung sensitiver Güter	ORG_26
Die Sicherheitspolitik wird nicht angewendet	ORG_18
Fehlender persönlicher Einsatz zum Schutz der Vertraulichkeit	ORG_37 PER_05
Verfahren zur Verwaltung und Anwendung der Ermächtigungen zu schwerfällig zu handhaben	ORG_36
Die Sicherheitsverantwortungen bezüglich der Klassifizierung von Informationen sind weder formalisiert noch allgemein bekannt	ORG_14 ORG_15
Fehlende Kontrolle sensitiver Güter	ORG_04 ORG_15
Fehlende Datenschutzpolitik	ORG_15
Nicht-Einhalten der Vorschriften zur Klassifizierung der Informationen	PER_03
Die Anwendung der Sicherheitspolitik wird durch die Direktion nicht gefördert	PER_13
Manipulierbares Personal	PER_02
Fehlende Sensibilisierung für den Schutz sensitiver Informationen	PER_03
Nicht-Einhalten der Zurückhaltungspflicht	PER_09
Verschaffung eines Vorteils bei Verbreitung einer Information	PER_08
Fehlende Kontrolle (oder fehlende Protokollierung) des Informationsaustauschs nach außen	PHY_07
Vorhandensein eines Kommunikationsnetzes für den Informationsaustausch nach außen	RES_02

Fichiers d'imputation complexes ou peu ergonomiques	ORG_42
Standardschnittstelle für den Informationsaustausch (z. B. Bluetooth-Schnittstelle mit standardmäßiger Akzeptanz von Kommunikationen aller Art)	RES_02
Möglichkeit zur Benutzung von Betriebsmitteln ohne Hinterlassen von Spuren	RES_03
Fehlende Benachrichtigung der Benutzer	RES_03
Komplexe Leitweglenkung zwischen den Nebennetzen	RES_05
Fehlende straffe Leitweglenkung zwischen den Nebennetzen	RES_05
Fehlende Filterung und Protokollierung an den Kommunikationsrelais zwischen den einzelnen Netzen	RES_02 RES_03
Anschluss des Systems an externe Netzwerk	RES_02
Fehlende Zugriffskontrolle zu den im Unternehmensverzeichnis gespeicherten Informationen	LOG_11
Fehlende Protokollierung der Zugriffe	RES_03
Fehlende Filtereinrichtung	RES_02
Fehlende oder schwierige Verwaltung der Privilegien für den Zugriff auf gemeinsame Informationen (Definition, Vergabe, Kontrolle)	LOG_11
Fehlende Abtrennung der Kommunikationsnetze	RES_02
Fehlende Maßnahmen zur Vermeidung von Nachlässigkeiten beim Senden von Informationen	LOG_17
Das System ist von allen Mitarbeitern benutzbar	LOG_13
Das System kann Informationen im Anhang übermitteln	PER_02
Kein wirksamer und operationeller Anti-Virenschutz	ORG_06
Fehlende Verwaltung der Privilegien für den Zugriff auf Informationen (Möglichkeit der Beeinträchtigung öffentlicher Informationen)	LOG_11
Das System vereinfacht die Verbreitung von Informationen nach außen	PER_02

4.1.24 INFORMATIONEN OHNE HERKUNFTSGARANTIE

Schwachstelle	Abdeckung
Übernahme von Softwareprogrammen über nicht authentifizierte Sammelstellen	LOG_06 LOG_08
Möglichkeit zur Installation von Korrekturmaßnahmen, Updates, Patches, Hotfixes usw.	LOG_03 LOG_08 LOG_11
Fehlende sichere Mittel zur Identifikation	LOG_13
Fehlende Aufbewahrung von Protokolldaten, die Aufschluss über die Aktivitäten geben	LOG_10
Fehlende Vorkehrungen zur Garantie der Herkunft eines Betriebsmittels	ORG_20
Die Verantwortlichen haben keinen Kontakt zu den technologischen Prüf- und Überwachungsdiensten	ORG_34
Fehlende Datenschutz-Sicherheitspolitik an den verschiedenen Standorten der Institution	ORG_15 ORG_38
Fehlende Vorkehrungen zur Garantie der Herkunft gelieferter Waren	ORG_20
Fehlende Kontrolle bezüglich der Anwendung der Sicherheitspolitik	ORG_22
Fehlende Politik zur Aufbewahrung und Analyse aktivitätsspezifischer Protokolldaten	ORG_39
Fehlende Information bezüglich der Aufteilung der Verantwortungen und der Mittel zur Garantie der Berechtigung einer Anfrage	ORG_14
Fehlende Organisation zur garantierten Identifikation einer Person innerhalb der Institution oder eines Projekts	ORG_33
Die Anwendung der Sicherheitspolitik wird durch die Direktion nicht gefördert	PER_13
Fehlende Sensibilisierung für Risiken bei Benutzung einer fremden Identität (falsche	PER_03

Benutzung von Mitteln, die eine Authentifizierung garantieren wie z. B. Passwörter)	
Leichtgläubigkeit	PER_02
Unkenntnis der Bedeutung der Qualifikation einer Information	PER_10
Manipulierbares Personal	PER_02
Konfliktgeladenes soziales Klima	
Verschaffen eines Vorteils bei Fehlinformation	PER_08
Fehlende Mittel zur Garantie der Authentizität von Codes	ORG_20
Fehlende Kenntnis der Sicherheitsmaßnahmen	PER_03 PER_11
Möglichkeit der Beeinträchtigung einer Kommunikation	RES_02
Über das Protokoll kann der Geber einer Kommunikation nicht eindeutig authentifiziert werden	RES_03
Möglichkeit zur Benutzung von Betriebsmitteln ohne Hinterlassen von Spuren	RES_03
Komplexe bzw. wenig ergonomische Dateien	ORG_42
Die Relais identifizieren weder die Quellen noch die Ziele (mögliche Auswirkungen: Anfälligkeit des Systems für Spoofing-Angriffe)	RES_03
Möglichkeit, sich widerrechtlich Funktion des Unternehmensverzeichnisses anzueignen	RES_01
Das System kann den Autor einer Änderung nicht identifizieren	LOG_10
Über die Einrichtung besteht Zugriff auf nicht authentifizierbare Daten (z. B. Hoax)	ORG_12
Das System verfügt über keine Mittel zur Aufbewahrung aktivitätsspezifischer Journale	RES_03
Das System ermöglicht die Speicherung oder Änderung von Informationen ohne Authentifizierung der Autoren	RES_03
Das System ermöglicht das Senden und Empfangen von Informationen ohne Authentifizierung der Sender bzw. Empfänger	RES_03
Das System verfügt über keine Filter zur Verhinderung des Empfangs von außen kommender Falschmeldungen	ORG_12
Das System gestattet die Relayfunktion	RES_01
Das System kann die Person, die eine Anfrage gesendet hat, nicht identifizieren	RES_03

4.1.25 SABOTIEREN DER HARDWARE

Schwachstelle	Abdeckung
Möglichkeit zum Hinzufügen zusätzlicher Hardwarekomponenten zum Speichern, Übertragen oder Manipulieren (z. B. physisches Keyloggen)	MAT_10 RES_01
Fehlende Prozedur zur Kontrolle bei Eingriffen an der Systemausstattung der Institution durch externes Personal	ORG_25
Fehlende Kontrolle bezüglich der Anwendung der Sicherheitspolitik	ORG_22
Fehlende Sicherheitspolitik zum Schutz der Informationsverarbeitungsinfrastruktur an den verschiedenen Standorten der Institution	ORG_02 ORG_04 ORG_27 ORG_30 ORG_33 ORG_38
Die Verantwortlichen haben keinen Kontakt zu den technologischen Prüf- und Überwachungsdiensten	ORG_34
Fehlende Prozeduren zur operationellen Qualifikation	ORG_26
Fehlende Kontrolle sensitiver Güter	ORG_04 ORG_15
Fehlende Identifizierung sensitiver Güter	ORG_26
Fehlende Prozedur zur Validierung der Hardwarekomponenten bei Lieferung oder nach	ORG_20

Instandsetzung	
Unzureichende Abnahmeprüfung der Software, insbesondere hinsichtlich der Grenzwerte	ORG_26
Manipulierbares Personal	PER_02
Fehlende Wachsamkeit bei Eingriff eines Wartungstechnikers an einer Arbeitsstation oder am Server	PER_05
Geringe Sensibilisierung für den Schutz von Betriebsmitteln außerhalb der Institution	PER_01
Verschaffen eines Vorteils bei Fehlinformation	PER_08
Benutzung von Betriebsmitteln außerhalb der Institution (am Wohnsitz der Mitarbeiter, in einer anderen Institution usw.)	PER_01
Fehlende Zugangskontrolle zum Standort oder zu den Räumlichkeiten oder Eindringen über indirekte Zugänge möglich	PHY_03
Möglichkeit zur Installation einer Leitungsabzweigung	RES_01

4.1.26 SABOTIEREN DER SOFTWARE

Schwachstelle	Abdeckung
Die Hotline zur Telewartung ist permanent aktiviert	LOG_12 RES_06
Möglichkeit des Vorhandenseins versteckter Funktionen, die während der Entwurfs- oder Entwicklungsphase eingeschleust wurden	ORG_20 ORG_38
Möglichkeit zur Änderung oder Manipulation der Software	LOG_01
Fehlender Schutz gegen den Gebrauch fortgeschrittener Zugriffsprivilegien	LOG_11
Benutzung ungeprüfter Softwareprogramme	LOG_06
Fehlender Einsatz von Basis-Sicherheitsregeln, die bezüglich des Betriebssystems und der Softwareprogramme anzuwenden sind	LOG_04
Möglichkeit zur Erzeugung oder Änderung von Systembefehlen	LOG_08 LOG_11
Übernahme von Softwareprogrammen über nicht authentifizierte Sammelstellen	LOG_06 LOG_08
Möglichkeit zur Systemadministration aus der Entfernung mit nicht verschlüsselten Administrationstools	RES_02
Unzureichende Komplexität der Zugangspasswörter	ORG_10
Möglichkeit zur Installation von Korrekturmaßnahmen, Updates, Patches, Hotfixes usw.	LOG_03 LOG_08 LOG_11
Möglichkeit zur Fern-Systemadministration von jeder beliebigen Arbeitsstation aus	RES_01 RES_06
Benutzung eines Standard-Betriebssystems, auf das bereits Softwareangriffe durchgeführt wurden	LOG_06
Möglichkeit zur Fern-Systemadministration von jeder beliebigen Arbeitsstation aus	LOG_11
Möglichkeit zum Löschen, Ändern oder Installieren neuer Programme	LOG_08
Die SNMP-Schicht ist aktiviert	LOG_12 RES_06
Die Hardware kann von jedermann von einem beliebigen Peripheriegerät aus gebootet werden (z. B. Diskette, CD-ROM)	MAT_10
Fehlende Mittel zur Kontrolle der Unschädlichkeit von Datenträgern beim Eintreffen in der Institution	ORG_06
Fehlende Sicherheitspolitik zum Schutz der Informationsverarbeitungsinfrastruktur an den verschiedenen Standorten der Institution	ORG_02 ORG_04 ORG_27 ORG_30

	ORG_33 ORG_38
Die Verantwortlichen haben keinen Kontakt zu den technologischen Prüf- und Überwachungsdiensten	ORG_34
Fehlende Prozedur zur Kontrolle bei Eingriffen an der Systemausstattung der Institution durch externes Personal	ORG_25
Fehlende Vertragsklauseln über die Unschädlichkeitsgarantie von Lieferungen durch Unterauftragnehmer oder Lieferanten	ORG_20 ORG_38
Fehlende Globalpolitik zum Kampf gegen maligne Codes	ORG_06
Fehlende Identifizierung sensitiver Güter	ORG_26
Fehlende Kontrolle bezüglich der Anwendung der Sicherheitspolitik	ORG_22
Fehlende Kontrolle sensitiver Güter	ORG_04 ORG_15
Fehlende Politik zum Schutze der Arbeitsstationen	ORG_04 ORG_06
Fehlende Politik zur Aufbewahrung und Analyse aktivitätsspezifischer Protokolldaten	ORG_39
Fehlende Maßnahmen zur Kontrolle der Entwicklungen	ORG_20
Fehlende Maßnahmen zum Schutze der Integrität von Codes während der Entwurfs-, Installations- und Betriebsphasen	ORG_04 ORG_20
Benutzung von Softwareprogrammen ohne Herkunftsgarantie	PER_10
Konfliktgeladenes soziales Klima	
Fehlende Sensibilisierung für maligne Codes	PER_03
Unkenntnis der anzuwendenden Reflexe bei Detektion einer Anomalie	PER_11
Nicht-Einhalten der Vorschriften zur Aktualisierung der Anti-Virenprogramme	PER_03
Manipulierbares Personal	PER_02
Verschaffung eines Vorteils bei Störung des IT-Systems	PER_08
Konfliktgeladenes Klima	
Fehlende Kenntnis der Sicherheitsmaßnahmen	PER_03 PER_11
Fehlende Mittel zur Garantie der Authentizität von Entwicklungen	ORG_20
Betreiber oder Inhaber verfügen über erweiterte Zugriffsprivilegien	PER_02
Unkenntnis der einzuleitenden Prozeduren bei Detektion einer Anomalie	PER_03
Benutzung von Betriebsmitteln außerhalb der Institution (am Wohnsitz der Mitarbeiter, in einer anderen Institution usw.)	PER_01
Fehlende Zugangskontrolle zum Standort oder zu den Räumlichkeiten oder Eindringen über indirekte Zugänge möglich	PHY_03
Das Netzwerk vereinfacht die Nutzung von Ressourcen durch Unbefugte	RES_01
Komplexe bzw. wenig ergonomische Dateien	ORG_42
Möglichkeit zum Hinzufügen von Softwareabzweigungen	RES_01
Das Netzwerk lässt es zu, Systemressourcen zu ändern oder auf sie einzuwirken	RES_01
Möglichkeit zum Hinzufügen zusätzlicher Softwarekomponenten zum Speichern, Übertragen oder Manipulieren (z. B. Keyloggen)	RES_01
Möglichkeit zur Benutzung von Betriebsmitteln ohne Hinterlassen von Spuren	RES_03
Möglichkeit zur Änderung bzw. zum Austausch von Anwendungsprogrammen	LOG_11
Möglichkeit zum Löschen oder Ändern von Systemprogrammen oder -dateien	LOG_11
Fehlende Sensibilisierung für die Risiken beim Herunterladen von Softwareprogrammen	PER_03
Fehlende Antivirenkontrolle beim Informationsaustausch	ORG_06
Die Einrichtung ermöglicht eine Ausnutzung des Asynchronbetriebs bestimmter Bereiche	LOG_04

oder Befehle des Betriebssystems (z. B. Javascript-Komponenten zur Erkundung des Inhalts der Festplatte)	LOG_11
Vorhandene Einrichtung zur Änderung oder Installation von Anwendungen aus der Entfernung	LOG_11
Gemeinsam genutzter Speicherplatz	LOG_11
Verwendung einer veralteten Version des Mailboxservers	LOG_09 ORG_13
Verwendung einer Verteilungsliste, auf der eine Großteil aller Mitarbeiter verzeichnet ist	ORG_12
Verwendung eines Protokolls ohne Authentifizierungsfunktion	RES_03
Möglichkeit zum automatischen Versenden von Mitteilungen	LOG_14 ORG_06
Fehlende Sensibilisierung für die Risiken beim Versand von Anhängen	PER_03
Die Mailfunktion ermöglicht eine Ausnutzung des Asynchronbetriebs bestimmter Bereiche oder Befehle des Betriebssystems (z. B. automatischer Start von Anhängen)	LOG_04
Fehlende Überprüfung der Anwendungsprogramme vor der Installation	LOG_06
Über die Mailfunktion können Software-Updates installiert werden (z. B. Patches, Antivirenprogramme usw.)	LOG_11
Fehlende Mittel zur Antivirenfilterung	ORG_06
Möglichkeit zur Installation von Piratenprogrammen	LOG_11

