IT Grundschutz Compliance on Amazon Web Services

Inhaltsverzeichnis

Inhaltsverzeichnis 2

Einleitung 3

Geteilte Verantwortung für die Sicherheit in einer Cloud-Umgebung und Ausrichtung am IT-Grundschutz-Schichtenmodell 4

Abschnitt 1 – Kundesicht 5

Beschreibung der zu modellierenden IT-Grundschutz Kataloge 5

Das IT-Grundschutz Rahmenwerk - Übersicht 5

Zu modellierende IT-Grundschutz Bausteine 6

Beschreibung der Bausteine, die durch den Kunden anzuwenden sind 12

Wie ist der Katalog B 1.11 Outsourcing umzusetzen? 16

Welche Bausteine müssen durch AWS geliefert werden? 17

Abschnitt 2 – AWS Sicht: 20

Beschreibung, was durch den Kunden bereitgestellt werden muss 20

Sicherheit **IN DER** Cloud 20

Wie können Anforderungen aus Bausteinen mit bestehenden AWS Zertifizierungen oder Maßnahmen abgedeckt werden 20

Sicherheit **DER** Cloud 20

Mapping der vorhandenen Zertifizierungen und Maßnahmen zu den Anforderungen der Grundschutz Bausteine 23

AWS Referenz Architekturen 45

Architekturübersicht und Anwendung der IT-Grundschutz Kataloge 45

Einleitung

Bei Amazon Web Services (AWS) handelt es sich um eine hochsichere Cloud-Plattform, die regelmäßigen Audits unterzogen wird und mit deren Hilfe Kunden die unterschiedlichsten Anforderungen hinsichtlich behördlicher Vorschriften und Best Practices zur Gewährleistung der Informations- und Datensicherheit erfüllen können. Dazu gehören unter anderem die IT-Grundschutz Standards und IT-Grundschutz Kataloge des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI).

Das vorliegende Whitepaper gibt Aufschluss darüber, wie die entsprechenden Vorgaben aus den BSI Standards 100-1 und 100-2[1] sowie die Vorgaben zur IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten[2] umgesetzt werden müssen, um eine bestehende Zertifizierung nicht zu gefährden bzw. eine angestrebte Zertifizierung problemlos umsetzen zu können, wenn AWS Cloud Plattform-Services innerhalb des ISMS genutzt werden sollen.

Kunden können die sichere globale Infrastruktur und die Dienstleistungen von AWS verwenden, um die Anforderungen eines ISMS nach ISO 27001 auf der Basis von IT-Grundschutz des BSI zu erfüllen. Das Verständnis des Modells der zwischen dem Kunden und AWS geteilten Verantwortung hierfür ist Voraussetzung für die effektive Verwaltung und den Betrieb einer sicheren Cloud Computing-Umgebung. Kunden können eine breite Palette von AWS-Sicherheitsfunktionen und Partnerprodukten nutzen, um die Einhaltung der relevanten Sicherheitsanforderungen zu ermöglichen. Die von AWS angewendeten Prozesse und Kontrollen können vom Kunden anhand von AWS-Zertifizierungen und Berichten, die in diesem Dokument referenziert sind, validiert werden. Die jeweiligen AWS-Compliance-Zertifizierungen und -Berichte können bei AWS individuell angefordert werden[3]. Weitere Informationen zu AWS-Compliance-Programmen sind ebenfalls auf den AWS Webseiten zu finden[4]. Die zudem durch AWS umgesetzten technischen und organisatorischen Informationssicherheits-Maßnahmen sind ebenfalls in diesem Dokument beschrieben.

Kunden, die bereits ein Informationssicherheits-Managementsystem (ISMS) betreiben oder sich im Aufbau von ISMS Strukturen befinden, können die sicheren Infrastrukturen von AWS problemlos in ihr eigenes ISMS integrieren und somit weiterhin in Einklang mit der Vorgehensweise und den Empfehlungen des IT-Grundschutzes stehen. Auch einer bestehenden oder angestrebten Zertifizierung des ISMS nach ISO 27001 auf der Basis von IT-Grundschutz steht somit nichts mehr im Wege. Hierfür ist es wichtig, dass sich jeder Kunde im Rahmen seines ISMS darüber bewusst ist, welche Prozesse und darin verarbeiteten und gespeicherten Informationen und Daten er aus seinem Unternehmen auslagert und wie diese angemessen zu schützen sind. Dazu sind neben den AWS Sicherheitsmaßnahmen noch eigene Maßnahmen auf Kundenseite zu etablieren und mit den Anforderungen des BSI IT-Grundschutzes abzugleichen. Diese und die durch AWS bereitgestellten Informationssicherheits-Maßnahmen müssen im eigenen Risikomanagementprozess auf ihre Angemessenheit hin überprüft und ggf. durch zusätzliche Maßnahmen des Kunden ergänzt werden.

Trotz vorhandener Informationssicherheits-Maßnahmen auf Seiten von AWS verbleit die endgültige Verantwortung für die korrekte und sichere Verarbeitung und Speicherung aller Daten und Informationen immer beim Kunden.

Hinweis: Sollten Kunden bereits eine bestehende Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz besitzen, so ist zu beachten, dass die Umstellung auf die Nutzung von AWS Cloud Plattform-Services eine Änderung im IT-Verbund der Zertifizierung bedeuten kann, die dem BSI gegenüber mitzuteilen ist.

