

UNIFIED FACILITIES CRITERIA (UFC)

CYBER-SICHERHEIT VON LIEGENSCHAFTSABHÄNGIGEN KONTROLLSYSTEMEN



FÜR DIE VERÖFFENTLICHUNG FREIGEgeben, OHNE EINSCHRÄNKUNG

UNIFIED FACILITIES CRITERIA (UFC)

CYBER-SICHERHEIT VON LIEGENSCHAFTSABHÄNGIGEN KONTROLLSYSTEMEN

Alles urheberrechtlich geschützte Material in diesen UFC-Vorschriften ist an entsprechender Stelle als solches gekennzeichnet.

Für die Verwendung von urheberrechtlich geschütztem Material, außer in diesen UFC-Vorschriften, ist die Genehmigung des Urhebers einzuholen.

U.S. ARMY CORPS OF ENGINEERS

NAVAL FACILITIES ENGINEERING COMMAND (Herausgeber)

AIR FORCE CIVIL ENGINEER CENTER

Änderungsverfolgung (die Änderungen sind folgendermaßen gekennzeichnet: \1\ ... /1/)

Änderungsnr.	Datum	Ort
1	19.01.2017	<u>Überarbeitete Abschnitte 3-3, 3-6 (zweiter Aufzählungspunkt), 3-6.2, 4-3 (zweiter bis letzter Aufzählungspunkt) und 5-2.2.2.</u>

VORWORT

Das System der Unified Facilities Criteria (UFC) wird von MIL-STD 3007 vorgeschrieben und enthält Kriterien zu Planung, Ausführung, Bau, Erhaltung, Instandsetzung und Modernisierung und gilt für Military Departments, Defense Agencies und DoD Field Activities gemäß [USD \(AT&L\) Memorandum](#) vom 9. Mai 2002. Die UFC gelten für sämtliche Projekte des US-Verteidigungsministeriums sowie, wo zutreffend, für Arbeiten anderer Kunden. Jede Baumaßnahme außerhalb der Vereinigten Staaten wird ebenfalls von Status of Forces Agreements (SOFA), den Host Nation Funded Construction Agreements (HNFA) und in einigen Fällen den Bilateral Infrastructure Agreements (BIA) geregelt. Deshalb muss das Akquisitionsteam die Einhaltung der strengeren UFC, SOFA, HNFA und BIA, je nachdem was zutreffend ist, sicherstellen.

Die UFC sind lebendige Dokumente und werden periodisch überprüft, auf den neuesten Stand gebracht und den Nutzern als Teil der Dienstleistungs-Verantwortung für technische Kriterien für Militärbaumaßnahmen zur Verfügung gestellt. Headquarters, U.S. Army Corps of Engineers (HQUSACE), Naval Facilities Engineering Command (NAVFAC) und Air Force Civil Engineer Center (AFCEC) sind für die Verwaltung des UFC-Systems verantwortlich. Die Verteidigungsbehörden sollten sich zwecks Interpretation und Verbesserungen an die ausstellende Behörde wenden. Der technische Inhalt der UFC liegt im Verantwortungsbereich der entsprechenden Arbeitsgruppe des US-Verteidigungsministeriums. Die empfohlenen Änderungen mit den entsprechenden Begründungen sind dem entsprechenden Service Proponent Office mit dem folgenden elektronischen Formblatt zu übermitteln: [Änderungsantrag für Vorschriften](#). Das Formblatt ist auch über die unten aufgeführten Internetseiten zugänglich.

Die UFC ist zum Zeitpunkt des Erlasses gültig und wird nur über elektronische Medien der folgenden Quelle verteilt:

- Whole Building Design Guide web site <http://dod.wbdg.org/>

Papierausdrucke der UFC, die mit Hilfe elektronischer Medien ausgedruckt werden, sind vor Verwendung mit der aktuellen elektronischen Ausgabe abzugleichen, um sicherzugehen, dass die Ausdrucke aktuell sind.

GENEHMIGT VON:

JAMES C. DALTON, P.E.
Chief, Engineering and Construction
U.S. Army Corps of Engineers

JOSEPH E. GOTT, P.E.
Chief Engineer
Naval Facilities Engineering Command

EDWIN H. OSHIBA, SES, DAF
Deputy Director of Civil Engineers
DCS/Logistics, Engineering &
Force Protection

MICHAEL McANDREW
DASD (Facilities Investment and Management)
Office of the Assistant Secretary of Defense
(Energy, Installations, and Environment)

UNIFIED FACILITIES CRITERIA (UFC)
ZUSAMMENFASSUNG DES NEUEN DOKUMENTS

Dokument: UFC 4-010-06, *Cybersicherheit von liegenschaftsabhängigen Kontrollsystemen*

Ersetzt: -

Beschreibung: UFC 4-010-06 enthält Anforderungen für die Einbeziehung der Cybersicherheit in die Planung liegenschaftsabhängiger Kontrollsysteme.

Begründung: DoDI 8500.01, Cybersicherheit, fordert die Implementierung eines „mehrstufigen Risikomanagementprozesses für die Cybersicherheit... wie in den Veröffentlichungen National Institute of Standards and Technology (NIST) Special Publication (SP) 800-39 und Committee on National Security Systems (CNSS) Policy 22“ beschrieben. Ferner ist die Anwendung der NIST SP 800-37 und der Übergang auf CNSSI Nr. 1253 und NIST SP 800-53 vorgeschrieben. NIST SP 800-82 R2, Anhang G, wird als Schablone gemäß CNSSI Nr. 1253 für Kontrollsysteme verwendet. Diese UFC enthält Kriterien für die Einbeziehung der Cybersicherheit in die Planung von Kontrollsystemen, so dass entsprechende Sicherheitskontrollen (Risk Management Framework (RMF)) während der Planung und bei der anschließenden Ausführung berücksichtigt werden können.

Auswirkung: Obwohl die Einbeziehung der Cybersicherheit in die Planung und Ausführung von Kontrollsystemen zu höheren Planungs- und Ausführungskosten führt, ist es kostengünstiger, diese Sicherheitskontrollen bereits zu Beginn der Planung zu berücksichtigen, als diese für ein bereits geplantes und installiertes System umzusetzen. In der Vergangenheit wurden diese Anforderungen an die Cybersicherheit nicht für Kontrollsysteme berücksichtigt, folglich wird die Umsetzung dieser Anforderungen an die Cybersicherheit sowohl die Kosten als auch die Sicherheit erhöhen. Diese Kostenerhöhung wird niedriger sein als die Kostenerhöhung für eine nachträgliche Berücksichtigung dieser Anforderungen.

Anmerkung: Diese UFC basiert auf NIST SP 800-53 R4 und NIST SP 800-82 R2. Sobald neue Versionen der NIST-Publikationen veröffentlicht werden, können entsprechende Informationen über den RMF Knowledge Service (<https://rmfks.osd.mil>) abgerufen werden. Außerdem werden diese auch in den aktualisierten und überarbeiteten Versionen dieser UFC berücksichtigt.

INHALTSVERZEICHNIS

KAPITEL 1: EINLEITUNG	1
1-1 HINTERGRUND	1
1-2 ZIEL UND UMFANG	1
1-3 GELTUNGSBEREICH	1
1-4 ALLGEMEINE BAUANFORDERUNGEN	1
1-5 Organisation	2
1-6 ANSPRECHPARTNER FÜR CYBER-SICHERHEIT NACH TEILSTREITKRÄFTEN ...	2
1-7 QUELLENANGABEN	2
1-8 GLOSSAR	2
KAPITEL 2: ÜBERBLICK - CYBER-SICHERHEIT BEI KONTROLLSYSTEMEN	3
2-1 ÜBERBLICK ÜBER DAS RISK MANAGEMENT FRAMEWORK	3
2-1.1 Sicherheitskontrollen	3
2-1.2 Ziel des RMF	3
2-1.3 Plattform-Informationstechnik	3
2-1.4 Vererbte Sicherheitskontrollen	4
2-1.5 Anwendbarkeit von RMF-Sicherheitskontrollen auf die Planung	4
2-2 5-STUFIGER AUFBAU DES KONTROLLSYSTEMS	5
2-2.1 "Standard-IT"-Anteile des Kontrollsystems	6
2-2.2 "Nicht-Standard-IT"-Anteile des Kontrollsystems	7
2-2.3 Plattform Enclave	7
2-3 ÜBERBLICK ÜBER DIE BESCHAFFUNG VON KONTROLLSYSTEMEN	7
KAPITEL 3: ANWENDUNG VON CYBER-SICHERHEIT IN DER PLANUNG	9
3-1 ÜBERSICHT	9
3-1.1 Fünf Schritte für die Planung der Cyber-Sicherheit	9
3-1.2 Definition von "Organisation"	9
3-2 SCHRITT 1: AUSWIRKUNGSGRAD FÜR DAS KONTROLLSYSTEM FESTLEGEN	10
3-3 SCHRITT 2: FESTLEGUNG DER SICHERHEITSKONTROLLEN	10
3-3.1 Individuell anzupassende empfohlene Sicherheitskontrollen	11
3-4 SCHRITT 3: IDENTIFIKATION VON CCIS	11
3-5 SCHRITT 4: ZUORDNUNG VON CCIS NACH ZUSTÄNDIGKEIT	11
3-6 SCHRITT 5: EINBINDUNG VON ANFORDERUNGEN AN DIE CYBER- SICHERHEIT	12

3-6.1	Umgang mit vom US-Verteidigungsministerium festgelegten Werten bei CCIs	13
3-6.2	Sonstige "Von der Organisation festgelegte Werte" bei CCIs	13
3-6.3	CCIs für die Definition von Anforderungen und die Implementierung.....	13
KAPITEL 4: MINDESTPLANUNGSANFORDERUNGEN AN CYBER-SICHERHEIT		15
4-1	AUSFALLMINIMIERUNGSPLANUNG	15
4-1.1	Reduzierung der Netzwerkabhängigkeit	15
4-1.2	Reduzierung irrelevanter Funktionen.....	15
4-2	AUSFALLMANAGEMENTPLANUNG	15
4-2.1	Planung eines sanften Ausfalls	15
4-2.2	Verminderter Betrieb	16
4-2.3	Redundanz.....	16
4-3	ES SIND KEINE IT-STANDARDFUNKTIONEN ZU IMPLEMENTIEREN	16
4-4	ES IST KEIN FERNZUGRIFF VORZUSEHEN.....	17
KAPITEL 5: DOKUMENTATION DER CYBER-SICHERHEIT		19
5-1	ÜBERSICHT	19
5-2	ANFORDERUNGEN NACH PLANUNGSPHASE.....	19
5-2.1	Planungsgrundlage	19
5-2.2	Planungsvorlagen	19
ANHANG A: QUELLENANGABEN.....		21
ANHANG B: GLOSSAR		23
B-1	ABKÜRZUNGEN.....	23
B-1.1	Allgemeine Abkürzungen	23
B-1.2	Abkürzungen für den Bereich Sicherheitskontrolle	24
B-2	BEGRIFFSDEFINITIONEN	25
ANHANG C: RISK MANAGEMENT FRAMEWORK (RMF), ÜBERSICHT		31
C-1	RMF - ÜBERSICHT	31
C-2	RMF - VORGANG	31
C-3	DEFINITION VON KONTROLLEN GEMÄSS NIST UND DODI 8510.....	32
C-3.1	Kontrollfamilien.....	32
C-3.2	Kontrollelemente und Erweiterungen.....	33
C-3.3	Control Correlation Identifier.....	35
C-4	ANFORDERUNGSBESCHREIBUNG UND -UMSETZUNG.....	36
C-4.1	CCIs zur Anforderungsbeschreibung.....	36

C-4.2	CCIs zur Anforderungsumsetzung.....	37
C-5	PLATTFORM-INFORMATIONSTECHNOLOGIE	37
ANHANG D: PLATFORM ENCLAVE		39
D-1	PLATFORM ENCLAVE, KONZEPT-ÜBERSICHT	39
D-2	PLATFORM ENCLAVE MIT ZWEI AUTORISIERUNGEN.....	39
D-3	Vorteile der Platform Enclave	39
D-4	PLATFORM-ENCLAVE-ANSATZ DER ARMY.....	40
D-5	PLATFORM-ENCLAVE-ANSATZ DER NAVY FÜR BCS UND UCS	40
D-6	PLATFORM-ENCLAVE-ANSATZ DER AIR FORCE.....	40
ANHANG E: 5-STUFIGER AUFBAU DES KONTROLLSYSTEMS		43
E-1	EINLEITUNG	43
E-2	5-STUFIGER AUFBAU - ÜBERSICHT	44
E-3	LEVEL 0: SENSOREN UND AKTOREN	45
E-4	LEVEL 1: FIELD CONTROL SYSTEM (NICHT IP)	47
E-5	LEVEL 2: FIELD CONTROL SYSTEM (IP)	49
E-6	LEVEL 3: FIELD POINT OF CONNECTION (FPOC)	54
E-7	LEVEL 4: FRONTEND KONTROLLSYSTEM UND IP-NETZWERK KONTROLLSYSTEM	55
E-8	LEVEL 5: EXTERNE VERBINDUNG UND KONTROLLSYSTEM-MANAGEMENT ...	57
ANHANG F: CYBER-SICHERHEIT – ÜBERLEGUNGEN ZUR EINBINDUNG KRITISCHER SYSTEME DER GEBÄUDELEITTECHNIK UND VERSORGUNGSTECHNIK IN EIN NICHT KRITISCHES SYSTEM (UMCS)		59
F-1	EINLEITUNG	59
F-2	BESCHRÄNKUNG EXTERNER FUNKTIONEN.....	60
F-3	MÖGLICHKEITEN ZUR ANBINDUNG VON FCS AN UMCS	60
F-3.1	E/A-Schnittstelle (Hardware)	61
F-3.2	Gateway-Schnittstelle (Hardware)	62
F-3.3	Firewall-Schnittstelle	63
F-4	WEITERE ÜBERLEGUNGEN	64
F-4.1	Lokale Benutzeroberflächen.....	64
F-4.2	Risikomanagement	64
ANHANG G: LEITFADEN ZUR IMPLEMENTIERUNG VON SICHERHEITSKONTROLLEN		67
G-1	EINLEITUNG	67
G-2	ALLGEMEIN.....	67

G-2.1	Terminologie für Kontrollsysteme im Vergleich zu Standard-IT-Systemen.....	67
G-2.2	Durch das US-Verteidigungsministerium festgelegte Werte	67
G-2.3	Sicherheitskontrollen die „automatisch erfüllt“ werden	67
G-2.4	Anwendbarkeit von Sicherheitskontrollen gemäß 5-stufigem Aufbau	68
G-2.5	Anwendbarkeit Auswirkungsgrad	68
G-3	LEITFADEN FÜR INDIVIDUELLE SICHERHEITSKONTROLLEN	68
G-3.1	Kontrollfamilie Zugangskontrolle (AC)	68
G-3.2	Kontrollfamilie Prüfungs- und Rechenschaftspflicht (AU).....	72
G-3.3	Kontrollfamilie Sicherheitsbewertung und Autorisierung (CA).....	73
G-3.4	Kontrollfamilie Konfigurationsmanagement (CM).....	74
G-3.5	Kontrollfamilie Krisenplanung (CP).....	75
G-3.6	Kontrollfamilie Identifizierung und Autorisierung (IA)	76
G-3.7	Kontrollfamilie Vorfallreaktion (IR)	78
G-3.8	Kontrollfamilie Wartung (MA).....	78
G-3.9	Kontrollfamilie Medienschutz (MP)	78
G-3.10	Kontrollfamilie physische Sicherheitssysteme und Schutz vor Umwelteinflüssen (PE)	79
G-3.11	Kontrollfamilie Planung (PL)	80
G-3.12	Kontrollfamilie Programm-Management (PM).....	81
G-3.13	Kontrollfamilie Personalsicherheit (PS).....	82
G-3.14	Kontrollfamilie Risikobewertung (RA)	82
G-3.15	Kontrollfamilie Übernahme von Systemen und Diensten (SA)	83
G-3.16	Kontrollfamilie System- und Kommunikationsschutz (SC)	84
G-3.17	Kontrollfamilie System- und Informationsintegrität (SI)	87
ANHANG H:	CONTROL CORRELATION IDENTIFIER (CCI) - TABELLEN	89
H-1	EINLEITUNG	89
H-2	TABELLENSTRUKTUR UND INHALT	89
H-3	ANMERKUNGEN ZU CCI-TABELLEN	90
H-3.1	Von der Plattform Enclave vererbte Kontrollen.....	90
H-3.2	CCIs in mehreren Tabellen.....	90
H-4	BESCHREIBUNGEN ZU DEN CCI-TABELLEN.....	91
H-4.1	CCI-Übersichtstabelle	91
H-4.2	Für Kontrollsysteme ungeeignete CCIs	91
H-4.3	CCIs, die aus der Grundvorgabe für Kontrollsysteme mit GERINGEN Auswirkungen entfernt wurden	91

H-4.4	Planer-CCIs	91
H-4.5	Platform Enclave CCIs	91
H-5	CCI-TABELLEN	92

ABBILDUNGEN

Abbildung 2-1: 5-stufiger Aufbau des Kontrollsystems	6
Abbildung 2-2: Aufbau des Kontrollsystems	8
Abbildung C-3: NIST Risk Management Framework Schritte	32
Abbildung C-4: NIST SP 800-53 Kontrolle AC-2.....	34
Abbildung D-1: Navy and Air Force Platform Enclave und operative Architektur.....	40
Abbildung E-1: 5-stufiger Aufbau des Kontrollsystems.....	44
Abbildung F-1: E/A-Schnittstelle (Hardware), Beispiel.....	61

TABELLEN

Tabelle E-2: Level 1.....	47
Tabelle E-3: Level 2.....	49
Tabelle E-4: Level 3.....	54
Tabelle E-5: Level 4.....	55
Tabelle E-6: Level 5.....	57
Tabelle G-1: Kontrollfamilie Zugangskontrolle (AC).....	69
Tabelle G-2 Kontrollfamilie Prüfungs- und Rechenschaftspflicht (AU).....	72
Tabelle G-3: Kontrollfamilie Sicherheitsbewertung und Autorisierung (CA).....	73
Tabelle G-4: Kontrollfamilie Konfigurationsmanagement (CM).....	74
Tabelle G-5: Kontrollfamilie Krisenplanung (CP)	75
Tabelle G-6: Kontrollfamilie Identifizierung und Autorisierung (IA)	77
Tabelle G-7: Kontrollfamilie Wartung (MA)	78
Tabelle G-8: Kontrollfamilie Medienschutz (MP).....	79
Tabelle G-9: Kontrollfamilie physische Sicherheitssysteme und Schutz vor Umwelteinflüssen (PE)	80
Tabelle G-10: Kontrollfamilie Planung (PL).....	81
Tabelle G-11: Kontrollfamilie Programm-Management (PM)	82
Tabelle G-12: Kontrollfamilie Risikobewertung (RA).....	83
Tabelle G-13: Kontrollfamilie Übernahme von Systemen und Diensten (SA)	84
Tabelle G-14: Kontrollfamilie System- und Kommunikationsschutz (SC)	85
Tabelle G-15: Kontrollfamilie System- und Informationsintegrität (SI)	87
Tabelle H-1: Überblick über CCIs für Systeme mit GERINGEN und MITTLEREN Auswirkungen	92
Tabelle H-2: Für Kontrollsysteme ungeeignete CCIs.....	123
Tabelle H-3: CCIs, die aus der Grundvorgabe für Kontrollsysteme mit GERINGEN Auswirkungen entfernt wurden	127
Tabelle H-4: Planer-CCIs für Kontrollsysteme mit GERINGEN und MITTLEREN Auswirkungen	129
Tabelle H-5: Zusätzliche Planer-CCIs für Kontrollsysteme mit MITTLEREN Auswirkungen	141
Tabelle H-6 Platform Enclave-CCIs für Kontrollsysteme mit GERINGEN und MITTLEREN Auswirkungen.....	153

Tabelle H-7 Zusätzliche Plattform Enclave CCIs für Kontrollsysteme mit MITTLERER Auswirkung	165
--	-----

KAPITEL 1: EINLEITUNG

1-1 HINTERGRUND

Ein Kontrollsystem besteht in der Regel aus vernetzten digitalen Controllern und einer Benutzeroberfläche zur Überwachung und üblicherweise auch Steuerung von Geräten. Es gibt viele Arten von Kontrollsystemen, von der Gebäudeleittechnik über die Produktionsüberwachung bis hin zu Waffensteuerungssystemen, jeweils mit unterschiedlichen Bezeichnungen und unterschiedlicher Terminologie. Liegenschaftsabhängige Kontrollsysteme sind eine Untergruppe der Kontrollsysteme, die dazu dienen, Geräte und Anlagen für Liegenschaften des US-Verteidigungsministeriums (z.B. Gebäudeleittechnik, Versorgungstechnik, elektronische Sicherheitssysteme sowie Brand- und Personenschutzanlagen) zu überwachen und zu kontrollieren.

Das Risk Management Framework (RMF) ist das Verfahren des US-Verteidigungsministeriums für die Anwendung von Cyber-Sicherheit in der Informationstechnik (IT), einschließlich Kontrollsystemen. Das RMF unterteilt Anlagen nach den möglichen Auswirkungen auf den Betrieb der Organisation in die Auswirkungsgrade HOCH, MITTEL und GERING. Das RMF wird in KAPITEL 2 und ANHANG C näher beschrieben.

1-2 ZIEL UND UMFANG

Diese UFC beschreibt Anforderungen für die Einbeziehung der Cyber-Sicherheit in alle Planungen für liegenschaftsabhängige Kontrollsysteme. Sie beschreibt einen auf dem Risk Management Framework basierenden Prozess, der für alle Kontrollsysteme und Auswirkungsgrade geeignet ist, und gibt Leitlinien für die Auswirkungsgrade GERING, MITTEL oder HOCH vor.

1-3 GELTUNGSBEREICH

Diese UFC gilt unabhängig von der Finanzierungsquelle für alle an Liegenschaften des US-Verteidigungsministeriums anfallenden Planungen und Entwürfe sowie den Bau, die Renovierung und Sanierung von neuen oder bestehenden Gebäuden und Einrichtungen. Anlagen mit MITTLERER oder HOHER Auswirkung erfordern im Allgemeinen größere Sachkenntnis und Detailgenauigkeit als eine UFC bieten kann. Die Planung von Anlagen mit MITTLERER oder HOHER Auswirkung erfordert üblicherweise zusätzliche, auf den Einzelfall zugeschnittene Anforderungen, um ein angemessenes Niveau an Cyber-Sicherheit zu erreichen. Die Planung einer solchen Anlage sollte mit den in Abschnitt 1-6 genannten Stellen abgestimmt werden.

Bei der Definition der spezifischen Anforderungen für Anlagen mit GERINGER oder MITTLERER Auswirkung geht diese UFC davon aus, dass das Kontrollsystem in einer Liegenschaft des US-Verteidigungsministeriums eingerichtet wird. Bei Anlagen, die nicht in einer Liegenschaft des US-Verteidigungsministeriums eingerichtet werden, sind Anpassungen der in dieser UFC genannten Anforderungen nötig.

1-4 ALLGEMEINE BAUANFORDERUNGEN

Die Bauvorschriften des US-Verteidigungsministeriums nach UFC 1-200-01 (General Building Requirements) sind zu befolgen. Die UFC 1-200-01 regelt die Anwendbarkeit der Musterbauordnungen und US-spezifischen Kriterien für typische Planungsgewerke und Gebäudetechnik sowie für die Zugänglichkeit, den Antiterror-Schutz, die Sicherheit, die hohe Leistung und Nachhaltigkeit sowie die Sicherheit. Diese UFC ist zusätzlich zur UFC 1-200-01 und den hier beschriebenen UFCs und Kriterien der US-Regierung anzuwenden.

1-5 Organisation

KAPITEL 2 gibt einen Überblick über das RMF in Bezug auf Kontrollsysteme, die Architektur von Kontrollsystemen und den Umgang von Kontrollsystemen mit dem Thema Cyber-Sicherheit. KAPITEL 3 beschreibt einen Ansatz, wie Cyber-Sicherheit in fünf Schritten in die Planung von Kontrollsystemen einbezogen werden kann. KAPITEL 4 legt die planerischen Mindestanforderungen fest, die zusätzlich zu den in fünf Schritten gemäß KAPITEL 3 bestimmten individuellen Anforderungen bei Kontrollsystemen umzusetzen sind. KAPITEL 5 definiert die Anforderungen an die Planvorlagen im Hinblick auf die Dokumentation von Aspekten der Cyber-Sicherheit bei der Konzeption von Kontrollsystemen.

ANHANG C gibt einen Überblick über das Risk Management Framework in Bezug auf Kontrollsysteme. D enthält zusätzliche Leitlinien für das Konzept "Platform Enclave". ANHANG E beschreibt die fünfstufige Architektur für Kontrollsysteme. ANHANG F beschäftigt sich mit Überlegungen zur Einbindung kritischer Gebäudesysteme in ein nichtkritisches UMCS. G enthält Leitlinien zu Sicherheitskontrollfamilien sowie einzelnen Sicherheitskontrollen. ANHANG H untergliedert CCIs nach Auswirkungsgrad und Verantwortlichkeiten.

1-6 ANSPRECHPARTNER FÜR CYBER-SICHERHEIT NACH TEILSTREITKRÄFTEN

Die Richtlinien für und der Umgang mit Cyber-Sicherheit sind ständigen Änderungen unterworfen und können einzigartige Anforderungen beinhalten. Unterstützung zum Thema Cyber-Sicherheit bei Kontrollsystemen ist bei den Teilstreitkräften an folgenden Stellen erhältlich:

- Army: ICS Cybersecurity Center of Expertise, Huntsville Engineering and Support Center
- Navy: Naval Facilities Engineering Command, Command Information Office (CIO)
- Air Force: Civil Engineer Maintenance, Inspection, and Repair Team (CEMIRT) ICS Branch, Tyndall AFB
- Marine Corps: Anfragen zum Ansprechpartner beim Marine Corps sind an den Ansprechpartner bei der Navy zu richten.

Hinweis: Alle Anfragen nach Unterstützung sind durch den COR bzw. bei von der Regierung geplanten Projekten durch den Projektverantwortlichen einzureichen.

1-7 QUELLENANGABEN

ANHANG A enthält eine Liste von Quellen, die in diesem Dokument verwendet werden. Die Daten der Veröffentlichung oder Änderung der Vorschriften bzw. Normen sind in diesem Dokument nicht immer enthalten. Wenn kein Veröffentlichungs- oder Änderungsdatum angegeben ist, wird im Allgemeinen die zuletzt veröffentlichte Ausgabe verwendet.

1-8 GLOSSAR

ANHANG B enthält Akronyme, Abkürzungen und Begriffe.

KAPITEL 2: ÜBERBLICK - CYBER-SICHERHEIT BEI KONTROLLSYSTEMEN

2-1 ÜBERBLICK ÜBER DAS RISK MANAGEMENT FRAMEWORK

Im Folgenden werden die wichtigsten Aspekte des Risk Management Framework (RMF) im Hinblick auf die Planung von Kontrollsystemen zusammengefasst. ANHANG C enthält einen ausführlicheren Überblick über das RMF im Zusammenhang mit dieser UFC. Für Leser, die mit dem RMF nicht vertraut sind, ist es auf jeden Fall ratsam, zuerst ANHANG C zu lesen, bevor sie Anforderungen an die Cyber-Sicherheit in die Planung von Kontrollsystemen einbinden.

2-1.1 Sicherheitskontrollen

Das RMF setzt auf die Implementierung von Sicherheitskontrollen, wobei eine Kontrolle eine bestimmte Aktion zur Absicherung eines Systems ist. Es ist zu beachten, dass das Wort Kontrolle hier nicht als Steuerung zu verstehen ist wie in der Steuerungs- und Regeltechnik, wo die Kontrolltheorie angewendet wird, um Anlagen mit gewünschten Verhaltensweisen zu konstruieren. Zur begrifflichen Abgrenzung wird in dieser UFC der Begriff "Sicherheitskontrolle" im Sinne von Cyber-Sicherheitskontrollen verwendet.

2-1.2 Ziel des RMF

Ziel des RMF ist es, Schwachstellen so weit zu reduzieren und auszugleichen, bis das Risiko für den Systemeigentümer (SO) und den Autorisierungsbefugten (AO) akzeptabel ist. Im RMF ist Risikoreduzierung nicht gleichbedeutend mit "Alles oder Nichts" - die Sicherheitslösung muss das Risiko senken und dabei gleichzeitig die begrenzten Mittel und die Betriebsanforderungen berücksichtigen. Bei der Anwendung von RMF auf Kontrollsysteme muss die Bestimmung des Cyber-Sicherheitsrisikos auch alle zusätzlichen Risiken für die Systemfunktionalität aufgrund des Einsatzes von Sicherheitskontrollen berücksichtigen.

Ob ein Risikopotential akzeptabel ist, wird durch den von der Regierung beauftragten AO entschieden. Der Planer trägt zur Risikoanalyse bei, indem er darüber aufklärt, ob und welche Auswirkungen bei der Anwendung von Sicherheitskontrollen auf das Kontrollsystem zu erwarten sind.

2-1.3 Plattform-Informationstechnik

Die Anweisungen 8500.01 und 8510.01 des US-Verteidigungsministeriums definieren das Risk Management Framework (RMF) für das US-Verteidigungsministerium und führen unter der Bezeichnung Plattform-Informationstechnik (PIT) eine Kategorie für "Sondersysteme" ein, die keine Informationstechnik oder Informationssysteme im herkömmlichen Sinne sind. Diese PIT-Systeme, zu denen auch Kontrollsysteme zählen, verwenden Kombinationen aus maßgeschneiderten Sicherheitskontrollen, für die der AO sich mit dem System auskennen muss.

Für die Auswahl der Sicherheitskontrollen, die beim jeweiligen System umzusetzen sind, ist der AO verantwortlich. Der Planer trägt zur Auswahl der Sicherheitskontrollen bei, indem er über die Umsetzbarkeit und möglichen Auswirkungen des Einsatzes einer Sicherheitskontrolle aufklärt.

2-1.4 Vererbte Sicherheitskontrollen

Eine vererbte Sicherheitskontrolle ist eine Sicherheitskontrolle, die ein System deshalb besteht, weil sie an anderer Stelle bereits so umgesetzt wurde, dass sie für das gesamte System gilt. In der Regel kann ein Kontrollsystem Sicherheitskontrollen auf drei verschiedene Arten erben: weil es innerhalb einer physischen Sicherheitsgrenze besteht, weil es durch bestehende Richtlinien und Verfahrensweisen abgedeckt wird oder weil es an ein anderes System angebunden ist, das die Sicherheitskontrollen erfüllt.

Da der SO sich im Vererbungsfall häufig mit Anderen abstimmen muss, ist es überaus wichtig, genau zu dokumentieren welche Sicherheitskontrollen an das Kontrollsystem vererbt werden sollen. Bei der Planung des Systems muss der Planer alle zu vererbenden Sicherheitskontrollen aufzuführen und zu dokumentieren.

2-1.4.1 Beispiel für vererbte physische Sicherheit

Liegenschaften des US-Verteidigungsministeriums setzen physische Sicherheitsmaßnahmen ein, um das Risiko auf ein akzeptables Maß zu senken. Bei einem Kontrollsystem in einer Liegenschaft des US-Verteidigungsministeriums gilt eine Sicherheitskontrolle, die verlangt, dass die Komponenten eines Kontrollsystems nicht ungehindert öffentlich zugänglich sind, als erfüllt, wenn sich das Kontrollsystem innerhalb dieser physischen Grenze befindet. Militärische Einrichtungen sind zwar gelegentlich für die Öffentlichkeit zugänglich, beispielsweise bei Abschlussfeiern, aber der Zugang ist nicht unbeschränkt und dieser Zugangslevel wurde von der Liegenschaftssicherheit akzeptiert. Da die Kontrollsysteme von Haus aus mit den zu kontrollierenden physischen Systemen verbunden und gemeinsam mit diesen verortet sind, kann ein Kontrollsystem in den meisten Fällen physische Sicherheit von der Liegenschaft oder gesondert abgesicherten Einrichtungen erben.

2-1.4.2 Beispiel für vererbte Richtlinien und Verfahrensweisen

Beim US-Verteidigungsministerium gibt es Richtlinien, die viele Aspekte der Cyber-Sicherheit abdecken. Ein Kontrollsystem kann daher eine Sicherheitskontrolle erben, beispielsweise "Die Organisation legt fest, wie häufig die aktuellen Richtlinien zur Sicherheitsplanung überprüft und aktualisiert werden."

2-1.4.3 Beispiel für Vererbung bei Anschluss an ein anderes System

Wenn ein Kontrollsystem mit einem anderen System wie z.B. einem liegenschaftsweiten Netzwerk verbunden ist, gibt es möglicherweise keine automatische Vererbung, sondern diese erfordert eine Vereinbarung zwischen den SOs der einzelnen Systeme. Eine solche Vereinbarung würde das akzeptable Verhalten des Kontrollsystems abdecken und die vom anderen System vererbten Sicherheitskontrollen ausdrücklich definieren.

2-1.5 Anwendbarkeit von RMF-Sicherheitskontrollen auf die Planung

Sicherheitskontrollen decken ein breites Spektrum von Anforderungen ab. Viele davon müssen außerhalb des Planungsprozesses für das Kontrollsystem angegangen werden. So wird beispielsweise eine Sicherheitskontrolle¹¹, die besagt: "Die Organisation schützt das Kontrollsystem gegen unberechtigte Änderungen durch Mitglieder der Organisation" in der Regel nicht vom Planer umgesetzt, sondern durch von der Organisation, die das Kontrollsystem besitzt und betreibt, eingeführte Richtlinien und Verfahrensweisen.

¹ Hier handelt es sich nicht um eine tatsächliche Sicherheitskontrolle, sondern ein anschauliches Beispiel mit einer fiktiven Kontrolle.

2-1.5.1 Anwendbarkeit von RMF-Sicherheitskontrollen auf die Planung von kritischen Systemen

Bei kritischeren Systemen (mit größeren Auswirkungen) kann die Entscheidung, ob bei der Planung eine Sicherheitskontrolle anzuwenden ist, besonders komplex werden. Während es bei Systemen mit GERINGER Auswirkung vielleicht ausreicht, davon auszugehen, dass eine bestimmte Sicherheitskontrolle von einer anderen Entität übernommen wird, muss der Planer eines Systems mit HOHER Auswirkung eine Sicherheitskontrolle möglicherweise explizit berücksichtigen, um die ordnungsgemäße Umsetzung zu gewährleisten, sie mit höherem Standard anzuwenden oder den Verantwortlichen Hilfsmittel zur Umsetzung der Sicherheitskontrolle an die Hand zu geben.

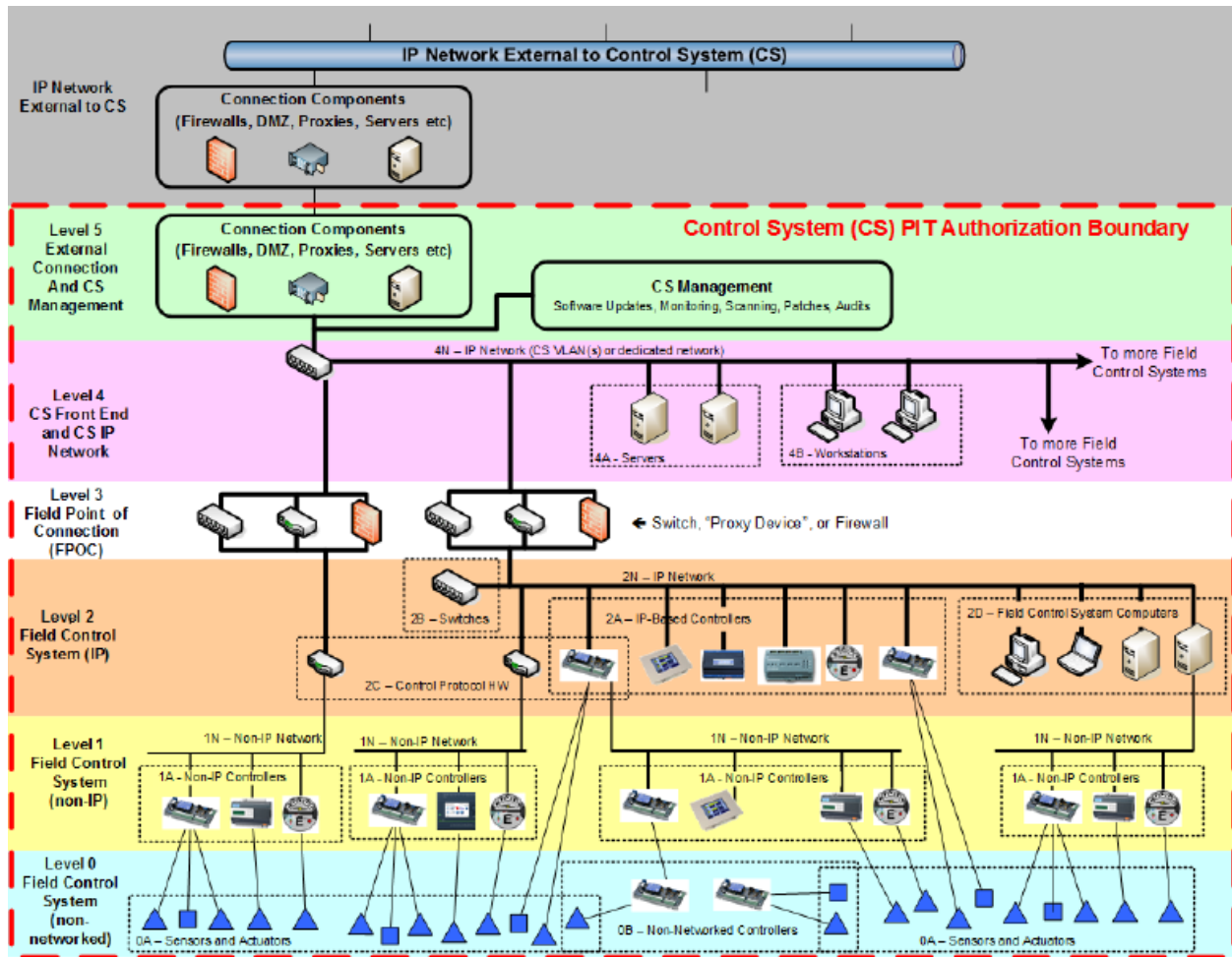
So kann bei einer Sicherheitskontrolle, die besagt: "Die Organisation schützt das Kontrollsystem gegen unberechtigte Änderungen durch Mitglieder der Organisation" für ein System mit GERINGEN Auswirkungen die Umsetzung mittels Richtlinien und Verfahrensweisen ausreichend sein, während der Planer bei einem System mit höheren Auswirkungen explizit Barrieren gegen ungenehmigte Änderungen vorsehen oder die Organisation im Hinblick auf die Wichtigkeit der ordnungsgemäßen Absicherung des Kontrollsystems gegen Änderungen beraten muss. In diesem Fall ist es jedoch unabdingbar, die möglichen Auswirkungen dieser Einschränkungen auf die Durchführung notwendiger, genehmigter Änderungen zu berücksichtigen. Daher sollten Planer bei Systemen mit HOHEN Auswirkungen auf den Betrieb höchstwahrscheinlich die Unterstützung eines auf Cyber-Sicherheit spezialisierten Ingenieurs in Anspruch nehmen. Systeme mit MITTLEREN Auswirkungen können im Einzelfall ebenfalls die Mitwirkung eines Spezialisten erfordern.

2-2 5-STUFIGER AUFBAU DES KONTROLLSYSTEMS

Kontrollsysteme werden Standard-IT-Systemen zwar immer ähnlicher, aber es bestehen nach wie vor große Unterschiede, die nicht außer Acht gelassen werden dürfen. Der in Abbildung 2-1 dargestellte 5-stufige Aufbau des Kontrollsystems bildet ein Grundgerüst für die Beschreibung eines jeden Kontrollsystems. Diese Architektur ermöglicht Unterscheidungen zwischen den Teilen des Kontrollsystems, die Standard-Informationstechnik ähneln, und den Teilen, die nicht wie Standard-IT aussehen. Dies ist wichtig, da viele Sicherheitskontrollen in dem Bereich des Kontrollsystems, das einem Standard-IT-System ähneln, ganz normal angewendet werden können, wohingegen sie in dem Bereich, der nicht wie ein Standard-IT-System aussieht, nicht ohne Änderungen (teilweise überhaupt nicht) angewendet werden können.

Eine detailliertere Beschreibung des 5-stufigen Aufbaus des Kontrollsystems ist in ANHANG E zu finden.

Abbildung 2-1: 5-stufiger Aufbau des Kontrollsystems



2-2.1 "Standard-IT"-Anteile des Kontrollsystems

Die Bereiche des Kontrollsystems, die einem standardmäßigen oder herkömmlichen IT-System am meisten ähneln, werden "Standard-IT"-Anteile genannt:

- IP-Netzwerk-Anteil von Level 4 (Level 4N)
- IP-Netzwerk-Anteil von Level 2 (Level 2N und 2B)
- Field Point of Connection (FPOC) bei Level 3
- Computer-Hardware sowohl für Server als auch für Arbeitsplatzrechner (Level 2D, 4A, 4B)
- Computer-Betriebssysteme und sonstige Standardpakete (z.B. Virenschutz) sowohl für Server als auch für Arbeitsplatzrechner (Desktops und Laptops) (Level 2D, 4A, 4B)
- Externe Verbindungen und Kontrollsystem-Management auf Level 5

Die Cyber-Sicherheit für die "Standard-IT"-Bereiche des Kontrollsystems wird größtenteils durch Standard-Vorgehensweisen für Cyber-Sicherheit abgedeckt und gehört im Allgemeinen nicht zum Leistungsumfang der Kontrollsystemplanung. Sie wird in dieser UFC nicht behandelt.

Der Planer muss das IP-Netzwerk auf Level 2N behandeln, die in der Regel vom Auftragnehmer für das Kontrollsystem beschafft und installiert wird, sowie die im Frontend eingesetzte spezifische Software für das Kontrollsystem, die von Standard-IT-Ansätzen in der Regel nicht ausreichend abgedeckt wird.

2-2.2 "Nicht-Standard-IT"-Anteile des Kontrollsystems

Die Herausforderung bei der Cyber-Sicherheit für ein Kontrollsystem besteht in den Anteilen des Kontrollsystems, die im Allgemeinen nicht wie ein Standard-IT-System aussehen: Level 0, Level 1, Level 2A, Level 2C sowie die Kontrollsystem-Anwendungen auf Level 2D, Level 4A und Level 4B. Zur Unterscheidung von den "Standard-IT"-Anteilen werden diese Teile des Kontrollsystems als "Nicht-Standard-IT"-Anteile bezeichnet. Herkömmliche Tools und Anforderungen für Cyber-Sicherheit wie z.B. Warnungen zum Umgang mit Schwachstellen, Merkblätter, Richtlinien für die sichere technische Umsetzung (Secure Technical Implementation Guides, STIGs) und Richtlinien des US-Verteidigungsministeriums sind auf diese Komponenten selten anwendbar, insbesondere bei Geräten auf Level 0, 1 oder 2. So gilt beispielsweise eine Sicherheitskontrolle², die das Sperren des Bildschirms beim Verlassen des Computers fordert, nicht für Geräte, die nicht über einen Bildschirm verfügen oder ein Benutzer-Login unterstützen. Verschiedene Levels der Systemarchitektur haben unterschiedliche Probleme bei der Anwendung von Standardtools und Anforderungen für Cyber-Sicherheit.

Die Cyber-Sicherheit für diese Bereiche des Kontrollsystems obliegt dem Planer des Kontrollsystems.

2-2.3 Platform Enclave

Wesentliche Anteile des Kontrollsystems ähneln einem Standard-IT-System, das für verschiedene Kontrollsysteme unabhängig von den Details des Kontrollsystems selbst standardmäßig umgesetzt werden kann. Hieraus entstand das Konzept der Platform Enclave, das die Standard-IT-Anteile des Kontrollsystems sowie die entsprechenden Standard-Richtlinien und -Verfahrensweisen in ein System eingruppiert, das getrennt vom restlichen Kontrollsystem behandelt werden kann. In einigen Fällen wird diese Platform Enclave separat autorisiert, und das gesamte Kontrollsystem verfügt über zwei Autorisierungen - eine für die Platform Enclave und eine für die operative Architektur, welche hauptsächlich die "Nicht-Standard-IT"-Komponenten des Systems abdeckt. In anderen Fällen wird für das gesamte System nur eine Autorisierung verwendet. Auch in Fällen, in denen nur eine Autorisierung verwendet wird, ist es jedoch hilfreich, den Anteil an Standard-IT-Elementen des Kontrollsystems zu identifizieren und zu kategorisieren. Weitere Informationen zum Konzept der Platform Enclave sind in [\[0\]](#) zu finden.

2-3 ÜBERBLICK ÜBER DIE BESCHAFFUNG VON KONTROLLSYSTEMEN

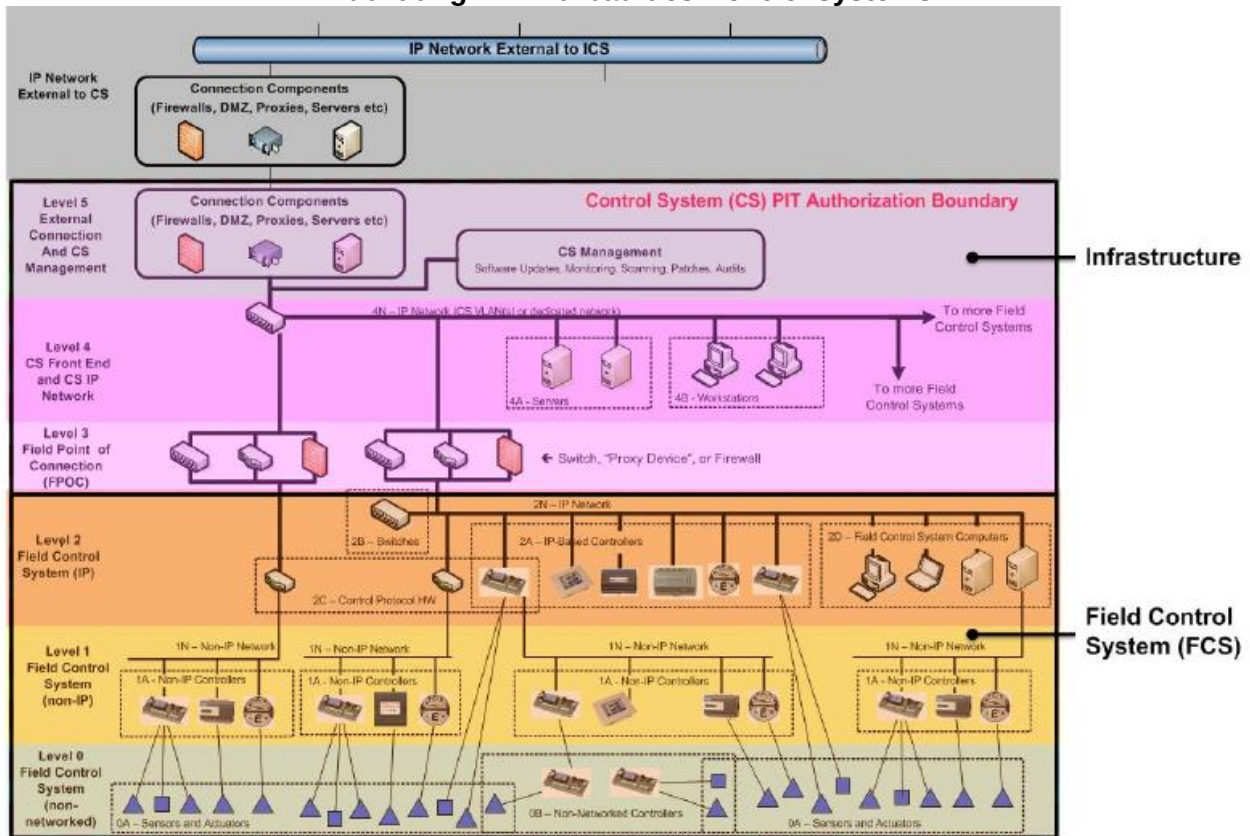
Das US-Verteidigungsministerium beschafft die meisten liegenschaftsweiten Kontrollsysteme nicht als 5-stufiges System, wie in Abbildung 2-1 dargestellt. Üblicherweise werden einige Field Control Systeme (FCS, Architekturlevel 0, 1 und 2 - vgl. Abbildung 2-2) mit einem Frontend beschafft, und mit der Zeit werden weitere FCS beschafft. Diese weiteren FCS werden in das bestehende Frontend integriert und zur Betriebsautorisierung für das bestehende System hinzugefügt, um das liegenschaftsweite System zu erweitern. Bei der Planung eines FCS, das zu einem bestehenden System hinzugefügt wird, können Anforderungen an die Cyber-Sicherheit speziell für die Autorisierung im bestehenden System vorliegen, die in die FCS-Planung eingebunden werden müssen.

² Hinweis: Sicherheitskontrolle AC-11 beschäftigt sich mit den Anforderungen für das Sperren von Sitzungen

Diese UFC kann sich nicht mit standortspezifischen Anforderungen befassen; bei der Planung von Systemen, die zu einer bestehenden Systemautorisierung hinzugefügt werden, ist eine Abstimmung mit dem Projektstandort erforderlich, um die entsprechenden Anforderungen aus dem bestehenden System zu erhalten.

Einige Kontrollsysteme werden zum eigenständigen Betrieb beschafft, ohne Einbindung in ein größeres System und ohne nennenswerte Erweiterungen. Abhängig von den Umständen und der Systemarchitektur sind diese Systeme entweder als Komplettsysteme mit allen 4 oder 5 Levels oder als FCS (Level 0-2) mit eigener Benutzerschnittstelle auf Level 1 oder 2 zu behandeln. Weitere Informationen zu Level 2D Computern sind in Tabelle E-3 in ANHANG E zu finden.

Abbildung 2-2: Aufbau des Kontrollsystems



KAPITEL 3: ANWENDUNG VON CYBER-SICHERHEIT IN DER PLANUNG

3-1 ÜBERSICHT

Die Planung der Cyber-Sicherheit für liegenschaftsabhängige Kontrollsysteme erfolgt in fünf Schritten. In einigen Fällen kann ein bestimmter Schritt durch andere Personen als den Planer ausgeführt werden, wobei dennoch Angaben des Planers erforderlich sind. Die Dokumentation der Planungsentscheidungen in Bezug auf die Cyber-Sicherheit und die Beteiligung Dritter wird in KAPITEL 5 beschrieben.

Zusätzlich zu den besonderen Anforderungen für Control Correlation Identifier (CCIs) sind alle Kontrollsysteme gemäß den in KAPITEL 4 beschriebenen Mindestanforderungen für die Planung von Cyber-Sicherheit sowie sonstigen standardmäßigen Anforderungen an Cyber-Sicherheit für Systeme der gleichen Art wie das betreffende Kontrollsystem zu planen.

3-1.1 Fünf Schritte für die Planung der Cyber-Sicherheit

Die fünf Schritte für die Planung der Cyber-Sicherheit sind:

Schritt 1: Ausgehend vom Einsatzbereich und den Details des Kontrollsystems legen der Systemeigentümer (SO) und der Autorisierungsbefugte (AO) die Auswirkungsgrade (GERING, MITTEL oder HOCH) auf die Vertraulichkeit, Integrität und Verfügbarkeit (confidentiality, integrity, availability oder C-I-A) fest.

Schritt 2: Mit Hilfe der Auswirkungsgrade wird die passende Liste von Kontrollen aus NIST SP 800-82 ausgewählt.

Schritt 3: Unter Verwendung der Master-CCI-Liste des US-Verteidigungsministeriums werden ausgehend von den in Schritt 2 gewählten Kontrollen die entsprechenden CCIs ausgewählt.

Schritt 4: Es erfolgt eine Eingruppierung der CCIs sowie die Festlegung der CCIs, für die ein Beitrag des Planers erforderlich ist oder die in den Verantwortungsbereich des Planers fallen.

Schritt 5: Die in den Projektspezifikationen enthaltenen Anforderungen an die Cyber-Sicherheit sind mit einzubeziehen; sofern erforderlich, wird Input an andere Stellen gegeben.

ANHANG H enthält Tabellen zu den Schritten 2-4 für Systeme mit GERINGEM und MITTEL-REM Auswirkungsgrad unter der Annahme, dass eine Plattform Enclave besteht. Diese Tabellen sind zusammen mit zusätzlichen Informationen als filterbare Tabelle auch im Excel-Format beim RMF Knowledge Service (<https://rmfks.osd.mil>) erhältlich. Diese Website ist auf CAC ausgelegt; Planer ohne CAC müssen die entsprechende Stelle um Unterstützung bitten, wenn keine Tabellen und Informationen bereitgestellt wurden. O bietet zusätzliche Anleitungen für die Umsetzung von bestimmten Kontrollen.

3-1.2 Definition von "Organisation"

Sicherheitskontrollen beziehen sich bei der Identifizierung von Zuständigkeiten und Risiken häufig auf die "Organisation". Sofern nichts Anderes angegeben ist, gilt für die Implementierung des RMF in Kontrollsystemen:

- Bei der Festlegung des Auswirkungsgrads eines Systems ist unter "Organisation" die jeweilige Teilstreitkraft (Army, Navy, Air Force) zu verstehen.
- Bei der Festlegung der Implementierungsanforderungen für spezifische Kontrollen ist unter "Organisation" die Liegenschaft (Garnison, Militärposten oder -basis) bzw. die Region (bei regionalen Systemen) zu verstehen. Hinweis: Dies steht nicht im Widerspruch zur oben stehenden Aussage bezüglich der Organisation bei der Festlegung des Auswirkungsgrads, sondern gibt an, welche Teilstreitkraft für die Implementierung der Kontrolle zuständig ist.

3-2 SCHRITT 1: AUSWIRKUNGSGRAD FÜR DAS KONTROLLSYSTEM FESTLEGEN

Der SO legt mit Zustimmung des AO die Auswirkungsgrade für das Kontrollsystem fest. Der SO kann bei der Definition der Funktionen des Kontrollsystems, der im Kontrollsystem enthaltenen Informationen und der Auswirkung des Ausfalls des Kontrollsystems den Planer des Kontrollsystems um Unterstützung bitten. Für das US-Verteidigungsministerium werden die Auswirkungsgrade auf der Grundlage der Aufgaben der jeweiligen Teilstreitkraft festgelegt, und in vielen Fällen kann die Einstufung der Bedeutung für militärische Aufgaben (unterstützend/kritisch/wichtig für die militärischen Aufgaben) als Ausgangspunkt für die Festlegung des Auswirkungsgrads des Kontrollsystems dienen. Es ist auch zu berücksichtigen, dass Kontrollsysteme in der Regel die Verfügbarkeit an die erste Stelle setzen, gefolgt von Integrität und schließlich Vertraulichkeit, während ein herkömmliches Informationssystem generell der Vertraulichkeit die höchste Priorität vor Integrität und Verfügbarkeit einräumt.

Wenn keine Auswirkungsgrade vorgegeben sind, fordern Sie diese von der Teilstreitkraft an. Wenn die Teilstreitkraft die Auswirkungsgrade nicht angeben kann, erbitten Sie Anhaltspunkte von der Teilstreitkraft und gehen Sie je nach Anweisung gemäß einer der beiden folgenden Methoden vor:

1. Verwenden Sie die "Ausgangswerte" der Auswirkungsgrade für das Kontrollsystem und die Einstufung der Liegenschaft (unterstützend/kritisch/wichtig für die militärischen Aufgaben) aus der Master-Liste für Kontrollsysteme, die auf der Website des RMF Knowledge Service zur Verfügung steht (<https://rmfks.osd.mil>).
2. Fahren Sie mit der Planung erst fort, wenn die Einstufung der Auswirkungsgrade gemäß C-I-A vorliegt.

3-3 SCHRITT 2: FESTLEGUNG DER SICHERHEITSKONTROLLEN

Wenn von der Teilstreitkraft die Liste der entsprechenden Steuerungen nicht vorgelegt wird, legen Sie als Ausgangsbasis eine Liste von Kontrollen fest, die auf den von der \1\Teilstreitkraft/1/ vorgegebenen Einstufungen der Auswirkungsgrade nach Vertraulichkeit (Confidentiality), Integrität (Integrity) und Verfügbarkeit (Availability) (C-I-A-Einstufung) basiert. Das US-Verteidigungsministerium verwendet NIST SP 800-82 als Schablone für die Festlegung der grundlegenden ersten Einstufung der Sicherheitskontrollen für die Kontrollsysteme. Der RMF Knowledge Service (<https://rmfks.osd.mil>) enthält Leitlinien für die Festlegung von Kontrollen aufgrund von C-I-A-Einstufungen, einschließlich einer Excel-Datei, die eine Kontrollliste auf der Grundlage der Einstufung in Auswirkungsgrade und der Leitlinien gemäß NIST SP 800-82 generiert. Diese Website ist auf CAC ausgelegt; Planer ohne CAC müssen die entsprechende Stelle um Unterstützung bitten, wenn keine Tabellen und Informationen bereitgestellt wurden.

3-3.1 Individuell anzupassende empfohlene Sicherheitskontrollen

Die grundlegenden Standard-Sicherheitskontrollen wurden für Standard-Informationssysteme entwickelt und enthalten Sicherheitskontrollen, die für Kontrollsysteme (oder andere Plattform-Informationstechnik) völlig ungeeignet sind oder deren Einsatz sich aufgrund von technischen oder finanziellen Einschränkungen verbietet. Der RMF-Prozess erlaubt eine Anpassung dieser grundlegenden Werte für das Projekt durch Entfernen oder Hinzufügen von speziellen Kontrollen. Prüfen Sie die Liste der Kontrollen und geben Sie im Rahmen der in KAPITEL 5 geforderten Dokumentation zur Cyber-Sicherheit Empfehlungen ab, welche Kontrollen aus dem Satz von Sicherheitskontrollen im Einzelfall entfernt (bzw. hinzugefügt) werden sollen.

Hinweis: Diese individuelle Anpassung kann im Planungsprozess entweder in Schritt 2 auf der Sicherheitskontrollstufe oder in Schritt 3 auf dem CCI-Level erfolgen. Für ein System mit GERINGEN Auswirkungen sollten, die in Tabelle H-2 und Tabelle H-3 empfohlenen CCIs individuell angepasst/entfernt werden.

3-4 SCHRITT 3: IDENTIFIKATION VON CCIS

Erstellen Sie unter Verwendung der Liste aus Schritt 2 eine Liste der entsprechenden Control Correlation Identifier (CCIs). Diese Liste von CCIs dient als Ausgangspunkt für die Identifizierung der Anforderungen an die Cyber-Sicherheit, die bei der Planung des Kontrollsystems zu berücksichtigen sind. Die vollständige Liste der CCIs ist auf der Website des RMF Knowledge Service <https://rmfks.osd.mil/rmf/General/SecurityControls/Pages/ControlsExplorer.aspx> unter dem Link "Export All Assessment Procedures to Spreadsheet" verfügbar.

Wählen Sie unter dieser URL aus dem Pulldown-Menü "Choose Control Family" die Option "All Control Families". Wenn die Kontrollen auf der Seite angezeigt werden, klicken Sie auf "Export Implementation Guidance and Assessment Procedures", um die CCIs in Excel herunterzuladen.

Hinweis: Diese Website ist auf CAC ausgelegt; Planer ohne CAC müssen die CCI-Liste von der Teilstreitkraft anfordern, wenn sie nicht bereitgestellt wurde.

3-5 SCHRITT 4: ZUORDNUNG VON CCIS NACH ZUSTÄNDIGKEIT

Ordnen Sie jeden in Schritt 3 identifizierten CCI einer oder mehreren der folgenden Kategorien zu:

- **Definition durch DoD:** Entweder hat das US-Verteidigungsministerium (DoD) einen Orientierungswert für die Werte der „gewählten Organisation“ bestimmt, oder die Anleitung des US-Verteidigungsministeriums zur Umsetzung gibt an, dass der CCI bereits durch bestehende Bestimmungen oder Vorschriften eingehalten wird. Diese Werte werden in der vom RMF Knowledge Service heruntergeladenen CCI-Liste definiert. **Hinweis: Vorgesehene Definitionen oder Richtlinien können für ein Kontrollsystem möglicherweise nicht relevant sein - die Definitionen der Organisation wurden aus dem Blickwinkel eines traditionellen Informationssystems festgelegt, nicht für ein Kontrollsystem.**
- **Planer:** Der Planer spielt bei diesem CCI eine Rolle. Entweder muss der Planer Planungsvorgaben erstellen, um eine Anforderung an das Kontrollsystem selbst abzudecken, oder der Planer muss Anderen Vorgaben bezüglich der Umsetzung oder der mangelnden Umsetzbarkeit des CCI machen (normalerweise weil der CCI für ein IT-System geschrieben wurde, nicht für ein Kontrollsystem).

- **Nicht Planer:** Der CCI liegt außerhalb der Zuständigkeit des Planers und liegt im Verantwortungsbereich eines Anderen - normalerweise des Systemeigentümers (SO). Dies verringert nicht die Wichtigkeit dieser CCIs, aber da diese CCIs nicht im Zuständigkeitsbereich des Planers liegen, befinden sie sich außerhalb des Geltungsbereichs dieser UFC.
- **Platform Enclave:** Der CCI enthält eine Anforderung, die in der Platform Enclave umgesetzt und vom Kontrollsystem übernommen werden soll, oder die größtenteils bei der Platform Enclave umgesetzt wird, jedoch auch innerhalb des Field Control Systems erforderlich ist (in diesem Fall fällt der CCI ebenso in die Kategorie "Planer"). Beispielsweise wenn Passwörter für die Platform Enclave implementiert werden, aber auch bei der Benutzerschnittstelle des Kontrollsystems selbst, bei lokalen Anzeigegeräten und einigen Controllern (mit Passwortunterstützung) erforderlich sind. Während die Umsetzung der Platform Enclave nicht in der Verantwortung des Planers liegt (ein Schlüsselaspekt der Platform Enclave ist die Tatsache, dass sie ein Standardverfahren ist, das über mehrere Kontrollsysteme hinweg umgesetzt werden kann), ist es wichtig, zu dokumentieren, bei welchen CCIs das Kontrollsystem erwartet, dass diese von der Platform Enclave vererbt werden.

Die Kategorie Platform Enclave ist in vielerlei Hinsicht ein Sonderfall der Kategorie "Nicht Planer", da sie anzeigt, dass ein CCI anderweitig abgedeckt wird.

- **Nicht zweckmäßig:** Der CCI ist für die volle Umsetzung in einem Kontrollsystem nicht zweckmäßig, kann jedoch in beschränktem Umfang für mindestens einen Teil des Kontrollsystems angewendet werden. Meist sind dies CCIs, die auf Level 4 der Struktur umgesetzt werden; es wäre jedoch unerschwinglich aufwändig, diese auf Level 0, 1 oder 2 umzusetzen.

Viele CCIs werden mehreren Kategorien zugeordnet. Eine Sicherheitskontrolle bezüglich Passwörtern würde beispielsweise sowohl der Kategorie "Platform Enclave" als auch der Kategorie "Planer" zugeordnet, da sie sowohl bei den Computern auf Level 4 als auch auf Level 1 und Level 2 zu behandeln ist. Wenn das US-Verteidigungsministerium für die Verwendung bei dieser Kontrolle eine Mindest-Passwortlänge festgelegt hat, die nicht von allen Geräten erfüllt werden kann, würde dies auch als "Nicht zweckmäßig" eingestuft, und der Planer muss dokumentieren, wie die Sicherheitskontrolle für Geräte, die den vom US-Verteidigungsministerium festgelegten Wert nicht erreichen, umgesetzt wurde.

3-6 SCHRITT 5: EINBINDUNG VON ANFORDERUNGEN AN DIE CYBER-SICHERHEIT

Zusätzlich zu den besonderen Anforderungen für CCIs sind alle Kontrollsysteme gemäß den in KAPITEL 4 beschriebenen Mindestanforderungen für die Planung von Cyber-Sicherheit sowie sonstigen standardmäßigen Anforderungen an Cyber-Sicherheit für Systeme der gleichen Art wie das betreffende Kontrollsystem zu planen.

Behandeln Sie jeden als "Planer" gekennzeichneten CCI auf eine der drei folgenden Arten:

- Nehmen Sie eine Planungsanforderung in die Spezifikationen für das Kontrollsystem auf.

- Wählen oder kennzeichnen Sie erforderliche Änderungen gegenüber den Standardanforderungen für CCI, die sich auf die Implementierung auswirken, z.B. den Wert eines bestimmten Parameters. Hinweis: Die Genehmigung oder Ablehnung eines dieser Werte durch die \1\Teilstreitkraft (den AO oder dessen benannten Vertreter)/1/ wirkt sich auf die Planung des Kontrollsystems aus.
- Versorgen Sie Andere mit Informationen zur Planung, sodass sie einen CCI implementieren können. Dokumentieren Sie insbesondere CCIs, die von einem anderen System oder der Plattform Enclave an das System vererbt werden sollen.

3-6.1 Umgang mit vom US-Verteidigungsministerium festgelegten Werten bei CCIs

Viele CCIs haben vom US-Verteidigungsministerium festgelegte Standardwerte und sind in der Master-CCI-Liste basierend auf dem Standardwert als automatisch erfüllt oder vererbt angegeben. Diese CCIs wurden von den allgemeinen Sicherheitskontrollen in NIST SP 800-53 abgeleitet, ohne eventuelle besonderen Anforderungen für ein Kontrollsystem zu berücksichtigen, z.B. individuelle Anpassung und zusätzliche Leitlinien in NIST SP 800-82. Viele dieser CCIs können nicht mit der vom US-Verteidigungsministerium angeführten Methode auf Kontrollsysteme angewendet werden. In diesem Fall ist der CCI soweit machbar zu implementieren, und die nicht kompatiblen Punkte sind zu kennzeichnen.