4.1.27 GEOLOKALISATION

Schwachstelle	Abdeckung
Lokalisierbares Material (z. B. Triangulation)	PHY_05
Fehlende Datenschutz-Sicherheitspolitik an den verschiedenen Standorten der Institution	ORG_15 ORG_38
Fehlende Schutzvorschriften hinsichtlich der Vertraulichkeit von Informationen, die zur Lokalisierung von Mitarbeitern genutzt werden könnten (Auskünfte über Tickets, Verzeichnis über Ein- und Ausgänge usw.)	ORG_15
Fehlende Kenntnis der Sicherheitsmaßnahmen	PER_03 PER_11
Fehlende Zurückhaltung und Wachsamkeit	PER_09
Die Anwendung der Sicherheitspolitik wird durch die Direktion nicht gefördert	PER_13

4.1.28 AUSFALL VON BETRIEBSMITTELN

Schwachstelle	Abdeckung
Fehlende Diagnosefunktion zur Vorbeugung gegen den Ausfall von Betriebsmitteln	LOG_14
Fehlender Schutz gegen elektrische Störungen	PHY_03
Schlechte Nutzungsbedingungen	MAT_14
Wartungsfehler	ORG_27
Schlechte Zuverlässigkeit der Betriebsmittel	MAT_15
Veralterung des Materials	ORG_13
Datenträger nicht an die Lebensdauer der zu archivierenden Daten angepasst	MAT_03 MAT_04
Schlechte Lagerungsbedingungen	PHY_03
Fehlende Klausel über die Fristen zum Eingreifen oder Austauschen bei Ausfall eines Betriebsmittels	ORG_38
Fehlende Organisation zur Aktualisierung der Wartungsverträge	ORG_27
Fehlende Aktualisierung der Wartungs- und Unterstützungsverträge mit den Lieferanten	ORG_27

Fehlendes Ausfallreporting (Volumen, Kosten der Zwischenfälle, Dauer)	ORG_21
Fehlende Vorschriften über die Anwendungsbedingungen der Infrastrukturen zur Informationsverarbeitung (in Räumlichkeiten mit IT-Material ist Rauchen, Essen und Trinken verboten)	ORG_04 PHY_08
Fehlender Plan zur Wiederaufnahme der wesentlichen Aktivitäten innerhalb der Institution	ORG_16
Fehlende Anweisungen über Sofortmaßnahmen zum Schutz der Betriebsmittel bei Wasserschäden oder Brand	ORG_24
Fehlende Organisation einer Analyse, ob die Kapazitäten der Betriebsmittel den Bedürfnissen angepasst sind	ORG_09
Fehlende Vorschriften über die Anwendungsbedingungen der Infrastrukturen zur Informationsverarbeitung (in Räumlichkeiten mit IT-Material ist Rauchen, Essen und Trinken verboten)	
Fehlende Weiterverfolgung der Zwischenfälle zur Verhinderung eventueller Ausfälle oder Überlastungen (Kontrollschemen)	PER_05
Keine Informationsweitergabe zur Gewährleistung einer zentralisierten Ausfallanalyse	PER_05
Unkenntnis der Anwendungsvorschriften der Betriebsmittel	PER_03
Fehlende Berücksichtigung der spezifischen, das Fehler- und Ausfallrisiko erhöhenden Umgebung (überhitzte Atmosphäre, industrielle Umgebung usw.)	PHY_10
Fehlende Funktionsprüfung der Ersatz-Betriebsmittel	ORG_16
Manuelles Auslösen der Notlösung	ORG_16
Schlechte Zuverlässigkeit der Informationsträger	MAT_15
Veralterung des Informationsträgers	ORG_13

4.1.29 FEHLERHAFTER BETRIEB VON BETRIEBSMITTELN

Schwachstelle	Abdeckung
Fehlende Diagnosefunktion zur Vorbeugung von Ausfällen der Betriebsmittel	LOG_14
Fehlender Schutz gegen elektrische Störungen	PHY_03
Schlechte Nutzungsbedingungen	MAT_14
Schlechte Zuverlässigkeit der Betriebsmittel	MAT_15
Mögliche Inkompatibilität zwischen den einzelnen Betriebsmitteln	RES_04
Datenträger nicht an die Lebensdauer der zu archivierenden Daten angepasst	MAT_03 MAT_04
Schlechte Lagerungsbedingungen	PHY_03
Fehlende Weiterverfolgung der Zwischenfälle zur Verhinderung eventueller Ausfälle oder Überlastungen (Kontrollschemen)	ORG_09
Fehlende Vorschriften über die Anwendungspflicht von Normen	ORG_04
Fehlende Klausel über die Fristen zum Eingreifen oder Austauschen bei fehlerhaftem Betrieb eines Betriebsmittels	ORG_38
Fehlendes Fehlerreporting	ORG_21
Fehlender Plan zur Wiederaufnahme der wesentlichen Aktivitäten innerhalb der Institution	ORG_16
Fehlende Prozeduren zur operationellen Qualifikation	ORG_26
Fehlende Vorschriften über die Betriebsumgebung der Infrastrukturen zur Informationsverarbeitung (Temperatur, Hygrometrie usw.)	ORG_04 PHY_10
Fehlende Organisation einer Analyse, ob die Kapazitäten der Betriebsmittel den Bedürfnissen angepasst sind	ORG_09
Fehlende Weiterverfolgung der Zwischenfälle zur Verhinderung eventueller Ausfälle oder Überlastungen (Kontrollschemen)	PER_05

Unkenntnis der Anwendungsvorschriften der Betriebsmittel	PER_03
Keine Informationsweitergabe zur Gewährleistung einer zentralisierten Ausfallanalyse	PER_05
Fehlende Berücksichtigung der spezifischen, das Fehler- und Ausfallrisiko erhöhenden Umgebung (überhitzte Atmosphäre, industrielle Umgebung usw.)	PHY_10
Fehlende Funktionsprüfung der Ersatz-Betriebsmittel	ORG_16
Manuelles Auslösen der Notlösung	ORG_16
Veralterung des Informationsträgers	ORG_13
Mögliche Inkompatibilität zwischen den Informationsträgern und anderen Komponenten	RES_04
Medien und Informationsträger enthalten technische Merkmale, die sie lokalisierbar machen (z. B. verschiedene ADSl-Konfigurationsparameter zwischen Frankreich und Großbritannien)	RES_04
Schlechte Zuverlässigkeit der Informationsträger	MAT_15
Wartungsfehler	ORG_27
Schnittstelle enthält landesspezifische technische Merkmale (z. B. verschiedene Telefonsteckertypen zwischen Frankreich und Großbritannien)	RES_04
Möglichkeit zur fehlerhaften Konfiguration, Installation oder Modifikation der Relais	RES_04
Veralterung des Materials	ORG_13
Mögliche Inkompatibilität zwischen den einzelnen Betriebsmitteln	RES_04

4.1.30 ÜBERLASTUNG DES INFORMATIONSSYSTEMS

Schwachstelle	Abdeckung
Fehlender Filter zum Schutz des Systems gegen Überlauf	LOG_14
Unnötiger Einsatz von Betriebsmitteln	LOG_14
Anwendung erfordert IT-Ressourcen, die der Hardware nicht angepasst ist (z. B. unzureichender Arbeitsspeicher)	MAT_09
Bei Definition der Projektanforderungen fehlende Berücksichtigung von Ausnahmesituationen, bei denen das System die Grenzbedingungen erreicht	LOG_14
Fehlende Qualifikation der Entwicklungen in einem betriebsähnlichen Kontext	LOG_06
Schlechte Dimensionierung der Ressourcen (z. B. unzureichende Autonomie einer Laptop-Batterie)	MAT_09
Unerwünschtes Fortbestehen von Daten auf den Datenträgern	ORG_09
Fehlende Vorschriften über die Anwendungspflicht von Normen	ORG_04
Fehlende Weiterverfolgung der Zwischenfälle zur Verhinderung eventueller Ausfälle oder Überlastungen (Kontrollschemen)	ORG_09
Fehlende Vertragsklausel über die Qualität der von den Systemen am Rande der Grenzbedingungen zu erbringenden Dienste (intensive Inanspruchnahme des Systems, Eingabe nicht konformer Daten, Dateneingabe bei extremen Betriebsbedingungen)	ORG_38
Fehlende Politik zur Nachkontrolle der angemessenen Dimensionierung der Informationsverarbeitungsinfrastruktur einschließlich der Ersatz-Betriebsmittel	ORG_09
Fehlende Anweisungen bezüglich der korrekten Benutzung der IT-Ressourcen zur Vermeidung von Verhalten, die eine Überlastung der Speicherkapazitäten oder Verarbeitungsressourcen hervorrufen	ORG_09
Fehlende Anweisungen zum Verhalten bei Zwischenfällen (Detektion, Aktion usw.)	ORG_24
Fehlende Entscheidung zur Neudimensionierung bei Erkennung einer signifikanten Erhöhung der Inanspruchnahme der IT-Ressourcen	PER_05
Fehlende Weiterverfolgung der Zwischenfälle zur Verhinderung eventueller Ausfälle oder Überlastungen (Kontrollschemen)	PER_05
Ausbildungsmangel hinsichtlich der korrekten Anwendung der IT-Mittel (Störung des Systems, Installation nicht kompatibler Software usw.)	PER_03 PER_12

Verschaffung eines Vorteils bei Störung des IT-Systems	PER_08
Fehlende Sensibilisierung für das Bedürfnis, mit den IT-Ressourcen der Institution sparsam umzugehen (schlechte Nutzung des Speicherplatzes u. ä.)	PER_03
Schlechte Dimensionierung z. B der Telekom-Ressourcen, indem täglich auch die Ressourcen benutzt werden, die als Reservelösung vorgesehen sind	ORG_16
Schlechte Dimensionierung der Reserve-Ressourcen	ORG_16
Möglicherweise sind die Relais einer zu großen Anzahl an Anfragen oder einer intensiven Störung ausgesetzt (z. B. Denial-of-service-Attacke vom Typ "smurf" oder "SYN flood")	LOG_14 MAT_05
Möglichkeit zur fehlerhaften Konfiguration, Installation oder Modifikation der Relais	RES_04
Schlechte Dimensionierung (z. B. zu viele Daten bezogen auf die maximale Bandbreite)	RES_02
Schlechte Dimensionierung der Ressourcen (z. B. zu viele Benutzer bezogen auf die maximale Kapazität des Verzeichnisses)	ORG_09
Möglichkeit, die Einrichtung einer zu großen Anzahl an Anfragen ohne Beschränkung auszusetzen	ORG_09
Vorhandensein eines Zeitraums oder eines Ereignisses mit ausgesprochen signifikanter Erhöhung der Inanspruchnahme des Systems	ORG_09
Schlechte Dimensionierung der Ressourcen (z. B. zu viele gleichzeitige Anschaltungen)	ORG_09
Fehlende Verwaltung der Schreibzugriffsrechte auf gemeinsame Speicherbereiche	LOG_11
Schlechte Dimensionierung der Betriebs- oder Wartungs-Ressourcen	ORG_09
Fehlende Abtrennung der Kommunikationsnetze	RES_02
Benutzung interner Verteilungslisten, die allen zugänglich sind	ORG_12
Schlechte Dimensionierung der Speicherbereiche für erhaltene Mitteilungen	ORG_09
Möglichkeit zum automatischen Versenden von Mitteilungen	LOG_14 ORG_06
Fehlender Spam-Schutz	ORG_12
Fehlende Größenbegrenzung der Anhänge	LOG_14
Schlechte Benutzungsgewohnheiten des Nachrichtenübermittlungsdienstes durch die Benutzer (Benutzung der Mailboxen als Archivierbereich)	PER_03
Publikumszugang zum Portal	ORG_09
Schlechte Dimensionierung der Ressourcen (z. B. zu viele gleichzeitige Anschaltungen)	ORG_09

4.1.31 FEHLERHAFTER BETRIEB VON SOFTWAREPROGRAMMEN

Schwachstelle	Abdeckung
Mögliche Seiteneffekte infolge der Aktualisierung einer Softwarekomponente	LOG_02
Fehlende Aufbewahrung von Protokolldaten, die Aufschluss über die Verarbeitungen geben	LOG_10
Fehlende Schulung bezüglich der Nutzung oder Wartung neuer Softwareprogramme	ORG_14 PER_06 PER_12
Fehlende Wartungsprozedur	LOG_09 ORG_41
Fehlende Qualifikationsprozedur vor Installation oder Aktualisierung	LOG_06
Fehlende Prozedur zur Synchronisierung der Zeitgeber	LOG_10
Keine Informationsweitergabe zur Gewährleistung einer zentralisierten Bearbeitung von Betriebsstörungen	LOG_15
Möglichkeit zur fehlerhaften Konfiguration, Installation oder Modifikation des Betriebssystems	LOG_04
Fehlende Protokollierung der Wartungsoperationen	LOG_03

	LOG_08
Fehlende oder fehlerhafte Konfigurationsverwaltung der Softwarekomponenten (z. B. Benutzung eines UK-Patches, der für die französische Version nicht angemessen ist)	LOG_08
Die Unterlagen sind nicht auf neuestem Stand	ORG_28
Fehlende Überprüfung der Anwendungsprogramme vor der Installation	LOG_06
Verwendung einer veralteten Version des Betriebssystems oder der Anwendungsprogramme	LOG_09 ORG_13
Fehlende Vorschriften über die Anwendungspflicht von Normen	ORG_04
Fehlende Weiterverfolgung der Zwischenfälle zur Verhinderung eventueller Ausfälle oder Überlastungen (Kontrollschemen)	ORG_09
Fehlende Vertragsklauseln bezüglich der Unterstützungs- und Eingriffsbedingungen	ORG_38
Fehlende Politik zur räumlichen Abtrennung von Benutzerumgebungen, um eine Autorisierung von Berechtigungen zur Änderung von Systemen oder Anwendungen zu vermeiden	ORG_33
Fehlende Anweisungen bezüglich der korrekten Benutzung der IT-Ressourcen zur Vermeidung risikoträchtigen Verhaltens	ORG_04
Fehlende Anweisungen zum Verhalten bei Zwischenfällen (Detektion, Aktion usw.)	ORG_24
Fehlender Plan zur Wiederaufnahme der wesentlichen Aktivitäten innerhalb der Institution	ORG_16
Fehlende Homogenität der IT-Ausstattung	ORG_42
Unzureichende Abnahmeprüfung der Software (die Testserien decken nicht alle Betriebsbedingungen ab – intensive Inanspruchnahme des Systems, Eingabe nicht konformer Daten, Dateneingabe bei extremen Betriebsbedingungen)	ORG_26
Fehlende Weiterverfolgung der Zwischenfälle zur Verhinderung eventueller Betriebsstörungen (Kontrollschemen)	PER_05
Fehlende Schulung	PER_12
Fehlende Sicherheitsvorschriften bei den Entwicklungen	PER_10
Ausbildungsmangel hinsichtlich Wartung und Betrieb neuer Betriebsmittel	PER_12
Schlechte Dimensionierung der Betriebs- oder Wartungs-Ressourcen	ORG_09
Nicht-Einhalten der einzuleitenden Eingriffsprozeduren	PER_03
Ausbildungsmangel hinsichtlich der korrekten Anwendung der IT-Mittel (Störung des Systems, Installation nicht kompatibler Software usw.)	PER_03 PER_12
Möglichkeit zur fehlerhaften Konfiguration, Installation oder Modifikation der Relais	RES_04
Schlechte Verwaltung der einzelnen Versionen und der Driverkonfigurationen	RES_04
Seiteneffekte der Schnittstellen (z. B Kompatibilitätsprobleme zwischen den einzelnen Protokollen)	RES_04
Möglicherweise wird die Einrichtung mit unkorrekten Anfragen bzw. Daten konfrontiert (z. B. Buffer overflow, Dienstverweigerung am LDAP-Server, SMTP, POP3, IMAP)	LOG_14
Nicht-Einhalten der Installations- oder Wartungsprozeduren	ORG_04
Möglichkeit, die Einrichtung einer zu großen Anzahl an Anfragen ohne Beschränkung auszusetzen	ORG_09
Inkompatibilität der Softwareprogramme (z. B. Seiteneffekt eines Antivirenprogramms zur Filterung der Nachrichten)	RES_04
Möglicherweise wird die Einrichtung mit unkorrekten Anfragen bzw. Daten konfrontiert (z. B. Buffer overflow, Dienstverweigerung am LDAP-Server, SMTP, POP3, IMAP)	LOG_14
Verwendung einer veralteten Version des Mailboxservers	LOG_09 ORG_13