Grundlegende Hinweise

Dieses Whitepaper wurde in Zusammenarbeit der TÜV TRUST IT GmbH Unternehmensgruppe TÜV Austria mit Amazon Webservices erstellt. Hierbei wurden die Anforderungen des BSI aus den folgenden Dokumenten berücksichtigt:

- BSI Standard 100-1: Managementsysteme für Informationssicherheit (ISMS), Version 1.5
- BSI Standard 100-2: IT-Grundschutz-Vorgehensweise, Version 2.0
- Vorgaben zur IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten, Version 1.0
- IT-Grundschutz-Kataloge 14. Ergänzungslieferung-2014

[1] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html
[2] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Zertifikat/Veroeffentl/Outsourcing_pdf.pdf?__blob=publicationFile
[3] Kontakt zu AWS über: https://aws.amazon.com/compliance/contact
[4] https://aws.amazon.com/compliance

Alle Informationen wurden dieses Whitepapers wurden basierend auf den genannten Anforderungen sowie den Informationen zu den bei AWS umgesetzten technischen und organisatorischen Maßnahmen nach bestem Wissen aufgrund der langjährigen Erfahrungen beider Unternehmen in der Informationssicherheit zusammengetragen. Dieses Whitepaper bietet eine Orientierungshilfe aber trotz aller Sorgfalt keine Garantie dafür, dass Kunden eine Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz ohne eventuelle Nachbesserungen oder Nachforderungen durchlaufen, da die Kundenanforderungen je nach Schutzbedarf und Kritikalität ihrer Services sowie der Informationen und Daten sehr unterschiedlich ausfallen können.

Es wird in jedem Fall empfohlen, einen geplanten IT-Verbund sowie Modellierungsfragen vor Antragstellung mit dem BSI abzustimmen. Sofern Kunden bereits eine Zertifizierung umgesetzt haben, sollte vor der Umsetzung des Outsourcing Vorhabens mit dem BSI geklärt werden, welche Auswirkungen auf die bestehende Zertifizierung zu erwarten sind.

Geteilte Verantwortung für die Sicherheit in einer Cloud-Umgebung

Wie bei jedem Outsourcing Dienstleister führt die Verwendung von AWS zu einem Modell geteilter Verantwortung hinsichtlich des Einsatzes und der Steuerung von Informationssicherheits-Maßnahmen. Dieses Modell kann den Kunden von AWS einen Teil der Arbeit abnehmen, denn sie und AWS teilen sich die Verantwortung für Informationssicherheits-Maßnahmen. Bei Sicherheitsmaßnahmen kann es sich um geteilte, vererbte oder duale Maßnahmen handeln.

Bei der Erfüllung der Informationssicherheits-Anforderungen im Cloud Computing muss zwischen der Compliance der Cloud-Lösung selbst und der Nutzung der Cloud-Lösung durch den Kunden unterschieden werden. "Sicherheit **DER** Cloud" bezieht sich auf die Compliance-Pläne und -Maßnahmen, die der Cloud Service Provider (AWS) innerhalb der AWS-Infrastruktur implementiert. "Sicherheit **IN DER** Cloud" bezieht sich auf die Implementierung von Informationssicherheits-Maßnahmen im Zusammenhang mit den Abläufen und Prozessen, die in dieser AWS-Infrastruktur ausgeführt werden inkl. der darin verarbeiteten Daten und Informationen.

Abschnitt 1 – Kundesicht

Beschreibung der zu modellierenden IT-Grundschutz Kataloge

Das IT-Grundschutz Rahmenwerk - Übersicht

Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) hat ein Programm entwickelt, das Unternehmen die notwendige Methodik an die Hand gibt, um effektive Informationssicherheits-Prozesse zu schaffen. Die IT-Grundschutz-Methodik stützt sich dabei auf vier Standards, die organisatorische Hinweise zum Aufbau eines Informationssicherheits-Managementsystems (ISMS), die empfohlene Vorgehensweise zur Implementierung und Bewertung des IT-Grundschutzes, Informationen zur Durchführung einer Risikoanalyse anhand der IT-Grundschutzanforderungen und schließlich Informationen zur Entwicklung eines Plans zum Notfallmanagement umfassen. Gestützt wird diese Methodik durch die IT-Grundschutzkataloge, die technische und organisatorische Maßnahmen zum Schutz vor den wichtigsten Gefährdungen der Informations- und Datensicherheit enthalten. Die folgende Abbildung gibt Aufschluss über die Strukturen des IT-Grundschutz Rahmenwerkes:

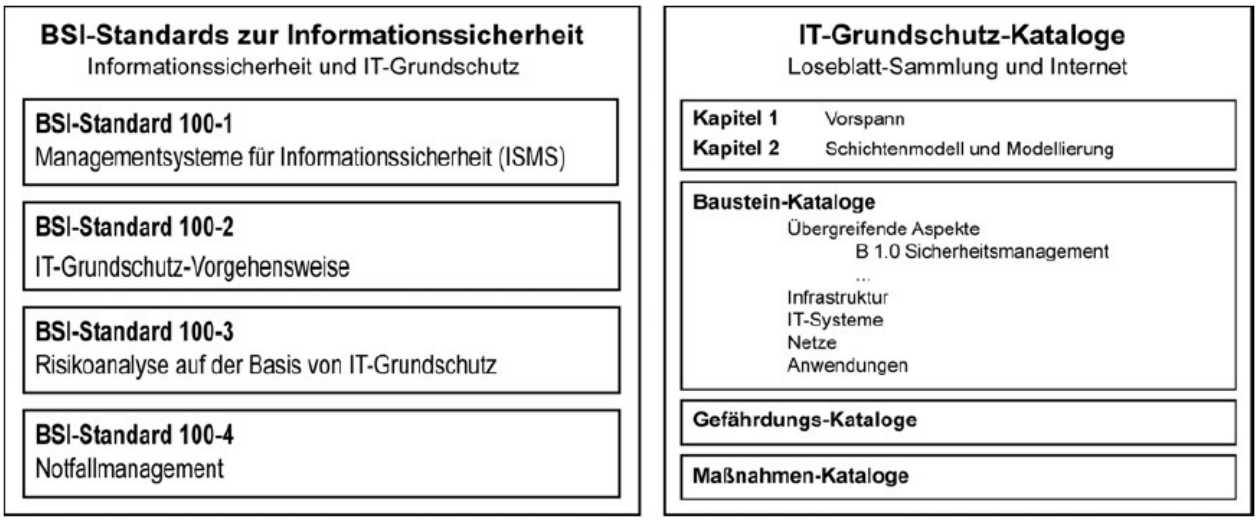

Abbildung 1: Übersicht BSI Standards und IT-Grundschutzkataloge[5]

Der Standard „100-1 Managementsysteme für Informationssicherheit (ISMS)“ definiert allgemeine Anforderungen an ein ISMS. Er ist vollständig kompatibel zum ISO-Standard 27001 und berücksichtigt weiterhin die Empfehlungen der ISO-Standards 27000 und 27002[6].