3-6.2 Sonstige "Von der Organisation festgelegte Werte" bei CCIs

Bei CCIs, die sich auf "Von der Organisation festgelegte Werte" beziehen und für die weder vom US-Verteidigungsministerium ein Wert festgelegt noch ein Wert vorgegeben wurde, fordern Sie die entsprechenden Werte von der \1\Teilstreitkraft an. Wenn die Teilstreitkraft/1/ diese Werte nicht bereitstellen kann, schlagen Sie angemessene Werte vor und dokumentieren Sie den vorgeschlagenen Wert mit Begründung.

3-6.3 CCIs für die Definition von Anforderungen und die Implementierung

Häufig definiert ein CCI eine Anforderung, und ein zweites verlangt die Umsetzung dieser Anforderung. Hier ein hypothetisches Beispiel³:

- CCI #1 besagt: "Die Organisation legt fest, welche Komponenten Prüfprotokolle sammeln." Die Implementierungshilfe für diesen CCI besagt: "Dies ist automatisch erfüllt, da das US-Verteidigungsministerium die Komponenten als '**alle Komponenten**' definiert hat."
- CCI #2 besagt: "Das Informationssystem sammelt Prüfprotokolle an den festgelegten Komponenten."

Zusammen bilden diese beiden eine unmögliche Anforderung: Wenn man die Definition in #1 akzeptiert (d.h. "automatisch erfüllt"), dann kann das System #2 nicht erfüllen, weil beispielsweise Sensoren auf Level 0 keine Prüfprotokolle sammeln können. In diesem Fall sind beide CCIs der Kategorie "Planer" zuzuordnen; schlagen Sie für CCI #1 angemessene Werte vor, implementieren Sie CCI #2 mit diesem Wert und dokumentieren Sie die vorgeschlagenen Werte für CCI #1.

³ Aus Gründen der Anschaulichkeit verwendet dieses Beispiel vereinfachte, fiktive CCIs. Die AU-Familie von Sicherheitskontrollen befasst sich mit Prüfprotokollen.

Diese Seite wurde absichtlich freigelassen.

KAPITEL 4: MINDESTPLANUNGSANFORDERUNGEN AN CYBER-SICHERHEIT

4-1 AUSFALLMINIMIERUNGSPLANUNG

4-1.1 Reduzierung der Netzwerkabhängigkeit

Zur Durchführung von Kontrollstrategien ist eine Netzwerkabhängigkeit zu vermeiden. So sollte zum Beispiel ein Notstromgenerator immer basierend auf einer lokalen Verfügbarkeitsmessung anlaufen und keinen „START“-Befehl aus dem Netzwerk erfordern. Wenn sich eine Netzwerkabhängigkeit nicht vermeiden lässt, ist dieser Teil des Netzwerks so zu isolieren, dass nicht lokale Netzausfälle keine Auswirkung auf diesen Teil des Netzwerks haben. Eine lokale Schnittstelle (lokales Anzeigetableau) oder ein zugeordnetes Frontend (Level 2 Frontend), räumlich bei den Geräten angeordnet, ist in Betracht zu ziehen, sofern eine Benutzeroberfläche für die Funktion einer Kontrollstrategie absolut erforderlich ist.

Weitere Maßnahmen zum Schutz kritischer Funktionen gegen Manipulation aus dem Netz sind in manchen Fällen notwendig (z.B. ein Controller, der aufgrund seiner Ausführung die Manipulation kritischer Parameter über das Netz ermöglicht). In diesen Fällen sind Schutzwälle gegen Manipulation im Kontrollnetzwerk selbst einzuplanen. Siehe ANHANG F für einen möglichen Ansatz.

4-1.2 Reduzierung irrelevanter Funktionen

Da zusätzliche Fähigkeiten auch häufig zusätzliche Schwachstellen bedeuten, ist eines der Hauptkonzepte zur Cyber-Sicherheit die „geringste Funktionalität“, d.h. es werden keine Fähigkeiten eingerichtet, die nicht speziell erforderlich sind. Kontrollsystemanlagen sind so zu planen, dass zusätzliche Funktionen, die Schwachstellen im Kontrollsystem schaffen, minimiert werden; u.a.:

- Vor der Umsetzung einer Fernanpassung von Systemparametern, bei denen eine Änderung weder zu erwarten noch erforderlich ist, sind die Betriebsanforderungen in Betracht zu ziehen. So sollte zum Beispiel ein kritisches Klimagerät zur Versorgung eines Datenzentrums, eines kritischen Steuer- und Regelungsgebäudes oder eines USV-Raums, in dem die Temperatur ständig auf 65 Grad Fahrenheit gehalten werden muss, keinen Betriebsplan bzw. keinen Sollwert haben, der über das Netz konfiguriert werden kann.
- Für hochentwickelte oder komplexe Kontrollstrategien sind häufig weitere Sensoreneingänge und ein erhöhter Wartungsaufwand erforderlich. Diese Strategieanforderungen sind mit Vorsicht zu stellen, da eine erhöhte Komplexität auch ein erhöhtes Ausfallpotential bedeutet, wenn das System nicht ordnungsgemäß gewartet wird oder falls ein bestimmter Parameter beeinträchtigt ist.

4-2 AUSFALLMANAGEMENTPLANUNG

4-2.1 Planung eines sanften Ausfalls

4-2.1.1 Kontrollsysteme ohne Untersysteme

Bei Kontrollsystemen für einen einzelnen Prozessor oder ein Gerät sind Absprachen mit dem Ausstattungsplaner erforderlich, um weitere Anforderungen an Redundanz bzw. Ausfälle festzulegen, und das Kontrollsystem ist passend für die Basisausstattung zu planen.

In jedem Fall sind diese Systeme mit „sicherem“ Ausfall gemäß den Anforderungen für das Kontrollsystem vorzusehen. So müssen zum Beispiel gemäß den UFC-Anforderungen an Heizung, Lüftung und Kühlung, die Außenluftklappen in kalten Klimazonen bei Ausfall in den geschlossenen Zustand gehen.

4-2.1.2 Kontrollsysteme mit unabhängigen Untersystemen

Viele Kontrollsysteme werden als Einzelsystem beschrieben, obwohl sie tatsächlich aus vielen (hundert, sogar tausenden) von grundsätzlich unabhängigen Systemen zusammengestellt sind. Ein gängiges Beispiel wäre hier der liegenschaftsweite Einbau eines zentralen UMCS-Systems, in dem die Controller der Belüftungseinheiten in einem Gebäude nicht von den Belüftungseinheiten in einem anderen Gebäude abhängig sind und oft sogar unabhängig von Belüftungseinheiten im selben Gebäude funktionieren.

Bei Kontrollsystemen mit unabhängigen Untersystemen ist jedes Untersystem gemäß Paragraph 4-2.1.1 Kontrollsysteme ohne Untersysteme zu planen. Außerdem ist das Gesamtsystem so auszulegen, dass der Ausfall eines einzelnen Untersystems keine Auswirkung auf den Betrieb des restlichen Systems hat. Geteilte Informationen zwischen den Unterstationen sind zu reduzieren und die Abhängigkeit vom Netzwerk ist zu minimieren. Bei Untersystemen, die sich auf andere Untersysteme stützen, ist ein Ausfallverhalten („Ersatz“) festzulegen, sollte es zu einer Störung des anderen Untersystems kommen.

4-2.2 Verminderter Betrieb

Nachdem ein System bis zu einem sicheren Stand ausgefallen ist, muss dieses möglicherweise den Betrieb mit verminderter Leistung mit Hilfe eines automatischen oder manuellen Prozesses wieder aufnehmen, wissend, dass dabei zwar ein Risiko besteht, dieses aber überschaubar ist und von den Betriebsanforderungen überwogen wird.

Je nach den Betriebsanforderungen sollten Hilfsmittel für manuellen Betrieb gefordert werden, die sowohl Überwachungsgeräte (z.B. Thermometer, Druckmessgeräte, Zähler) als auch manuelle Stellgeräte (z.B. „Hand-Aus-Auto“-Schalter und Stellgeräte mit Handauslösefähigkeit) umfassen.

4-2.3 Redundanz

Sollte aufgrund des kritischen Einsatzbereichs Redundanz in der Planung des Kontrollsystems erforderlich sein, muss das System so gestaltet werden, dass es ohne Eingriff von außen, besonders ohne menschlichen Eingriff, funktioniert. Die Kontrollstrategien sind so zu planen, dass Reserveeinheiten automatisch anfahren, wenn laufende Einheiten abschalten, oder so, dass alle Einheiten laufen und sich eine Last teilen. Bei Lastteilung ist darauf zu achten, dass der Betreiber informiert wird, wenn eine Einheit des redundanten Satzes ausfällt, da die übrigen Einheiten automatisch, ohne Unterbrechung, die Last übernehmen. Man darf sich nicht darauf verlassen, dass ein Betreiber eine Reserveeinheit startet; das Risiko, dass der Betreiber nicht verfügbar ist oder falsch reagiert, ist zu hoch. Es sind Signale vorzusehen, die den Betreiber auf Ausfälle aufmerksam machen.

4-3 ES SIND KEINE IT-STANDARDFUNKTIONEN ZU IMPLEMENTIEREN

Als eine Art IT-Plattform stellen Kontrollsysteme Anlagen mit speziellem Zweck dar und sind daher nicht als allgemeine EDV-Mittel einzusetzen. Das heißt insbesondere:

- Kontrollsystemquellen sind nicht mit anderen Systemen zu teilen, besonders nicht mit nicht-PIT-Systemen. Einige Ausnahmen, wie z.B. getrennte virtuelle Server mit gemeinsamer Hardware oder gemeinsame Ethernetmedien mit getrenntem VLAN sind möglicherweise zulässig, jedoch ist die Überlappung zwischen Kontrollsystemen und anderen Systemen auf ein Minimum zu reduzieren.
- Es darf Kontrollsystemen nicht möglich sein, anderen Anwendungen für standardmäßige IT-Leistungen Quellen zur Verfügung zu stellen oder mit diesen zu teilen. Insbesondere sind Kontrollsystemteile nicht als Domain Name System (DNS) Server einzusetzen. (DNS-Server können möglicherweise in der Plattform Enclave auf Level 5 umgesetzt werden; dies liegt jedoch außerhalb des Verantwortungsbereichs des Kontrollsystemplaners und wird in dieser UFC nicht behandelt.)
- Kontrollsysteme dürfen nicht öffentlich zugänglich sein (d.h. Authentifizierung vor Zugriff ist erforderlich).
- Mobilcode ist zu unterbinden; ausgenommen auf Level 4. Dort ist Mobilecode möglicherweise zulässig. Hinweis: Kontrollsysteme dürfen Mobilcode-Technologien, insbesondere Java, innerhalb des Kontrollsystems nutzen, es darf aber kein Code ohne direkte Zustimmung des Benutzers heruntergeladen werden.
- Kontrollsystemcomputer sind nicht als Standardcomputer für allgemeine Anwendungen einzusetzen.
- Im Kontrollsystem ist keine VoIP-Internet-Telefonie zu implementieren.
- Innerhalb des Kontrollsystems sind keine gemeinschaftlichen EDV-Geräte, Technologien oder Protokolle zu realisieren.
- Das Kontrollsystem darf keinen Zugriff auf nicht-militärische IP-Adressbereiche haben, es sei denn dies wurde speziell von der \1\Teilstreitkraft/1/ genehmigt und ist aufgrund des Projektstandortes erforderlich. Komponenten des Kontrollsystems dürfen keinen Zugriff auf soziale Netzwerke haben. (Hinweis: Zugriff auf nicht-militärische IP-Adressbereiche ist allgemein nicht notwendig und falls doch, ist das normalerweise eine Funktion des Frontends, nicht des Field Control Systems.)
- Es darf Kontrollsystemen nicht möglich sein, E-Mails zu empfangen (Hinweis: für Level 4 ist evtl. eine Möglichkeit zum Versenden von E-Mails für Mitteilungszwecke erforderlich).

4-4 ES IST KEIN FERNZUGRIFF VORZUSEHEN

Ein Fernzugriff auf das Kontrollsystem ist nicht vorzusehen. Falls erforderlich, sollte ein Fernzugriff auf das Level 4 Netzwerk über die Plattform Enclave oder die IT-Organisation vor Ort eingerichtet werden. Anforderungen bzgl. Fernzugriff sind mit der IT-Organisation für den Projektstandort und mit den in KAPITEL 1 aufgelisteten Ansprechpartnern abzustimmen.

Diese Seite wurde absichtlich freigelassen.

KAPITEL 5: DOKUMENTATION DER CYBER-SICHERHEIT

In diesem Kapitel wird die Dokumentation zur Cyber-Sicherheit, die als Teil des Kontrollsystem-Planungspakets erforderlich ist, beschrieben. Diese Dokumentation muss zusätzlich zu den Dokumenten, die für die maßgeblichen Kontrollsystem-Planungskriterien erforderlich sind, vorgelegt werden.

5-1 ÜBERSICHT

In der Dokumentation zur Cyber-Sicherheit für die Kontrollsystemplanung sind die im Kontrollsystem angewendeten Sicherheitskontrollen und CCIs zusammen mit Annahmen bzgl. der CCI-Umsetzung und Informationen, die von anderen benötigt werden, dokumentiert.

5-2 ANFORDERUNGEN NACH PLANUNGSPHASE

Die Anforderungen an die Dokumentation der Cyber-Sicherheit sind nach den typischen Design-Build- bzw. Design-Bid-Build-Vorlagen angegeben. Sollte die Planung nach einem anderen Vorlageplan ausgeführt werden, sind diese entsprechend anzupassen.

Die Anforderungen hier beziehen sich auf den 5-stufigen Planungsprozess für Cyber-Sicherheit, wie in KAPITEL 3 beschrieben.

5-2.1 Planungsgrundlage

Es ist eine einzige Vorlage zu liefern, in der der C-I-A-Auswirkungsgrad für das Kontrollsystem angegeben ist, einschließlich einer Auflistung der in Schritt 2 erstellten Sicherheitskontrollen, zusammen mit Vorschlägen und Begründungen für weiterer Anpassungen des Sicherheitskontrollensets.

5-2.2 Planungsvorlagen

5-2.2.1 KVM-Bau-Vorlage (10-15%)

Es ist eine einzige Vorlage zu liefern, in der die CCIs, die sich aus der genehmigten, angepassten Sicherheitskontrollenliste (Schritt 3) ergeben, sowie eine erste Klassifizierung für jedes CCI (Schritt 4) angegeben sind.

5-2.2.2 HU-Bau-Vorlage (35-50 %).

In einer einzigen Vorlage ist folgendes zu dokumentieren:

- Die endgültige Klassifizierung jedes CCIs (Schritt 4).
- Die in Schritt 5 festgelegten Änderungen der standardmäßigen CCI-Anforderungen, einschließlich einer Erläuterung der Änderungen.
- Die CCIs, die in die Kontrollsystemplanung eingearbeitet wurden (Schritt 5). Dokumentänderungen im Vergleich zu den Standardanforderungen, bzw. die getroffene Auswahl, wenn mehrere Optionen zur Verfügung stehen. Ansonsten ist es nicht notwendig die Details der Anforderung zu dokumentieren, lediglich ob ein spezielles CCI eingebunden wurde.
- Informationen für Dritte nach Erfordernis (Schritt 5).

Das vorgeschlagene Format für diese Vorlage ist \1\0/1/ mit einer zusätzlichen Spalte für die Dokumentation erforderlicher Informationen.

5-2.2.3 AFU-Bau-Vorlage (90 %)

Eine Vorlage mit Aktualisierung der HU-Bau-Vorlage, einschließlich aller endgültigen Angaben, ist zu liefern.

5-2.2.4 AFU-Bau-Vorlage (100 %)

Eine Vorlage mit Aktualisierung der AFU-Bau-Vorlage (90%), einschließlich aller endgültigen Angaben, ist zu liefern.

ANHANG A: QUELLENANGABEN

COMMITTEE ON NATIONAL SECURITY SYSTEMS (CNSS) - KOMMISSION FÜR NATIONALE SICHERHEITSSYSTEME

<https://www.cnss.gov/CNSS/issuances/Instructions.cfm>

CNSSI Nr. 1253, *Sicherheitskategorien und Kontrollauswahl für nationale Sicherheitssysteme*

CNSSI Nr. 4009, *Kommission für nationale Sicherheitssysteme (CNSS) Glossar*

US-VERTEIDIGUNGSMINISTERIUM

<http://www.dtic.mil>

US-Verteidigungsministerium, Anweisung 8500.01, *Cyber-Sicherheit*, März 2014

US-Verteidigungsministerium, Anweisung 8510.01, *Risk Management Framework (RMF) für Informationstechnik (IT) des US-Verteidigungsministeriums*, März 2014

FEDERAL INFORMATION PROCESSING STANDARDS (FIPS) - NORMEN ZUR BUNDESWEITEN INFORMATIONSVERARBEITUNG

<http://csrc.nist.gov/publications/PubsFIPS.html>

FIPS PUB 200, *Mindestsicherheitsanforderungen für Bundesinformations- und Informationssysteme*

FIPS PUB 201-2, *Personal Identity Verification (PIV) für Bundesangestellte und Auftragnehmer*

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE) - BERUFSVERBAND DER ELEKTRO- UND ELEKTRONIK-INGENIEURE

<http://standards.ieee.org/findstds/standard/802.1X-2010.htm>

IEEE 802.1X, *Port-basierende Netzwerkzugriffskontrolle*

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) - NATIONALES INSTITUT FÜR NORMEN UND TECHNOLOGIE

<http://www.nist.gov/>

NIST SP 800-37, *Richtlinie zur Anwendung des Risk Management Frameworks für Bundesinformationssysteme*, Februar 2010

NIST SP 800-53 Revision 4, *Sicherheits- und Datenschutz für Bundesinformationssysteme und -organisationen*, April 2013

NIST SP 800-82 Revision 2, *Richtlinie zur Sicherheit von industriellen Kontrollsystemen (ICS)*, Mai 2015

UNIFIED FACILITIES CRITERIA (UFC)

http://www.wbdg.org/ccb/browse_cat.php?o=29&c=4

UFC 1-200-01, *BAUVORSCHRIFTEN DES US-VERTEIDIGUNGSMINISTERIUMS (ALLGEMEINE BAUANFORDERUNGEN)*

UNIFIED FACILITIES GUIDE SPECIFICATIONS (UFGS)

http://www.wbdg.org/ccb/browse_cat.php?o=29&c=3

UFGS 25 10 10, *ZENTRALES ENERGIEÜBERWACHUNGS- UND REGELSYSTEM (UMCS), FRONTEND UND INTEGRATION*

ANHANG B: GLOSSAR

B-1 ABKÜRZUNGEN

B-1.1 Allgemeine Abkürzungen

<u>Abkürzung</u>	<u>Begriff</u>
ACL	Access Control List: Zugangskontrollliste
AO	Authorizing Official: Autorisierungsbefugter
BAS	Building Automation System: Gebäudeautomationssystem
BCS	Building Control System: Gebäudekontrollsystem
CCTV	Closed Circuit Television: Videoüberwachungsanlage
CNSSI	Committee on National Security Systems Instruction: Anweisung der Kommission für nationale Sicherheitssysteme
CCI	Control Correlation Identifier
COTS	Commercial Off The Shelf: handelsüblich
CS	Control System: Kontrollsystem
DoD	Department of Defense: US-Verteidigungsministerium
ESS	Electronic Security System: elektronisches Sicherheitssystem
EMCS	Energy Monitoring and Control System: Energieüberwachungs- und -regelsystem
FCN	Field Control Network
FCS	Field Control System
FIPS	Federal Information Processing Standards: Bundesnormen zur Informationsverarbeitung
FISMA	Federal Information Security Management Act: Gesetz zur Informationssicherheit
FPOC	Field Point of Connection
GFE	Government Furnished Equipment: bauseits gelieferte Ausstattungen
ICS	Industrial Control System: industrielles Kontrollsystem
IDS	Intrusion Detection System: Einbruchmeldeanlage
ISSE	Information System Security Manager: Informationssystemssicherheitsmanager
ISSO	Information System Security Officer: Informationssystemssicherheitsbeauftragter
IP	Internet Protocol: Internetprotokoll
IT	Information Technology: Informationstechnik
MOA	Memorandum Of Agreement: Niederschrift des Vertrags
MOU	Memorandum Of Understanding: gemeinsame Absichtserklärung
NIST	National Institute of Standards and Technology: Nationales Institut für Normen und Technologie
OS	Operating System: Betriebssystem

Abkürzung Begriff

PIT	Platform Information Technology: Plattform-Informationstechnik
PKI	Public Key Infrastructure: Public-Key-Infrastruktur
SO	System Owner: Systembesitzer
UCS	Utility Control System: Versorgungskontrollsystem
UFC	Unified Facilities Criteria: Standardplanungskriterien für Anlagen und Einrichtungen
UFGS	Unified Facilities Guide Specification: Leitbeschreibungen für einheitliche Anlagen und Einrichtungen
UMCS	Utility Monitoring and Control System: Versorgungsüberwachungs- und -regelsystem
UPS	Uninterruptible Power Supply: unterbrechungsfreie Stromversorgung
USACE	U.S. Army Corps of Engineers: Ingenieurkorps der US-Armee

B-1.2 Abkürzungen für den Bereich Sicherheitskontrolle

Abkürzung Begriff

AC	Access Control: Zugangskontrolle
AT	Awareness and Training: Sensibilisierung und Schulung
AU	Audit and Accountability: Prüfungs- und Rechenschaftspflicht
CA	Security Assessment and Authorization: Sicherheitsbeurteilung und Autorisierung
CM	Configuration Management: Konfigurationsmanagement
CP	Contingency Planning: Krisenplanung
IA	Identification and Authorization: Identifizierung und Autorisierung
IR	Incident Response: Vorfalldreaktion
MA	Maintenance: Wartung
MP	Media Protection: Medienschutz
PE	Physical and Environmental Protection: Physische Sicherheitssysteme und Schutz vor Umwelteinflüssen
PL	Planning: Planung
PM	Program Management: Programm-Management
PS	Personnel Security: Personalsicherheit
RA	Risk Assessment: Risikobewertung
SA	System and Services Acquisition: Übernahme von Systemen und Diensten
SC	System and Communications Protection: System- und Kommunikationsschutz
SA	System and Information Integrity: System- und Informationsintegrität

B-2 BEGRIFFSDEFINITIONEN

<u>Begriff</u>	<u>Definition</u>
Genehmigungsbefugter (CNSSI Nr. 4009)	Ein höherer (Bundes-) Beamter bzw. leitender Angestellter mit der offiziellen Befugnis, bei einem annehmbaren Risikopotential für Betriebsprozesse (einschl. Einsatz, Funktionen, Ansehen und Ruf), Betriebsvermögen, Personen, andere Organisationen und die Nation die Verantwortung für den Betrieb eines Informationssystems zu übernehmen.
Gebäudeautomations-system (BAS)	Die Anlage besteht aus einem UMCS-Frontend, verbundener Gebäudeleit-technik, die die elektrischen und haustechnischen Systeme im Gebäude reguliert, und Benutzeroberflächen für Gebäudeleitüberwachung. Das BAS ist ein Untersystem der Versorgungsüberwachungs- und regelsystems. Dieser Begriff wird zunehmend durch „UMCS“ ersetzt.
Gebäudekontrollsystem (BCS)	Eine Anlage, die die elektrischen und haustechnischen Systeme wie HLK (einschl. zentraler Anlagen), Beleuchtung, senkrechte Fördersysteme und Bewässerungsanlagen, steuert. Gebäudekontrollsysteme verfügen in der Regel nicht über eine voll ausgestattete Benutzeroberfläche; sie haben möglicherweise lokale Anzeigetableaus, normalerweise wird aber das UMCS-Front End für sämtliche Funktionen der Benutzeroberfläche genutzt. Das BCS ist ein Untersystem des Versorgungsüberwachungs- und regel-systems und ist eine Art Field Control System.
Videoüberwachungsan-lage (CCTV)	Dieses elektronische Sicherheitssystem (ESS) ermöglicht die Videobeurtei-lung von Alarmzuständen durch Fernüberwachung und die Aufnahme von Videoereignissen. Videoüberwachung kann auch in anderen Systemen integriert sein, die nicht zur Videoüberwachungsanlage gehören.
Control Correlation Identifier (CCI)	Der Control Correlation Identifier (CCI) liefert eine Standardkennung und -beschreibung für jede einzelne, umsetzbare Anweisung, die eine Sicher-heitskontrolle umfasst.
Kontrollsystem (CS)	Ein System aus digitalen Controllern, Kommunikationsarchitektur und Be-nutzeroberflächen, mit welchen die Infrastruktur und Geräte überwacht bzw. überwacht und kontrolliert werden.
Controller	Ein elektronisches Gerät, in der Regel ausgestattet mit interner Program-mierungslogik und digitalen sowie analogen Ein-/Ausgängen, das Kontroll-funktionen durchführt. Die beiden primären Arten von Controllern sind Ge-rätecontroller und Überwachungscontroller.
Verteiltes Kontrollsys-tem	Dieser Ausdruck wird zunehmend durch BCS, UCS bzw. UMCS ersetzt.

<u>Begriff</u>	<u>Definition</u>
Elektronisches Sicherheitssystem (ESS)	Ein integriertes elektronisches System, das (physische) Einbruchmeldeanlagen (IDS) im Innen- und Außenbereich, Videoüberwachungsanlagen zur Beurteilung von Alarmzuständen, Zugangskontrollsysteme, Datenübertragungsmedien und Alarmmeldeanlagen zur Überwachung, Steuerung und Anzeige, umfasst.
Energieüberwachungs- und -regelsystem (EMCS)	Eine weitere Bezeichnung für ein Versorgungsüberwachungs- und -regelsystem. Siehe UMCS.
Engineering Tool Software	Software, die zur Durchführung von Geräte- bzw. Netzwerkmanagement für ein Kontrollsystem zum Einsatz kommt; einschließlich Netzwerkkonfiguration, Controllerkonfiguration und Controllerprogrammierung.
Gerätecontroller (EC)	Ein Controller zur Umsetzung von Kontrolllogik zur Steuerung eines Geräts. Hinweis: Ein Controller definiert sich über seine Nutzung; viele ECs können auch als Überwachungscontroller (SC) eingesetzt werden. Beispiele für Gerätecontroller: Klimagerätecontroller, Schutzrelais und Pumpencontroller. Es ist zu beachten, dass Geräte wie Stromzähler oder Smart-Sensoren, die lediglich Überwachungsfunktionen ausführen, trotzdem als Gerätecontroller zählen (auch wenn sie nicht wirklich irgendetwas steuern).
Liegenschaftsabhängiges Kontrollsystem	Ein Kontrollsystem, das die Geräte und Infrastruktur als Teil eines Gebäudes, eines Bauwerks oder einer linearen Struktur des US-Verteidigungsministeriums kontrolliert.
Field Control System (FCS)	Ein Gebäudekontrollsystem, Versorgungskontrollsystem, Zugangskontrollsystem, usw. innerhalb der Liegenschaft und dem FPOC „nachgeschaltet“.
Field Control Network (FCN)	Ein Netzwerk, das vom Gebäudekontrollsystem, Versorgungskontrollsystem, usw. innerhalb der Liegenschaft genutzt wird und dem FPOC „nachgeschaltet“ ist. Dies umfasst: IP, Ethernet, RS-485, TP/FT-10 und weitere Netzwerkinfrastrukturen, die Kontrollsysteme in einer Liegenschaft unterstützen.
Field Point of Connection (FPOC)	Der FPOC ist der Verbindungspunkt zwischen dem IP-Netzwerk des Kontrollsystems und dem Field Control Network (IP-Netzwerk, Nicht-IP-Netzwerk oder beides). Bei der Hardware, die die Verbindung an dieser Stelle zur Verfügung stellt, handelt es sich um ein IT-Gerät, wie z.B. einen Schalter, IP-Router oder eine Firewall.
[UMCS, ESS, usw.] Frontend	Der Teil des Kontrollsystems, der überwiegend aus EDV-Geräten, wie z.B. Computern und zugehörigem Equipment besteht, und genutzt wird, um Betriebsfunktionen auszuführen und Überwachungs- bzw. Kontroll-/Engineering Tool-Anwendungen ablaufen zu lassen. Das Frontend kontrolliert die physischen Systeme nicht direkt; es kommuniziert mit diesen nur über das Field Control System. Das Frontend ist ein Bestandteil der Infrastruktur [von UMCS, ESS usw.] (siehe Definition).

<u>Begriff</u>	<u>Definition</u>
Auswirkung	Die Auswirkung auf betriebliche Abläufe der Organisation, Betriebsvermögen oder Personen aufgrund von mangelhafter Vertraulichkeit, Integrität oder Verfügbarkeit im Kontrollsystem. Der Auswirkungsgrad wird in eine von drei Stufen kategorisiert: • GERING: begrenzte negative Auswirkung • MITTEL: erhebliche negative Auswirkung • HOCH: schwerwiegende bzw. katastrophale negative Auswirkung Im Sinne der Klarheit wird der Auswirkungsgrad eines Systems allgemein komplett in GROSSBUCHSTABEN geschrieben.
Vorfall (FIPS PUB 200)	Ein Vorfall, der die Vertraulichkeit, Integrität oder Verfügbarkeit eines Informationssystems oder der in einem System verarbeiteten, gespeicherten oder weitergeleiteten Informationen tatsächlich oder potentiell gefährdet, bzw. der eine Verletzung oder unmittelbare bevorstehende Verletzung der Sicherheitsauflagen, Sicherheitsabläufe bzw. der Nutzungsrichtlinien darstellt.
Industrielles Kontrollsystem (ICS)	Eine Art Kontrollsystem. Genauer gesagt, ein Kontrollsystem, das die industriellen (Herstellungs-)Prozesse kontrolliert. Wird auch manchmal mit Bezug auf andere Arten von Kontrollsystemen eingesetzt; insbesondere Versorgungskontrollsysteme, wie Elektro-, Gas- oder Wasserverteilungssysteme.
Informationssystem (CNSSI Nr. 4009)	Eine eigenständige Reihe von Informationsquellen, strukturiert für das Sammeln, Verarbeiten, Unterhalten, Nutzen, Teilen, Verbreiten bzw. Verwenden von Informationen. Hinweis: Informationssysteme umfassen auch spezielle Systeme wie z.B. industrielle/ Ablauf bezogene Kontrollsysteme, Telefonschaltungen und Nebenstellenanlagen (PBX).
Informationstechnik (IT)	Jegliche Ausstattungsgeräte oder miteinander verbundene Systeme bzw. Untersysteme von Ausstattungsgeräten, die von der Verwaltungsstelle zur automatischen Beschaffung, Speicherung, Bearbeitung, Verwaltung, Verschiebung, Kontrolle, Anzeige, Austausch, Weiterleitung oder Erhalt von Daten bzw. Informationen eingesetzt werden.
[UMCS, ESS, ...] Infrastruktur	Der Teil des Kontrollsystems (z.B. ein UMCS oder ESS), welcher alle Komponenten umfasst, die nicht Teil des Field Control Systems sind. Bei diesen Komponenten handelt es sich u.a. um den FPOC, die Plattform Enclave und das Frontend (d.h. die zugehörigen Architekturlevels 3, 4 und 5).

<u>Begriff</u>	<u>Definition</u>
Einbruchmeldeanlage (IDS) [physisch/ESS]	Ein System bestehend aus inneren und äußeren Sensoren, Überwachungsgeräten und zugehörigen Kommunikationsuntersystemen, die zusammen einen Einbruch in ein spezielles Grundstück, eine Einrichtung bzw. in den Umkreis feststellen und einen Alarm absetzen.
Einbruchmeldeanlage (IDS) [Internet]	Ein Gerät bzw. eine Softwareanwendung, das die Netzwerk- oder Systemaktivitäten mit Hinblick auf schädliche Aktivitäten bzw. Regelverletzungen überwacht und Berichte für die Verwaltung erstellt.
Prinzip der geringsten Privilegien (CNSSI Nr. 4009)	Das Prinzip, nach dem eine Sicherheitsarchitektur so auszulegen ist, dass für jede Dateneinheit die Mindestsystemquellen und -berechtigungen eingerichtet sind, welche die Dateneinheit benötigt, um ihre Funktion ausführen zu können.
Mobilcode (NIST SP 800-53r4)	Softwareprogramme bzw. Teile von Programmen, die ohne explizite Installation bzw. Ausführung durch den Empfänger über Ferninformationssysteme bezogen, über ein Netzwerk weitergeleitet und auf einem lokalen Informationssystem ausgeführt werden.
Mobilcode-Technologie (NIST SP 800-53r4)	Softwaretechnologien, die den Mechanismus zur Erstellung und Nutzung von Mobilcode zur Verfügung stellen (z.B. Java, JavaScript, ActiveX, VBScript)
Fernwartung (NIST SP 800-53)	Wartungsaufgaben, die von Personen per Kommunikation über ein Netzwerk ausgeführt werden; entweder über ein externes Netzwerk (z.B. das Internet) oder ein internes Netzwerk.
Betriebsarchitektur (Operational Architecture - OA)	Die Komponenten eines Kontrollsystems, die ausschließlich Betriebskomponenten eines Systems sind, z.B. Controller, Frontend-Software und andere Geräte, die Betriebsfunktionen unterstützen. Wenn der Platform-Enclave-Ansatz zur Autorisierung eines Kontrollsystems eingesetzt wird, haben die „nicht-Standard-IT“-Anteile des Kontrollsystems die Zulassung als Betriebsarchitektur und das Gesamtsystem hat zwei Berechtigungen: Platform Enclave und Betriebsarchitektur.
[UMCS, ESS, ...] Platform Enclave	Die Komponenten eines Kontrollsystems, bei denen es sich um Standard-IT-Komponenten handelt und die standardmäßig und unabhängig von der Art des Kontrollsystems gesichert werden können. Diese Komponenten dienen ausschließlich dem Kontrollsystem und umfassen IP-Netzwerk, Netzwerkmanagement und Sicherheitsgeräte (z.B. Schalter, Router), Software, Computer bzw. andere Geräte zur Verwaltung und Sicherung des Netzwerks.
Platform IT (PIT)	IT-Hard- oder Software, die physisch Bestandteil von Systemen mit besonderen Aufgaben ist, speziell dafür gedacht ist oder für die Ausführung der Aufgaben in Echtzeit unentbehrlich ist.

<u>Begriff</u>	<u>Definition</u>
Fernzugriff (NIST SP 800-53)	Der Fernzugriff stellt den Zugriff auf Informationssysteme der Organisation durch den Benutzer (oder Prozesse, die für den Benutzer agieren) dar und kommuniziert über ein externes Netzwerk (z.B. das Internet).
Risiko (NIST SP 800-53)	Das Ausmaß des Umfangs, bis zu welchem eine Dateneinheit von potentiellen Umständen oder Ereignissen bedroht wird, und ein Maß für: (i) die negativen Auswirkungen, die entstehen würden, falls der Umstand bzw. das Ereignis eintritt; und (ii) die Wahrscheinlichkeit des Vorfalls. Sicherheitsrisiken bezogen auf das Informationssystem sind solche Risiken, die durch den Verlust von Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen oder Informationssystemen entstehen, und die potentielle negative Auswirkungen auf betriebliche Abläufe der Organisation (einschl. Einsatz, Funktionen, Ansehen und Ruf), Betriebsvermögen, Personen, andere Organisationen und die Nation, darstellen.
Risikomanagement (NIST SP 800-53)	Der Vorgang des Risikomanagements für betriebliche Abläufe der Organisation (einschließlich Einsatz, Funktionen, Ansehen, Ruf), Betriebsvermögen, Personen, andere Organisationen und die Nation, der sich aus dem Einsatz eines Informationssystems ergibt, und Folgendes einschließt: (i) die Durchführung einer Risikobewertung; (ii) das Umsetzen einer Risikominierungsstrategie; und (iii) die Anwendung von Techniken und Vorgängen zu einer kontinuierlichen Überwachung des Sicherheitszustandes des Informationssystems.
Supervisory Control and Data Acquisition (SCADA)	Je nach Zusammenhang kann dieser Begriff die verschiedensten Bedeutungen haben; daher wird der Ausdruck in dieser UFC nicht verwendet. Stattdessen wird BCS, UCS und UMCS eingesetzt, da diese Begriffe genauer und eindeutiger sind.
Überwachungscontroller	Ein Controller zur Umsetzung einer Kombination aus Überwachungslogik (globale Kontrolle oder Optimierungsstrategien), Terminplanung, Alarmgebung, Eventmanagement, Trends, Webservices bzw. Netzwerkmanagement. Ein Überwachungscontroller kann zwischen der Plattform Enclave und dem Field Control System als Datenkonsolidierungsleitung zwischen dem FCS und dem Frontend angeordnet werden. Es ist zu beachten, dass diese Anordnung durch die Nutzung definiert wird; viele Überwachungscontroller bieten auch die Möglichkeit, Geräte direkt zu steuern, und dienen sowohl als Überwachungscontroller als auch als Gerätecontroller.
Systembesitzer (System Owner - SO) (CNSSI Nr. 4009)	Die Person bzw. Organisation, die für Entwicklung, Beschaffung, Integration, Modifizierung, Betrieb und Wartung bzw. für die endgültige Anordnung eines Informationssystems verantwortlich ist.

<u>Begriff</u>	<u>Definition</u>
Versorgungskontrollsystem (UCS)	Eine Art Field Control System für die Kontrolle von Versorgungssystemen, wie z.B. Elektroverteilung und -erzeugung, Abwassersammlung und -behandlung, Wassererzeugung und -pumpen, usw. Gebäudesteuerungen sind nicht in einem UCS enthalten, es ist jedoch möglich sowohl ein Versorgungskontrollsystem als auch ein Gebäudekontrollsystem in der gleichen Einrichtung vorzusehen, wobei diese Systeme Komponenten wie z.B. das FPOC gemeinsam nutzen. Das UCS ist ein Untersystem des Versorgungsüberwachungs- und -regelsystems (UMCS) und eine Art Field Control System (FCS).
Versorgungsüberwachungs- und -regelsystem (UMCS)	Ein System bestehend aus einem oder mehreren Gebäudekontrollsystemen bzw. Versorgungskontrollsystemen und der zugehörigen UMCS-Infrastruktur. Mit anderen Worten: es handelt sich hier um das gesamte Versorgungsüberwachungssystem - vom Frontend bis zu den Gerätecontrollern. Auf dem höchsten Level besteht die UMCS aus einer UMCS-Platform Enclave und einem UMCS-Frontend (zusammen betitelt als UMCS-Infrastruktur) und ist mit Field Control Systemen verbunden.
Schwachstellen (NIST SP 800-53)	Schwachstellen in einem Informationssystem, in Systemsicherheitsabläufen, internen Steuerungen oder der Umsetzung, die von einer Gefahrenquelle ausgenutzt bzw. ausgelöst werden könnten.

ANHANG C: RISK MANAGEMENT FRAMEWORK (RMF), ÜBERSICHT

C-1 RMF - ÜBERSICHT

Gemäß Definition des National Institute of Standards and Technology (NIST) ist RMF „der Vorgang des Risikomanagements für betriebliche Abläufe der Organisation (einschließlich Einsatz, Funktionen, Ansehen, Ruf), Betriebsvermögen, Personen, andere Organisationen und die Nation, der sich aus dem Einsatz eines Informationssystems ergibt, und Folgendes einschließt: (i) die Durchführung einer Risikobewertung; (ii) das Umsetzen einer Risikominderungsstrategie; und (iii) die Anwendung von Techniken und Vorgängen zur kontinuierlichen Überwachung des Sicherheitszustandes des Informationssystems.“ Im RMF wird detailliert dargestellt, wie Risikomanagement im Hinblick auf die Informationstechnik des US-Verteidigungsministeriums gemäß DoDI 8510.01 angewendet wird.

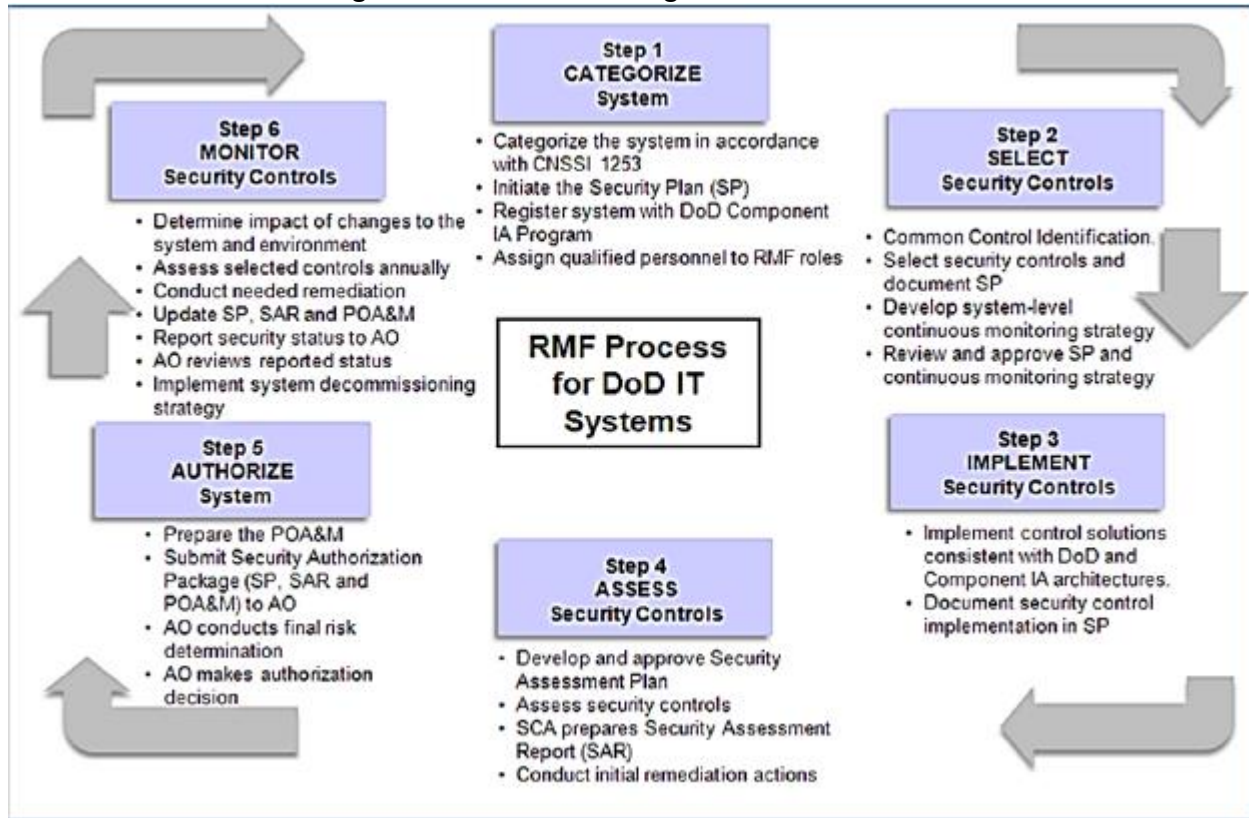
C-2 RMF - VORGANG

Wie in Abbildung C-3 dargestellt, handelt es sich bei RMF um einen Vorgang in 6 Schritten:

1. Kategorisierung des Systems: Kategorisierung des Kontrollsystems anhand des Auswirkungsgrads auf Vertraulichkeit, Integrität und Verfügbarkeit (C-I-A), sowohl unter Berücksichtigung des Betriebs als auch der Bedeutung des Kontrollsystems für den Betrieb. Der Systemeigentümer (SO) legt den C-I-A Auswirkungsgrad fest; dieser ist daher nicht Teil des Umfangs dieser UFC.
2. Auswahl eines Sicherheitskontrolltyps: Basierend auf dem C-I-A Grad werden aus dem CNSSI Nr. 1253 und NIST SP 800-82 eine Reihe von Kontrolltypen und eine Schablone ausgewählt. In vielen Fällen werden diese Kontrolltypen weiter angepasst, abhängig von den Anforderungen des Kontrollsystems vor ihrer Umsetzung. Während diese einen UFC Leitfaden im Hinblick auf die Anwendbarkeit spezieller Kontrollen anbietet, obliegt der Auswahlvorgang von Sicherheitskontrollen im Allgemeinen nicht dem Planer.
3. Umsetzung von Sicherheitskontrollen: Die Umsetzung vieler Sicherheitskontrollen liegt außerhalb des Verantwortungsbereichs des Planers. Die vorliegende UFC konzentriert sich auf Sicherheitskontrollen, die der Planer in irgendeiner Form im Design mit einbeziehen muss, im Allgemeinen durch das Einbinden von Anforderungen in die Pläne und Zeichnungen, und auf Sicherheitskontrollen, über die der Planer möglicherweise Auskunft geben muss.
4. Bewertung von Sicherheitskontrollen: Nach der Umsetzung wird die Effizienz der Umsetzung bewertet.
5. Autorisierung des Systems: Wenn die Bewertung zufriedenstellend ausgefallen ist, so wird das vom Kontrollsystem ausgehende Restrisiko offiziell durch den AO akzeptiert und er autorisiert den Betrieb des Systems durch das Aushändigen einer Betriebsgenehmigung.

6. Überwachung von Sicherheitskontrollen: Das RMF tritt in eine Überwachungs- und Bewertungsphase ein, in der das Kontrollsystem überwacht und periodisch neu bewertet wird.

Abbildung C-3: NIST Risk Management Framework Schritte



C-3 DEFINITION VON KONTROLLEN GEMÄSS NIST UND DODI 8510

C-3.1 Kontrollfamilien

Da die Bewertung einer Leistungsanforderung schwierig ist („Reduzieren des Risikos unter ein bestimmtes Niveau“), stellt NIST einen Katalog mit möglichen Anforderungen zur Verfügung, wobei die Erfüllung einer bestimmten Anforderung das Gesamtrisiko für das System verringert. Diese Anforderungen sind weitestgehend in den folgenden Gruppierungen kategorisiert (diese werden oft als „Kontrollfamilien“ bezeichnet):

- AC - Access Control: Zugangskontrolle
- AT - Awareness and Training: Sensibilisierung und Schulung
- AU - Audit and Accountability: Prüfungs- und Rechenschaftspflicht
- CA - Security Assessment and Authorization: Sicherheitsbeurteilung und Autorisierung
- CM - Configuration Management: Konfigurationsmanagement
- CP - Contingency Planning: Krisenplanung

- IA - Identification and Authorization: Identifizierung und Autorisierung
- IR - Incident Response: Vorfallreaktion
- MA - Maintenance: Wartung
- MP - Media Protection: Medienschutz
- PE - Physical and Environmental Protection: Physische Sicherheitssysteme und Schutz vor Umwelteinflüssen
- PL - Planning: Planung
- PM - Program Management: Programm-Management
- PS - Personnel Security: Personalsicherheit
- RA - Risk Assessment: Risikobewertung
- SA - System and Services Acquisition: Übernahme von Systemen und Diensten
- SC - System and Communications Protection: System- und Kommunikationsschutz
- SI - System and Information Integrity: System- und Informationsintegrität

C-3.2 Kontrollelemente und Erweiterungen

Innerhalb jeder Kontrollfamilie gibt es viele verschiedene Kontrollen, von denen die meisten eine große Anzahl an Unterelementen aufweisen. Für viele Kontrollen gibt es außerdem Erweiterungen; dabei handelt es sich um zusätzliche Aktionen, die durchgeführt werden können, um den Effektivität der Kontrolle zu steigern. Einzelnen Kontrollen wird eine Zahl innerhalb der Kontrollfamilie zugeordnet, Erweiterungen sind unternummeriert, und Kontroll- oder Erweiterungselemente sind mit Buchstaben versehen. Erweiterungen und Kontrollelemente stehen in Klammern nach der Kontrollnummer. Ein Beispiel aus NIST SP 800-53 AC-2 findet sich in Abbildung C-4.

Abbildung C-4: NIST SP 800-53 Kontrolle AC-2

AC-2 ACCOUNT MANAGEMENT

Control: The organization manages information system accounts, including:

Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary);

- a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [*Assignment: organization-defined information system account types*];
- b. Assigns account managers for information system accounts;
- c. Establishing conditions for group and role membership;
- d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
- e. Requires approvals by [*Assignment: organization-defined personnel or roles*] for requests to create information system accounts;
- f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [*Assignment: organization-defined procedures or conditions*];
- g. Monitors the use of information system accounts;
- h. Notifying account managers:
 1. When accounts are no longer required;
 2. When users are terminated or transferred; and
 3. When individual information system usage or need-to-know changes;
- i. Authorizes access to the information system based on:
 1. A valid access authorization;
 2. Intended system usage; and
 3. Other attributes as required by the organization or associated missions/business functions;
- j. Reviews accounts for compliance with account management requirements [*Assignment: organization-defined frequency*]; and
- k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

Supplemental Guidance: Information system account types include, for example, individual, shared,...⁴

Related controls: AC-3, AC-4, AC-5, AC-6, AC-10, AC-17, AC-19, AC-20, AU-9, IA-2, IA-4, IA-5, IA-8, CM-5, CM-6, CM-11, MA-3, MA-4, PL-4, SC-13.

Control Enhancements:

(1) ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT ⁴

The organization employs automated mechanisms to support the management of information system accounts.

(2) ACCOUNT MANAGEMENT | REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS ⁴

The information system automatically [*Selection: removes; disables*] terminates temporary and emergency accounts after [*Assignment: organization-defined time period for each type of account*].

(3) ACCOUNT MANAGEMENT | DISABLE INACTIVE ACCOUNTS

The information system automatically disables inactive accounts after [*Assignment: organization defined time period*].

(4) ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS ⁴

The information system automatically audits account creation, modification, enabling, disabling, and removal actions and notifies [*Assignment: organization-defined personnel or roles*].

(5) ACCOUNT MANAGEMENT | INACTIVITY LOGOUT ⁴

The organization requires that users log out when [*Assignment: organization-defined time-period of expected inactivity or description of when to log out*].

⁴Der Kürze halber ist nicht der vollständige 'Supplemental Guidance' Text des AC-2 ACCOUNT MANagements abgebildet.

- (6) ACCOUNT MANAGEMENT | DYNAMIC PRIVILEGE MANAGEMENT⁴
The information system implements the following dynamic privilege management capabilities: [Assignment: organization-defined list of dynamic privilege management capabilities].
- (7) ACCOUNT MANAGEMENT | ROLE-BASED SCHEMES⁴
The organization:
 - (a) Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles;
 - (b) Monitors privileged role assignments; and
 - (c) Takes [Assignment: organization-defined actions] when privileged role assignments are no longer appropriate.
- (8) ACCOUNT MANAGEMENT | DYNAMIC ACCOUNT CREATION⁴
The information system creates [Assignment: organization-defined information system accounts] dynamically.
- (9) ⁴ACCOUNT MANAGEMENT | RESTRICTIONS ON USE OF SHARED / GROUP ACCOUNTS
The organization only permits the use of shared/group accounts that meet [Assignment: organization-defined conditions for establishing shared/group accounts].
- (10) ACCOUNT MANAGEMENT | SHARED / GROUP ACCOUNT CREDENTIAL TERMINATION
The information system terminates shared/group account credentials when members leave the group.
- (11) ACCOUNT MANAGEMENT | USAGE CONDITIONS⁴
The information system enforces [Assignment: organization-defined circumstances and/or usage conditions] for [Assignment: organization-defined information system accounts].
- (12) ACCOUNT MANAGEMENT | ACCOUNT MONITORING / ATYPICAL USAGE⁴
The organization:
 - (a) Monitors information system accounts for [Assignment: organization-defined atypical usage]; and
 - (b) Reports atypical usage of information system accounts to [Assignment: organization-defined personnel or roles].
- (13) ACCOUNT MANAGEMENT | DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS⁴
The organization disables accounts of users posing a significant risk within [Assignment: organization-defined time period] of discovery of the risk.

In dieser Darstellung ist AC-2 (5) Erweiterung 5: "The organization requires that users log out when....".

C-3.3 Control Correlation Identifier

Die Umsetzung des US-Verteidigungsministeriums für NIST-Kontrollen für Kontrollsysteme ist DoDI 8500. Das US-Verteidigungsministerium hat darüber hinaus noch jede Kontrolle und jedes Kontrollelement in konkrete Aktionen unterteilt; dabei ist jede Aktion mit einem eigenen Control Correlation Identifier (CCI) versehen. So ist beispielsweise die oben abgebildete Kontrolle AC-2 in 61 separate CCIs unterteilt, mit allein 11 unterschiedlichen CCIs nur für AC-2 (4).

Während dies auf der einen Seite zu einem sehr feinen Umsetzungsgrad führt (das Kontrollsystem könnte die Kontoerstellung kontrollieren, dafür aber nicht die Kontoveränderung), führt es auf der anderen Seite zu vielen Abhängigkeiten zwischen CCIs. Zwei der CCIs die mit der Sicherheitskontrolle AC-2(4) verbunden und auf dem RMF Knowledge Service (Security Control Explorer) zu finden sind:

- CCI-000018: "The information system automatically audits account creation actions." (Das Informationssystem prüft automatisch Handlungen zur Accounterstellung.)
- CCI-001683: "The information system notifies organization-defined personnel or roles for account creation actions." (Das Informationssystem informiert von der Organisation festgelegte Personen oder Rollen über Aktionen zur Kontoerstellung.)

Hinweis: Die Website des RMF Knowledge Service ist <https://rmfks.osd.mil>.

Auch wenn diese als unabhängige CCIs geschrieben sind, hängen sie doch eng miteinander zusammen und es ist schwierig, sich ein Benachrichtigungssystem vorzustellen, bei dem keine Audit-Funktion mit eingeschlossen ist.

C-4 ANFORDERUNGSBESCHREIBUNG UND -UMSETZUNG

Allgemein gesprochen, können CCIs in Anforderungsbeschreibung und Anforderungsumsetzung unterteilt werden.

1. Ein CCI beschreibt eine Anforderung, wenn das CCI so aufgebaut ist, dass „<jemand> eine <Anforderung> beschreibt“. Beispiele für CCIs, die eine Anforderung beschreiben, sind Formulierungen wie: „Die Organisation definiert...“
 - a. „... ein Mindestmaß bezüglich der Detailliertheit der Dokumentation“,
 - b. „... eine Mindestanforderung für die Häufigkeit an, mit der einige Kriterien überprüft werden müssen“
 - c. „... eine Reihe von Ereignissen, die eine Gefahr für die Sicherheit darstellen“, oder
 - d. „...eine Methode oder Vorgehensweise zur Abänderung des Kontrollsystems“
2. Ein CCI beschreibt eine Anforderung, wenn der CCI so aufgebaut ist, dass „<jemand/etwas> eine <Anforderung> erfüllt“, wobei die CCI-Anforderung normalerweise in einem entsprechenden CCI beschrieben wird. Beispiele für CCIs, die eine Anforderung umsetzen, die in einem vorherigen Beispiel beschrieben wurde, sind Formulierungen wie: „Die Organisation ...“
 - a. ... erreicht das erforderliche Dokumentationsniveau“,
 - b. ... überprüft einen Sicherheitsplan jährlich“,
 - c. ... antwortet auf physische Sicherheitslücken“, oder
 - d. ... stimmt der Änderung des Kontrollsystems durch ein Gremium für Konfigurationsmanagement zu“

C-4.1 CCIs zur Anforderungsbeschreibung

CCIs, die eine Anforderung beschreiben, können vom Planer gestaltet werden, aber sie werden oftmals von der Organisation selbst gestaltet oder sind bereits vom US-Verteidigungsministerium einheitlich beschrieben worden. In einigen Fällen wird die finale Formulierung der Anforderung von der Organisation selbst stammen, allerdings basierend auf dem Input durch den Planer, der das Kontrollsystem kennt und über dessen besondere Schwachpunkte, die angesprochen werden müssen, Bescheid weiß.

Beispielsweise muss der Planer Input zur Passwort-Komplexität bereitstellen, da nicht alle Komponenten des Kontrollsystems Passwörter unterstützen werden, und diejenigen, die es tun, werden möglicherweise Passwörter mit unterschiedlicher Komplexität unterstützen. In vielen Fällen sind durch das US-Verteidigungsministerium formulierte Anforderungen völlig ungeeignet für Kontrollsysteme und der Planer muss die Abweichungen von den Beschreibungen des US-Verteidigungsministeriums in der Planung dokumentieren.

C-4.2 CCI zur Anforderungsumsetzung

CCIs, die eine Anforderung umsetzen, können noch weiter unterteilt werden, im Hinblick darauf wer/was die Umsetzung durchführt: die Organisation (bzw. Vererbung von einem anderem Element) oder das Kontrollsystem. „Die Organisation führt Hintergrundchecks durch“ ist ein Beispiel für ersteres, „Das Kontrollsystem loggt Benutzer aus, wenn sie über einen längeren Zeitraum inaktiv waren“ gehört zu letzterem. In einigen Fällen ist dies nicht klar definierbar - ein CCI mit der Formulierung „Die Organisation stellt eine minimale Passwortlänge sicher“⁵⁵ stellt scheinbar eine Anforderung an die Organisation dar, aber nach kurzer Überlegung wird klar, dass es sich dabei um eine Aktion handelt, die durch das Kontrollsystem umgesetzt werden muss (da das Kontrollsystem eine Passworteintragung entweder akzeptiert oder zurückweist), und nicht durch die Organisation. Durch die Organisation umgesetzte CCIs werden nicht vom Planer entworfen und liegen außerhalb des Umfangs dieser UFC. Auf der anderen Seite werden CCIs, die vom Kontrollsystem umgesetzt werden, normalerweise vom Planer entworfen, da die Umsetzung eines CCI zu einer Ausführungsanforderung für die Spezifikation des Kontrollsystems wird.

C-5 PLATTFORM-INFORMATIONSTECHNOLOGIE

Die Umsetzung des US-Verteidigungsministeriums der RMF beschreibt die Plattform-Informationstechnik (PIT) als „IT-Hard- oder Software, die physisch Bestandteil von Systemen mit besonderen Aufgaben ist, speziell dafür gedacht ist oder für die Ausführung der Aufgaben in Echtzeit unentbehrlich ist“, und unterscheidet PIT-Systeme von gewöhnlichen Informationssystemen. Insbesondere besagt DoDI 8500.01, dass PIT-Systeme „eine individuell zugeschnittene Reihe von Sicherheitskontrollen und Kontrollvalidierungsvorgängen benötigen und Sicherheitsbewerter und AOs mit besonderen Qualifikationen erfordern“

Die Cyber-Sicherheit von PIT-Systemen, wie z.B. Kontrollsystemen, erfordert nicht nur die Nutzung von individualisierbaren Referenzwerten, sondern auch ein weiteres Zuschneiden der Kontrollen, die für das spezifische Kontrollsystem geeignet sind.

⁵ Hierbei handelt es sich nicht um den Text eines tatsächlichen CCI, sondern es handelt sich dabei lediglich um ein fiktives Beispiel zu Illustrationszwecken.

Diese Seite wurde absichtlich freigelassen.

ANHANG D: PLATFORM ENCLAVE

D-1 PLATFORM ENCLAVE, KONZEPT-ÜBERSICHT

Die Tatsache, dass ein beträchtlicher Teil des Kontrollsystems einem Standard IT-System ähnelt, welches für verschiedene Kontrollsysteme verwendet werden kann, unabhängig von den Details des Kontrollsystem selbst, hat zur Shaffung der Platform Enclave geführt. Dieses Konzept gruppiert die Standard-IT Anteile des Kontrollsystems in ein System ein, welches separat vom restlichen Kontrollsystem behandelt werden kann. In einigen Fällen wird diese Platform Enclave separat autorisiert und das gesamte Kontrollsystem verfügt über zwei Autorisierungen, während in anderen Fällen eine einzelne Autorisierung für das Gesamtsystem verwendet wird. Auch in Fällen, in denen nur eine Autorisierung verwendet wird, ist es jedoch hilfreich, den Anteil an Standard-IT-Elementen des Kontrollsystems zu identifizieren und kategorisieren.

D-2 PLATFORM ENCLAVE MIT ZWEI AUTORISIERUNGEN

Ein Hauptgrund für die Erstellung einer Platform Enclave ist die Möglichkeit eines Ansatzes, bei dem ein Kontrollsystem mit **zwei** Risk Management Framework Autorisierungen umgesetzt werden kann, davon eine für die Anteile der Platform Enclave und eine für die Anteile außerhalb der Platform Enclave des Kontrollsystems, die manchmal als die „Nicht-Standard-IT“ Anteile bezeichnet werden. Auch wenn dies scheinbar dazu führt, dass der Aufwand verdoppelt wird, so ist das doch im Allgemeinen nicht der Fall:

- Auch wenn viele Kontrollen wie zum Beispiel Richtlinien und Verfahrensweisen sowohl bei der Platform Enclave als auch bei den „Nicht-Standard-IT“ Anteilen durchgeführt werden müssen, können diese Richtlinien und Verfahrensweisen oftmals entweder von einer anderen Autorisierungsinstanz übernommen werden oder sowohl in der Platform Enclave und der „Nicht-Standard-IT“ genau gleich umgesetzt werden.
- Einige Kontrollen können in der Platform Enclave angewendet und dann vom „Nicht-Standard-IT“ übernommen werden. Beispielsweise können Kontrollen, die mit dem Fernzugriff zusammenhängen, durch die Platform Enclave unabhängig von der „Nicht-Standard-IT“ definiert werden, und dann ggf. von der „Nicht-Standard-IT“ übernommen werden.
- Während einige Kontrollen sowohl in der Platform Enclave als auch in der „Nicht-Standard-IT“ umgesetzt werden müssen, so müssen sie doch unterschiedlich durchgeführt werden und oftmals auch jeweils mit unterschiedlichem Umfang.

D-3 Vorteile der Platform Enclave

Der Hauptvorteil des Ansatzes der Platform Enclave ist, dass dies eine Differenzierung zwischen „Standard IT“ und „Nicht-Standard-IT“ Komponenten des Kontrollsystems ermöglicht, und darüber hinaus eine Einzelautorisierung für den IT-Anteil zulässt, um verschiedene Kontrollsystemtypen abzudecken. Diese Vorgehensweise macht am meisten Sinn, wenn bereits eine Netzwerk- und Cyber-Sicherheitsinfrastruktur besteht, auf der die Platform Enclave eingerichtet wird, wie dies bei den meisten Liegenschaften des US-Verteidigungsministeriums der Fall ist. Im Idealfall wird die Platform Enclave standardmäßig eingerichtet und für die jeweiligen Teilstreitkräfte zur Umsetzung in jeder Liegenschaft autorisiert, im Gegensatz zu den „Nicht-Standard-IT“ Anteilen des Kontrollsystems („operative Architektur“), bei denen Faktoren wie der Typ, der Verkäufer und das Protokoll des Kontrollsystems eher dazu führen, dass jede Autorisierung individuell ist und nicht dem Standard entspricht.

D-4 PLATFORM-ENCLAVE-ANSATZ DER ARMY

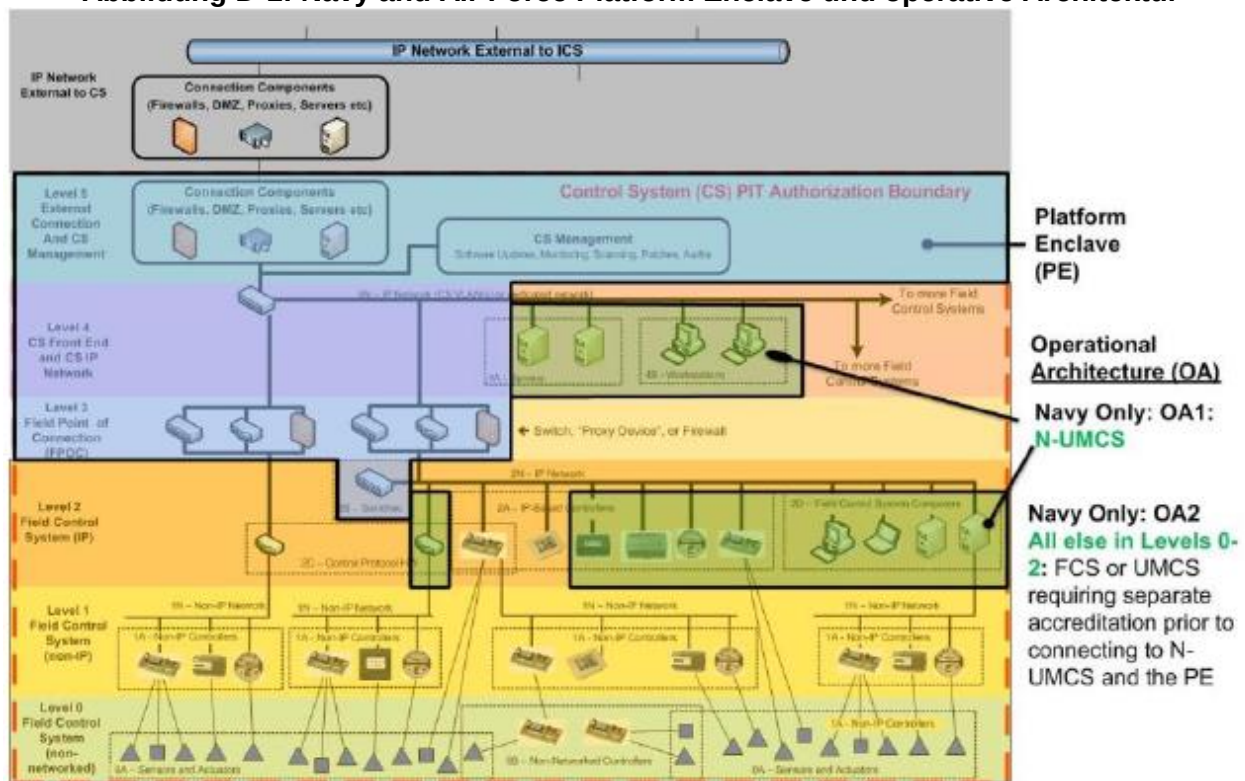
Die Army hat keinen Platform Enclave Ansatz formalisiert.