4.1.32 BEEINTRÄCHTIGUNG DER WARTBARKEIT DES INFORMATIONSSYSTEMS

Schwachstelle	Abdeckung
Fehlende Überprüfung der Anwendungsprogramme vor der Installation	LOG_06
Fehlende Ersatzprozedur bei Notfällen	ORG_24
Fehlende Prozedur zum Rücksetzen im Fall einer Anomalie infolge einer Modifikation	LOG_02
Fehlende Wartungsprozedur	LOG_09 ORG_41
Die Unterlagen sind nicht auf neuestem Stand	ORG_28
Fehlende Protokollierung der Wartungsoperationen	LOG_03 LOG_08
Fehlende Aufbewahrung von Protokolldaten, die Aufschluss über die Bearbeitungen und Modifikationen geben	LOG_03
Spezifische Softwareprogramme	ORG_09
Fehlende Schulung bezüglich der Nutzung oder Wartung neuer Softwareprogramme	ORG_14 PER_06 PER_12
Veraltete Softwareprogramme	LOG_09
Softwareprogramme ohne weiterentwicklungsfähige Konfigurationen	LOG_06
Von außen (außerhalb der Institution) oder vom Ausland (Länder mit großem Zeitunterschied) nicht zugängliche Unterstützungsmittel	MAT_13
Hardware ohne weiterentwicklungsfähige Konfigurationen	ORG_13
Veraltete Betriebsmittel	ORG_13
Spezifische Hardware	ORG_09 ORG_27
Änderung der Betriebsmittel, Softwareprogramme oder Speicherprozeduren ohne Berücksichtigung der alten Abspeicherungen oder Archivierungen	ORG_05
Veralteter Datenträger	ORG_13
Verlust oder schlechte Verwaltung von Original-Unterlagen (Unterstützungsverträge, Lizenzen usw.)	ORG_08
Fehlende Sicherheitspolitik zum Schutz der Informationsverarbeitungsinfrastruktur an den verschiedenen Standorten der Institution	ORG_02 ORG_04 ORG_27 ORG_30 ORG_33 ORG_38
Fehlende Vertragsklausel zur Sicherstellung der Aktivität (bei Einstellen der Aktivität, bei Konkurs eines Lieferanten usw.)	ORG_38
Fehlende Garantie hinsichtlich der Beständigkeit der Institution	ORG_27
Fehlende Aktualisierung der Wartungs- und Unterstützungsverträge mit den Lieferanten	ORG_27
Fehlende Anweisungen zum Verhalten bei Zwischenfällen (Detektion, Aktion usw.)	ORG_24
Fehlendes Qualitätssicherungshandbuch	ORG_29
Fehlende Organisation zum Schutz der Systemunterlagen und -Wartungsmittel	ORG_30
Fehlender Plan zur Wiederaufnahme der wesentlichen Aktivitäten innerhalb der Institution	ORG_16
Fehlende Prozeduren zur Verwaltung der Systemkonfigurationen	LOG_08
Nicht-Beachtung der Normen oder Standards bei Entwicklung des Informationssystems	ORG_04 ORG_04
Fehlender Ausbildungsplan bezüglich der Wartung neuer Systeme	ORG_14
Auswahl von Technologien ohne Gewährleistung ihrer Beständigkeit	ORG_13

Geringes Wartungsbudget	PER_13
Vorhandensein veralteter Komponenten innerhalb der Informationsverarbeitungsinfrastruktur (Entwicklungen in nicht mehr benutzten Programmiersprachen)	ORG_13
Nicht-Einhalten der Qualitätsvorschriften	PER_10
Fehlende Standards oder Normen	PER_10
Nicht-Einhalten der Entwicklungsvorschriften	PER_10
Ausbildungsmangel hinsichtlich der korrekten Anwendung der IT-Mittel (Störung des Systems, Installation nicht kompatibler Software usw.)	PER_03 PER_12
Benutzung von Softwareprogrammen oder Entwicklungen, die nicht den Institutionsnormen und -standards entsprechen	PER_10
Wartungsfehler	ORG_27
Fehlender Verkabelungsplan	PHY_11
Wartung oder Betrieb der Betriebsmittel erfordert die Verfügbarkeit der Netzunterstützungen	RES_02
Wartung oder Betrieb des Systems erfolgt über das Netz	RES_02
Fehlende Höchstfristen bei der Unterstützungsgarantie	MAT_04
Verwendung einer veralteten Version des Betriebssystems oder der Anwendungsprogramme	LOG_09 ORG_13
Verwendung einer veralteten Version des Mailboxservers	LOG_09 ORG_13
Verwendung eines veralteten Systems	LOG_09
Verwendung eines nicht standardmäßigen Systems	ORG_28
Fehlende Nachkontrolle der Installations- und Wartungsprozeduren (Konfigurations- und Parametrierhefte)	ORG_04
Fehlendes internes Unterstützungsmittel	ORG_27

4.1.33 UNZULÄSSIGE BENUTZUNG DER BETRIEBSMITTEL

Schwachstelle	Abdeckung
Fehlende Verwaltung der Lizenzen und der Eintragungs- bzw. Aktiviereinrichtung	LOG_07
Möglichkeit zur Benutzung einer Backdoor oder eines Trojanischen Pferdes im Betriebssystem	LOG_08 LOG_13
Gemeinsame Nutzung der Benutzeridentifikation	LOG_11
Durch die gemeinsame Nutzung der Ressourcen wird der Systemzugriff durch Unbefugte vereinfacht	LOG_12
Anschluss des Betriebsmittels an externe Netzwerke	MAT_10
Das verwendete Betriebsmittel kann zu anderen, ursprünglich nicht vorgesehenen Zwecken eingesetzt werden (z. B. Entwicklung von Software, die nicht für die Institution bestimmt ist)	LOG_11 PER_03
Datenträger allgemein zugänglich	MAT_07 ORG_15 ORG_30
In der Betriebsordnung werden mit keinem Thema die Sicherheitsverantwortungen im Hinblick auf die Informationssysteme angesprochen	ORG_14
Fehlende Sicherheitspolitik zum Schutz der Informationsverarbeitungsinfrastruktur an den verschiedenen Standorten der Institution	ORG_02 ORG_04 ORG_27 ORG_30 ORG_33 ORG_38
Die Verantwortlichen haben keinen Kontakt zu den technologischen Prüf- und	ORG_34

Überwachungsdiensten	
Fehlende Sensibilisierung über die Risiken von Sanktionen	ORG_37 PER_08
Fehlende Vertragsklauseln über die Benutzung von IT-Material	ORG_04
Fehlende Anweisungen hinsichtlich der Benutzung von IT-Material	ORG_04
Möglichkeit zur freien Benutzung der Ressourcen der Institution (Selbstbedienung)	LOG_11 ORG_33
Fehlende Überwachungsprozedur	ORG_33
Die Sicherheitspolitik wird nicht angewendet	ORG_18
Fehlende Informatik-Charta, in der die Benutzungsanforderungen definiert werden	ORG_04 PER_03
Fehlende Kenntnis der Sicherheitsmaßnahmen	PER_03 PER_11
Fehlende Sensibilisierung des Personals über die Risiken von Sanktionen	PER_08
Die zugestandenen Rechte gehen über den gerechtfertigten Bedarf hinaus	PER_07
Verschaffung eines Vorteils	PER_08
Nicht-Einhalten der Informatik-Charta, in der die Benutzungsanforderungen definiert werden	PER_03
Fehlende Kontrolle der materiellen Bedürfnisse bei Entwicklung einer Anwendung	ORG_32
Fehlende moralische oder ethische Vorschriften	PER_08
Fehlende Verwaltung des Betriebsmittelausstattung	PER_05
Fehlende Prozeduren zur Kontrolle der Ermächtigungen beim Zugang des Personals zum Standort oder zu den Räumlichkeiten	PHY_07
Fehlende Prozeduren zur Identitätskontrolle beim Zugang von Personen zu den Räumlichkeiten oder Zonen	PHY_07
Fehlende Protokollierung der Personenzugänge	PHY_07
Fehlende Sicherung der Kommunikationsleitungen und -ausstattung	PHY_07
Die Systemausstattung ermöglicht eine Benutzung der Systemressourcen von außen	RES_01
Die Systemausstattung ist allgemein zugänglich	RES_01
Die Systemausstattung ist an externe Netzwerke angeschlossen	RES_01
Die Systemausstattung kann für andere Zwecke benutzt werden als ursprünglich vorgesehen	RES_06
Die jeweilige Einrichtung kann für andere Zwecke benutzt werden als ursprünglich vorgesehen	PER_03
Fehlende Auditierung bzw. Überwachung der Zugänge (v. a. Bestandsaufnahme der Zugänge von außen in die Institution und Typologie der Personenströme)	ORG_22
Fehlende Zugangsvorschriften	LOG_11
Anschluss der Einrichtung an externe Netzwerke	RES_01 RES_03
Die Einrichtung ist allgemein zugänglich	LOG_11 ORG_01

4.1.34 BETRÜGERISCHE KOPIE VON SOFTWAREPROGRAMMEN

Schwachstelle	Abdeckung
Fehlende Verwaltung der Zugriffsprivilegien der einzelnen Profile (Administratoren, Anwender, Gäste usw.)	LOG_11 LOG_11
Fehlende Verwaltung der Lizenzen und der Eintragungs- oder Aktiviereinrichtung	LOG_07
Attraktive Softwareprogramme oder Programme für ein breites Publikum	ORG_04
Möglichkeit zur problemlosen Kopie von Softwareprogrammen oder Programmpaketen	ORG_04

Möglichkeit zur problemlosen Kopie von betriebssytemeigenen Distributionen	ORG_04
Attraktives Betriebssystem oder Betriebssystem für ein breites Publikum	ORG_04
Hardware zur Aufzeichnung von Daten auf Datenträgern (Diskette, ZIP, CD/DVD-Brenner)	
Hardware zur Aufzeichnung von Daten auf Datenträgern (Diskette, ZIP, CD-ROM/DVD-Brenner)	ORG_15
Fehlende Informationen über die für die Informationsverarbeitung spezifischen Gesetze und Vorschriften	ORG_40 ORG_41
In der Betriebsordnung werden mit keinem Thema die Sicherheitsverantwortungen im Hinblick auf die Informationssysteme angesprochen	ORG_14
Fehlende, an den Standorten der Institution vorgeschriebene Politik zur Kontrolle der Lizenzen	LOG_07 ORG_38
Fehlende Vertragsklausel über die Benutzung von betrügerischen Softwarekopien	ORG_38 ORG_40
Fehlende Informatik-Charta, in der die Benutzungsanforderungen definiert werden	ORG_04 PER_03
Fehlende Sensibilisierung über die Risiken von Sanktionen	ORG_37 PER_08
Fehlende Sensibilisierung oder Aufklärung über die Gesetzgebung hinsichtlich der Urheberrechte	ORG_40 ORG_41
Fehlende Überwachungsprozedur	ORG_33
Die Sicherheitspolitik wird nicht angewendet	ORG_18
Die Anwendung der Sicherheitspolitik wird durch die Direktion nicht gefördert	PER_13
Fehlende Kenntnis der Sicherheitsmaßnahmen	PER_03 PER_11
Verschaffung eines Vorteils	PER_08
Nicht-Einhalten der Informatik-Charta, in der die Benutzungsanforderungen definiert werden	PER_03
Fehlende Sensibilisierung des Personals über die Risiken von Sanktionen	PER_08
Fehlende Prozeduren zur Identitätskontrolle beim Zugang von Personen zu den Räumlichkeiten oder Zonen	PHY_07
Fehlende Prozeduren zur Kontrolle der Ermächtigungen beim Zugang des Personals zum Standort oder zu den Räumlichkeiten	PHY_07
Fehlende Protokollierung der Personenzugänge	PHY_07
Fehlende Herkunftskontrolle der Anwendungsprogramme vor der Installation	ORG_20
Die Zugangseinrichtung ermöglicht die Speicherung von Softwareprogrammen	RES_01
Die Zugangseinrichtung ermöglicht das Herunterladen von Softwareprogrammen	RES_01

4.1.35 BENUTZUNG GEFÄLSCHTER ODER KOPIERTER SOFTWAREPROGRAMME

Schwachstelle	Abdeckung
Fehlende Verwaltung der Lizenzen und der Eintragungs- bzw. Aktiviereinrichtung	LOG_07
Möglichkeit zur problemlosen Kopie von Softwareprogrammen oder Programmpaketen	ORG_04
Attraktive Softwareprogramme oder Programme für ein breites Publikum	ORG_04
Möglicherweise funktionieren die Systeme mit unzulässig kopierten oder gefälschten Betriebssystemen	LOG_07 LOG_08 ORG_04
In der Betriebsordnung werden mit keinem Thema die Sicherheitsverantwortungen im Hinblick auf die Informationssysteme angesprochen	ORG_14
Fehlende, an den Standorten der Institution vorgeschriebene Politik zur Kontrolle der	LOG_07

Lizenzen	ORG_38
Fehlende Vertragsklausel über die Identifizierung und Überprüfung der Herkunft von Softwareprogrammen	ORG_38
Fehlende Sensibilisierung oder Aufklärung über die Gesetzgebung hinsichtlich der Urheberrechte	ORG_40 ORG_41
Fehlende Kontrolle der Zertifizierung von Produkten	ORG_20
Fehlende Kontrolle der Herkunft von Produkten	ORG_20
Fehlende Informatik-Charta, in der die Benutzungsanforderungen definiert werden	ORG_04 PER_03
Die Sicherheitspolitik weist nicht ausdrücklich auf die zivilen, strafrechtlichen und vorschriftsmäßigen Pflichten und Verantwortungen eines jeden hin	ORG_40 ORG_41
Fehlende Definition von Zugriffsprivilegien zur Einschränkung der Installationsmöglichkeiten an den Arbeitsstationen	LOG_11 ORG_33
Fehlende Sensibilisierung des Personals über die Risiken von Sanktionen	PER_08
Nicht-Einhalten der Informatik-Charta, in der die Benutzungsanforderungen definiert werden	PER_03
Fehlende Kenntnis der Sicherheitsmaßnahmen	PER_03 PER_11
Die Anwendung der Sicherheitspolitik wird durch die Direktion nicht gefördert	PER_13
Keine Zertifizierung der Produkte	LOG_06
Keine Prozedur zur Evaluierung der Produkte	ORG_20
Fehlende Prozedur und Mittel zur Überprüfung der Herkunft der Software (Codesignatur, Binärsignatur usw.)	ORG_20
Fehlende Protokollierung der Personenzugänge	PHY_07
Fehlende Prozeduren zur Kontrolle der Ermächtigungen beim Zugang des Personals zum Standort oder zu den Räumlichkeiten	PHY_07
Fehlende Prozeduren zur Identitätskontrolle beim Zugang von Personen zu den Räumlichkeiten oder Zonen	PHY_07
Fehlende Herkunftskontrolle der Anwendungsprogramme vor der Installation	ORG_20
Die Zugangseinrichtung ermöglicht die Speicherung von Softwareprogrammen	RES_01
Die Zugangseinrichtung ermöglicht das Herunterladen von Softwareprogrammen	RES_01