Der Standard „100-2 IT-Grundschutz-Vorgehensweise“ interpretiert die sehr allgemein gehaltenen Anforderungen der zuvor genannten ISO-Standards 27000, 27001 und 27002 und hilft den Anwendern in der Praxis bei der Umsetzung mit vielen Hinweisen, Hintergrund-Informationen und Beispielen[7].

Zur Umsetzung dieser Standards und zur Festlegung der für das ISMS relevanten Maßnahmen zur Sicherung der Informations- und Datensicherheit wird in der Grundschutz-Vorgehensweise die Methodik der Modellierung von Bausteinen beschrieben. Hierin muss der zuvor definierte IT-Verbund mit den durch das BSI zur Verfügung gestellten Bausteinen nachgebildet, also modelliert werden. Die jeweiligen Bausteine sind in 5 Schichten eingeteilt.

[5] Quelle: BSI Standard 100-1: Managementsysteme für Informationssicherheit (ISMS), Version 1.5, Seite 10
[6] Quelle: BSI Standard 100-1: Managementsysteme für Informationssicherheit (ISMS), Version 1.5, Seite 10 Absatz 3
[7] Quelle: BSI Standard 100-1: Managementsysteme für Informationssicherheit (ISMS), Version 1.5, Seite 11 Absatz 2

Diese Schichten lauten:

- Schicht 1: Übergreifende Aspekte
- Schicht 2: Infrastruktur
- Schicht 3: IT-Systeme
- Schicht 4: Netze
- Schicht 5: Anwendungen

Die jeweiligen Modellierungsregeln geben Aufschluss darüber, wie die vorhandenen Bausteine mit ihren zugehörigen Maßnahmen im IT-Verbund modelliert werden müssen[8]. Die Modellierung erfolgt in Abhängigkeit der eingesetzten Produkte, Technologien und vorhandener Prozesse sowie unter Berücksichtigung von Outsourcing Maßnahmen innerhalb der Organisation.

Das vorliegende Dokument beschreibt die zu modellierenden IT-Grundschutz Bausteine in Abhängigkeit der durch AWS angebotenen Services und der hierin genutzten Technologien. Hierin sind die „Vorgaben zur IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten“ bereits berücksichtigt.

Zu modellierende IT-Grundschutz Bausteine

Die zu modellierenden Bausteine basieren auf dem definierten IT-Verbund der Organisation. Bei einem Outsourcing von Dienstleistungen zu AWS müssen bei der Modellierung Vorgaben beachtet werden, die in den „Vorgaben zur IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten“ beschrieben sind. Diese bieten in der Version 1.0 verbindlich Regelungen bei komplett oder teilweise ausgelagerten Komponenten oder Services, da sich diese zumindest in Teilen nicht unter Kontrolle des Kunden sondern im Verantwortungsbereich von AWS befinden.

Generell gilt, dass ein Outsourcing von Komponenten oder Services für eine Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz nur dann relevant ist, wenn die folgenden Bedingungen[9] erfüllt sind:

- IT-Systeme, Anwendungen oder Geschäftsprozesse werden zu einem externen Dienstleister ausgelagert, und
- die Bindung an den Dienstleister erfolgt auf längere Zeit, und
- durch die Dienstleistung kann die Informationssicherheit des Auftraggebers beeinflusst werden, und
- im Rahmen der Dienstleistungen erbringt der Dienstleister auch regelmäßig nennenswerte Tätigkeiten im Bereich Informationssicherheitsmanagement.

Die Erbringung „nennenswerter Tätigkeiten im Bereich Informationssicherheitsmanagement“ umfasst hierbei bereits Tätigkeiten, wie z. B. Verschlüsselungsdienstleistungen, das zur Verfügung stellen ausfallsicherer Anbindungen oder Services sowie die Durchführung sicherheitsrelevanter Konfigurationen etc.

Die Modellierung der entsprechenden Bausteine bezieht sich auf die Nutzung eines oder aller der drei folgenden Anwendungsszenarien bei AWS:

- AWS Fault Tolerance & High Availability (Fault Tolerance HA services)
- AWS Financial Services Grid Computing (FS Grid Computing)
- AWS Web Application Hosting (Web App Hosting)

[8] Nähere Informationen zur korrekten Modellierung: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/allgemein/modellierung/02001.html
[9] Quelle: IT-Grundschutz-Kataloge 14. Ergänzungslieferung-2014, Kap. 2.1

Berücksichtigt werden bei der Modellierung die in den jeweils zugehörigen Architektur-Übersichten dargestellten Services und Technologien. Auf weitere im IT-Verbund des Kunden zu modellierende Bausteine kann an dieser Stelle nicht referenziert werden, da die Kundenumgebungen nicht bekannt sind. Die durch den Kunden zusätzlich für das AWS Outsourcing zu modellierenden Bausteine sind in der folgenden Tabelle dokumentiert[10].

Die jeweils mit „X“ markierten Bausteine sollten gemäß den Vorgaben modelliert werden. Bei Bausteinen, die mit „(X)“ markiert sind, empfiehlt sich eine Modellierung in Abhängigkeit der Kundenanforderungen, der eingesetzten Produkte sowie den verarbeiteten und gespeicherten Daten und Informationen.