D-5 PLATFORM-ENCLAVE-ANSATZ DER NAVY FÜR BCS UND UCS

Abbildung D-1 zeigt, welche Komponenten der 5-stufigen Kontrollsystemarchitektur in der Platform Enclave (PE) der Navy, er sog. Control System Platform Enclave (CS-PE) enthalten sind. Die Navy CS-PE wird heutzutage bei Navy-Liegenschaften implementiert und verwendet. Die Navy setzt eine operative Architektur (OA) mit dem Namen Navy Utilities Monitoring and Control System (NUMCS) ein, die in Abbildung D-1 dargestellt ist.

Alle Kontrollsysteme müssen sich mit der Platform Enclave verbinden und entweder separat autorisiert werden oder unter die Typenfreigabe für CS-PE und NUMCS fallen.

Abbildung D-1: Navy and Air Force Platform Enclave und operative Architektur



D-6 PLATFORM-ENCLAVE-ANSATZ DER AIR FORCE

Abbildung D-1 zeigt, welche Komponenten der 5-stufigen der Kontrollsystemarchitektur in der Platform Enclave und den operativen Architekturbereichen enthalten sind. Der Bereich der Platform Enclave soll laut dem Autorisierungsbefugten der Air Force für Plattform-Informationstechnik bei Industriellen Kontrollsystemen (AF ICS PIT AO) Archetypen (zugelassene Typen) entsprechen. Außerdem soll der Bereich operative Architektur laut AF ICS PIT AO, soweit sinnvoll und so gut wie möglich, auch den Archetypen der Air Force entsprechen. Abschließend soll die Betriebszentrale (Server Level 4a und Workstations Level 4b) später auch durch AF ICS standardisiert werden.

Bei Abbildung D-1 soll die operative Architektur (gelber Abschnitt), die spezielle „Standard IT“ und „Nicht-Standard IT“ Komponenten sowie Systeme ausschließlich und einzig für die Durchführung und Wartung des Kontrollsystems enthält, im Verlauf der RMF Vorgänge laut AF ICS PIT SCA NUR BEWERTET werden. Jedoch wird die Platform Enclave (blauer Abschnitt), die Komponenten, Untersysteme und Systeme der AF-Enterprise IT beinhaltet, von AFCYBER geregelt und ist als Teil des AF Netzwerkes vorhanden. Daher sind Kontrollsysteme, die entweder mit dem AF-Netzwerk zusammengeführt werden oder dessen grundlegende IT Infrastruktur für inaktive oder durchlaufende Daten nutzen, durch den AF ICS PIT AO zu bewerten und die Nutzung der vollständigen RMF Vorgänge für die Platform Enclave zu autorisieren.

Diese Seite wurde absichtlich freigelassen.

ANHANG E: 5-STUFIGER AUFBAU DES KONTROLLSYSTEMS

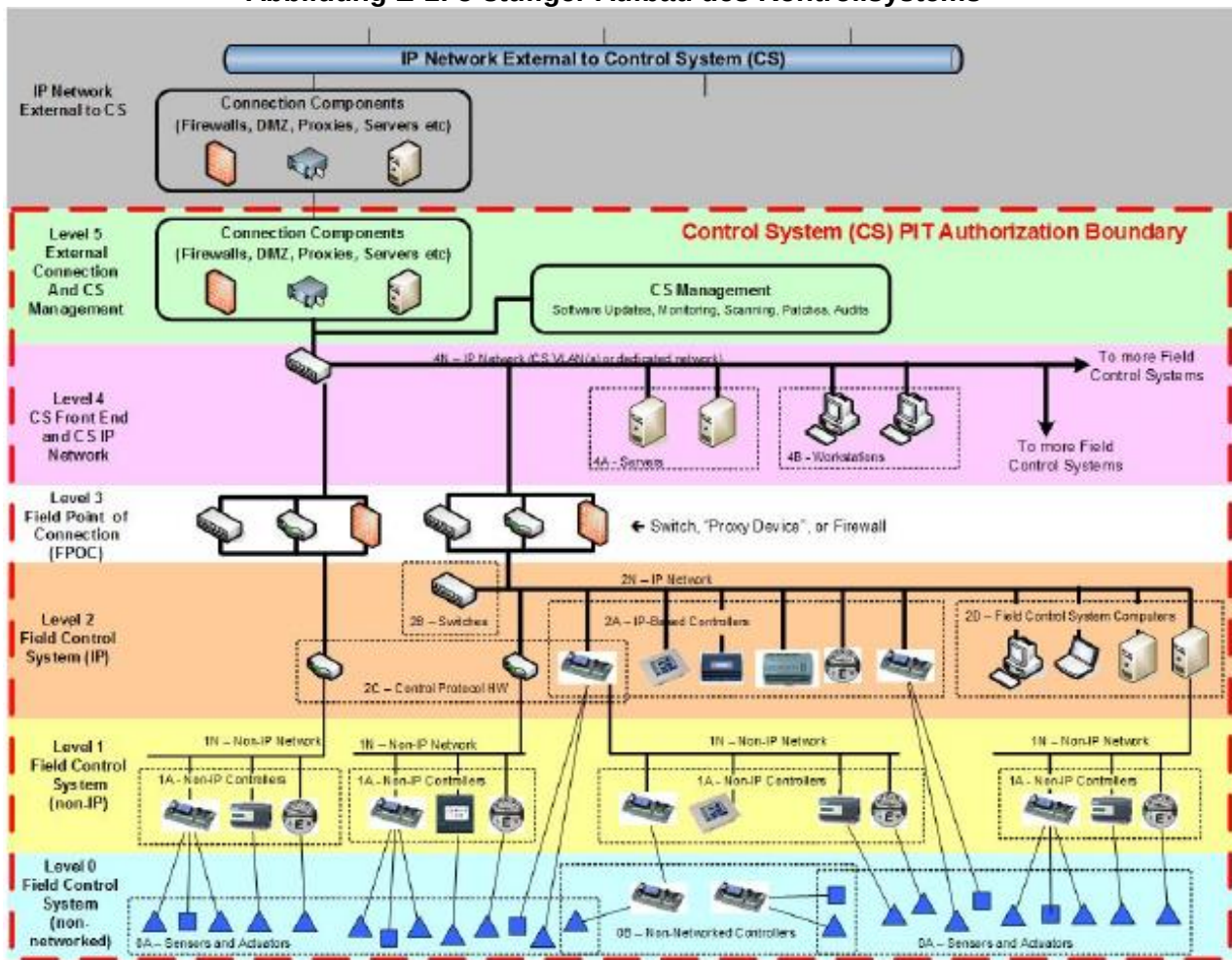
E-1 EINLEITUNG

Wie in Abbildung E-1 aufgezeigt, werden die Kontrollsysteme als 5-stufige Struktur abgebildet, wobei jeder Level für eine Sammlung von Komponenten steht, die logisch nach Funktion gruppiert sind und die allgemein eine gemeinsame Strategie bezüglich Cyber-Sicherheit haben. Diese Struktur ist als allgemeine Struktur festgelegt, die für eine Vielzahl von Kontrollsystemen geeignet ist; somit gibt es einige Hauptgesichtspunkte, wenn diese zur Beschreibung eines bestimmten Kontrollsystems verwendet wird.

- Nicht jede Umsetzung eines Kontrollsystems wird jeden Level nutzen, oder jede Art von Komponente, die auf einem Level angegeben ist.
- Dasselbe Gerät kann sich auf verschiedenen Levels befinden, abhängig von seiner Konfiguration. Beispielsweise können einige Controller aufgrund eingebauter Switches verschiedene Netzwerke versorgen, und daher könnte sich dasselbe Gerät sowohl auf Level 1 als auch auf Level 2 befinden.
- In vielen Fällen kann ein Gerät in mehreren Unterebenen innerhalb derselben Hauptebene, meist innerhalb von Level 2, eingesetzt werden. Beispielsweise kann ein Level 2A Controller als Level 2C Router zu einem Netzwerk auf dem darunter liegenden Level 1 fungieren.

Dieser Anhang beschreibt den 5-stufigen Aufbau für Kontrollsysteme und zeigt für jeden Level Aspekte der Cyber-Sicherheit auf. Hinweis: Obgleich in der Struktur in Abbildung E-1 tatsächlich mehr als fünf Levels dargestellt sind, wird dies allgemein als „5-stufige Struktur des Kontrollsystems“ bezeichnet. Diese Struktur gilt für alle Arten von Kontrollsystemen; obgleich viele der als Beispiel aufgeführten Komponenten oder Technologien, die in diesem Anhang aufgezeigt sind, auf Gebäude- bzw. Versorgungstechnik basieren, soll dies nicht bedeuten, dass diese Struktur spezifisch für diese Arten von Kontrollsystemen ist.

Abbildung E-1: 5-stufiger Aufbau des Kontrollsystems



E-2 5-STUFIGER AUFBAU - ÜBERSICHT

Hier eine kurze Beschreibung der einzelnen Level (von einfachen bis zu komplexen Geräten):

- Level 0. Nicht vernetzte Geräte, die anhand analoger Signale kommunizieren. Diese beinhalten („nicht intelligente“) Sensoren und Ansteuerungen sowie nicht vernetzte Controller (einschließlich ihrer fest zugeordneten Sensoren und Aktoren). Diese kommunizieren mit Level 1 über Hardware Ein- und Ausgänge (analoge und binäre Signale).
- Level 1. Vernetzte Controller, nicht auf einem IP-Netzwerk (z.B. BACnet MS/TP, RS-485 (z.B. DNP, Modbus), LonWorks TP/FT-10).
- Level 2. Vernetzte Controller auf einem IP-Netzwerk.
- Level 3. Der „Field Point of Connection“ (FPOC) der eine Verbindung zwischen dem Field Control System des IP-Netzwerks auf Level 2 und dem IP Netzwerk auf Level 4 darstellt.

- Level 4. Das standortweite IP-Netzwerk, das für das Kontrollsystem genutzt wird, zusammen mit Frontend-Servern und Arbeitsplatzgeräten (Desktops und Laptops).
- Level 5. Schnittstellen zu „externen“ Netzwerken (IP-Netzwerke außer dem Kontrollsystem-Netzwerk).

Bitte beachten Sie, dass einige Levels Unterebenen enthalten, wie in Abbildung E-1 angegeben.

E-3 LEVEL 0: SENSOREN UND AKTOREN

Level 0 besteht aus nicht-vernetzten Geräten, die mittels analoger Signale kommunizieren. Diese beinhalten („nicht intelligente“) Sensoren und Aktoren sowie nicht vernetzte Controller. Diese kommunizieren mit Level 1 oder Level 2 über Hardware Ein- und Ausgänge (analoge und binäre Signale). Angaben über Level 0 finden Sie in Tabelle E-1.

Tabelle E-1: Level 0

LEVEL 0: Sensoren und Aktoren	
Definition	Level 0 Geräte haben kein Netzwerk und können daher nicht über ein Netzwerk angegriffen werden. Level 0 Geräte nutzen - falls sie überhaupt kommunizieren - nur einfache analoge und binäre Signale, sie nutzen keine Form digitaler Protokolle zur Kommunikation. Ein Sensor oder Aktor, der ein Kommunikationsprotokoll nutzt (z.B. Zigbee, Bluetooth) ist ein Gerät mit Level 1 (nicht IP) bzw. Level 2 (IP).
Funktionsbeschreibung	Die Schnittstelle zwischen dem Kontrollsystem und dem zugrunde liegenden geführten Prozess / Gerät, wo elektrische Signale im Kontrollsystem zu/von physikalischen Größen und Funktionen in das zugrunde liegende kontrollierte System umgewandelt werden. Level 0A besteht aus Sensoren und Aktoren Level 0B besteht aus nicht vernetzten Controllern und deren eingebauten Sensoren und Aktoren. Level 0B Geräte können eine gewisse Intelligenz besitzen und sogar ein internes Netzwerk, durch das Gerät kommt jedoch kein internes Netzwerk mit anderen Geräten in Kontakt. Diese Geräte sind normalerweise Verpackungseinheiten mit integrierten werksseitig installierten Controllern. Hinweis: Ein „eigenständiges“ mehrteiliges Gerät mit mehreren, vor Ort eingebauten Controllern, die über ein Netzwerk kommunizieren, das spezifisch für dieses Gerät ist, stellt KEINE Level 0 Komponente dar, sondern ein eigenständiges, eigenes Field Control System .

LEVEL 0: Sensoren und Aktoren	
Umgesetzt mittels	Geräten, die: • Physische Eigenschaften (z.B. Temperatur, Druck, etc.) in ein binäres oder analoges elektrisches Signal umwandeln. • Anhand eines binären oder analogen elektrischen Signals eine physische Bewegung (z.B. Öffnen / Schließen eines Ventils oder Klappe, etc.) erzeugen. Diese elektrischen Signale sind rein binär oder analog - es gibt keine exponierten digitalen Signale oder Netzwerke auf diesem Level. Beachten Sie ebenfalls, dass „intelligente“ Sensoren oder „intelligente“ Aktoren, die einen Controller und Netzwerkverbindung beinhalten, als Level 1 oder Level 2 Geräte betrachtet werden.
Installiert von	AN Kontrollen während der Installation oder Erneuerung des zugrunde liegenden mechanischen oder elektrischen Systems.
Beispiel-Komponenten	Die große Mehrheit dieser Geräte besteht aus sehr einfachen („nicht intelligenten“) Sensoren oder Aktoren, komplexere Geräte können sich jedoch auf Level 0 befinden - solange die Netzwerkanbindung fehlt. Einige Beispiele sind: • Ein Thermistor Temperaturfühler, der nur eine Widerstandsänderung als Temperaturanzeige liefert, ist ein Level 0A Gerät. • Ein elektrischer Aktor der mit einem 4-20 mA Signal eine proportionale physische Reaktion erzeugt, ist ein Level 0A Gerät. • Ein Präsenzmelder, der mittels BACnet Präsenzwerte übermittelt, ist ein Level 1 (oder Level 2) Gerät und kein Level 0 Gerät. • Ein variabler Frequenzantrieb, der einen Klimagerätventilator steuert und nur binäre und analoge Signale nutzt, um mit dem Controller des Klimagerätes zu kommunizieren, ist ein Level 0B Gerät. • Ein Vorlauffühler, der HART über eine analoge Leitung nutzt, verwendet ein digitales Protokoll (HART) und ist ein Level 1 Gerät, kein Level 0 Gerät. • Ein verpackter Dieselmotor, der in einer eigenständigen Konfiguration betrieben wird - nochmals, ohne Netzwerkanbindung an andere Geräte - ist ein Level 0B Gerät. Die letzten zwei Beispiele veranschaulichen, dass das bestimmende Merkmal für Level 0 nicht die Komplexität des Geräts ist, sondern ob das Gerät mit anderen Geräten über ein Netzwerk kommuniziert.

LEVEL 0: Sensoren und Aktoren	
Überlegungen zur Sicherheitskontrolle	Allgemein können Führungs- und Ablaufkontrolle wie beispielsweise physische Sicherheit und Zugangskontrolle noch für diesen Level Anwendung finden. Diese Geräte sind physisch an dem mechanischen/elektrischen System angeschlossen und physische Sicherheit wird aufgrund des physischen Zugangs zu den Geräten vorgegeben und umgesetzt. Medienschächte, Haustechnik-, Elektro- Sanitäräume, Pumpenstationen usw. sollten gesichert sein und nur autorisiertes Personal sollte Zugang haben. Diese Geräte, obwohl ohne Netzwerkverbindung, können physischen Schaden verursachen, zum Beispiel ein Ventil, das in Stellung „Offen“ gelassen wird.

E-4 **LEVEL 1: FIELD CONTROL SYSTEM (NICHT IP)**

Level 1 enthält vernetzte Controller, die sich nicht auf einem IP-Netzwerk (z.B. BACnet MS/TP, RS-485 (z.B. DNP, Modbus), LonWorks TP/FT-10) befinden. Angaben über Level 1 finden Sie in Tabelle E-2.

Tabelle E-2: Level 1

LEVEL 1: Field Control System (nicht-IP)	
Definition	Der Teil des Kontrollnetzes, der das IP-Protokoll nicht verwendet. Dies beinhaltet sowohl die Controller selbst (Level 1A) als auch das Netz (Level 1N).
Funktionsbeschreibung	(Level 1A) Hier befindet sich die Steuerungslogik und wird in oder von binären und analogen elektrischen Signalen umgewandelt, sowie der Teil des Kontrollsystems, wo: • Analoge und binäre Signale (von Sensoren) über analog-zu-digital (A-D)-Wandlern zu digitalen Signalen umgewandelt werden. • Digitale Information in analoge und binäre elektrische Signale (zu Aktoren) über digital-zu-analog (D-A)-Wandlern umgewandelt wird. • Digitale Informationen über ein Netzwerk übertragen und empfangen werden. • Digitale Informationen nach einer benutzerdefinierten Abfolge verarbeitet werden, um neue digitale Informationen zu erzeugen. • Geräte integrale Level 0 Sensoren und Aktoren enthalten können, zum Beispiel können viele variable Volumenstromregler (VVS-Regler) einen elektrischen Aktor enthalten.

LEVEL 1: Field Control System (nicht-IP)	
	Nicht alle Controller werden Hardware-Eingänge haben. Obgleich ein Datenaustausch über das Netzwerk besteht, erfordert eine gute Planung, dass der Großteil der Datenverarbeitung mittels Nutzung von lokalen Sensordaten und lokalen Aktorenausgaben stattfindet; das System ist geplant, um die Abhängigkeit von vernetzten Daten zu minimieren. (Level 1N) Das Level 1 Netz (Medien und Hardware) nutzt kein IP. Es nutzt eine Vielzahl Medien auf Ebenen 1 und 2 (einige sind Standard, andere nicht) und nutzt Ebene 3 Protokolle außer IP. Einige Beispiele sind: • BACnet über MS/TP, oder BACnet über ARCnet • LonTalk über TP/FT-10 oder LonTalk über TP/XF-1250 • Modbus über RS-485 Aus diesem Grund ist dies allgemein sehr spezifisch für die Kontrollanwendung und kann nicht für „Standard“ IT-Protokolle und Anwendungen genutzt werden.
Umgesetzt mittels	(Level 1A) Controller, normalerweise mit mehrfachen analogen und binären Ein- und Ausgänge ausgestattet und entsprechenden A-D und D-A Wandlern. Aus Kostengründen haben diese Geräte die minimale Funktionalität für die Anwendung und sind in Bezug auf Arbeitsspeicher (RAM), Rechenleistung und Netzwerk-Ein-/ Ausgänge (E/A) sehr eingeschränkt. Zudem gibt es diese Geräte in einer großen Vielfalt von Bauarten, Prozessoren, Anbietern und Firmware. (Level 1N) Netzwerk-Medien und Hardware sind in ähnlicher Weise diesem spezifischen Steuerprotokoll zugeordnet und werden von vielen Anbietern hergestellt.
Installiert von	AN Kontrollen während der Installation oder Erneuerung des zugrunde liegenden mechanischen oder elektrischen Systems. Im allgemeinen bei Neubauten und größeren Renovierungen.
Beispiel-Komponenten	VVS Regler Vernetzter (nicht IP) Stromzähler Intelligente (vernetzte) Temperaturregler LonWorks TP/XF-1250 (Medien) zu TP/FT-10 (Medien) Router. (Dies ist kein IP-Router, sondern er sendet das Kontrollsystem-Kommunikationsprotokoll bei Open Systems Verbindungen Ebene 3.)
Überlegungen zur Sicherheitskontrolle	Da Geräte (Controller) auf dieser Ebene meist einfachere Geräte sind, können häufig nur wenig Sicherheitskontrollen angewendet werden, besonders nachdem das System geplant und installiert wurde.

LEVEL 1: Field Control System (nicht-IP)	
	Einige grundlegende Kontrollen/Maßnahmen, die auf dieser Ebene angewendet werden können, umfassen: • das Blockieren (oder zumindest unterbinden) von sekundären Netzwerkverbindungen (Verbindungen außer zum Level 1 Netzwerk) • Die Verwendung von Passwörtern bei Geräten wie z.B. Displays (bis zu den vom Gerät unterstützten Möglichkeiten - von denen viele z.B. keine Passwörter mit 14 Zeichen erlauben) • Den Einsatz physischer Sicherheitsmaßnahmen - die durch die zugrundeliegenden Geräte vorgeschrieben und durchgeführt werden

E-5 LEVEL 2: FIELD CONTROL SYSTEM (IP)

Level 2 besteht aus vernetzten Controllern auf einem IP-Netzwerk. Angaben über Level 2 finden Sie in Tabelle E-3.

Tabelle E-3: Level 2

LEVEL 2: Field Control System (IP)		
Definition		Der Teil des Kontrollsystems, Der IP nutzt, der jedoch nicht gemeinsam mit einem anderen System genutzt wird. In diesem Zusammenhang bezieht sich „gemeinsam nutzen“ vorwiegend auf physische Geräte und Medien.
Funktionsbeschreibung	2 A	Auf diesem Level (zusammen mit Level 1) befindet sich die Steuerlogik und wird hier zu/und von elektrischen Signalen umgewandelt und kann die ersten IP-Verbindungen besitzen. Dies ist der Teil des Kontrollsystems, wo: • analoge und binäre elektrische Signale (von Sensoren) mittels A-D-Wandlern in digitale Signale umgewandelt werden (obgleich nicht alle Controller Hardware-Eingänge besitzen werden). • Digitale Informationen über D-A-Wandler in analoge und binäre elektrische Signale (zu Aktoren) umgewandelt werden. • Digitale Informationen über ein Netzwerk übertragen und empfangen werden.

LEVEL 2: Field Control System (IP)		
		• Digitale Informationen nach einer benutzerdefinierten Abfolge verarbeitet werden, um neue digitale Informationen zu erzeugen. • Diese Geräte können integrale Level 0 Sensoren und Aktoren aufnehmen, beispielsweise können viele variable Volumenstromregler (VVS-Regler) einen elektrischen Aktor aufnehmen.
	2N/2B	Das IP-Netzwerk (Medien und Hardware), welches dem Kontrollnetzwerk zugeordnet ist und das Kontrollprotokoll überträgt (z. B. Distributed Network Protocol (DNP), IEC-61850, BACnet/IP oder Lon/IP). In der Regel IP über Ethernet.
	2C	Kontrollprotokoll-Router und Gateways. Kontrollprotokoll-Router senden das Kontrollprotokoll - d.h. Sie übermitteln selektiv Kontrollprotokoll-Pakete auf Grundlage der Zieladresse. Sie sind keine IP-Router. Kontrollprotokoll-Gateways wandeln Kontrollprotokolle untereinander um.
	2D	Wo für das lokale Kontrollsystem eine erhöhte C-I-A Anforderung besteht, eine Anforderung an Ausfallsicherheit, eine Betreiber-Ansprechzeit oder eine Anforderung für lokale Betreiber, die nicht durch das standortweite Remote Frontend erfüllt werden kann, kann das Anlagenkontrollsystem eine lokale Bedienoberfläche enthalten, die der ähnelt, die normalerweise auf Level 4 zu finden ist, jedoch diesem spezifischen Kontrollsystem zugeordnet ist. In anderen Fällen, bei Altsystemen oder autarken Systemen (nicht zwingend abgeschlossenen Systemen, sondern autarke, wobei diese nicht von einem anderen System abhängig sind, wie beispielsweise einem Kontrollsystem), kann die Frontend Bedienoberfläche zu diesem System physisch dezentral sein. In diesem Fall wird die Bedienoberfläche als Teil von Level 2 angesehen, da sie diesem Gebäude oder dieser Einrichtung fest zugeordnet ist und der Verkehr zwischen dieser und den Geräten der Level 1 und Level 2 nicht über den FPOC der Level 3 läuft.
Umgesetzt mittels	2 A	Controller, normalerweise mit mehrfachen analogen Ein- und Ausgängen und entsprechenden A-D und D-A Wandlern ausgestattet. Diese Geräte müssen aus Kostengründen die minimale Funktionalität für die Anwendung haben und sind sehr eingeschränkt in Bezug auf RAM, Rechenleistung, und Netzwerk-Ein-/Ausgängen. Zudem gibt es diese Geräte in einer großen Vielfalt von Bauarten, Prozessoren, Anbietern und Firmware.

LEVEL 2: Field Control System (IP)		
		Außer der Tatsache, dass diese IP nutzen und im Allgemeinen leistungsfähiger als Level 1A Geräten sind, sind sie ansonsten mit den Level 1A Geräten identisch. Es gibt viele Geräte sowohl als Level 1A oder 2A Geräte, wo die Hardware mit Ausnahme des Sendempfangsgeräts identisch ist, einige von ihnen können sogar auf die eine oder andere Art Feld-konfiguriert werden.
	2N/2B	Das Level 2N Netzwerk ist allgemein Ethernet und die Netzwerk-Hardware auf Level 2B besteht aus Standard IT Netzwerk Hardware, obgleich zum Teil mit funktionaler Einschränkung. Es darf beispielsweise keine Anforderung bezüglich Remote verwalteten Netzwerkschwitches bestehen. Ebenso ist nur selten ein IP-Router nötig, da sich Field Control Systeme im allgemeinen innerhalb eines einzelnen (privaten) IP-Subnetzes befinden.
	2C	Controller, die den Hardware-Merkmalen von Level 2A Geräten sehr ähneln, außer dass diese Geräte normalerweise mehrere Netzwerkschnittstellen besitzen.
	2D	Computer (wie für Level 4) Computer für Altsysteme Benutzerdefinierte oder modifizierte Computer mit einer Touchscreen-Oberfläche.
Installiert von		AN Kontrollen während der Installation oder Erneuerung des zugrunde liegenden mechanischen oder elektrischen Systems. Im allgemeinen bei Neubauten und größeren Renovierungen
Beispiel-Komponenten	2 A	Controller für das Klimagerät Controller für den Kälteerzeuger Controller für den Heizungskessel Controller für ein Endgerät Controller für die Warmwasseranlage Überwachungscontroller Steuerprogramm des Systems Stromzähler Lokale Anzeigentableaus Elektrisches Schutzrelais

LEVEL 2: Field Control System (IP)		
		Controller für Spannungsregler
	2 B	Ethernet Switch
	2C	BACnet MS/TP zu BACnet/IP Router LonWorks TP/FT-10 zu LonWorks IP Router
	2D	Kontrollsystem an einer zentralen Anlage, wo Art und Kritikalität der Anlage eine lokale Betreiberschnittstelle erfordern.
Überlegungen zur Sicherheitskontrolle	2 A	Controller, die sich auf dem spezifischen IP-Netzwerk befinden, unterscheiden sich in hohem Maße von Geräten, die sich auf einem typischen IP-Netzwerk befinden. • Sie nutzen ein einzelnes festes Protokoll (oder eine kleine Anzahl fester Protokolle) • Häufig unterstützten sie keine „Log in“ Funktionalität • Es gibt häufig keine „Sitzungs-“Fähigkeit • Normalerweise besitzen sie keine Benutzeroberfläche, falls dies doch der Fall ist, ist diese allgemein äußerst begrenzt. • Sie haben sehr begrenzte Hardware-Fähigkeiten (RAM, CPU, Speicher, etc.) • Sie nutzen in der Regel nicht Windows, und selten Linux. Sie sind in der Regel eine Variante eines Echtzeitbetriebssystems (RTOS). Viele Controller haben dieselben Einschränkungen wie die Controller auf Level 1, wo die meisten Sicherheitskontrollen nicht zutreffen können/werden. Einige Controller besitzen jedoch deutlich mehr Leistungsvermögen, und zusätzliche Kontrollen sind angebracht. In jedem Fall sollten die Controller alle Netzwerkverbindungen oder Dienste blockieren, die nicht für den Betrieb des Kontrollsystems erforderlich sind.
	2N/2B	Dieses Netzwerk ist dem Kontrollsystem zugeordnet und wird im Allgemeinen vom AN Kontrollsystem installiert, nicht der IT-Organisation. Dadurch wird die Notwendigkeit, das Netzwerk zu sichern, nicht verringert, sondern es hat Auswirkungen auf die Art, wie das Netzwerk gesichert wird, und die Risiken und Schwachstellen, die anzugehen sind. Einige Hauptunterscheidungsmerkmale zwischen einem Level 2 Netzwerk und einem Standard-IP Netzwerk sind: • Netzwerkstruktur und angeschlossene Geräte bleiben über die gesamte Lebensdauer des Systems eher statisch.

LEVEL 2: Field Control System (IP)		
		Im Allgemeinen werden Komponenten nicht regelmäßig hinzugefügt und entfernt. • Das/die verwendete(n) Protokoll(e) sind feststehend, und in vielen Fällen wird nur ein einziges Protokoll verwendet. Die Protokolle unterscheiden sich von „normalen“ IP-Netzwerken dadurch, dass sie eher Kontrollsystemprotokolle anstelle von Standard-IT-Protokollen sind. • Die Bandbreitennutzung ist geringer. Da die Netzwerkkonfiguration statischer ist, ist auch die Bandbreitennutzung konstanter. • Die Geräte, die sich auf dem Netzwerk befinden, besitzen weniger Leistungsvermögen und unterstützen im Allgemeinen keine Netzwerk-Sicherheitsstandards wie beispielsweise IEEE 802.1X. • Das Kontrollsystem erfordert nicht das Funktionalitätsniveau, das Netzinfrastruktur-Geräte der Liste zugelassener Produkte (APL) bieten. Die Navy benötigt jedoch für alle IP-Netzwerk Hardware APL-Produkte. • Standard-IT-Geräte entsprechen normalerweise nicht den Anforderungen der UL Liste für Brandschutz- und Personenschutzsysteme, sodass spezielle Netzwerkhardware erforderlich sein könnte, um den Anforderungen des Kontrollsystems zu entsprechen.
	2C	Diese Geräte werden nicht von herkömmlichen IT-Firmen hergestellt und laufen nicht über Standard-IT Software. Ihre Funktionalität ist häufig als Teil eines Level 2A Gerätes enthalten. Kein IP-Routing.
	2D	Während Level 2D Komponenten in Bezug auf Funktionalität den Computern auf Level 4 ähneln, bedeutet die Tatsache, dass sie dezentral zu (und fest zugeordnet zu) einem speziellen Kontrollsystem sind, von der Perspektive der Sicherheitskontrollen, dass es besser wäre, sie als Level 2 Komponente zu behandeln. Es gibt zwei Hauptgründe für Computer auf Level 2D: • Altsysteme, die nicht gepatched werden können. Es ist möglich, dass die Computer auf Level 2D ein älteres Betriebssystem verwenden und einige Sicherheitskontrollen nicht unterstützen. In diesem Fall sollten die Kontrollen, die ohne einen negativen Einfluss auf die Systemverfügbarkeit angewendet werden können, tatsächlich angewendet werden, und, falls ansonsten erforderlich, sollten schadensbegrenzende Kontrollen und Maßnahmen ergriffen werden.

LEVEL 2: Field Control System (IP)		
		Systeme, die diese Computer beinhalten, sollten nicht mit anderen Systemen verbunden sein (d.h. sollten eigenständig betrieben werden, bis sie richtig behandelt werden können, wobei die Computer ausgetauscht oder ansonsten auf die Standards von Level 4 aufgerüstet werden. • Wo für ein neues System ein dezentrales Frontend erforderlich ist, das, aus welchem Grund auch immer, nicht auf dem IP-Netzwerk (Level 4) installiert werden kann, das überall im Standort gemeinsam genutzt wird. Dies ist normalerweise aufgrund einer C-I-A Anforderung erforderlich. Wenn ein neues System mit einem Level 2 Frontend installiert wird, ist es wichtig, darauf zu achten, dass das Level 2 Frontend denselben Kontrollen unterliegt wie ein Level 4 Frontend. Während sich Umsetzung und Übernahme der Sicherheitskontrollen auf diesem Level vom Level 4 Frontend unterscheiden können, sollten Computer auf diesem Level denselben Kontrollen unterliegen wie ein „normales“ Level 4 Frontend von gleicher Kritikalität.

E-6 LEVEL 3: FIELD POINT OF CONNECTION (FPOC)

Level 3 enthält den „Field Point of Connection“ (FPOC), der eine logische Verbindung zwischen dem Field Control System des IP-Netzwerks auf Level 2 und dem IP Netzwerk auf Level 4 darstellt. Angaben über Level 3 finden Sie in Tabelle E-4.

Tabelle E-4: Level 3

LEVEL 3: Field Point of Connection (FPOC)	
Definition	Das Gerät, das das spezifische Level 2 IP-Netzwerk mit dem IP-Netzwerk auf Level 4 verbindet.
Funktionsbeschreibung	Bei jedem Field Control System ist der FPOC der spezielle einzelne Demarkationspunkt im Kontrollsystem zwischen diesem Field Control System und dem Frontend-System. Der FPOC ist ein Standard-IT-Gerät, normalerweise ein Ethernet Switch. Für den FPOC bestehen allgemein Sicherheitskontrollen, wobei der Zugang (durch Benutzer, Protokoll oder speziellen Befehlen) zwischen den Levels darüber und darunter beschränkt wird. Bitte beachten Sie, dass ein großes System hunderte dieser FPOC Geräte besitzt, eines an jeder Verbindung eines Field Control Systems zu einem lokalen Netzwerk.

LEVEL 3: Field Point of Connection (FPOC)	
Umgesetzt mittels	Fast immer ein Ethernet Switch oder IP Router
Installiert von	Im Allgemeinen vom für das Netzwerk des Standorts zuständigen Personals installiert oder von dem AN Kontrollsysteme unter Aufsicht durch das Netzwerk-Personal.
Beispiel-Komponenten	Standard IT-verwalteter Ethernet Switch oder IP Router
Überlegungen zur Sicherheitskontrolle	Dieses Gerät ist aus der Sicht der Sicherheitskontrollen von entscheidender Bedeutung, da es sich dort befindet, wo das lokale Field Control Network an das standortweite IP-Netzwerk anschließt. Normalerweise wird durch die Absicherung dieses Gerätes das standortweite Netzwerk von den lokalen Feldsystemen (die häufig den Anforderungen der Sicherheitskontrollen nur schwer nachkommen) geschützt. Gelegentlich, wenn es ein kritisches Field Control System gibt, kann dieses Gerät das kritischere Field Control System von weniger sicheren lokalen Systemen schützen (z.B. wenn es 99 unkritische Systeme gibt und 1 kritisches, ist es besser, das 1 von den 99 abzutrennen als zu versuchen, die 99 abzusichern). In der Tat sollte dieses Gerät eine „alle verweigern / Genehmigung im Ausnahmefall“ Strategie anwenden. Der FPOC sollte mit dem restriktivsten möglich Satz von Zugangskontrolllisten (ACL) angelegt werden.

E-7 LEVEL 4: FRONTEND KONTROLLSYSTEM UND IP-NETZWERK KONTROLL-SYSTEM

Level 4 besteht aus dem standortweiten IP-Netzwerk, das für das Kontrollsystem genutzt wird, zusammen mit Frontend-Servern und Arbeitsplatzgeräten (Desktops und Laptops). Angaben über Level 4 finden Sie in Tabelle E-5.

Tabelle E-5: Level 4

LEVEL 4: Frontend Kontrollsystem und IP-Netzwerk Kontrollsystem	
Definition	Frontend Computer und das IP-Netzwerk, das mehrere FCS verbindet und nicht einem speziellen FCS zugeordnet ist. Das IP-Netzwerk kann ein fest zugeordnetes physisches Netzwerk sein, oder ein virtuelles Local Area Network (VLAN), oder ein virtuelles Private Network (VPN), das auf einem anderen Netzwerk läuft.
Funktionsbeschreibung	Level 4A und 4B) Mehrfach-Anlagen Betreiber-Schnittstelle für das System. Dies ist normalerweise ein webbasiertes Client-Server-System mit Servern (Level 4A), die mit herstellerspezifischer Software auf Standard Server PCS laufen und den Clients (Level 4B), die auf die Server mittels Standard Web-Browser Software zugreifen. Einige Aufgaben des Kontrollsystems sind:

LEVEL 4: Frontend Kontrollsystem und IP-Netzwerk Kontrollsystem	
	• grafische Bildschirme zur Überwachung und Kontrolle des Systems zur Verfügung stellen • Betreibern zu ermöglichen, Systeme zu planen, historische Tendenzen zu erstellen und auf Alarmzustände zu reagieren. • für globale Kontroll- und Optimierungsstrategien, deren Umsetzung innerhalb des Kontrollsystems nicht zweckmäßig ist, zu sorgen und diese zu fördern. • Durchführung analytischer Auswertungen und Ergreifen entsprechende Echtzeit-Maßnahmen. Dieser Level nutzt auch Engineering Tool Software, die Mittel zur Erstellung und Modifizierung des Kontrollsystems liefert. Das Level 4N Netzwerk ist das Netzwerk, das Netzwerke zahlreicher Einrichtungen in ein gemeinsames standortweites Netzwerk zusammenfügt.
Umgesetzt mittels	Entweder ein fest zugeordnetes physisches Netzwerk, oder ein virtuelles Local Area Network (VLAN) oder ein virtuelles Private Network (VPN) m das auf einem weiteren Netzwerk läuft, oder eine Kombination dieser Möglichkeiten. PCs, Server und Netzwerkgeräte
Installiert von	Normalerweise wird das Netzwerk (Level 4N) bauseits gestellt. Die Computer (Servers und Arbeitsplatzrechner auf Level 4A und 4B) werden häufig bauseits gestellt. Die Softwareanwendung wird normalerweise vom Anbieter der Steuerungen geliefert, installiert und konfiguriert.
Beispiel-Komponenten	Server und Datenschränke, Computer, Laptops, Betreiberschnittstellen und Netzwerkgeräte Wahrscheinlich werden die Kontrollsystem-Datenschränke, Hardware und Software in einer Energiebetriebszentrale, anlagenweiten Betriebszentrale, Anlagenbetriebszentrale, Anlagen- und Energiebetriebszentrale, Betriebszentrale EDV-Sicherheit oder regionalen Betriebszentrale aufgestellt.
Überlegungen zur Sicherheitskontrolle	Auf Level 4 ähneln die Kontrollsysteme einem „Standard“ Informationssystem am meisten, und die meisten Sicherheitskontrollen können auf diesem Level angewendet werden. Es ist unbedingt zu beachten, dass ein Kontrollsystem KEIN Standard-Informationssystem ist, dass Kontrollen jedoch so angewendet werden müssen, dass diese nicht die Verfügbarkeit des Systems beeinträchtigen.

LEVEL 4: Frontend Kontrollsystem und IP-Netzwerk Kontrollsystem	
	Beispielsweise sind für einige Kontrollsysteme Softwareupdates des Herstellers vor der Anwendung eines Java Patches erforderlich, und Kontrollen, die sich auf die Anwendung von Patches beziehen, dürfen nicht so implementiert werden, dass automatisches oder sofortiges Patchen erforderlich ist, ohne sicherzustellen, dass dies nicht dazu führen könnte, dass das System offline geht. Im Gegensatz zu Standard IT-Anwendungen (wie Virus-Software oder Büroautomationstools), sind diese PIT-Anwendungen im Allgemeinen ein Nischenprodukt und während die Standardanleitung einige Aspekte der Absicherung dieser Anwendung abdeckt, wird dies wahrscheinlich nicht ausreichen, um diese komplett abzusichern.

E-8 LEVEL 5: EXTERNE VERBINDUNG UND KONTROLLSYSTEM-MANAGEMENT

Level 5 enthält Schnittstellen zu „externen“ Netzwerken (IP-Netzwerke außer dem Kontrollsystem-Netzwerk). Angaben über Level 5 finden Sie in Tabelle E-6.

Tabelle E-6: Level 5

LEVEL 5: Externe Verbindung und Kontrollsystem-Management	
Definition	Zusätzliche Hardware, Software oder Vernetzungen, die zur Verwaltung des Kontrollsystems, Erstellung von Sicherheitsfunktionalität, Benutzerverwaltung und für externen Zugriff genutzt werden. Dies sind IT-Management und IT-Sicherheitsfunktionen und diese bieten keine Kontrollsystem-Funktionalität.
Funktionsbeschreibung	In vielen Architekturen stellt dieser Level die Absicherung der Außengrenze der Enclave zwischen dem Kontrollsystem (auf Level 4 und darunter) und IP Netzwerken, die außerhalb des Kontrollsystems liegen. (In anderen Architekturen erfolgt die Grenzsicherung im externen Netzwerk). In vielen Fällen gibt es eine Komponente innerhalb des Kontrollsystems, die sich auf Level 5 befinden würde. Dieser Level kann aus einer Vielzahl von Gründen fehlen - vielleicht besteht keine externe Verbindung, oder die Verbindung kann über das externe Netzwerk erfolgen. Zusätzliche Funktionsweisen, die durch externe Verbindungen ermöglicht werden, können folgendes beinhalten: • Senden von Alarmmeldungen mittels abgehenden Zugriff auf einen SMTP E-Mail-Server.

LEVEL 5: Externe Verbindung und Kontrollsystem-Management	
	Hochladen historischer Daten und Zählerdaten auf einen Enterprise-Server mittels abgehendem HTTP/HTTPS Zugriff zum Hochladen. In einigen Fällen kann eingehendes HTTP von Web-Clients auf dem externen Netzwerk zum Level 4A Server möglich sein, dies ist jedoch nicht erforderlich und häufig aus Sicherheitsgründen untersagt. Die Navy verbietet diese Funktionsweise.
Umgesetzt mittels	Firewalls DMZ/Perimeter Networking Proxy Server Domain Controller, etc.
Installiert von	IT- und Kommunikationspersonal und AN
Beispiel-Komponenten	Wide Area Networks Metropolitan Area Networks Local Area Networks Campus Area Networks Virtuelle Private Netzwerke Point of Presence Demarcation Point oder Main Point of Presence
Überlegungen zur Sicherheitskontrolle	Im Allgemeinen, wenn das Kontrollsystem in einer völlig isolierten Konfiguration funktionieren kann, sollte es das tun, und es sollte keine externe Verbindung geben. Dieser Level sollte eine „alle verweigern / Genehmigung im Ausnahmefall“ Strategie umsetzen, um das Kontrollsystem vor dem externen Netzwerk und das externe Netzwerk vor dem Kontrollsystem zu schützen.

ANHANG F: CYBER-SICHERHEIT – ÜBERLEGUNGEN ZUR EINBINDUNG KRITISCHER SYSTEME DER GEBÄUDELEITTECHNIK UND VERSOR- GUNGSTECHNIK IN EIN NICHT KRITISCHES SYSTEM (UMCS)

HINWEIS: Dieser Anhang gilt für die Systeme der Gebäudeleittechnik und Versorgungstechnik. Der Begriff Field Control Systems (FCS) wird in diesem Anhang sowohl für Utility Control Systems (UCS) als auch für Building Control Systems (BCS) verwendet, aber nicht zwangsläufig für andere Field Control Systems (FCS).

F-1 EINLEITUNG

Wenn das Building Control System (BCS) oder das Utility Control System (UCS) vertrauliche Informationen enthält, eine kritische Infrastruktur darstellt oder anderweitig missionskritisch ist oder die Sicherheit betrifft, so ist das Field Control System (FCS) ein kritisches System. Während einige der Anforderungen zum Schutz des FCS durch die aufgelisteten CCIs abgedeckt sind, die für Systeme mit MITTLERER oder HOHER Auswirkung zu berücksichtigen sind, gibt es Belange, die insbesondere die kritischen Systeme einer typischen Liegenschaft betreffen, in der die meisten Systeme nicht kritische Systeme sind.

Es gibt drei Möglichkeiten zur Anbindung eines kritischen Systems (FCS) an ein UMCS:

1. **Gleicher Schutzgrad für UMCS und FCS.** Planerisch gesehen ist dies am einfachsten. Hierzu ist es jedoch erforderlich, dass das UMCS Frontend mit einem höheren Auswirkungsgrad zu berücksichtigen ist und dass alle anderen angebotenen FCS-Systeme, die keinen hohen Auswirkungsgrad haben (und deshalb an ein System mit höherer Auswirkung anbinden), besondere Berücksichtigung finden. In einer typischen Liegenschaft des US-Verteidigungsministeriums gibt es mehr nicht kritische FCS-Systeme als kritische FCS-Systeme, weshalb sich dieser Ansatz häufig als nicht realisierbar erweist, insbesondere dann, wenn ein FCS mit einem geringeren Auswirkungsgrad an ein UMCS Frontend mit höherem Auswirkungsgrad angebunden wird. Die Navy sieht diese Möglichkeit als bevorzugte Lösung an und zeigt einen Lösungsvorschlag auf, wie Systeme mit geringer Auswirkung angebunden werden können, ohne dass für diese ein höherer Auswirkungsgrad zu berücksichtigen ist.
2. **Installieren eines autarken UMCS für das FCS.** In diesem Fall ist das FCS Bestandteil eines dezidierten kritischen UMCS-Systems, das nicht an das liegenschaftsweite UMCS angebunden ist. Bei dieser Variante wird verhindert, dass an ein weniger kritisches System angebunden wird. Dies setzt aber voraus, dass das kritische UMCS mit seinen eigenen dezidierten UMCS-Bedienstellen unabhängig funktioniert. Eine Fernüberwachung des kritischen Systems oder eine Einbindung des kritischen Systems in die liegenschaftsweiten Überwachungsfunktionen ist ebenfalls unmöglich.

In vielen Fällen ist dies jedoch logistisch nicht möglich und muss vor Umsetzung sorgfältig geprüft werden. Das Bedien- und Wartungspersonal der Einrichtung muss gewillt und in der Lage sein, die autarke Einrichtung zu bedienen, damit dies umgesetzt werden kann.

3. **Herstellen einer sicheren Verbindung zwischen einem kritischen FCS und einem nicht kritischen UMCS.** Bei dieser Variante wird das kritische FCS so an das liegenschaftsweite UMCS angebunden, dass der Auswirkungsgrad des UMCS nicht erhöht wird.

Diese Anbindung muss zwar mit größter Sorgfalt geplant werden, kann aber eine zweckmäßigere Lösung für die Anbindung des kritischen FCS darstellen als ein autarkes UMCS zu installieren oder den Auswirkungsgrad des liegenschaftsweiten UMCS zu erhöhen.

Dadurch wird eine sichere Trennung zwischen FCS und UMCS sichergestellt, was auch von der Army bevorzugt wird.

Dieser Anhang enthält Planungsüberlegungen insbesondere zur Anbindung kritischer BCS an nicht kritische UMCS, wie in Variante 3 erläutert. Überlegungen zur Umsetzung von Variante 1 oder 2 werden hier NICHT berücksichtigt. Während die in diesem Anhang betrachteten Überlegungen auch auf andere Kontroll- und Steuerungssysteme zutreffen können, insbesondere auf andere Building Control Systems oder Utility Control Systems, werden sie hier im Zusammenhang mit einem HLK-Steuerungssystem betrachtet.

F-2 BESCHRÄNKUNG EXTERNER FUNKTIONEN

Das Schlüsselkonzept bei der Anbindung eines kritischen FCS an ein nicht kritisches UMCS ist es, den Einfluss des UMCS auf das FCS zu begrenzen. Die Wechselwirkungen zwischen FCS und UMCS sollten spezifisch sein und genau definiert werden, und nur auf die beschränkt werden, die für den Betrieb des Systems erforderlich sind. Im Allgemeinen bedeutet dies, dass Überwachungsdaten vom FCS an das UMCS weitergeleitet werden und gleichzeitig nur sehr wenige oder gar keine Kontrollinformationen vom UMCS an das FCS gesendet werden. Beispiel: Ein kritisches System (FCS) kann eine Status- und Alarmmeldung an ein nicht kritisches System (UMCS) senden, sollte aber keine Start- und Stoppbefehle vom UMCS erhalten, da dies zu Schwachstellen im kritischen System führt. Manuelle Eingriffe in das kritische FCS sollten in jedem Fall sorgfältig abgewogen werden – durch einen Bediener, ***der sich seines Handelns voll bewusst ist und die Auswirkungen seines Handelns kennt.***

F-3 MÖGLICHKEITEN ZUR ANBINDUNG VON FCS AN UMCS

Die Begrenzung ***möglicher*** Eingriffe durch vernetzte Controller ist sehr schwer umzusetzen. In vielen Fällen kann der Angreifer seinen Laptop an das UMCS-Netzwerk anschließen und ein neues Programm auf ein Gerät aufspielen, das Bestandteil des kritischen FCS ist. Das heißt nicht, dass der Schutz gegen solche Eingriffe in Frage gestellt wird, sondern dass das UMCS nicht ausreichend geschützt ist, um das FCS zu schützen. Deshalb ist davon auszugehen, dass ein solcher Eingriff möglich ist. Dem ist vorzubeugen. Dies ist mit der zusätzlichen physischen Sicherheit, die normalerweise eine kritische Einrichtung schützt, vergleichbar. Auch wenn es Schutzmaßnahmen gibt, die allgemein den Zugang zur Liegenschaft beschränken, wird unterstellt, dass ein Angreifer Zugang zur Liegenschaft erlangt, und dass kritische Einrichtungen über eine zusätzliche physische Sicherheit verfügen, um weiteren Zugang zu verhindern.

Es gibt drei verschiedene Möglichkeiten, um eine sichere Verbindung zwischen einem kritischen FCS und einem nicht kritischen UMCS herzustellen: eine E/A-Schnittstelle (Hardware), Hardware-Gateway und Netzwerk-Firewall. Von diesen drei Möglichkeiten, wird für das kritische FCS die Verwendung der E/A-Schnittstelle (Hardware) empfohlen.

F-3.1 E/A-Schnittstelle (Hardware)

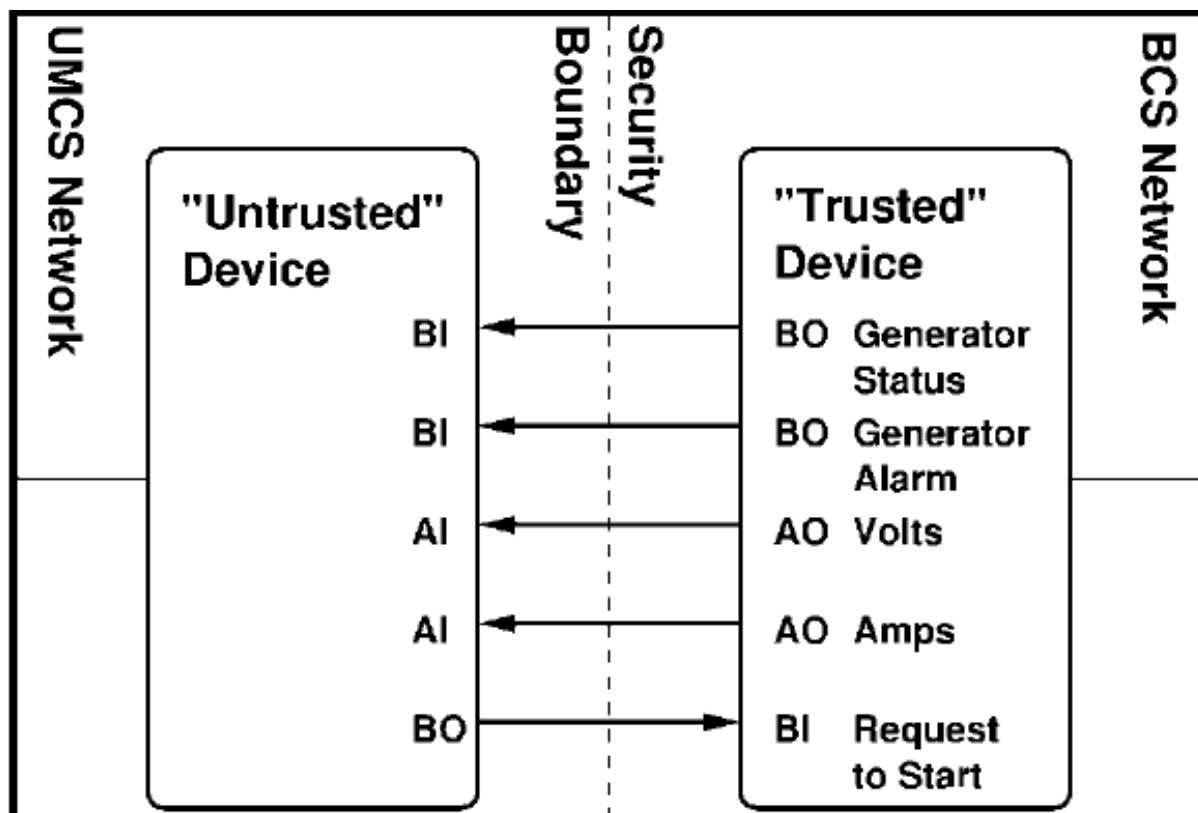
Die sicherste Methode, das FCS an das UMCS anzuschließen, ist es, Daten nur mittels analogen und binären Signalen auszutauschen. Das FCS ist **nicht** über ein Netzwerk an das UMCS anzubinden. Durch die Verwendung der E/A-Schnittstelle (Hardware) wird verhindert, dass ein Angreifer mittels „Hotlinking“ einen unerwünschten Befehl auf die Schnittstelle aufspielt, da der Datenaustausch durch die Hardware-Anschlüsse definiert und beschränkt ist. Selbst wenn ein Angreifer ein nicht vertrauenswürdiges Gerät steuert, so kann das vertrauenswürdige Gerät nur die Befehle empfangen, die es gemäß Planung und Konstruktion empfangen soll.

F-3.1.1 Übersicht E/A-Schnittstelle (Hardware)

Eine E/A-Schnittstelle (Hardware) besteht aus zwei Controllern, welche über binäre oder analoge Ein-/Ausgänge (normalerweise potentialfreie Kontakte, 4-20 mA Signale oder 0-10 V Signale) Daten zwischen den Systemen austauschen.

Abbildung F-1 zeigt die E/A-Schnittstelle (Hardware), wo ein Generator, der eine kritische Einrichtung versorgt, einige wichtige Überwachungspunkte an das UMCS sendet und einen Kontrollpunkt „Anforderung zum Starten“ vom UMCS erhält. Es ist wichtig, dass das System durch diesen Punkt lediglich **aufgefordert** wird, zu starten, und dass die eigentliche Entscheidung, ob der Generator startet oder stoppt, vom kritischen FCS getroffen werden **muss**.

Abbildung F-1: E/A-Schnittstelle (Hardware), Beispiel



F-3.1.2 Implementierung E/A-Schnittstelle (Hardware)

Für die Implementierung einer E/A-Schnittstelle (Hardware) werden sowohl für das FCS als auch für das UMCS Controller mit entsprechenden Hardwarepunkten benötigt. Ein Angreifer könnte die E/A-Leitungen unter zu hohe Spannung setzen und somit den Controller des FCS physisch beschädigen. Um dies zu verhindern, ist entweder:

- Ein Controller zu verwenden, der fest der Kommunikationsschnittstelle zugeordnet ist und keine weiteren Funktionen auf der Seite des FCS übernimmt, sodass dies im Falle einer Beschädigung keine Auswirkungen auf das Kontrollsystem hat.

Oder

- Eine optische Trennung der analogen und binären Signale zwischen den Geräten vorzusehen.

Der Controller auf der UMCS-Seite der Anbindung kann sich an einem Controller befinden, der andere Funktionen übernimmt, da befürchtet wird, dass das kritischere FCS einem Risiko ausgesetzt wird, das vom UMCS ausgeht, und nicht umgekehrt. Während der Controller auf der UMCS-Seite logischerweise Bestandteil des UMCS ist (eine E/A-Schnittstelle in Hardwareform), kann es bezüglich Beschaffung und Einbau einfacher sein, wenn es vom AN FCS bereitgestellt und eingebaut wird.

F-3.1.3 Vor- und Nachteile E/A-Schnittstelle (Hardware)

Diese Methode ist bei weitem die sicherste Methode zur Kommunikation zwischen FCS und UMCS, da ein Angreifer nichts tun kann, was Auswirkungen auf das kritische System hat. Ein möglicher Nachteil dieser Variante sind die zusätzlichen Kosten für die Beschaffung und den Einbau von zwei zusätzlichen E/A-Punkten in Hardwareform (jeweils zur Überwachung bzw. Kontrolle). Abhängig von der Menge und Komplexität der auszutauschenden Daten kann diese Variante teurer als andere Varianten sein oder auch nicht.

Außerdem ist diese Variante - planerisch gesehen - am einfachsten zu realisieren und erfordert kein besonderes Fachwissen zum Thema Cyber-Sicherheit. Lediglich den Kontrollpunkten ist besonderes Augenmerk zu schenken.

F-3.2 Gateway-Schnittstelle (Hardware)

Ein Gateway in Hardwareform ist eine andere Möglichkeit, ein kritisches FCS an ein nicht kritisches UMCS anzubinden. Obwohl dies nicht so sicher wie eine E/A-Schnittstelle (Hardware) ist, so ist es sehr viel kostengünstiger, wenn eine große Datenmenge zwischen FCS und UMCS ausgetauscht wird.

F-3.2.1 Übersicht zum Gateway in Hardwareform

In diesem Zusammenhang ist ein Gateway ein Gerät mit einer Verbindung zum UMCS-Netzwerk und mit einer **separaten** Verbindung zum FCS-Netzwerk, das keinen Datenverkehr zwischen den beiden Verbindungen durchlässt (d.h. es leitet keine Pakete zwischen den beiden Netzwerken weiter). Stattdessen empfängt das Gateway die Daten von einem Netzwerk, verarbeitet sie und leitet diese identischen Daten an das andere Netzwerk weiter. Während in der Theorie sowohl das UMCS als auch das FCS das gleiche Protokoll (z.B. BACnet) verwenden können, kann es in der Praxis schwierig sein, ein ausreichend sicheres Gateway zu finden, das „auf beiden Seiten“ das gleiche Protokoll verwendet, da eine typische Planung die gleiche Verbindung für passende Protokolle vorsieht.

F-3.2.2 Implementierung eines Gateways in Hardwareform

An die Implementierung eines sicheren Gateways bestehen folgende Anforderungen:

- Das Gateway muss eine vollständige Trennung zwischen dem Netzwerk des UMCS und dem Netzwerk des FCS sicherstellen. Dies erfordert 2 getrennte Netzwerkanschlüsse, was schwierig sein kann, wenn sowohl das FCS als auch das UMCS die gleichen Protokolle verwendet.
- Das Gateway muss vom Netzwerk des UMCS aus weder programmiert, noch konfiguriert, noch anderweitig verändert werden können. Da das Gateway wahrscheinlich über das „primäre“ Netzwerk konfiguriert werden kann, ist diese Anforderung nur schwer zu erfüllen, wenn das UMCS und das FCS die gleichen Protokolle verwenden. Wenn beide das gleiche Protokoll verwenden, dann ist es wahrscheinlicher, dass das Gateway sowohl über das UMCS als auch über das FCS konfiguriert werden kann. Die Möglichkeit zur Konfiguration hängt von der tatsächlichen Implementierung des Gateways ab. Deshalb ist darauf zu achten, dass vorgeschrieben wird, dass das Gateway nicht vom Netzwerk des UMCS aus konfiguriert werden kann.
- Das Gateway muss so konfiguriert werden, dass nur die Punkte, die für das UMCS unerlässlich sind, angezeigt werden.

Das Gateway ist Bestandteil des FCS und sollte vom AN FCS eingebaut werden.

F-3.2.3 Vor- und Nachteile eines Gateways in Hardwareform

Die größten Sicherheitsbedenken bei einem Gateway (unter der Annahme, dass die oben genannten Anforderungen erfüllt werden) sind die Sicherheitslücken bei der Implementierung des Gateways. Genauso wie ein Webserver eine Schwachstelle haben kann, die einem Angreifer erlaubt, die Kontrolle über den Server zu übernehmen, so kann auch ein Gateway einen Implementierungsfehler aufweisen, der eine Kontrolle des Gateways ermöglichen würde; sobald der Angreifer einmal das Gateway kontrolliert, kann er das Gateway neu konfigurieren und so das FCS selbst angreifen.

Bei Systemen mit der Anforderung, dass viele Punkte gemeinsam genutzt werden, kann ein Gateway eine kostengünstige Alternative zur Verwendung von E/A-Punkten (Hardware) sein, und die Kosten für ein Gateway hängen im Gegensatz zur E/A-Schnittstelle (Hardware) nicht so sehr von der Anzahl der Punkte ab.

F-3.3 Firewall-Schnittstelle

Die dritte Möglichkeit, eine Netzwerkverbindung zwischen UMCS und FCS abzusichern, ist es, eine Netzwerkverbindung zu erlauben, aber eine Firewall zu verwenden, um den Datenverkehr zwischen den beiden Netzwerken gezielt zu blockieren. Für die Firewall ist eine Netzwerkanbindung erforderlich. Deshalb kann sie nur verwendet werden, wenn sowohl das UMCS als auch das FCS das gleiche Protokoll verwendet.

F-3.3.1 Übersicht zur Firewall-Schnittstelle

Im Gegensatz zu einem Gateway, bei dem es keine Netzwerkverbindung zwischen den beiden Netzwerken gibt und das Gateway Daten von einem Netzwerk zum anderen sendet, sind bei einer Firewall die beiden Netzwerke miteinander verbunden und die Firewall reduziert gezielt den zulässigen Datenverkehr zwischen den beiden Netzwerken. Dadurch ist die Firewall grundsätzlich nicht so sicher wie das Gateway.

F-3.3.2 Implementierung einer Firewall-Schnittstelle

An eine sichere Firewall werden die folgenden Anforderungen gestellt:

- Die Firewall selbst kann nur in einer kritischen Einrichtung programmiert werden. Für gewöhnlich ist diese Anforderung leicht zu erfüllen, da Firewalls als Sicherheitsanwendungen über eine „sichere“ Seite und eine „nicht sichere“ Seite verfügen.
- Anders als gewöhnliche IT-Firewalls, muss die Firewall in der Lage sein, den Datenverkehr auf Grundlage der detaillierten Informationen im Paket zu filtern. Während eine normale Firewall den Datenverkehr auf Grundlage der IP-Adresse und des TCP/UDP-Port reduzieren kann sowie jeglichen Datenverkehr - mit Ausnahme des ein- und ausgehenden Datenverkehrs vom UMCS-Server - blockieren kann, muss die Firewall des Kontrollsystems auch in der Lage sein, alle bis auf spezifische Befehle zu blockieren. Diese kann nicht nur den gesamten Datenverkehr, mit Ausnahme des ein- und ausgehenden Datenverkehrs vom UMCS-Frontend-Server, blockieren, sondern auch den gesamten Datenverkehr, mit Ausnahme bestimmter Meldungen – wie z.B. BACnet ReadProperty Anfragen für bestimmte Punktwerte. Dies erfordert eine Firewall, die ein bestimmtes Kontrollprotokoll versteht (in diesem Fall BACnet) und auf Grundlage dieser speziellen Information den Datenverkehr gezielt blockieren kann.

F-3.3.3 Pro und Kontra Firewall-Schnittstelle

Das Hauptproblem bei der Implementierung einer Firewall ist die fehlende Verfügbarkeit einer Firewall, die Pakete an Kontrollprotokollen lesen und aufgrund einer Meldung gezielt filtern kann. Ein Vorteil der Firewall gegenüber dem Gateway ist, dass die Firewall für Sicherheitsanwendungen entwickelt wird und im Vergleich zu einem Gateway, das normalerweise nicht für Sicherheitsanwendungen gedacht ist, ein Implementierungsfehler weniger wahrscheinlich ist.

F-4 WEITERE ÜBERLEGUNGEN

F-4.1 Lokale Benutzeroberflächen

Kritische Systeme sollten zusätzlich mit lokalen Benutzeroberflächen ausgestattet sein, sodass das Wartungspersonal im gesicherten Bereich Zugang zu den Kontrolldaten erhält, um Fehler beheben zu können. Eine großzügige Verwendung von lokalen Anzeigetableaus wird dringend empfohlen. Für größere kritische Systeme wäre es wünschenswert, eine zweckmäßigere Schnittstelle (im Vergleich zu einer normalerweise in der lokalen Benutzeroberfläche verfügbaren Schnittstelle) wie z.B. ein unabhängiges UMCS-Frontend oder eine Webschnittstelle zu verwenden. Für die größten oder kritischsten Systeme sollte der Einbau eines UMCS mit vielen Funktionen gemäß UFGS 25 10 10 in Erwägung gezogen werden. Dieses UMCS sollte dem FCS vorbehalten sein (z.B. ein Level 2D-Frontend) und sich vollständig innerhalb der physischen Sicherheit der kritischen Systeme befinden.

F-4.2 Risikomanagement

Man muss immer bedenken, dass es für die Cyber-Sicherheit von Kontrollsystemen keine perfekte Lösung gibt. Cybersicherheitsexperten sagen oft: „Es gibt keine Schlupflöcher“.

Richtiger wäre es zu sagen: „Es findet sich immer ein Schlupfloch“. Die Absicht bleibt bestehen – ein Angreifer wird immer einen Weg finden, die Sicherheitsmaßnahmen zu umgehen. Ziel bei der Planung der Cyber-Sicherheit von Kontrollsystemen, insbesondere kritischen Kontrollsystemen, ist es, das zu tun, was auch immer möglich ist, um dies so schwer wie möglich zu machen.

Diese Seite wurde absichtlich freigelassen.