4.1.36 DATENMANIPULATION

Schwachstelle	Abdeckung
Fehlende Kontrolle der Integrität von Produkten	LOG_01
Fehlende Ermächtigungsprozedur und -einrichtung zur Datenänderung	LOG_11
Die Hotline zur Telewartung ist permanent aktiviert	LOG_12 RES_06
Fehlende Beschränkung der Software-Eingangspunkte	LOG_13
Fehlende Überprüfung der Anwendungsprogramme vor der Installation	LOG_06
Fehlender Einsatz von Basis-Sicherheitsregeln, die bezüglich des Betriebssystems und der Softwareprogramme anzuwenden sind	LOG_04
Über die Software besteht Zugriff auf die Daten (Inhalt der Festplatte, Datenbank usw.)	LOG_11
Möglichkeit zur Fern-Systemadministration von jeder beliebigen Arbeitsstation aus	LOG_11
Möglichkeit zur Systemadministration aus der Entfernung mit nicht verschlüsselten Administrationstools	RES_02
Über das Betriebssystem besteht Zugriff auf die Daten (Datenbank u. ä.)	LOG_11
Unzureichende Komplexität der Zugangspasswörter	ORG_10
Fehlende Überprüfung des Betriebssystems vor der Installation	LOG_06

Durch die gemeinsame Nutzung der Ressourcen wird der Systemzugriff durch Unbefugte vereinfacht	LOG_12
Möglichkeit zur Systemadministration aus der Entfernung	RES_01 RES_06
Die SNMP-Schicht ist aktiviert	LOG_12 RES_06
Fehlende Datenschutzvorschriften	ORG_15
Die Hardware kann von jedermann von einem beliebigen Peripheriegerät aus gebootet werden (z. B. Diskette, CD-ROM)	MAT_10
Veraltete Betriebsmittel	ORG_13
Fehlende Redundanz oder Speicherprozedur	MAT_01 ORG_08
Abnutzung der Datenträger	MAT_14
Fehlende Mittel zum Schutz und zur Kontrolle der Integrität der Daten	LOG_01 LOG_01
Fehlende Vorschriften und fehlende Prozedur zur Ermächtigung des Personals	ORG_30
Fehlen der an den Standorten der Institution vorgeschriebenen Politik zur Verwaltung und Kontrolle der Zugangsermächtigungen	LOG_11 ORG_14 ORG_15 ORG_38
Fehlende, an den Standorten der Institution vorgeschriebene Datenschutzpolitik	ORG_15 ORG_38
In der Betriebsordnung werden mit keinem Thema die Sicherheitsverantwortungen im Hinblick auf die Informationssysteme angesprochen	ORG_14
Fehlende Politik bezüglich der Ermächtigungen zum Informationszugriff	ORG_30
Fehlende Absicherung der Zugänge zum IS (Gateways, Intrusionsdetektion, Überwachung der Sicherheitsereignisse usw.)	ORG_30
Fehlende Vertragsklauseln über den Schutz des IT-Materials	ORG_38
Fehlende Kontrolle bezüglich der Anwendung der Sicherheitspolitik	ORG_22
Fehlende Anweisungen hinsichtlich der Benutzung von IT-Material	ORG_04
Fehlende Vorbeugung und Detektion von Viren und sonstigen Softwareprogrammen mit böser Absicht	ORG_06
Fehlende Informationszugriffskontrolle	ORG_15 ORG_30
Fehlender Ausbildungsplan im Hinblick auf Sicherheitsprobleme	PER_02
Fehlende Prozedur zur Kontrolle externer Disketten	ORG_06
Fehlende Informatik-Charta, in der die Benutzungsanforderungen definiert werden	ORG_04 PER_03
Nicht-Einhalten der Informatik-Charta, in der die Benutzungsanforderungen definiert werden	PER_03
Fehlender Schutz und fehlende Klassifizierung der Informationen	ORG_15
Fehlende Sensibilisierung des Personals über die Risiken von Sanktionen	PER_08
Fehlende Kenntnis der Sicherheitsmaßnahmen	PER_03 PER_11
Manipulierbares Personal	PER_02
Konfliktgeladenes Klima zwischen den einzelnen Personen	
Die Anwendung der Sicherheitspolitik wird durch die Direktion nicht gefördert	PER_13
Fehlende Prozeduren zur Identitätskontrolle beim Zugang von Personen zu den Räumlichkeiten oder Zonen	PHY_07
Fehlende Prozeduren zur Kontrolle der Ermächtigungen beim Zugang des Personals	PHY_07

zum Standort oder zu den Räumlichkeiten	
Fehlende Protokollierung der Personenzugänge	PHY_07
Fehlende Sicherung der Kommunikationsleitungen und -ausstattung	PHY_07
Fehlender physischer und logischer Schutz (z. B durch Abtrennung)	RES_01 RES_02
Möglichkeit zur Einwirkung auf die über ein Kommunikationsmedium übertragenen Date	RES_02
Das Netzwerk lässt es zu, Systemressourcen zu ändern oder auf sie einzuwirken	RES_01
Das Netzwerk vereinfacht die Nutzung von Ressourcen durch Unbefugte	RES_01
Fehlende robuste Einrichtung zur Zugangskontrolle	MAT_10 RES_01
Fehlende Speicherprozedur	ORG_08
Die Einrichtung ermöglicht das Löschen, Ändern oder Installieren von Programmen aus der Entfernung	LOG_11
Über die Einrichtung können feindselige Programme wie z. B. Trojanische Pferde, Viren, Würmer oder logische Bomben eingeschleust werden	ORG_06
Die Einrichtung ermöglicht eine Ausnutzung des Asynchronbetriebs bestimmter Bereiche oder Befehle des Betriebssystems (z. B. Javascript-Komponenten zur Erkundung des Inhalts der Festplatte)	LOG_04 LOG_11
Fehlende Abtrennung der Kommunikationsnetze	RES_02
Die Mailfunktion ermöglicht eine Ausnutzung des Asynchronbetriebs bestimmter Bereiche oder Befehle des Betriebssystems (z. B. automatischer Start von Anhängen)	LOG_04
Fehlende Auditierung bzw. Überwachung der Zugänge	ORG_22
Fehlende Zugangsvorschriften	LOG_11

4.1.37 UNZULÄSSIGE VERARBEITUNG VON DATEN

Schwachstelle	Abdeckung
Jedermann zugängliche Software (z. B. zur Fernadministration einer Station ist kein Passwort erforderlich)	LOG_13
Fehlende Verschlüsselungseinrichtung	RES_02
Möglichkeit zur Benutzung einer Backdoor oder eines Trojanischen Pferdes im Betriebssystem	LOG_08 LOG_13
Möglichkeit, mehrere Betriebssysteme auf dem gleichen Rechner zu betreiben (z. B. Zugang zu NTFS-Partitionen via Linux)	LOG_08
Möglichkeit zur Benutzung einer Backdoor oder eines Trojanischen Pferdes im Betriebssystem	
Fehlender physischer Schutz	ORG_01 PHY_03 RES_01
Fehlendes Mittel zur Identifizierung der Sensibilität der auf den Datenträgern enthaltenen Informationen	ORG_15
Datenträger allgemein zugänglich	MAT_07 ORG_15 ORG_30
Attraktive Datenträger (Marktwert und technologische und strategische Werte)	MAT_07
Mobile oder leicht zu transportierende Datenträger (z. B. Disketten, ZIP, externe Festplatten)	MAT_07
Fehlendes Mittel zur Verschlüsselung	ORG_15
Fehlende Prozedur und fehlendes Mittel zur Vernichtung	MAT_08
Fehlende Informationen über die für die Informationsverarbeitung spezifischen Gesetze und Vorschriften	ORG_40 ORG_41

Die Verantwortlichen haben keinen Kontakt zu den technologischen Prüf- und Überwachungsdiensten	ORG_34
In der Betriebsordnung werden mit keinem Thema die Sicherheitsverantwortungen im Hinblick auf die Informationssysteme angesprochen	ORG_14
Fehlende, an den Standorten der Institution vorgeschriebene Datenschutzpolitik	ORG_15 ORG_38
Fehlende Vertragsklausel über die Vertraulichkeit	PER_09
Fehlende Verschlüsselungseinrichtung	ORG_37 PER_08
Fehlende Anweisungen zum Verhalten bei Zwischenfällen (Detektion, Aktion usw.)	ORG_24
Fehlende Informationszugriffskontrolle	ORG_15 ORG_30
Fehlende Sensibilisierung bezüglich der individuellen Verantwortungen	ORG_14 PER_05
Fehlender Verantwortlicher für den Individuen-spezifischen Daten- und Informationsschutz	ORG_14 ORG_15
Nicht-Anwendung der Sicherheitspolitik, insbesondere was die Bearbeitung nominativer Daten anbelangt	ORG_18
Fehlende Sensibilisierung des Personals	ORG_14 PER_05
Fehlender Schutz und fehlendes Audit bezüglich des Zugriffs auf sensitive Informationen	ORG_15 ORG_35
Fehlende Sensibilisierung des Personals über die Risiken von Sanktionen	PER_08
Fehlende Schulung über die Bedingungen einer zulässigen Nutzung von Informationen	PER_10
Fehlender Schutz und fehlende Klassifizierung der Informationen	ORG_15
Fehlende Kenntnis der Sicherheitsmaßnahmen	PER_03 PER_11
Existenz eines unzulässigen Abhörpunkts	RES_02
Fehlende Identifizierung der Schutzniveaus der Systeme	ORG_22
Fehlende Kontrolle des Inhalts	ORG_30
Fehlende Auditierung bzw. Überwachung der Zugänge	ORG_22
Fehlende Verwaltung der Zugangsermächtigungen	LOG_11
Die Einrichtung vereinfacht die Verbreitung von Informationen nach außen	PER_02
Anschluss der Einrichtung an externe Netzwerke	RES_01 RES_03

4.1.38 BENUTZUNGSFEHLER

Schwachstelle	Abdeckung
Fehlende klare Dokumentation über die Anwendungssysteme	ORG_28
Mangelnde Kompetenz des Benutzers	PER_12
Fehlende Test- und Abnahmeprozedur gemäß den Spezifikationen	LOG_06
Fehlende Validierung der Eingangsdaten (Erfassungsdaten)	LOG_17
Fehlende Verantwortung	ORG_14 PER_05
Komplexe Benutzungsanwendung	LOG_17
Informationsmedien sind dem Benutzer nicht zugänglich	ORG_27
Keine intuitive Benutzung der Software	LOG_17
Fehlende Kompetenz	ORG_14
Informationsmedien nicht zugänglich	ORG_27

Fehlende Schulung bezüglich der Nutzung oder Wartung neuer Softwareprogramme	ORG_14 PER_06 PER_12
Komplex anzuwendende Software	LOG_17
Komplex anzuwendende und wenig ergonomische Hardware	MAT_11
Schlechte Nutzungsbedingungen	MAT_14
Möglichkeit, dass bestimmte Betriebsmittel schädliche Einwirkungen auf das benutzende Personal haben (Arbeiten am Bildschirm, Wellen usw.)	MAT_11 MAT_12
Fehlende Labelisierung der Datenträger	MAT_06
Komplex anzuwendende und wenig ergonomische Datenträger	MAT_11
Fehlende Kontrolle kritischer Prozesse durch die Mutterorganisation	ORG_38
Fehlende doppelte Kontrolle kritischer Prozesse	ORG_43
Fehlende Schulung bezüglich der zum Einsatz kommenden Hardware- und Softwarekomponenten	PER_12
Schlechte Kenntnis der Verantwortungen	PER_05
Fehlende Formalisierung der allgemein bekannten Verantwortungen	PER_05
Ungünstige Arbeitsbedingungen	ORG_45
Fehlender Professionalismus	PER_05
Nicht-Einhalten der Anweisungen	PER_10
Benutzendes Personal nur wenig oder schlecht ausgebildet	PER_12
Vorhandensein von hochsensitiven Operationen, die von einer einzelnen Person ausgeführt werden können	PER_07
Fehlende Benutzungsunterlagen über die vorhandenen Anwendungsprogramme	PER_12
Fehlende Motivation für Arbeiten, die mit der Datenerfassung zu tun haben	PER_05
Mit der Datenerfassung wenig vertrautes Personal	PER_06
Ungünstige Arbeitsumgebung (zu kleine Räume, kein Platz zum Wegräumen usw.)	PHY_12
Fehlende Etikettierung von Kabeln oder fehlender Kabelplan	PHY_11
Platzmangel in den technischen Räumlichkeiten	PHY_12
Fehlende Betriebsprozedur	ORG_04
Fehlende Etikettierung und fehlendes Architekturschema auf neuestem Stand	MAT_06
Fehlender Verkabelungsplan	PHY_11
Schnittstelle enthält landesspezifische technische Merkmale (z. B. verschiedene Telefonsteckertypen zwischen Frankreich und Großbritannien)	RES_04
Medien und Informationsträger enthalten technische Merkmale, die sie lokalisierbar machen (z. B. verschiedene ADSl-Konfigurationsparameter zwischen Frankreich und Großbritannien)	RES_04
Fehlende Schutzmaßnahmen (nur Lesemodus z. B.)	LOG_11
Fehlendes Überwachungstool	MAT_13

4.1.39 RECHTSMISSBRAUCH

Schwachstelle	Abdeckung
Fehlende Audit-Politik	ORG_22
Fehlende Speicherung der Ereignisjournale	ORG_08
Fehlende Ereignisprotokollierung	LOG_15
Komplexe bzw. wenig ergonomische Dateien	ORG_42
Unzureichende Komplexität der Zugangspasswörter	ORG_10
Möglichkeit zur Systemadministration aus der Entfernung mit nicht verschlüsselten	RES_02