Baustein ID	Titel	Modellierung			
		Übergreifende Anwendung[11]	Fault Tolerance HA services[12]	FS Grid Computing	Web App Hosting
B 1 Übergreifende Aspekte					
B 1.0	Sicherheitsmanagement	X			
B 1.1	Organisation	X			
B 1.2	Personal	X			
B 1.3	Notfallmanagement	X			
B 1.4	Datensicherungskonzept		X	X	X
B 1.5	Datenschutz[13]		(X)	(X)	(X)
B 1.6	Schutz vor Schadprogrammen		X	X	X
B 1.7	Kryptokonzept[14]		(X)	(X)	(X)
B 1.8	Behandlung von Sicherheitsvorfällen	X			
B 1.9	Hard- und Software-Management	X			
B 1.10	Standardsoftware		X	X	X
B 1.11	Outsourcing		X	X	X
B 1.12	Archivierung			X	
B 1.13	Sensibilisierung und Schulung zur Informationssicherheit				
B 1.14	Patch- und Änderungsmanagement		X	X	X
B 1.15	Löschen und Vernichten von Daten		X	X	X
B 1.16	Anforderungsmanagement		X	X	X
B 1.17	Cloud-Nutzung		X	X	X
B 2 Infrastruktur					
B 2.1	Allgemeines Gebäude		X	X	X
B 2.2	Elektrotechnische Verkabelung		X	X	X
B 2.3	Büroraum / Lokaler Arbeitsplatz				
B 2.4	Serverraum				
B 2.5	Datenträgerarchiv				
B 2.6	Raum für technische Infrastruktur				
B 2.7	Schutzschränke				
B 2.8	Häuslicher Arbeitsplatz				
B 2.9	Rechenzentrum		X	X	X

[10] Die gelisteten Bausteine beziehen sich auf die 14. Ergänzungslieferung der BSI IT-Grundschutzkataloge (14.EL - 2014)
[11] Die Auswahl dieser Bausteine erfolgte aufgrund der Regelungen im Dokument „Vorgaben zur IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten“, die Bausteine sind bei Kunde und AWS immer getrennt anzuwenden
[12] Die Auswahl dieser Bausteine erfolgte aufgrund der verwendeten Technologien in den Anwendungsszenarien „Fault Tolerance HA services“, „FS Grid Computing“ und „Web App Hosting“
[13] In Abhängigkeit der Verarbeitung personenbezogener Daten
[14] In Abhängigkeit der Vertraulichkeit der verarbeiteten Daten

Baustein ID	Titel	Modellierung			
		Übergreifende Anwendung[11]	Fault Tolerance HA services[12]	FS Grid Computing	Web App Hosting
B 2.10	Mobiler Arbeitsplatz				
B 2.11	Besprechungs-, Veranstaltungs- und Schulungsräume				
B 2.12	IT-Verkabelung		X	X	X
B 3 IT-Systeme					
B 3.101	Allgemeiner Server		X	X	X
B 3.102	Server unter Unix[15]		(X)	(X)	(X)
B 3.103	*Server unter Windows NT - **entfallen***	*-/-*	*-/-*	*-/-*	*-/-*
B 3.104	*Server unter Novell Netware 3.x - **entfallen***	*-/-*	*-/-*	*-/-*	*-/-*
B 3.105	*Server unter Novell Netware Version 4.x - **entfallen***	*-/-*	*-/-*	*-/-*	*-/-*
B 3.106	*Server unter Windows 2000 - **entfallen***	*-/-*	*-/-*	*-/-*	*-/-*
B 3.107	S/390- und zSeries-Mainframe				
B 3.108	Windows Server 2003[16]		(X)	(X)	(X)
B 3.109	Windows Server 2008[17]		(X)	(X)	(X)
B 3.201	Allgemeiner Client				
B 3.202	Allgemeines nicht vernetztes IT-System				
B 3.203	Laptop				
B 3.204	Client unter Unix				
B 3.205	*Client unter Windows NT - **entfallen***	*-/-*	*-/-*	*-/-*	*-/-*
B 3.206	*Client unter Windows 95 - **entfallen***	*-/-*	*-/-*	*-/-*	*-/-*
B 3.207	*Client unter Windows 2000 - **entfallen***	*-/-*	*-/-*	*-/-*	*-/-*
B 3.208	Internet-PC				
B 3.209	Client unter Windows XP				
B 3.210	Client unter Windows Vista				
B 3.211	Client unter Mac OS X				
B 3.212	Client unter Windows 7				
B 3.301	Sicherheitsgateway (Firewall)				
B 3.302	Router und Switches		X	X	X
B 3.303	Speicherlösungen / Cloud Storage		X	X	X
B 3.304	Virtualisierung		X	X	X
B 3.305	Terminalserver				
B 3.401	TK-Anlage				
B 3.402	Faxgerät				
B 3.403	*Anrufbeantworter - **entfallen***	*-/-*	*-/-*	*-/-*	*-/-*
B 3.404	Mobiltelefon				
B 3.405	Smartphones, Tablets und PDAs				
B 3.406	Drucker, Kopierer und Multifunktionsgeräte				

[15] In Abhängigkeit des in der Cloud betriebenen Betriebssystems
[16] In Abhängigkeit des in der Cloud betriebenen Betriebssystems
[17] In Abhängigkeit des in der Cloud betriebenen Betriebssystems