ANHANG G: LEITFADEN ZUR IMPLEMENTIERUNG VON SICHERHEITS- KONTROLLEN

G-1 EINLEITUNG

Dieser Anhang ist ein Leitfaden für Planer von Kontrollsystemen zur Implementierung von Sicherheitskontrollen für Kontrollsysteme. Der Fokus dieses Leitfadens liegt auf Systemen mit einem GERINGEN Auswirkungsgrad (Auswirkungsgrad L-L-L C-I-A), die in einer Liegenschaft des US-Verteidigungsministeriums zu finden sind, insbesondere Building Control Systems und Utility Monitoring and Control Systems. ANHANG H enthält Tabellen, in denen die Zuständigkeiten des Kontrollsystems und der jeweilige CCI dargestellt sind. Die in diesem Anhang enthaltenen Hinweise ergänzen diese aufgelisteten CCIs.

G-2 ALLGEMEIN

G-2.1 Terminologie für Kontrollsysteme im Vergleich zu Standard-IT-Systemen

Sicherheitskontrollen und CCIs wurden für herkömmliche IT-Systeme entwickelt und viele enthalten Begriffe und Anforderungen, die verwirrend und widersprüchlich sind, wenn sie für Kontrollsysteme anzuwenden sind. Zum Beispiel: „Vorfall“, wie der Begriff in der Kontrollfamilie IR von Sicherheitskontrollen verwendet wird, umfasst alle Vorfälle – ein defekter Keilriemen ist ein „Vorfall“, aber ein „Mangel“, wie er in der Sicherheitskontrolle SI-2 verwendet wird, deckt nur Sicherheitsmängel ab und keine betrieblichen Mängel – ein defekter Sensor ist kein „Mangel“.

In den meisten Fällen wird die Anwendung einer Sicherheitskontrolle für ein Kontrollsystem mit Hilfe der unten stehenden Erklärungen verständlich. In anderen Fällen sollte die Richtlinie NIST SP 800-53 herangezogen werden, da sie die Sicherheitskontrollen am besten definiert und einen „ergänzenden Leitfaden“ enthält, mit dessen Hilfe die CCIs interpretiert und in einem Kontrollsystem angewendet werden können. NIST SP 800-82 (Abschnitt 6.2 der Revision 2) enthält auch allgemeine Angaben zu den Sicherheitskontrollfamilien, sowie einen Leitfaden für die Anwendung von Sicherheitskontrollen in industriellen Kontrollsystemen, die eine Untergruppe der Kontrollsysteme sind und ähnliche Eigenschaften wie liegenschaftsabhängige Kontrollsysteme aufweisen.

G-2.2 Durch das US-Verteidigungsministerium festgelegte Werte

Viele CCIs enthalten durch das US-Verteidigungsministerium festgelegte Werte für „alle Mitarbeiter“ und viele CCIs enthalten durch das US-Verteidigungsministerium definierte Werte für „alle Komponenten“ oder ähnlich, wobei diese Detailgenauigkeit für Systeme mit einem GERINGEN Auswirkungsgrad nicht zutreffend ist. Es ist erforderlich, die Werte für die CCIs neu zu definieren (und zu dokumentieren), wenn die durch das US-Verteidigungsministerium definierten Werte für die Kontrollsysteme nicht sinnvoll sind.

G-2.3 Sicherheitskontrollen die „automatisch erfüllt“ werden

Einige Sicherheitskontrollen können „automatisch“ sein (in dem Sinne, dass sie bereits für ein anderes Informationssystem oder Kontrollsystem implementiert wurden). Eine Sicherheitskontrolle, die besagt, dass „die Organisation <etwas> macht...“, kann bereits als Anforderung für eine andere Autorisierung für ein anderes System erfüllt sein.

G-2.4 Anwendbarkeit von Sicherheitskontrollen gemäß 5-stufigem Aufbau

Bei den meisten Kontrollsystemen können viele Sicherheitskontrollen nur schwer oder gar nicht unterhalb von Level 3 angewendet werden. Es ist jedoch zu beachten, dass einige Systeme wie z.B. elektronische Sicherheitssysteme (ESS) in der Lage sind, viele dieser Sicherheitskontrollen unterhalb von Level 3 zu erfüllen. Beispiel: Ein Controller für ein RLT-Gerät (mit einer Benutzeroberfläche) kann mit einem Passwort mit nur 4 Zeichen versehen werden oder aber auch ohne Passwortunterstützung verwendet werden. Ein Türschloss an einem ESS kann mit einem CAC-Leser ausgestattet werden.

G-2.5 Anwendbarkeit Auswirkungsgrad

Nur Sicherheitskontrollen für Systeme mit einem „GERINGEN Auswirkungsgrad“ (L-L-L) und „MITTLEREN Auswirkungsgrad“ (M-M-M) werden in diesem Anhang und in den CCI-Tabellen in ANHANG H berücksichtigt. Der Leitfaden für die grundlegenden Sicherheitskontrollen basiert auf dem C-I-A-Auswirkungsgrad für das Kontrollsystem:

- Grundlegende Sicherheitskontrollen L-L-L: Der Leitfaden bezieht sich auf ein System mit einem GERINGEN Auswirkungsgrad. Die gleichen Sicherheitskontrollen werden auch für ein System mit einem MITTLEREN (oder HOHEN) Auswirkungsgrad benötigt, aber ein zusätzlicher Leitfaden zur Verbesserung und Implementierung der Sicherheit kann erforderlich werden. Wenn dieser Leitfaden für Systeme mit einem MITTLEREN (oder HOHEN) Auswirkungsgrad angewendet wird, so ist der Leitfaden zu prüfen, um festzustellen, ob er für das System angewendet oder abgeändert werden muss.
- Grundlegende Sicherheitskontrollen M-M-M: Der Leitfaden bezieht sich auf ein System mit einem MITTLEREN Auswirkungsgrad. Diese Sicherheitskontrollen werden nicht für Systeme mit einem GERINGEN Auswirkungsgrad angewendet. Dieser Leitfaden ist möglicherweise anders als bei Systemen mit einem HOHEN Auswirkungsgrad (bei Anwendung gleicher Sicherheitskontrollen).

Der Leitfaden in diesem Anhang und in den CCI-Tabellen in ANHANG H betrifft hauptsächlich Systeme mit einem GERINGEN Auswirkungsgrad, die am besten standardisiert werden können. Wenn dieser Leitfaden für Systeme mit einem MITTLEREN oder HOHEN Auswirkungsgrad angepasst wird, so muss dies sorgfältig geschehen.

G-3 LEITFADEN FÜR INDIVIDUELLE SICHERHEITSKONTROLLEN

G-3.1 Kontrollfamilie Zugangskontrolle (AC)

Tabelle G-1 enthält einen Leitfaden zur Planung von Zugangskontrollen.

Tabelle G-1: Kontrollfamilie Zugangskontrolle (AC)

Sicherheitskontroll-ID	Bezeichnung und Leitfaden zur Planung von Sicherheitskontrollen
AC-2	Kontoverwaltung: Es ist festzulegen, welche Kontoarten welche Berechtigungen im Kontrollsystem zulassen (z.B. „nur ansehen“, „Alarme quittieren“, „Sollwerte ändern“, usw.). Es ist zu beachten, dass der Planer diese Rollen dem ISSM / ISSO erläutern muss, sodass sie ihre vom US-Verteidigungsministerium definierten Aufgaben innerhalb dieser Kontrolle ausführen können. Es ist zu beachten, dass „Konten“ (und insbesondere „temporäre“ Konten oder „Notfall“-Konten) wahrscheinlich auf Level 4 existieren sind und abhängig vom Kontrollsystem auf Level 1 oder 2 vorkommen können oder auch nicht. (Beispiel: Viele Building Control Systems verfügen - anders als viele Utility Control Systems - auf diesen Leveln nicht über Benutzerkonten). Durch den Planer sind die fehlenden „Konten“ bei Level 1 und 2 zu erläutern. In den Spezifikationen sollte gefordert werden, dass Kontoaktivitäten geprüft (aufgezeichnet) werden können. Jedoch sollte die Prüfung auf Softwareanwendungen begrenzt werden und die Benachrichtigungsfunktion muss unterstützt werden. Es ist zu beachten, dass bei einer Benachrichtigung (z.B. E-Mail, Rollup auf ein anderes System) üblicherweise eine Plattform Enclave oder ein anderer Level 4 Support und Level 5 Support für die tatsächliche Ausführung erforderlich ist.
AC-3	Zugangsregelung: AC-3 wird durch die Verpflichtung des AN, jede Komponente des Kontrollsystems, die über ein STIG oder SRG verfügt, gemäß dieser STIG oder SRG zu konfigurieren, erfüllt.
AC-4	Regelung Informationsfluss: Der Informationsfluss kann durch die IT-Organisation am FPOC geregelt werden. Vorhandene Level 2N Geräte können auf Level 2 zur Regelung des Informationsflusses verwendet werden. Ähnliche Geräte können auf Level 1N vorhanden sein. In den Spezifikationen sind Anforderungen aufzunehmen, dass der ausführende AN notwendige Kommunikationen (für „Whitelisting“) dokumentieren muss. Ist die Regelung des Informationsflusses eine Anforderung bei Level 2N, so sind in den Spezifikationen Anforderungen zur Implementierung zu berücksichtigen.

Sicherheitskontroll-ID	Bezeichnung und Leitfaden zur Planung von Sicherheitskontrollen
AC-6	Prinzip der geringsten Privilegien: Innerhalb des Kontrollsystems (im Gegensatz zur Platform Enclave) sollte das Prinzip der geringsten Privilegien mittels Spezifikationen realisiert werden, welche die Anwenderfunktion am Frontend beschränken (Beispiel: einige Benutzer können Punkte nur ansehen, andere Benutzer können Sollwerte ändern, usw.). Es ist zu beachten, dass seitens des US-Verteidigungsministeriums definiert ist, wo eine ausdrückliche Autorisierung erforderlich ist und dass (für ein Kontrollsystem) alles – einschließlich Hardware – enthalten ist. Dies ist möglicherweise nicht praktikabel. Von Seiten des Planers ist die Implementierung über projektspezifische Anforderungen einschließlich physischer Sicherheit sicherzustellen. Es ist auch zu beachten, dass es für AC-6 (2) erforderlich ist, dass der Bediener des Kontrollsystems, der Zugang zu privilegierten Funktionen hat (mittels Login in ein privilegiertes Konto), nur über ein separates Konto Zugriff auf nicht-privilegierte Funktionen hat. Im Hinblick auf die Rolle, die ein Bediener spielt, ist dies wahrscheinlich nicht möglich bzw. nicht erstrebenswert für Kontrollsystemanwendungen (wo es beispielsweise nicht möglich ist, zu erwarten, dass ein Bediener sich ausloggt und dann wieder einloggt, um einen Punkt zu überschreiben).
AC-7	Fehlgeschlagene Anmeldeversuche: Es ist zu beachten, dass die Anforderung einer HOHEN Verfügbarkeit am Frontend die Sperrung eines Kontos bei fehlgeschlagenen Anmeldeversuchen ausschließt. Unterhalb von Level 3 ist diese Kontrolle nicht möglich und sogar bei Level 4 ist dies nur durch das Einloggen in das Betriebssystem möglich, als Voraussetzung für den Zugang zum Kontrollsystem. Durch den Planer ist zu bestimmen, wo dies unterstützt werden kann, und in den Spezifikationen sind Anforderungen aufzunehmen, wo dies erforderlich ist.
AC-8	Benachrichtigung Systemnutzung: Login-Banner müssen implementiert werden, wenn sich Benutzer an PCs der Regierung anmelden – z.B. Platform Enclave, Level 4 und Level 2 PCs. Benutzeroberflächen auf Level 0, 1 und 2 (z.B. lokale Anzeigetableaus) werden normalerweise einen Login-Banner nicht unterstützen. Login-Banner sind - wo immer dies gemäß den Leitlinien der Industrie für bewährte Praxis möglich ist - vorzuschreiben und es ist anzugeben, wo eine Implementierung nicht möglich ist.
AC-11 und AC-12	Sperrung und Beendigung einer Sitzung: Das Konzept einer „Sitzung“ ist normalerweise nur auf einem PC sinnvoll (d.h. Level 4), und bei PCs sollten diese Kontrollen vom Betriebssystem implementiert und von der Platform Enclave übernommen werden. Bei Level 1 und Level 2 Geräten gibt es üblicherweise keine Benutzeroberflächen. Durch den Planer ist vorzugeben, dass Geräte mit Benutzeroberflächen (z.B. lokale Anzeigetableaus) durch ein Passwort geschützt sind und einen Benutzer nach einer gewissen Zeit der Inaktivität automatisch abmelden.

Sicherheitskontroll-ID	Bezeichnung und Leitfaden zur Planung von Sicherheitskontrollen
AC-14	Zulässige Aktionen ohne Identifikation oder Authentifizierung: Level 4: Für alle Aktionen sollte eine Authentifizierung für das (Windows) Betriebssystem erforderlich sein. Benutzeroberflächen auf Level 1 oder 2 sollten mit einem Passwort geschützt sein. Es ist zu beachten, dass diese Sicherheitskontrolle konkret die Benutzeranwendungen betrifft und nicht die „für den Benutzer ausgeführten Prozesse“. In den meisten Fällen wird dies durch den Benutzer selbst erfüllt, der sich an einem PC angemeldet hat. Physische Sicherheit kann erforderlich sein, um den Zugang zu Geräten und Anlagen zu verweigern, und kann bei verschiedenen Leveln beispielsweise durch abschließbare Einhausungen, Deckelschalter, Zugangskontrollen, Schleusen und (Papier) Zugriffsprotokolle implementiert werden. Einige Benutzerzugänge (lokale Anzeigetableaus, Hand-Aus-Auto-Schalter usw.) unterstützen möglicherweise keine Authentifizierung. Hier sollte die erforderliche physische Sicherheit in Betracht gezogen werden. Wenn für solche Geräte physische Sicherheit geplant ist, so ist es im Allgemeinen nicht von Vorteil, eine Schnittstelle, welche zusammen mit den kontrollierten Geräten untergebracht ist, zu sichern, ohne dass auch die kontrollierten Geräte selbst gesichert werden, da die Geräte weiterhin anfällig wären.
AC-17	Fernzugriff: Der Fernzugriff sollte durch die Plattform Enclave abgedeckt sein (siehe allgemeine Anmerkungen zur Kontrollfamilie Zugangskontrolle (AC)).
AC-18	Drahtloser Zugang: Der drahtlose Zugang sollte bei Level 4 von der entsprechenden IT-Organisation vorgesehen werden. Bei Level 1 und 2 ist ein drahtloser Zugang weitestgehend zu vermeiden. Ein drahtloser Zugang ist für Nachrüstungen in Betracht zu ziehen, wo die Verlegung von Leitungen nicht gestattet ist und andere Technologien (wie z.B. Powerline Carrier) vorrangig verwendet werden sollen. Wenn ein drahtloser Zugang zulässig ist, ist eine sehr begrenzte Reichweite vorzuschreiben, sodass Signale außerhalb der erforderlichen Bereiche nicht verfügbar sind. In vielen Fällen werden auf den Leveln 1 und 2 Authentifizierung und Verschlüsselung nur in geringem Maße unterstützt.
AC-19	Zugangskontrolle für mobile Geräte: Mobile Geräte schließen Tablets, Telefone usw. ein. Diese werden in der Plattform Enclave geregelt. Sofern sie zulässig sind, können sie als Arbeitsplätze für browserbasierte Clients verwendet werden oder aber auch darauf beschränkt werden, Alar-me/Meldungen vom Kontrollsystem zu empfangen.
AC-20	Nutzung von externen Informationssystemen: Anbindungen von externen Systemen und portablen Datenträgern sollten über die Plattform Enclave erfolgen.
AC-21	Zusammenarbeit und Informationsaustausch: Kontrollsysteme sollten normalerweise keine Informationen austauschen. Jeglicher Austausch erfolgt über die Plattform Enclave.

Sicherheitskontroll-ID	Bezeichnung und Leitfaden zur Planung von Sicherheitskontrollen
AC-22	Öffentlich zugängliche Inhalte: Kontrollsysteme sollten nicht öffentlich zugänglich sein.

G-3.2 Kontrollfamilie Prüfungs- und Rechenschaftspflicht (AU)

Eine Prüfung (im Sinne der Cyber-Sicherheit) kann normalerweise nur bei Level 4 erfolgen, obwohl einige Level 1 oder Level 2 Geräte möglicherweise über begrenzte Prüfungsmöglichkeiten verfügen. Wo dies möglich ist, ist seitens des Planers eine Prüfung vorzuschreiben. Der Planer muss darauf vorbereitet sein, dass er Rechenschaft ablegen muss, wenn er eine Prüfung nicht vorsieht, wenn dies schlichtweg nicht möglich ist. Der Planer kann dazu beitragen festzulegen, was geprüft werden kann, wo es geprüft werden kann und welche Informationen gewonnen werden können. Es kann sinnvoll sein, dass diese Kontrollen von der Plattform Enclave übernommen werden.

Tabelle G-2 enthält einen Leitfaden zur Planung von Kontrollen in der Kontrollfamilie Prüfungs- und Rechenschaftspflicht (AU).

Tabelle G-2 Kontrollfamilie Prüfungs- und Rechenschaftspflicht (AU)

Sicherheitskontroll-ID	Bezeichnung und Leitfaden zur Planung von Sicherheitskontrollen
AU-2	Prüfereignisse: Keine zusätzlichen kontrollspezifischen Leitlinien. Nutzen Sie den allgemeinen Leitfaden für Kontrollfamilien, den Sie oberhalb der Tabelle für diese Kontrolle finden.
AU-3	Inhalte von Prüfaufzeichnungen: Es ist zu beachten, dass dies – insbesondere der „Benutzer“-Anteil – nur bei Level 4 möglich ist.
AU-4	Speicherkapazität von Prüfungen: Eine dauerhafte Speicherung der Prüfungen erfolgt auf einem Level 4 PC. Die Übertragung vom Kontrollsystem auf einen dauerhaften Speicher erfolgt voraussichtlich manuell oder möglicherweise mittels eines Scripts über das PC-Betriebssystem, ist aber wahrscheinlich kein charakteristisches Merkmal des Kontrollsystems. Durch den Planer ist vorzugeben, dass die Kontrollsystemprüfungen mittels Tools des Betriebssystems zugänglich sind (z.B. das Kontrollsystem unterstützt oder exportiert in Standard-Dateiformate).
AU-5	Vorgehen bei Prüfprozessfehlern: Benachrichtigungen und konkrete Aktionen sind nur auf Level 4 möglich.

Sicherheitskontroll-ID	Bezeichnung und Leitfaden zur Planung von Sicherheitskontrollen
AU-6	Auswertung, Analyse und Berichterstattung von Prüfungen: Keine zusätzlichen kontrollspezifischen Leitlinien. Nutzen Sie den allgemeinen Leitfaden für Kontrollfamilien, den Sie oberhalb der Tabelle für diese Kontrolle finden.
AU-7	Reduzierung von Prüfungen und Berichterstellung: Eine nachträgliche Bearbeitung von Prüfprotokollen ist normalerweise nur mittels externer Tools auf Level 4 möglich. Da diese Tools aber für das Prüfprotokollformat des Kontrollsystems spezifisch sind, muss dies voraussichtlich über das Kontrollsystem und nicht über die Plattform Enclave realisiert werden.
AU-8	Zeitstempel: Normalerweise sind die Anforderungen des Kontrollsystems ausreichend.
AU-9	Schutz der Prüfinformationen: Hierfür kommt nur der Frontend-Server oder ein anderer Level 4 PC in Frage. Prüfprotokolle müssen dort gespeichert (und geschützt) werden.
AU-11	Aufbewahrung von Prüfaufzeichnungen: Keine zusätzlichen kontrollspezifischen Leitlinien. Nutzen Sie den allgemeinen Leitfaden für Kontrollfamilien, den Sie oberhalb der Tabelle für diese Kontrolle finden.
AU-12	Generierung von Prüfungen: Keine zusätzlichen kontrollspezifischen Leitlinien. Nutzen Sie den allgemeinen Leitfaden für Kontrollfamilien, den Sie oberhalb der Tabelle für diese Kontrolle finden.

G-3.3 Kontrollfamilie Sicherheitsbewertung und Autorisierung (CA)

Tabelle G-3 enthält einen Leitfaden zur Planung von Kontrollen in der Kontrollfamilie Sicherheitsbewertung und Autorisierung (CA).

Tabelle G-3: Kontrollfamilie Sicherheitsbewertung und Autorisierung (CA)

Sicherheitskontroll-ID	Bezeichnung und Leitfaden zur Planung von Sicherheitskontrollen
CA-3	Systemanbindungen: Es ist zu beachten, dass es sich hier um Anbindungen an andere Systeme handelt. Diese sollten in der Plattform Enclave dokumentiert werden. Die Spezifikationen sollten ein spezifisches Protokoll definieren.
CA-6	Sicherheitsautorisierung: Der Autorisierungsbefugte ist ein leitender Angestellter (senior-level executive) oder ein Leiter (manager).

Sicherheitskontroll-ID	Bezeichnung und Leitfaden zur Planung von Sicherheitskontrollen
CA-9	Interne Systemanbindungen: Bei dem Kontrollsystem handelt es sich um ein System mit besonderen Aufgaben. In der Planung sollten nur die erforderlichen Anbindungen zulässig sein; für gewöhnlich bedeutet das, dass ein einzelnes spezifisches Protokoll mit begrenzten Möglichkeiten zur Anwendung kommt. Diese Spezifikationen, Datenpunktlisten und Netzwerkkonzepte dokumentieren diese Kontrollen.

G-3.4 Kontrollfamilie Konfigurationsmanagement (CM)

Tabelle G-4 enthält einen Leitfaden zur Planung von Kontrollen in der Kontrollfamilie Konfigurationsmanagement (CM).

Tabelle G-4: Kontrollfamilie Konfigurationsmanagement (CM)

Sicherheitskontroll-ID	Bezeichnung und Leitfaden zur Planung von Sicherheitskontrollen
CM-2	Grundlegende Configuration: Typische vertraglich geforderte Vorlagen für ein Kontrollsystem (Pläne, Softwarelizenzen, programmierbare Controller „Quellcode“ usw.) sollten diesen CCI erfüllen. Bei der Bestimmung, welche Geräte in Bereichen mit einem erheblichen Risiko liegen und welche zusätzlichen Konfigurationen für diese Geräte notwendig sind, sollte der Planer eingebunden werden. Es ist zu beachten, dass Kontrollsysteme (die feststehende Einrichtungen unterstützen) nicht mobil sind.
CM-5	Zugangsbeschränkungen bei Änderungen: Ein Großteil des Kontrollsystems kann sich außerhalb des Kontrollbereichs der Organisation befinden. Gilt wahrscheinlich nur für Level 4. Siehe Kommentare zu PE-Kontrollen.
CM-6	Konfigurationseinstellungen: Durch den Planer ist weitestgehend sicherzustellen, dass andere Planungsanforderungen bzgl. Sicherheit in den Anforderungen des Kontrollsystems enthalten sind und dass diese Anforderungen während der Inbetriebnahme des Kontrollsystems geprüft werden. Der Planer sollte sicherstellen, dass in den Spezifikationen unnötige Ports, Protokolle und Dienste deaktiviert sind. Hinweis: Die Annahme, dass das Kontrollsystem aufgrund vorhandener STIGs usw. „automatisch“ konform ist, ist unterhalb von Level 3 komplett falsch und der muss Planer möglicherweise rechtfertigen, warum das Kontrollsystem nicht den Standardprüflisten entspricht. Da ein Kontrollsystem auf regelmäßig konfigurierbare Parameter ausgelegt ist, ist die Dokumentation und Genehmigung von jeglichen Änderungen an den Level 1 und Level 2 Controllern nicht möglich. Wesentliche Änderungen der architektonischen Konfiguration sollten dennoch dokumentiert und genehmigt werden.

Sicherheitskontroll-ID	Bezeichnung und Leitfaden zur Planung von Sicherheitskontrollen
CM-7	Geringste Funktionalität: Das Kontrollsystem dient einem besonderen Zweck (nicht einem allgemeinen) und seine Funktionen (und Einschränkungen) sind sowohl durch seine Architektur als auch durch seine Protokolle vorgeschrieben. Es sollte vorausgesetzt werden, dass alle Ports/Protokolle/Dienste, die nicht speziell für das Kontrollsystem benötigt werden, in den Spezifikationen deaktiviert werden. Die erforderliche Software sollte in den Spezifikationen enthalten sein; alle anderen Softwareprodukte sollten nicht zulässig sein.
CM-8	Bestand Informationssystem-Komponente: Die Erstkonfiguration ist den Bestandsunterlagen zu entnehmen. In den meisten Fällen stehen automatische Tools für den Komponentenbestand unterhalb von Level 3 für viele Systeme gegenwärtig nicht zur Verfügung, wenngleich neue Tools zukünftig für Systeme verfügbar sein können und auch implementiert werden sollten, sobald sie verfügbar sind.
CM-9 und CM-10	Konfigurationsmanagementplan und Einschränkungen der Softwarenutzung: Aus den vertraglichen Dokumenten muss hervorgehen, dass die Softwarelizenzen der Regierung Rechte an technischen Daten gewähren, um die Systeme betreiben und warten zu können, und die Software wie gewünscht nutzen zu können.

G-3.5 Kontrollfamilie Krisenplanung (CP)

Tabelle G-5 enthält einen Leitfaden zur Planung von Kontrollen in der Kontrollfamilie Krisenplanung (CP).

Tabelle G-5: Kontrollfamilie Krisenplanung (CP)

Sicherheitskontroll-ID	Bezeichnung und Leitfaden zur Planung von Sicherheitskontrollen
CP-2	Krisenplanung: Der Planer sollte zur Bestimmung kritischer Kontrollsystem-Komponenten, die wesentliche Aufgaben unterstützen, beitragen.
CP-6	Alternativer Speicherort: Für ein Kontrollsystem ist ein alternativer Speicherort nur für Backups sinnvoll. Dieser befindet sich auf der Plattform Enclave.

Sicherheitskontroll-ID	Bezeichnung und Leitfaden zur Planung von Sicherheitskontrollen
CP-7 und CP-8	Alternativer Verarbeitungsort und Kommunikationsdienste: Ein PIT-System kann über ein alternatives Frontend (Level 4) verfügen bzw. über alternative Verbindungen zwischen Frontend und niedrigeren Leveln, jedoch kann das Kontrollsystem nicht von den kontrollierten Geräten getrennt werden – egal welcher Vorfall vor Ort den Controller des RLT-Gerät deaktiviert, wird auch das RLT-Gerät deaktivieren. Diese Kontrollen gelten nur für die Platform Enclave (Level 4). Wenn bestimmt wird, ob diese gelten, ist zu beachten, dass für ein Frontend (Level 4) normalerweise niedrigere Anforderungen an die Verfügbarkeit bestehen als für Feldsteuerungen (Level 1 und 2). Wenn sich die Anforderungen auf ein redundantes Kontrollsystem am Field Control System beziehen, dann sollten auch die redundanten, kontrollierten Geräte bzw. redundanten Mandantenbereiche berücksichtigt werden.
CP-9	Backup Informationssystem: Nur Backups auf Level 4 / Platform Enclave.
CP-10	Wiederherstellung Informationssystem: Der Planer sollte Vorlagen verlangen, aus denen ausreichende Daten, Dokumentationen und Informationen zur Software hervorgehen, um den Zustand des Systems zum Zeitpunkt der Abnahme wiederherstellen zu können. Dies muss die kundenspezifische Programmierung und Konfiguration der Controller und Arbeitsplätze mit einschließen.
CP-12	Abgesicherter Modus: Der Planer sollte auf Grundlage der Wichtigkeit der kontrollierten Geräte festlegen, welche Bedingungen zu beachten sind und welche Maßnahmen ggf. vom Kontrollsystem zu ergreifen sind, wenn diese Bedingungen erfüllt sind. All das sollte in der Kontrolllogik (z.B. Betriebsablauf), insbesondere unter Berücksichtigung der Normalstellung/Fehlerstellung der Ausgangsgeräte, und in der Gesamtplanung des Systems festgelegt werden. Wenn eine hohe Betriebssicherheit erforderlich ist, sollten in der Planung zusätzlich redundante Geräte berücksichtigt werden. Siehe auch SC-24 und SI-17, sowie KAPITEL 4.

G-3.6 Kontrollfamilie Identifizierung und Autorisierung (IA)

Es ist zu beachten, dass ein Authentifikator entweder physisch (z.B. CAC-Karten, Token), nicht-physisch (z.B. Passwörter) oder biometrisch sein kann. Während bei Level 4 (Platform Enclave) alle möglich sind, unterstützen die meisten Kontrollsysteme auf Level 2 und darunter nur Passwörter – und selbst eine Passwortunterstützung ermöglicht nur „unsichere“ Passwörter (z.B. IA-5 wird größtenteils nicht unterstützt, außer auf Level 4). Deshalb sind die durch das US-Verteidigungsministerium formulierten Anforderungen bei Level 2 und darunter möglicherweise nicht zweckmäßig. Es ist zu beachten, dass ESS-Systeme eine Ausnahme bilden. ESS-Systeme unterstützen voraussichtlich CAC oder Biometrik - z.B. Zugangskarten. Der Planer sollte vorgeben, wo dies gemäß dem Standard/gemäß den Leitlinien der Industrie für bewährte Praxis möglich ist und vorbereitet sein, diese Entscheidung zu verteidigen, wenn dies nicht den IT-Standards des US-Verteidigungsministeriums entspricht.

Tabelle G-6 enthält einen Leitfaden zur Planung von Kontrollen in der Kontrollfamilie Identifizierung und Autorisierung (IA).

Tabelle G-6: Kontrollfamilie Identifizierung und Autorisierung (IA)

Sicherheitskontroll-ID	Bezeichnung und Leitfaden zur Planung von Sicherheitskontrollen
IA-2	Identifizierung und Authentifikation (Benutzer, die der Organisation angehören): Vieles davon kann nur auf Level 4 erreicht werden und vieles davon hängt vom Betriebssystem des PCs ab. Wo möglich, sollten vom Planer Angaben gemacht werden und er sollte darauf vorbereitet sein, die Nicht-Implementierung im Kontrollsystem zu rechtfertigen. Wann immer dies möglich ist, ist vorzuschreiben, dass das Kontrollsystem (für einen Zugang über den PC) CAC-Logins (oder ähnlich) unterstützt. Es ist zu beachten, dass ein Fernzugriff über die Plattform Enclave abgedeckt ist.
IA-3	Geräteidentifizierung und -authentifikation: Vieles davon kann nur auf Level 4 erreicht werden und vieles davon hängt vom Betriebssystem des PCs ab. Normalerweise kann eine Authentifikation zwischen Geräten zwischen PCs (Level 2 und 4) oder zwischen der Netzwerkhardware (Level 2, 3 oder 4) implementiert werden. Eine Authentifikation kann möglicherweise zwischen Controllern unterstützt werden, wobei nicht alle Controller diese Fähigkeit unterstützen werden und dies häufiger auf Level 4 als auf Level 2 unterstützt wird. Im Allgemeinen ist eine Geräteauthentifikation zwischen Controllern für Systeme mit GERINGEM Auswirkungsgrad nicht erforderlich, kann aber möglicherweise für Systeme mit MITTLEREM oder HOHEM Auswirkungsgrad erforderlich sein. Wo möglich, sollten vom Planer Angaben zur Authentifikation gemacht werden und er sollte darauf vorbereitet sein, die Nicht-Implementierung im Kontrollsystem zu rechtfertigen.
IA-5	Authentifikator-Management: Die Komponenten des Kontrollsystems können möglicherweise die durch das US-Verteidigungsministerium festgelegten Werte zur Passwortkomplexität nicht einhalten. Wo möglich, ist die Passwortkomplexität mit den durch das US-Verteidigungsministerium definierten Werten vorzuschreiben. Es ist zu fordern, dass voreingestellte Passwörter geändert werden können und dass Passwörter auf sichere Art und Weise übertragen werden. Bei PKI-Systemen sollten die Zertifikatspfade von der Plattform Enclave zur Verfügung gestellt werden.
IA-6 und IA-7	Rückmeldung Authentifikator und Authentifikation Kryptographie-Modul: Mit hoher Wahrscheinlichkeit nur Plattform Enclave und keine Unterstützung unterhalb dieses Levels. Hier ist möglicherweise die Zuarbeit/eine Begründung des Planers erforderlich.

Sicherheitskontroll-ID	Bezeichnung und Leitfaden zur Planung von Sicherheitskontrollen
IA-8	Identifizierung und Authentifikation (Benutzer, die nicht der Organisation angehören): Da dies Benutzer betrifft, die nicht der Organisation angehören, gilt diese Kontrolle im Allgemeinen nicht für Kontrollsysteme mit Ausnahme von ESS-Systemen. Dies wird möglicherweise von der Plattform Enclave geregelt (über Anforderungen zum PC-Login).

G-3.7 Kontrollfamilie Vorfallreaktion (IR)

Hinweis: Die Definition von "Vorfall" beinhaltet auch Störfälle ohne Sicherheitsbezug. Ein defekter Keilriemen ist ein "Vorfall", ebenso ein klemmendes Ventil oder ein nicht kalibrierter Sensor. Möglicherweise sind Beiträge des Planers zum Vorfallreaktionsplan erforderlich, um spezifische Aktionen des Kontrollsystems zu behandeln. So könnte die Reaktion auf einen erfolgreichen Angriff auf das Frontend beispielsweise sein, die Geräte auf manuelle bzw. Handschaltung umzustellen.

G-3.8 Kontrollfamilie Wartung (MA)

Tabelle G-7 enthält einen Leitfaden zur Planung von Kontrollen in der Kontrollfamilie Wartung (MA).

Tabelle G-7: Kontrollfamilie Wartung (MA)

Sicherheitskontroll-ID	Bezeichnung und Leitfaden zur Planung von Sicherheitskontrollen
MA-3	Wartungstools: Anforderung, dass Wartungstools für das Kontrollsystem (für die Wartung des Kontrollsystems benötigte Soft- oder Hardware - meist Engineering Tool Software) bereitgestellt wird.
MA-4	Wartung nicht vor Ort: Dies wird durch ein Betriebssystem-Login für den Einsatz der Engineering Tool Wartungssoftware gewährleistet.

G-3.9 Kontrollfamilie Medienschutz (MP)

Der Medienschutz wird nur bei der Plattform Enclave behandelt.

Tabelle G-8 enthält einen Leitfaden zur Planung von Kontrollen in der Kontrollfamilie Medienschutz (MP).

Tabelle G-8: Kontrollfamilie Medienschutz (MP)

Sicherheitskontroll-ID	Bezeichnung und Leitfaden zur Planung von Sicherheitskontrollen
MP-5	Medientransport: CCI-001027 (MP-5 (4)) stellt eine Anforderung an das Kontrollsystem, jedoch nur wenn sich das Kontrollsystem außerhalb eines "kontrollierten Bereichs" befindet, wobei "kontrollierte Bereiche" in CCI-001016 definiert werden als Bereiche, die für die Informationsverarbeitung freigegeben wurden. Per Definition muss ein Bereich für die Verarbeitung der für die Kontrollsysteme in diesem Bereich erforderlichen Informationen freigegeben sein. Für den Transport aus diesem Bereich heraus müssten die Daten durch von der Plattform Enclave bereitgestellte Tools verschlüsselt werden.

G-3.10 Kontrollfamilie physische Sicherheitssysteme und Schutz vor Umwelteinflüssen (PE)

Es ist zu beachten, dass Kontrollsysteme oft nicht zentralisiert sind und große Teile des Systems sich in Bereichen befinden, die nicht der Kontrolle der Organisation unterliegen. Dies hat Auswirkungen auf viele PE-Kontrollen. Insbesondere PE-16 kann nur für Bereiche erfüllt werden, die der Kontrolle der Organisation unterliegen. Im Allgemeinen werden diese von der Plattform Enclave erfüllt, aber unterhalb dieser Ebene ist die Umsetzung möglicherweise lückenhaft. Der Planer sollte nach Möglichkeit verschlossene Räume vorschreiben. Geräte auf Level 4, 3 und 2N sollten sich entweder in verschlossenen Räumen oder in verschlossenen Einhausungen befinden. Geräte auf Level 2, Level 1 und Level 0 liegen häufig in Mandantenbereichen außerhalb der Kontrolle der Organisation. Bei einigen Systemen kann es nötig sein, für einige Level 2 und Level 1 Controller verschließbare Einhausungen vorzuschreiben; dies muss jedoch gegen die nötige Zugangsmöglichkeit zu den Geräten für Wartungspersonal abgewogen werden. Im Allgemeinen bringt es kaum Vorteile, abschließbare Einhausungen vorzuschreiben, wenn die betreffenden Geräte vom Controllerstandort aus leicht zugänglich sind.

Der Großteil des Kontrollsystems befindet sich nicht in "normalen" Serverräumen. Für die normalen Serverräume werden die PE-Anforderungen in der Plattform Enclave erfüllt. Für den Rest des Kontrollsystems treffen die PE-Anforderungen (z.B. Temperatur- und Feuchtigkeitsanforderungen von PE-14) entweder nicht zu, oder sie werden durch Planungsvorgaben abgedeckt. Hinweis: Laut NIST-Leitfaden gelten mehrere PEs (z.B. PE-10, PE-12, PE-13, PE-14 und PE-15) nur für größere Serverräume, nicht für einzelne Komponenten. Diese werden durch die Plattform Enclave abgedeckt und sind im Kontrollsystem nicht zutreffend. Tabelle G-9 enthält einen Leitfaden zur Planung von Kontrollen in der Kontrollfamilie physische Sicherheitssysteme und Schutz vor Umwelteinflüssen (PE).

Tabelle G-9: Kontrollfamilie physische Sicherheitssysteme und Schutz vor Umwelteinflüssen (PE)

Sicherheitskontroll-ID	Bezeichnung und Leitfaden zur Planung von Sicherheitskontrollen
PE-4	Zugangskontrollen für Übertragungsmedium: Der Planer sollte physische Sicherheit für Netzwerkmedien vorschreiben und muss sich bezüglich der Anforderungen für Leitungsrohre mit dem Elektroplaner abstimmen. Hinweis: Auch außerhalb von Bereichen, die von der Organisation kontrolliert werden, kann physische Sicherheit erforderlich sein. Siehe SC-8.
PE-5	Zugangskontrollen für Ausgabegeräte: Hinweis: "Physische Ausgaben" für ein Kontrollsystem entsprechen der Position der kontrollierten Geräte, die ebenfalls gesichert werden müssen, sodass zusätzliche Anforderungen für die Komponenten des Kontrollsystems unwahrscheinlich sind
PE-9	Starkstromgeräte und Kabel: Bei Systemen, die eine redundante Stromversorgung erfordern, sollte der Planer sich mit dem Elektroplaner abstimmen. Die Schwachstelle in puncto Zuverlässigkeit sind häufig die kontrollierten Geräte. Wenn beispielsweise ein einzelnes Notstromaggregat benötigt wird, ist ein System mit 2 Generatoren - jeweils mit einem einzelnen Controller - zuverlässiger als ein einzelner Generator mit redundanten Controllern.
PE-11	Notstrom: Innerhalb des Kontrollsystems ist ein unterbrechungsfreie Stromversorgung (USV) entweder in den Spezifikationen für das Kontrollsystem oder durch Abstimmung mit den Elektrospezifikationen vorzusehen, wenn eine Notstromversorgung erforderlich ist. Im Frontend könnte dies entweder durch die Platform Enclave oder auch durch Anforderungen in der Spezifikation des Kontrollsystems erfüllt werden. Für die meisten Systeme mit NIEDRIGEN Auswirkungen wird diese Kontrolle nicht implementiert.
PE-16	Anlieferung und Abholung: Keine zusätzlichen kontrollspezifischen Leitlinien. Nutzen Sie den allgemeinen Leitfaden für Kontrollfamilien, den Sie über der Tabelle für diese Kontrolle finden.
PE-17	Alternativer Arbeitsplatz: PE-17 kann ausschließlich auf Level 4 angewendet werden - es gibt keinen möglichen "alternativen Arbeitsplatz" für PIT. Dies befindet sich alles in der Platform Enclave.

G-3.11 Kontrollfamilie Planung (PL)

Tabelle G-10 enthält einen Leitfaden zur Planung von Kontrollen in der Kontrollfamilie Planung (PL).

Tabelle G-10: Kontrollfamilie Planung (PL)

Sicherheitskontroll-ID	Bezeichnung und Leitfaden zur Planung von Sicherheitskontrollen
PL-2	Systemsicherheitsplan: Der Planer ist zwar nicht direkt für die System-sicherheit an sich verantwortlich, aber er muss Informationen bereitstellen, die in diesem Plan verwendet werden. So ist beispielsweise die Zeichnung zur Systemarchitektur Teil der Definition der Autorisierungsgrenze. Möglicherweise muss der Planer auch einen Beitrag zur Sicherheitseinstufung leisten, da er über Fachkenntnisse der zugrunde liegenden mechanischen/elektrischen Systeme verfügt und bei der Bewertung der Auswirkungen dieser Systeme auf die Mandanten der Kontrollsysteme behilflich sein kann
PL-4	Verhaltensregeln: Wie in KAPITEL 4 angemerkt, sollten soziale Medien vom Kontrollsystem aus überhaupt nicht zugänglich sein.
PL-7	Sicherheits-Betriebskonzept: Der Planer muss einen Beitrag zum Sicherheits-Betriebskonzept leisten, da die Bandbreite der möglichen betrieblichen Nutzungen durch die zugrunde liegenden Geräte, Betriebsabfolgen, Controllerauswahl und Möglichkeiten im Frontend bestimmt wird.
PL-8	Informationssicherheitsarchitektur: Die Vorlagen für die Systemarchitektur sind notwendige Beiträge zur Sicherheitsarchitektur. Abhängigkeiten von externen Systemen sollten auf in Minimum begrenzt werden oder gar nicht vorhanden sein.

G-3.12 Kontrollfamilie Programm-Management (PM)

Im allgemeinen ist der Planer nicht in die Projektplanung mit eingebunden. Die Verantwortung für PM-Kontrollen liegt daher nicht in erster Linie beim Planer; er muss jedoch Andere unterstützen.

Tabelle G-11 enthält einen Leitfaden zur Planung von Kontrollen in der Kontrollfamilie Programm-Management (PM).

Tabelle G-11: Kontrollfamilie Programm-Management (PM)

Sicherheitskontroll-ID	Bezeichnung und Leitfaden zur Planung von Sicherheitskontrollen
PM-3	Informationssicherheitsressourcen: Siehe Leitfaden für Kontrollfamilie PM und SA-2.
PM-5	Bestand Informationssystem: Der Anfangsbestand wird in Form eines Bestandsverzeichnisses vorgelegt.
PM-11	Definition des Betriebs / der betrieblichen Prozesse: Hier wird verlangt, dass "...erreichbare Schutzbedürfnisse umgesetzt werden", was die Mitwirkung des Planers erfordern kann.

G-3.13 Kontrollfamilie Personalsicherheit (PS)

Der Planer ist für keine der Personalsicherheitskontrollen verantwortlich.

G-3.14 Kontrollfamilie Risikobewertung (RA)

Die Implementierung der RA-Kontrollen liegt im Großen und Ganzen außerhalb des Verantwortungsbereichs des Planers.

Tabelle G-12 enthält einen Leitfaden zur Planung von Kontrollen in der Kontrollfamilie Risikobewertung (RA).

Tabelle G-12: Kontrollfamilie Risikobewertung (RA)

Sicherheitskontroll-ID	Bezeichnung und Leitfaden zur Planung von Sicherheitskontrollen
RA-3	Risikobewertung: Der Planer kennt sich mit dem Kontrollsystem und den zugrunde liegenden mechanischen/elektrischen Systemen sehr gut aus und muss daher möglicherweise bei der Erkennung von Risiken für die vom Kontrollsystem bedienten Mandanten behilflich sein.
RA-5	Schwachstellenprüfung: Die Prüfung kann auf Level 3 und 4 erfolgen, und die Prüfung des Kontrollsystems auf diesem Level sollte durch die Platform Enclave durchgeführt werden. Eine Prüfung unterhalb dieses Levels - insbesondere auf Level 1 - ist bestenfalls problematisch, da typische Kontrollsysteme derartige Scans nicht unterstützen und herkömmliche IT-zentrierte Scanning Tools beim Scannen eines Controllers häufig komplett versagen. Hinweis: Scanning Tools sollten sich innerhalb der Platform Enclave befinden; das Scannen von außerhalb der Platform Enclave bietet nur ein Schlupfloch für Angreifer. Der Planer muss Organisationen, die versuchen, RA-5 zu erfüllen, zu diesem Prozess möglicherweise Input geben. Siehe SC-7, SI-3

G-3.15 Kontrollfamilie Übernahme von Systemen und Diensten (SA)

Die NIST-Beschreibung zu "Externe Informationsdienste" (SA-9) macht deutlich, dass es sich um ein "externes Informationssystem" handelt, nicht um "externe Dienstleistungen (z.B. Auftragnehmer) auf diesem System"

Tabelle G-13 enthält einen Leitfaden zur Planung von Kontrollen in der Kontrollfamilie Übernahme von Systemen und Diensten (SA).

Tabelle G-13: Kontrollfamilie Übernahme von Systemen und Diensten (SA)

Sicherheitskontroll-ID	Bezeichnung und Leitfaden zur Planung von Sicherheitskontrollen
SA-2	Ressourcenverteilung: Der Planer muss zu diesem Prozess möglicherweise Input geben. Siehe PM-3
SA-4	Übernahmeverfahren: SA-4 wird zumindest teilweise erfüllt, indem der Planer sicherheitsspezifische Anforderungen in die Planung aufnimmt, darunter eine Abnahmeprüfung. Die Anforderungen für FIPS PUB 201-2 gelten wahrscheinlich nur für die Plattform Enclave, und der Planer muss möglicherweise eine Rechtfertigung dafür liefern, dass diese Anforderung im Kontrollsystem nicht erfüllt wird. Ähnlich verhält es sich bei den Anforderungen an den Planer, von denen viele bei einem handelsüblichen System wahrscheinlich nicht durchsetzbar sind. ESS-Systeme müssen auf Level 1 und 2 möglicherweise FIPS PUB 201-2 erfüllen.
SA-5	Dokumentation des Informationssystems: Der Planer sollte Vorlagen verlangen, in denen dokumentiert ist, was durch diese CCIs verlangt wird. Hinweis: Teile der erforderlichen Dokumentation sind möglicherweise nicht erhältlich, insbesondere für ein handelsübliches System.
SA-9	Externe Dienstleistungen für Informationssysteme: Im allgemeinen sollten Kontrollsysteme keine externen Informationssysteme verwenden, sodass diese Kontrolle nicht zutrifft. Sofern sie doch zutrifft, wird sie in der Plattform Enclave behandelt.
SA-10 und SA-11	Konfigurationsmanagement für Entwickler und Sicherheitsprüfung und -bewertung für Entwickler: SA-10, SA-11 sind bei handelsüblichen Systemen wahrscheinlich unmöglich. Der Planer muss vorgeben, was vorgegeben werden kann (was häufig zusätzliche Vorlagen erfordert), und erklären, was nicht vorgegeben werden kann. Hinweis: Die Kontrolle geht davon aus, dass der Entwickler bei der Implementierung und/oder beim Betrieb eine Rolle spielt - dies ist häufig nicht der Fall.

G-3.16 Kontrollfamilie System- und Kommunikationsschutz (SC)

Tabelle G-14 enthält einen Leitfaden zur Planung von Kontrollen in der Kontrollfamilie Übernahme von Systemen und Diensten (SA).

Tabelle G-14: Kontrollfamilie System- und Kommunikationsschutz (SC)

Sicherheitskontroll-ID	Bezeichnung und Leitfaden zur Planung von Sicherheitskontrollen
SC-2	Anwendungspartitionierung: Dies wird erfüllt, indem die Computerverwaltung herausgelöst wird, und durch Planungsvorgaben, die unterschiedliche Benutzerrechte innerhalb des Kontrollsystems verlangen (z.B. "Daten ansehen" und "Daten ändern").
SC-4	Informationen in gemeinsam genutzten Bereichen: In der Regel sind alle Kontrollsysteme dezidierte Hard- und Software; es gibt also keine gemeinsam genutzten Bereiche. Diese Kontrolle kann möglicherweise zu einem bestimmten Grad auf Level 4 zutreffen, wenn Computerressourcen gemeinsam genutzt werden.
SC-5	Schutz vor Denial of Service: Innerhalb de Kontrollsystems werden Denial-of-Service Angriffe abgefangen, indem das System so geplant wird, dass es nicht vom Netzwerk abhängig ist. Ansonsten ist dies eine Kontrolle für die Platform Enclave.
SC-7	Schutz der Außengrenze: Die Einrichtung einer Außengrenze sollte im Verantwortungsbereich der Platform Enclave liegen. Die Platform Enclave kann eine Überwachung/Verkehrskontrolle auf Level 3 und vielleicht an wichtigen Stellen bei Level 4 Komponenten durchführen. An anderen Stellen kann diese Kontrolle innerhalb des Kontrollsystems schwer zu erfüllen sein. Der Planer muss sich möglicherweise dafür rechtfertigen, dass er den Verkehr unterhalb von Level 3 nicht überwacht oder kontrolliert. Es ist möglicherweise nicht die beste Lösung, wenn das Kontrollsystem nach dem Verlust eines Geräts zum Schutz der Außengrenze auf einen "sicheren" Status zurückfällt, da ein Angriffsvektor so kontrollierte Geräte außer Betrieb setzen könnte, indem er das Gerät an der Außengrenze ausschaltet. Kontrollsysteme müssen unabhängig weiterlaufen, wenn Geräte an der Außengrenze ausfallen. Siehe Kommentare zu CP-12 und RA-5, SI-3, SC-24
SC-8	Übertragungsvertraulichkeit und -integrität: Hinweis: Laut NIST trifft dies wohl nur auf Informationen außerhalb einer sicheren physischen Grenze zu. Wenn diese Kontrolle nicht erfüllt werden kann, können andere physische Sicherungsmaßnahmen wie ein geschütztes Verteilsystem eingesetzt werden.
SC-10	Verlust der Netzwerkverbindung: Die Daten innerhalb eines Kontrollsystems werden oft ohne den Aufbau einer "Sitzung" übermittelt. Die meisten Kontrollsysteme verwenden Sitzungen nur für die Kommunikation innerhalb von Level 4.
SC-12	Einrichtung und Verwaltung von Kryptographieschlüsseln: Unterhalb von Level 4 ist bei Kontrollsystemen die Unterstützung für Kryptographieschlüssel stark eingeschränkt, und die Implementierung vieler solcher Kontrollen ist nicht zweckmäßig.

Sicherheitskontroll-ID	Bezeichnung und Leitfaden zur Planung von Sicherheitskontrollen
SC-13	Kryptographieschutz: Hinweis: NIST schreibt für diese Komponente keine Kryptographie vor, sondern beschreibt lediglich die Anforderungen für die Implementierung von Kryptographie, sofern diese irgendwo erforderlich sein sollte. Die große Mehrzahl der Kontrollsysteme sollte keine Informationen beinhalten, für die eine Verschlüsselung erforderlich wäre (und in den wenigen Fällen, wo dies überhaupt möglich ist, sollte der Planer prüfen, ob das Kontrollsystem wirklich über diese Informationen verfügen muss).
SC-15	Gemeinschaftliche EDV-Geräte: Kontrollsysteme sollten generell keine gemeinschaftlichen EDV-Geräte nutzen
SC-18	Mobilcode: Diese Kontrolle kann und sollte auf Level 4 vollständig umgesetzt werden. Auf dem Level darunter gibt es eine wichtige Unterscheidung zwischen "Mobilcode" und "Mobilcode-Technologien": Java ist eine "Mobilcode-Technologie", die von vielen Kontrollsystemen auf Level 2 (und möglicherweise auf anderen Leveln) genutzt wird, aber Java sollte nicht als "Mobilcode" (d.h. Code, der ohne Zutun des Benutzers heruntergeladen und ausgeführt wird) verwendet werden. Während Mobilcode-Technologien also unterhalb von Level 4 erlaubt sein können, sollte dies für Mobilcode nicht der Fall sein. Mobilcode-Einschränkungen innerhalb des Kontrollsystems sollten durch die Planungsspezifikationen abgedeckt werden. Viele Gebäudekontrollsysteme nutzen beispielsweise Java, um Webseiten an Kunden auszugeben. Diese Seiten stellen keinen Mobilcode dar. Das Herunterladen einer Java-Anwendung wäre dagegen ein Beispiel für Mobilcode.
SC-21 und SC-22	Sichere Namen-/Addressenauflösungs-Dienste (rekursiver Resolver oder Resolver mit Cache) und -Architektur sowie Vorkehrungen für Namen-/Adressauflösungs-Dienst: Diese Kontrollen treffen nur für die Plattform Enclave zu.
SC-23	Sitzungsauthentizität: Siehe Kommentare zu SC-10.
SC-24	Ausfall in bekanntem Zustand: Hier ist der Status der kontrollierten Geräte nach einem Ausfall des Kontrollsystems entscheidend. Der Planer sollte dies vorgeben, soweit erforderlich. Hinweis: Die Anforderung des US-Verteidigungsministeriums an einen "sicheren Status" ist möglicherweise nicht anwendbar und würde dann durch einen "abgesicherten Status" oder einen Status "Betriebsunterstützung" überschrieben. Die bei einem Ausfall gesicherten Daten können aufgrund der Art des Kontrollsystems begrenzt sein, und der Planer sollte vorgeben, was angemessen ist. Siehe CP-12.

Sicherheitskontroll-ID	Bezeichnung und Leitfaden zur Planung von Sicherheitskontrollen
SC-28	Schutz von inaktiven Informationen: Viele (wenn nicht alle) Kontrollsysteme verfügen über keine Daten, die im inaktiven Zustand geschützt werden müssen, da sie keine personenbezogenen oder vertraulichen Daten enthalten. Es ist jedoch zu beachten, dass elektronische Sicherheitssysteme häufig den Schutz inaktiver Daten verlangen.
SC-39	Prozessisolierung: Bei Kontrollsystemen, die mehrere Systeme kontrollieren, wird dies durch ein verteiltes Kontrollsystem erfüllt.
SC-41	Port- und E/A-Geräte-Zugriff: Siehe Kommentare zu CM-7

G-3.17 Kontrollfamilie System- und Informationsintegrität (SI)

Tabelle G-15 enthält einen Leitfaden zur Planung von Kontrollen in der Kontrollfamilie System- und Informationsintegrität (SI).

Tabelle G-15: Kontrollfamilie System- und Informationsintegrität (SI)

Sicherheitskontroll-ID	Bezeichnung und Leitfaden zur Planung von Sicherheitskontrollen
SI-2	Fehlerbehebung: Bei SI-2 geht es um Sicherheitsupdates und Patches für Soft- und Firmware. Dies kann (und sollte) zwar auf Level 3 und Level 4 angewendet werden, aber unterhalb von Level 3 dürfte diese Kontrolle größtenteils "nicht zutreffend" oder "nicht zweckmäßig" sein, da Updates relativ selten verfügbar sind und das Patchen von Controllern auf Level 1 und 2 sich schwierig gestaltet. Dies ist auf Level 1 und 2 auch größtenteils irrelevant, da Fehler bei den zugrunde liegenden Geräten, die wahrscheinlich viel häufiger und viel gravierender sind, ignoriert werden.
SI-3	Schutz gegen Schadcode: Dies sollte durch die Plattform Enclave an den Ein- und Ausgangspunkten umgesetzt werden. Periodische Scans innerhalb des Kontrollsystems können sich schwierig gestalten, und der Planer muss möglicherweise erklären, warum diese nicht umgesetzt wurden. Siehe RA-5, SC-7.

Sicherheitskontroll-ID	Bezeichnung und Leitfaden zur Planung von Sicherheitskontrollen
SI-4	Überwachung des Informationssystems: Gesammelte Daten können nur in der Plattform Enclave erhalten bleiben. Der Planer sollte einen Input für die Überwachungsziele und -methoden auf der Grundlage des Kontrollsystems, der zugrunde liegenden mechanischen/elektrischen Systeme und der Auswirkung auf Mandanten liefern. Hinweis: Hier geht es nicht um die operative Überwachung des Kontrollsystems (z.B. Anzeige von Grafiken, Empfang von Alarmen), sondern um eine Überwachung zu Sicherheitszwecken.
SI-7	Software-, Firmware- und Informationsintegrität: Tools zur Integritätsprüfung sind nur auf Level 4 möglich. Der Planer sollte Input dazu geben, was aufgrund der Möglichkeiten des Kontrollsystems angemessen ist, bzw. wo eine solche Kontrolle nicht machbar ist.
SI-10	Validierung von Informationseingaben: Dies könnte Netzwerkdaten, Sensormeldungen oder Benutzereingaben abdecken. Der Planer könnte zusätzliche Plausibilitätsprüfungen bei Sensormeldungen oder redundante Sensoren vorschreiben. Die Validierung von Benutzereingaben wäre wahrscheinlich über Richtlinien abzudecken. Eine Netzwerkvalidierung ist möglicherweise nur auf Level 4 möglich.
SI-11	Fehlerbehandlung: Um dies zu erfüllen, sollte der Planer Alarmmeldungen und andere Rückmeldungen des Kontrollsystems vorschreiben. Hinweis: Die Definition des US-Verteidigungsministeriums für "Empfänger" trifft bei einem Kontrollsystem nicht zu.
SI-16	Speicherschutz: Speicherschutz ist nur auf Level 4 sinnvoll.
SI-17	Ausfallsichere Verfahren: Siehe Kommentare zu SC-24 und CP-12, wo Ausfall eine der zu berücksichtigenden Bedingungen ist.

ANHANG H: CONTROL CORRELATION IDENTIFIER (CCI) - TABELLEN

H-1 EINLEITUNG

In diesem Anhang sind einige Tabellen aufgeführt, die bei der Einstufung der CCIs für ein System mit GERINGEN oder MITTLEREN Auswirkungen in einer Einrichtung des US-Verteidigungsministerium helfen sollen, wo es für die Plattform Enclave eine eigene Genehmigung gibt und die planerischen Mindestanforderungen für Cyber-Sicherheit beachtet wurden.

H-2 TABELLENSTRUKTUR UND INHALT

Nachfolgende Spalten werden für jede Tabelle festgelegt. Bitte beachten Sie, dass nicht in allen Tabellen alle Spalten verwendet werden:

- **CCI:** Die CCI-Nummer.
- **NIST SP 800-53 Kontrolltext-Indikator:** NIST SP 800-53 gliedert einzelne Kontrollelemente (z.B. einzelne Kontroll-IDs) in mehrere Elemente und Erweiterungen auf, wobei eine Erweiterung eine strengere Anforderung darstellt als die Grundregelung. Anhand des Kontrolltext-Indikators werden die einzelnen Elemente und Erweiterungen eindeutig gekennzeichnet. Ein Buchstabe zeigt ein Element innerhalb eines Kontrollelements auf, eine Zahl bezeichnet eine Erweiterung. Zum Beispiel ist „AC-17 (4)(b)“ das zweite Element der vierten Erweiterung zu AC-17.
- **CCI-Definition:** Die Definition des CCI.
- **Für Auswirkungsgrad mindestens:** Dieser CCI sollte angewendet werden, wenn die Auswirkung des Kontrollsystems diesem entspricht bzw. darüber hinaus geht.
- **Tabellenverweis:** Angabe, in welcher/welchen weitere(n) Tabelle(n) in diesem Anhang der CCI enthalten ist.
- **Gilt für Kontrollsystem:** Ist dieser CCI für ein Kontrollsystem anwendbar?
- **Begründung bei Nichtaufnahme:** Grund, weshalb der CCI nicht für Kontrollsysteme anwendbar ist
- **Begründung für Entfernung aus Grundvorgabe GERING:** Grund, weshalb der CCI aus der Grundvorgabe für ein Kontrollsystem mit GERINGEN Auswirkungen entfernt werden sollte.
- **Zuständigkeit:** Zeigt an, wer für die Durchführung der Kontrolle zuständig ist. Mehrfachnennungen sind möglich
- **Definition durch DoD:** Entweder hat das US-Verteidigungsministerium einen Orientierungswert für die Werte der „gewählten Organisation“ bestimmt, oder die Anleitung des US-Verteidigungsministerium zur Umsetzung gibt an, dass der CCI bereits durch bestehende Bestimmungen oder Vorschriften eingehalten wird.
Hinweis: Vorgesehene Definitionen oder Richtlinien können für ein Kontrollsystem möglicherweise nicht relevant sein - die Definitionen der Organisation wurden aus dem Blickwinkel eines traditionellen Informationssystems festgelegt, nicht für ein Kontrollsystem.

- **Planer:** Der Planer spielt bei diesem CCI eine Rolle. Entweder muss der Planer Planungsvorgaben erstellen, um eine Anforderung an das Kontrollsystem selbst abzudecken, oder der Planer muss anderen Vorgaben bezüglich der Umsetzung oder der mangelnden Umsetzbarkeit des CCI machen (normalerweise weil der CCI in Anbetracht eines IT Systems geschrieben wurde, nicht eines Kontrollsystems).
- **Nicht Planer:** Der CCI liegt außerhalb der Zuständigkeit des Planers und liegt im Verantwortungsbereich eines Anderen - normalerweise des Systemeigentümers (SO). Dies verringert nicht die Wichtigkeit dieser CCIs, aber da diese CCIs nicht im Zuständigkeitsbereich des Planers liegen, befinden sie sich außerhalb des Geltungsbereichs dieser UFC.
- **Platform Enclave:** Der CCI enthält eine Anforderung, von der angenommen wird, dass diese in der Platform Enclave umgesetzt werden soll und vom Kontrollsystem übernommen wird, oder sie ist größtenteils bei der Platform Enclave umgesetzt, ist jedoch auch innerhalb des Field Control Systems erforderlich. Hinweis: Sollte es keine Platform Enclave geben, dann befinden sich die CCIs, die in der Kategorie „Platform Enclave“ aufgeführt sind, stattdessen in der Kategorie „Nicht Planer“.
- **Nicht zweckmäßig:** Der CCI ist für die volle Umsetzung in einem Kontrollsystem nicht zweckmäßig, kann jedoch in beschränktem Umfang für mindestens einen Teil des Kontrollsystems angewendet werden. Meist können die CCIs, welche nur für einen Teil des Kontrollsystems angewendet werden können, auf Level 4 der Struktur umgesetzt werden, es wäre jedoch unerschwinglich aufwändig, diese auf Level 1 oder 2 umzusetzen. Hinweis: Die Bewertung „unerschwinglich aufwändig“ basiert auf einem typischen Kontrollsystem mit GERINGEN Auswirkungen - für ein MITTLERES oder HOHES System kann es sinnvoll sein, diese Kontrollen auf allen möglichen Ebenen umzusetzen, auch wenn dies erhebliche Kosten und Aufwand mit sich bringt.

H-3 ANMERKUNGEN ZU CCI-TABELLEN

H-3.1 Von der Platform Enclave vererbte Kontrollen

Es ist zu beachten, dass nicht alle Kontrollen, die von der Platform Enclave übernommen werden können, **zwangsläufig** als solche kenntlich gemacht wurden - einige Kontrollen, die als „Nicht Planer“ bezeichnet sind, können tatsächlich auf der Platform Enclave umgesetzt werden und das Kontrollsystem übernimmt von da.

H-3.2 CCIs in mehreren Tabellen

Bitte beachten Sie, dass einige CCIs in mehreren Tabellen vorkommen, normalerweise „Planer und Platform Enclave“ oder „Platform Enclave und Andere“. Beispielsweise sollte das Scannen (RA-5) auf der Ebene der Platform Enclave erfolgen und nicht im Kontrollsystem. Der Planer sollte jedoch vielleicht Angaben zur Auswahl der Scanning Tools, die für das Kontrollsystem geeignet sind, machen. Der Zweck dieser Tabellen ist es, die Zuständigkeiten für jede Kontrolle aufzugliedern, so dass eine bestimmte Person/Rolle nicht alle Tabellen durchsehen müsste, um zu bestimmen, was zu tun ist.

H-4 BESCHREIBUNGEN ZU DEN CCI-TABELLEN

Mehrere CCI Tabellen sind in diesem Anhang aufgeführt. Jede enthält die CCIs, die, wie beschreiben, bestimmte Merkmale erfüllen. Eine elektronische Version der CCI-Tabellen im Excel-Format steht auf der Internetseite RMF Knowledge Service zur Verfügung.

H-4.1 CCI-Übersichtstabelle

In Tabelle H-1 sind alle CCIs zusammengefasst, die für ein MITTLERES oder niedrigeres Kontrollsystem angewendet werden können, auf Grundlage der NIST 800-82. In dieser Tabelle ist auch aufgezeigt, in welchen weiteren Tabellen die einzelnen CCIs aufzufinden sind.

H-4.2 Für Kontrollsysteme ungeeignete CCIs

In Tabelle H-2 sind CCIs aufgeführt, die (unter der Annahme, dass die Mindestanforderungen an Cyber-Sicherheit laut KAPITEL 4 eingehalten wurden) niemals für ein Kontrollsystem anzuwenden sind, und liefert eine Begründung, weshalb diese nicht angewendet werden.

H-4.3 CCIs, die aus der Grundvorgabe für Kontrollsysteme mit GERINGEN Auswirkungen entfernt wurden

Tabelle H-3 enthält CCIs, die in NIST 800-82 in der Grundvorgabe für GERINGE Auswirkungen aufgeführt werden, die jedoch nicht für ein Kontrollsystem mit GERINGEN Auswirkungen zutreffen, und liefert eine Begründung. Bitte beachten Sie, dass die CCIs hier zwar als GERING aufgeführt werden, jedoch nicht bei GERINGEN Auswirkungen angewendet werden.

H-4.4 Planer-CCIs

Verwenden Sie Tabelle H-4 für ein System mit GERINGEN Auswirkungen, um die CCIs, die in der Planung behandelt werden sollten, zu ermitteln. Verwenden Sie sowohl Tabelle H-4 als auch Tabelle H-5 für ein System mit MITTLEREN Auswirkungen, um die CCIs, die in der Planung behandelt werden sollten, zu ermitteln. In vielen Fällen finden Sie eine Anleitung, wie bestimmte Sicherheitskontrollen in der Planung zu thematisieren sind, in 0.