Administrationstools	
Die Passwörter-Datenbank des Betriebssystems ist entschlüsselbar	ORG_10
Die SNMP-Schicht ist aktiviert	LOG_12 RES_06
Möglicherweise wird das Betriebssystem mit unkorrekten Anfragen bzw. Daten konfrontiert (z. B. Buffer overflow)	LOG_14
Die Hotline zur Telewartung ist permanent aktiviert	LOG_12 RES_06
Möglichkeit zur Systemadministration aus der Entfernung	RES_01 RES_06
Die Logs und Journale des Betriebssystem können von jedermann geändert werden	LOG_11
Durch die gemeinsame Nutzung der Ressourcen wird der Systemzugriff durch Unbefugte vereinfacht	LOG_12
Das Betriebssystem ist allgemein zugänglich und von jedermann benutzbar (z. B. über das Konto "Gast")	LOG_11
Das Betriebssystem protokolliert keine Logs oder Systemereignisse	LOG_15
Das Betriebssystem ermöglicht die Herstellung anonymer Verbindungen	LOG_13
Das Betriebssystem ermöglicht das Öffnen einer Session ohne Passwort	LOG_13
Möglichkeit zur Fern-Systemadministration von jeder beliebigen Arbeitsstation aus	LOG_11
Verwendung einer veralteten Version des Betriebssystems oder der Anwendungsprogramme	LOG_09 ORG_13
Die Passwörter zum Zugang zum Betriebssystem sind entschlüsselbar	ORG_10
Möglichkeit, mehrere Betriebssysteme auf dem gleichen Rechner zu betreiben (z. B. Zugang zu NTFS-Partitionen via Linux)	LOG_08
Jedermann zugängliche Software (z. B. zur Fernadministration einer Station ist kein Passwort erforderlich)	LOG_13
Fehlender physischer Schutz	ORG_01 PHY_03 RES_01
Fehlende robuste Einrichtung zur Zugangskontrolle	MAT_10 RES_01
Fehlendes Audit über die Prozeduren bezüglich der physischen Zugriffskontrolle	ORG_22
Fehlen der an den Standorten der Institution vorgeschriebenen Politik zur Verwaltung und Kontrolle der Ermächtigungen	LOG_11 ORG_14 ORG_15 ORG_38
In der Betriebsordnung werden mit keinem Thema die Sicherheitsverantwortungen im Hinblick auf die Informationssysteme angesprochen	ORG_14
Die Verantwortlichen haben keinen Kontakt zu den technologischen Prüf- und Überwachungsdiensten	ORG_34
Fehlende Vertragsklauseln zur Begrenzung der Verantwortungen beider Parteien	ORG_38
Fehlende Definition des Begriffs "Informationsanspruch"	ORG_33
Fehlende Einrichtung zur Kontrolle und Verhängung von Sanktionen	ORG_37 PER_08
Fehlende Verordnung, mit Definition der Rechte	ORG_33
Die Zuweisungen von Benutzerrechten sind nicht klar definiert	ORG_14
Fehlende Kontrolle hinsichtlich der Zuweisung von Benutzerrechten	LOG_11
Vorrangstellung von Personalkategorien	PER_05
Die Anwendung der Sicherheitspolitik wird durch die Direktion nicht gefördert	PER_13
Vorhandensein von hochsensitiven Operationen, die von einer einzelnen Person	PER_07

ausgeführt werden können	
Verschaffung eines Vorteils	PER_08
Fehlende Definition des Begriffs "Recht" für das Personal	PER_05
Fehlende Prozeduren zur Kontrolle der Ermächtigungen beim Zugang des Personals zum Standort oder zu den Räumlichkeiten	PHY_07
Fehlender physischer und logischer Schutz	RES_01
Der Least-Privileg-Grundsatz wird nicht angewendet	LOG_11
Möglichkeit zur Benutzung von Betriebsmitteln ohne Hinterlassen von Spuren	RES_03
Die Einrichtung ist allgemein zugänglich	LOG_11 ORG_01

4.1.40 RECHTSANMASSUNG

Schwachstelle	Abdeckung
Fehlende Audit-Politik	ORG_22
Fehlende Speicherung der Ereignisjournale	ORG_08
Fehlende Ereignisprotokollierung	LOG_15
Die Logs und Journale des Betriebssystem können von jedermann geändert werden	LOG_11
Das Betriebssystem ermöglicht das Öffnen einer Session ohne Passwort	LOG_13
Das Betriebssystem ermöglicht die Herstellung anonymer Verbindungen	LOG_13
Das Betriebssystem protokolliert keine Logs oder Systemereignisse	LOG_15
Das Betriebssystem ist allgemein zugänglich und von jedermann benutzbar (z. B. über das Konto "Gast")	LOG_11
Durch die gemeinsame Nutzung der Ressourcen wird der Systemzugriff durch Unbefugte vereinfacht	LOG_12
Die Passwörter-Datenbank des Betriebssystems ist entschlüsselbar	ORG_10
Die SNMP-Schicht ist aktiviert	LOG_12 RES_06
Komplexe bzw. wenig ergonomische Dateien	ORG_42
Möglichkeit zur Systemadministration aus der Entfernung mit nicht verschlüsselten Administrationstools	RES_02
Möglichkeit zur Systemadministration aus der Entfernung	RES_01 RES_06
Die Hotline zur Telewartung ist permanent aktiviert	LOG_12 RES_06
Die Passwörter zum Zugang zum Betriebssystem sind entschlüsselbar	ORG_10
Unzureichende Komplexität der Zugangspasswörter	ORG_10
Verwendung einer veralteten Version des Betriebssystems oder der Anwendungsprogramme	LOG_09 ORG_13
Möglicherweise wird das Betriebssystem mit unkorrekten Anfragen bzw. Daten konfrontiert (z. B. Buffer overflow)	LOG_14
Möglichkeit, mehrere Betriebssysteme auf dem gleichen Rechner zu betreiben (z. B. Zugang zu NTFS-Partitionen via Linux)	LOG_08
Möglichkeit zur Fern-Systemadministration von jeder beliebigen Arbeitsstation aus	LOG_11
Jedermann zugängliche Software (z. B. zur Fernadministration einer Station ist kein Passwort erforderlich)	LOG_13
Anschluss des Betriebsmittels an externe Netzwerke	MAT_10
Fehlende robuste Einrichtung zur Zugangskontrolle	MAT_10 RES_01
Fehlende Abtrennung der Systemausstattung	MAT_10

Fehlender Schutz der Datenträger	ORG_30
Fehlendes Audit über die Prozeduren bezüglich der physischen Zugriffskontrolle	ORG_22
Die Verantwortlichen haben keinen Kontakt zu den technologischen Prüf- und Überwachungsdiensten	ORG_34
Fehlende Vorschriften und fehlende Prozedur zur Ermächtigung des Personals	ORG_30
Fehlende Sensibilisierung über die Risiken von Sanktionen	ORG_37 PER_08
In der Betriebsordnung werden mit keinem Thema die Sicherheitsverantwortungen im Hinblick auf die Informationssysteme angesprochen	ORG_14
Fehlende Überwachungsprozedur	ORG_33
Möglichkeit zur freien Benutzung der Ressourcen der Institution (Selbstbedienung)	LOG_11 ORG_33
Fehlender Schutz der Bereiche, die dem Austausch bzw. der gemeinsamen Nutzung von Informationen vorbehalten sind	ORG_30
Fehlende Prozedur zur Ermächtigung des Personals	LOG_11 ORG_30
Kein Klima des Vertrauens untereinander	ORG_37 PER_05
Die Sicherheitsverantwortungen bezüglich der Ermächtigungsverwaltung sind nicht formalisiert	ORG_14 ORG_15
Fehlende Kommunikation und Unterrichtung des Personals bezüglich der Ermächtigungsprozeduren	ORG_41
Fehlende Prozedur hinsichtlich der Informationsweitergabe im Falle von Detektionen	ORG_24
Die Sicherheitspolitik wird nicht angewendet	ORG_18
Unangepasste Organisation	ORG_14
Die zugestandenen Rechte gehen über den gerechtfertigten Bedarf hinaus	PER_07
Konfliktgeladenes Klima zwischen den einzelnen Personen	
Fehlende moralische oder ethische Vorschriften	PER_08
Verschaffung eines Vorteils	PER_08
Vorhandensein von hochsensitiven Operationen, die von einer einzelnen Person ausgeführt werden können	PER_07
Die Anwendung der Sicherheitspolitik wird durch die Direktion nicht gefördert	PER_13
Für das Personal unangemessene Missionen	ORG_14
Fehlende Prozeduren zur Kontrolle der Ermächtigungen beim Zugang des Personals zum Standort oder zu den Räumlichkeiten	PHY_07
Fehlender physischer und logischer Schutz (z. B durch Abtrennung)	RES_01 RES_02
Fehlende Netzabtrennung	RES_01 RES_02
Die Schnittstellen sind an externe Netzwerke angeschlossen	RES_01
Die Informationsträger und Kommunikationsmedien sind an externe Netzwerke angeschlossen	RES_01
Technische Merkmale können geändert werden (z. B. MAC-Adresse einer Ethernet-Karte)	LOG_11
Fehlender physischer Schutz	ORG_01 PHY_03 RES_01
Das Netzwerk lässt es zu, Systemressourcen zu ändern oder auf sie einzuwirken	RES_01
Verwendung eines Protokolls ohne Authentifizierungsfunktion	RES_03
Die Schnittstellen sind allgemein zugänglich	RES_01

Das Netzwerk ermöglicht eine problemlose Nutzung der Ressourcen durch Unbefugte	RES_01
Die Relais identifizieren weder die Quellen noch die Ziele (mögliche Auswirkungen: Anfälligkeit des Systems für Spoofing-Angriffe)	RES_03
Die Einrichtung ist allgemein zugänglich	LOG_11 ORG_01
Möglicherweise wird die Einrichtung mit unkorrekten Anfragen bzw. Daten konfrontiert (z. B. Buffer overflow)	LOG_14
Fehlende Überprüfung der Anwendungsprogramme vor der Installation	LOG_06
Die Einrichtung zur Nachrichtenübermittlung ist über Internet zugänglich	RES_01
Verwendung einer veralteten Version des Mailboxservers	LOG_09 ORG_13

4.1.41 VERLEUGNUNG VON AKTIONEN

Schwachstelle	Abdeckung
Fehlende Audit-Politik	ORG_22
Fehlende Speicherung der Ereignisjournale	ORG_08
Fehlende Ereignisprotokollierung	LOG_15
Das Betriebssystem protokolliert keine Logs oder Systemereignisse	LOG_15
Die SNMP-Schicht ist aktiviert	LOG_12 RES_06
Möglichkeit zur Systemadministration aus der Entfernung mit nicht verschlüsselten Administrationstools	RES_02
Komplexe bzw. wenig ergonomische Dateien	ORG_42
Unzureichende Komplexität der Zugangspasswörter	ORG_10
Die Passwörter zum Zugang zum Betriebssystem sind entschlüsselbar	ORG_10
Die Passwörter-Datenbank des Betriebssystems ist entschlüsselbar	ORG_10
Das Betriebssystem ermöglicht die Herstellung anonymer Verbindungen	LOG_13
Möglicherweise wird das Betriebssystem mit unkorrekten Anfragen bzw. Daten konfrontiert (z. B. Buffer overflow)	LOG_14
Möglichkeit zur Fern-Systemadministration von jeder beliebigen Arbeitsstation aus	LOG_11
Verwendung einer veralteten Version des Betriebssystems oder der Anwendungsprogramme	LOG_09 ORG_13
Das Betriebssystem ist allgemein zugänglich und von jedermann benutzbar (z. B. über das Konto "Gast")	LOG_11
Möglichkeit zur Systemadministration aus der Entfernung	RES_01 RES_06
Die Logs und Journale des Betriebssystem können von jedermann geändert werden	LOG_11
Möglichkeit, mehrere Betriebssysteme auf dem gleichen Rechner zu betreiben (z. B. Zugang zu NTFS-Partitionen via Linux)	LOG_08
Das Betriebssystem ermöglicht das Öffnen einer Session ohne Passwort	LOG_13
Die Hotline zur Telewartung ist permanent aktiviert	LOG_12 RES_06
Durch die gemeinsame Nutzung der Ressourcen wird der Systemzugriff durch Unbefugte vereinfacht	LOG_12
Jedermann zugängliche Software (z. B. zur Fernadministration einer Station ist kein Passwort erforderlich)	LOG_13
Fehlende Einrichtung für Protokolldaten und Audits	ORG_39 RES_03
Die Hardware ist allgemein zugänglich und von jedermann benutzbar	MAT_10

Datenträger allgemein zugänglich	MAT_07 ORG_15 ORG_30
Fehlende Prozedur über den Zugriff auf klassifizierte Informationen	ORG_15
Änderung der Organisationspolitik oder -strategie	ORG_14 ORG_33
Fehlende Definition der Verantwortungen	ORG_14
In der Betriebsordnung werden mit keinem Thema die Sicherheitsverantwortungen im Hinblick auf die Informationssysteme angesprochen	ORG_14
Fehlende Disziplinarverfahren	ORG_37
Tiefgreifende politisch-wirtschaftliche Konsequenzen absehbar	ORG_31
Fehlende Globalpolitik zur Verwaltung und Archivierung von Protokolldaten und sonstigen Beweiselementen	ORG_39
Fehlende Vertragsklausel über die Definition von Prozeduren für Kommunikation und Datenaustausch	ORG_03 ORG_38
Fehlende gegenseitige Code-Kontrolle	ORG_20 ORG_38
Übertriebene oder nicht dem Kontext angepasste Straf- oder Sanktionsklausel	ORG_37 ORG_38
Fehlende Mechanismen zur Weiterverfolgung von Aktionen und Ereignis- oder Alarmjournalen	ORG_39
Möglichkeit zur freien Benutzung der Ressourcen der Institution (Selbstbedienung)	LOG_11 ORG_33
Fehlende Hierarchisierung der Organisation und fehlende Reporting-Prozedur	ORG_21
Keine Unterscheidung zwischen Auditfunktionen und Funktionen zur Nachkontrolle	ORG_22 PER_07
Die Anwendung der Sicherheitspolitik wird durch die Direktion nicht gefördert	PER_13
Verschaffung eines Vorteils	PER_08
Fehlendes Vertrauen in die Organisation	
Verantwortung jedes einzelnen unbekannt	PER_05
Konfliktgeladenes Klima zwischen den einzelnen Personen	
Fehlende Protokollierung der ein- und ausgehenden Personen	PHY_07
Die Relais sind allgemein zugänglich	RES_01
Das Kommunikationsmedium ermöglicht eine Benutzung des Systems von außen	RES_01
Die Informationsträger und Kommunikationsmedien sind allgemein zugänglich und standardmäßig aktiv (z. B. alle angeschlossenen RJ45-Stecker)	RES_01
Das Netzwerk vereinfacht die Nutzung von Ressourcen durch Unbefugte	RES_01
Das Protokoll erlaubt keine eindeutige Identifizierung des Absenders	RES_03
Das Netzwerk lässt es zu, Systemressourcen zu ändern oder auf sie einzuwirken	RES_01
Das Protokoll ermöglicht nicht den Versand einer Empfangsbestätigung	RES_03
Möglichkeit zur Benutzung von Betriebsmitteln ohne Hinterlassen von Spuren	RES_03
Die Zugangseinrichtung protokolliert keine betriebsspezifischen Protokolldaten	ORG_39
Der Zugriff zur Protokolliereinrichtung ist nicht geschützt	LOG_11
Die Einrichtung ist allgemein zugänglich (z. B. keine Authentifizierung der Client-Stationen oder der Benutzer durch die Einrichtung)	LOG_11
Anschluss der Einrichtung an externe Netzwerke	RES_01 RES_03

4.1.42 BEEINTRÄCHTIGUNG DER PERSONALVERFÜGBARKEIT

Schwachstelle	Abdeckung
Möglichkeit, dass bestimmte Betriebsmittel schädliche Einwirkungen auf das benutzende Personal haben (Arbeiten am Bildschirm, Wellen usw.)	MAT_11 MAT_12
Fehlende Prozedur zur Archivierung	ORG_07
Ungünstiges soziales Klima	
Politisch-wirtschaftlicher Konflikt zwischen dem Mutterland der Organisation und dem gastgebenden Land der Institution	ORG_31
Fehlende Klausel oder Vorschriften zum Thema Wissenstransfer	ORG_38 PER_06
Fehlende finanzielle oder technologische Beständigkeit der Institution	ORG_13
Fehlende Klausel über die Kontinuität bei der Erbringung von Dienstleistungen	ORG_16 ORG_38
Fehlende Einheit zum Schutz des Personals	ORG_45
Ausbruch einer lokalen Virusepidemie	PER_04
Fehlende Prozeduren im Hinblick auf den Wissenstransfer	PER_06
Soziales Klima innerhalb der Organisation nicht förderlich für die Aktivität	
Fehlender Plan zur Sensibilisierung und Schulung in Prozessen zur Kontinuität der beruflichen Aktivität	ORG_16 PER_10
Fehlende Verwaltungsprozesse zur Kontinuität der beruflichen Aktivität innerhalb der Institution	ORG_16
Unterdimensionierung der Organisation	ORG_14 PER_04
Keine Redundanz des strategischen Personals	PER_04
Fehlende redundante Organisation der sensitiven Funktionen	ORG_14 PER_04
Fehlende Verwaltungsprozesse zur Kontinuität der beruflichen Aktivität innerhalb der Projektgruppe	ORG_16
Fehlende Unterlagendatenbank über Vorschriften und Prozeduren	ORG_41
Nichtverfügbarkeit infolge konkurrenzieller Belange	PER_05
Nichtverfügbarkeit auf Grund von Krankheit	PER_04
Nichtverfügbarkeit durch Fernbleiben von der Arbeit	PER_04 PER_05
Provozierte Nichtverfügbarkeit (Überfall, Geiselnahme usw.)	PER_04
Soziale Probleme	
Konfliktgeladenes soziales Klima	
Schwieriges soziales Klima mit möglichen Streiks in den Transportbetrieben	PHY_04
Unterbringung des Fachpersonals in großer Entfernung	PHY_04
Wohnsitze der Mitarbeiter in großer Entfernung	PHY_04
Mögliche schädliche Einwirkung auf das benutzende Personal (Übertragung per Funk, Wellen usw.)	MAT_12

5 Vorschlag zur Abdeckung der allgemeinen Sicherheitsziele durch Sicherheitsanforderungen

Mit Hilfe der folgenden Tabellen können die allgemeinen Sicherheitsanforderungen, die in der Lage sind, den einzelnen allgemeinen Sicherheitszielen zu genügen (und deren Codes denen der vorhergehenden Abschnitte entsprechen), problemlos bestimmt werden.