Baustein ID	Titel	Modellierung			
		Übergreifende Anwendung[11]	Fault Tolerance HA services[12]	FS Grid Computing	Web App Hosting
B 4 Netze					
B 4.1	Heterogene Netze		X	X	X
B 4.2	Netz- und Systemmanagement				
B 4.3	Modem				
B 4.4	VPN[18]			(X)	
B 4.5	LAN-Anbindung eines IT-Systems über ISDN				
B 4.6	WLAN				
B 4.7	VoIP				
B 4.8	Bluetooth				
B 5 Anwendungen					
B 5.1	*Peer-to-Peer-Dienste - **entfallen***	*-/-*	*-/-*	*-/-*	*-/-*
B 5.2	Datenträgeraustausch				
B 5.3	Groupware[19]		(X)	(X)	(X)
B 5.4	Webserver		X	X	X
B 5.5	Lotus Notes / Domino[20]		(X)	(X)	(X)
B 5.6	Faxserver				
B 5.7	Datenbanken			X	X
B 5.8	Telearbeit				
B 5.9	Novell eDirectory				
B 5.10	*Internet Information Server - **entfallen***	*-/-*	*-/-*	*-/-*	*-/-*
B 5.11	*Apache Webserver - **entfallen***	*-/-*	*-/-*	*-/-*	*-/-*
B 5.12	Microsoft Exchange/Outlook[21]		(X)	(X)	(X)
B 5.13	SAP System				
B 5.14	Mobile Datenträger				
B 5.15	Allgemeiner Verzeichnisdienst[22]		(X)	(X)	(X)
B 5.16	Active Directory[23]		(X)	(X)	(X)
B 5.17	Samba				
B 5.18	DNS-Server[24]		(X)	(X)	X
B 5.19	Internet-Nutzung				
B 5.20	OpenLDAP[25]		(X)	(X)	(X)
B 5.21	Webanwendungen		X	X	X
B 5.22	Protokollierung		X	X	X
B 5.23	Cloud Management		X	X	X
B 5.24	Web-Services		X	X	X
B 5.25	Allgemeine Anwendungen		X	X	X

[18] In Abhängigkeit der Anbindung des Kunden an AWS
[19] In Abhängigkeit der bei AWS betriebenen Services
[20] In Abhängigkeit der bei AWS betriebenen Services
[21] In Abhängigkeit der bei AWS betriebenen Services
[22] In Abhängigkeit der bei AWS genutzten Technologie
[23] In Abhängigkeit der bei AWS genutzten Technologie
[24] In Abhängigkeit der bei AWS genutzten Technologie
[25] In Abhängigkeit der bei AWS genutzten Technologie

Wichtig: In Abhängigkeit der Schutzbedarfsanalyse des Kunden kann es erforderlich sein, weitere Bausteine zu modellieren oder eigene Bausteine zu entwickeln, um weiterführende Sicherheitsmaßnahmen zu etablieren. Dies kann dann erforderlich werden, wenn ein hoher oder sehr hoher Schutzbedarf vorliegt, besondere Einsatzbedingungen existieren oder wenn genutzte Komponenten nicht mit den vorhandenen Bausteinen der BSI IT-Grundschutz Kataloge modelliert werden können[26].

[26] Quelle: BSI Standard 100-2, Version 2.0, Seite 38, Kap. „Weiterführende Sicherheitsmaßnahmen“

Beschreibung der Bausteine, die durch den Kunden anzuwenden sind

Die in der nachfolgenden Tabelle dargestellten Bausteine sind gemäß den Informationen aus Kapitel „Zu modellierende IT-Grundschutz Bausteine“ durch den Kunden anzuwenden.

Die jeweils mit „X“ markierten Bausteine sollten gemäß den Vorgaben modelliert werden. Bei Bausteinen, die mit „(X)“ markiert sind, empfiehlt sich eine Modellierung in Abhängigkeit der Kundenanforderungen, der eingesetzten Produkte sowie den verarbeiteten und gespeicherten Daten und Informationen.

Baustein ID	Titel	Anwendung durch Kunden	Zusatzinformation / Bemerkung
B 1 Übergreifende Aspekte			
B 1.0	Sicherheitsmanagement	X	Dieser Baustein ist laut „Vorgaben zur IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten“ für Auftraggeber und Dienstleister immer getrennt anzuwenden.
B 1.1	Organisation	X	Dieser Baustein ist laut „Vorgaben zur IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten“ für Auftraggeber und Dienstleister immer getrennt anzuwenden.
B 1.2	Personal	X	Dieser Baustein ist laut „Vorgaben zur IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten“ für Auftraggeber und Dienstleister immer getrennt anzuwenden.
B 1.3	Notfallmanagement	X	Dieser Baustein ist laut „Vorgaben zur IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten“ für Auftraggeber und Dienstleister immer getrennt anzuwenden.
B 1.4	Datensicherungskonzept	X	Die Kunden sind für ihre Daten und Informationen verantwortlich und müssen angemessene Maßnahmen zur Datensicherung in Einklang mit ihren Sicherheitsrichtlinien umsetzen.
B 1.5	Datenschutz[27]	(X)	Die Kunden sind für ihre Daten und Informationen verantwortlich und müssen angemessene Maßnahmen zum Datenschutz in Einklang mit ihren Sicherheitsrichtlinien umsetzen.
B 1.6	Schutz vor Schadprogrammen	X	Die Kunden sind für ihre Daten und Informationen verantwortlich und müssen angemessene Maßnahmen zum Schutz vor Schadprogrammen in Einklang mit ihren Sicherheitsrichtlinien umsetzen.
B 1.7	Kryptokonzept[28]	(X)	Die Kunden sind für ihre Daten und Informationen verantwortlich und müssen angemessene Krypto-Maßnahmen in Einklang mit ihren Sicherheitsrichtlinien umsetzen.
B 1.8	Behandlung von Sicherheitsvorfällen	X	Dieser Baustein ist laut „Vorgaben zur IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten“ für Auftraggeber und Dienstleister immer getrennt anzuwenden.
B 1.9	Hard- und Software-Management	X	Dieser Baustein ist laut „Vorgaben zur IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten“ für Auftraggeber und Dienstleister immer getrennt anzuwenden.