H-4.5 Platform Enclave CCIs

In Tabelle H-6 sind CCIs in der Kategorie „Platform Enclave“ aufgeführt, die für ein System mit GERINGEN oder MITTLEREN Auswirkungen angewendet werden sollten. In Tabelle H-7 sind CCIs in der Kategorie „Platform Enclave“ aufgeführt, die für ein System mit MITTLEREN Auswirkungen (höher als GERING) angewendet werden sollten.

Während die Implementierung der Platform Enclave nicht in der Verantwortung des Planers liegt (ein Schlüsselaspekt der Platform Enclave ist die Tatsache, dass sie ein Standardverfahren ist, dass über mehrere Kontrollsysteme umgesetzt werden kann), müssen sich diejenigen, die für die Platform Enclave zuständig sind, über CCIs im Klaren sein, von denen das Kontrollsystem erwartet, dass diese von der Platform Enclave übernommen werden.

H-5 CCI-TABELLEN

Tabelle H-1: Überblick über CCIs für Systeme mit GERINGEN und MITTLEREN Auswirkungen				
CCI #	800-53 Kontrolltext-Indikator	Für Auswirkungsgrad mindestens	Tabellenverweis	Gilt für Kontrollsystem?
CCI 002107	AC-1 (a)	GERING	Keine (Nicht Planer)	WAHR
CCI 002108	AC-1 (a)	GERING	Keine (Nicht Planer)	WAHR
CCI 000001	AC-1 (a) (1)	GERING	Keine (Nicht Planer)	WAHR
CCI 000002	AC-1 (a) (1)	GERING	Keine (Nicht Planer)	WAHR
CCI 002106	AC-1 (a) (1)	GERING	Keine (Nicht Planer)	WAHR
CCI 000004	AC-1 (a) (2)	GERING	Keine (Nicht Planer)	WAHR
CCI 000005	AC-1 (a) (2)	GERING	Keine (Nicht Planer)	WAHR
CCI 002109	AC-1 (a) (2)	GERING	Keine (Nicht Planer)	WAHR
CCI 000003	AC-1 (b) (1)	GERING	Keine (Nicht Planer)	WAHR
CCI 001545	AC-1(b)(1)	GERING		WAHR
CCI 000006	AC-1(b)(2)	GERING	Keine (Nicht Planer)	WAHR
CCI 001546	AC-1(b)(2)	GERING		WAHR
CCI 002110	AC-2(a)	GERING	Tabelle H-4 (Planer)	WAHR
CCI 002111	AC-2(a)	GERING	Keine (Nicht Planer)	WAHR
CCI 002112	AC-2(b)	GERING	Keine (Nicht Planer)	WAHR
CCI 000008	AC-2(c)	GERING	Keine (Nicht Planer)	WAHR
CCI 002113	AC-2(c)	GERING	Keine (Nicht Planer)	WAHR
CCI 002115	AC-2(d)	GERING	Keine (Nicht Planer)	WAHR
CCI 002116	AC-2(d)	GERING	Keine (Nicht Planer)	WAHR
CCI 002117	AC-2(d)	GERING	Keine (Nicht Planer)	WAHR
CCI 002118	AC-2(d)	GERING	Keine (Nicht Planer)	WAHR
CCI 002119	AC-2(d)	GERING	Keine (Nicht Planer)	WAHR
CCI 002120	AC-2(e)	GERING	Keine (Nicht Planer)	WAHR
CCI 000010	AC-2(e)	GERING	Keine (Nicht Planer)	WAHR
CCI 000011	AC-2(f)	GERING	Keine (Nicht Planer)	WAHR
CCI 002121	AC-2(f)	GERING	Keine (Nicht Planer)	WAHR
CCI 002122	AC-2(g)	GERING	Keine (Nicht Planer)	WAHR
CCI 002123	AC-2(h)(1)	GERING	Keine (Nicht Planer)	WAHR
CCI 002124	AC-2(h)(2)	GERING	Keine (Nicht Planer)	WAHR
CCI 002125	AC-2(h)(3)	GERING	Keine (Nicht Planer)	WAHR
CCI 002126	AC-2(i)(1)	GERING	Keine (Nicht Planer)	WAHR
CCI 002127	AC-2(i)(2)	GERING	Keine (Nicht Planer)	WAHR
CCI 002128	AC-2(i)(3)	GERING	Keine (Nicht Planer)	WAHR
CCI 000012	AC-2(j)	GERING	Keine (Nicht Planer)	WAHR
CCI 001547	AC-2(j)	GERING		WAHR
CCI 002129	AC-2(k)	GERING	Keine (Nicht Planer)	WAHR
CCI 000015	AC-2(1)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-001682	AC-2(2)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-000016	AC-2(2)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-001361	AC-2(2)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-001365	AC-2(2)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-000017	AC-2(3)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR

Tabelle H-1: Überblick über CCIs für Systeme mit GERINGEN und MITTLEREN Auswirkungen				
CCI #	800-53 Kontrolltext-Indikator	Für Auswirkungsgrad mindestens	Tabellenverweis	Gilt für Kontrollsystem?
CCI-000217	AC-2(3)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-000018	AC-2(4)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-001403	AC-2(4)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-001404	AC-2(4)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-001405	AC-2(4)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-002130	AC-2(4)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-002131	AC-2(4)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-001683	AC-2(4)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-001684	AC-2(4)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-001685	AC-2(4)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-001686	AC-2(4)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-002132	AC-2(4)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-000213	AC-3	GERING	Tabelle H-4 (Planer)	WAHR
CCI-001368	AC-4	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-001414	AC-4	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-001548	AC-4	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-001549	AC-4	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-001550	AC-4	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-001551	AC-4	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-000036	AC-5(a)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-002219	AC-5(a)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-001380	AC-5(b)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-002220	AC-5(c)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-000225	AC-6	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-001558	AC-6(1)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-002221	AC-6(1)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-002222	AC-6(1)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-002223	AC-6(1)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-000039	AC-6(2)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-001419	AC-6(2)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-002226	AC-6(5)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-002227	AC-6(5)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-002234	AC-6(9)	MITTEL	Tabelle H-5 (Planer)	WAHR

Tabelle H-1: Überblick über CCIs für Systeme mit GERINGEN und MITTLEREN Auswirkungen				
CCI #	800-53 Kontrolltext-Indikator	Für Auswirkungsgrad mindestens	Tabellenverweis	Gilt für Kontrollsystem?
CCI-002235	AC-6(10)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-000043	AC-7(a)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-000044	AC-7(a)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-001423	AC-7(a)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-002236	AC-7(b)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-002237	AC-7(b)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-002238	AC-7(b)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-000048	AC-8(a)	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-002247	AC-8(a)	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-002243	AC-8(a)(1)	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-002244	AC-8(a)(2)	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-002245	AC-8(a)(3)	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-002246	AC-8(a)(4)	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-000050	AC-8(b)	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-001384	AC-8(c)(1)	GERING		FALSCH
CCI-002248	AC-8(c)(1)	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-001385	AC-8(c)(2)	GERING		FALSCH
CCI-001386	AC-8(c)(2)	GERING		FALSCH
CCI-001387	AC-8(c)(2)	GERING		FALSCH
CCI-001388	AC-8(c)(3)	GERING		FALSCH
CCI-002332	AC-10(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-000058	AC-11(a)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-000059	AC-11(a)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-000056	AC-11(b)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-000060	AC-11(1)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-002360	AC-12	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-002361	AC-12	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-000061	AC-14(a)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-000232	AC-14(b)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-000063	AC-17(a)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002310	AC-17(a)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002311	AC-17(a)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002312	AC-17(a)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-000065	AC-17(b)	GERING	Tabelle H-6 (Enclave)	WAHR

Tabelle H-1: Überblick über CCIs für Systeme mit GERINGEN und MITTLEREN Auswirkungen				
CCI #	800-53 Kontrolltext-Indikator	Für Auswirkungsgrad mindestens	Tabellenverweis	Gilt für Kontrollsystem?
CCI-000067	AC-17(1)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-002314	AC-17(1)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-000068	AC-17(2)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-001453	AC-17(2)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-000069	AC-17(3)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-001561	AC-17(3)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-002315	AC-17(3)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-000070	AC-17(4)(a)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-002316	AC-17(4)(a)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-002317	AC-17(4)(a)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-002318	AC-17(4)(a)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-002319	AC-17(4)(b)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-002320	AC-17(4)(b)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-001438	AC-18(a)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-001439	AC-18(a)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-002323	AC-18(a)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-001441	AC-18(b)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-001443	AC-18(1)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-001444	AC-18(1)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-000082	AC-19(a)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-000083	AC-19(a)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002325	AC-19(a)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002326	AC-19(a)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-000084	AC-19(b)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002231	AC-19(5)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-002329	AC-19(5)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-002330	AC-19(5)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-000093	AC-20(a)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002333	AC-20(1)(a)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-002334	AC-20(1)(a)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-002335	AC-20(1)(a)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-002336	AC-20(1)(a)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-002337	AC-20(1)(a)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-000097	AC-20(2)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-000098	AC-21(a)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-001470	AC-21(a)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-001471	AC-21(b)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-001472	AC-21(b)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-001473	AC-22(a)	GERING		FALSCH
CCI-001474	AC-22(b)	GERING		FALSCH
CCI-001475	AC-22(c)	GERING		FALSCH
CCI-001476	AC-22(d)	GERING		FALSCH
CCI-001477	AC-22(d)	GERING		FALSCH
CCI-001478	AC-22(e)	GERING		FALSCH
CCI-002048	AT-1(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-002049	AT-1(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-000100	AT-1(a)(1)	GERING	Keine (Nicht Planer)	WAHR
CCI-000101	AT-1(a)(1)	GERING	Keine (Nicht Planer)	WAHR

Tabelle H-1: Überblick über CCIs für Systeme mit GERINGEN und MITTLEREN Auswirkungen				
CCI #	800-53 Kontrolltext-Indikator	Für Auswirkungsgrad mindestens	Tabellenverweis	Gilt für Kontrollsystem?
CCI-000103	AT-1(a)(2)	GERING	Keine (Nicht Planer)	WAHR
CCI-000104	AT-1(a)(2)	GERING	Keine (Nicht Planer)	WAHR
CCI-000102	AT-1(b)(1)	GERING		WAHR
CCI-001564	AT-1(b)(1)	GERING		WAHR
CCI-000105	AT-1(b)(2)	GERING	Keine (Nicht Planer)	WAHR
CCI-001565	AT-1(b)(2)	GERING		WAHR
CCI-000106	AT-2(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-000112	AT-2(b)	GERING		WAHR
CCI-001479	AT-2(c)	GERING		WAHR
CCI-001480	AT-2	GERING		WAHR
CCI-002055	AT-2(2)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-000108	AT-3(a)	GERING		WAHR
CCI-000109	AT-3(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-000110	AT-3(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-000111	AT-3(c)	GERING		WAHR
CCI-000113	AT-4(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-000114	AT-4(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-001336	AT-4(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-001337	AT-4(b)	GERING		WAHR
CCI-001930	AU-1(a)	GERING		WAHR
CCI-001931	AU-1(a)	GERING		WAHR
CCI-000117	AU-1(a)(1)	GERING	Keine (Nicht Planer)	WAHR
CCI-001832	AU-1(a)(1)	GERING	Keine (Nicht Planer)	WAHR
CCI-000120	AU-1(a)(2)	GERING	Keine (Nicht Planer)	WAHR
CCI-001834	AU-1(a)(2)	GERING	Keine (Nicht Planer)	WAHR
CCI-000119	AU-1(b)(1)	GERING	Keine (Nicht Planer)	WAHR
CCI-001569	AU-1(b)(1)	GERING		WAHR
CCI-000122	AU-1(b)(2)	GERING	Keine (Nicht Planer)	WAHR
CCI-001570	AU-1(b)(2)	GERING		WAHR
CCI-000123	AU-2(a)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-001571	AU-2(a)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-000124	AU-2(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-000125	AU-2(c)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-000126	AU-2(d)	GERING	Keine (Nicht Planer)	WAHR
CCI-001485	AU-2(d)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-001484	AU-2(d)	GERING		WAHR
CCI-000127	AU-2(3)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-001486	AU-2(3)	MITTEL		WAHR
CCI-000130	AU-3	GERING	Tabelle H-4 (Planer)	WAHR
CCI-000131	AU-3	GERING	Tabelle H-4 (Planer)	WAHR
CCI-000132	AU-3	GERING	Tabelle H-4 (Planer)	WAHR
CCI-000133	AU-3	GERING	Tabelle H-4 (Planer)	WAHR
CCI-000134	AU-3	GERING	Tabelle H-4 (Planer)	WAHR
CCI-001487	AU-3	GERING	Tabelle H-4 (Planer)	WAHR
CCI-000135	AU-3(1)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-001488	AU-3(1)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-001848	AU-4	GERING	Tabelle H-4 (Planer)	WAHR
CCI-001849	AU-4	GERING	Tabelle H-4 (Planer)	WAHR

Tabelle H-1: Überblick über CCIs für Systeme mit GERINGEN und MITTLEREN Auswirkungen				
CCI #	800-53 Kontrolltext-Indikator	Für Auswirkungsgrad mindestens	Tabellenverweis	Gilt für Kontrollsystem?
CCI-001850	AU-4(1)	GERING	Keine (Nicht Planer)	WAHR
CCI-001851	AU-4(1)	GERING	Keine (Nicht Planer)	WAHR
CCI-000139	AU-5(a)	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-001572	AU-5(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-000140	AU-5(b)	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-001490	AU-5(b)	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-000148	AU-6(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-000151	AU-6(a)	GERING		WAHR
CCI-001862	AU-6(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-000149	AU-6(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-001863	AU-6(b)	GERING		WAHR
CCI-001864	AU-6(1)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-001865	AU-6(1)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-000153	AU-6(3)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-001875	AU-7(a)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-001876	AU-7(a)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-001877	AU-7(a)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-001878	AU-7(a)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-001879	AU-7(a)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-001880	AU-7(a)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-001881	AU-7(b)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-001882	AU-7(b)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-000158	AU-7(1)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-001883	AU-7(1)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-000159	AU-8(a)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-001889	AU-8(b)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-001890	AU-8(b)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-001888	AU-8(b)	GERING		WAHR
CCI-001891	AU-8(1)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-001892	AU-8(1)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-002046	AU-8(1)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-000161	AU-8(1)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-001492	AU-8(1)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-000162	AU-9	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-000163	AU-9	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-000164	AU-9	GERING	Tabelle H-6 (Enclave)	WAHR

Tabelle H-1: Überblick über CCIs für Systeme mit GERINGEN und MITTLEREN Auswirkungen				
CCI #	800-53 Kontrolltext-Indikator	Für Auswirkungsgrad mindestens	Tabellenverweis	Gilt für Kontrollsystem?
CCI-001493	AU-9	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-001494	AU-9	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-001495	AU-9	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-001894	AU-9(4)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-001351	AU-9(4)(a)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-000167	AU-11	GERING	Keine (Nicht Planer)	WAHR
CCI-000168	AU-11	GERING		WAHR
CCI-000169	AU-12(a)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-001459	AU-12(a)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-000171	AU-12(b)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-001910	AU-12(b)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-000172	AU-12(c)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-002061	CA-1(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-002062	CA-1(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-000239	CA-1(a)(1)	GERING	Keine (Nicht Planer)	WAHR
CCI-000240	CA-1(a)(1)	GERING	Keine (Nicht Planer)	WAHR
CCI-000242	CA-1(a)(2)	GERING	Keine (Nicht Planer)	WAHR
CCI-000243	CA-1(a)(2)	GERING	Keine (Nicht Planer)	WAHR
CCI-000238	CA-1(b)(1)	GERING		WAHR
CCI-000241	CA-1(b)(1)	GERING		WAHR
CCI-000244	CA-1(b)(2)	GERING	Keine (Nicht Planer)	WAHR
CCI-001578	CA-1(b)(2)	GERING		WAHR
CCI-000245	CA-2(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-000246	CA-2(a)(1)	GERING	Keine (Nicht Planer)	WAHR
CCI-000247	CA-2(a)(2)	GERING		WAHR
CCI-000248	CA-2(a)(3)	GERING	Keine (Nicht Planer)	WAHR
CCI-002070	CA-2(a)(3)	GERING	Keine (Nicht Planer)	WAHR
CCI-000251	CA-2(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-000252	CA-2(b)	GERING		WAHR
CCI-000253	CA-2(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-000254	CA-2(d)	GERING	Keine (Nicht Planer)	WAHR
CCI-002071	CA-2(d)	GERING		WAHR
CCI-000255	CA-2(1)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-002063	CA-2(1)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-000257	CA-3(a)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-000258	CA-3(b)	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-000259	CA-3(b)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-000260	CA-3(b)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002083	CA-3(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-002084	CA-3(c)	GERING		WAHR
CCI-002080	CA-3(5)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-002081	CA-3(5)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-002082	CA-3(5)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-000264	CA-5(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-000265	CA-5(b)	GERING		WAHR
CCI-000266	CA-5(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-000270	CA-6(a)	GERING	Keine (Nicht Planer)	WAHR

Tabelle H-1: Überblick über CCIs für Systeme mit GERINGEN und MITTLEREN Auswirkungen				
CCI #	800-53 Kontrolltext-Indikator	Für Auswirkungsgrad mindestens	Tabellenverweis	Gilt für Kontrollsystem?
CCI-000271	CA-6(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-000272	CA-6(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-000273	CA-6(c)	GERING		WAHR
CCI-002087	CA-7(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-002088	CA-7(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-002089	CA-7(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-000279	CA-7(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-002090	CA-7(d)	GERING	Keine (Nicht Planer)	WAHR
CCI-002091	CA-7(e)	GERING	Keine (Nicht Planer)	WAHR
CCI-002092	CA-7(f)	GERING	Keine (Nicht Planer)	WAHR
CCI-000280	CA-7(g)	GERING	Keine (Nicht Planer)	WAHR
CCI-000281	CA-7(g)	GERING	Keine (Nicht Planer)	WAHR
CCI-001581	CA-7(g)	GERING	Keine (Nicht Planer)	WAHR
CCI-000274	CA-7	GERING	Keine (Nicht Planer)	WAHR
CCI-000282	CA-7(1)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-002085	CA-7(1)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-002102	CA-9(a)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-002101	CA-9(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-002103	CA-9(b)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-002104	CA-9(b)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-002105	CA-9(b)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-001821	CM-1(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-001824	CM-1(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-000287	CM-1(a)(1)	GERING	Keine (Nicht Planer)	WAHR
CCI-001822	CM-1(a)(1)	GERING	Keine (Nicht Planer)	WAHR
CCI-000290	CM-1(a)(2)	GERING	Keine (Nicht Planer)	WAHR
CCI-001825	CM-1(a)(2)	GERING	Keine (Nicht Planer)	WAHR
CCI-000286	CM-1(b)(1)	GERING	Keine (Nicht Planer)	WAHR
CCI-000289	CM-1(b)(1)	GERING	Keine (Nicht Planer)	WAHR
CCI-000292	CM-1(b)(2)	GERING	Keine (Nicht Planer)	WAHR
CCI-001584	CM-1(b)(2)	GERING	Keine (Nicht Planer)	WAHR
CCI-000293	CM-2	GERING	Tabelle H-4 (Planer)	WAHR
CCI-000295	CM-2	GERING	Keine (Nicht Planer)	WAHR
CCI-000296	CM-2(1)(a)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-001497	CM-2(1)(a)	MITTEL		WAHR
CCI-000297	CM-2(1)(b)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-001585	CM-2(1)(b)	MITTEL		WAHR
CCI-000298	CM-2(1)(c)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-000299	CM-2(1)(c)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-000304	CM-2(3)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-001736	CM-2(3)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-001739	CM-2(7)a	MITTEL		FALSCH
CCI-001737	CM-2(7)a	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-001738	CM-2(7)a	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-001815	CM-2(7)b	MITTEL		FALSCH
CCI-001816	CM-2(7)b	MITTEL		FALSCH
CCI-000313	CM-3(a)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-000314	CM-3(b)	MITTEL	Keine (Nicht Planer)	WAHR

Tabelle H-1: Überblick über CCIs für Systeme mit GERINGEN und MITTLEREN Auswirkungen				
CCI #	800-53 Kontrolltext-Indikator	Für Auswirkungsgrad mindestens	Tabellenverweis	Gilt für Kontrollsystem?
CCI-001740	CM-3(b)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-001741	CM-3(c)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-001819	CM-3(d)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-000316	CM-3(e)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-002056	CM-3(e)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-000318	CM-3(f)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-000319	CM-3(g)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-000320	CM-3(g)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-000321	CM-3(g)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-001586	CM-3(g)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-000327	CM-3(2)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-000328	CM-3(2)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-000329	CM-3(2)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-000333	CM-4	GERING	Keine (Nicht Planer)	WAHR
CCI-000338	CM-5	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-000339	CM-5	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-000340	CM-5	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-000341	CM-5	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-000342	CM-5	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-000343	CM-5	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-000344	CM-5	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-000345	CM-5	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-000363	CM-6(a)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-000364	CM-6(a)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-000365	CM-6(a)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-001588	CM-6(a)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-000366	CM-6(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-000367	CM-6(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-000368	CM-6(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-000369	CM-6(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-001755	CM-6(c)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-001756	CM-6(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-001502	CM-6(d)	GERING	Keine (Nicht Planer)	WAHR
CCI-001503	CM-6(d)	GERING	Keine (Nicht Planer)	WAHR
CCI-000381	CM-7(a)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-000380	CM-7(b)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-000382	CM-7(b)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-001760	CM-7(1)(a)	GERING		WAHR
CCI-000384	CM-7(1)(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-001761	CM-7(1)(b)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-001762	CM-7(1)(b)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-001592	CM-7(2)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-001763	CM-7(2)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-001764	CM-7(2)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-001772	CM-7(5)a	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-001773	CM-7(5)a	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-001774	CM-7(5)b	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-001775	CM-7(5)c	MITTEL	Keine (Nicht Planer)	WAHR

Tabelle H-1: Überblick über CCIs für Systeme mit GERINGEN und MITTLEREN Auswirkungen				
CCI #	800-53 Kontrolltext-Indikator	Für Auswirkungsgrad mindestens	Tabellenverweis	Gilt für Kontrollsystem?
CCI-001777	CM-7(5)c	MITTEL	Keine (Nicht Planer)	WAHR
CCI-000389	CM-8(a)(1)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-000392	CM-8(a)(2)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-000395	CM-8(a)(3)	GERING	Keine (Nicht Planer)	WAHR
CCI-000398	CM-8(a)(4)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-000399	CM-8(a)(4)	GERING	Keine (Nicht Planer)	WAHR
CCI-001779	CM-8(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-001780	CM-8(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-000408	CM-8(1)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-000409	CM-8(1)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-000410	CM-8(1)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-000415	CM-8(3)(a)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-000416	CM-8(3)(a)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-001783	CM-8(3)(b)	MITTEL		WAHR
CCI-001784	CM-8(3)(b)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-000419	CM-8(5)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-000421	CM-9(a)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-000423	CM-9(a)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-001790	CM-9(b)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-001792	CM-9(b)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-001793	CM-9(b)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-001795	CM-9(b)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-000424	CM-9(c)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-000426	CM-9(c)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-001796	CM-9(c)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-001798	CM-9(c)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-001799	CM-9(d)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-001801	CM-9(d)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-001726	CM-10(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-001727	CM-10(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-001728	CM-10(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-001729	CM-10(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-001730	CM-10(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-001731	CM-10(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-001802	CM-10(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-001803	CM-10(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-001732	CM-10(c)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-001733	CM-10(c)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-001804	CM-11(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-001805	CM-11(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-001806	CM-11(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-001807	CM-11(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-001808	CM-11(c)	GERING		WAHR
CCI-001809	CM-11(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-000438	CP-1(a)(1)	GERING		WAHR
CCI-000439	CP-1(a)(1)	GERING	Keine (Nicht Planer)	WAHR
CCI-002825	CP-1(a)(1)	GERING	Keine (Nicht Planer)	WAHR
CCI-000441	CP-1(a)(2)	GERING		WAHR

Tabelle H-1: Überblick über CCIs für Systeme mit GERINGEN und MITTLEREN Auswirkungen				
CCI #	800-53 Kontrolltext-Indikator	Für Auswirkungsgrad mindestens	Tabellenverweis	Gilt für Kontrollsystem?
CCI-001597	CP-1(a)(2)	GERING	Keine (Nicht Planer)	WAHR
CCI-002826	CP-1(a)(2)	GERING	Keine (Nicht Planer)	WAHR
CCI-000437	CP-1(b)(1)	GERING		WAHR
CCI-000440	CP-1(b)(1)	GERING	Keine (Nicht Planer)	WAHR
CCI-001596	CP-1(b)(2)	GERING		WAHR
CCI-001598	CP-1(b)(2)	GERING	Keine (Nicht Planer)	WAHR
CCI-000444	CP-2(a)(1)	GERING		FALSCH
CCI-000443	CP-2(a)(1)	GERING	Tabelle H-3 (entfernt aus GERING)	WAHR
CCI-000445	CP-2(a)(1)	GERING	Keine (Nicht Planer)	WAHR
CCI-000446	CP-2(a)(2)	GERING	Keine (Nicht Planer)	WAHR
CCI-000447	CP-2(a)(2)	GERING	Keine (Nicht Planer)	WAHR
CCI-000448	CP-2(a)(2)	GERING	Keine (Nicht Planer)	WAHR
CCI-000449	CP-2(a)(3)	GERING	Keine (Nicht Planer)	WAHR
CCI-000451	CP-2(a)(4)	GERING		FALSCH
CCI-000453	CP-2(a)(4)	GERING		FALSCH
CCI-000455	CP-2(a)(4)	GERING		FALSCH
CCI-000450	CP-2(a)(4)	GERING	Tabelle H-3 (entfernt aus GERING)	WAHR
CCI-000452	CP-2(a)(4)	GERING	Tabelle H-3 (entfernt aus GERING)	WAHR
CCI-000454	CP-2(a)(4)	GERING	Tabelle H-3 (entfernt aus GERING)	WAHR
CCI-000456	CP-2(a)(5)	GERING	Keine (Nicht Planer)	WAHR
CCI-000457	CP-2(a)(6)	GERING	Keine (Nicht Planer)	WAHR
CCI-002830	CP-2(a)(6)	GERING		WAHR
CCI-000458	CP-2(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-000459	CP-2(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-000460	CP-2(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-000461	CP-2(d)	GERING		WAHR
CCI-000462	CP-2(d)	GERING	Keine (Nicht Planer)	WAHR
CCI-000463	CP-2(e)	GERING	Keine (Nicht Planer)	WAHR
CCI-000464	CP-2(e)	GERING	Keine (Nicht Planer)	WAHR
CCI-000465	CP-2(e)	GERING	Keine (Nicht Planer)	WAHR
CCI-000466	CP-2(e)	GERING	Keine (Nicht Planer)	WAHR
CCI-000468	CP-2(f)	GERING	Keine (Nicht Planer)	WAHR
CCI-002831	CP-2(f)	GERING	Keine (Nicht Planer)	WAHR
CCI-002832	CP-2(g)	GERING	Keine (Nicht Planer)	WAHR
CCI-000469	CP-2(1)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-000474	CP-2(3)	MITTEL		FALSCH
CCI-000476	CP-2(3)	MITTEL		FALSCH
CCI-000473	CP-2(3)	MITTEL		WAHR
CCI-000475	CP-2(3)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-002829	CP-2(8)	MITTEL		FALSCH
CCI-002828	CP-2(8)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-000486	CP-3(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-002833	CP-3(a)	GERING		WAHR
CCI-002834	CP-3(b)	GERING	Keine (Nicht Planer)	WAHR

Tabelle H-1: Überblick über CCIs für Systeme mit GERINGEN und MITTLEREN Auswirkungen				
CCI #	800-53 Kontrolltext-Indikator	Für Auswirkungsgrad mindestens	Tabellenverweis	Gilt für Kontrollsystem?
CCI-000485	CP-3(c)	GERING		WAHR
CCI-000487	CP-3(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-000490	CP-4(a)	GERING		WAHR
CCI-000492	CP-4(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-000494	CP-4(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-000496	CP-4(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-000497	CP-4(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-000498	CP-4(1)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-000505	CP-6(a)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-002836	CP-6(b)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-000507	CP-6(1)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-000509	CP-6(3)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-001604	CP-6(3)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-000514	CP-7(a)	MITTEL		FALSCH
CCI-000510	CP-7(a)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-000513	CP-7(a)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-002839	CP-7(a)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-000515	CP-7(b)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-000521	CP-7(c)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-000516	CP-7(1)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-000517	CP-7(2)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-001606	CP-7(2)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-000518	CP-7(3)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-000523	CP-8	MITTEL		FALSCH
CCI-000525	CP-8	MITTEL		FALSCH
CCI-002841	CP-8	MITTEL		FALSCH
CCI-000522	CP-8	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-000524	CP-8	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-002840	CP-8	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-000526	CP-8(1)(a)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-000527	CP-8(1)(a)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-000528	CP-8(1)(b)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-000529	CP-8(1)(b)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-000530	CP-8(2)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-000535	CP-9(a)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-000534	CP-9(a)	GERING		WAHR
CCI-000537	CP-9(b)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-000536	CP-9(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-000539	CP-9(c)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-000538	CP-9(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-000540	CP-9(d)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-000541	CP-9(1)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-000542	CP-9(1)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-000550	CP-10	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-000551	CP-10	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR

Tabelle H-1: Überblick über CCIs für Systeme mit GERINGEN und MITTLEREN Auswirkungen				
CCI #	800-53 Kontrolltext-Indikator	Für Auswirkungsgrad mindestens	Tabellenverweis	Gilt für Kontrollsystem?
CCI-000552	CP-10	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-000553	CP-10(2)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-002855	CP-12	GERING	Tabelle H-4 (Planer)	WAHR
CCI-002856	CP-12	GERING	Tabelle H-4 (Planer)	WAHR
CCI-002857	CP-12	GERING	Tabelle H-4 (Planer)	WAHR
CCI-001933	IA-1(a)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-001934	IA-1(a)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-000756	IA-1(a)(1)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-000757	IA-1(a)(1)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-001932	IA-1(a)(1)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-000760	IA-1(a)(2)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-000761	IA-1(a)(2)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-000758	IA-1(b)(1)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-000759	IA-1(b)(1)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-000762	IA-1(b)(2)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-000763	IA-1(b)(2)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-000764	IA-2	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-000765	IA-2(1)	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-000766	IA-2(2)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-000767	IA-2(3)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-001949	IA-2(11)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-001951	IA-2(11)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-001952	IA-2(11)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-001948	IA-2(11)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-001950	IA-2(11)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-001947	IA-2(11)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-001953	IA-2(12)	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-001954	IA-2(12)	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-000777	IA-3	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-000778	IA-3	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-001958	IA-3	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-001959	IA-3(1)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-001967	IA-3(1)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-001965	IA-3(4)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-001966	IA-3(4)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-001968	IA-3(4)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-001969	IA-3(4)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-001970	IA-4(a)	GERING	Tabelle H-6 (Enclave)	WAHR

Tabelle H-1: Überblick über CCIs für Systeme mit GERINGEN und MITTLEREN Auswirkungen				
CCI #	800-53 Kontrolltext-Indikator	Für Auswirkungsgrad mindestens	Tabellenverweis	Gilt für Kontrollsystem?
CCI-001971	IA-4(a)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-001972	IA-4(b)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-001973	IA-4(c)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-001974	IA-4(d)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-001975	IA-4(d)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-000794	IA-4(e)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-000795	IA-4(e)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-001980	IA-5(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-000176	IA-5(b)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-001544	IA-5(c)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-001981	IA-5(d)	GERING	Keine (Nicht Planer)	WAHR
CCI-001982	IA-5(d)	GERING	Keine (Nicht Planer)	WAHR
CCI-001983	IA-5(d)	GERING	Keine (Nicht Planer)	WAHR
CCI-001984	IA-5(d)	GERING	Keine (Nicht Planer)	WAHR
CCI-001985	IA-5(d)	GERING	Keine (Nicht Planer)	WAHR
CCI-001986	IA-5(d)	GERING	Keine (Nicht Planer)	WAHR
CCI-001987	IA-5(d)	GERING	Keine (Nicht Planer)	WAHR
CCI-001998	IA-5(d)	GERING	Keine (Nicht Planer)	WAHR
CCI-001989	IA-5(e)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-000179	IA-5(f)	GERING	Keine (Nicht Planer)	WAHR
CCI-000180	IA-5(f)	GERING	Keine (Nicht Planer)	WAHR
CCI-000181	IA-5(f)	GERING	Keine (Nicht Planer)	WAHR
CCI-000182	IA-5(g)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-001610	IA-5(g)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-000183	IA-5(h)	GERING	Keine (Nicht Planer)	WAHR
CCI-002042	IA-5(h)	GERING	Keine (Nicht Planer)	WAHR
CCI-002365	IA-5(i)	GERING	Keine (Nicht Planer)	WAHR
CCI-002366	IA-5(i)	GERING	Keine (Nicht Planer)	WAHR
CCI-001990	IA-5(j)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-000192	IA-5(1)(a)	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-000193	IA-5(1)(a)	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-000194	IA-5(1)(a)	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-000205	IA-5(1)(a)	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-001611	IA-5(1)(a)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-001612	IA-5(1)(a)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-001613	IA-5(1)(a)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-001614	IA-5(1)(a)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-001619	IA-5(1)(a)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-000195	IA-5(1)(b)	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-001615	IA-5(1)(b)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-000196	IA-5(1)(c)	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR

Tabelle H-1: Überblick über CCIs für Systeme mit GERINGEN und MITTLEREN Auswirkungen				
CCI #	800-53 Kontrolltext-Indikator	Für Auswirkungsgrad mindestens	Tabellenverweis	Gilt für Kontrollsystem?
CCI-000197	IA-5(1)(c)	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-000198	IA-5(1)(d)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-000199	IA-5(1)(d)	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-001616	IA-5(1)(d)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-001617	IA-5(1)(d)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-000200	IA-5(1)(e)	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-001618	IA-5(1)(e)	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-002041	IA-5(1)(f)	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-000185	IA-5(2)(a)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-000186	IA-5(2)(b)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-000187	IA-5(2)(c)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-001991	IA-5(2)(d)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-001992	IA-5(3)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-001993	IA-5(3)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-001994	IA-5(3)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-001995	IA-5(3)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-002002	IA-5(11)	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-002003	IA-5(11)	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-000206	IA-6	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-000803	IA-7	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-000804	IA-8	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002009	IA-8(1)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002010	IA-8(1)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002011	IA-8(2)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002012	IA-8(3)	GERING	Keine (Nicht Planer)	WAHR
CCI-002013	IA-8(3)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002014	IA-8(4)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002776	IR-1(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-002777	IR-1(a)	GERING		WAHR
CCI-000805	IR-1(a)(1)	GERING		WAHR
CCI-000806	IR-1(a)(1)	GERING		WAHR
CCI-000809	IR-1(a)(2)	GERING	Keine (Nicht Planer)	WAHR
CCI-000810	IR-1(a)(2)	GERING	Keine (Nicht Planer)	WAHR
CCI-000807	IR-1(b)(1)	GERING	Keine (Nicht Planer)	WAHR
CCI-000808	IR-1(b)(1)	GERING		WAHR

Tabelle H-1: Überblick über CCIs für Systeme mit GERINGEN und MITTLEREN Auswirkungen

CCI #	800-53 Kontrolltext-Indikator	Für Auswirkungsgrad mindestens	Tabellenverweis	Gilt für Kontrollsystem?
CCI-000811	IR-1(b)(2)	GERING	Keine (Nicht Planer)	WAHR
CCI-000812	IR-1(b)(2)	GERING		WAHR
CCI-000813	IR-2(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-002778	IR-2(a)	GERING		WAHR
CCI-002779	IR-2(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-000814	IR-2(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-000815	IR-2(c)	GERING		WAHR
CCI-000818	IR-3	MITTEL	Keine (Nicht Planer)	WAHR
CCI-000819	IR-3	MITTEL		WAHR
CCI-000820	IR-3	MITTEL		WAHR
CCI-001624	IR-3	MITTEL	Keine (Nicht Planer)	WAHR
CCI-002780	IR-3(2)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-000822	IR-4(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-000823	IR-4(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-000824	IR-4(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-001625	IR-4(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-000825	IR-4(1)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-000832	IR-5	GERING	Keine (Nicht Planer)	WAHR
CCI-000834	IR-6(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-000835	IR-6(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-000836	IR-6(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-002791	IR-6(b)	GERING		WAHR
CCI-000837	IR-6(1)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-000839	IR-7	GERING	Keine (Nicht Planer)	WAHR
CCI-000840	IR-7(1)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-002794	IR-8(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-002795	IR-8(a)(1)	GERING	Keine (Nicht Planer)	WAHR
CCI-002796	IR-8(a)(2)	GERING	Keine (Nicht Planer)	WAHR
CCI-002797	IR-8(a)(3)	GERING	Keine (Nicht Planer)	WAHR
CCI-002798	IR-8(a)(4)	GERING	Keine (Nicht Planer)	WAHR
CCI-002799	IR-8(a)(5)	GERING	Keine (Nicht Planer)	WAHR
CCI-002800	IR-8(a)(6)	GERING	Keine (Nicht Planer)	WAHR
CCI-002801	IR-8(a)(7)	GERING	Keine (Nicht Planer)	WAHR
CCI-000844	IR-8(a)(8)	GERING	Keine (Nicht Planer)	WAHR
CCI-002802	IR-8(a)(8)	GERING		WAHR
CCI-000845	IR-8(b)	GERING		WAHR
CCI-000846	IR-8(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-000847	IR-8(c)	GERING		WAHR
CCI-000848	IR-8(c)	GERING		WAHR
CCI-000849	IR-8(d)	GERING	Keine (Nicht Planer)	WAHR
CCI-000850	IR-8(e)	GERING	Keine (Nicht Planer)	WAHR
CCI-002803	IR-8(e)	GERING		WAHR
CCI-002804	IR-8(f)	GERING	Keine (Nicht Planer)	WAHR
CCI-002861	MA-1(a)	GERING		WAHR
CCI-002862	MA-1(a)	GERING		WAHR
CCI-000852	MA-1(a)(1)	GERING	Keine (Nicht Planer)	WAHR
CCI-000853	MA-1(a)(1)	GERING	Keine (Nicht Planer)	WAHR
CCI-000855	MA-1(a)(2)	GERING	Keine (Nicht Planer)	WAHR

Tabelle H-1: Überblick über CCIs für Systeme mit GERINGEN und MITTLEREN Auswirkungen

CCI #	800-53 Kontrolltext Indikator	Gilt für oder über der Auswir- kung	Tabellenverweis	Anwendbar für ein Kontroll- system?
CCI-000856	MA-1(a)(2)	GERING	Keine (Nicht Planer)	WAHR
CCI-000851	MA-1(b)(1)	GERING		WAHR
CCI-000854	MA-1(b)(1)	GERING	Keine (Nicht Planer)	WAHR
CCI-000857	MA-1(b)(2)	GERING	Keine (Nicht Planer)	WAHR
CCI-001628	MA-1(b)(2)	GERING	Keine (Nicht Planer)	WAHR
CCI-002866	MA-2(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-002867	MA-2(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-002868	MA-2(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-002869	MA-2(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-002870	MA-2(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-002871	MA-2(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-002872	MA-2(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-002873	MA-2(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-000859	MA-2(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-000860	MA-2(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-002874	MA-2(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-000861	MA-2(d)	GERING	Keine (Nicht Planer)	WAHR
CCI-000862	MA-2(e)	GERING	Keine (Nicht Planer)	WAHR
CCI-002875	MA-2(f)	GERING	Keine (Nicht Planer)	WAHR
CCI-002876	MA-2(f)	GERING	Keine (Nicht Planer)	WAHR
CCI-000865	MA-3	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-000866	MA-3	MITTEL	Keine (Nicht Planer)	WAHR
CCI-000867	MA-3	MITTEL	Keine (Nicht Planer)	WAHR
CCI-000869	MA-3(1)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-000870	MA-3(2)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-000873	MA-4(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-000874	MA-4(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-000876	MA-4(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-000877	MA-4(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-000878	MA-4(d)	GERING	Keine (Nicht Planer)	WAHR
CCI-000879	MA-4(e)	GERING	Keine (Nicht Planer)	WAHR
CCI-000881	MA-4(2)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-000890	MA-5(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-000891	MA-5(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-002894	MA-5(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-002895	MA-5(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-000903	MA-6	MITTEL	Keine (Nicht Planer)	WAHR
CCI-002896	MA-6	MITTEL	Keine (Nicht Planer)	WAHR
CCI-002897	MA-6	MITTEL		WAHR
CCI-000995	MP-1(a)(1)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-000996	MP-1(a)(1)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002566	MP-1(a)(1)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-000999	MP-1(a)(2)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-001000	MP-1(a)(2)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-000997	MP-1(b)(1)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-000998	MP-1(b)(1)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-001001	MP-1(b)(2)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-001002	MP-1(b)(2)	GERING	Tabelle H-6 (Enclave)	WAHR

Tabelle H-1: Überblick über CCIs für Systeme mit GERINGEN und MITTLEREN Auswirkungen

CCI #	800-53 Kontrolltext Indikator	Gilt für oder über der Auswir- kung	Tabellenverweis	Anwendbar für ein Kontroll- system?
CCI-001003	MP-2	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-001004	MP-2	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-001005	MP-2	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-001010	MP-3(a)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-001011	MP-3(b)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-001012	MP-3(b)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-001013	MP-3(b)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-001014	MP-4(a)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-001015	MP-4(a)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-001016	MP-4(a)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-001018	MP-4(b)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-001020	MP-5(a)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-001021	MP-5(a)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-001022	MP-5(a)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-001023	MP-5(b)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-001025	MP-5(c)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-001024	MP-5(d)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-001027	MP-5(4)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-001028	MP-6(a)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002578	MP-6(a)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002579	MP-6(a)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002580	MP-6(b)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002581	MP-7	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002582	MP-7	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002583	MP-7	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002584	MP-7	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002585	MP-7(1)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-002908	PE-1(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-002909	PE-1(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-000904	PE-1(a)(1)	GERING	Keine (Nicht Planer)	WAHR
CCI-000905	PE-1(a)(1)	GERING	Keine (Nicht Planer)	WAHR
CCI-000908	PE-1(a)(2)	GERING	Keine (Nicht Planer)	WAHR
CCI-000909	PE-1(a)(2)	GERING	Keine (Nicht Planer)	WAHR
CCI-000906	PE-1(b)(1)	GERING	Keine (Nicht Planer)	WAHR
CCI-000907	PE-1(b)(1)	GERING		WAHR
CCI-000910	PE-1(b)(2)	GERING	Keine (Nicht Planer)	WAHR
CCI-000911	PE-1(b)(2)	GERING		WAHR
CCI-000912	PE-2(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-002910	PE-2(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-002911	PE-2(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-000913	PE-2(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-000914	PE-2(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-000915	PE-2(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-001635	PE-2(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-000919	PE-3(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-002915	PE-3(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-000920	PE-3(a)(1)	GERING	Keine (Nicht Planer)	WAHR
CCI-000921	PE-3(a)(2)	GERING	Keine (Nicht Planer)	WAHR

Tabelle H-1: Überblick über CCIs für Systeme mit GERINGEN und MITTLEREN Auswirkungen

CCI #	800-53 Kontrolltext Indikator	Gilt für oder über der Auswir- kung	Tabellenverweis	Anwendbar für ein Kontroll- system?
CCI-002916	PE-3(a)(2)	GERING	Keine (Nicht Planer)	WAHR
CCI-002917	PE-3(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-002918	PE-3(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-002919	PE-3(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-002920	PE-3(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-002921	PE-3(d)	GERING	Keine (Nicht Planer)	WAHR
CCI-002922	PE-3(d)	GERING	Keine (Nicht Planer)	WAHR
CCI-002923	PE-3(d)	GERING	Keine (Nicht Planer)	WAHR
CCI-002924	PE-3(d)	GERING	Keine (Nicht Planer)	WAHR
CCI-000923	PE-3(e)	GERING	Keine (Nicht Planer)	WAHR
CCI-000924	PE-3(f)	GERING	Keine (Nicht Planer)	WAHR
CCI-000925	PE-3(f)	GERING		WAHR
CCI-002925	PE-3(f)	GERING		WAHR
CCI-000926	PE-3(g)	GERING	Keine (Nicht Planer)	WAHR
CCI-000927	PE-3(g)	GERING		WAHR
CCI-000936	PE-4	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-002930	PE-4	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-002931	PE-4	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-000937	PE-5	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-002939	PE-6(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-000939	PE-6(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-000940	PE-6(b)	GERING		WAHR
CCI-002940	PE-6(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-002941	PE-6(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-000941	PE-6(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-000942	PE-6(1)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-002950	PE-6(4)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-002951	PE-6(4)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-000947	PE-8(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-002952	PE-8(a)	GERING		WAHR
CCI-000948	PE-8(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-000949	PE-8(b)	GERING		WAHR
CCI-000952	PE-9	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-002953	PE-9(1)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-002954	PE-9(1)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-000956	PE-10(a)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-000957	PE-10(b)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-000958	PE-10(b)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-000959	PE-10(c)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-002955	PE-11	GERING	Tabelle H-3 (entfernt aus GERING)	WAHR
CCI-000961	PE-11(1)	GERING	Tabelle H-3 (entfernt aus GERING)	WAHR
CCI-000963	PE-12	GERING		FALSCH
CCI-000965	PE-13	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-000968	PE-13(3)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-000971	PE-14(a)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-000972	PE-14(a)	GERING	Tabelle H-6 (Enclave)	WAHR

Tabelle H-1: Überblick über CCIs für Systeme mit GERINGEN und MITTLEREN Auswirkungen

CCI #	800-53 Kontrolltext Indikator	Gilt für oder über der Auswir- kung	Tabellenverweis	Anwendbar für ein Kontroll- system?
CCI-000973	PE-14(b)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-000974	PE-14(b)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-000977	PE-15	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-000978	PE-15	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-000979	PE-15	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-000981	PE-16	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-000982	PE-16	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-000983	PE-16	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-000984	PE-16	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002974	PE-16	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-000985	PE-17(a)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-002975	PE-17(a)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-000987	PE-17(b)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-000988	PE-17(c)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-003047	PL-1(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-003048	PL-1(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-000563	PL-1(a)(1)	GERING	Keine (Nicht Planer)	WAHR
CCI-000564	PL-1(a)(1)	GERING	Keine (Nicht Planer)	WAHR
CCI-000566	PL-1(a)(2)	GERING	Keine (Nicht Planer)	WAHR
CCI-001636	PL-1(b)(1)	GERING		WAHR
CCI-001637	PL-1(b)(1)	GERING	Keine (Nicht Planer)	WAHR
CCI-000567	PL-1(b)(2)	GERING	Keine (Nicht Planer)	WAHR
CCI-000568	PL-1(b)(2)	GERING	Keine (Nicht Planer)	WAHR
CCI-001638	PL-1(b)(2)	GERING		WAHR
CCI-003049	PL-2(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-003050	PL-2(a)(1)	GERING	Keine (Nicht Planer)	WAHR
CCI-003051	PL-2(a)(2)	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-003052	PL-2(a)(3)	GERING	Keine (Nicht Planer)	WAHR
CCI-003053	PL-2(a)(4)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-003054	PL-2(a)(5)	GERING	Keine (Nicht Planer)	WAHR
CCI-003055	PL-2(a)(6)	GERING	Keine (Nicht Planer)	WAHR
CCI-003056	PL-2(a)(7)	GERING	Keine (Nicht Planer)	WAHR
CCI-003057	PL-2(a)(8)	GERING	Keine (Nicht Planer)	WAHR
CCI-000571	PL-2(a)(9)	GERING	Keine (Nicht Planer)	WAHR
CCI-003059	PL-2(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-003060	PL-2(b)	GERING		WAHR
CCI-003061	PL-2(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-003062	PL-2(b)	GERING		WAHR
CCI-000572	PL-2(c)	GERING		WAHR
CCI-000573	PL-2(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-000574	PL-2(d)	GERING	Keine (Nicht Planer)	WAHR
CCI-003063	PL-2(e)	GERING	Keine (Nicht Planer)	WAHR
CCI-003064	PL-2(e)	GERING	Keine (Nicht Planer)	WAHR
CCI-003065	PL-2(3)	GERING	Keine (Nicht Planer)	WAHR
CCI-003067	PL-2(3)	GERING	Keine (Nicht Planer)	WAHR
CCI-000592	PL-4(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-001639	PL-4(a)	GERING	Keine (Nicht Planer)	WAHR

Tabelle H-1: Überblick über CCIs für Systeme mit GERINGEN und MITTLEREN Auswirkungen				
CCI #	800-53 Kontrolltext Indikator	Gilt für oder über der Auswir- kung	Tabellenverweis	Anwendbar für ein Kontroll- system?
CCI-000593	PL-4(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-003068	PL-4(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-003069	PL-4(c)	GERING		WAHR
CCI-003070	PL-4(d)	GERING	Keine (Nicht Planer)	WAHR
CCI-000594	PL-4(1)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-000595	PL-4(1)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-003071	PL-7(a)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-000577	PL-7(b)	MITTEL		WAHR
CCI-000578	PL-7(b)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-003072	PL-8(a)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-003073	PL-8(a)(1)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-003074	PL-8(a)(2)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-003075	PL-8(a)(3)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-003076	PL-8(b)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-003077	PL-8(b)	MITTEL		WAHR
CCI-003078	PL-8(c)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-003079	PL-8(c)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-003080	PL-8(c)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-000073	PM-1(a)(1)	GERING	Keine (Nicht Planer)	WAHR
CCI-002985	PM-1(a)(1)	GERING	Keine (Nicht Planer)	WAHR
CCI-001680	PM-1(a)(2)	GERING		WAHR
CCI-002986	PM-1(a)(2)	GERING	Keine (Nicht Planer)	WAHR
CCI-002984	PM-1(a)(3)	GERING		WAHR
CCI-002987	PM-1(a)(3)	GERING	Keine (Nicht Planer)	WAHR
CCI-000074	PM-1(a)(4)	GERING		WAHR
CCI-002988	PM-1(a)(4)	GERING	Keine (Nicht Planer)	WAHR
CCI-000075	PM-1(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-000076	PM-1(b)	GERING		WAHR
CCI-000077	PM-1(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-002989	PM-1(d)	GERING	Keine (Nicht Planer)	WAHR
CCI-002990	PM-1(d)	GERING	Keine (Nicht Planer)	WAHR
CCI-000078	PM-2	GERING		WAHR
CCI-000080	PM-3(a)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-000081	PM-3(b)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-000141	PM-3(c)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-000142	PM-4(a)(1)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002991	PM-4(a)(1)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-000170	PM-4(a)(2)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002992	PM-4(a)(3)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002993	PM-4(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-000207	PM-5	GERING	Tabelle H-4 (Planer)	WAHR
CCI-000209	PM-6	GERING		WAHR
CCI-000210	PM-6	GERING		WAHR
CCI-000211	PM-6	GERING	Keine (Nicht Planer)	WAHR
CCI-000212	PM-7	GERING	Keine (Nicht Planer)	WAHR
CCI-000216	PM-8	GERING	Tabelle H-3 (entfernt aus GERING)	WAHR

Tabelle H-1: Überblick über CCIs für Systeme mit GERINGEN und MITTLEREN Auswirkungen				
CCI #	800-53 Kontrolltext Indikator	Gilt für oder über der Auswir- kung	Tabellenverweis	Anwendbar für ein Kontroll- system?
CCI-001640	PM-8	GERING	Tabelle H-3 (entfernt aus GERING)	WAHR
CCI-000227	PM-9(a)	GERING		WAHR
CCI-000228	PM-9(b)	GERING		WAHR
CCI-002994	PM-9(c)	GERING		WAHR
CCI-002995	PM-9(c)	GERING		WAHR
CCI-000229	PM-10(a)	GERING		WAHR
CCI-000230	PM-10(a)	GERING		WAHR
CCI-000231	PM-10(a)	GERING		WAHR
CCI-000233	PM-10(b)	GERING		WAHR
CCI-000234	PM-10(c)	GERING		WAHR
CCI-000235	PM-11(a)	GERING		WAHR
CCI-000236	PM-11(b)	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-002996	PM-12	GERING	Keine (Nicht Planer)	WAHR
CCI-002997	PM-13	GERING		WAHR
CCI-002998	PM-14(a)(1)	GERING	Keine (Nicht Planer)	WAHR
CCI-002999	PM-14(a)(1)	GERING	Keine (Nicht Planer)	WAHR
CCI-003000	PM-14(a)(1)	GERING	Keine (Nicht Planer)	WAHR
CCI-003001	PM-14(a)(1)	GERING	Keine (Nicht Planer)	WAHR
CCI-003002	PM-14(a)(1)	GERING	Keine (Nicht Planer)	WAHR
CCI-003003	PM-14(a)(1)	GERING	Keine (Nicht Planer)	WAHR
CCI-003004	PM-14(a)(2)	GERING	Keine (Nicht Planer)	WAHR
CCI-003005	PM-14(a)(2)	GERING	Keine (Nicht Planer)	WAHR
CCI-003006	PM-14(a)(2)	GERING	Keine (Nicht Planer)	WAHR
CCI-003007	PM-14(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-003008	PM-14(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-003009	PM-14(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-003010	PM-15(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-003011	PM-15(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-003012	PM-15(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-003013	PM-16	GERING	Keine (Nicht Planer)	WAHR
CCI-003017	PS-1(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-003018	PS-1(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-001504	PS-1(a)(1)	GERING		WAHR
CCI-001505	PS-1(a)(1)	GERING		WAHR
CCI-001509	PS-1(a)(2)	GERING		WAHR
CCI-001510	PS-1(a)(2)	GERING		WAHR
CCI-001506	PS-1(b)(1)	GERING		WAHR
CCI-001507	PS-1(b)(1)	GERING		WAHR
CCI-001508	PS-1(b)(2)	GERING		WAHR
CCI-001511	PS-1(b)(2)	GERING		WAHR
CCI-001512	PS-2(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-001513	PS-2(b)	GERING		WAHR
CCI-001514	PS-2(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-001515	PS-2(c)	GERING		WAHR
CCI-001516	PS-3(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-001517	PS-3(b)	GERING	Keine (Nicht Planer)	WAHR

Tabelle H-1: Überblick über CCIs für Systeme mit GERINGEN und MITTLEREN Auswirkungen				
CCI #	800-53 Kontrolltext Indikator	Gilt für oder über der Auswir- kung	Tabellenverweis	Anwendbar für ein Kontroll- system?
CCI-001518	PS-3(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-001519	PS-3(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-001522	PS-4(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-003022	PS-4(a)	GERING		WAHR
CCI-003023	PS-4(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-001523	PS-4(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-003024	PS-4(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-001524	PS-4(d)	GERING	Keine (Nicht Planer)	WAHR
CCI-001525	PS-4(e)	GERING	Keine (Nicht Planer)	WAHR
CCI-001526	PS-4(e)	GERING	Keine (Nicht Planer)	WAHR
CCI-003016	PS-4(f)	GERING		WAHR
CCI-003025	PS-4(f)	GERING		WAHR
CCI-003026	PS-4(f)	GERING		WAHR
CCI-001527	PS-5(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-001528	PS-5(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-001529	PS-5(b)	GERING		WAHR
CCI-001530	PS-5(b)	GERING		WAHR
CCI-003031	PS-5(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-003032	PS-5(d)	GERING	Keine (Nicht Planer)	WAHR
CCI-003033	PS-5(d)	GERING		WAHR
CCI-003034	PS-5(d)	GERING		WAHR
CCI-003035	PS-6(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-001532	PS-6(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-001533	PS-6(b)	GERING		WAHR
CCI-001531	PS-6(c)(1)	GERING	Keine (Nicht Planer)	WAHR
CCI-003036	PS-6(c)(2)	GERING	Keine (Nicht Planer)	WAHR
CCI-003037	PS-6(c)(2)	GERING		WAHR
CCI-001539	PS-7(a)	GERING		WAHR
CCI-003040	PS-7(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-001540	PS-7(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-003041	PS-7(d)	GERING	Keine (Nicht Planer)	WAHR
CCI-003042	PS-7(d)	GERING		WAHR
CCI-003043	PS-7(d)	GERING		WAHR
CCI-001541	PS-7(e)	GERING	Keine (Nicht Planer)	WAHR
CCI-001542	PS-8(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-003044	PS-8(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-003045	PS-8(b)	GERING		WAHR
CCI-003046	PS-8(b)	GERING		WAHR
CCI-002368	RA-1(a)	GERING		WAHR
CCI-002369	RA-1(a)	GERING		WAHR
CCI-001037	RA-1(a)(1)	GERING		WAHR
CCI-001038	RA-1(a)(1)	GERING		WAHR
CCI-001041	RA-1(a)(2)	GERING		WAHR
CCI-001042	RA-1(a)(2)	GERING		WAHR
CCI-001039	RA-1(b)(1)	GERING		WAHR
CCI-001040	RA-1(b)(1)	GERING		WAHR
CCI-001043	RA-1(b)(2)	GERING		WAHR
CCI-001044	RA-1(b)(2)	GERING		WAHR

Tabelle H-1: Überblick über CCIs für Systeme mit GERINGEN und MITTLEREN Auswirkungen				
CCI #	800-53 Kontrolltext Indikator	Gilt für oder über der Auswir- kung	Tabellenverweis	Anwendbar für ein Kontroll- system?
CCI-001045	RA-2(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-001046	RA-2(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-001047	RA-2(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-001048	RA-3(a)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-001049	RA-3(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-001642	RA-3(b)	GERING		WAHR
CCI-001050	RA-3(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-001051	RA-3(c)	GERING		WAHR
CCI-002370	RA-3(d)	GERING	Keine (Nicht Planer)	WAHR
CCI-002371	RA-3(d)	GERING		WAHR
CCI-001052	RA-3(e)	GERING	Keine (Nicht Planer)	WAHR
CCI-001053	RA-3(e)	GERING		WAHR
CCI-001054	RA-5(a)	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-001055	RA-5(a)	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-001056	RA-5(a)	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-001641	RA-5(a)	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-001643	RA-5(a)	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-001057	RA-5(b)	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-001058	RA-5(c)	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-001059	RA-5(d)	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-001060	RA-5(d)	GERING		WAHR
CCI-001061	RA-5(e)	GERING	Keine (Nicht Planer)	WAHR
CCI-002376	RA-5(e)	GERING		WAHR
CCI-001062	RA-5(1)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-001063	RA-5(2)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-001064	RA-5(2)	MITTEL		WAHR
CCI-001067	RA-5(5)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-001645	RA-5(5)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-002906	RA-5(5)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-003089	SA-1(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-003090	SA-1(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-000602	SA-1(a)(1)	GERING		WAHR
CCI-000603	SA-1(a)(1)	GERING		WAHR
CCI-000605	SA-1(a)(2)	GERING		WAHR
CCI-000606	SA-1(a)(2)	GERING		WAHR
CCI-000601	SA-1(b)(1)	GERING		WAHR

Tabelle H-1: Überblick über CCIs für Systeme mit GERINGEN und MITTLEREN Auswirkungen				
CCI #	800-53 Kontrolltext Indikator	Gilt für oder über der Auswir- kung	Tabellenverweis	Anwendbar für ein Kontroll- system?
CCI-000604	SA-1(b)(1)	GERING		WAHR
CCI-000607	SA-1(b)(2)	GERING		WAHR
CCI-001646	SA-1(b)(2)	GERING		WAHR
CCI-003091	SA-2(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-000610	SA-2(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-000611	SA-2(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-000612	SA-2(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-000613	SA-2(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-000614	SA-2(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-000615	SA-3(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-003092	SA-3(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-000616	SA-3(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-000618	SA-3(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-003093	SA-3(d)	GERING	Keine (Nicht Planer)	WAHR
CCI-003094	SA-4(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-003095	SA-4(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-003096	SA-4(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-003097	SA-4(d)	GERING	Keine (Nicht Planer)	WAHR
CCI-003098	SA-4(e)	GERING	Keine (Nicht Planer)	WAHR
CCI-003099	SA-4(f)	GERING	Keine (Nicht Planer)	WAHR
CCI-003100	SA-4(g)	GERING	Keine (Nicht Planer)	WAHR
CCI-000623	SA-4(1)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-003101	SA-4(2)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-003102	SA-4(2)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-003103	SA-4(2)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-003104	SA-4(2)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-003105	SA-4(2)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-003106	SA-4(2)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-003114	SA-4(9)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-003116	SA-4(10)	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-003124	SA-5(a)(1)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-003125	SA-5(a)(1)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-003126	SA-5(a)(1)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-003127	SA-5(a)(2)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-003128	SA-5(a)(3)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-003129	SA-5(b)(1)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-003130	SA-5(b)(2)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-003131	SA-5(b)(3)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-000642	SA-5(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-003132	SA-5(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-003133	SA-5(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-003134	SA-5(d)	GERING	Keine (Nicht Planer)	WAHR
CCI-003135	SA-5(e)	GERING	Keine (Nicht Planer)	WAHR
CCI-003136	SA-5(e)	GERING		WAHR
CCI-000664	SA-8	MITTEL	Keine (Nicht Planer)	WAHR
CCI-000665	SA-8	MITTEL	Keine (Nicht Planer)	WAHR
CCI-000666	SA-8	MITTEL	Keine (Nicht Planer)	WAHR

Tabelle H-1: Überblick über CCIs für Systeme mit GERINGEN und MITTLEREN Auswirkungen

CCI #	800-53 Kontrolltext Indikator	Gilt für oder über der Auswir- kung	Tabellenverweis	Anwendbar für ein Kontroll- system?
CCI-000667	SA-8	MITTEL	Keine (Nicht Planer)	WAHR
CCI-000668	SA-8	MITTEL	Keine (Nicht Planer)	WAHR
CCI-000669	SA-9(a)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-000670	SA-9(a)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-003137	SA-9(a)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-000671	SA-9(b)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-000672	SA-9(b)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-000673	SA-9(b)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-000674	SA-9(b)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-003138	SA-9(c)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-003139	SA-9(c)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-003143	SA-9(2)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-003144	SA-9(2)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-003155	SA-10(a)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-003156	SA-10(b)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-003157	SA-10(b)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-003158	SA-10(b)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-003159	SA-10(b)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-000692	SA-10(c)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-000694	SA-10(d)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-003160	SA-10(d)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-003161	SA-10(e)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-003162	SA-10(e)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-003163	SA-10(e)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-003164	SA-10(e)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-003171	SA-11(a)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-003172	SA-11(a)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-003173	SA-11(b)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-003174	SA-11(b)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-003175	SA-11(c)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-003176	SA-11(c)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-003177	SA-11(d)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-003178	SA-11(e)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-002378	SC-1(a)	GERING		WAHR
CCI-002380	SC-1(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-001074	SC-1(a)(1)	GERING		WAHR
CCI-001075	SC-1(a)(1)	GERING		WAHR
CCI-002377	SC-1(a)(1)	GERING		WAHR
CCI-001078	SC-1(a)(2)	GERING		WAHR
CCI-001079	SC-1(a)(2)	GERING		WAHR
CCI-002379	SC-1(a)(2)	GERING	Keine (Nicht Planer)	WAHR
CCI-001076	SC-1(b)(1)	GERING		WAHR
CCI-001077	SC-1(b)(1)	GERING		WAHR
CCI-001080	SC-1(b)(2)	GERING		WAHR
CCI-001081	SC-1(b)(2)	GERING		WAHR
CCI-001082	SC-2	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-001090	SC-4	MITTEL	Tabelle H-7 (Enclave)	WAHR

Tabelle H-1: Überblick über CCIs für Systeme mit GERINGEN und MITTLEREN Auswirkungen				
CCI #	800-53 Kontrolltext Indikator	Gilt für oder über der Auswir- kung	Tabellenverweis	Anwendbar für ein Kontroll- system?
CCI-001093	SC-5	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-002385	SC-5	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-002386	SC-5	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-001097	SC-7(a)	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-002395	SC-7(b)	GERING		FALSCH
CCI-001098	SC-7(c)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-001101	SC-7(3)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-001102	SC-7(4)(a)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-001103	SC-7(4)(b)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-002396	SC-7(4)(c)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-001105	SC-7(4)(d)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-001106	SC-7(4)(e)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-001107	SC-7(4)(e)	MITTEL		WAHR
CCI-001108	SC-7(4)(e)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-001109	SC-7(5)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-002397	SC-7(7)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-001126	SC-7(18)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-002418	SC-8	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-002419	SC-8(1)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-002421	SC-8(1)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-001133	SC-10	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-001134	SC-10	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-002428	SC-12	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002429	SC-12	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002430	SC-12	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002431	SC-12	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002432	SC-12	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002433	SC-12	GERING	Keine (Nicht Planer)	WAHR
CCI-002434	SC-12	GERING	Keine (Nicht Planer)	WAHR
CCI-002435	SC-12	GERING	Keine (Nicht Planer)	WAHR
CCI-002436	SC-12	GERING	Keine (Nicht Planer)	WAHR
CCI-002437	SC-12	GERING	Keine (Nicht Planer)	WAHR
CCI-002438	SC-12	GERING	Keine (Nicht Planer)	WAHR
CCI-002439	SC-12	GERING	Keine (Nicht Planer)	WAHR
CCI-002440	SC-12	GERING	Keine (Nicht Planer)	WAHR
CCI-002441	SC-12	GERING	Keine (Nicht Planer)	WAHR
CCI-002442	SC-12	GERING	Keine (Nicht Planer)	WAHR
CCI-002449	SC-13	GERING	Tabelle H-3 (entfernt aus GERING)	WAHR
CCI-002450	SC-13	GERING	Tabelle H-3 (entfernt aus GERING)	WAHR
CCI-001150	SC-15(a)	GERING	Tabelle H-6 (Enclave)	WAHR