5.1 MAT : Hardware

MAT_01	
Abdeckung	BGC_INT.1.1 BGC_PRE.1.1 CGS_GSS.1.1 CGS_SVG.1.3 CGS_SVG.1.4 CGS_SVG.1.5 CGS_SVG.1.6 CGS_SVG.1.7 CGS_SVG.1.8 CGS_SVG.1.9 FRU_FLT.1.1 FRU_FLT.2.1

MAT_02	
Abdeckung	BGC_INT.1.1 CGS_SVG.1.1 CGS_SVG.1.2

MAT_03	
Abdeckung	BMA_MAA.2.1 BPE_SEM.1.1

MAT_04	
Abdeckung	BGC_MSS.1.1 CGS_ARC.1.1 CGS_ARC.1.2

MAT_05	
Abdeckung	CAR_AAR.1.1 CAR_PAR.1.1 FRU_FLT.1.1

MAT_06	
Abdeckung	BCM_RLC.1.1

MAT_07	
Abdeckung	BCM_RLC.1.1 BMA_REU.2.1 BPE_SEM.1.1 BPE_SEM.5.1 BPE_ZOS.1.1 BPE_ZOS.2.1 BSP_RIS.5.1 BSP_RIS.5.2 CET_EGT.1.10 CET_EGT.1.8 CET_EGT.1.9 CET_EGT.2.3 CET_EGT.3.1 CGS_PPS.2.1

	CGS_PPS.3.1 CGS_PPS.3.2 FIA_UAU.1.2/2.1 FIA_UAU.6.1 FIA_UID.1.2/2.1
MAT_08	
Abdeckung	BGC_INT.1.1 BGC_MSS.2.1 CGS_SVG.1.2
MAT_09	
Abdeckung	BDM_ESS.1.1 BGC_PRS.1.1 CAR_AAR.1.1 CEI_ABS.1.5
MAT_10	
Abdeckung	BGC_EIL.2.1 BGC_MSS.3.1 BGC_PRE.4.1 BPE_SEM.1.1 BPE_ZOS.2.1 CGS_GLI.2.1 FTA_TAB.1.1
MAT_11	
Abdeckung	BSP_FOU.2.1 CEI_CDT.2.1 CEI_CDT.2.2
MAT_12	
Abdeckung	BSP_FOU.2.1 CEI_CDT.2.1 CEI_CDT.2.2
MAT_13	
Abdeckung	CGS_GSU.1.1 CGS_GSU.1.3 CGS_SUP.1.1
MAT_14	
Abdeckung	CGS_OML.1.1

5.2 LOG : Software

LOG_01	
Abdeckung	BDM_COC.3.1 FDP_ITT.3.1 FDP_ITT.3/4.2 FDP_SDI.1/2.1 FDP_SDI.2.1 FPT_ITI.1/2.2 FPT_ITT.3.1 FPT_ITT.3.2 FPT_TST.1.2

LOG_02	
Abdeckung	BDM_SED.1.1 BDM_SED.2.1 BDM_SED.3.1 BDM_SED.4.1 BDM_SED.5.1 BGC_PRE.2.1 BGC_PRS.2.1 CDO_SDC.1.2 CGS_GMA.6.1

LOG_03	
Abdeckung	BCO_RPS.2.1 BDM_SED.1.1 BDM_SED.2.1 BDM_SED.4.1 BGC_PRE.2.1 BGC_PRE.2.2 BMA_SAS.1.1 CET_EIP.1.3 CET_EIP.1.4 CET_EIP.1.5 CET_EIP.1.6

LOG_04	
Abdeckung	CGS_CSR.1.2 FMT_MSA.3.1

LOG_05	
Abdeckung	

LOG_06	
Abdeckung	BDM_SED.4.1 BDM_SFS.1.1 BGC_PLM.1.1 BGC_PRS.2.1 CGS_OML.1.1 CGS_OML.1.2 CGS_PPS.2.4

LOG_07	
Abdeckung	BCM_RLC.1.1 BCO_CEL.3.1 CGS_GLI.1.1 CGS_GLI.1.2 CGS_GLI.1.3 CGS_GLI.1.4

LOG_08

Abdeckung	BCM_RLC.1.1 BCO_RPS.2.1 BDM_SED.1.1 BDM_SED.3.1 BDM_SED.4.1 BGC_PRE.2.1 BGC_PRE.2.2 BGC_PRS.2.1 BMA_MAS.3.1 CDO_SDC.1.1 CGS_PPS.1.1 CGS_PPS.2.1 CGS_PPS.2.3 CGS_PPS.2.4 FIA_UAU.7.1 FPT_RVM.1.1 FPT_SEP.1.1
LOG_09	
Abdeckung	BGC_PRE.1.1 CDO_APP.1.1 CDO_APP.1.2 CEI_CDT.1.1 CEI_CDT.1.2
LOG_10	
Abdeckung	BMA_MAS.3.1 BMA_SAS.1.1 BMA_SAS.3.1 FPT_STM.1.1
LOG_11	
Abdeckung	BCM_CLI.1.1 BCM_CLI.1.2 BCM_CLI.2.1 BCO_CEL.4.1 BCO_CEL.5.1 BDM_SED.1.1 BDM_SED.2.1 BDM_SED.3.1 BDM_SED.4.1 BDM_SFS.1.1 BGC_EIL.6.1 BGC_MSS.2.1 BGC_MSS.3.1 BGC_PRE.2.1 BGC_PRS.2.1 BMA_GAU.1.1 BMA_GAU.2.1 BMA_GAU.4.1 BMA_MAA.1.1 BMA_MAR.1.1 BMA_MAR.7.1 BMA_MAS.2.1 BMA_MAS.3.1 BMA_MAS.5.1 BPE_SEM.6.1 BPS_PSI.1.5 CGS_CSR.1.2 CGS_GDH.1.1 CGS_GDH.1.2 CGS_GDH.1.3 CGS_GDH.1.4

	CGS_GDH.1.5 CGS_GDH.1.6 CGS_GDH.1.7 CGS_GDH.1.8 CGS_GDH.1.9 CGS_GDH.2.1 CGS_GDT.1.1 CGS_GLI.2.1 CGS_PAI.1.1 CGS_PAI.1.2 CGS_PAI.1.3 CGS_PEP.1.1 CGS_PPS.2.1 CGS_PPS.2.5 FDP_RIP.1.1 FDP_RIP.2.1 FMT_MOF.1.1 FMT_MSA.1.1 FMT_MSA.3.2 FMT_MTD.1.1 FMT_MTD.2.1
LOG_12	
Abdeckung	FAU_SAA.2.3
LOG_13	
Abdeckung	BDM_SED.4.1 BMA_MAS.3.1 BMA_MAS.7.1 BMA_MAS.8.1 CGS_GDH.1.2 CGS_GDH.2.1 CGS_PPS.2.3 CGS_PPS.2.4 FIA_UAU.7.1 FTA_SSL.1.1 FTA_SSL.2.1 FTA_SSL.3.1
LOG_14	
Abdeckung	BDM_SSA.1.1 BGC_EIL.4.1 CAR_AAR.1.1 CGS_CME.1.1 CGS_PPS.2.4 FRU_FLT.1.1
LOG_15	
Abdeckung	BMA_SAS.1.1 CET_EGT.1.6 FAU_GEN.1.1 FAU_GEN.1.2
LOG_16	
Abdeckung	BMA_MAS.7.1 BMA_MAS.8.1 CIS_ADL.1.1 FTA_SSL.1.1 FTA_SSL.2.1 FTA_SSL.3.1
LOG_17	
Abdeckung	BGC_EIL.4.1

	BGC_EIL.5.1 CGS_PPS.2.3

5.3 RES : Netzwerk

RES_01	
Abdeckung	BCO_CEL.5.1 BDM_COC.2.1 BDM_COC.4.1 BGC_EIL.1.1 BGC_EIL.4.1 BGC_PLM.1.1 BGC_PRE.4.1 BMA_EMA.1.1 BMA_GAU.2.1 BMA_MAA.1.1 BMA_MAA.2.1 BMA_MAR.1.1 BMA_MAR.3.1 BMA_MAR.4.1 BMA_MAR.5.1 BMA_MAR.6.1 BMA_MAR.7.1 BMA_MAS.2.1 BMA_MAS.3.1 BMA_REU.2.1 BPE_SEM.1.1 BPE_ZOS.1.1 BPE_ZOS.2.1 CAR_PAR.1.1 CET_EGT.1.1 CGS_CSR.1.1 CGS_CSR.1.2 CGS_CSR.1.3 CGS_GDA.1.1 CGS_GDA.3.1 CGS_GDA.3.2 CGS_GDH.1.1 CIS_PSI.1.1 FMT_MOF.1.1 FMT_MSA.1.1 FMT_MSA.3.2 FMT_MTD.1.1 FMT_MTD.2.1 FPT_ITA.1.1 FPT_ITI.1/2.1 FPT_ITI.1/2.2 FPT_ITI.2.3 FPT_ITT.3.1 FPT_ITT.3.2 FTA_TAB.1.1 FTA_TSE.1.1

RES_02	
Abdeckung	BDM_COC.1.1 BDM_COC.2.1 BDM_COC.4.1 BDM_COC.5.1 BGC_GER.1.1 BGC_PRE.4.1 BGC_PRS.1.1 BMA_EMA.1.1 BMA_GAU.2.1 BMA_MAA.1.1

	BMA_MAA.2.1 BMA_MAR.1.1 BMA_MAR.4.1 BMA_MAR.5.1 BMA_MAR.6.1 BMA_MAR.7.1 BPE_SEM.1.1 BPE_SEM.3.1 BPE_ZOS.2.1 CAR_PAR.1.1 CGS_CSR.1.2 CGS_PPS.1.2 CGS_PPS.1.3 FCO_NRO.2.1 FCS_COP.1.1 FDP_ITT.1/2.1 FDP_UCT.1.1 FPT_ITC.1.1 FPT_ITT.1/2.1 FTA_TAB.1.1
RES_03	
Abdeckung	BDM_COC.4.1 BGC_EIL.4.1 BGC_EIL.5.1 BMA_MAR.4.1 BMA_MAS.1.1 BMA_MAS.2.1 BMA_MAS.3.1 BMA_MAS.6.1 BMA_SAS.1.1 BMA_SAS.2.1 BMA_SAS.3.1 BPE_SEM.1.1 CGS_GDA.1.3 FAU_STG.1/2.1 FAU_STG.1/2.2 FAU_STG.2.3 FCO_NRO.1.1 FCO_NRO.1.2 FCO_NRO.1.3 FCO_NRO.2.1 FCO_NRR.1.1 FCO_NRR.1.2 FCO_NRR.1.3 FCO_NRR.2.1 FDP_UCT.1.1 FIA_UAU.1.2/2.1 FTA_TAB.1.1
RES_04	
Abdeckung	BGC_PRS.2.1 BMA_MAR.8.1 CGS_PPS.2.2 CGS_PPS.2.3 CIS_PSI.1.2
RES_05	
Abdeckung	BMA_MAR.8.1 BPE_SEM.3.1
RES_06	
Abdeckung	BDM_COC.4.1

	BGC_PLM.1.1 BMA_GAU.2.1 BMA_MAR.5.1

5.4 PER : Personal

PER_01	
Abdeckung	BGC_EIL.1.1 BGC_EIL.2.1 BGC_EIL.4.1 BGC_EIL.5.1 BGC_EIL.6.1 BGC_EIL.7.1 BGC_MSS.1.1 BMA_IMT.1.1 BMA_IMT.2.1 BPE_SEM.5.1 BSP_FOU.1.1 CCS_CSG.1.3

PER_02	
Abdeckung	BCM_CLI.1.1 BCM_CLI.1.2 BCM_CLI.2.1 BCO_CEL.4.1 BGC_EIL.4.1 BGC_EIL.5.1 BGC_EIL.6.1 BGC_MSS.2.1 BOS_ISI.3.1 BPE_MMG.2.1 BPE_SEM.6.1 BPS_PSI.1.5 BSP_FOU.1.1 BSP_RIS.5.1 BSP_RIS.5.2 BSP_SPR.1.1 BSP_SPR.3.1 BSP_SPR.4.1 CCS_SRI.1.1 CET_EGT.2.3 CFO_SPS.1.1 CGS_CIR.1.1 CGS_CIR.1.2 CGS_CIR.1.3 CRR_SEN.1.1

PER_03	
Abdeckung	BCM_CLI.1.1 BCM_CLI.1.2 BCM_CLI.2.1 BCO_CEL.1.1 BCO_CEL.2.1 BCO_CEL.4.1 BCO_CEL.5.1 BDM_SED.1.1 BDM_SED.3.1 BDM_SED.4.1 BDM_SFS.1.1 BGC_EIL.2.1 BGC_EIL.4.1 BGC_INT.3.1 BGC_MSS.3.1 BGC_PLM.1.1 BGC_PRE.1.1

	BGC_PRE.2.1 BGC_PRE.2.2 BMA_GAU.2.1 BMA_MAS.5.1 BMA_REU.1.1 BPS_PSI.1.4 BPS_PSI.1.5 BSP_FOU.1.1 BSP_FOU.2.1 BSP_RIS.1.1 BSP_RIS.3.1 BSP_RIS.5.1 BSP_RIS.5.2 BSP_SPR.1.1 BSP_SPR.4.1 CCS_CHI.1.1 CCS_CSG.1.1 CCS_CSG.1.2 CCS_CSG.1.3 CCS_CSG.1.4 CFO_SPS.1.1 CGI_GIS.1.1 CGI_GIS.1.8 CGS_GDH.1.2 CGS_GDH.2.1 CGS_GMP.1.1 CGS_GMP.1.3 CGS_OML.1.2 CGS_PPS.2.1 CGS_PPS.2.3 CPD_DGL.1.1 CPD_DGL.1.2 CRR_SEN.1.1
PER_04	
Abdeckung	BSP_RIS.5.1 BSP_RIS.5.2 CFO_FRS.1.1 CFO_FRS.1.2 CFO_FRS.1.3 CFO_FRS.1.4 CFO_FRS.1.5 CRH_DDE.1.1 CRH_DDE.1.2 CRH_PDP.1.1
PER_05	
Abdeckung	BGC_PRS.1.1 BOS_ISI.3.1 BOS_SAT.1.3 BPS_PSI.1.3 BSP_FOU.1.1 BSP_RIS.5.1 BSP_RIS.5.2 BSP_SPR.1.1 BSP_SPR.3.1 BSP_SPR.4.1 CDO_SDC.1.1 CET_EIP.1.3 CET_EIP.1.4 CET_EIP.1.5 CFO_FRS.1.1 CFO_FRS.1.2