[27] In Abhängigkeit der Verarbeitung personenbezogener Daten
[28] In Abhängigkeit der Vertraulichkeit der verarbeiteten Daten

Baustein ID	Titel	Anwendung durch Kunden	Zusatzinformation / Bemerkung
B 1.10	Standardsoftware	X	Die Kunden sind für die Evaluierung von Standardsoftware verantwortlich. Innerhalb der AWS Umgebung wird keine Standardsoftware eingesetzt.
B 1.11	Outsourcing	X	Die Kunden sind für ihre Daten und Informationen verantwortlich und müssen angemessene Maßnahmen zum Outsourcing in Einklang mit ihren Sicherheitsrichtlinien umsetzen.
B 1.12	Archivierung	X	Die Kunden sind für ihre Daten und Informationen verantwortlich und müssen angemessene Maßnahmen zur Archivierung in Einklang mit ihren Sicherheitsrichtlinien umsetzen.
B 1.14	Patch- und Änderungsmanagement	X	Die Kunden sind für ihre Daten und Informationen verantwortlich und müssen angemessene Maßnahmen zum Patch- und Änderungsmanagement in Einklang mit ihren Sicherheitsrichtlinien umsetzen.
B 1.15	Löschen und Vernichten von Daten	X	Die Kunden sind für ihre Daten und Informationen verantwortlich und müssen angemessene Maßnahmen zum Löschen und Vernichten von Daten in Einklang mit ihren Sicherheitsrichtlinien umsetzen.
B 1.16	Anforderungsmanagement	X	Die Kunden sind für ihre Daten und Informationen verantwortlich und müssen angemessene Maßnahmen zum Anforderungsmanagement in Einklang mit ihren Sicherheitsrichtlinien umsetzen.
B 1.17	Cloud-Nutzung	X	Die Kunden sind für ihre Daten und Informationen verantwortlich und müssen angemessene Maßnahmen zur Cloud Nutzung in Einklang mit ihren Sicherheitsrichtlinien umsetzen.
B 3 IT-Systeme			
B 3.101	Allgemeiner Server	X	Die Kunden sind für ihre Daten und Informationen verantwortlich und müssen angemessene Maßnahmen zum allgemeinen Server in Einklang mit ihren Sicherheitsrichtlinien umsetzen.
B 3.102	Server unter Unix[29]	(X)	Die Kunden sind für ihre Daten und Informationen verantwortlich und müssen angemessene Maßnahmen zum Server unter Unix in Einklang mit ihren Sicherheitsrichtlinien umsetzen.
B 3.108	Windows Server 2003[30]	(X)	Die Kunden sind für ihre Daten und Informationen verantwortlich und müssen angemessene Maßnahmen zum Windows Server 2003 in Einklang mit ihren Sicherheitsrichtlinien umsetzen.
B 3.109	Windows Server 2008[31]	(X)	Die Kunden sind für ihre Daten und Informationen verantwortlich und müssen angemessene Maßnahmen zum Windows Server 2008 in Einklang mit ihren Sicherheitsrichtlinien umsetzen.
B 3.302	Router und Switches	X	Die Kunden sind für ihre Daten und Informationen verantwortlich und müssen angemessene Maßnahmen zu Routern und Switches in Einklang mit ihren Sicherheitsrichtlinien umsetzen.

[29] In Abhängigkeit des in der Cloud betriebenen Betriebssystems
[30] In Abhängigkeit des in der Cloud betriebenen Betriebssystems
[31] In Abhängigkeit des in der Cloud betriebenen Betriebssystems

Baustein ID	Titel	Anwendung durch Kunden	Zusatzinformation / Bemerkung
B 3.303	Speicherlösungen / Cloud Storage	X	Die Kunden sind für ihre Daten und Informationen verantwortlich und müssen angemessene Maßnahmen zu Speicherlösungen / Cloud Storage in Einklang mit ihren Sicherheitsrichtlinien umsetzen.
B 3.304	Virtualisierung	X	Die Kunden sind für ihre Daten und Informationen verantwortlich und müssen angemessene Maßnahmen zur Virtualisierung in Einklang mit ihren Sicherheitsrichtlinien umsetzen.
B 4 Netze			
B 4.1	Heterogene Netze	X	Die Kunden sind für ihre Daten und Informationen verantwortlich und müssen angemessene Maßnahmen zu heterogenen Netzen in Einklang mit ihren Sicherheitsrichtlinien umsetzen.
B 4.4	VPN[32]	(X)	Die Kunden sind für ihre Daten und Informationen verantwortlich und müssen angemessene Maßnahmen zu VPNs in Einklang mit ihren Sicherheitsrichtlinien umsetzen.
B 5 Anwendungen			
B 5.3	Groupware[33]	(X)	Die Kunden sind für ihre Daten und Informationen verantwortlich und müssen angemessene Maßnahmen zu Groupware in Einklang mit ihren Sicherheitsrichtlinien umsetzen.
B 5.4	Webserver	X	Die Kunden sind für ihre Daten und Informationen verantwortlich und müssen angemessene Maßnahmen zu Webservern in Einklang mit ihren Sicherheitsrichtlinien umsetzen.
B 5.5	Lotus Notes / Domino[34]	(X)	Die Kunden sind für ihre Daten und Informationen verantwortlich und müssen angemessene Maßnahmen zu Lotus Notes / Domino in Einklang mit ihren Sicherheitsrichtlinien umsetzen.
B 5.7	Datenbanken	X	Die Kunden sind für ihre Daten und Informationen verantwortlich und müssen angemessene Maßnahmen zu Datenbanken in Einklang mit ihren Sicherheitsrichtlinien umsetzen.
B 5.12	Microsoft Exchange/Outlook[35]	(X)	Die Kunden sind für ihre Daten und Informationen verantwortlich und müssen angemessene Maßnahmen zu Microsoft Exchange/Outlook in Einklang mit ihren Sicherheitsrichtlinien umsetzen.
B 5.15	Allgemeiner Verzeichnisdienst[36]	(X)	Die Kunden sind für ihre Daten und Informationen verantwortlich und müssen angemessene Maßnahmen zum allgemeinen Verzeichnisdienst in Einklang mit ihren Sicherheitsrichtlinien umsetzen.
B 5.16	Active Directory[37]	(X)	Die Kunden sind für ihre Daten und Informationen verantwortlich und müssen angemessene Maßnahmen zum Active Directory in Einklang mit ihren Sicherheitsrichtlinien umsetzen.