Tabelle H-1: Überblick über CCIs für Systeme mit GERINGEN und MITTLEREN Auswirkungen				
CCI #	800-53 Kontrolltext Indikator	Gilt für oder über der Auswir- kung	Tabellenverweis	Anwendbar für ein Kontroll- system?
CCI-001151	SC-15(a)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-001152	SC-15(b)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-001159	SC-17	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-002456	SC-17	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-001160	SC-18(a)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-001161	SC-18(b)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-001162	SC-18(b)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-001163	SC-18(c)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-001164	SC-18(c)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-001165	SC-18(c)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-001173	SC-19(a)	MITTEL		FALSCH
CCI-001174	SC-19(a)	MITTEL		FALSCH
CCI-001175	SC-19(b)	MITTEL		FALSCH
CCI-001176	SC-19(b)	MITTEL		FALSCH
CCI-001177	SC-19(b)	MITTEL		FALSCH
CCI-001178	SC-20(a)	GERING		FALSCH
CCI-002462	SC-20(a)	GERING		FALSCH
CCI-001179	SC-20(b)	GERING		FALSCH
CCI-001663	SC-20(b)	GERING		FALSCH
CCI-002465	SC-21	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002466	SC-21	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002467	SC-21	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002468	SC-21	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-001182	SC-22	GERING		FALSCH
CCI-001183	SC-22	GERING		FALSCH
CCI-001184	SC-23	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-001190	SC-24	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-001191	SC-24	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-001192	SC-24	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-001193	SC-24	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-001665	SC-24	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-001199	SC-28	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-002472	SC-28	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-002530	SC-39	GERING	Tabelle H-4 (Planer)	WAHR
CCI-002546	SC-41	GERING	Tabelle H-4 (Planer)	WAHR
CCI-002544	SC-41	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-002545	SC-41	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-002601	SI-1(a)	GERING		WAHR

Tabelle H-1: Überblick über CCIs für Systeme mit GERINGEN und MITTLEREN Auswirkungen

CCI #	800-53 Kontrolltext Indikator	Gilt für oder über der Auswir- kung	Tabellenverweis	Anwendbar für ein Kontroll- system?
CCI-001217	SI-1(a)(1)	GERING		WAHR
CCI-001218	SI-1(a)(1)	GERING	Keine (Nicht Planer)	WAHR
CCI-001220	SI-1(a)(2)	GERING		WAHR
CCI-001221	SI-1(a)(2)	GERING		WAHR
CCI-001219	SI-1(b)(1)	GERING		WAHR
CCI-001223	SI-1(b)(1)	GERING		WAHR
CCI-001222	SI-1(b)(2)	GERING		WAHR
CCI-001224	SI-1(b)(2)	GERING		WAHR
CCI-001227	SI-2(a)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-001225	SI-2(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-001226	SI-2(a)	GERING	Keine (Nicht Planer)	WAHR
CCI-001228	SI-2(b)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-001229	SI-2(b)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002602	SI-2(b)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002603	SI-2(b)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002604	SI-2(c)	GERING		WAHR
CCI-002605	SI-2(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-002606	SI-2(c)	GERING		WAHR
CCI-002607	SI-2(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-001230	SI-2(d)	GERING	Keine (Nicht Planer)	WAHR
CCI-001233	SI-2(2)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-001234	SI-2(2)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-002619	SI-3(a)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002620	SI-3(a)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002621	SI-3(a)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002622	SI-3(a)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-001240	SI-3(b)	GERING	Keine (Nicht Planer)	WAHR
CCI-001241	SI-3(c)(1)	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-002623	SI-3(c)(1)	GERING	Tabelle H-4 (Planer)	WAHR
CCI-001242	SI-3(c)(1)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002624	SI-3(c)(1)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-001243	SI-3(c)(2)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-001244	SI-3(c)(2)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-001245	SI-3(d)	GERING	Keine (Nicht Planer)	WAHR
CCI-001246	SI-3(1)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-001247	SI-3(2)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-001253	SI-4(a)(1)	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-002641	SI-4(a)(1)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002644	SI-4(a)(2)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002642	SI-4(a)(2)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002643	SI-4(a)(2)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002645	SI-4(b)	GERING	Tabelle H-4 (Planer) Tabelle H-6 (Enclave)	WAHR
CCI-002646	SI-4(b)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-001255	SI-4(c)	GERING	Keine (Nicht Planer)	WAHR
CCI-001256	SI-4(c)	GERING	Tabelle H-6 (Enclave)	WAHR

Tabelle H-1: Überblick über CCIs für Systeme mit GERINGEN und MITTLEREN Auswirkungen

CCI #	800-53 Kontrolltext Indikator	Gilt für oder über der Auswir- kung	Tabellenverweis	Anwendbar für ein Kontroll- system?
CCI-002647	SI-4(d)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002648	SI-4(d)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002649	SI-4(d)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-001257	SI-4(e)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-001258	SI-4(f)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002650	SI-4(g)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002651	SI-4(g)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002652	SI-4(g)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002654	SI-4(g)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-001260	SI-4(2)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-002659	SI-4(4)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-002660	SI-4(4)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-002661	SI-4(4)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-002662	SI-4(4)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-001264	SI-4(5)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-002663	SI-4(5)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-002664	SI-4(5)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-001285	SI-5(a)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002692	SI-5(a)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-001286	SI-5(b)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-001287	SI-5(c)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-001288	SI-5(c)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002693	SI-5(c)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002694	SI-5(c)	GERING		WAHR
CCI-001289	SI-5(d)	GERING	Tabelle H-6 (Enclave)	WAHR
CCI-002703	SI-7	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-002704	SI-7	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-002705	SI-7(1)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-002706	SI-7(1)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-002707	SI-7(1)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-002710	SI-7(1)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-002711	SI-7(1)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-002712	SI-7(1)	MITTEL	Tabelle H-5 (Planer) Tabelle H-7 (Enclave)	WAHR
CCI-002708	SI-7(1)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-002709	SI-7(1)	MITTEL		WAHR
CCI-002719	SI-7(7)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-002720	SI-7(7)	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-002741	SI-8(a)	MITTEL		FALSCH
CCI-002742	SI-8(a)	MITTEL		FALSCH
CCI-001306	SI-8(b)	MITTEL		FALSCH
CCI-001307	SI-8(1)	MITTEL		FALSCH

Tabelle H-1: Überblick über CCIs für Systeme mit GERINGEN und MITTLEREN Auswirkungen				
CCI #	800-53 Kontrolltext Indikator	Gilt für oder über der Auswir- kung	Tabellenverweis	Anwendbar für ein Kontroll- system?
CCI-001308	SI-8(2)	MITTEL		FALSCH
CCI-001310	SI-10	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-002744	SI-10	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-001312	SI-11(a)	MITTEL	Tabelle H-5 (Planer)	WAHR
CCI-001314	SI-11(b)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-002759	SI-11(b)	MITTEL	Keine (Nicht Planer)	WAHR
CCI-001315	SI-12	GERING	Keine (Nicht Planer)	WAHR
CCI-001678	SI-12	GERING	Keine (Nicht Planer)	WAHR
CCI-002823	SI-16	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-002824	SI-16	MITTEL	Tabelle H-7 (Enclave)	WAHR
CCI-002773	SI-17	GERING	Tabelle H-4 (Planer)	WAHR
CCI-002774	SI-17	GERING	Tabelle H-4 (Planer)	WAHR
CCI-002775	SI-17	GERING	Tabelle H-4 (Planer)	WAHR

Tabelle H-2: Für Kontrollsysteme ungeeignete CCIs			
CCI #	800-53 Kontroll-text Indikator	CCI-Definition	Begründung für Nicht-aufnahme
CCI-001473	AC-22(a)	Die Organisation benennt Personen, die berechtigt sind, Informationen auf einem öffentlich zugänglichen Informationssystem zu veröffentlichen.	Kontrollsysteme sind nicht öffentlich zugänglich
CCI-001474	AC-22(b)	Die Organisation schult die autorisierten Personen, um sicherzustellen, dass öffentlich zugängliche Informationen keine nichtöffentlichen Informationen enthalten.	Kontrollsysteme sind nicht öffentlich zugänglich
CCI-001475	AC-22(c)	Die Organisation prüft die geplanten Informationsinhalte vor Veröffentlichung im öffentlich zugänglichen Informationssystem, um sicherzustellen, dass keine nichtöffentlichen Informationen enthalten sind.	Kontrollsysteme sind nicht öffentlich zugänglich
CCI-001476	AC-22(d)	Die Organisation prüft die Inhalte im öffentlich zugänglichen Informationssystem auf nichtöffentliche Informationen in einer von der Organisation festgelegten Häufigkeit.	Kontrollsysteme sind nicht öffentlich zugänglich
CCI-001477	AC-22(d)	Die Organisation bestimmt die Häufigkeit, in der die Inhalte öffentlich zugänglicher Informationssysteme auf nichtöffentliche Informationen geprüft werden.	Kontrollsysteme sind nicht öffentlich zugänglich
CCI-001478	AC-22(e)	Die Organisation entfernt bei Auffinden nichtöffentlicher Informationen diese vom öffentlich zugänglichen Informationssystem.	Kontrollsysteme sind nicht öffentlich zugänglich
CCI-001384	AC-8(c)(1)	Das Informationssystem zeigt für öffentlich zugängliche Systeme Informationen zur Systemnutzung mit durch die Organisation festgelegten Bedingungen an, ehe weiterer Zugang gewährt wird.	Kontrollsysteme sind nicht öffentlich zugänglich
CCI-001385	AC-8(c)(2)	Das Informationssystem zeigt für öffentlich zugängliche Systeme, falls vorhanden, Hinweise in Bezug auf Beobachtung an, die mit Datenschutzregelungen für diese Art Systeme übereinstimmen, wo diese Maßnahmen allgemein untersagt sind.	Kontrollsysteme sind nicht öffentlich zugänglich
CCI-001386	AC-8(c)(2)	Das Informationssystem zeigt für öffentlich zugängliche Systeme, falls vorhanden, Hinweise in Bezug auf Aufzeichnungen an, die mit Datenschutzregelungen für diese Art Systeme übereinstimmen, wo diese Maßnahmen allgemein untersagt sind.	Kontrollsysteme sind nicht öffentlich zugänglich
CCI-001387	AC-8(c)(2)	Das Informationssystem zeigt für öffentlich zugängliche Systeme, falls vorhanden, Hinweise in Bezug auf Überprüfungen an, die mit Datenschutzregelungen für diese Art Systeme übereinstimmen, wo diese Maßnahmen allgemein untersagt sind.	Kontrollsysteme sind nicht öffentlich zugänglich
CCI-001388	AC-8(c)(3)	Das Informationssystem enthält für öffentlich zugängliche Systeme eine Beschreibung der autorisierten Nutzungen des Systems.	Kontrollsysteme sind nicht öffentlich zugänglich
CCI-001739	CM-2(7)a	Die Organisation gibt von der Organisation festgelegte Informationssysteme, Systemkomponenten oder Geräte mit von der Organisation festgelegten Konfigurationen an Personen aus, die an Orte reisen, die die Organisation als Orte mit erheblichem Risiko erachtet.	Kontrollsysteme sind nicht mobil.

Tabelle H-2: Für Kontrollsysteme ungeeignete CCIs			
CCI #	800-53 Kontroll-text Indikator	CCI-Definition	Begründung für Nicht-aufnahme
CCI-001815	CM-2(7)b	Die Organisation legt die Sicherheitsmaßnahmen fest, die für die Geräte anzuwenden sind, wenn diese aus den Gebieten mit erheblichem Risiko zurückkommen.	Kontrollsysteme sind nicht mobil.
CCI-001816	CM-2(7)b	Die Organisation wendet von der Organisation festgelegte Sicherheitsmaßnahmen für Geräte an, wenn Personen aus Gebieten mit erheblichem Risiko zurückkommen.	Kontrollsysteme sind nicht mobil.
CCI-000474	CP-2(3)	Die Organisation bestimmt den Zeitraum zur Planung der Wiederaufnahme wichtiger betrieblicher Funktionen als Ergebnis der Inkraftsetzung des Krisenplans.	Kontrollsysteme sind keine Geschäftssysteme
CCI-000476	CP-2(3)	Die Organisation plant die Wiederaufnahme wichtiger betrieblicher Funktionen im von der Organisation festgelegten Zeitraum der Inkraftsetzung des Krisenplans.	Kontrollsysteme sind keine Geschäftssysteme
CCI-002829	CP-2(8)	Die Organisation bestimmt kritische Informationssystem-Komponenten, die wichtige betriebliche Funktionen unterstützen.	Kontrollsysteme sind keine Geschäftssysteme
CCI-000444	CP-2(a)(1)	Die Organisation entwickelt einen Krisenplan für das Informationssystem, der wichtige betriebliche Funktionen regelt.	Kontrollsysteme sind keine Geschäftssysteme
CCI-000451	CP-2(a)(4)	Die Organisation entwickelt einen Krisenplan für das Informationssystem, der den Erhalt wichtiger betrieblicher Funktionen trotz Beeinträchtigung des Informationssystems regelt.	Kontrollsysteme sind keine Geschäftssysteme
CCI-000453	CP-2(a)(4)	Die Organisation entwickelt einen Krisenplan für das Informationssystem, der den Erhalt wichtiger betrieblicher Funktionen trotz Gefährdung des Informationssystems regelt.	Kontrollsysteme sind keine Geschäftssysteme
CCI-000455	CP-2(a)(4)	Die Organisation entwickelt einen Krisenplan für das Informationssystem, der den Erhalt wichtiger betrieblicher Funktionen trotz Ausfall des Informationssystems regelt.	Kontrollsysteme sind keine Geschäftssysteme
CCI-000514	CP-7(a)	Die Organisation richtet einen alternativen Verarbeitungstandort einschließlich erforderlicher Vereinbarungen ein, sodass von der Organisation bestimmte Informationssystem-Transaktionen für wesentliche betriebliche Funktionen innerhalb einer von der Organisation festgelegten Zielvorgabe für Wiederherstellungszeit und -termin übertragen und wieder aufgenommen werden können, wenn primäre Verarbeitungskapazitäten nicht verfügbar sind.	Kontrollsysteme sind keine Geschäftssysteme
CCI-000523	CP-8	Die Organisation bestimmt den Zeitraum, um die Wiederaufnahme der von der Organisation festgelegten Informationssystem-Transaktionen für wesentliche betriebliche Funktionen zu gestatten, wenn die primären Telekommunikationsmöglichkeiten weder am primären noch am alternativen Verarbeitungs- oder Speicherort verfügbar sind.	Kontrollsysteme sind keine Geschäftssysteme

Tabelle H-2: Für Kontrollsysteme ungeeignete CCIs

CCI #	800-53 Kontroll-text Indikator	CCI-Definition	Begründung für Nicht-aufnahme
CCI-000525	CP-8	Die Organisation richtet alternative Telekommunikationsdienste einschließlich erforderlicher Vereinbarungen ein, um die Wiederaufnahme der von der Organisation festgelegten Informationssystem-Transaktionen für wesentliche betriebliche Funktionen innerhalb eines von der Organisation bestimmten Zeitraums zu gestatten, wenn die primären Telekommunikationsmöglichkeiten weder am primären noch am alternativen Verarbeitungs- oder Speicherort verfügbar sind.	Kontrollsysteme sind keine Geschäftssysteme
CCI-002841	CP-8	Die Organisation legt die Informationssystem-Transaktionen fest, die für wesentliche betriebliche Funktionen innerhalb des von der Organisation bestimmten Zeitraums wieder aufzunehmen sind, wenn die primären Telekommunikationsmöglichkeiten weder am primären noch am alternativen Verarbeitungs- oder Speicherort verfügbar sind.	Kontrollsysteme sind keine Geschäftssysteme
CCI-000963	PE-12	Die Organisation nutzt und unterhält eine automatische Notbeleuchtung für das Informationssystem, die sich im Fall von Stromausfällen oder -unterbrechungen einschaltet und die Notausgänge und Fluchtwege innerhalb der Einrichtung abdeckt.	Kontrollsysteme erfordern keine Beleuchtung, sie funktionieren auch einwandfrei im Dunkeln.
CCI-001173	SC-19(a)	Die Organisation legt auf Basis der Möglichkeiten, bei arglistiger Nutzung das Informationssystem zu beschädigen, Nutzungsbeschränkungen für Voice over Internet Protocol (VoIP) Technologien fest.	Kontrollsysteme nutzen kein VoIP
CCI-001174	SC-19(a)	Die Organisation legt auf Basis der Möglichkeiten, bei arglistiger Nutzung das Informationssystem zu beschädigen, Richtlinien zur Umsetzung von Voice over Internet Protocol (VoIP) Technologien fest.	Kontrollsysteme nutzen kein VoIP
CCI-001175	SC-19(b)	Die Organisation genehmigt die Nutzung von VoIP innerhalb des Informationssystems.	Kontrollsysteme nutzen kein VoIP
CCI-001176	SC-19(b)	Die Organisation überwacht die Nutzung von VoIP innerhalb des Informationssystems.	Kontrollsysteme nutzen kein VoIP
CCI-001177	SC-19(b)	Die Organisation kontrolliert die Nutzung von VoIP innerhalb des Informationssystems.	Kontrollsysteme nutzen kein VoIP
CCI-001178	SC-20(a)	Das Informationssystem stellt zusätzliche Authentifizierungswerkzeuge für Datenquellen sowie autoritative Namensauflösungsangaben zur Verfügung, die das System als Reaktion auf externe Namen-/Adressenauflösungs-Anfragen zurücksendet.	Kontrollsysteme agieren nicht als DNS Server für externe Clients
CCI-002462	SC-20(a)	Das Informationssystem stellt zusätzliche Authentifizierungswerkzeuge für Integrität sowie autoritative Namensauflösungsangaben zur Verfügung, die das System als Reaktion auf externe Namen-/Adressenauflösungs-Anfragen zurücksendet.	Kontrollsysteme agieren nicht als DNS Server für externe Clients
CCI-001179	SC-20(b)	Wenn es als Teil eines verteilten, hierarchischen Namensraums betrieben wird, stellt das Informationssystem die Mittel bereit, um den Sicherheitsstatus von untergeordneten Zonen anzuzeigen.	Kontrollsysteme agieren nicht als DNS Server für externe Clients

Tabelle H-2: Für Kontrollsysteme ungeeignete CCIs			
CCI #	800-53 Kontroll- text Indikator	CCI-Definition	Begründung für Nicht- aufnahme
CCI-001663	SC-20(b)	Wenn es als Teil eines verteilten, hierarchischen Namensraums betrieben wird, stellt das Informationssystem die Mittel bereit, um die Verifizierung einer Vertrauens- kette zwischen übergeordneten und untergeordneten Domains zu ermöglichen (wenn die untergeordnete si-	Kontrollsysteme agieren nicht als DNS Server für externe Clients
CCI-001182	SC-22	Die Informationssysteme, die gemeinsam Namens-/Adressenauflösungs-Dienste für eine Organisation bereitstellen, sind fehlertolerant.	Kontrollsysteme agieren nicht als DNS Server für externe Clients
CCI-001183	SC-22	Die Informationssysteme, die gemeinsam Namens-/Adressenauflösungs-Dienste für eine Organisation bereitstellen, implementieren interne/externe Rollentrennung.	Kontrollsysteme agieren nicht als DNS Server für externe Clients
CCI-002395	SC-7(b)	Das Informationssystem implementiert Subnetze für öffentlich zugängliche Systemkomponenten, die physisch bzw. logisch von internen organisationsbezogenen Netzwerken getrennt sind.	Kontrollsysteme sind nicht öffentlich zugänglich
CCI-002741	SI-8(a)	Die Organisation nutzt Mechanismen zum Spamschutz an Eingangspunkten des Informationssystems, um unerwünschte Nachrichten zu erfassen und entsprechende	Kontrollsystem nutzt keine eingehende E-Mail.
CCI-002742	SI-8(a)	Die Organisation nutzt Mechanismen zum Spamschutz an Ausgangspunkten des Informationssystems, um unerwünschte Nachrichten zu erfassen und entsprechende	Kontrollsystem nutzt keine eingehende E-Mail.
CCI-001306	SI-8(b)	Die Organisation aktualisiert Spamschutz-Mechanismen, wenn neue Versionen gemäß organisationsbezogener Richtlinien und Verfahrensweisen im Konfigurationsmanagement verfügbar sind.	Kontrollsystem nutzt keine eingehende E-Mail.
CCI-001307	SI-8(1)	Die Organisation verwaltet Spamschutz-Mechanismen zentral.	Kontrollsystem nutzt keine eingehende E-Mail.
CCI-001308	SI-8(2)	Das Informationssystem aktualisiert Spamschutz-Mechanismen automatisch.	Kontrollsystem nutzt keine eingehende E-Mail.

Tabelle H-3: CCIs, die aus der Grundvorgabe für Kontrollsysteme mit GERINGEN Auswirkungen entfernt wurden			
CCI #	800-53 Kontroll-text Indikator	CCI-Definition	Begründung für Entfernung aus Grundvorgabe GERING
CCI-000443	CP-2(a)(1)	Die Organisation entwickelt für das Informationssystem einen Krisenplan, der wesentliche Aufgaben bezeichnet.	Ein Kontrollsystem mit GERINGEN Auswirkungen hat keine „wesentliche“ Aufgabe.
CCI-000450	CP-2(a)(4)	Die Organisation entwickelt für das Informationssystem einen Krisenplan, der den Erhalt wesentlicher Aufgaben trotz Beeinträchtigung des Informationssystems bestimmt.	Ein Kontrollsystem mit GERINGEN Auswirkungen hat keine „wesentliche“ Aufgabe.
CCI-000452	CP-2(a)(4)	Die Organisation entwickelt für das Informationssystem einen Krisenplan, der den Erhalt wesentlicher Aufgaben trotz Gefährdung des Informationssystems bestimmt.	Ein Kontrollsystem mit GERINGEN Auswirkungen hat keine „wesentliche“ Aufgabe.
CCI-000454	CP-2(a)(4)	Die Organisation entwickelt einen Krisenplan für das Informationssystem, welcher den Erhalt wesentlicher Aufgaben trotz Ausfall des Informationssystems bestimmt.	Ein Kontrollsystem mit GERINGEN Auswirkungen hat keine „wesentliche“ Aufgabe.
CCI-002955	PE-11	Die Organisation stellt eine kurzzeitige unterbrechungsfreie Stromversorgung zur Verfügung, um eine ordnungsgemäße Abschaltung des Informationssystems bzw. den Übergang des Informationssystems zu einer dauerhaften alternativen Stromversorgung im Fall eines Verlusts einer primären Stromquelle zu ermöglichen.	NIST 800-53 sieht dies bei den Grundvorgaben für GERINGE Auswirkungen nicht vor. In NIST 800-82 ist dies mit der Begründung „Kontrollsystem kann wichtige Maßnahmen unterstützen...“ aufgeführt. Per Definition ist ein Kontrollsystem, das „wichtige Maßnahmen“ unterstützt, kein System mit GERINGEN Auswirkungen.
CCI-000961	PE-11(1)	Die Organisation stellt eine dauerhafte alternative Stromversorgung für das Informationssystem zur Verfügung, die in der Lage ist, die erforderliche Mindest-Funktionsbereitschaft im Falle eines längeren Ausfalls der primären Stromquelle zu erhalten.	NIST 800-53 sieht dies bei den Grundvorgaben für GERINGE Auswirkungen nicht vor. In NIST 800-82 ist dies mit der Begründung „Kontrollsystem kann wichtige Maßnahmen unterstützen...“ aufgeführt. Per Definition ist ein Kontrollsystem, das „wichtige Maßnahmen“ unterstützt, kein System mit GERINGEN Auswirkungen.
CCI-000216	PM-8	Die Organisation entwickelt und dokumentiert einen Schutzplan für kritische Infrastruktur und Schlüsselressourcen, der Fragen der Informationssicherheit behandelt.	Ein Kontrollsystem mit GERINGEN Auswirkungen befasst sich nicht mit kritischer Infrastruktur.
CCI-001640	PM-8	Die Organisation aktualisiert den Schutzplan für kritische Infrastruktur und Schlüsselressourcen, der Fragen der Informationssicherheit behandelt.	Ein Kontrollsystem mit GERINGEN Auswirkungen befasst sich nicht mit kritischer Infrastruktur.
CCI-002449	SC-13	Die Organisation legt die kryptographischen Nutzungen und die Art der für die jeweilige Nutzung erforderlichen Verschlüsselung fest, die durch das Informationssystem umgesetzt werden soll.	Ein Kontrollsystem mit GERINGEN Auswirkungen enthält keine vertraulichen Informationen

Tabelle H-3: CCIs, die aus der Grundvorgabe für Kontrollsysteme mit GERINGEN Auswirkungen entfernt wurden			
CCI #	800-53 Kontroll-text Indikator	CCI-Definition	Begründung für Entfernung aus Grundvorgabe GERING
CCI-002450	SC-13	Das Informationssystem implementiert die von der Organisation festgelegten kryptographischen Nutzungen und die Art der für die jeweilige Nutzung erforderlichen Verschlüsselung gemäß gültigen Bundesgesetzen, Durchführungsverordnungen, Richtlinien, Regelwerken, Vorschriften und Normen.	Ein Kontrollsystem mit GERINGEN Auswirkungen enthält keine vertraulichen Informationen

Tabelle H-4: Planer-CCIs für Kontrollsysteme mit GERINGEN und MITTLEREN Auswirkungen			
CCI #	800-53 Kontroll- text Indikator	CCI-Definition	Zuständigkeit
CCI-000048	AC-8(a)	Bevor Zugang zum System gewährt wird, zeigt das Informationssystem eine von der Organisation festgelegte Meldung bzw. ein Banner zur Systemnutzung mit Hinweisen zu Datenschutz und Sicherheit an, die den gültigen Bundesgesetzen, Durchführungsverordnungen, Richtlinien, Regelwerken, Vorschriften und Normen entsprechen.	Enclave Planer Nicht zweckmäßig
CCI-002247	AC-8(a)	Die Organisation legt die Meldung zur Systemnutzung bzw. das Banner fest, das den Benutzern das Informationssystem angezeigt wird, bevor Zugang zum System gewährt wird.	Def. durch DoD Enclave Planer Nicht zweckmäßig
CCI-002243	AC-8(a)(1)	Die von der Organisation festgelegte Meldung bzw. das Banner zur Nutzung des Informationssystems soll angeben, dass Benutzer auf ein Informationssystem der US-Regierung zugreifen.	Def. durch DoD Enclave Planer Nicht zweckmäßig
CCI-002244	AC-8(a)(2)	Die von der Organisation festgelegte Meldung bzw. das Banner zur Nutzung des Informationssystems soll angeben, dass die Nutzung des Informationssystems überwacht oder aufgezeichnet werden und einer Überprüfung unterliegen kann.	Def. durch DoD Enclave Planer Nicht zweckmäßig
CCI-002245	AC-8(a)(3)	Die von der Organisation festgelegte Meldung bzw. das Banner zur Nutzung des Informationssystems soll angeben, dass die nicht genehmigte Nutzung des Informationssystems unzulässig ist und straf- und zivilrechtlich verfolgt werden kann.	Def. durch DoD Enclave Planer Nicht zweckmäßig
CCI-002246	AC-8(a)(4)	Die von der Organisation festgelegte Meldung bzw. das Banner zur Nutzung des Informationssystems soll angeben, dass die Nutzung des Informationssystems als Zustimmung zur Überwachung und Aufzeichnung gilt.	Def. durch DoD Enclave Planer Nicht zweckmäßig
CCI-000050	AC-8(b)	Das Informationssystem lässt die Meldung bzw. das Banner auf dem Bildschirm bestehen, bis die Benutzer die Nutzungsbedingungen bestätigen und eindeutige Schritte zum Einloggen bzw. zum weiteren Zugriff unternehmen.	Enclave Planer
CCI-002248	AC-8(c)(1)	Die Organisation legt die Nutzungsbedingungen fest, die den Benutzern angezeigt werden sollen, bevor weiterer Zugang gewährt wird.	Def. durch DoD Enclave Planer Nicht zweckmäßig
CCI-000139	AU-5(a)	Das Informationssystem alarmiert bestimmte, von der Organisation benannte Personen bzw. Rollen im Falle eines Fehlers bei der Prüfungsabwicklung.	Enclave Planer Nicht zweckmäßig
CCI-000140	AU-5(b)	Das Informationssystem ergreift im Falle eines Fehlers bei der Überwachung (z.B. Herunterfahren des Informationssystems, Überschreiben der ältesten Prüfaufzeichnungen, Unterbinden der Erstellung von Prüfaufzeichnungen) von der Organisation festgelegte Maßnahmen.	Enclave Planer Nicht zweckmäßig
CCI-001490	AU-5(b)	Die Organisation legt die Maßnahmen fest, die das Informationssystem bei einem Fehler bei der Überwachung ergreifen soll (z.B. Herunterfahren des Informationssystems, Überschreiben der ältesten Prüfaufzeichnungen, Unterbinden der Erstellung von Prüfaufzeichnungen).	Enclave Planer Nicht Planer Nicht zweckmäßig

Tabelle H-4: Planer-CCIs für Kontrollsysteme mit GERINGEN und MITTLEREN Auswirkungen			
CCI #	800-53 Kontroll- text Indikator	CCI-Definition	Zuständigkeit
CCI-000258	CA-3(b)	Die Organisation dokumentiert bei jeder Verbindung die Schnittstellenmerkmale.	Enclave Planer Nicht Planer
CCI-000550	CP-10	Nach einer Störung sorgt die Organisation für die Wiederherstellung und das Zurücksetzen des Informationssystems auf einen bekannten Stand.	Enclave Planer Nicht Planer
CCI-000551	CP-10	Nach einer Gefährdung sorgt die Organisation für die Wiederherstellung und Rekonstitution des Informationssystems auf einen bekannten Stand.	Enclave Planer Nicht Planer
CCI-000552	CP-10	Nach einem Ausfall sorgt die Organisation für die Wiederherstellung und Rekonstitution des Informationssystems auf einen bekannten Stand.	Enclave Planer Nicht Planer
CCI-000764	IA-2	Das Informationssystem identifiziert und authentifiziert eindeutig Benutzer der Organisation (oder Prozesse, die im Auftrag der Benutzer der Organisation agieren).	Enclave Planer Nicht zweckmäßig
CCI-000765	IA-2(1)	Das Informationssystem führt eine von verschiedenen Faktoren abhängige Authentifizierung für den Netzwerkzugriff auf privilegierte Konten durch.	Enclave Planer Nicht zweckmäßig
CCI-001953	IA-2(12)	Das Informationssystem akzeptiert Personal Identity Verification (PIV) Berechtigungsnachweise.	Enclave Planer Nicht zweckmäßig
CCI-001954	IA-2(12)	Das Informationssystem führt eine elektronische Prüfung der Personal Identity Verification (PIV) Berechtigungsnachweise durch.	Enclave Planer Nicht zweckmäßig
CCI-000777	IA-3	Die Organisation legt eine Liste mit speziellen Geräten bzw. Gerätetypen fest, für die eine Identifikation und Authentifizierung erforderlich ist, bevor eine Verbindung zum Informationssystem hergestellt wird.	Def. durch DoD Enclave Planer Nicht zweckmäßig
CCI-000778	IA-3	Das Informationssystem identifiziert eindeutig eine von der Organisation festgelegte Liste spezieller Geräte bzw. Gerätetypen, bevor eine lokale Verbindung, Remote-Verbindung oder Netzwerkverbindung hergestellt wird.	Enclave Planer Nicht zweckmäßig
CCI-001958	IA-3	Das Informationssystem authentifiziert eine von der Organisation festgelegte Liste spezieller Geräte bzw. Gerätetypen, bevor eine lokale Verbindung, Remote-Verbindung oder Netzwerkverbindung hergestellt wird.	Enclave Planer Nicht zweckmäßig
CCI-000192	IA-5(1)(a)	Das Informationssystem erzwingt Passwort-Komplexität durch die Mindestanzahl verwendeter Großbuchstaben.	Enclave Planer
CCI-000193	IA-5(1)(a)	Das Informationssystem erzwingt Passwort-Komplexität durch die Mindestanzahl verwendeter Kleinbuchstaben.	Enclave Planer
CCI-000194	IA-5(1)(a)	Das Informationssystem erzwingt Passwort-Komplexität durch die Mindestanzahl verwendeter Ziffern.	Enclave Planer
CCI-000205	IA-5(1)(a)	Das Informationssystem erzwingt eine Mindestlänge für Passwörter.	Enclave Planer

Tabelle H-4: Planer-CCIs für Kontrollsysteme mit GERINGEN und MITTLEREN Auswirkungen			
CCI #	800-53 Kontroll- text Indikator	CCI-Definition	Zuständigkeit
CCI-001619	IA-5(1)(a)	Das Informationssystem erzwingt Passwort-Komplexität durch die Mindestanzahl verwendeter Sonderzeichen.	Enclave Planer
CCI-000195	IA-5(1)(b)	Das Informationssystem erzwingt bei der Erstellung neuer Passwörter zur passwortbasierten Authentifizierung, dass mindestens eine von der Organisation bestimmte Anzahl von Zeichen geändert wird.	Enclave Planer
CCI-000196	IA-5(1)(c)	Für eine passwortbasierte Authentifizierung speichert das Informationssystem nur kryptographisch gesicherte Passwörter.	Enclave Planer Nicht zweckmäßig
CCI-000197	IA-5(1)(c)	Für eine passwort-basierte Authentifizierung übermittelt das Informationssystem nur kryptographisch gesicherte Passwörter.	Enclave Planer
CCI-000199	IA-5(1)(d)	Das Informationssystem erzwingt Begrenzungen bei der maximalen Nutzungsdauer der Passwörter.	Enclave Planer
CCI-000200	IA-5(1)(e)	Das Informationssystem untersagt die Wiederverwendung von Passwörtern für eine von der Organisation festgelegten Anzahl von Passwortgenerierungen.	Enclave Planer Nicht Planer Nicht zweckmäßig
CCI-001618	IA-5(1)(e)	Die Organisation bestimmt die Anzahl der Passwortgenerierungen, für die eine Wiederverwendung des Passworts untersagt ist.	Def. durch DoD Enclave Planer Nicht zweckmäßig
CCI-002041	IA-5(1)(f)	Das Informationssystem erlaubt die Verwendung eines temporären Passworts, um sich in ein System einzuloggen, wo dann sofort auf ein permanentes Passwort gewechselt wird.	Enclave Planer Nicht zweckmäßig
CCI-002002	IA-5(11)	Die Organisation definiert die Qualitätsanforderungen für die Token, die durch die Mechanismen des Informationssystems bei einer tokenbasierten Authentifizierung verwendet werden.	Def. durch DoD Enclave Planer Nicht zweckmäßig
CCI-002003	IA-5(11)	Bei einer tokenbasierten Authentifizierung verwendet das Informationssystem Mechanismen, die die von der Organisation festgelegten Qualitätsanforderungen in Bezug auf Token erfüllen.	Enclave Planer Nicht zweckmäßig
CCI-000206	IA-6	Das Informationssystem verbirgt das Feedback der Authentifizierungsinformation während des Authentifizierungsvorgangs, um die Informationen vor möglicher Instrumentalisierung/Nutzung durch nicht autorisierte Personen zu schützen.	Enclave Planer Nicht zweckmäßig
CCI-000803	IA-7	Das Informationssystem setzt Mechanismen zur Authentifizierung in ein kryptografisches Modul um, das den Anforderungen der gültigen Bundesgesetze, Durchführungsverordnungen, Richtlinien, Regelwerke, Vorschriften und Normen, und Anleitungen für eine solche Authentifizierung entspricht.	Enclave Planer Nicht zweckmäßig
CCI-003051	PL-2(a)(2)	Der Sicherheitsplan der Organisation für das Informationssystem bestimmt eindeutig die Autorisierungsgrenze für das System.	Enclave Planer Nicht Planer

Tabelle H-4: Planer-CCIs für Kontrollsysteme mit GERINGEN und MITTLEREN Auswirkungen			
CCI #	800-53 Kontroll-text Indikator	CCI-Definition	Zuständigkeit
CCI-000236	PM-11(b)	Die Organisation legt die Anforderungen an den Schutz von Informationen fest, die aus den definierten Betriebs-/ Geschäftsprozessen entstehen, und ändert die Prozesse gegebenenfalls, bis eine erzielbare Reihe von Schutzbedürfnissen erreicht wird.	Enclave Planer Nicht Planer
CCI-001054	RA-5(a)	Die Organisation durchsucht das Informationssystem nach Anfälligkeiten und gehosteten Anwendungen in einer von der Organisation festgelegten Häufigkeit.	Enclave Planer Nicht Planer
CCI-001055	RA-5(a)	Die Organisation bestimmt die Häufigkeit, in der das Informationssystem und gehostete Anwendungen auf Anfälligkeiten durchsucht werden.	Def. durch DoD Enclave Planer Nicht zweckmäßig
CCI-001056	RA-5(a)	Die Organisation durchsucht das Informationssystem und gehostete Anwendungen, wenn neue Schwachstellen, die das System/die Anwendungen möglicherweise beeinträchtigen könnten, festgestellt und gemeldet werden.	Enclave Planer Nicht Planer
CCI-001641	RA-5(a)	Die Organisation bestimmt den Prozessablauf zur Durchführung von Random Scans auf Schwachstellen des Informationssystems und gehosteter Anwendungen.	Enclave Planer Nicht Planer Nicht zweckmäßig
CCI-001643	RA-5(a)	Die Organisation durchsucht das Informationssystem nach Anfälligkeiten und gehosteten Anwendungen mit einem von der Organisation festgelegten Prozessablauf für Random Scans.	Enclave Planer Nicht Planer
CCI-001057	RA-5(b)	Die Organisation verwendet Scanning Tools, um Schwachstellen zu finden und Techniken, die Interoperabilität zwischen den Tools ermöglichen und Teilbereiche des Schwachstellen-Management Prozesses automatisieren, indem Standards für folgendes verwendet werden: Spezifizierung von Plattformen, Softwarefehler und unrichtige Konfigurationen, Formatieren von Checklisten und Prüfverfahren und Erfassung der Auswirkungen von Schwachstellen.	Enclave Planer Nicht Planer Nicht zweckmäßig
CCI-001058	RA-5(c)	Die Organisation analysiert die Berichte und Ergebnisse der Schwachstellenscans von Sicherheitskontrollbeurteilungen.	Enclave Planer Nicht Planer
CCI-001059	RA-5(d)	Die Organisation beseitigt Legitimate Vulnerabilities (zulässige Schwachstellen) in von der Organisation festgelegten Reaktionszeiten entsprechend einer organisationsbezogenen Risikobewertung.	Enclave Planer Nicht Planer Nicht zweckmäßig
CCI-003116	SA-4(10)	Die Organisation nutzt nur IT-Produkte, die auf der von FIPS PUB 201-2 genehmigten Produktliste für Personal Identity Verification (PIV)-Fähigkeit stehen, die innerhalb der organisationsbezogenen Informationssysteme umgesetzt werden.	Enclave Planer Nicht zweckmäßig
CCI-001093	SC-5	Die Organisation bestimmt die Arten von Denial-of-Service Angriffen (oder gibt Verweise auf Quellen aktueller Denial-of-Service Angriffe), die das Informationssystem angehen kann.	Enclave Planer

Tabelle H-4: Planer-CCIs für Kontrollsysteme mit GERINGEN und MITTLEREN Auswirkungen			
CCI #	800-53 Kontroll-text Indikator	CCI-Definition	Zuständigkeit
CCI-002385	SC-5	Das Informationssystem schützt vor oder beschränkt die Auswirkungen der von der Organisation festgelegten Arten von Denial-of-Service Angriffen, indem von der Organisation festgelegte Sicherheitsmaßnahmen eingesetzt werden.	Enclave Planer
CCI-002386	SC-5	Die Organisation legt die Sicherheitsmaßnahmen fest, die eingesetzt werden sollen, um das Informationssystem gegen die Auswirkungen von Denial-of Service Angriffen zu schützen/diese zu beschränken.	Enclave Planer Nicht Planer
CCI-001097	SC-7(a)	Das Informationssystem überwacht und kontrolliert Kommunikationen an der äußeren Grenze des Systems und an wichtigen internen Grenzen innerhalb des Systems.	Def. durch DoD Enclave Planer Nicht zweckmäßig
CCI-002544	SC-41	Die Organisation definiert die Informationssysteme oder Informationssystem-Komponenten, auf denen von der Organisation festgelegte Verbindungsschnittstellen bzw. Ein-/Ausgangsgeräte physisch deaktiviert oder entfernt werden sollen.	Enclave Planer Nicht Planer
CCI-002545	SC-41	Die Organisation definiert Verbindungsschnittstellen bzw. Ein-/Ausgangsgeräte, die von durch die Organisation festgelegten Informationssystemen oder Informationssystem-Komponenten physisch deaktiviert oder entfernt werden sollen.	Enclave Planer Nicht Planer
CCI-001241	SI-3(c)(1)	Die Organisation konfiguriert Schutzmechanismen gegen Schadcode, um regelmäßige Scans des Informationssystems in einer von der Organisation bestimmten Häufigkeit durchzuführen.	Enclave Planer Nicht Planer
CCI-001253	SI-4(a)(1)	Die Organisation definiert die Zielvorgaben der Überwachung zur Verhinderung von Angriffen und Indikatoren möglicher Angriffe auf das Informationssystem.	Def. durch DoD Enclave Planer Nicht zweckmäßig
CCI-002645	SI-4(b)	Die Organisation legt die Techniken und Methoden fest, die verwendet werden, um die unbefugte Nutzung des Informationssystems zu erkennen.	Enclave Planer Nicht Planer
CCI-002110	AC-2(a)	Die Organisation bestimmt die Kontoarten des Informationssystems, welche die organisationsbezogenen Aufgaben/betriebliche Funktionen unterstützt.	Planer
CCI-000213	AC-3	Das Informationssystem erzwingt genehmigte Autorisierungen für den logischen Zugang zu Informationen und Systemressourcen gemäß gültiger Zugangskontrollrichtlinien.	Planer
CCI-000043	AC-7(a)	Die Organisation bestimmt die maximale Anzahl der aufeinanderfolgenden ungültigen Login-Versuche in das Informationssystem durch einen Benutzer in einem von der Organisation festgelegten Zeitraum.	Definition durch DoD Planer Nicht zweckmäßig
CCI-000044	AC-7(a)	Das Informationssystem erzwingt die von der Organisation festgelegte Beschränkung von aufeinanderfolgenden ungültigen Login-Versuchen durch einen Benutzer in einem von der Organisation festgelegten Zeitraum.	Planer
CCI-001423	AC-7(a)	Die Organisation legt den Zeitraum fest, in dem die von der Organisation festgelegte maximale Anzahl aufeinanderfolgender ungültiger Login-Versuche erfolgt.	Definition durch DoD Planer Nicht zweckmäßig

Tabelle H-4: Planer-CCIs für Kontrollsysteme mit GERINGEN und MITTLEREN Auswirkungen			
CCI #	800-53 Kontroll-text Indikator	CCI-Definition	Zuständigkeit
CCI-002236	AC-7(b)	Die Organisation bestimmt den Zeitraum, in dem das Informationssystem das Konto / die Verbindung automatisch sperrt, wenn die maximale Anzahl misslungener Versuche überschritten ist.	Definition durch DoD Planer Nicht zweckmäßig
CCI-002237	AC-7(b)	Die Organisation bestimmt den Verzögerungsalgorithmus, den das Informationssystem anwenden soll, um die nächste Login-Aufforderung zu verzögern, wenn die maximale Anzahl misslungener Versuche überschritten ist.	Definition durch DoD Planer Nicht zweckmäßig
CCI-002238	AC-7(b)	Das Informationssystem sperrt automatisch das Konto / die Verbindung für entweder einen von der Organisation festgesetzten Zeitraum, bis das gesperrte Konto / die Verbindung von einem Administrator freigegeben wird, oder verzögert die nächste Login-Aufforderung entsprechend dem von der Organisation festgelegten Verzögerungsalgorithmus, wenn die maximale Anzahl misslungener Versuche überschritten wird.	Planer Nicht zweckmäßig
CCI-000061	AC-14(a)	Die Organisation bezeichnet und bestimmt von der Organisation festgelegte Benutzeraktionen, die auf dem Informationssystem ohne Identifizierung oder Authentifizierung im Einklang mit organisationsbezogenen Aufgaben/betriebliche Funktionen durchgeführt werden können.	Planer
CCI-000232	AC-14(b)	Die Organisation dokumentiert und liefert unterstützende Begründungen im Sicherheitsplan für das Informationssystem, Benutzeraktionen, für die keine Identifizierung oder Authentifizierung erforderlich ist.	Planer
CCI-001438	AC-18(a)	Die Organisation richtet Nutzungsbeschränkungen für drahtlosen Zugriff ein.	Planer Kein Planer
CCI-001439	AC-18(a)	Die Organisation erstellt Anleitungen zur Umsetzung für drahtlosen Zugriff.	Planer Kein Planer
CCI-002323	AC-18(a)	Die Organisation erstellt Konfigurationen / Anschlussbedingungen für drahtlosen Zugriff.	Planer Kein Planer
CCI-001441	AC-18(b)	Die Organisation autorisiert drahtlosen Zugriff zum Informationssystem, bevor sie diese Art Verbindung ermöglicht.	Planer Kein Planer
CCI-000123	AU-2(a)	Die Organisation bestimmt, dass das Informationssystem in der Lage sein muss, eine Prüfung einer von der Organisation festgelegte Liste prüfbarer Ereignisse durchzuführen.	Planer Kein Planer
CCI-001571	AU-2(a)	Die Organisation legt die prüfbaren Ereignisse des Informationssystems fest.	Definition durch DoD Planer Nicht zweckmäßig
CCI-000125	AU-2(c)	Die Organisation liefert eine Begründung, weshalb die Liste prüfbarer Ereignisse als angemessen gilt, um nachträgliche Untersuchungen von Sicherheitsvorfällen zu unterstützen.	Planer Kein Planer
CCI-001485	AU-2(d)	Die Organisation legt die Ereignisse fest, die auf dem Informationssystem mit einer von der Organisation festgelegten (oder situationsabhängigen) Prüfungshäufigkeit jedes bezeichneten Ereignisses zu prüfen sind.	Planer Kein Planer

Tabelle H-4: Planer-CCIs für Kontrollsysteme mit GERINGEN und MITTLEREN Auswirkungen			
CCI #	800-53 Kontroll-text Indikator	CCI-Definition	Zuständigkeit
CCI-000130	AU-3	Das Informationssystem generiert Prüfprotokolle, die Informationen enthalten, aus denen hervorgeht, welche Art Ereignis eingetreten ist.	Planer
CCI-000131	AU-3	Das Informationssystem generiert Prüfprotokolle, die Informationen enthalten, aus denen hervorgeht, wann ein Ereignis eingetreten ist.	Planer
CCI-000132	AU-3	Das Informationssystem generiert Prüfprotokolle, die Informationen enthalten, aus denen hervorgeht, wo das Ereignis eingetreten ist.	Planer
CCI-000133	AU-3	Das Informationssystem generiert Prüfprotokolle, die Informationen enthalten, aus denen die Quelle des Ereignisses hervorgeht.	Planer
CCI-000134	AU-3	Das Informationssystem generiert Prüfprotokolle, die Informationen enthalten, aus denen das Ergebnis des Ereignisses hervorgeht.	Planer
CCI-001487	AU-3	Das Informationssystem generiert Prüfprotokolle, die Informationen enthalten, aus denen die Identität aller Personen oder Objekten, die mit dem Ereignis in Verbindung stehen, hervorgeht.	Planer Nicht zweckmäßig
CCI-001848	AU-4	Die Organisation legt die Anforderungen für die Aufbewahrung von Prüfprotokollen fest.	Planer Kein Planer
CCI-001849	AU-4	Die Organisation stellt Kapazitäten zur Aufbewahrung von Prüfprotokollen gemäß von der Organisation festgelegten Anforderungen für die Aufbewahrung von Prüfprotokollen bereit.	Planer Kein Planer
CCI-000159	AU-8(a)	Das Informationssystem nutzt interne Zeitmesser, um Zeitstempel für Prüfprotokolle zu generieren.	Planer
CCI-001889	AU-8(b)	Das Informationssystem erfasst Zeitstempel für Prüfprotokolle, die die von der Organisation festgelegte Detailgenauigkeit der Zeitmessung erfüllen.	Planer
CCI-001890	AU-8(b)	Das Informationssystem erfasst Zeitstempel für Prüfprotokolle, die auf Coordinated Universal Time (UTC) oder Greenwich Mean Time (GMT) gemappt werden können.	Planer
CCI-000169	AU-12(a)	Das Informationssystem bietet die Fähigkeit, Prüfprotokolle für die prüfbaren Ereignisse, die in AU-2(a) definiert sind, bei von der Organisation festgelegten Informationssystem-Komponenten zu generieren.	Planer
CCI-001459	AU-12(a)	Die Organisation legt die Informationssystem-Komponenten fest, die in der Lage sind, Prüfprotokolle zu generieren.	Definition durch DoD Planer Nicht zweckmäßig
CCI-000171	AU-12(b)	Das Informationssystem ermöglicht von der Organisation festgelegten Personen bzw. Rollen die Auswahl, welche prüfbaren Ereignisse durch bestimmte Komponente des Informationssystems zu prüfen sind.	Planer Nicht zweckmäßig
CCI-001910	AU-12(b)	Die Organisation bestimmt Personen bzw. die Rollen, die befugt sind auszuwählen, welche prüfbaren Ereignisse durch bestimmte Komponente des Informationssystems zu prüfen sind.	Definition durch DoD Planer Nicht zweckmäßig

Tabelle H-4: Planer-CCIs für Kontrollsysteme mit GERINGEN und MITTLEREN Auswirkungen			
CCI #	800-53 Kontroll-text Indikator	CCI-Definition	Zuständigkeit
CCI-000172	AU-12(c)	Das Informationssystem generiert Prüfprotokolle für die in AU-2(d) definierten Ereignisse mit dem in AU-3 definierten Inhalt.	Planer
CCI-002102	CA-9(a)	Die Organisation bestimmt die IT-Komponente oder Komponentenklassen, die autorisiert sind, interne Verbindungen zum Informationssystem zu haben.	Planer
CCI-002103	CA-9(b)	Die Organisation dokumentiert die Schnittstellenmerkmale für jede interne Verbindung.	Planer
CCI-002104	CA-9(b)	Die Organisation dokumentiert die Sicherheitsanforderungen für jede interne Verbindung.	Planer
CCI-002105	CA-9(b)	Die Organisation dokumentiert die Art der kommunizierten Informationen für jede interne Verbindung.	Planer
CCI-000293	CM-2	Die Organisation entwickelt und dokumentiert eine aktuelle Basiskonfiguration des Informationssystems.	Planer
CCI-000363	CM-6(a)	Die Organisation legt Checklisten für Sicherheitskonfigurationen fest, die genutzt werden sollen, um Konfigurationseinstellungen für die eingesetzten IT-Systemprodukte einzurichten und zu dokumentieren.	Planer
CCI-000364	CM-6(a)	Die Organisation legt anhand von der Organisation festgelegter Checklisten für Sicherheitskonfigurationen Konfigurationseinstellungen für IT-Produkte fest, die innerhalb des Informationssystems eingesetzt werden,	Planer
CCI-000365	CM-6(a)	Die Organisation dokumentiert anhand von der Organisation festgelegter Checklisten für Sicherheitskonfigurationen, die den restriktivsten Modus im Einklang mit betrieblichen Anforderungen berücksichtigen, Konfigurationseinstellungen für IT-Produkte, die innerhalb des Informationssystems eingesetzt werden,	Definition durch DoD Planer Nicht Planer Nicht zweckmäßig
CCI-001588	CM-6(a)	Die von der Organisation festgelegten Checklisten zur Sicherheitskonfiguration berücksichtigen den restriktivsten Modus im Einklang mit betrieblichen Anforderungen.	Definition durch DoD Planer Nicht Planer Nicht zweckmäßig
CCI-001755	CM-6(c)	Die Organisation definiert die Informationssystem-Komponenten, für die jede Abweichung von den festgelegten Konfigurationseinstellungen erkannt, dokumentiert und genehmigt werden muss.	Definition durch DoD Planer Nicht Planer
CCI-000381	CM-7(a)	Die Organisation konfiguriert das Informationssystem so, dass es nur wesentliche Fähigkeiten anbietet.	Planer
CCI-000380	CM-7(b)	Die Organisation legt Funktionen, Ports, Protokolle, bzw. Dienste fest, die für das Informationssystem unzulässig bzw. eingeschränkt sind.	Planer
CCI-000382	CM-7(b)	Die Organisation konfiguriert das Informationssystem so, dass die Nutzung von durch die Organisation festgelegten Funktionen, Ports, Protokollen, bzw. Diensten unzulässig bzw. eingeschränkt ist.	Planer

Tabelle H-4: Planer-CCIs für Kontrollsysteme mit GERINGEN und MITTLEREN Auswirkungen			
CCI #	800-53 Kontroll-text Indikator	CCI-Definition	Zuständigkeit
CCI-001761	CM-7(1)(b)	Die Organisation bestimmt die Funktionen, Ports, Protokolle und Dienste innerhalb des Informationssystems, die zu deaktivieren sind, wenn sie als unnötig bzw. unsicher erachtet werden.	Planer
CCI-001762	CM-7(1)(b)	Die Organisation deaktiviert von der Organisation festgelegte Funktionen, Ports, Protokolle und Dienste innerhalb des Informationssystems, wenn sie als unnötig bzw. unsicher erachtet werden.	Planer Nicht zweckmäßig
CCI-000389	CM-8(a)(1)	Die Organisation entwickelt und dokumentiert einen Bestand an Informationssystemkomponenten, der das aktuelle Informationssystem exakt wiedergibt.	Planer
CCI-000392	CM-8(a)(2)	Die Organisation entwickelt und dokumentiert einen Bestand an Informationssystemkomponenten, der alle Komponenten innerhalb der Autorisierungsgrenze des Informationssystems beinhaltet.	Planer
CCI-000398	CM-8(a)(4)	Der Organisation definiert die Informationen, die als erforderlich erachtet werden, um eine effektive Rechenschaftspflicht für die Informationssystemkomponente zu erlangen.	Definition durch DoD Planer Nicht Planer Nicht zweckmäßig
CCI-002855	CP-12	Wenn von der Organisation festgelegte Bedingungen festgestellt werden, geht das Informationssystem in einen abgesicherten Betriebsmodus mit von der Organisation festgelegten Einschränkungen des abgesicherten Betriebsmodus.	Planer
CCI-002856	CP-12	Die Organisation legt die Bedingungen fest, unter denen, wenn diese festgestellt werden, das Informationssystem in einen abgesicherten Betriebsmodus mit von der Organisation festgelegten Beschränkungen des abgesicherten Betriebsmodus übergeht.	Planer
CCI-002857	CP-12	Die Organisation legt die Einschränkungen des abgesicherten Betriebsmodus fest, in den das Informationssystem geht, wenn von der Organisation festgelegte Bedingungen festgestellt werden.	Planer
CCI-000176	IA-5(b)	Die Organisation verwaltet Informationssystem-Authentifikatoren, indem sie einen ersten Authentifikatorinhalt für Authentifikatoren, die von der Organisation festgelegt werden, festsetzt.	Planer Kein Planer
CCI-001544	IA-5(c)	Die Organisation verwaltet Informationssystem-Authentifikatoren, indem sie sicherstellt, dass Authentifikatoren ausreichende Mechanismusstärke für die geplante Nutzung besitzen.	Planer Nicht Planer Nicht zweckmäßig
CCI-001989	IA-5(e)	Die Organisation verwaltet Informationssystem-Authentifikatoren, indem sie Default-Inhalte von Authentifikatoren vor der Installation im Informationssystem ändert.	Planer
CCI-000182	IA-5(g)	Die Organisation verwaltet Informationssystem-Authentifikatoren, indem sie Authentifikatoren entsprechend der von der Organisation festgelegten Zeitspanne nach Art des Authentifikators ändert/aktualisiert.	Definition durch DoD Planer Nicht Planer Nicht zweckmäßig
CCI-001610	IA-5(g)	Die Organisation bestimmt die Zeitspanne (nach Art des Authentifikators) zur Änderung/Aktualisierung von Authentifikatoren.	Definition durch DoD Planer Nicht Planer Nicht zweckmäßig

Tabelle H-4: Planer-CCIs für Kontrollsysteme mit GERINGEN und MITTLEREN Auswirkungen			
CCI #	800-53 Kontroll-text Indikator	CCI-Definition	Zuständigkeit
CCI-001611	IA-5(1)(a)	Die Organisation bestimmt die Mindestanzahl an Sonderzeichen für die Durchsetzung der Passwortkomplexität.	Definition durch DoD Planer Nicht zweckmäßig
CCI-001612	IA-5(1)(a)	Die Organisation bestimmt die Mindestanzahl an Großbuchstaben für die Durchsetzung der Passwortkomplexität.	Definition durch DoD Planer Nicht zweckmäßig
CCI-001613	IA-5(1)(a)	Die Organisation bestimmt die Mindestanzahl an Kleinbuchstaben für die Durchsetzung der Passwortkomplexität.	Definition durch DoD Planer Nicht zweckmäßig
CCI-001614	IA-5(1)(a)	Die Organisation bestimmt die Mindestanzahl an Ziffern für die Durchsetzung der Passwortkomplexität.	Definition durch DoD Planer Nicht zweckmäßig
CCI-001615	IA-5(1)(b)	Die Organisation bestimmt die Mindestanzahl Zeichen, die geändert werden, wenn neue Passwörter erstellt werden.	Definition durch DoD Planer Nicht zweckmäßig
CCI-000198	IA-5(1)(d)	Das Informationssystem erzwingt Einschränkungen bei der Mindest-Nutzungsdauer der Passwörter.	Planer Nicht zweckmäßig
CCI-001616	IA-5(1)(d)	Die Organisation legt Einschränkungen für die Mindest-Nutzungsdauer der Passwörter fest.	Definition durch DoD Planer Nicht zweckmäßig
CCI-001617	IA-5(1)(d)	Die Organisation legt Einschränkungen für die maximale Nutzungsdauer der Passwörter fest.	Definition durch DoD Planer Nicht zweckmäßig
CCI-003053	PL-2(a)(4)	Der Sicherheitsplan der Organisation für das Informationssystem liefert die Sicherheitseinstufung des Informationssystems einschließlich unterstützender Begründung.	Planer Kein Planer
CCI-000207	PM-5	Die Organisation entwickelt und führt ein Bestandsverzeichnis ihres Informationssystems.	Planer Nicht Planer Nicht zweckmäßig
CCI-001048	RA-3(a)	Die Organisation führt eine Risikobewertung des Informationssystems sowie der Informationen durch, die es verarbeitet, speichert oder übermittelt, einschließlich Wahrscheinlichkeit und Ausmaß des Schadens, der durch unbefugten Zugriff, Nutzung, Offenlegung, Zusammenbruch, Modifizierung oder Zerstörung entsteht.	Planer Kein Planer
CCI-003124	SA-5(a)(1)	Die Organisation beschafft sich Administrator-Unterlagen für das Informationssystem, die Systemkomponente oder Informationssystem-Dienste, die eine sichere Konfiguration des Systems, der Komponente oder der Dienste erläutern.	Planer Kein Planer

CCI-003125	SA-5(a)(1)	Die Organisation beschafft sich Administrator-Unterlagen für das Informationssystem, die Systemkomponente oder Informationssystem-Dienste, die eine sichere Installation des Systems, der Komponente oder der Dienste erläutern.	Planer Kein Planer
CCI-003126	SA-5(a)(1)	Die Organisation beschafft sich Administrator-Unterlagen für das Informationssystem, die Systemkomponente oder Informationssystem-Dienste, die einen sicheren Betrieb des Systems, der Komponente oder der Dienste erläutern.	Planer Kein Planer

Tabelle H-4: Planer-CCIs für Kontrollsysteme mit GERINGEN und MITTLEREN Auswirkungen			
CCI #	800-53 Kontroll- text Indikator	CCI-Definition	Zuständigkeit
CCI-003127	SA-5(a)(2)	Die Organisation beschafft sich Administrator-Unterlagen für das Informationssystem, die Systemkomponente oder Informationssystem-Dienste, die eine effektive Nutzung und Erhaltung der Sicherheitsfunktionen/-mechanismen erläutern.	Planer Kein Planer
CCI-003128	SA-5(a)(3)	Die Organisation beschafft sich Administrator-Unterlagen für das Informationssystem, der Systemkomponente oder Informationssystem-Dienste, die bekannte Schwachstellen in Bezug auf Konfiguration und Nutzung von Verwaltungsfunktionen (d.h. privilegierte Funktionen) erläutern.	Planer Kein Planer
CCI-003129	SA-5(b)(1)	Die Organisation beschafft sich Benutzerdokumentation für das Informationssystem, die Systemkomponente oder den Informationssystem-Dienst, die für die Benutzer zugänglichen Sicherheitsfunktionen/-mechanismen erläutern sowie beschreiben, wie diese Sicherheitsfunktionen/-mechanismen effektiv genutzt werden können.	Planer Kein Planer
CCI-003130	SA-5(b)(2)	Die Organisation beschafft sich Benutzerdokumentation für das Informationssystem, die Systemkomponente oder den Informationssystem-Dienst, in welcher Verfahren für Benutzerinteraktionen beschrieben sind, die Personen in die Lage versetzen, das System, die Komponente oder den Dienst auf sicherere Weise zu nutzen.	Planer Kein Planer
CCI-003131	SA-5(b)(3)	Die Organisation beschafft sich Benutzerdokumentation für das Informationssystem, die Systemkomponente oder den Informationssystem-Dienst, in der die Pflichten des Benutzers bezüglich Erhaltung der Sicherheit des Systems, der Komponente oder des Dienstes beschrieben sind.	Planer Kein Planer
CCI-002530	SC-39	Das Informationssystem unterhält eine eigene Ausführungsdomäne für jede Prozessausführung.	Planer
CCI-002546	SC-41	Die Organisation deaktiviert oder entfernt von der Organisation festgelegte Verbindungsschnittstellen bzw. Ein-/Ausgangsgeräte physisch auf von der Organisation festgelegten Informationssystemen bzw. Informationssystemkomponenten.	Planer Nicht zweckmäßig
CCI-002623	SI-3(c)(1)	Die Organisation bestimmt die Häufigkeit, mit der regelmäßige Scans des Informationssystem auf Schadcodes durchgeführt werden.	Definition durch DoD Planer Nicht zweckmäßig
CCI-002773	SI-17	Die Organisation legt ausfallsichere Verfahren fest, die das Informationssystem umsetzen muss, wenn von der Organisation festgelegte Ausfallbedingungen auftreten.	Planer
CCI-002774	SI-17	Die Organisation legt Ausfallbedingungen fest, bei denen, sollten sie eintreten, das Informationssystem die von der Organisation festgelegten ausfallsicheren Verfahren umsetzt.	Planer
CCI-002775	SI-17	Das Informationssystem setzt von der Organisation festgelegte ausfallsichere Verfahren um, wenn von der Organisation festgelegte Umstände eintreten.	Planer

Tabelle H-5: Zusätzliche Planer-CCIs für Kontrollsysteme mit MITTLEREN Auswirkungen			
CCI #	800-53 Kontroll- text Indikator	CCI-Definition	Zuständigkeit
CCI-001682	AC-2(2)	Das Informationssystem entfernt oder deaktiviert nach Ablauf eines durch die Organisation für alle Kontoarten festgelegten Zeitraums automatisch Notfallkonten.	Def. durch DoD Enclave Planer Nicht Planer Nicht zweckmäßig
CCI-001361	AC-2(2)	Die Organisation legt einen Zeitraum fest, nach dessen Ablauf zeitlich begrenzte Konten automatisch gelöscht werden.	Def. durch DoD Enclave Planer Nicht Planer Nicht zweckmäßig
CCI-001365	AC-2(2)	Die Organisation legt einen Zeitraum fest, nach dessen Ablauf Notfallkonten automatisch gelöscht werden.	Def. durch DoD Enclave Planer Nicht Planer Nicht zweckmäßig
CCI-000017	AC-2(3)	Nach Ablauf eines Zeitraums, der von der Organisation festgelegt wird, werden inaktive Konten automatisch deaktiviert.	Def. durch DoD Enclave Planer Nicht Planer Nicht zweckmäßig
CCI-000217	AC-2(3)	Die Organisation legt einen Zeitraum fest, nach dessen Ablauf zeitlich begrenzte Konten automatisch deaktiviert werden.	Def. durch DoD Planer Nicht zweckmäßig
CCI-000018	AC-2(4)	Das Informationssystem kontrolliert automatisch Handlungen zur Kontoerstellung.	Enclave Planer Nicht zweckmäßig
CCI-001403	AC-2(4)	Das Informationssystem kontrolliert automatisch Handlungen zur Kontoänderung.	Enclave Planer Nicht zweckmäßig
CCI-001404	AC-2(4)	Das Informationssystem kontrolliert automatisch Handlungen zur Kontodeaktivierung.	Enclave Planer Nicht zweckmäßig
CCI-001405	AC-2(4)	Das Informationssystem überprüft automatisch Handlungen zur Kontolöschung.	Enclave Planer Nicht zweckmäßig
CCI-002130	AC-2(4)	Das Informationssystem überprüft automatisch Handlungen zur Kontoaktivierung.	Enclave Planer Nicht zweckmäßig
CCI-001683	AC-2(4)	Das Informationssystem erkennt von der Organisation zugelassene Personen oder Rollen bei der Durchführung der Kontoerstellung.	Enclave Planer
CCI-001684	AC-2(4)	Das Informationssystem erkennt von der Organisation zugelassene Personen oder Rollen bei der Durchführung der Kontoänderung.	Enclave Planer
CCI-001685	AC-2(4)	Das Informationssystem erkennt von der Organisation zugelassene Personen oder Rollen bei der Durchführung der Kontodeaktivierung.	Enclave Planer
CCI-001686	AC-2(4)	Das Informationssystem erkennt von der Organisation zugelassene Personen oder Rollen bei der Durchführung der Kontolöschung.	Enclave Planer