	CFO_FRS.1.3 CFO_FRS.1.4 CFO_FRS.1.5 CFO_SPS.1.1 CGI_GIS.3.1 CGI_GIS.3.2 CGI_GIS.3.3 CGI_GIS.3.4 CGI_GIS.3.5 CGI_GIS.3.6 CGS_GDH.1.2 CGS_HSI.1.1 CGS_HSI.1.2 CGS_PAI.2.1 CGS_PAI.2.3 CPS_PAQ.2.1 CPS_PAQ.2.2 CRH_DDE.1.1 CRH_DDE.1.2
PER_06	
Abdeckung	BSP_FOU.1.1 BSP_FOU.2.1 CDO_APP.1.1 CDO_APP.1.2 CFO_FRS.2.1 CFO_FRS.2.2 CFO_FRS.2.3 CFO_FRS.2.4 CPS_PAQ.3.1
PER_07	
Abdeckung	BOS_ISI.7.1 CGS_GDH.1.1 CGS_GDH.1.3 CGS_GDH.1.4 CGS_GDH.1.5 CGS_GDH.1.7 CGS_GPC.2.1 CGS_GPC.2.2 CGS_GPC.2.3 CGS_GPC.2.4
PER_08	
Abdeckung	BMA_MAS.6.1 BSP_RIS.5.1 BSP_RIS.5.2 BSP_SPR.3.1 CCS_CHI.1.1
PER_09	
Abdeckung	BGC_PRE.6.1 BOS_SOT.1.1 BOS_SOT.1.2 BSP_RIS.5.1 BSP_RIS.5.2 BSP_SPR.3.1 CFO_SPS.1.1 CPD_DGL.1.1 CPD_DGL.1.2
PER_10	
Abdeckung	BCM_CLI.1.1

	BCO_CEL.1.1 BCO_CEL.2.1 BCO_CEL.4.1 BCO_CEL.5.1 BCO_RPS.1.1 BCO_RPS.1.2 BCO_RPS.2.1 BDM_SED.4.1 BDM_SFS.1.1 BDM_SFS.3.1 BMA_GAU.2.1 BMA_MAS.5.1 BPS_PSI.1.3 BPS_PSI.1.4 BPS_PSI.1.5 BSP_FOU.1.1 BSP_RIS.5.1 BSP_RIS.5.2 BSP_SPR.1.1 BSP_SPR.4.1 CFO_SPS.1.1 CGS_OML.1.2 CGS_PPS.2.1 CGS_PPS.2.3 CPS_DEV.1.1 CPS_DEV.1.2 CPS_PAQ.1.1 CPS_PAQ.1.2 CPS_PAQ.1.3 CPS_PAQ.1.6
PER_11	
Abdeckung	BCA_AGC.1.1 BCA_AGC.5.1 BGC_INT.3.1 BPS_PSI.1.4 BSP_FOU.1.1 BSP_RIS.1.1 BSP_RIS.3.1 CCS_SIN.2.1 CCS_SIN.2.2 CCS_SIN.2.3 CCS_SIN.3.4 CCS_SIN.3.5 CCS_SSE.1.2 CCS_SSE.1.3 CCS_SSE.1.7 CGI_GDC.1.4 CGI_GDC.3.1 CGI_GDC.3.2 CGI_GDC.3.3 CGI_GDC.3.4 CGI_GDC.3.5 CGI_GDC.3.6 CGI_GIS.1.8 CRR_SEN.1.2
PER_12	
Abdeckung	BSP_FOU.1.1 BSP_FOU.2.1 CCS_CSG.1.2 CDO_APP.1.1 CDO_APP.1.2

	CGS_GMA.2.1
PER_13	
Abdeckung	BOS_ISI.1.1 BPS_PSI.1.1 CGS_GMA.5.1

5.5 PHY : Standort

PHY_01	
Abdeckung	BGC_PRE.6.1 BPE_SEM.2.1 BPE_SEM.4.1 BSP_FOU.2.1 CAR_AAR.1.1 CDS_DES.1.1 CDS_DES.1.2 CGS_GMA.1.1 CGS_GMA.1.2 CGS_GMA.3.1 CGS_GMA.3.2 CGS_GMA.3.3 CGS_GSS.1.1 CGS_GSS.1.2 CIS_ADL.2.1 CIS_MPP.1.1 CIS_MPP.1.2 CIS_MPP.1.3

PHY_02	
Abdeckung	BPE_MMG.1.1 BPE_SEM.3.1 BPE_ZOS.1.1 BPE_ZOS.4.1 CIS_ADL.1.1 CIS_ADL.1.2

PHY_03	
Abdeckung	BOS_SAT.1.2 BPE_SEM.1.1 BPE_SEM.2.1 BPE_ZOS.1.1 BPE_ZOS.2.1 BPE_ZOS.3.1 BPE_ZOS.4.1 BPE_ZOS.5.1 CEI_ERS.1.1 CET_EGT.1.1 CGS_PDI.1.1 CIS_ADL.1.2 CIS_ADL.2.1 CIS_ADL.2.2 CIS_MPP.1.2 CIS_MPP.2.2 CIS_MPP.3.1 CIS_MPP.3.2 CIS_MPP.3.3 CIS_MPP.3.4 CIS_PSI.1.1 CIS_PSI.1.2 CIS_SSI.1.2 CIS_ZOS.1.1 FPT_PHP.1/2.1 FPT_PHP.2.3 FPT_PHP.3.1

PHY_04

Abdeckung	CIS_ADL.2.1 CIS_CDL.1.1 CIS_SSI.1.1 CIS_SSI.1.2 CIS_SSI.1.3 CIS_SSI.1.4 CRH_PDP.1.1 CRH_PDP.1.2 CRH_PDP.1.3 CRR_ETU.1.1 CRR_ETU.1.2 CRR_ETU.2.1 CRR_ETU.2.2
PHY_05	
Abdeckung	BGC_GER.1.1 BPE_SEM.3.1 BPE_ZOS.1.1 BPE_ZOS.4.1 CIS_ADL.1.1 CIS_ADL.1.2 CPD_DGL.1.1
PHY_06	
Abdeckung	CEI_ERS.1.1
PHY_07	
Abdeckung	BGC_GER.1.1 BGC_INT.2.1 BMA_SAS.1.1 BMA_SAS.2.1 BMA_SAS.3.1 BPE_SEM.3.1 BPE_ZOS.1.1 BPE_ZOS.2.1 BPE_ZOS.4.1 CET_EGT.1.3 CET_EGT.1.5 CET_EGT.1.6 CET_EGT.3.1 CET_EGT.3.2 CET_EGT.3.3 CET_EGT.3.4 CET_EGT.3.5 CIS_ADL.1.1 CIS_ADL.3.1 CIS_CSI.1.1 CIS_MPP.1.1
PHY_08	
Abdeckung	CCS_CSG.1.2
PHY_09	
Abdeckung	CIS_CSI.1.1 CIS_CSI.1.2 CIS_MPP.2.1 CIS_MPP.2.2
PHY_10	
Abdeckung	BPE_SEM.4.1 CCS_RGI.1.1 CGS_GMA.1.1 CGS_GMA.1.2

	CGS_GMA.3.1 CGS_GMA.3.2 CGS_GMA.3.3 CIS_ADL.2.1 CIS_CSI.1.1 CIS_CSI.2.1 CIS_MPP.2.2 CIS_PSI.1.1 CIS_PSI.1.2
PHY_11	
Abdeckung	CIS_ADL.3.1 CIS_CSI.1.1
PHY_12	
Abdeckung	CIS_ADL.2.3 CRH_CDT.1.1

5.6 ORG : Organisation

ORG_01	
Abdeckung	BPE_SEM.1.1 BPE_ZOS.1.1 BPE_ZOS.2.1 CET_EGT.1.1 CET_EGT.2.3 CET_EGT.3.1 CGS_GDH.1.2 CGS_GDH.2.1 CIS_PSI.1.1 CIS_PSI.1.2 FCO_NRO.2.1

ORG_02	
Abdeckung	BPE_SEM.1.1 BPE_ZOS.1.1 BPE_ZOS.2.1 BPE_ZOS.3.1 BPE_ZOS.4.1 BPE_ZOS.5.1 CET_EGT.1.10 CET_EGT.1.8 CET_EGT.1.9 CGS_PDI.1.1 FPT_PHP.1/2.1 FPT_PHP.2.3

ORG_03	
Abdeckung	BGC_EIL.1.1 BGC_EIL.2.1 BGC_EIL.4.1 BGC_EIL.7.1

ORG_04	
Abdeckung	BCM_CLI.2.1 BCM_RLC.1.1 BCO_CEL.2.1 BCO_RPS.1.2 BCO_RPS.2.1 BDM_SED.3.1 BDM_SED.5.1 BDM_SFS.1.1 BDM_SFS.2.1 BDM_SFS.3.1 BGC_EIL.5.1 BGC_MSS.1.1 BGC_MSS.3.1 BGC_PRE.1.1 BGC_PRE.2.2 BMA_IMT.2.1 BOS_SAT.1.2 BOS_SAT.1.5 BOS_SAT.2.1 BPE_MMG.1.1 BPE_MMG.2.1 BPE_SEM.1.1 BPE_SEM.2.1 BPE_SEM.3.1 BPE_SEM.3.2

	BPE_SEM.5.1 BPE_ZOS.1.1 BPE_ZOS.2.1 BPE_ZOS.3.1 BPE_ZOS.4.1 BPE_ZOS.5.1 BSP_FOU.1.1 BSP_RIS.5.1 BSP_RIS.5.2 BSP_SPR.1.1 BSP_SPR.4.1 CCS_CHI.1.1 CCS_CSG.1.1 CCS_CSG.1.2 CCS_CSG.1.3 CCS_CSG.1.4 CCS_CSG.1.5 CCS_CSG.1.6 CCS_CSG.1.7 CDO_SDC.1.1 CET_EIP.1.3 CET_EIP.1.4 CET_EIP.1.5 CET_EIP.1.6 CGS_GLI.1.4 CGS_GLI.2.1 CGS_PDI.1.1 CGS_PPS.2.1 CGS_PPS.2.5 CPS_DEV.1.1 CPS_DEV.1.2 CPS_PPT.1.1 CPS_PPT.1.2 CPS_PPT.1.3 CPS_PPT.1.4 CPS_PPT.1.5 FPT_PHP.1/2.1 FPT_PHP.2.3 FPT_PHP.3.1
ORG_05	
Abdeckung	CDO_SDC.1.2 CGS_ARC.1.7 CGS_SVG.1.7
ORG_06	
Abdeckung	BDM_SED.4.1 BGC_EIL.4.1 BGC_EIL.5.1 BGC_MSS.1.1 BGC_PLM.1.1 CGS_CME.1.1 CGS_OML.1.1 CGS_OML.1.3 CGS_PPS.2.3 CGS_PPS.2.4 CPS_PPT.1.1 CPS_PPT.1.2 CPS_PPT.1.3 CPS_PPT.1.4 CPS_PPT.1.5
ORG_07	

Abdeckung	BGC_PRE.1.1 CGS_ARC.1.3 CGS_ARC.1.4 CGS_ARC.1.5 CGS_ARC.1.6 CGS_ARC.1.7 CGS_ARC.1.8 CGS_ARC.1.9

ORG_08

Abdeckung	BGC_INT.1.1 BGC_PRE.1.1 CGS_GLI.1.2 CGS_GSS.1.1 CGS_SVG.1.1 CGS_SVG.1.2 CGS_SVG.1.3 CGS_SVG.1.4 CGS_SVG.1.5 CGS_SVG.1.6 CGS_SVG.1.7 CGS_SVG.1.8 CGS_SVG.1.9

ORG_09

Abdeckung	BCA_AGC.1.1 BCA_AGC.3.1 BCA_AGC.5.1 BGC_MSS.2.1 BGC_PRS.1.1 BGC_PRS.2.1 BPE_SEM.6.1 BSP_FOU.1.1 CCS_CSG.1.2 CDO_APP.1.1 CDO_APP.1.2 CDS_DES.1.1 CEI_ABS.1.5 CFO_FRS.2.2 CGI_GIS.3.1 CGI_GIS.3.2 CGI_GIS.3.3 CGS_CSR.1.2 CRH_DDE.1.1 CRH_DDE.1.2 FDP_RIP.1.1 FDP_RIP.2.1

ORG_10

Abdeckung	BMA_MAS.4.1 BMA_REU.1.1 BMA_REU.2.1 CGS_GMP.1.1 CGS_GMP.1.2 FIA_SOS.1.1 FIA_SOS.2.1 FIA_SOS.2.2

ORG_11

Abdeckung	

ORG_12

Abdeckung	BGC_EIL.4.1

	CCS_CSG.1.1 CCS_CSG.1.2 CFO_SPS.1.1 CFO_SPS.1.2 CGS_CME.1.1 CGS_CSR.1.2

ORG_13	
Abdeckung	BGC_PRS.2.1 BPE_SEM.4.1 CCC_RGF.1.1 CCC_RGF.1.2 CEI_CDT.1.1 CEI_CDT.1.2

ORG_14	
Abdeckung	BCM_CLI.1.2 BDM_SSA.3.1 BGC_EIL.1.1 BMA_GAU.1.1 BMA_GAU.2.1 BMA_GAU.4.1 BMA_MAS.2.1 BMA_MAS.3.1 BMA_SAS.2.1 BOS_ISI.3.1 BPS_PSI.1.3 BSP_FOU.1.1 BSP_FOU.2.1 BSP_SPR.1.1 BSP_SPR.3.1 BSP_SPR.4.1 CCS_SRI.1.1 CDO_APP.1.1 CDO_APP.1.2 CFO_FRS.1.2 CFO_FRS.1.3 CFO_FRS.1.5 CGI_GDC.2.3 CGI_GDC.2.4 CGI_GDC.2.5 CGI_GDC.3.3 CGI_GDC.3.5 CGI_GDC.3.6 CGI_GDC.4.5 CGI_LCI.1.4 CGI_LCI.1.5 CGI_LCI.1.6 CGI_LCI.1.7 CGS_CIR.1.3 CGS_GDH.1.1 CGS_GDH.1.2 CGS_GDH.1.3 CGS_GDH.1.5 CGS_GDH.1.6 CGS_GDH.1.7 CGS_GDH.1.8 CGS_GDH.1.9 CGS_GDH.2.1 CGS_GDH.2.2 CGS_GMA.2.1

	CGS_OES.1.1 CGS_OES.1.2 CGS_OES.1.3 CGS_PAI.1.1 CGS_PAI.1.2 CGS_PAI.1.3 CRH_DDE.1.1 CRH_DDE.1.2 CRH_QDP.1.1

ORG_15

Abdeckung	BCM_CLI.1.1 BCM_CLI.1.2 BCM_CLI.2.1 BCO_CEL.4.1 BCO_CEL.5.1 BDM_COC.2.1 BGC_EIL.2.1 BGC_EIL.4.1 BGC_EIL.7.1 BGC_GER.1.1 BGC_MSS.1.1 BGC_MSS.2.1 BGC_MSS.3.1 BMA_IMT.2.1 BMA_MAA.1.1 BPE_MMG.1.1 BPE_MMG.2.1 BPE_SEM.6.1 BPS_PSI.1.5 BSP_SPR.3.1 CGS_CIR.1.1 CGS_CIR.1.2 CGS_GDH.1.1 CGS_GDH.1.4 CGS_GMR.1.1 CGS_GMR.1.2 CPD_DGL.1.1 FDP_RIP.1.1 FDP_RIP.2.1