[32] In Abhängigkeit der Anbindung des Kunden an AWS
[33] In Abhängigkeit der bei AWS betriebenen Services
[34] In Abhängigkeit der bei AWS betriebenen Services
[35] In Abhängigkeit der bei AWS betriebenen Services
[36] In Abhängigkeit der bei AWS genutzten Technologie
[37] In Abhängigkeit der bei AWS genutzten Technologie

Baustein ID	Titel	Anwendung durch Kunden	Zusatzinformation / Bemerkung
B 5.18	DNS-Server[38]	X	Die Kunden sind für ihre Daten und Informationen verantwortlich und müssen angemessene Maßnahmen zum DNS Server in Einklang mit ihren Sicherheitsrichtlinien umsetzen.
B 5.20	OpenLDAP[39]	(X)	Die Kunden sind für ihre Daten und Informationen verantwortlich und müssen angemessene Maßnahmen zu OpenLDAP in Einklang mit ihren Sicherheitsrichtlinien umsetzen.
B 5.21	Webanwendungen	X	Die Kunden sind für ihre Daten und Informationen verantwortlich und müssen angemessene Maßnahmen zu Webanwendungen in Einklang mit ihren Sicherheitsrichtlinien umsetzen.
B 5.22	Protokollierung	X	Die Kunden sind für ihre Daten und Informationen verantwortlich und müssen angemessene Maßnahmen zur Protokollierung in Einklang mit ihren Sicherheitsrichtlinien umsetzen.
B 5.24	Web-Services	X	Die Kunden sind für ihre Daten und Informationen verantwortlich und müssen angemessene Maßnahmen zu Web-Services in Einklang mit ihren Sicherheitsrichtlinien umsetzen.
B 5.25	Allgemeine Anwendungen	X	Die Kunden sind für ihre Daten und Informationen verantwortlich und müssen angemessene Maßnahmen zu allgemeinen Anwendungen in Einklang mit ihren Sicherheitsrichtlinien umsetzen.

Wichtig: In Abhängigkeit der Schutzbedarfsanalyse des Kunden kann es erforderlich sein, weitere Bausteine zu modellieren oder eigene Bausteine zu entwickeln, um weiterführende Sicherheitsmaßnahmen zu etablieren. Dies kann dann erforderlich werden, wenn ein hoher oder sehr hoher Schutzbedarf vorliegt, besondere Einsatzbedingungen existieren oder wenn genutzte Komponenten nicht mit den vorhandenen Bausteinen der BSI IT-Grundschutz Kataloge modelliert werden können[40].

[38] In Abhängigkeit der bei AWS genutzten Technologie
[39] In Abhängigkeit der bei AWS genutzten Technologie
[40] Quelle: BSI Standard 100-2, Version 2.0, Seite 38, Kap. „Weiterführende Sicherheitsmaßnahmen“

Wie ist der Katalog B 1.11 Outsourcing umzusetzen?

Sollte das Outsourcing aufgrund der Einstufung nach den im Kapitel „Zu modellierende IT-Grundschutz Bausteine“ genannten Kriterien für eine Zertifizierung relevant sein, so gelten die folgenden Regelungen zur Anwendung des Bausteins „B 1.11 Outsourcing“:

- Fall 1: Outsourcing stellt eine unbedeutende Gefährdung für den Untersuchungsgegenstand dar:

  Die Empfehlungen des Outsourcing-Bausteins sind in diesem Fall optional

- Fall 2: Ausgelagerte Komponenten sind bedeutenden Gefährdungen ausgesetzt:

  Der Baustein Outsourcing ist in diesem Fall anzuwenden

- Fall 3: Begrenztes Schadensausmaß (Sonderfall):

  Der Baustein Outsourcing ist in diesem Fall anzuwenden

- Fall 4: Der Outsourcing-Dienstleister verfügt über ein IT-Grundschutz-Zertifikat:

  Der Baustein Outsourcing ist in diesem Fall anzuwenden

Im weiteren Verlauf des vorliegenden Dokumentes wird davon ausgegangen, dass eine Zertifizierungsrelevanz vorliegt und der Baustein „B 1.11 Outsourcing“ gemäß dem oben beschriebenen Fall 2 umzusetzen ist[41]. Die Definition, dass die ausgelagerten Komponenten „bedeutenden Gefährdungen ausgesetzt sind“ bedeutet, dass Komponenten des ausgelagerten IT-Verbunds hohen oder sogar sehr hohen Schutzbedarf haben oder wesentliche Teile des IT-Verbunds ausgelagert sind[42].