Tabelle H-5: Zusätzliche Planer-CCIs für Kontrollsysteme mit MITTLEREN Auswirkungen			
CCI #	800-53 Kontroll-text Indikator	CCI-Definition	Zuständigkeit
CCI-002132	AC-2(4)	Das Informationssystem erkennt von der Organisation zugelassene Personen oder Rollen bei der Durchführung der Kontoaktivierung.	Enclave Planer
CCI-001368	AC-4	Das Informationssystem setzt genehmigte Autorisierungen zur Kontrolle des Informationsflusses innerhalb des Systems gemäß den durch die Organisation vorgegebenen Vorgänge zur Kontrolle des Informationsflusses um.	Enclave Planer Nicht zweckmäßig
CCI-001414	AC-4	Das Informationssystem setzt genehmigte Autorisierungen zur Kontrolle des Informationsflusses zwischen den verbundenen Systemen gemäß den durch die Organisation vorgegebenen Vorgänge zur Kontrolle des Informationsflusses um.	Enclave Planer Nicht zweckmäßig
CCI-001548	AC-4	Die Organisation legt die Vorgänge zur Kontrolle des Informationsflusses für die Kontrolle des Informationsflusses innerhalb des Systems fest.	Enclave Planer Nicht Planer Nicht zweckmäßig
CCI-001549	AC-4	Die Organisation legt die Vorgänge zur Kontrolle des Informationsflusses für die Kontrolle des Informationsflusses zwischen verbundenen Systemen fest.	Enclave Planer Nicht Planer Nicht zweckmäßig
CCI-001550	AC-4	Die Organisation legt zugelassene Autorisierungen für die Kontrolle des Informationsflusses innerhalb des Systems fest.	Enclave Planer Nicht Planer Nicht zweckmäßig
CCI-001551	AC-4	Die Organisation legt zugelassene Autorisierungen für die Kontrolle des Informationsflusses zwischen verbundenen Systemen fest.	Enclave Planer Nicht Planer Nicht zweckmäßig
CCI-001558	AC-6(1)	Die Organisation legt Sicherheitsfunktionen (zur Anwendung bei Hardware, Software und Firmware) fest, für die der Zugang explizit autorisiert werden muss.	Def. durch DoD Planer Nicht zweckmäßig
CCI-002221	AC-6(1)	Die Organisation legt sicherheitsrelevante Informationen fest, für die der Zugang explizit autorisiert werden muss.	Def. durch DoD Planer Nicht zweckmäßig
CCI-002222	AC-6(1)	Die Organisation wird den Zugang zu durch die Organisation festgelegten Sicherheitsfunktionen explizit autorisieren.	Def. durch DoD Planer Nicht zweckmäßig
CCI-002223	AC-6(1)	Die Organisation wird den Zugang zu durch die Organisation festgelegten sicherheitsrelevanten Informationen explizit autorisieren.	Def. durch DoD Planer Nicht zweckmäßig
CCI-000039	AC-6(2)	Durch die Organisation wird gefordert, dass Benutzer oder Rollen bei den Konten des Informationssystems, die einen Zugang zu durch die Organisation definierten Sicherheitsfunktionen oder sicherheitsrelevanten Informationen haben, nicht-privilegierte Konten oder Rollen benutzen, wenn sie auf Funktionen, die nicht die Sicherheit betreffen, zugreifen.	Def. durch DoD Planer Nicht zweckmäßig
CCI-001419	AC-6(2)	Die Organisation legt die Sicherheitsfunktionen bzw. sicherheitsrelevanten Informationen fest, auf die Benutzer, Konten, oder Rollen des Informationssystems Zugriff haben.	Def. durch DoD Planer Nicht zweckmäßig

Tabelle H-5: Zusätzliche Planer-CCIs für Kontrollsysteme mit MITTLEREN Auswirkungen			
CCI #	800-53 Kontroll-text Indikator	CCI-Definition	Zuständigkeit
CCI-002234	AC-6(9)	Das Informationssystem prüft die Ausführung privilegierter Funktionen.	Planer Nicht zweckmäßig
CCI-002235	AC-6(10)	Das Informationssystem hält nicht-privilegierte Benutzer davon ab, privilegierte Funktionen auszuführen, die das Deaktivieren, Umgehen, oder Verändern der angewendeten Sicherheitsmaßnahmen/Gegenmaßnahmen mit einschließen.	Planer Nicht zweckmäßig
CCI-000058	AC-11(a)	Das Informationssystem gibt den Benutzern die Möglichkeit, Mechanismen zur Sperrung von Sitzungen direkt zu veranlassen.	Enclave Planer Nicht zweckmäßig
CCI-000059	AC-11(a)	Die Organisation legt einen Inaktivitätszeitraum fest, nach dessen Ablauf das Informationssystem eine Sperrung der Sitzung veranlasst.	Def. durch DoD Enclave Planer Nicht zweckmäßig
CCI-000056	AC-11(b)	Das Informationssystem hält die Sperrung der Sitzung so lange aufrecht, bis der Benutzer die festgelegten Identifizierungs- und Authentifizierungsvorgänge durchgeführt hat, um den Zugang zu erneuern.	Enclave Planer Nicht zweckmäßig
CCI-000060	AC-11(1)	Das Informationssystem verdeckt bei Sperrung der Sitzung Informationen, die vorher auf dem Bildschirm sichtbar waren, durch ein Bild, das für die Öffentlichkeit zugelassen ist.	Enclave Planer Nicht zweckmäßig
CCI-002360	AC-12	Die Bedingungen oder Auslöser für eine Deaktivierung der Sitzung, die vom Informationssystem angewendet werden, um eine Benutzersitzung automatisch zu beenden werden von der Organisation festgelegt.	Enclave Planer Nicht zweckmäßig
CCI-002361	AC-12	Das Informationssystem beendet eine Benutzersitzung automatisch, wenn eine Bedingung oder ein Auslöser vorliegt, die gemäß Festlegung der Organisation eine Sitzungs-Deaktivierung erforderlich macht.	Enclave Planer Nicht zweckmäßig
CCI-001443	AC-18(1)	Das Informationssystem schützt den drahtlosen Zugang zum System durch die Authentifizierung von Benutzern bzw. Geräten.	Planer Nicht zweckmäßig
CCI-001444	AC-18(1)	Das Informationssystem schützt den drahtlosen Zugang zum System durch Verschlüsselung.	Planer Nicht zweckmäßig
CCI-000135	AU-3(1)	Das Informationssystem erstellt Prüfprotokolle, die durch die Organisation festgelegte zusätzliche und detailliertere Informationen enthalten, welche in Prüfprotokollen enthalten sein müssen.	Planer Nicht zweckmäßig
CCI-001488	AU-3(1)	Die Organisation definiert zusätzliche und detailliertere Informationen, welche in den Prüfprotokollen enthalten sein müssen.	Planer Kein Planer
CCI-001875	AU-7(a)	Das Informationssystem bietet die Möglichkeit, die Anzahl der Prüfungen durch Prüfungen und Analysen auf Abruf zu reduzieren.	Enclave Planer Nicht zweckmäßig
CCI-001876	AU-7(a)	Das Informationssystem bietet die Möglichkeit, die Anzahl der Prüfungen durch Berichterstattung auf Abruf zu reduzieren.	Enclave Planer Nicht zweckmäßig
CCI-001877	AU-7(a)	Das Informationssystem bietet die Möglichkeit, die Anzahl der Prüfungen durch nachträgliche Untersuchungen von Sicherheitsvorfällen zu reduzieren.	Enclave Planer Nicht zweckmäßig

Tabelle H-5: Zusätzliche Planer-CCIs für Kontrollsysteme mit MITTLEREN Auswirkungen			
CCI #	800-53 Kontroll-text Indikator	CCI-Definition	Zuständigkeit
CCI-001878	AU-7(a)	Das Informationssystem bietet die Möglichkeit, Berichte auf Grundlage der Prüfung und Analyse auf Anfrage zu erstellen.	Enclave Planer Nicht zweckmäßig
CCI-001879	AU-7(a)	Das Informationssystem bietet die Möglichkeit, Berichte durch Berichterstattung auf Anfrage zu erstellen.	Enclave Planer Nicht zweckmäßig
CCI-001880	AU-7(a)	Das Informationssystem bietet die Möglichkeit Berichte durch nachträgliche Untersuchungen von Sicherheitsvorfällen zu erstellen.	Enclave Planer Nicht zweckmäßig
CCI-001881	AU-7(b)	Das Informationssystem bietet die Möglichkeit, Prüfungen zu reduzieren, ohne deren ursprünglichen Inhalt bzw. die zeitliche Reihenfolge von Prüfberichten zu verändern.	Enclave Planer Nicht zweckmäßig
CCI-001882	AU-7(b)	Das Informationssystem bietet die Möglichkeit, Berichte zu erstellen, ohne deren ursprünglichen Inhalt bzw. die zeitliche Reihenfolge von Prüfberichten zu verändern.	Enclave Planer Nicht zweckmäßig
CCI-000158	AU-7(1)	Das Informationssystem bietet die Möglichkeit, Prüfberichte für interessenbasierte Ereignisse auf der Grundlage von durch die Organisation festgelegten Prüffeldern innerhalb der Prüfberichte durchzuführen.	Enclave Planer Nicht zweckmäßig
CCI-001891	AU-8(1)	Das Informationssystem vergleicht interne Zeitmesser des Informationssystems mit einer durch die Organisation definierten Frequenz mit Hilfe einer durch die Organisation definierten autoritativen Zeitquelle.	Planer
CCI-001892	AU-8(1)	Die Organisation legt den Zeitunterschied fest, bei dessen Überschreitung das Informationssystem die internen Zeitmesser des Informationssystems mit der durch die Organisation bestimmten autoritativen Zeitquelle synchronisieren muss.	Planer Kein Planer
CCI-002046	AU-8(1)	Das Informationssystem synchronisiert die internen Zeitmesser mit der autoritativen Zeitquelle, wenn der Zeitunterschied den durch die Organisation festgelegte Zeitraum überschreitet.	Planer
CCI-000298	CM-2(1)(c)	Die Organisation überprüft und aktualisiert die Referenzwertkonfiguration des Informationssystems als wesentlichen Teil von Komponenteninstallationen des Informationssystems.	Planer Kein Planer
CCI-001737	CM-2(7)a	Die Organisation definiert Informationssysteme, Systemkomponenten oder Geräte, bei denen durch die Organisation definierte Konfigurationen zur Anwendung kommen müssen, wenn sie sich in Bereichen mit erheblichem Risiko befinden.	Planer Kein Planer
CCI-001738	CM-2(7)a	Die Organisation legt Sicherheitskonfigurationen fest, die bei Informationssystemen, Systemkomponenten oder Geräten umgesetzt werden müssen, wenn diese sich in Bereichen mit erheblichem Risiko befinden.	Planer Kein Planer
CCI-001592	CM-7(2)	Die Organisation definiert die Regeln, welche die allgemeinen Bedingungen für die Nutzung von Softwareprogrammen des Informationssystems autorisieren.	Planer
CCI-001763	CM-7(2)	Die Organisation definiert die Vorgehensweise im Hinblick auf die Nutzung von Softwareprogrammen und Beschränkungen.	Planer Kein Planer

Tabelle H-5: Zusätzliche Planer-CCIs für Kontrollsysteme mit MITTLEREN Auswirkungen			
CCI #	800-53 Kontroll-text Indikator	CCI-Definition	Zuständigkeit
CCI-001764	CM-7(2)	Das Informationssystem verhindert die Ausführung von Programmen gemäß den von der Organisation definierten Vorgehensweisen für die Nutzung und Beschränkung von Softwareprogrammen bzw. Regeln, welche die Bedingungen für die Nutzung von Softwareprogrammen autorisieren.	Planer
CCI-001772	CM-7(5)a	Die Organisation legt die Softwareprogramme fest, die für die Ausführung im Informationssystem autorisiert sind.	Planer
CCI-001773	CM-7(5)a	Die Organisation bestimmt die durch die Organisation festgelegten Softwareprogramme, die für die Ausführung im Informationssystem autorisiert sind.	Planer
CCI-001774	CM-7(5)b	Die Organisation wendet eine deny-all (alle ablehnen), und permit-by exception (Ausnahmeerlaubnis) Strategie an, um die Ausführung autorisierter Softwareprogramme im Informationssystem zu ermöglichen.	Planer
CCI-002828	CP-2(8)	Die Organisation bestimmt kritische Informationssystem-Komponenten, die wesentliche Aufgaben unterstützen.	Planer
CCI-000553	CP-10(2)	Das Informationssystem führt eine Transaktions-Wiederherstellung für transaktionsbasierte Systeme durch.	Planer
CCI-000766	IA-2(2)	Das Informationssystem führt eine von verschiedenen Faktoren abhängige Authentifizierung für den Netzwerkzugang auf nicht-privilegierte Konten durch.	Enclave Planer Nicht zweckmäßig
CCI-000767	IA-2(3)	Das Informationssystem führt eine von verschiedenen Faktoren abhängige Authentifizierung für den lokalen Zugriff auf privilegierte Konten durch.	Enclave Planer Nicht zweckmäßig
CCI-001959	IA-3(1)	Die Organisation legt die speziellen Geräte bzw. Gerätetypen fest, die das Informationssystem authentifizieren muss bevor eine Verbindung hergestellt wird.	Def. durch DoD Planer Nicht zweckmäßig
CCI-001967	IA-3(1)	Das Informationssystem authentifiziert von der Organisation festgelegte Geräte bzw. Typen, bevor eine lokale Verbindung oder eine Fern- bzw. Netzwerkverbindung mit kryptographiebasierter bidirektionaler Authentifizierung hergestellt wird.	Planer Nicht zweckmäßig
CCI-000185	IA-5(2)(a)	Das Informationssystem für PKI-basierte Authentifizierung bewertet Zertifizierungen, indem es einen Zertifizierungspfad zu einem zugelassenen Trust Anchor aufbaut und nachweist; dies schließt auch die Überprüfung der Information des Zertifizierungsstatus mit ein.	Enclave Planer Nicht zweckmäßig
CCI-000186	IA-5(2)(b)	Das Informationssystem für PKI-basierte Authentifizierung setzt den autorisierten Zugriff auf den zugehörigen Public Key durch.	Enclave Planer
CCI-000187	IA-5(2)(c)	Bei PKI-basierter Authentifizierung bildet das Informationssystem die authentifizierte Identität auf dem individuellen Konto oder dem Gruppenkonto ab.	Enclave Planer
CCI-001991	IA-5(2)(d)	Das Informationssystem für PKI-basierte Authentifizierung führt einen lokalen Cache für Widerrufsdaten durch, um die Pfaderkennung sowie die Bewertung im Falle von Inaktivität für den Zugang zu Widerrufsinformationen durch das Netzwerk zu unterstützen.	Enclave Planer
CCI-000865	MA-3	Die Organisation lässt Wartungstools für das Informationssystem zu.	Planer Kein Planer

Tabelle H-5: Zusätzliche Planer-CCIs für Kontrollsysteme mit MITTLEREN Auswirkungen			
CCI #	800-53 Kontroll-text Indikator	CCI-Definition	Zuständigkeit
CCI-000936	PE-4	Die Organisation kontrolliert den physischen Zugriff auf durch die Organisation festgelegte Verteilungs- und Übertragungsleitungen des Informationssystems innerhalb der Einrichtungen der Organisation mit Hilfe von durch die Organisation festgelegten Sicherheitsmaßnahmen.	Planer Kein Planer
CCI-002930	PE-4	Die Organisation kontrolliert den physischen Zugriff auf durch die Organisation festgelegte Verteilungs- und Übertragungsleitungen des Informationssystems innerhalb der Einrichtungen der Organisation mit Hilfe von durch die Organisation festgelegten Sicherheitsmaßnahmen.	Planer Kein Planer
CCI-002931	PE-4	Die Organisation legt Sicherheitsmaßnahmen fest um den physischen Zugriff auf durch die Organisation festgelegte Verteilungs- und Übertragungsleitungen des Informationssystems innerhalb der Einrichtungen der Organisation zu kontrollieren.	Planer Kein Planer
CCI-000937	PE-5	Die Organisation kontrolliert den physischen Zugang zu Ausgabegeräten, um unbefugte Personen davon abzuhalten, die Ausgabedaten an sich zu bringen.	Planer Kein Planer
CCI-000952	PE-9	Die Organisation schützt elektrische Einrichtungen und Stromkabel des Informationssystems vor Schäden und Zerstörung.	Planer Kein Planer
CCI-002953	PE-9(1)	Die Organisation verwendet redundante Stromverkabelungswege, die physisch durch einen von der Organisation definierten Abstand getrennt sind.	Planer Kein Planer
CCI-002954	PE-9(1)	Die Organisation legt den Abstand für die physische Trennung von redundanten Stromverkabelungswegen fest.	Planer Kein Planer
CCI-002955	PE-11	Die Organisation stellt eine kurzzeitige unterbrechungsfreie Stromversorgung zur Verfügung, um eine ordnungsgemäße Abschaltung des Informationssystems bzw. den Übergang des Informationssystems zu einer dauerhaften alternativen Stromversorgung im Fall eines Verlusts einer primären Stromquelle zu ermöglichen.	Enclave Planer Nicht zweckmäßig
CCI-000961	PE-11(1)	Die Organisation stellt eine dauerhafte alternative Stromversorgung für das Informationssystem zur Verfügung, die in der Lage ist, die erforderliche Mindest-Funktionalität im Falle eines längeren Ausfalls der primären Stromquelle zu erhalten.	Enclave Planer
CCI-003071	PL-7(a)	Die Organisation entwickelt ein Sicherheitskonzept für den Betrieb (CONOPS) des Informationssystems, in dem mindestens enthalten sein muss, wie die Organisation das System im Hinblick auf Informationssicherheit betreiben will.	Planer Kein Planer
CCI-003072	PL-8(a)	Die Organisation entwickelt eine Informationssicherheits-Architektur für das Informationssystem.	Planer Kein Planer
CCI-003073	PL-8(a)(1)	Die Informationssicherheits-Architektur der Organisation für das Informationssystem beschreibt die geplante Philosophie, die Anforderungen und den Ansatz ganzheitlich im Hinblick auf den Schutz der Vertraulichkeit, Integrität und Zugänglichkeit von Informationen der Organisation.	Planer Kein Planer

Tabelle H-5: Zusätzliche Planer-CCIs für Kontrollsysteme mit MITTLEREN Auswirkungen			
CCI #	800-53 Kontroll- text Indikator	CCI-Definition	Zuständigkeit
CCI-003075	PL-8(a)(3)	Die Informationssicherheits-Architektur der Organisation für das Informationssystem beschreibt alle Annahmen über Informationssicherheit sowie die Abhängigkeiten von externen Diensten.	Planer Kein Planer
CCI-001062	RA-5(1)	Die Organisation wendet Scanning Tools an, die das System auf Schwachstellen testen und im Hinblick auf die Schwachstellen des Informationssystems, die gescannt werden müssen, aktualisierbar sind.	Enclave Planer
CCI-001067	RA-5(5)	Das Informationssystem führt die privilegierte Zugangs-autorisierung für von der Organisation festgelegte System-Komponenten für ausgewählte, von der Organisation festgelegte Scans auf Schwachstellen durch.	Enclave Planer
CCI-001645	RA-5(5)	Die Organisation bestimmt die Komponenten des Informationssystems, für die ein privilegierter Zugang für von der Organisation festgelegte Scans auf Schwachstellen autorisiert ist.	Def. durch DoD Enclave Planer Nicht zweckmäßig
CCI-002906	RA-5(5)	Die Organisation definiert die Scans auf Schwachstellen, durch die das Informationssystem privilegierten Zugang zu von der Organisation definierte Informationssystem-Komponenten autorisiert.	Enclave Planer
CCI-000623	SA-4(1)	Die Organisation fordert vom Entwickler des Informationssystems, der Systemkomponente oder des Informationssystem-Dienstes, dass er eine Beschreibung der funktionalen Eigenschaften der umzusetzenden Sicherheitskontrollen vorlegt.	Planer Nicht Planer Nicht zweckmäßig
CCI-003101	SA-4(2)	Die Organisation fordert vom Entwickler des Informationssystems, der Systemkomponente oder des Informationssystem-Dienstes, dass er Informationen zur Planung der anzuwendenden Sicherheitskontrollen vorlegt, welche sicherheitsrelevante externe Systemschnittstellen, Highlevel Design, Lowlevel Design, Quellcode, Hardware Schemata bzw. von der Organisation definierte Konfigurationen/Informationen bei von der Organisation definierte Detailabstufungen mit einschließen.	Planer Nicht Planer Nicht zweckmäßig
CCI-003102	SA-4(2)	Die Organisation fordert vom Entwickler des Informationssystems, der Systemkomponente oder des Informationssystem-Dienstes, dass er Informationen zur Umsetzung der anzuwendenden Sicherheitskontrollen vorlegt, welche sicherheitsrelevante externe Systemschnittstellen, Highlevel Design, Lowlevel Design, Quellcode, Hardware Schemata bzw. von der Organisation definierte Umsetzungen/Informationen bei von der Organisation definierte Detailabstufungen mit einschließen.	Planer Nicht Planer Nicht zweckmäßig
CCI-003103	SA-4(2)	Die Organisation definiert die Planungsinformationen, die der Entwickler des Informationssystems, Systemkomponente oder Informationssystem-Dienstes für die anzuwendenden Sicherheitskontrollen vorlegen muss.	Planer Nicht Planer Nicht zweckmäßig

Tabelle H-5: Zusätzliche Planer-CCIs für Kontrollsysteme mit MITTLEREN Auswirkungen			
CCI #	800-53 Kontroll-text Indikator	CCI-Definition	Zuständigkeit
CCI-003104	SA-4(2)	Die Organisation definiert die Implementierungsinformationen, die der Entwickler des Informationssystems, der Systemkomponente oder Informationssystem-Dienstes für die anzuwendenden Sicherheitskontrollen vorlegen muss.	Planer Nicht Planer Nicht zweckmäßig
CCI-003105	SA-4(2)	Die Organisation definiert die Detailabstufung der Planungsinformationen für Sicherheitskontrollen, welche vom Entwickler des Informationssystems, der Systemkomponente oder des Informationssystem-Dienstes vorzulegen sind.	Planer Nicht Planer Nicht zweckmäßig
CCI-003106	SA-4(2)	Die Organisation definiert die Detailabstufung der Umsetzungsinformationen für Sicherheitskontrollen, welche vom Entwickler des Informationssystems, Systemkomponente oder Informationssystem-Dienstes vorzulegen sind.	Planer Nicht Planer Nicht zweckmäßig
CCI-003114	SA-4(9)	Die Organisation fordert vom Entwickler des Informationssystems, der Systemkomponente oder des Informationssystem-Dienstes, dass er zu einem frühen Zeitpunkt der Systementwicklung die Lebensdauer, Funktionen, Ports, Protokolle und Dienste ermittelt, die für den Betrieb geplant sind.	Planer Nicht Planer Nicht zweckmäßig
CCI-003155	SA-10(a)	Die Organisation fordert vom Entwickler des Informationssystems, der Systemkomponente oder des Informationssystem-Dienstes, dass er während des Entwurfs, der Entwicklung, der Umsetzung bzw. dem Betrieb des Systems, der Komponente oder des Dienstes ein Konfigurationsmanagement durchführt.	Planer Nicht Planer Nicht zweckmäßig
CCI-003156	SA-10(b)	Die Organisation fordert vom Entwickler des Informationssystems, der Systemkomponente oder des Informationssystem-Dienstes, dass er die Integrität von Änderungen an von der Organisation definierten Konfigurations-Items während des Konfigurationsmanagements dokumentiert.	Planer Nicht Planer Nicht zweckmäßig
CCI-003157	SA-10(b)	Die Organisation fordert vom Entwickler des Informationssystems, der Systemkomponente oder des Informationssystem-Dienstes, dass er die Integrität von Änderungen an von der Organisation festgelegten Konfigurations-Items während des Konfigurationsmanagements reguliert.	Planer Nicht Planer Nicht zweckmäßig
CCI-003158	SA-10(b)	Die Organisation fordert vom Entwickler des Informationssystems, der Systemkomponente oder des Informationssystem-Dienstes, dass er die Integrität von Änderungen an von der Organisation festgelegten Konfigurations-Items während des Konfigurationsmanagements kontrolliert.	Planer Nicht Planer Nicht zweckmäßig
CCI-003159	SA-10(b)	Die Organisation legt die Konfigurations-Items für das Konfigurationsmanagement fest, für die das Dokumentieren, Managen und Kontrollieren der Integrität der Änderungen erforderlich ist.	Planer Nicht Planer Nicht zweckmäßig
CCI-000692	SA-10(c)	Die Organisation fordert vom Entwickler des Informationssystems, der Systemkomponente oder des Informationssystem-Dienstes, dass er nur von der Organisation zugelassene Änderungen am System, der Komponente oder dem Dienst vornimmt.	Planer Nicht Planer Nicht zweckmäßig

Tabelle H-5: Zusätzliche Planer-CCIs für Kontrollsysteme mit MITTLEREN Auswirkungen			
CCI #	800-53 Kontroll- text Indikator	CCI-Definition	Zuständigkeit
CCI-000694	SA-10(d)	Die Organisation fordert vom Entwickler des Informationssystems, der Systemkomponente oder des Informationssystem-Dienstes, dass er zugelassene Änderungen am System, der Komponente oder dem Dienst dokumentiert.	Planer Nicht Planer Nicht zweckmäßig
CCI-003160	SA-10(d)	Die Organisation fordert vom Entwickler des Informationssystems, der Systemkomponente oder des Informationssystem-Dienstes, dass er potentielle Sicherheitsauswirkungen der zugelassenen Änderungen am System, der Komponente oder dem Dienst dokumentiert.	Planer Nicht Planer Nicht zweckmäßig
CCI-003161	SA-10(e)	Die Organisation fordert vom Entwickler des Informationssystems, der Systemkomponente oder des Informationssystem-Dienstes, dass er Sicherheitslücken innerhalb des Systems, der Komponente oder des Dienstes protokolliert.	Planer Nicht Planer Nicht zweckmäßig
CCI-003162	SA-10(e)	Die Organisation fordert vom Entwickler des Informationssystems, der Systemkomponente oder des Informationssystem-Dienstes, dass er die Behebung von Sicherheitslücken innerhalb des Systems, der Komponente oder des Dienstes protokolliert.	Planer Nicht Planer Nicht zweckmäßig
CCI-003163	SA-10(e)	Die Organisation fordert vom Entwickler des Informationssystems, der Systemkomponente oder des Informationssystem-Dienstes, dass er Sicherheitslücken und Behebungen von Sicherheitslücken innerhalb des Systems, der Komponente oder des Dienstes meldet.	Planer Nicht Planer Nicht zweckmäßig
CCI-003171	SA-11(a)	Die Organisation fordert vom Entwickler des Informationssystems, Systemkomponenten oder Informationssystem-Dienstes, dass er einen Plan zur Sicherheitsbewertung erstellt.	Planer Nicht Planer Nicht zweckmäßig
CCI-003172	SA-11(a)	Die Organisation fordert vom Entwickler des Informationssystems, der Systemkomponente oder des Informationssystem-Dienstes, dass er einen Plan zur Sicherheitsbewertung umsetzt.	Planer Nicht Planer Nicht zweckmäßig
CCI-003173	SA-11(b)	Die Organisation fordert vom Entwickler des Informationssystems, der Systemkomponente oder des Informationssystem-Dienstes, Tests/Bewertungen mit von der Organisation festgelegtem Umfang und Abdeckung für Units, Integration, Systeme bzw. Regression durchzuführen.	Planer Nicht Planer Nicht zweckmäßig
CCI-003174	SA-11(b)	Die Organisation legt den Umfang und die Abdeckung fest, mit der Tests/Bewertungen für Units, Systeme bzw. Regression durchgeführt werden.	Planer Nicht Planer Nicht zweckmäßig
CCI-003175	SA-11(c)	Die Organisation fordert vom Entwickler des Informationssystems, der Systemkomponente oder des Informationssystem-Dienstes, den Nachweis, dass der Plan zur Sicherheitsbewertung umgesetzt wurde.	Planer Nicht Planer Nicht zweckmäßig
CCI-003176	SA-11(c)	Die Organisation fordert vom Entwickler des Informationssystems, der Systemkomponente oder des Informationssystem-Dienstes, dass er die Ergebnisse der Sicherheitstests/Sicherheitsbewertungen vorlegt.	Planer Nicht Planer Nicht zweckmäßig

Tabelle H-5: Zusätzliche Planer-CCIs für Kontrollsysteme mit MITTLEREN Auswirkungen			
CCI #	800-53 Kontroll-text Indikator	CCI-Definition	Zuständigkeit
CCI-003177	SA-11(d)	Die Organisation fordert vom Entwickler des Informationssystems, der Systemkomponente oder des Informationssystem-Dienstes, dass er einen nachweisbaren Vorgang zur Fehlerbehebung anwendet.	Planer Nicht Planer Nicht zweckmäßig
CCI-003178	SA-11(e)	Die Organisation fordert vom Entwickler des Informationssystems, der Systemkomponente oder des Informationssystem-Dienstes, dass er während der Sicherheitstests/Sicherheitsbewertungen gefundene Fehler behebt.	Planer Nicht Planer Nicht zweckmäßig
CCI-001082	SC-2	Das Informationssystem trennt die Benutzerfunktionalität (einschließlich Benutzerschnittstellendienste) von der Funktionalität des Informationssystem-Managements.	Enclave Planer Nicht Planer
CCI-001109	SC-7(5)	Das Informationssystem verweigert an regulierten Schnittstellen den Kommunikationsfluss im Netzwerk durch Defaults und erlaubt den Kommunikationsfluss im Netzwerk durch Ausnahmeregelungen (z.B. deny all, permit by exception).	Enclave Planer
CCI-001126	SC-7(18)	Im Fall einer Betriebsstörung bei einer Schutzeinrichtung für seine Grenzen fällt das Informationssystem geschützt aus.	Planer Nicht zweckmäßig
CCI-002418	SC-8	Das Informationssystem schützt die Vertraulichkeit bzw. Integrität der übermittelten Informationen.	Planer
CCI-002419	SC-8(1)	Die Organisation legt alternative physische Schutzeinrichtungen fest, die dann angewendet werden, wenn keine Verschlüsselungsmechanismen vorgesehen sind, um die Informationen während der Übertragung zu schützen.	Def. durch DoD Planer
CCI-002421	SC-8(1)	Das Informationssystem setzt Verschlüsselungsmechanismen ein, um die Offenlegung von Informationen an Unbefugte zu verhindern, bzw. um Änderungen der Informationen während der Übertragung zu erkennen, wenn keine alternativen physischen Schutzeinrichtungen gemäß Festlegung durch die Organisation vorgesehen sind.	Planer
CCI-001133	SC-10	Das Informationssystem beendet die Netzwerkverbindung, die einer Kommunikationssitzung zugeordnet ist, wenn diese Sitzung beendet wurde oder nach einem durch die Organisation festgelegtem Inaktivitätszeitraum.	Enclave Planer Nicht zweckmäßig
CCI-001134	SC-10	Die Organisation legt den Inaktivitätszeitraum fest, nach dessen Ablauf das Informationssystem eine Netzwerkverbindung beendet, die einer Kommunikationssitzung zugeordnet ist.	Def. durch DoD Planer Nicht zweckmäßig
CCI-002449	SC-13	Die Organisation bestimmt die kryptographischen Nutzungen, die Art der Verschlüsselung, die für jede Nutzung erforderlich ist, die durch das Informationssystem umgesetzt werden soll.	Def. durch DoD Enclave Planer Nicht zweckmäßig
CCI-002450	SC-13	Das Informationssystem führt die von der Organisation bestimmten kryptographische Nutzungen und die Art der Verschlüsselung, die für jede Nutzung erforderlich ist, gemäß gültigen Bundesgesetzen, Durchführungsverordnungen, Richtlinien, Regelwerken, Vorschriften und Normen, durch.	Enclave Planer Nicht zweckmäßig
CCI-001160	SC-18(a)	Die Organisation legt akzeptablen und inakzeptablen Mobilcode und Mobilcode-Technologien fest.	Enclave Planer

Tabelle H-5: Zusätzliche Planer-CCIs für Kontrollsysteme mit MITTLEREN Auswirkungen			
CCI #	800-53 Kontroll-text Indikator	CCI-Definition	Zuständigkeit
CCI-001161	SC-18(b)	Die Organisation führt Nutzungsbeschränkungen für akzeptablen Mobilcode und Mobilcode-Technologien ein.	Enclave Planer
CCI-001162	SC-18(b)	Die Organisation führt eine Richtlinie für die Umsetzung von akzeptablem Mobilcode und Mobilcode-Technologien ein.	Enclave Planer
CCI-001163	SC-18(c)	Die Organisation genehmigt die Nutzung von Mobilcode innerhalb des Informationssystems.	Enclave Planer
CCI-001164	SC-18(c)	Die Organisation überprüft die Nutzung von Mobilcode innerhalb des Informationssystems.	Enclave Planer
CCI-001165	SC-18(c)	Die Organisation kontrolliert die Nutzung von Mobilcode innerhalb des Informationssystems.	Enclave Planer
CCI-001184	SC-23	Das Informationssystem schützt die Authentizität der Kommunikationssitzungen.	Enclave Planer Nicht zweckmäßig
CCI-001190	SC-24	Das Informationssystem fällt bis zu einem von der Organisation festgelegten Zustand für von der Organisation festgelegte Ausfallarten aus.	Planer
CCI-001191	SC-24	Die Organisation legt die bekannten Zustände fest, bis zu denen das Informationssystem ausfallen könnte, falls es zu einem von der Organisation definierten Systemausfall kommt.	Def. durch DoD Planer Nicht zweckmäßig
CCI-001192	SC-24	Die Organisation definiert Ausfalltypen, bei denen das Informationssystem bis zu einem durch die Organisation festgelegten Zustand ausfallen sollte.	Def. durch DoD Planer Nicht zweckmäßig
CCI-001193	SC-24	Die Organisation legt Systemstatus-Informationen fest, die auch im Falle eines Systemausfalls erhalten bleiben sollten.	Def. durch DoD Planer Nicht zweckmäßig
CCI-001665	SC-24	Im Falle eines Systemausfalls erhält das Informationssystem von der Organisation festgelegte Systemstatus-Informationen aufrecht.	Planer Nicht zweckmäßig
CCI-001199	SC-28	Das Informationssystem schützt die Vertraulichkeit bzw. Integrität der durch die Organisation festgelegten inaktiven Informationen.	Enclave Planer Nicht zweckmäßig
CCI-002472	SC-28	Die Organisation legt inaktive Informationen fest, die durch das Informationssystem geschützt werden müssen.	Planer Nicht Planer Nicht zweckmäßig
CCI-002703	SI-7	Die Organisation legt die Software, Firmware und Informationen fest, die der Prüfung durch Integritäts-Nachweis-Tools unterliegen, um unbefugte Änderungen daran festzustellen.	Enclave Planer
CCI-002705	SI-7(1)	Die Organisation legt die Software fest, bei der Integritätsprüfungen durchgeführt werden.	Enclave Planer
CCI-002706	SI-7(1)	Die Organisation legt die Firmware fest, bei der Integritätsprüfungen durchgeführt werden.	Enclave Planer
CCI-002707	SI-7(1)	Die Organisation legt die Informationen fest, bei denen Integritätsprüfungen durchgeführt werden.	Enclave Planer

Tabelle H-5: Zusätzliche Planer-CCIs für Kontrollsysteme mit MITTLEREN Auswirkungen			
CCI #	800-53 Kontroll- text Indikator	CCI-Definition	Zuständigkeit
CCI-002710	SI-7(1)	Das Informationssystem führt Integritätsprüfungen von durch die Organisation festgelegter Software beim Startup, bei durch die Organisation festgelegten Übertragungszuständen, sicherheitsrelevanten Vorkommnissen, oder mit einer durch die Organisation festgelegten Häufigkeit durch.	Enclave Planer
CCI-002711	SI-7(1)	Das Informationssystem führt Integritätsprüfungen von durch die Organisation festgelegter Firmware beim Startup, bei durch die Organisation festgelegten Übertragungszuständen, sicherheitsrelevanten Vorkommnissen, oder mit einer durch die Organisation festgelegten Häufigkeit durch.	Enclave Planer
CCI-002712	SI-7(1)	Das Informationssystem führt Integritätsprüfungen von durch die Organisation festgelegten Informationen beim Startup, bei durch die Organisation festgelegten Übertragungszuständen, sicherheitsrelevanten Vorkommnissen, oder mit einer durch die Organisation festgelegten Häufigkeit durch.	Enclave Planer
CCI-001310	SI-10	Das Informationssystem überprüft die Validität der durch die Organisation festgelegten Eingabedaten.	Planer Kein Planer
CCI-002744	SI-10	Die Organisation definiert die Eingabedaten, für welche das Informationssystem Validitätsprüfungen durchführen muss.	Def. durch DoD Planer
CCI-001312	SI-11(a)	Das Informationssystem generiert Fehlermeldungen, die die notwendigen Informationen für Korrekturmaßnahmen enthalten, aber keinerlei Informationen, die von Gegnern ausgenutzt werden könnten.	Planer

Tabelle H-6 Plattform Enclave-CCIs für Kontrollsysteme mit GERINGEN und MITTLEREN Auswirkungen		
CCI #	800-53 Kontrolltext	CCI-Definition
CCI-000048	AC-8(a)	Bevor Zugang zum System gewährt wird, zeigt das Informationssystem eine von der Organisation festgelegte Meldung bzw. ein Banner zur Systemnutzung mit Hinweisen zu Datenschutz und Sicherheit an, die den gültigen Bundesgesetzen, Durchführungsverordnungen, Richtlinien, Regelwerken, Vorschriften und Normen entsprechen.
CCI-002247	AC-8(a)	Die Organisation legt die Meldung zur Systemnutzung bzw. das Banner fest, das den Benutzern das Informationssystem angezeigt wird, bevor Zugang zum System gewährt wird.
CCI-002243	AC-8(a)(1)	Die von der Organisation festgelegte Meldung bzw. das Banner zur Nutzung des Informationssystems soll angeben, dass Benutzer auf ein Informationssystem der US-Regierung zugreifen.
CCI-002244	AC-8(a)(2)	Die von der Organisation festgelegte Meldung bzw. das Banner zur Nutzung des Informationssystems soll angeben, dass die Nutzung des Informationssystems überwacht oder aufgezeichnet werden und einer Überprüfung unterliegen kann.
CCI-002245	AC-8(a)(3)	Die von der Organisation festgelegte Meldung bzw. das Banner zur Nutzung des Informationssystems soll angeben, dass die nicht genehmigte Nutzung des Informationssystems unzulässig ist und straf- und zivilrechtlich verfolgt werden kann.
CCI-002246	AC-8(a)(4)	Die von der Organisation festgelegte Meldung bzw. das Banner zur Nutzung des Informationssystems soll angeben, dass die Nutzung des Informationssystems als Zustimmung zur Überwachung und Aufzeichnung gilt.
CCI-000050	AC-8(b)	Das Informationssystem lässt die Meldung bzw. das Banner auf dem Bildschirm bestehen, bis die Benutzer die Nutzungsbedingungen bestätigen und eindeutige Schritte zum Einloggen bzw. zum weiteren Zugriff unternehmen.
CCI-002248	AC-8(c)(1)	Die Organisation legt die Nutzungsbedingungen fest, die den Benutzern angezeigt werden sollen, bevor weiterer Zugang gewährt wird.
CCI-000063	AC-17(a)	Die Organisation legt zulässige Methoden für den Fernzugriff auf das Informationssystem fest.
CCI-002310	AC-17(a)	Die Organisation führt Nutzungseinschränkungen für jede Art von zulässigen Fernzugriffen ein und dokumentiert diese.
CCI-002311	AC-17(a)	Die Organisation führt Konfigurations-/Verbindungsanforderungen für jede Art von zulässigen Fernzugriffen ein und dokumentiert diese.
CCI-002312	AC-17(a)	Die Organisation führt Richtlinien für die Umsetzung für jede Art von zulässigen Fernzugriffen ein und dokumentiert diese.
CCI-000065	AC-17(b)	Die Organisation autorisiert Fernzugriffe auf das Informationssystem bevor diese Art der Verbindung zugelassen wird.
CCI-000082	AC-19(a)	Die Organisation führt Nutzungsbeschränkungen für von der Organisation kontrollierte Mobilgeräte ein.
CCI-000083	AC-19(a)	Die Organisation führt eine Richtlinie für die Nutzung der von der Organisation kontrollierten Mobilgeräten ein.
CCI-002325	AC-19(a)	Die Organisation führt Konfigurationsanforderungen für von der Organisation kontrollierte Mobilgeräte ein.
CCI-002326	AC-19(a)	Die Organisation führt Verbindungsanforderungen für von der Organisation kontrollierte Mobilgeräte ein.
CCI-000084	AC-19(b)	Die Organisation autorisiert die Verbindung von Mobilgeräten mit dem Informationssystem der Organisation.

Tabelle H-6 Platform Enclave-CCIs für Kontrollsysteme mit GERINGEN und MITTLEREN Auswirkungen		
CCI #	800-53 Kontrolltext	CCI-Definition
CCI-000093	AC-20(a)	Die Organisation führt Bedingungen ein, die nicht mit den Vertrauensverhältnissen zu anderen Organisationen bezüglich Besitz, Betrieb, bzw. Wartung externer Informationssysteme in Konflikt stehen, und die befugten Personen von externen Informationssystemen aus Zugriff auf das Informationssystem gewähren.
CCI-000098	AC-21(a)	Die Organisation erleichtert das Teilen von Informationen, indem es befugten Personen erlaubt, festzulegen ob dem Partner gewährte Zugangsautorisierungen mit den Zugangsbeschränkungen im Hinblick auf Informationen für von der Organisation festgelegte Bedingungen, die Diskretion erfordern, übereinstimmen.
CCI-001470	AC-21(a)	Die Organisation definiert Bedingungen, die beim Teilen von Informationen Diskretion erfordern.
CCI-001471	AC-21(b)	Die Organisation wendet automatische, von der Organisation festgelegte Mechanismen oder manuelle Vorgänge an, die erforderlich sind um den Benutzern dabei zu helfen, Entscheidungen bezüglich des Teilens und der Zusammenarbeit zu treffen.
CCI-001472	AC-21(b)	Die Organisation legt Mechanismen oder manuelle Vorgänge fest, die erforderlich sind um die Benutzer bei Entscheidungen bezüglich des Teilens und der Zusammenarbeit zu unterstützen.
CCI-000139	AU-5(a)	Das Informationssystem alarmiert ernannte, von der Organisation festgelegte Personen bzw. Rollen im Falle eines Fehlers bei der Prüfungsabwicklung.
CCI-000140	AU-5(b)	Das Informationssystem ergreift im Falle eines Fehlers bei der Überwachung (z.B. Herunterfahren des Informationssystems, Überschreiben der ältesten Prüfaufzeichnungen, Unterbinden der Erstellung von Prüfaufzeichnungen) von der Organisation festgelegte Maßnahmen.
CCI-001490	AU-5(b)	Die Organisation legt die Maßnahmen fest, die das Informationssystem bei einem Fehler bei der Überwachung ergreifen soll (z.B. Herunterfahren des Informationssystems, Überschreiben der ältesten Prüfaufzeichnungen, Unterbinden der Erstellung von Prüfaufzeichnungen).
CCI-000162	AU-9	Das Informationssystem schützt Prüfungsinformationen vor unbefugtem Zugriff.
CCI-000163	AU-9	Das Informationssystem schützt Prüfungsinformationen vor unbefugter Änderung.
CCI-000164	AU-9	Das Informationssystem schützt Prüfungsinformationen vor unbefugter Löschung.
CCI-001493	AU-9	Das Informationssystem schützt Prüfungstools vor unbefugtem Zugriff.
CCI-001494	AU-9	Das Informationssystem schützt Prüfungstools vor unbefugter Änderung.
CCI-001495	AU-9	Das Informationssystem schützt Prüfungstools vor unbefugter Löschung.
CCI-000257	CA-3(a)	Die Organisation autorisiert Verbindungen zwischen dem Informationssystem und anderen Informationssystemen durch Anwendung einer Sicherheitsvereinbarung für Verbindungen zwischen Systemen (ISA).
CCI-000258	CA-3(b)	Die Organisation dokumentiert bei jeder Verbindung die Schnittstellenmerkmale.
CCI-000259	CA-3(b)	Die Organisation dokumentiert bei jeder Verbindung die Sicherheitsanforderungen.
CCI-000260	CA-3(b)	Die Organisation dokumentiert bei jeder Verbindung die Art der kommunizierten Information.
CCI-001732	CM-10(c)	Die Organisation kontrolliert die Verwendung von Peer-to-Peer Filesharing-Technologien, um sicherzustellen, dass diese Funktion nicht für das unbefugte Teilen, Veröffentlichen, Ausführen oder Kopieren von kopiergeschützter Arbeit genutzt wird.

Tabelle H-6 Platform Enclave-CCIs für Kontrollsysteme mit GERINGEN und MITTLEREN Auswirkungen		
CCI #	800-53 Kontrolltext	CCI-Definition
CCI-001733	CM-10(c)	Die Organisation dokumentiert die Verwendung von Peer-to-Peer Filesharing-Technologien, um sicherzustellen, dass diese Funktion nicht für das unbefugte Teilen, Veröffentlichen, Ausführen oder Kopieren kopiergeschützter Arbeit genutzt wird.
CCI-000535	CP-9(a)	Die Organisation führt Backups von Informationen auf Benutzerlevel mit einer durch die Organisation festgelegten Häufigkeit durch, die mit den Zielen für Wiederherstellungszeit und Wiederherstellungspunkt vereinbar ist.
CCI-000537	CP-9(b)	Die Organisation führt Backups von Informationen auf Systemlevel mit einer durch die Organisation festgelegten Häufigkeit durch, die mit den Zielen für Wiederherstellungszeit und Wiederherstellungspunkt vereinbar ist.
CCI-000539	CP-9(c)	Die Organisation führt Backups der Informationssysteme Dokumentation, einschließlich der Sicherheitsdokumentation, mit einer durch die Organisation festgelegten Häufigkeit durch, die mit den Zielen für Wiederherstellungszeit und Wiederherstellungspunkt vereinbar ist.
CCI-000540	CP-9(d)	Die Organisation schützt die Vertraulichkeit, Integrität und Verfügbarkeit der Backup-Informationen an Speicherorten.
CCI-000550	CP-10	Nach einer Störung sorgt die Organisation für die Wiederherstellung und das Zurücksetzen des Informationssystems auf einen bekannten Stand.
CCI-000551	CP-10	Nach einer Gefährdung sorgt die Organisation für die Wiederherstellung und das Zurücksetzen des Informationssystems auf einen bekannten Stand.
CCI-000552	CP-10	Nach einem Ausfall sorgt die Organisation für die Wiederherstellung und das Zurücksetzen des Informationssystems auf einen bekannten Stand.
CCI-001933	IA-1(a)	Die Organisation legt Personen oder Rollen fest, die Empfänger der Identifizierungs- und Authentifizierungsstrategie sowie der Verfahren zur leichten Umsetzung der Identifizierungs- und Authentifizierungsstrategie und der damit verbundenen Identifizierungs- und Authentifizierungskontrollen sind.
CCI-001934	IA-1(a)	Die Organisation dokumentiert Abläufe zur Erleichterung der Umsetzung der Identifizierungs- und Authentifizierungsstrategie und den damit verbundenen Identifizierungs- und Authentifizierungskontrollen.
CCI-000756	IA-1(a)(1)	Die Organisation entwickelt eine Identifizierungs- und Authentifizierungsstrategie, in der Zweck, Umfang, Rollen, Verantwortlichkeiten, Verwaltungsverpflichtung, Abstimmung der betrieblichen Einheiten und Einhaltung thematisiert sind.
CCI-000757	IA-1(a)(1)	Die Organisation gibt an von der Organisation festgelegte Personen oder Rollen eine Identifizierungs- und Authentifizierungsstrategie heraus, in der Zweck, Umfang, Rollen, Verantwortlichkeiten, Verwaltungsverpflichtung, Abstimmung der betrieblichen Einheiten und Einhaltung thematisiert sind.
CCI-001932	IA-1(a)(1)	Die Organisation dokumentiert eine Strategie zur Identifizierung und Authentifizierung, in welcher Zweck, Umfang, Rollen, Verantwortlichkeiten, Verwaltungsverpflichtung, Abstimmung der betrieblichen Einheiten und Einhaltung thematisiert sind.
CCI-000760	IA-1(a)(2)	Die Organisation entwickelt Abläufe zur Erleichterung der Umsetzung der Identifizierungs- und Authentifizierungsstrategie und den damit verbundenen Identifizierungs- und Authentifizierungskontrollen.
CCI-000761	IA-1(a)(2)	Die Organisation gibt an von der Organisation festgelegte Personen oder Rollen Abläufe zur Erleichterung der Umsetzung der Identifizierungs- und Authentifizierungsstrategie und der damit verbundenen Identifizierungs- und Authentifizierungskontrollen heraus.

Tabelle H-6 Platform Enclave-CCIs für Kontrollsysteme mit GERINGEN und MITTLEREN Auswirkungen		
CCI #	800-53 Kontrolltext	CCI-Definition
CCI-000758	IA-1(b)(1)	Die Organisation überprüft und aktualisiert die Identifizierungs- und Authentifizierungsstrategie mit der von der Organisation festgelegten Häufigkeit.
CCI-000759	IA-1(b)(1)	Die Organisation legt die Häufigkeit der Prüfungen und Aktualisierungen der Identifizierungs- und Authentifizierungsstrategie fest.
CCI-000762	IA-1(b)(2)	Die Organisation überprüft und aktualisiert die Identifizierungs- und Authentifizierungsmaßnahmen mit der von der Organisation festgelegten Häufigkeit.
CCI-000763	IA-1(b)(2)	Die Organisation legt die Häufigkeit der Prüfungen und Aktualisierungen der Identifizierungs- und Authentifizierungsmaßnahmen fest.
CCI-000764	IA-2	Das Informationssystem bezeichnet und authentifiziert eindeutig Benutzer der Organisation (oder Prozesse, die im Auftrag der Benutzer der Organisation agieren).
CCI-000765	IA-2(1)	Das Informationssystem führt eine von verschiedenen Faktoren abhängige Authentifizierung für den Netzwerkzugriff auf privilegierte Konten durch.
CCI-001953	IA-2(12)	Das Informationssystem akzeptiert Personal Identity Verification (PIV) Berechtigungsnachweise.
CCI-001954	IA-2(12)	Das Informationssystem führt eine elektronische Prüfung der Personal Identity Verification (PIV) Berechtigungsnachweise durch.
CCI-000777	IA-3	Die Organisation legt eine Liste mit speziellen Geräten bzw. Gerätetypen fest, für die eine Identifizierung und Authentifizierung erforderlich sind, bevor eine Verbindung zum Informationssystem hergestellt wird.
CCI-000778	IA-3	Das Informationssystem bezeichnet eindeutig eine von der Organisation festgelegte Liste spezieller Geräte bzw. Gerätetypen, bevor eine lokale Verbindung, Remote-Verbindung oder Netzwerkverbindung hergestellt wird.
CCI-001958	IA-3	Das Informationssystem authentifiziert eine von der Organisation festgelegte Liste spezieller Geräte bzw. Gerätetypen, bevor eine lokale Verbindung, Remote-Verbindung oder Netzwerkverbindung hergestellt wird.
CCI-001970	IA-4(a)	Die Organisation legt Personen oder Rollen fest, die die Zuordnung von individuellen IDs, Gruppen-, Rollen- und Geräte-IDs autorisieren.
CCI-001971	IA-4(a)	Die Organisation verwaltet Informationssystem-IDs, indem sie Autorisierungen von durch die Organisation festgelegte Personen oder Rollen erhält, die eine individuelle IDs, Gruppen-, Rollen- oder Geräte-IDs vergeben.
CCI-001972	IA-4(b)	Die Organisation verwaltet IDs des Informationssystems indem sie eine ID auswählt, die als Beispiel für ein Individuum, eine Gruppe, eine Rolle oder ein Gerät dient.
CCI-001973	IA-4(c)	Die Organisation verwaltet Informationssystem-IDs, indem sie die ID dem vorgesehenen Individuum, der Gruppe, Rolle oder dem Gerät zuordnet.
CCI-001974	IA-4(d)	Die Organisation legt den Zeitraum fest, nach dessen Ablauf die Wiederverwendung von IDs nicht mehr zulässig ist.
CCI-001975	IA-4(d)	Die Organisation verwaltet IDs des Informationssystems indem sie verhindert, dass eine ID nach Ablauf des von der Organisation festgelegten Zeitraumes wiederverwendet werden kann.
CCI-000794	IA-4(e)	Die Organisation legt einen Inaktivitätszeitraum fest, nach dessen Ablauf die ID deaktiviert wird.
CCI-000795	IA-4(e)	Die Organisation verwaltet IDs des Informationssystems indem sie eine ID nach Ablauf des von der Organisation festgelegten Zeitraumes deaktiviert.
CCI-001990	IA-5(j)	Die Organisation verwaltet Authentifikatoren für Gruppen-/Rollenkonten, wenn sich die Mitgliedschaft dieser Konten verändert.
CCI-000192	IA-5(1)(a)	Das Informationssystem setzt die Passwort-Komplexität durch die Mindestanzahl verwendeter Großbuchstaben durch.

Tabelle H-6 Platform Enclave-CCIs für Kontrollsysteme mit GERINGEN und MITTLEREN Auswirkungen		
CCI #	800-53 Kontrolltext	CCI-Definition
CCI-000193	IA-5(1)(a)	Das Informationssystem setzt die Passwort-Komplexität durch eine Mindestanzahl verwendeter Kleinbuchstaben durch.
CCI-000194	IA-5(1)(a)	Das Informationssystem erzwingt Passwort-Komplexität durch die Mindestanzahl verwendeter Ziffern.
CCI-000205	IA-5(1)(a)	Das Informationssystem setzt eine Mindestlänge für Passwörter durch.
CCI-001619	IA-5(1)(a)	Das Informationssystem setzt die Passwort-Komplexität durch eine Mindestanzahl verwendeter Sonderzeichen durch.
CCI-000195	IA-5(1)(b)	Das Informationssystem erzwingt bei der Erstellung neuer Passwörter zur passwortbasierten Authentifizierung, dass mindestens eine von der Organisation bestimmte Anzahl von Zeichen geändert wird.
CCI-000196	IA-5(1)(c)	Für eine passwortbasierte Authentifizierung speichert das Informationssystem nur kryptographisch gesicherte Passwörter.
CCI-000197	IA-5(1)(c)	Für eine passwort-basierte Authentifizierung übermittelt das Informationssystem nur kryptographisch gesicherte Passwörter.
CCI-000199	IA-5(1)(d)	Das Informationssystem setzt Einschränkungen bei der maximalen Nutzungsdauer der Passwörter durch.
CCI-000200	IA-5(1)(e)	Das Informationssystem untersagt die Wiederverwendung von Passwörtern für eine von der Organisation festgelegten Anzahl von Passwortgenerierungen.
CCI-001618	IA-5(1)(e)	Die Organisation bestimmt die Anzahl der Passwortgenerierungen, für die eine Wiederverwendung des Passworts untersagt ist.
CCI-002041	IA-5(1)(f)	Das Informationssystem erlaubt die Verwendung eines temporären Passworts, um sich in ein System einzuloggen, wo dann sofort auf ein permanentes Passwort gewechselt wird.
CCI-002002	IA-5(11)	Die Organisation definiert die Qualitätsanforderungen für die Token, die durch die Mechanismen des Informationssystems bei einer tokenbasierten Authentifizierung verwendet werden.
CCI-002003	IA-5(11)	Bei einer tokenbasierten Authentifizierung verwendet das Informationssystem Mechanismen, die die von der Organisation festgelegten Qualitätsanforderungen in Bezug auf Token erfüllen.
CCI-000206	IA-6	Das Informationssystem verbirgt das Feedback der Authentifizierungsinformation während des Authentifizierungsvorgangs, um die Informationen vor möglicher Instrumentalisierung/Nutzung durch nicht autorisierte Personen zu schützen.
CCI-000803	IA-7	Das Informationssystem setzt Mechanismen zur Authentifizierung in ein kryptografisches Modul um, das den Anforderungen der gültigen Bundesgesetze, Durchführungsverordnungen, Richtlinien, Regelwerke, Vorschriften und Normen, und Anleitungen für eine solche Authentifizierung entspricht.
CCI-000804	IA-8	Das Informationssystem bezeichnet und authentifiziert eindeutig Benutzer die nicht der Organisation angehören (oder Prozesse, die im Auftrag der Benutzer, die nicht der Organisation angehören, agieren).
CCI-002009	IA-8(1)	Das Informationssystem akzeptiert Personal Identity Verification (PIV) Berechtigungsnachweise von anderen staatlichen Behörden.
CCI-002010	IA-8(1)	Das Informationssystem verifiziert Personal Identity Verification (PIV) Berechtigungsnachweise von anderen staatlichen Behörden elektronisch.
CCI-002011	IA-8(2)	Das Informationssystem akzeptiert von FICAM genehmigte Berechtigungsnachweise Dritter.
CCI-002013	IA-8(3)	Die Organisation wendet nur durch FICAM genehmigte Informationssystem-Komponenten in den von der Organisation festgelegten Informationssystemen die Berechtigungsnachweise Dritter akzeptieren.
CCI-002014	IA-8(4)	Das Informationssystem entspricht dem von FICAM veröffentlichten Profil.

Tabelle H-6 Platform Enclave CCI's für Kontrollsysteme mit GERINGEN und MITTLEREN Auswirkungen		
CCI #	800-53 Kontroll-text	Begriffserklärung CCI
CCI-000995	MP-1(a)(1)	Die Organisation entwickelt und dokumentiert eine Medienschutzvorschrift, in der Zweck, Umfang, Rolle, Verantwortlichkeiten, Verwaltungsverpflichtung, Abstimmung der betrieblichen Einheiten und Einhaltung thematisiert sind.
CCI-000996	MP-1(a)(1)	Die Organisation verteilt eine Medienschutzvorschrift an von der Organisation festgelegte Personen bzw. Rollen.
CCI-002566	MP-1(a)(1)	Die Organisation legt Personen bzw. Rollen fest, an welche die dokumentierten Medienschutzrichtlinien und -verfahren verteilt werden.
CCI-000999	MP-1(a)(2)	Die Organisation entwickelt und dokumentiert Abläufe zur Erleichterung der Umsetzung der Medienschutzvorschrift und dazugehöriger Medienschutzkontrollen.
CCI-001000	MP-1(a)(2)	Die Organisation verteilt Abläufe zur Erleichterung der Umsetzung der Medienschutzvorschrift und dazugehöriger Medienschutzkontrollen an von der Organisation festgelegte Personen bzw. Rollen.
CCI-000997	MP-1(b)(1)	Die Organisation überprüft und aktualisiert die aktuelle Medienschutzvorschrift mit der von der Organisation festgelegten Häufigkeit.
CCI-000998	MP-1(b)(1)	Die Organisation legt die Häufigkeit der Prüfungen und Aktualisierungen der aktuellen Medienschutzvorschrift fest.
CCI-001001	MP-1(b)(2)	Die Organisation überprüft und aktualisiert die aktuellen Medienschutzabläufe mit der von der Organisation festgelegten Häufigkeit.
CCI-001002	MP-1(b)(2)	Die Organisation legt die Häufigkeit der Prüfungen und Aktualisierungen der aktuellen Medienschutzabläufe fest.
CCI-001003	MP-2	Die Organisation schränkt den Zugriff zu von der Organisation festgelegte Arten an digitalen bzw. nicht-digitalen Medien für von der Organisation festgelegte Personen bzw. Rollen ein.
CCI-001004	MP-2	Die Organisation legt die Arten von digitalen bzw. nicht-digitalen Medien fest, für welche die Organisation den Zugriff einschränkt.
CCI-001005	MP-2	Die Organisation legt die Personen bzw. die Rollen mit eingeschränktem Zugriff auf von der Organisation festgelegte Arten an digitalen bzw. nicht-digitalen Medien fest.
CCI-001028	MP-6(a)	Die Organisation reinigt von der Organisation festgelegte Informationssystemmedien vor Beseitigung, Freigabe aus der Betriebskontrolle oder Freigabe zur Weiterverwendung mit Hilfe von Reinigungstechniken und -abläufen, die von der Organisation festgelegt wurden, gemäß den anzuwendenden Bundes- und Organisationsstandards und -vorschriften.
CCI-002578	MP-6(a)	Die Organisation legt fest, welche Informationssystemmedien vor Beseitigung, Freigabe aus der Betriebskontrolle oder Freigabe zur Weiterverwendung mit Hilfe von Reinigungstechniken und -abläufen, die von der Organisation festgelegt wurden, zu reinigen sind, gemäß den anzuwendenden Bundes- und Organisationsstandards und -vorschriften.
CCI-002579	MP-6(a)	Die Organisation legt die Reinigungstechniken und -abläufe fest, die gemäß den anzuwendenden Bundes- und Organisationsstandards und -vorschriften zur Reinigung von Informationssystemmedien festgelegt durch die Organisation zum Einsatz kommen, vor Beseitigung, Freigabe aus der Betriebskontrolle oder Freigabe zur Weiterverwendung.
CCI-002580	MP-6(b)	Die Organisation verwendet Reinigungsmechanismen deren Stärke und Integrität der Sicherheitskategorie bzw. -klassifikation der Information entsprechen.

Tabelle H-6 Plattform Enclave CCI's für Kontrollsysteme mit GERINGEN und MITTLEREN Auswirkungen		
CCI #	800-53 Kontroll-text	Begriffserklärung CCI
CCI-002581	MP-7	Die Organisation legt die Arten an Informationssystemmedien fest, die auf von der Organisation festgelegten Informationssystemen bzw. Anlageteilen eingeschränkt bzw. verboten sind unter Anwendung der von der Organisation festgelegten Sicherheitsmaßnahmen.
CCI-002582	MP-7	Die Organisation legt die Informationssysteme bzw. Anlageteile fest, für welche die Nutzung von von der Organisation festgelegte Arten an Informationssystemmedien einzuschränken bzw. zu verbieten ist unter Anwendung der von der Organisation festgelegten Sicherheitsmaßnahmen.
CCI-002583	MP-7	Die Organisation legt die Sicherheitsmaßnahmen zur Einschränkung bzw. zum Verbot der Nutzung von von der Organisation festgelegten Arten an Informationssystemmedien auf von der Organisation festgelegten Informationssystemen bzw. Anlageteilen fest.
CCI-002584	MP-7	Die Organisation schränkt die Nutzung von von der Organisation festgelegten Arten an Informationssystemmedien ein bzw. verbietet diese auf von der Organisation festgelegten Informationssystemen bzw. Anlageteilen unter Anwendung der von der Organisation festgelegten Sicherheitsmaßnahmen.
CCI-000965	PE-13	Die Organisation nutzt und unterhält Brandunterdrückungs- bzw. Brandmeldegeräte/ -anlagen für das Informationssystem, die von einer unabhängigen Energiequelle versorgt werden.
CCI-000971	PE-14(a)	Die Organisation hält Temperatur- und Feuchtigkeitswerte innerhalb der Einrichtung, in der das Informationssystem untergebracht ist, konstant auf von der Organisation festgelegten zulässigen Werten.
CCI-000972	PE-14(a)	Die Organisation legt die zulässigen Temperatur- und Feuchtigkeitswerte, die innerhalb der Einrichtung, in der das Informationssystem untergebracht ist, konstant zu halten sind, fest.
CCI-000973	PE-14(b)	Die Organisation überwacht die Temperatur- und Feuchtigkeitswerte mit der von der Organisation festgelegten Häufigkeit.
CCI-000974	PE-14(b)	Die Organisation legt die Häufigkeit der Überwachung von Temperatur- und Feuchtigkeitswerten fest.
CCI-000977	PE-15	Die Organisation schützt das Informationssystem vor Schäden aufgrund von auslaufendem Wasser mit Hilfe von zugänglichen Hauptabsperr- bzw. Sicherheitsabsperrventilen.
CCI-000978	PE-15	Die Organisation schützt das Informationssystem vor Schäden aufgrund von auslaufendem Wasser mit Hilfe von einwandfrei funktionierenden Hauptabsperr- bzw. Sicherheitsabsperrventilen.
CCI-000979	PE-15	Leitende Mitarbeiter haben Kenntnis über die Hauptabsperr- bzw. Sicherheitsabsperrventile für Wasser.
CCI-000981	PE-16	Die Organisation genehmigt die von der Organisation festgelegten Arten an Informationssystemkomponenten, die in die Einrichtung gebracht bzw. aus dieser entfernt werden.
CCI-000982	PE-16	Die Organisation überwacht die von der Organisation festgelegten Arten an Informationssystemkomponenten, die in die Einrichtung gebracht bzw. aus dieser entfernt werden.
CCI-000983	PE-16	Die Organisation kontrolliert die von der Organisation festgelegten Arten an Informationssystemkomponenten, die in die Einrichtung gebracht bzw. aus dieser entfernt werden.
CCI-000984	PE-16	Die Organisation führt Buch über die von der Organisation festgelegten Arten an Informationssystemkomponenten, die in die Einrichtung gebracht bzw. aus dieser entfernt werden.
CCI-002974	PE-16	Die Organisation legt die von der Organisation festgelegten Arten an Informationssystemkomponenten fest, für welche die Einbringung in die bzw. Entfernung aus der Einrichtung zu genehmigen, überwachen, kontrollieren und Buch zu führen ist.
CCI-003051	PL-2(a)(2)	Der Sicherheitsplan der Organisation für das Informationssystem bestimmt eindeutig die Autorisierungsgrenze für das System.