ORG_16

Abdeckung	BCA_AGC.1.1 BCA_AGC.2.1 BCA_AGC.3.1 BCA_AGC.4.1 BCA_AGC.5.1 BGC_PRE.3.1 BSP_RIS.1.1 CCS_SIN.2.1 CCS_SIN.2.3 CCS_SIN.3.1 CCS_SIN.3.2 CCS_SIN.3.4 CCS_SIN.3.5 CGS_GMA.1.1 CGS_GMA.1.2 CGS_GSS.1.3 CGS_GSS.1.4 CGS_GSS.2.1 CGS_GSS.2.2

ORG_17

Abdeckung	CCS_SIN.1.1 CCS_SIN.1.2 CCS_SIN.1.3 CCS_SIN.1.4 CCS_SIN.2.1 CCS_SIN.3.1 CCS_SIN.3.2

ORG_18

Abdeckung	BCO_CEL.4.1 BCO_RPS.1.1 BCO_RPS.1.2 BCO_RPS.2.1 BPS_PSI.1.4 BSP_RIS.5.1 BSP_RIS.5.2 BSP_SPR.1.1 BSP_SPR.4.1

ORG_19

Abdeckung	

ORG_20

Abdeckung	BDM_ESS.1.1 BDM_SED.1.1 BDM_SED.2.1 BDM_SED.4.1 BDM_SED.5.1 BDM_SFS.3.1 BGC_MSS.1.1 BGC_PLM.1.1 BGC_PRS.2.1 BOS_SAT.1.3 CGS_OML.1.1 CGS_OML.1.2 CGS_OML.1.3 CGS_PPS.2.3

ORG_21

Abdeckung	BOS_ISI.1.2 BSP_RIS.1.1 BSP_RIS.4.1 CGI_GIS.2.1 CGI_GIS.2.2 CGI_GIS.2.3 CGI_GIS.2.4 CGI_GIS.2.5 CGI_GIS.3.1 CGI_GIS.3.2 CGI_GIS.3.3

ORG_22

Abdeckung	BCO_RPS.1.1 BCO_RPS.1.2 BCO_RPS.2.1 BDM_COC.4.1 BGC_PRE.2.1 BMA_SAS.1.1 BMA_SAS.2.1 BMA_SAS.3.1 BOS_ISI.7.1 BOS_SAT.1.1 CCS_SIN.3.3

	CCS_SSE.1.1 CIS_CSI.1.3 CPD_INP.1.1 FAU_ARP.1.1 FAU_GEN.1.1 FAU_GEN.1.2 FAU_GEN.2.1 FAU_SAA.1.1 FAU_SAA.1.2 FAU_SAA.2.1 FAU_SAA.2.2 FAU_SAA.2.3 FAU_SAA.3.1 FAU_SAA.3.2 FAU_SAA.3.3 FAU_SAA.4.1 FAU_SAA.4.2 FAU_SAA.4.3
ORG_23	
Abdeckung	BCO_RPS.1.1 BCO_RPS.1.2 BPE_ZOS.1.1 CIS_CSI.1.1 CIS_CSI.1.2 CIS_PSI.1.1 CIS_PSI.1.2 CIS_PSI.1.3
ORG_24	
Abdeckung	BGC_PRE.1.1 BGC_PRE.3.1 BSP_RIS.1.1 BSP_RIS.2.1 CCS_SIN.2.1 CCS_SIN.2.3 CCS_SIN.3.1 CCS_SIN.3.2 CCS_SIN.3.4 CCS_SIN.3.5 CCS_SSE.1.1 CCS_SSE.1.2 CCS_SSE.1.3 CCS_SSE.1.4 CCS_SSE.1.5 CCS_SSE.1.6 CCS_SSE.1.7 CGI_GDC.1.1 CGI_GDC.1.2 CGI_GDC.1.3 CGI_GDC.1.4 CGI_GDC.2.1 CGI_GDC.2.2 CGI_GDC.2.6 CGI_GDC.3.1 CGI_GDC.3.2 CGI_GDC.3.4 CGI_GDC.4.1 CGI_GDC.4.2 CGI_GDC.4.3 CGI_GDC.4.4 CGI_GDC.4.6 CGI_GIS.1.1

	CGI_GIS.1.2 CGI_GIS.1.3 CGI_GIS.1.4 CGI_GIS.1.5 CGI_GIS.1.6 CGI_GIS.1.7 CGI_GIS.1.8 CGI_LCI.1.1 CGI_LCI.1.2 CGI_LCI.1.3 CGS_GSS.2.1 CGS_GSS.2.2 CIS_SSI.1.1
ORG_25	
Abdeckung	BOS_SAT.1.3 BOS_SAT.2.1 CCS_CSP.1.1 CCS_CSP.1.2 CCS_CSP.1.3 CCS_CSP.1.4 CCS_CSP.2.1 CCS_SIN.1.1 CET_EGT.1.1 CET_EGT.1.2 CET_EGT.1.3 CET_EGT.1.4 CET_EGT.1.5 CET_EGT.1.6 CET_EGT.2.1 CET_EGT.2.2 CET_EGT.2.3 CET_EIP.1.1 CET_EIP.1.3 CET_EIP.1.4 CET_EIP.1.5 CET_PLD.1.4
ORG_26	
Abdeckung	BCM_RLC.1.1 BDM_ESS.1.1 BDM_SED.4.1 BDM_SED.5.1 BDM_SFS.1.1 BGC_PRS.2.1 CGS_PPS.2.3 CGS_PPS.2.4 CGS_REC.1.1
ORG_27	
Abdeckung	BGC_INT.2.1 BGC_PRS.2.1 BOS_SAT.1.2 BPE_SEM.1.1 BPE_SEM.3.1 BPE_SEM.3.2 BPE_SEM.4.1 BPE_ZOS.1.1 BPE_ZOS.2.1 BPE_ZOS.3.1 BPE_ZOS.4.1 BPE_ZOS.5.1 CCC_RGF.1.1

	CCC_RGF.1.2 CET_EIP.1.3 CET_EIP.1.6 CGS_GMA.1.1 CGS_GMA.1.2 CGS_GMA.2.1 CGS_GMA.3.1 CGS_GMA.3.2 CGS_GMA.3.3 CGS_GSU.1.1 CGS_GSU.1.2 CGS_GSU.2.1 CGS_GSU.2.2 CGS_GSU.2.3 CGS_GSU.3.1 CGS_GSU.3.2 CGS_GSU.3.3 CGS_PDI.1.1 FPT_PHP.1/2.1 FPT_PHP.2.3 FPT_PHP.3.1
ORG_28	
Abdeckung	CDO_APP.1.1 CDO_APP.1.3 CGS_PPS.2.3
ORG_29	
Abdeckung	CPS_PAQ.1.1 CPS_PAQ.1.2 CPS_PAQ.1.3 CPS_PAQ.1.4 CPS_PAQ.1.5 CPS_PAQ.1.6
ORG_30	
Abdeckung	BCM_RLC.1.1 BCO_CEL.5.1 BDM_COC.2.1 BGC_GER.1.1 BGC_MSS.4.1 BGC_PRE.4.1 BMA_EMA.1.1 BMA_GAU.1.1 BMA_GAU.2.1 BMA_GAU.4.1 BMA_MAR.1.1 BMA_MAR.2.1 BMA_MAR.3.1 BMA_MAR.4.1 BMA_MAR.5.1 BMA_MAR.7.1 BMA_MAS.2.1 BMA_MAS.3.1 BMA_SAS.1.1 BMA_SAS.2.1 BOS_SAT.1.1 BOS_SAT.1.2 BOS_SAT.1.3 BOS_SAT.1.4 BOS_SAT.1.5 BOS_SAT.2.1 BPE_SEM.1.1

	BPE_SEM.3.1 BPE_SEM.3.2 BPE_ZOS.1.1 BPE_ZOS.2.1 BPE_ZOS.3.1 BPE_ZOS.4.1 BPE_ZOS.5.1 CEI_ABS.1.1 CET_EGT.2.3 CGS_CSR.1.3 CGS_GDH.1.1 CGS_GDH.1.2 CGS_GDH.1.3 CGS_GDH.1.4 CGS_GDH.1.5 CGS_GDH.1.6 CGS_GDH.1.7 CGS_GDH.1.8 CGS_GDH.1.9 CGS_GMA.4.1 CGS_PAI.1.2 CGS_PAI.1.3 CGS_PDI.1.1 CGS_PEP.1.1 CGS_PPS.3.2 FPT_PHP.1/2.1 FPT_PHP.2.3 FPT_PHP.3.1
ORG_31	
Abdeckung	CEI_ABS.1.6 CEI_ABS.1.7 CRH_PDP.1.1
ORG_32	
Abdeckung	BPS_PSI.2.2 BPS_PSI.2.4 CEI_ABS.1.1 CEI_ABS.1.2 CEI_ABS.1.3 CEI_ABS.1.4 CEI_ABS.1.5
ORG_33	
Abdeckung	BCO_RPS.1.1 BCO_RPS.1.2 BDM_SSA.1.1 BDM_SSA.4.1 BGC_PRE.4.1 BMA_EMA.1.1 BMA_GAU.2.1 BMA_MAA.1.1 BMA_MAA.2.1 BMA_MAR.1.1 BMA_MAR.6.1 BMA_MAR.7.1 BMA_MAS.1.1 BMA_MAS.3.1 BMA_MAS.5.1 BMA_REU.2.1 BOS_SAT.1.2 BOS_SAT.1.5 BPE_SEM.1.1

	BPE_SEM.3.1 BPE_SEM.3.2 BPE_ZOS.1.1 BPE_ZOS.2.1 BPE_ZOS.3.1 BPE_ZOS.4.1 BPE_ZOS.5.1 BSP_SPR.3.1 CET_EGT.1.3 CET_PLD.1.2 CGS_GLI.2.1 CGS_OES.1.2 CGS_OES.1.3 CGS_PAI.2.1 CGS_PAI.2.2 CGS_PAI.2.3 CGS_PDI.1.1 CGS_PPS.2.5 FPT_PHP.1/2.1 FPT_PHP.2.3 FPT_PHP.3.1
ORG_34	
Abdeckung	BOS_ISI.5.1 BOS_ISI.5.2 BOS_ISI.5.3 BOS_ISI.6.1 BOS_ISI.6.2 BOS_ISI.6.3
ORG_35	
Abdeckung	BMA_SAS.1.1 BMA_SAS.2.1 BMA_SAS.3.1
ORG_36	
Abdeckung	CGS_GDH.1.3 CGS_PAI.1.4
ORG_37	
Abdeckung	BCO_CEL.1.1 BCO_CEL.4.1 BCO_CEL.7.1 BCO_CEL.7.2 BDM_SSA.1.1 BDM_SSA.4.1 BMA_MAS.3.1 BMA_SAS.1.1 BMA_SAS.2.1 BMA_SAS.3.1 BOS_SAT.1.3 BOS_SAT.2.1 BSP_RIS.5.1 BSP_RIS.5.2 BSP_SPR.1.1 BSP_SPR.3.1 BSP_SPR.4.1 CCC_CLR.1.1
ORG_38	
Abdeckung	BDM_SED.4.1 BDM_SED.5.1 BGC_PRE.6.1

	BOS_ISI.4.1 BOS_ISI.7.1 BOS_SOT.1.1 BOS_SOT.1.2 CCC_CLR.1.2 CGS_GPC.1.1 CGS_GPC.1.2 CGS_PPS.2.3 CRI_MOF.1.1 CRI_MOF.2.1
ORG_39	
Abdeckung	BDM_COC.2.1 BDM_COC.4.1 BGC_INT.2.1 BMA_SAS.1.1 BMA_SAS.2.1 BMA_SAS.3.1 CGS_GDA.1.4 FAU_SAA.2.1 FAU_SAA.2.2 FAU_SAA.2.3 FAU_SAA.3.1 FAU_SAA.3.2 FAU_SAA.3.3 FAU_STG.1/2.1 FAU_STG.1/2.2 FAU_STG.2.3 FAU_STG.3.1 FAU_STG.4.1
ORG_40	
Abdeckung	BCO_CEL.1.1 BCO_CEL.2.1 BCO_CEL.4.1 BCO_CEL.5.1 BPS_PSI.1.3
ORG_41	
Abdeckung	BGC_PRE.1.1 BMA_GAU.1.1 BPS_PSI.1.3 BSP_FOU.1.1 CDO_APP.1.1 CDO_APP.1.2
ORG_42	
Abdeckung	BDM_ESS.1.1 BDM_SFS.1.1 BGC_PRS.2.1 BMA_GAU.2.1 CGS_REC.1.1 FCO_NRO.1.1
ORG_43	
Abdeckung	CGS_GPC.2.1 CGS_GPC.2.2 CGS_GPC.2.3 CGS_GPC.2.4
ORG_44	
Abdeckung	CRR_ETU.1.1 CRR_ETU.1.2

	CRR_ETU.2.2
ORG_45	
Abdeckung	CRH_CDT.1.1 CRH_CDT.1.2 CRH_PDP.1.1

Formular zur Meinungsäußerung

Dieses Formular kann an folgende Adresse gesendet werden:

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP
conseil.dcssi@sgdn.pm.gouv.fr

Identifizierung der Beitrags
Name und Institution (fakultativ): .....
Elektronische Adresse: .....
Datum: .....

Allgemeine Bemerkungen zu diesem Dokument
Entspricht das Dokument Ihren Bedarfe? Ja ☐ Nein ☐

Wenn ja:

Glauben Sie, dass es vom Inhalt her verbessert werden könnte? Ja ☐ Nein ☐

Wenn ja:

Was haben Sie vermisst?
.....
.....

Welche Teile des Dokuments erscheinen Ihnen überflüssig oder unangemessen?
.....
.....

Glauben Sie, dass es von der Form her verbessert werden könnte? Ja ☐ Nein ☐

Wenn ja:

In welchem Bereich ist es verbesserungsfähig?
- Leserlichkeit, Verständnis ☐
- Aufmachung ☐
- Sonstiges ☐

Formulieren Sie Ihre Wünsche bezüglich der Form:
.....
.....

Wenn nein:

Geben Sie den Bereich an, der Ihnen nicht gefällt und umschreiben Sie, was Ihnen gefallen hätte:
.....
.....

Welche weiteren Themen hätten Sie gerne vorgefunden?
.....
.....

Spezielle Bemerkungen zu diesem Dokument

In nachstehender Tabelle können Sie detailliert Stellung nehmen.

Unter Nr. ist die Laufnummer einzutragen.

In die Spalte "Typ" sind zwei Buchstaben einzutragen:

Mit dem ersten Buchstaben wird die Kategorie der Bemerkung umschrieben:

- R Rechtschreib- oder Grammatikfehler
- E Mangelnde Erläuterung oder Klärung des behandelten Punktes
- U Text unvollständig oder nicht vorhanden
- F Fehler

Der zweite Buchstabe beschreibt den Bedeutungsgrad:

- g geringfügig
- G Gravierend

Unter "Referenz" ist die genaue Lokalisierung im Text anzugeben (Kapitelnummer, Zeile...).

Unter "Wortlaut der Bemerkung" kann ein Kommentar abgegeben werden.

Unter "vorgeschlagene Lösung" können Mittel zur Lösung des aufgeworfenen Problems angegeben werden.

Nr.	Typ	Referenz	Wortlaut der Bemerkung	Vorgeschlagene Lösung
1				
2				
3				
4				
5				

Vielen Dank für Ihre Teilnahme