Tabelle H-6 Plattform Enclave CCI's für Kontrollsysteme mit GERINGEN und MITTLEREN Auswirkungen		
CCI #	800-53 Kontroll-text	Begriffserklärung CCI
CCI-000080	PM-3(a)	Die Organisation stellt sicher, dass sämtliche Kapitalplanungen und Investitionsanfragen die Betriebsmittel umfassen, die zur Umsetzung des Informationssicherheitsprogramms notwendig sind, und dokumentiert alle Ausnahmen zu dieser Anforderung.
CCI-000081	PM-3(b)	Die Organisation setzt ein Business Case/ Exhibit 300/ Exhibit 53 zur Dokumentierung der Betriebsmittel ein.
CCI-000141	PM-3(c)	Die Organisation stellt sicher, dass die Betriebsmittel für die Informationssicherheit wie für die Erweiterung geplant zur Verfügung stehen.
CCI-000142	PM-4(a)(1)	Die Organisation implementiert einen Prozess zur Sicherstellung der Einhaltung von Aktionsplänen und Meilensteinen des Sicherheitsprogramms sowie der zugehörigen Betriebsinformationssysteme.
CCI-002991	PM-4(a)(1)	Die Organisation implementiert einen Prozess zur Sicherstellung der Entwicklung von Aktionsplänen und Meilensteinen des Sicherheitsprogramms sowie der zugehörigen Betriebsinformationssysteme.
CCI-000170	PM-4(a)(2)	Die Organisation implementiert einen Prozess um sicherzustellen, dass die Aktionspläne und Meilensteine des Sicherheitsprogramms sowie der zugehörigen Betriebsinformationssysteme, die Abhilfemaßnahmen für Informationssicherheit darstellen, damit auf Gefährdungen für Betriebsprozesse und -vermögen, Personen, andere Betriebe und dem Staat, angemessen reagiert werden kann.
CCI-002992	PM-4(a)(3)	Die Organisation implementiert einen Prozess um sicherzustellen, dass die Aktionspläne und Meilensteine des Sicherheitsprogramms sowie der zugehörigen Betriebsinformationssysteme gemäß den Protokollierungsanforderungen von OMB FISMA protokolliert werden.
CCI-000236	PM-11(b)	Die Organisation legt Informationsschutzerfordernisse fest, die sich aus den festgelegten Einsatz-/Betriebsabläufen ergeben, und überarbeitet diese Abläufe wie erforderlich bis ein erreichbarer Satz an Schutzerfordernissen erzielt wurde.
CCI-001054	RA-5(a)	Die Organisation durchsucht das Informationssystem nach Schwachstellen und gehosteten Anwendungen in einer von der Organisation festgelegten Häufigkeit.
CCI-001055	RA-5(a)	Die Organisation bestimmt die Häufigkeit, in der das Informationssystem und gehostete Anwendungen auf Schwachstellen durchsucht werden.
CCI-001056	RA-5(a)	Die Organisation durchsucht das Informationssystem und gehostete Anwendungen, wenn neue Schwachstellen, die das System/die Anwendungen möglicherweise beeinträchtigen könnten, festgestellt und gemeldet werden.
CCI-001641	RA-5(a)	Die Organisation bestimmt den Prozessablauf zur Durchführung von Random Scans auf Schwachstellen des Informationssystems und gehosteter Anwendungen.
CCI-001643	RA-5(a)	Die Organisation durchsucht das Informationssystem nach Schwachstellen und gehosteten Anwendungen mit einem von der Organisation festgelegten Prozessablauf für Random Scans.
CCI-001057	RA-5(b)	Die Organisation verwendet Scanning Tools, um Schwachstellen zu finden, und Techniken, die Interoperabilität zwischen den Tools ermöglichen und Teilbereiche des Schwachstellen-Management Prozesses automatisieren, indem Standards für Folgendes verwendet werden: Spezifizierung von Plattformen, Softwarefehler und unrichtige Konfigurationen, Formatieren von Checklisten und Prüfverfahren und Erfassung der Auswirkungen von Schwachstellen.
CCI-001058	RA-5(c)	Die Organisation analysiert Schwachstellenscanberichte und die Ergebnisse von Sicherheitskontrollbeurteilungen.
CCI-001059	RA-5(d)	Die Organisation beseitigt legitime Schwachstellen innerhalb einer von der Organisation festgelegten Reaktionszeit gemäß einem betrieblichen Beurteilungsrisiko.

Tabelle H-6 Platform Enclave CCI's für Kontrollsysteme mit GERINGEN und MITTLEREN Auswirkungen		
CCI #	800-53 Kontroll-text	Begriffserklärung CCI
CCI-003116	SA-4(10)	Die Organisation nutzt ausschließlich IT-Produkte von der FIPS PUB 201-2 Liste zugelassener Produkte für PIV-Fähigkeit umgesetzt in Betriebsinformationssystemen.
CCI-000669	SA-9(a)	Die Organisation fordert, dass Anbieter von externen Informationssystemdienstleistungen die Informationssicherheitsauflagen der Organisation einhalten.
CCI-000670	SA-9(a)	Die Organisation fordert, dass Anbieter von externen Informationssystemdienstleistungen die von der Organisation festgelegten Sicherheitskontrollen gemäß gültigen Bundesgesetzen, Durchführungsverordnungen, Richtlinien, Regelwerken, Vorschriften, Normen und Leitfäden, einsetzen.
CCI-003137	SA-9(a)	Die Organisation legt die Sicherheitskontrollen fest, die Anbieter von externen Informationssystemdienstleistungen gemäß gültigen Bundesgesetzen, Durchführungsverordnungen, Richtlinien, Regelwerken, Vorschriften, Normen und Leitfäden anwenden.
CCI-000671	SA-9(b)	Die Organisation legt die Regierungsaufsicht mit Hinblick auf externe Informationssystemdienstleistungen fest.
CCI-000672	SA-9(b)	Die Organisation dokumentiert die Regierungsaufsicht mit Hinblick auf externe Informationssystemdienstleistungen.
CCI-000673	SA-9(b)	Die Organisation legt Benutzerrollen und -verantwortlichkeiten mit Hinblick auf externe Informationssystemdienstleistungen fest.
CCI-000674	SA-9(b)	Die Organisation dokumentiert Benutzerrollen und -verantwortlichkeiten mit Hinblick auf externe Informationssystemdienstleistungen.
CCI-003138	SA-9(c)	Die Organisation nutzt von der Organisation festgelegte Abläufe, Methoden und Techniken zur ständigen Überwachung der Einhaltung von Sicherheitskontrollen von externen Dienstleistungsanbietern.
CCI-003139	SA-9(c)	Die Organisation legt Abläufe, Methoden und Techniken fest, die zur ständigen Überwachung der Einhaltung von Sicherheitskontrollen von externen Dienstleistungsanbietern, einzusetzen sind.
CCI-001093	SC-5	Die Organisation bestimmt die Varianten der Denial-of-Service Angriffe (oder gibt Verweise auf Quellen aktueller Denial-of-Service Angriffe) die das Informationssystem angehen kann.
CCI-002385	SC-5	Das Informationssystem schützt vor oder beschränkt die Auswirkungen der von der Organisation festgelegten Varianten der Denial-of-Service Angriffe, indem von der Organisation festgelegte Sicherheitsmaßnahmen eingesetzt werden.
CCI-002386	SC-5	Die Organisation legt die Sicherheitsmaßnahmen fest, die eingesetzt werden sollen, um das Informationssystem gegen die Auswirkungen von Denial-of-Service Angriffen zu schützen/diese zu beschränken.
CCI-001097	SC-7(a)	Das Informationssystem überwacht und kontrolliert Kommunikationen an der äußeren Grenze des Systems und an wichtigen internen Grenzen innerhalb des Systems.
CCI-001098	SC-7(c)	Das Informationssystem ist nur über verwaltete Schnittstellen mit externen Netzwerken bzw. Informationssystemen verbunden; diese Schnittstellen bestehen aus Geräten zum Schutz der Außengrenze, die gemäß der Informationssicherheits-Architektur der Organisation angeordnet sind.
CCI-002428	SC-12	Die Organisation legt Anforderungen an die Kryptographieschlüsselerstellung fest, die innerhalb des Informationssystems zu nutzen ist.
CCI-002429	SC-12	Die Organisation legt Anforderungen an die Kryptographieschlüsselverteilung fest, die innerhalb des Informationssystems zu nutzen ist.

Tabelle H-6 Platform Enclave CCI's für Kontrollsysteme mit GERINGEN und MITTLEREN Auswirkungen		
CCI #	800-53 Kontroll-text	Begriffserklärung CCI
CCI-002430	SC-12	Die Organisation legt Anforderungen an die Kryptographieschlüsselspeicherung fest, die innerhalb des Informationssystems zu nutzen ist.
CCI-002431	SC-12	Die Organisation legt Anforderungen an den Kryptographieschlüsselzugriff fest, der innerhalb des Informationssystems zu nutzen ist.
CCI-002432	SC-12	Die Organisation legt Anforderungen an die Kryptographieschlüssellöschung fest, die innerhalb des Informationssystems zu nutzen ist.
CCI-001150	SC-15(a)	Das Informationssystem verbietet die Fernaktivierung von gemeinschaftlichen EDV-Geräten, außer bei den von der Organisation festgelegten Ausnahmen, für die eine Fernaktivierung zulässig ist.
CCI-001151	SC-15(a)	Die Organisation legt die Ausnahmen zur Einschränkung gemeinschaftlicher EDV-Geräte fest, für die Fernaktivierung zulässig sein soll.
CCI-001152	SC-15(b)	Das Informationssystem stellt den Benutzern körperlich anwesend an den gemeinschaftlichen EDV-Geräten klare Nutzeranweisungen zur Verfügung.
CCI-002465	SC-21	Das Informationssystem fordert einen Datenquellenauthentifizierungsnachweis für Antworten auf die Namens-/Adressenauflösung, die das System von autoritativen Quellen erhält.
CCI-002466	SC-21	Das Informationssystem fordert einen Datenintegritätssnachweis für Antworten auf die Namens-/Adressenauflösung, die das System von autoritativen Quellen erhält.
CCI-002467	SC-21	Das Informationssystem führt einen Datenintegrationsnachweis für Antworten auf die Namens-/Adressenauflösung, die das System von autoritativen Quellen erhält, durch.
CCI-002468	SC-21	Das Informationssystem führt einen Datenquellenauthentifizierungsnachweis für Antworten auf die Namens-/Adressenauflösung, die das System von autoritativen Quellen erhält, durch.
CCI-002544	SC-41	Die Organisation legt die Informationssysteme oder Informationssystem-Komponenten fest, auf denen von der Organisation festgelegte Verbindungsschnittstellen bzw. Ein-/Ausgangsgeräte physisch deaktiviert oder entfernt werden sollen.
CCI-002545	SC-41	Die Organisation legt Verbindungsschnittstellen bzw. Ein-/Ausgangsgeräte fest, die von von der Organisation festgelegten Informationssystemen oder Informationssystem-Komponenten physisch deaktiviert oder entfernt werden sollen.
CCI-001227	SI-2(a)	Die Organisation korrigiert Fehler im Informationssystem.
CCI-001228	SI-2(b)	Die Organisation prüft Software-Updates bzgl. Fehlerbehebung mit Hinblick auf Effektivität vor Installation.
CCI-001229	SI-2(b)	Die Organisation prüft Software-Updates bzgl. Fehlerbehebung mit Hinblick auf mögliche Nebeneffekte vor Installation.
CCI-002602	SI-2(b)	Die Organisation prüft Firmware-Updates bzgl. Fehlerbehebung mit Hinblick auf Effektivität vor Installation.
CCI-002603	SI-2(b)	Die Organisation prüft Firmware-Updates bzgl. Fehlerbehebung mit Hinblick auf mögliche Nebeneffekte vor Installation.
CCI-002619	SI-3(a)	Die Organisation nutzt Vorrichtungen zum Schutz gegen Schadcode an Zugangspunkten des Informationssystems, um Schadcode zu erkennen.
CCI-002620	SI-3(a)	Die Organisation nutzt Vorrichtungen zum Schutz gegen Schadcode an Ausgangspunkten des Informationssystems, um Schadcode zu erkennen.
CCI-002621	SI-3(a)	Die Organisation nutzt Vorrichtungen zum Schutz gegen Schadcode an Zugangspunkten des Informationssystems, um Schadcode zu eliminieren.
CCI-002622	SI-3(a)	Die Organisation nutzt Vorrichtungen zum Schutz gegen Schadcode an Ausgangspunkten des Informationssystems, um Schadcode zu eliminieren.

Tabelle H-6 Plattform Enclave CCI's für Kontrollsysteme mit GERINGEN und MITTLEREN Auswirkungen		
CCI #	800-53 Kontroll-text	Begriffserklärung CCI
CCI-001241	SI-3(c)(1)	Die Organisation konfiguriert Schutzmechanismen gegen Schadcode, um regelmäßige Scans des Informationssystems in einer von der Organisation bestimmten Häufigkeit durchzuführen.
CCI-001242	SI-3(c)(1)	Die Organisation konfiguriert Schutzmechanismen gegen Schadcode, um Echtzeitscans der Dateien von externen Quellen an den Endpunkten durchzuführen während Dateien heruntergeladen, geöffnet bzw. ausgeführt werden gemäß der Sicherheitsvorschrift der Organisation.
CCI-002624	SI-3(c)(1)	Die Organisation konfiguriert Schutzmechanismen gegen Schadcode, um Echtzeitscans der Dateien von externen Quellen an den Eingangs-/Ausgangspunkten des Netzwerks durchzuführen während Dateien heruntergeladen, geöffnet bzw. ausgeführt werden gemäß der Sicherheitsvorschrift der Organisation.
CCI-001243	SI-3(c)(2)	Die Organisation konfiguriert Schutzmechanismen gegen Schadcode, um von der Organisation festgelegte Aktionen durchzuführen als Reaktion auf die Entdeckung von Schadcodes.
CCI-001244	SI-3(c)(2)	Die Organisation legt eine bzw. mehrere Aktionen fest, die als Antwort auf die Entdeckung von Schadcode durchzuführen sind; z.B. das Blockieren von Schadcode, Quarantäne von Schadcode oder das Versenden von Alarmsignalen an den Administrator.
CCI-001253	SI-4(a)(1)	Die Organisation legt die Zielvorgaben der Überwachung zur Verhinderung von Angriffen und Indikatoren möglicher Angriffe auf das Informationssystem fest.
CCI-002641	SI-4(a)(1)	Die Organisation überwacht das Informationssystem, um Angriffe bzw. Hinweise auf mögliche Angriffe gemäß den von der Organisation festgelegten Überwachungszielen zu erkennen.
CCI-002644	SI-4(a)(2)	Die Organisation überwacht das Informationssystem, um unzulässige Fernverbindungen zu erkennen.
CCI-002642	SI-4(a)(2)	Die Organisation überwacht das Informationssystem, um unzulässige lokale Verbindungen zu erkennen.
CCI-002643	SI-4(a)(2)	Die Organisation überwacht das Informationssystem, um unzulässige Netzwerkverbindungen zu erkennen.
CCI-002645	SI-4(b)	Die Organisation legt die Techniken und Methoden fest, die verwendet werden, um die unbefugte Nutzung des Informationssystems zu erkennen.
CCI-002646	SI-4(b)	Die Organisation identifiziert die unbefugte Nutzung des Informationssystems mit von der Organisation festgelegten Techniken und Methoden.
CCI-001256	SI-4(c)	Die Organisation setzt Überwachungsgeräte an ad-hoc Stellen innerhalb des Systems ein, um spezielle Arten von Transaktionen, die für die Organisation interessant sind, nachverfolgen zu können.
CCI-002647	SI-4(d)	Die Organisation schützt Informationen, die sie von Einbruchmelde-Tools erhält, gegen unbefugten Zugriff.
CCI-002648	SI-4(d)	Die Organisation schützt Informationen, die sie von Einbruchmelde-Tools erhält, gegen unbefugte Änderungen.
CCI-002649	SI-4(d)	Die Organisation schützt Informationen, die sie von Einbruchmelde-Tools erhält, gegen unbefugtes Löschen.
CCI-001257	SI-4(e)	Die Organisation erhöht die Überwachungsaktivität des Informationssystems, wenn Hinweise auf ein erhöhtes Risiko für Betriebsprozesse und -vermögen, Personen, andere Betriebe und dem Staat aufgrund von Informationen durch Vollzugsbehörden, Geheimdiensten oder anderen vertrauenswürdigen Quellen, bestehen.

Tabelle H-6 Platform Enclave CCI's für Kontrollsysteme mit GERINGEN und MITTLEREN Auswirkungen		
CCI #	800-53 Kontroll-text	Begriffserklärung CCI
CCI-001258	SI-4(f)	Die Organisation holt sich juristischen Rat bezüglich der Überwachungsaktivitäten von Informationssystemen gemäß gültigen Bundesgesetzen, Durchführungsverordnungen, Richtlinien bzw. Regelwerken.
CCI-002650	SI-4(g)	Die Organisation legt die Überwachungsinformationen zum Informationssystem fest, die von der Organisation festgelegten Personen bzw. Rollen zur Verfügung gestellt werden.
CCI-002651	SI-4(g)	Die Organisation legt die Personen bzw. Rollen fest, die von der Organisation festgelegte Überwachungsinformationen zum System erhalten sollen.
CCI-002652	SI-4(g)	Die Organisation legt die Häufigkeit fest, mit der die Organisation von der Organisation festgelegte Überwachungsinformationen zum Informationssystem an von der Organisation festgelegte Personen bzw. Rollen weiter gibt.
CCI-002654	SI-4(g)	Die Organisation stellt die von der Organisation festgelegten Überwachungsinformationen zum Informationssystem den von der Organisation festgelegte Personen bzw. Rollen nach Erfordernis bzw. in der von der Organisation festgelegten Häufigkeit, zur Verfügung.
CCI-001285	SI-5(a)	Die Organisation erhält ständig Sicherheitswarnungen, Empfehlungen und Anweisungen zum Informationssystem von externen Organisationen festgelegt von der Organisation.
CCI-002692	SI-5(a)	Die Organisation legt die externen Organisationen fest, von denen sie Sicherheitswarnungen, Empfehlungen und Anweisungen zum Informationssystem erhält.
CCI-001286	SI-5(b)	Die Organisation erstellt interne Sicherheitswarnungen, Empfehlungen und Anweisungen nach Notwendigkeit.
CCI-001287	SI-5(c)	Die Organisation verteilt Sicherheitswarnungen, Empfehlungen und Anweisungen an von der Organisation festgelegte Personen bzw. Rollen, an von der Organisation festgelegte Elemente innerhalb der Organisation bzw. an von der Organisation festgelegte externe Organisationen.
CCI-001288	SI-5(c)	Die Organisation legt die Personen bzw. Rollen fest, an welche die Organisation Sicherheitswarnungen, Empfehlungen und Anweisungen verteilt.
CCI-002693	SI-5(c)	Die Organisation legt Elemente innerhalb der Organisation fest, an welche die Organisation Sicherheitswarnungen, Empfehlungen und Anweisungen verteilt.
CCI-001289	SI-5(d)	Die Organisation implementiert Sicherheitsanweisungen gemäß dem festgelegten Zeitrahmen, bzw. informiert die herausgebende Organisation über das Ausmaß der Nichtübereinstimmung.

Tabelle H-7 Zusätzliche Platform Enclave CCI's für Kontrollsysteme mit MITTLERER Auswirkung		
CCI #	800-53 Kontroll-text	Begriffserklärung CCI
CCI-000015	AC-2(1)	Die Organisation setzt automatische Mechanismen zur Unterstützung der Kontoverwaltungsfunktionen des Informationssystems ein.
CCI-001682	AC-2(2)	Das Informationssystem entfernt oder deaktiviert nach Ablauf eines durch die Organisation für alle Kontenarten festgelegten Zeitraumes automatisch Notfallkontos.
CCI-000016	AC-2(2)	Das Informationssystem entfernt oder deaktiviert nach Ablauf eines durch die Organisation für alle Kontenarten festgelegten Zeitraumes automatisch zeitlich begrenzte Konten.
CCI-001361	AC-2(2)	Die Organisation legt einen Zeitraum fest, nach dessen Ablauf zeitlich begrenzte Konten automatisch gelöscht werden.
CCI-001365	AC-2(2)	Die Organisation legt einen Zeitraum fest, nach dessen Ablauf Notfallkonten automatisch gelöscht werden.
CCI-000017	AC-2(3)	Nach Ablauf eines von der Organisation festgelegten Zeitraums werden inaktive Konten automatisch deaktiviert.
CCI-000018	AC-2(4)	Das Informationssystem kontrolliert automatisch Handlungen zur Kontorstellung.
CCI-001403	AC-2(4)	Das Informationssystem kontrolliert automatisch Handlungen zur Kontoänderung.
CCI-001404	AC-2(4)	Das Informationssystem kontrolliert automatisch Handlungen zur Kontodeaktivierung.
CCI-001405	AC-2(4)	Das Informationssystem überprüft automatisch Handlungen zur Kontolöschung.
CCI-002130	AC-2(4)	Das Informationssystem überprüft automatisch Handlungen zur Kontoaktivierung.
CCI-001683	AC-2(4)	Das Informationssystem erkennt von der Organisation zugelassene Personen oder Rollen bei der Durchführung der Kontoerstellung.
CCI-001684	AC-2(4)	Das Informationssystem erkennt von der Organisation zugelassene Personen oder Rollen bei der Durchführung der Kontoänderung.
CCI-001685	AC-2(4)	Das Informationssystem erkennt von der Organisation zugelassene Personen oder Rollen bei der Durchführung der Kontodeaktivierung.
CCI-001686	AC-2(4)	Das Informationssystem erkennt von der Organisation zugelassene Personen oder Rollen bei der Durchführung der Kontolöschung.
CCI-002132	AC-2(4)	Das Informationssystem erkennt von der Organisation zugelassene Personen oder Rollen bei der Durchführung der Kontoaktivierung.
CCI-001368	AC-4	Das Informationssystem setzt genehmigte Autorisierungen zur Kontrolle des Informationsflusses innerhalb des Systems gemäß den durch die Organisation vorgegebenen Vorgängen zur Kontrolle des Informationsflusses um.
CCI-001414	AC-4	Das Informationssystem setzt genehmigte Autorisierungen zur Kontrolle des Informationsflusses zwischen den verbundenen Systemen gemäß den durch die Organisation vorgegebenen Vorgängen zur Kontrolle des Informationsflusses um.
CCI-001548	AC-4	Die Organisation legt die Vorgänge zur Kontrolle des Informationsflusses für die Kontrolle des Informationsflusses innerhalb des Systems fest.
CCI-001549	AC-4	Die Organisation legt die Vorgänge zur Kontrolle des Informationsflusses für die Kontrolle des Informationsflusses zwischen verbundenen Systemen fest.
CCI-001550	AC-4	Die Organisation legt zugelassene Autorisierungen für die Kontrolle des Informationsflusses innerhalb des Systems fest.
CCI-001551	AC-4	Die Organisation legt zugelassene Autorisierungen für die Kontrolle des Informationsflusses zwischen verbundenen Systemen fest.
CCI-002220	AC-5(c)	Die Organisation legt Zugangsauthorisierungen zum Informationssystem zur Unterstützung der Aufgabentrennung fest.

Tabelle H-7 Zusätzliche Platform Enclave CCI's für Kontrollsysteme mit MITTLERER Auswirkung		
CCI #	800-53 Kontroll-text	Begriffserklärung CCI
CCI-000225	AC-6	Die Organisation nutzt das Prinzip der geringsten Privilegien, wonach Benutzer (und Prozesse, die im Auftrag des Nutzers agieren) nur solche Zugangsberechtigungen haben, die zur Erfüllung der gegebenen Aufgaben gemäß betrieblichen Aufgaben und Funktionen notwendig sind.
CCI-000058	AC-11(a)	Das Informationssystem gibt den Benutzern die Möglichkeit, Mechanismen zur Sperrung von Sitzungen direkt zu veranlassen.
CCI-000059	AC-11(a)	Die Organisation legt einen Inaktivitätszeitraum fest, nach dessen Ablauf das Informationssystem eine Sperrung der Sitzung veranlasst.
CCI-000056	AC-11(b)	Das Informationssystem hält die Sperrung der Sitzung so lange aufrecht, bis der Benutzer die festgelegten Identifikations- und Authentifizierungsvorgänge durchgeführt hat, um den Zugang zu erneuern.
CCI-000060	AC-11(1)	Das Informationssystem verdeckt bei Sperrung der Sitzung Informationen, die vorher auf dem Bildschirm sichtbar waren, durch ein Bild, das für die Öffentlichkeit zugelassen ist.
CCI-002360	AC-12	Die Bedingungen oder Auslöser für eine Deaktivierung der Sitzung, die vom Informationssystem angewendet werden, um eine Benutzersitzung automatisch zu beenden, werden von der Organisation festgelegt.
CCI-002361	AC-12	Das Informationssystem beendet eine Benutzersitzung automatisch, wenn eine Bedingung oder ein Auslöser vorliegt, die gemäß Festlegung der Organisation eine Sitzungs-Deaktivierung erforderlich macht.
CCI-000067	AC-17(1)	Das Informationssystem überwacht Fernzugriffsmethoden.
CCI-002314	AC-17(1)	Das Informationssystem kontrolliert Fernzugriffsmethoden.
CCI-000068	AC-17(2)	Das Informationssystem setzt kryptographische Mechanismen zum Schutz der Vertraulichkeit bei Fernzugriffsitzungen um.
CCI-001453	AC-17(2)	Das Informationssystem setzt kryptographische Mechanismen zum Schutz der Integrität bei Fernzugriffsitzungen um.
CCI-000069	AC-17(3)	Das Informationssystem führt alle Fernzugriffe über eine von der Organisation festgelegte Anzahl von verwalteten Netzwerkzugriffskontrollpunkten.
CCI-001561	AC-17(3)	Die Organisation legt die verwalteten Zugriffskontrollpunkte für Fernzugriff auf das Informationssystem fest.
CCI-002315	AC-17(3)	Die Organisation legt die Anzahl an verwalteten Netzwerkzugriffskontrollpunkten fest, über die das Informationssystem sämtliche Fernzugriffe führt.
CCI-000070	AC-17(4)(a)	Die Organisation lässt die Ausführung von privilegierten Befehlen über Fernzugriff nur für von der Organisation festgelegte Belange zu.
CCI-002316	AC-17(4)(a)	Die Organisation lässt den Zugriff auf sicherheitsrelevante Informationen über Fernzugriff nur für von der Organisation festgelegte Belange zu.
CCI-002317	AC-17(4)(a)	Die Organisation legt die betrieblichen Belange fest, für welche die Ausführung von privilegierten Befehlen über Fernzugriff zulässig sein soll.
CCI-002318	AC-17(4)(a)	Die Organisation legt die betrieblichen Belange fest, für welche der Zugriff auf sicherheitsrelevante Informationen über Fernzugriff zulässig sein soll.
CCI-002319	AC-17(4)(b)	Die Organisation dokumentiert die Gründe für die Zulassung der Ausführung von privilegierten Befehlen über Fernzugriff im Sicherheitsplan für das Informationssystem.
CCI-002320	AC-17(4)(b)	Die Organisation dokumentiert die Gründe für die Zulassung des Zugriffs auf sicherheitsrelevante Informationen über Fernzugriff im Sicherheitsplan für das Informationssystem.

Tabelle H-7 Zusätzliche Platform Enclave CCI's für Kontrollsysteme mit MITTLERER Auswirkung		
CCI #	800-53 Kontroll-text	Begriffserklärung CCI
CCI-002231	AC-19(5)	Die Organisation nutzt Kompletgerät-Verschlüsselung oder Container-Verschlüsselung zum Schutz der Integrität von Informationen auf von der Organisation festgelegten mobilen Geräten.
CCI-002329	AC-19(5)	Die Organisation legt die mobilen Geräte fest, auf welchen Kompletgerät-Verschlüsselung bzw. Container-Verschlüsselung zum Schutz der Vertraulichkeit und Integrität von Informationen auf dem Gerät einzusetzen ist.
CCI-002330	AC-19(5)	Die Organisation nutzt Kompletgerät-Verschlüsselung oder Container-Verschlüsselung zum Schutz der Vertraulichkeit von Informationen auf von der Organisation festgelegten mobilen Geräten.
CCI-002333	AC-20(1)(a)	Die Organisation erlaubt zugelassenen Personen den Einsatz eines externen Informationssystems für Zugriff auf das Informationssystem nur, wenn die Organisation die Umsetzung erforderlicher Sicherheitskontrollen des externen Systems gemäß Informationssicherheitsvorschrift und Sicherheitsplan der Organisation nachweist.
CCI-002334	AC-20(1)(a)	Die Organisation erlaubt zugelassenen Personen den Einsatz eines externen Informationssystems für die Weiterverarbeitung von von der Organisation kontrollierten Informationen nur, wenn die Organisation die Umsetzung erforderlicher Sicherheitskontrollen des externen Systems gemäß Informationssicherheitsvorschrift und Sicherheitsplan der Organisation nachweist.
CCI-002335	AC-20(1)(a)	Die Organisation erlaubt zugelassenen Personen den Einsatz eines externen Informationssystems für die Speicherung von von der Organisation kontrollierten Informationen nur, wenn die Organisation die Umsetzung erforderlicher Sicherheitskontrollen des externen Systems gemäß Informationssicherheitsvorschrift und Sicherheitsplan der Organisation nachweist.
CCI-002336	AC-20(1)(a)	Die Organisation erlaubt zugelassenen Personen den Einsatz eines externen Informationssystems für die Weiterleitung von von der Organisation kontrollierten Informationen nur, wenn die Organisation die Umsetzung erforderlicher Sicherheitskontrollen des externen Systems gemäß Informationssicherheitsvorschrift und Sicherheitsplan der Organisation nachweist.
CCI-002337	AC-20(1)(b)	Die Organisation erlaubt zugelassenen Personen den Einsatz eines externen Informationssystems für Zugriff auf das Informationssystem bzw. für die Weiterverarbeitung, Speicherung oder Weiterleitung von von der Organisation kontrollierten Informationen nur, wenn die Organisation zugelassene Informationssystemverbindungs- bzw. Verarbeitungsvereinbarungen mit der betrieblichen Einheit, die das externe Informationssystem betreut, hält.
CCI-000097	AC-20(2)	Die Organisation beschränkt bzw. verbietet den Einsatz von von der Organisation kontrollierten tragbaren Speichergeräten durch zugelassene Personen in externen Informationssystemen.
CCI-001875	AU-7(a)	Das Informationssystem bietet die Möglichkeit, die Anzahl der Prüfungen durch Prüfungen und Analysen auf Abruf zu reduzieren.
CCI-001876	AU-7(a)	Das Informationssystem bietet die Möglichkeit, die Anzahl der Prüfungen durch Berichterstattung auf Abruf zu reduzieren.
CCI-001877	AU-7(a)	Das Informationssystem bietet die Möglichkeit, die Anzahl der Prüfungen durch nachträgliche Untersuchungen von Sicherheitsvorfällen zu reduzieren.
CCI-001878	AU-7(a)	Das Informationssystem bietet die Möglichkeit, Berichte auf Grundlage der Prüfung und Analyse auf Anfrage zu erstellen.
CCI-001879	AU-7(a)	Das Informationssystem bietet die Möglichkeit, Berichte durch Berichterstattung auf Anfrage zu erstellen.

Tabelle H-7 Zusätzliche Platform Enclave CCI's für Kontrollsysteme mit MITTLERER Auswirkung		
CCI #	800-53 Kontroll-text	Begriffserklärung CCI
CCI-001880	AU-7(a)	Das Informationssystem bietet die Möglichkeit Berichte durch nachträgliche Untersuchungen von Sicherheitsvorfällen zu erstellen.
CCI-001881	AU-7(b)	Das Informationssystem bietet die Möglichkeit, Prüfungen zu reduzieren, ohne deren ursprünglichen Inhalt bzw. die Zeitnotierung von Prüfberichten zu verändern.
CCI-001882	AU-7(b)	Das Informationssystem bietet die Möglichkeit, Berichte zu erstellen, ohne deren ursprünglichen Inhalt bzw. die Zeitnotierung von Prüfberichten zu verändern.
CCI-000158	AU-7(1)	Das Informationssystem bietet die Möglichkeit, Prüfberichte für interessebasierte Ereignisse auf der Grundlage von durch die Organisation festgelegten Prüffeldern im Rahmen der Prüfberichte durchzuführen.
CCI-002080	CA-3(5)	Die Organisation nutzt entweder alle-zulassen, verweigern nach Ausnahme oder alle-verweigern Berechtigungen nach Ausnahmenvorschrift für die Freigabe der Verbindung von von der Organisation festgelegten Informationssystemen mit externen Informationssystemen.
CCI-002081	CA-3(5)	Die Organisation legt die Informationssysteme fest, die für die Freigabe der Verbindung mit externen Informationssystemen entweder alle-zulassen, verweigern nach Ausnahme oder alle-verweigern Berechtigungen nach Ausnahmenvorschrift nutzen.
CCI-002082	CA-3(5)	Die Organisation wählt entweder alle-zulassen, verweigern nach Ausnahme oder alle-verweigern Berechtigungen nach Ausnahmenvorschrift für die Freigabe der Verbindung von von der Organisation festgelegten Informationssystemen mit externen Informationssystemen.
CCI-000338	CM-5	Die Organisation legt physische Zugriffseinschränkungen mit Bezug auf Änderungen am Informationssystem fest.
CCI-000339	CM-5	Die Organisation dokumentiert physische Zugriffseinschränkungen mit Bezug auf Änderungen am Informationssystem.
CCI-000340	CM-5	Die Organisation genehmigt physische Zugriffseinschränkungen mit Bezug auf Änderungen am Informationssystem.
CCI-000341	CM-5	Die Organisation vollzieht physische Zugriffseinschränkungen mit Bezug auf Änderungen am Informationssystem.
CCI-000342	CM-5	Die Organisation legt logische Zugriffseinschränkungen mit Bezug auf Änderungen am Informationssystem fest.
CCI-000343	CM-5	Die Organisation dokumentiert logische Zugriffseinschränkungen mit Bezug auf Änderungen am Informationssystem.
CCI-000344	CM-5	Die Organisation genehmigt logische Zugriffseinschränkungen mit Bezug auf Änderungen am Informationssystem.
CCI-000345	CM-5	Die Organisation vollzieht logische Zugriffseinschränkungen mit Bezug auf Änderungen am Informationssystem.
CCI-000419	CM-8(5)	Die Organisation überprüft, dass keine Komponenten innerhalb der Autorisierungsgrenze des Informationssystems als Kopie in anderen Informationssystemverzeichnissen hinterlegt sind.
CCI-000505	CP-6(a)	Die Organisation richtet einen alternativen Speicherort ein; einschließlich der notwendigen Vereinbarungen zur Zulassung der Speicherung und Abrufung von Backup-Informationen des Informationssystems.
CCI-002836	CP-6(b)	Die Organisation stellt sicher, dass der alternative Speicherort mit den gleichen Informationssicherheitsmaßnahmen ausgestattet ist wie der primäre Speicherort.
CCI-000507	CP-6(1)	Die Organisation bestimmt einen alternativen Speicherort getrennt vom primären Speicherort, um die Anfälligkeit für gleiche Bedrohungen zu reduzieren.
CCI-000509	CP-6(3)	Die Organisation identifiziert mögliche Zugriffsprobleme zum alternativen Speicherort im Falle einer flächendeckenden Unterbrechung bzw. Katastrophe.

Tabelle H-7 Zusätzliche Platform Enclave CCI's für Kontrollsysteme mit MITTLERER Auswirkung		
CCI #	800-53 Kontroll-text	Begriffserklärung CCI
CCI-001604	CP-6(3)	Die Organisation beschreibt genaue Minderungsmaßnahmen für von der Organisation identifizierte Zugriffsprobleme zum alternativen Speicherort im Falle einer flächendeckenden Unterbrechung bzw. Katastrophe.
CCI-000510	CP-7(a)	Die Organisation legt den Zeitraum im Einklang mit den Wiederherstellungszeit- und Wiederherstellungspunktvorgaben für wesentliche aufgabenbezogene / betriebliche Funktionen fest, um die Übertragung und Wiederaufnahme von von der Organisation festgelegte Informationssystem-Transaktionen an einem alternativen Bearbeitungsort zuzulassen, wenn die primären Verarbeitungskapazitäten nicht zur Verfügung stehen.
CCI-000513	CP-7(a)	Die Organisation richtet einen alternativen Verarbeitungsstandort einschließlich erforderlicher Vereinbarungen ein, um die Übertragung und Wiederaufnahme von der Organisation bestimmten Informationssystem-Transaktionen für wesentliche Aufgaben innerhalb eines von der Organisation festgelegten Zeitraums, der mit den Wiederherstellungszeit- und Wiederherstellungspunktvorgaben vereinbar ist, wenn primäre Verarbeitungskapazitäten nicht verfügbar sind, zu gestatten.
CCI-002839	CP-7(a)	Die Organisation legt die Informationssystem-Transaktionen fest, die zur Übertragung und Wiederaufnahme an einem alternativen Verarbeitungsort für wesentliche aufgabenbezogene/betriebliche Funktionen zugelassen sind, wenn die primären Verarbeitungskapazitäten nicht zur Verfügung stehen.
CCI-000515	CP-7(b)	Die Organisation stellt sicher, dass die für die Übertragung und Wiederaufnahme des Betriebs notwendigen Geräte und Hilfsmaterialien am alternativen Verarbeitungsort zur Verfügung stehen bzw. das Verträge zur Unterstützung der Lieferung zum Verarbeitungsort innerhalb eines von der Organisation festgelegten Zeitrahmens für Übertragung/Wiederaufnahme bestehen.
CCI-000521	CP-7(c)	Die Organisation stellt sicher, dass der alternative Verarbeitungsort mit den gleichen Informationssicherheitsmaßnahmen ausgestattet ist wie der primäre Verarbeitungsort.
CCI-000516	CP-7(1)	Die Organisation bestimmt einen alternativen Verarbeitungsort getrennt vom primären Verarbeitungsort, um die Anfälligkeit für gleiche Bedrohungen zu reduzieren.
CCI-000517	CP-7(2)	Die Organisation identifiziert mögliche Zugriffsprobleme zum alternativen Verarbeitungsort im Falle einer flächendeckenden Unterbrechung bzw. Katastrophe.
CCI-001606	CP-7(2)	Die Organisation beschreibt genaue Minderungsmaßnahmen für von der Organisation identifizierte mögliche Zugriffsprobleme zum alternativen Verarbeitungsort im Falle einer flächendeckenden Unterbrechung bzw. Katastrophe.
CCI-000518	CP-7(3)	Die Organisation entwickelt alternative Verarbeitungsvereinbarungen, die Regulierungen zur Leistungspriorität gemäß den Verfügbarkeitsanforderungen der Organisation umfassen (einschließlich Wiederherstellungszeitvorgaben).
CCI-000522	CP-8	Die Organisation bestimmt den Zeitraum, um die Wiederaufnahme der von der Organisation festgelegten Informationssystem-Transaktionen für wesentliche Aufgaben zu gestatten, wenn die primären Möglichkeiten zur Fernübertragung in keiner der primären oder alternativen Verarbeitungs- oder Speicherstätten verfügbar sind.
CCI-000524	CP-8	Die Organisation errichtet alternative Fernübertragungsdienste, einschließlich erforderlicher Vereinbarungen, um die Wiederaufnahme der von der Organisation festgelegten Informationssystem-Transaktionen für wesentliche Aufgaben innerhalb eines von der Organisation bestimmten Zeitraums zu gestatten, wenn die primären Möglichkeiten zur Fernübertragung in keiner der primären oder alternativen Verarbeitungs- oder Speicherstätten verfügbar sind.

Tabelle H-7 Zusätzliche Platform Enclave CCI's für Kontrollsysteme mit MITTLERER Auswirkung		
CCI #	800-53 Kontroll-text	Begriffserklärung CCI
CCI-002840	CP-8	Die Organisation legt die Informationssystem-Transaktionen fest, die für wesentliche Aufgaben innerhalb des von der Organisation bestimmten Zeitraums wieder aufzunehmen sind, wenn die primären Möglichkeiten zur Fernübertragung in keiner der primären oder alternativen Verarbeitungs- oder Speicherstätten verfügbar sind.
CCI-000526	CP-8(1)(a)	Die Organisation entwickelt Vereinbarungen zu primären Fernübertragungsdienstleistungen, die Regulierungen zur Leistungspriorität gemäß den Verfügbarkeitsanforderungen der Organisation umfassen (einschließlich Wiederherstellungszeitvorgaben).
CCI-000527	CP-8(1)(a)	Die Organisation entwickelt alternative Vereinbarungen zu primären Fernübertragungsdienstleistungen, die Regulierungen zur Leistungspriorität gemäß den Verfügbarkeitsanforderungen der Organisation umfassen (einschließlich Wiederherstellungszeitvorgaben).
CCI-000528	CP-8(1)(b)	Die Organisation fordert Fernmeldedienstleistungspriorität für alle Fernmeldedienstleistungen, die zur Notfallvorsorge im Sinne der nationalen Sicherheit eingesetzt werden, falls die primären Fernmeldedienstleistungen von einer Telefongesellschaft zur Verfügung gestellt werden.
CCI-000529	CP-8(1)(b)	Die Organisation fordert Fernmeldedienstleistungspriorität für alle Fernmeldedienstleistungen, die zur Notfallvorsorge im Sinne der nationalen Sicherheit eingesetzt werden, falls die alternativen Fernmeldedienstleistungen von einer Telefongesellschaft zur Verfügung gestellt werden.
CCI-000530	CP-8(2)	Die Organisation bezieht alternative Fernmeldedienstleistungen, um die Wahrscheinlichkeit eines einzelnen, gemeinsamen Fehlerpunktes bei den primären Fernmeldedienstleistungen zu reduzieren.
CCI-000541	CP-9(1)	Die Organisation bestimmt die Häufigkeit der Prüfung von Backup-Informationen zum Nachweis der Medienzuvverlässigkeit und Informationsintegrität.
CCI-000542	CP-9(1)	Die Organisation prüft die Backup-Informationen gemäß der von der Organisation festgelegten Häufigkeit zum Nachweis der Medienzuvverlässigkeit und Informationsintegrität.
CCI-000766	IA-2(2)	Das Informationssystem führt eine von verschiedenen Faktoren abhängige Authentifizierung für den Netzwerkzugang auf nicht-privilegierte Konten durch.
CCI-000767	IA-2(3)	Das Informationssystem führt eine von verschiedenen Faktoren abhängige Authentifizierung für den lokalen Zugriff auf privilegierte Konten durch.
CCI-001949	IA-2(11)	Das Gerät, das zur Informationssystemumsetzung der von verschiedenen Faktoren abhängigen Authentifizierung für Fernzugriff für privilegierte Konten eingesetzt wird, erfüllt die von der Organisation festgelegten Anforderungen an Mechanismusstärke.
CCI-001951	IA-2(11)	Das Informationssystem setzt von verschiedenen Faktoren abhängige Authentifizierung für Fernzugriff auf nicht-privilegierte Konten so um, dass einer dieser Faktoren von einem anderen Gerät als dem System das zugreift, gestellt wird.
CCI-001952	IA-2(11)	Das Gerät, das zur Informationssystemumsetzung der von verschiedenen Faktoren abhängigen Authentifizierung für Fernzugriff für nicht-privilegierte Konten eingesetzt wird, erfüllt die von der Organisation festgelegten Anforderungen an Mechanismusstärke.
CCI-001948	IA-2(11)	Das Informationssystem setzt von verschiedenen Faktoren abhängige Authentifizierung für Fernzugriff auf privilegierte Konten so um, dass einer dieser Faktoren von einem anderen Gerät als dem System das zugreift, gestellt wird.
CCI-001950	IA-2(11)	Die Organisation legt die Mechanismusstärkeanforderungen an das Gerät fest, das vom zugreifenden System getrennt und so vorgesehen ist, dass ein Faktor der von verschiedenen Faktoren abhängigen Authentifizierung für nicht-privilegierte Konten zur Verfügung gestellt wird.

Tabelle H-7 Zusätzliche Platform Enclave CCI's für Kontrollsysteme mit MITTLERER Auswirkung		
CCI #	800-53 Kontroll-text	Begriffserklärung CCI
CCI-001947	IA-2(11)	Die Organisation legt die Mechanismusstärkeanforderungen an das Gerät fest, das vom zugreifenden System getrennt und so vorgesehen ist, dass ein Faktor der von verschiedenen Faktoren abhängigen Authentifizierung für privilegierte Konten zur Verfügung gestellt wird.
CCI-000185	IA-5(2)(a)	Das Informationssystem für PKI-basierte Authentifizierung bewertet Zertifizierungen, indem es einen Zertifizierungspfad zu einem zugelassenen Trust Anchor aufbaut und nachweist; dies schließt auch die Überprüfung der Information des Zertifizierungsstatus mit ein.
CCI-000186	IA-5(2)(b)	Das Informationssystem für PKI-basierte Authentifizierung setzt den autorisierten Zugriff auf den zugehörigen Public Key durch.
CCI-000187	IA-5(2)(c)	Das Informationssystem für PKI-basierte Authentifizierung bildet die authentifizierte Identität auf dem individuellen Konto oder dem Gruppenkonto ab.
CCI-001991	IA-5(2)(d)	Das Informationssystem für PKI-basierte Authentifizierung führt einen lokalen Cache für Widerrufsdaten durch, um die Pfaderkennung sowie die Bewertung im Falle von Inaktivität für den Zugang zu Widerrufsinformationen durch das Netzwerk zu unterstützen.
CCI-001992	IA-5(3)	Die Organisation legt die Personen bzw. Rollen fest, die für die Autorisierung der Registrierungsstelle der Organisation zuständig sind, die für den Authentifikatorregistrierungsprozess verantwortlich ist.
CCI-001993	IA-5(3)	Die Organisation legt die Registrierungsstelle fest, die für den Authentifikatorregistrierungsprozess verantwortlich ist.
CCI-001994	IA-5(3)	Die Organisation legt die Arten an bzw. spezielle Authentifikatoren fest, die dem Authentifikatorregistrierungsprozess unterliegen.
CCI-001995	IA-5(3)	Die Organisation fordert, dass der Registrierungsprozess für die Annahme von von der Organisation festgelegten Arten an bzw. speziellen Authentifikatoren persönlich oder durch einen vertrauenswürdigen Dritten vor der von der Organisation festgelegten Registrierungsstelle durch von der Organisation festgelegte Personen bzw. Rollen durchgeführt wird.
CCI-001010	MP-3(a)	Die Organisation markiert die Informationssystemmedien mit Angabe der Verteilereinschränkungen, Vorsichtsmaßnahmen zur Handhabung und zutreffende Sicherheitsmarkierungen der Informationen (falls erforderlich).
CCI-001011	MP-3(b)	Die Organisation schließt von der Organisation festgelegte Arten an Informationssystemmedien von der Markierungsanforderung aus, sofern diese Medien innerhalb des von der Organisation festgelegten kontrollierten Bereichs bleiben.
CCI-001012	MP-3(b)	Die Organisation legt die Arten an Informationssystemmedien fest, die von der Markierungsanforderung ausgeschlossen werden, sofern diese Medien innerhalb des von der Organisation festgelegten kontrollierten Bereichs bleiben.
CCI-001013	MP-3(b)	Die Organisation legt die kontrollierten Bereiche fest, in denen die von der Organisation festgelegten Arten an Informationssystemmedien von der Markierungsanforderung ausgeschlossen sind.
CCI-001014	MP-4(a)	Von der Organisation festgelegte Arten an digitalen bzw. nicht-digitalen Medien werden von der Organisation innerhalb der von der Organisation festgelegten kontrollierten Bereiche physisch kontrolliert und sicher gespeichert.
CCI-001015	MP-4(a)	Die Organisation legt die Arten von digitalen bzw. nicht-digitalen Medien fest, die in von der Organisation festgelegten kontrollierten Bereichen physisch zu kontrollieren und sicher zu speichern sind.
CCI-001016	MP-4(a)	Die Organisation legt kontrollierte Bereiche fest, in denen von der Organisation festgelegte Arten an digitalen bzw. nicht-digitalen Medien physisch kontrolliert und sicher gespeichert werden.

Tabelle H-7 Zusätzliche Platform Enclave CCI's für Kontrollsysteme mit MITTLERER Auswirkung		
CCI #	800-53 Kontroll-text	Begriffserklärung CCI
CCI-001018	MP-4(b)	Die Organisation schützt Informationssystemmedien bis zur Zerstörung bzw. Reinigung dieser Medien mit Hilfe von zugelassenen Geräten, Techniken und Abläufen.
CCI-001020	MP-5(a)	Die Organisation schützt und kontrolliert von der Organisation festgelegte Arten an Informationssystemmedien während des Transfers außerhalb von kontrollierten Bereichen unter Anwendung der von der Organisation festgelegten Sicherheitsmaßnahmen.
CCI-001021	MP-5(a)	Die Organisation legt die Arten an Informationssystemmedien fest, die während des Transfers außerhalb von kontrollierten Bereichen zu schützen und zu kontrollieren sind.
CCI-001022	MP-5(a)	Die Organisation legt die Sicherheitsmaßnahmen fest, die zum Schutz und zur Kontrolle von von der Organisation festgelegte Arten an Informationssystemmedien während des Transfers außerhalb von kontrollierten Bereichen anzuwenden sind.
CCI-001023	MP-5(b)	Die Organisation bleibt verantwortlich für die Informationssystemmedien während des Transfers außerhalb von kontrollierten Bereichen.
CCI-001025	MP-5(c)	Die Organisation dokumentiert Aktionen im Zusammenhang mit dem Transfer von Informationssystemmedien.
CCI-001024	MP-5(d)	Die Organisation beschränkt Aktionen im Zusammenhang mit dem Transfer von Informationssystemmedien auf autorisierte Mitarbeiter.
CCI-001027	MP-5(4)	Das Informationssystem setzt kryptographische Mechanismen zum Schutz der Vertraulichkeit und Integrität von gespeicherten Informationen auf digitalen Medien während des Transfers außerhalb von kontrollierten Bereichen ein.
CCI-002585	MP-7(1)	Die Organisation untersagt den Einsatz von mobilen Speichergeräten im Informationssystem der Organisation, wenn diese Geräte keinem Besitzer zugeordnet werden können.
CCI-000956	PE-10(a)	Die Organisation sieht die Möglichkeit vor, den Strom für das Informationssystem bzw. einzelne Anlageteile im Notfall ausschalten zu können.
CCI-000957	PE-10(b)	Die Organisation ordnet Not-Aus-Schalter bzw. Geräte an einer von der Organisation festgelegten Stelle gemäß Informationssystem bzw. Anlageteil an, um Mitarbeitern sicheren und einfachen Zugriff zu ermöglichen.
CCI-000958	PE-10(b)	Die Organisation legt die Stelle für Not-Aus-Schalter bzw. Geräte gemäß Informationssystem bzw. Anlageteil fest.
CCI-000959	PE-10(c)	Die Organisation schützt die Not-Aus-Schalter gegen Auslösung durch Unbefugte.
CCI-002955	PE-11	Die Organisation stellt eine kurzzeitige unterbrechungsfreie Stromversorgung zur Verfügung, um eine ordnungsgemäße Abschaltung des Informationssystems bzw. den Übergang des Informationssystem zu einer dauerhaften alternativen Stromversorgung im Fall eines Verlusts einer primären Stromquelle zu ermöglichen.
CCI-000961	PE-11(1)	Die Organisation stellt eine dauerhafte alternative Stromversorgung für das Informationssystem zur Verfügung, die in der Lage ist, die erforderliche Mindest-Funktionsbereitschaft im Falle eines längeren Ausfalls der primären Stromquelle zu erhalten.
CCI-000968	PE-13(3)	Die Organisation nutzt eine automatische Brandbekämpfungsanlage für Informationssysteme in Einrichtungen, die nicht dauerhaft besetzt sind.
CCI-000985	PE-17(a)	Die Organisation nutzt von der Organisation festgelegte Sicherheitskontrollen an alternativen Arbeitsplätzen.
CCI-002975	PE-17(a)	Die Organisation legt die Sicherheitskontrollen fest, die an alternativen Arbeitsplätzen einzusetzen sind.

Tabelle H-7 Zusätzliche Platform Enclave CCI's für Kontrollsysteme mit MITTLERER Auswirkung		
CCI #	800-53 Kontroll-text	Begriffserklärung CCI
CCI-000987	PE-17(b)	Die Organisation beurteilt die Wirksamkeit der Sicherheitskontrollen an alternativen Arbeitsplätzen so weit wie möglich.
CCI-000988	PE-17(c)	Die Organisation sieht eine Einrichtung vor, über welche die Mitarbeiter mit dem Informationssicherheitspersonal im Falle von Sicherheitsvorfällen bzw. Problemen kommunizieren können.
CCI-000594	PL-4(1)	Die Verhaltensregeln der Organisation umfassen ausdrückliche Einschränkungen der Nutzung von sozialen Medien/Netzwerken.
CCI-000595	PL-4(1)	Die Verhaltensregeln der Organisation umfassen ausdrückliche Einschränkungen zum Veröffentlichen von Informationen der Organisation auf öffentlichen Websites.
CCI-001062	RA-5(1)	Die Organisation wendet Scanning Tools an, die das System auf Schwachstellen testen und im Hinblick auf die Schwachstellen des Informationssystems, die gescannt werden müssen, aktualisierbar sind.
CCI-001063	RA-5(2)	Die Organisation aktualisiert die gescannten Informationssystemschwachstellen in einer von der Organisation festgelegten Häufigkeit, vor einem neuen Scan bzw. wenn neue Schwachstellen gefunden und gemeldet wurden.
CCI-001067	RA-5(5)	Das Informationssystem führt die privilegierte Zugangsautorisierung für von der Organisation festgelegte System-Komponenten für ausgewählte, von der Organisation festgelegte Scans auf Schwachstellen durch.
CCI-001645	RA-5(5)	Die Organisation bestimmt die Komponenten des Informationssystems für die ein privilegierter Zugang für von der Organisation festgelegte Scans auf Schwachstellen autorisiert ist.
CCI-002906	RA-5(5)	Die Organisation legt die Scans auf Schwachstellen fest, durch die das Informationssystem privilegierten Zugang auf von der Organisation festgelegte Informationssystem-Komponenten autorisiert.
CCI-003143	SA-9(2)	Die Organisation fordert von den Anbietern der von der Organisation festgelegten externen Informationssystemdienstleistungen die Identifizierung von Funktionen, Ports, Protokollen und anderen Leistungen, die für die Nutzung solcher Dienstleistungen erforderlich sind.
CCI-003144	SA-9(2)	Die Organisation legt die externen Informationssystemdienstleistungen fest, für welche die Anbieter die Funktionen, Ports, Protokolle und andere Leistungen, die für die Nutzung solcher Dienstleistungen erforderlich sind, identifizieren müssen.
CCI-001082	SC-2	Das Informationssystem trennt die Benutzerfunktionalität (einschließlich Benutzerschnittstellen Services) von der Funktionalität des Informationssystem-Managements.
CCI-001090	SC-4	Das Informationssystem verhindert den unbefugten und unabsichtlichen Transfer von Informationen über gemeinsame Systemquellen.
CCI-001101	SC-7(3)	Die Organisation schränkt die Anzahl der externen Netzwerkverbindungen zum Informationssystem ein.
CCI-001102	SC-7(4)(a)	Die Organisation setzt eine verwaltete Schnittstelle für jeden externen Fernmeldeservice ein.
CCI-001103	SC-7(4)(b)	Die Organisation entwickelt eine Verkehrsflussvorschrift für jede verwaltete Schnittstelle für jeden externen Fernmeldeservice.
CCI-002396	SC-7(4)(c)	Die Organisation schützt die Vertraulichkeit und Integrität der Informationen, die über jede Schnittstelle für jeden externen Fernmeldeservice übertragen werden.
CCI-001105	SC-7(4)(d)	Die Organisation dokumentiert jede Ausnahme zur Verkehrsflussvorschrift mit Angabe der Notwendigkeit für die Aufgabe/den Betrieb sowie der Dauer dieser Notwendigkeit für jeden externen Fernmeldeanschluss.
CCI-001106	SC-7(4)(e)	Die Organisation überprüft die Ausnahmen zur Verkehrsflussvorschrift in einer von der Organisation festgelegten Häufigkeit für jeden externen Fernmeldeservice.

Tabelle H-7 Zusätzliche Platform Enclave CCI's für Kontrollsysteme mit MITTLERER Auswirkung		
CCI #	800-53 Kontroll-text	Begriffserklärung CCI
CCI-001108	SC-7(4)(e)	Die Organisation löscht Ausnahmen zur Verkehrsflussvorschrift, wenn diese nicht mehr durch eine Notwendigkeit für die Aufgabe/den Betrieb begründet sind für jeden externen Fernmeldeservice.
CCI-001109	SC-7(5)	Das Informationssystem verweigert an regulierten Schnittstellen den Kommunikationsfluss im Netzwerk durch Defaults und erlaubt den Kommunikationsfluss im Netzwerk durch Ausnahmeregelungen (z.B. Alle-verweigern, Zulassung nach Ausnahme).
CCI-002397	SC-7(7)	In Verbindung mit einer Fernbedienung verhindert das Informationssystem, das Geräte gleichzeitig lokale Verbindungen mit dem System errichten und über eine andere Verbindung mit den Quellen des externen Netzwerks kommunizieren.
CCI-001133	SC-10	Das Informationssystem beendet die Netzwerkverbindung, die einer Kommunikationssitzung zugeordnet ist, wenn diese Sitzung beendet wurde oder nach einem durch die Organisation festgelegtem Inaktivitätszeitraum.
CCI-002449	SC-13	Die Organisation bestimmt die kryptographischen Nutzungen, die Art der Codierung, die für jede Nutzung erforderlich ist, die durch das Informationssystem umgesetzt werden soll.
CCI-002450	SC-13	Das Informationssystem führt die von der Organisation bestimmten kryptographischen Nutzungen und die Art der Codierung, die für jede Nutzung erforderlich ist, gemäß gültigen Bundesgesetzen, Durchführungsverordnungen, Richtlinien, Regelwerken, Vorschriften und Normen, durch.
CCI-001159	SC-17	Die Organisation gibt Public-Key-Zertifikate gemäß den von der Organisation festgelegten Zertifikatsvorschriften aus oder beschafft Public-Key-Zertifikate von zugelassenen Anbietern.
CCI-002456	SC-17	Die Organisation legt die Zertifikatsvorschriften fest, die für die Ausgabe von Public-Key-Zertifikaten eingesetzt werden.
CCI-001160	SC-18(a)	Die Organisation legt akzeptablen und inakzeptablen Mobilcode und Mobilcode-Technologien fest.
CCI-001161	SC-18(b)	Die Organisation führt Nutzungsbeschränkungen für akzeptablen Mobilcode und Mobilcode-Technologien ein.
CCI-001162	SC-18(b)	Die Organisation führt eine Richtlinie für die Umsetzung von akzeptablem Mobilcode und Mobilcode-Technologien ein.
CCI-001163	SC-18(c)	Die Organisation genehmigt die Nutzung von Mobilcode innerhalb des Informationssystems.
CCI-001164	SC-18(c)	Die Organisation überprüft die Nutzung von Mobilcode innerhalb des Informationssystems.
CCI-001165	SC-18(c)	Die Organisation kontrolliert die Nutzung von Mobilcode innerhalb des Informationssystems.
CCI-001184	SC-23	Das Informationssystem schützt die Authentizität der Kommunikationssitzungen.
CCI-001199	SC-28	Das Informationssystem schützt die Vertraulichkeit bzw. Integrität der durch die Organisation festgelegten inaktiven Informationen.
CCI-001233	SI-2(2)	Die Organisation nutzt automatische Mechanismen in einer von der Organisation festgelegten Häufigkeit zur Feststellung des Zustands der Informationssystemkomponenten mit Hinblick auf Fehlerbehebung.
CCI-001234	SI-2(2)	Die Organisation legt die Häufigkeit der Nutzung von automatischen Mechanismen zur Feststellung des Zustands der Informationssystemkomponenten mit Hinblick auf Fehlerbehebung fest.

Tabelle H-7 Zusätzliche Platform Enclave CCIs für Kontrollsysteme mit MITTLERER Auswirkung		
CCI #	800-53 Kontroll-text	Begriffserklärung CCI
CCI-001246	SI-3(1)	Die Organisation verwaltet Schadcode-Schutzmechanismen zentral.
CCI-001247	SI-3(2)	Das Informationssystem aktualisiert Schadcode-Schutzmechanismen automatisch.
CCI-001260	SI-4(2)	Die Organisation setzt automatische Tools zur Unterstützung der Echtzeit-Analyse von Ereignissen ein.
CCI-002659	SI-4(4)	Die Organisation legt die Häufigkeit mit der eingehende Kommunikation auf ungewöhnliche bzw. unzulässige Aktivitäten oder Zustände überwacht wird, fest.
CCI-002660	SI-4(4)	Die Organisation legt die Häufigkeit mit der ausgehende Kommunikation auf ungewöhnliche bzw. unzulässige Aktivitäten oder Zustände überwacht wird, fest.
CCI-002661	SI-4(4)	Das Informationssystem überwacht eingehenden Kommunikationsverkehr auf ungewöhnliche bzw. unzulässige Aktivitäten oder Zustände in der von der Organisation festgelegten Häufigkeit.
CCI-002662	SI-4(4)	Das Informationssystem überwacht ausgehenden Kommunikationsverkehr auf ungewöhnliche bzw. unzulässige Aktivitäten oder Zustände in der von der Organisation festgelegten Häufigkeit.
CCI-001264	SI-4(5)	Die Organisation legt Anzeichen von Gefährdungen oder möglichen Gefährdungen für die Sicherheit des Informationssystems fest, welche die Ausgabe von Informationssystemwarnungen an von der Organisation festgelegte Personen bzw. Rollen zur Folge haben.
CCI-002663	SI-4(5)	Die Organisation legt Personen bzw. Rollen fest, die Informationssystemwarnungen erhalten, wenn von der Organisation festgelegte Anzeichen von Gefährdungen oder möglichen Gefährdungen auftreten.
CCI-002664	SI-4(5)	Das Informationssystem alarmiert von der Organisation festgelegte Personen bzw. Rollen, wenn die von der Organisation festgelegten Gefährdungsanzeiger das Auftreten einer Gefährdung oder einer möglichen Gefährdung anzeigen.
CCI-002703	SI-7	Die Organisation legt die Software, Firmware und Informationen fest, die der Prüfung durch Integritäts-Nachweis-Tools unterliegen, um unbefugte Änderungen daran festzustellen.
CCI-002704	SI-7	Die Organisation setzt Integritäts-Nachweis-Tools ein, um unbefugte Änderungen an der von der Organisation festgelegten Software, Firmware und den Informationen festzustellen.
CCI-002705	SI-7(1)	Die Organisation legt die Software fest, bei der Integritätsprüfungen durchgeführt werden.
CCI-002706	SI-7(1)	Die Organisation legt die Firmware fest, bei der Integritätsprüfungen durchgeführt werden.
CCI-002707	SI-7(1)	Die Organisation legt die Informationen fest, bei denen Integritätsprüfungen durchgeführt werden.
CCI-002710	SI-7(1)	Das Informationssystem führt Integritätsprüfungen von durch die Organisation festgelegter Software beim Startup, bei durch die Organisation festgelegten Übertragungszuständen, sicherheitsrelevanten Vorkommnissen, oder mit einer durch die Organisation festgelegten Häufigkeit durch.
CCI-002711	SI-7(1)	Das Informationssystem führt Integritätsprüfungen von durch die Organisation festgelegter Firmware beim Startup, bei durch die Organisation festgelegten Übertragungszuständen, sicherheitsrelevanten Vorkommnissen, oder mit einer durch die Organisation festgelegten Häufigkeit durch.
CCI-002712	SI-7(1)	Das Informationssystem führt Integritätsprüfungen von durch die Organisation festgelegten Informationen beim Startup, bei durch die Organisation festgelegten Übertragungszuständen, sicherheitsrelevanten Vorkommnissen, oder mit einer durch die Organisation festgelegten Häufigkeit durch.

Tabelle H-7 Zusätzliche Platform Enclave CCI's für Kontrollsysteme mit MITTLERER Auswirkung		
CCI #	800-53 Kontroll-text	Begriffserklärung CCI
CCI-002708	SI-7(1)	Die Organisation legt die Übertragungszustände bzw. sicherheitsrelevanten Vorkommnisse fest, bei denen das Informationssystem eine Integritätsprüfung für Software, Firmware und Informationen durchführt.
CCI-002719	SI-7(7)	Die Organisation legt die unbefugten sicherheitsrelevanten Änderungen im Informationssystem fest, die in den Vorfallreaktionsplan der Organisation integriert werden müssen.
CCI-002720	SI-7(7)	Die Organisation integriert die Erkennung von unbefugten, von der Organisation festgelegten, sicherheitsrelevanten Änderungen im Informationssystem in den Vorfallreaktionsplan der Organisation.
CCI-002823	SI-16	Die Organisation legt die Sicherheitsmaßnahmen fest, die zum Schutz des Speichers des Informationssystems gegen unbefugte Code-Ausführung umzusetzen sind.
CCI-002824	SI-16	Das Informationssystem setzt von der Organisation festgelegte Sicherheitsmaßnahmen zum Schutz seines Speichers gegen unbefugte Code-Ausführung um.