Wie in allen Bausteinen der IT-Grundschutz Kataloge hat das BSI innerhalb des Bausteins „B 1.11 Outsourcing“ die wesentlichen Gefährdungen für ein Outsourcing Vorhaben bereits betrachtet, die je nach Kritikalität der ausgelagerten Systeme oder Services sehr vielschichtig sein können. Hierbei wird zwischen physikalischen, technischen und auch menschlichen Aspekten unterschieden. Die abgeleiteten Maßnahmen zur Planung und Umsetzung eines Outsourcing Vorhabens unterteilen sich in die folgenden 7 Phasen[43]:

- Phase 1: Strategische Planung des Outsourcing-Vorhabens
- Phase 2: Definition der wesentlichen Sicherheitsanforderungen
- Phase 3: Auswahl des Outsourcing-Dienstleisters
- Phase 4: Vertragsgestaltung
- Phase 5: Erstellung eines Sicherheitskonzepts für den ausgelagerten Informationsverbund
- Phase 6: Migrationsphase
- Phase 7: Planung und Sicherstellen des laufenden Betriebs

Gemäß der im BSI Standard 100-2 genannten Vorgehensweise müssen für die Erlangung und Aufrechterhaltung einer Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz alle im aktuellen Baustein genannten Maßnahmen der Qualifizierungsstufen A (Einstieg), B (Aufbau) und C (Zertifikat) auf ihre Umsetzung hin überprüft und bewertet werden. Die vorhandene Maßnahme „M 3.33 Sicherheitsüberprüfung von Mitarbeitern“ ist in die Qualifizierungsstufe Z (Zusätzlich) eingestuft und wird üblicherweise erst herangezogen, wenn hohe oder sehr hohe Schutzanforderungen an die ausgelagerten Services oder Prozesse ermittelt werden[44].

[41] Weitere Details zu den möglichen Umsetzungsszenarien können dem Dokument „Vorgaben zur IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten“ entnommen werden.
[42] Quelle: „Vorgaben zur IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten“, Version 1, Seite 3, 2. Fall
[43] Quelle: BSI IT-Grundschutz Kataloge, 14. EL – 2014, Seite 143, Kapitel B 1.11 Outsourcing
[44] Weitere Informationen zu den Qualifizierungsstufen der Maßnahmen finden sich im BSI Standard 100-2

Welche Bausteine müssen durch AWS geliefert werden?

Für den Fall, dass Aufgaben vollständig auf AWS ausgelagert werden, ist die Umsetzung der betreffenden Bausteine für den Kunden entbehrlich. Die in der nachfolgenden Tabelle dargestellten Bausteine sind gemäß der Informationen aus Kapitel „Zu modellierende IT-Grundschutz Bausteine“ durch AWS zu liefern.

Die jeweils mit „X“ markierten Bausteine sollten gemäß den Vorgaben modelliert werden. Bei Bausteinen, die mit „(X)“ markiert sind, empfiehlt sich eine Modellierung in Abhängigkeit der Kundenanforderungen, der eingesetzten Produkte sowie den verarbeiteten und gespeicherten Daten und Informationen.

Baustein ID	Titel	Anwendung durch AWS	Zusatzinformation / Bemerkung
B 1 Übergreifende Aspekte			
B 1.0	Sicherheitsmanagement	X	Dieser Baustein ist laut „Vorgaben zur IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten“ für Auftraggeber und Dienstleister immer getrennt anzuwenden. *Siehe AWS Ausrichtung nach BSI IT-Grundschutz, Behandlung von Risiken und Maßnahmen Abschnitt B 1.0.*
B 1.1	Organisation	X	Dieser Baustein ist laut „Vorgaben zur IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten“ für Auftraggeber und Dienstleister immer getrennt anzuwenden. *Siehe AWS Ausrichtung nach BSI IT-Grundschutz, Behandlung von Risiken und Maßnahmen Abschnitt B 1.1.*
B 1.2	Personal	X	Dieser Baustein ist laut „Vorgaben zur IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten“ für Auftraggeber und Dienstleister immer getrennt anzuwenden. *Siehe AWS Ausrichtung nach BSI IT-Grundschutz, Behandlung von Risiken und Maßnahmen Abschnitt B 1.2.*
B 1.3	Notfallmanagement	X	Dieser Baustein ist laut „Vorgaben zur IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten“ für Auftraggeber und Dienstleister immer getrennt anzuwenden. *Siehe AWS Ausrichtung nach BSI IT-Grundschutz, Behandlung von Risiken und Maßnahmen Abschnitt B 1.3*
B 1.6	Schutz vor Schadprogrammen	X	*Siehe AWS Ausrichtung nach BSI IT-Grundschutz, Behandlung von Risiken und Maßnahmen Abschnitt B 1.6.*
B 1.7	Kryptokonzept[45]	(X)	*Siehe AWS Ausrichtung nach BSI IT-Grundschutz, Behandlung von Risiken und Maßnahmen Abschnitt B 1.7.*

[45] In Abhängigkeit der Vertraulichkeit der verarbeiteten Daten

Baustein ID	Titel	Anwendung durch AWS	Zusatzinformation / Bemerkung
B 1.8	Behandlung von Sicherheitsvorfällen	X	Dieser Baustein ist laut „Vorgaben zur IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten“ für Auftraggeber und Dienstleister immer getrennt anzuwenden. *Siehe AWS Ausrichtung nach BSI IT-Grundschutz, Behandlung von Risiken und Maßnahmen Abschnitt B 1.8.*
B 1.9	Hard- und Software-Management	X	Dieser Baustein ist laut „Vorgaben zur IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten“ für Auftraggeber und Dienstleister immer getrennt anzuwenden. *Siehe AWS Ausrichtung nach BSI IT-Grundschutz, Behandlung von Risiken und Maßnahmen Abschnitt B 1.9.*
B 1.14	Patch- und Änderungsmanagement	X	*Siehe AWS Ausrichtung nach BSI IT-Grundschutz, Behandlung von Risiken und Maßnahmen Abschnitt B 1.14.*
B 1.15	Löschen und Vernichten von Daten	X	*Siehe AWS Ausrichtung nach BSI IT-Grundschutz, Behandlung von Risiken und Maßnahmen zur Vernichtung physikalischer Medien.*
B 1.16	Anforderungsmanagement	X	*Siehe AWS Ausrichtung nach BSI IT-Grundschutz, Behandlung von Risiken und Maßnahmen Abschnitt B 1.16.*
B 2 Infrastruktur			
B 2.1	Allgemeines Gebäude	X	*Siehe AWS Ausrichtung nach BSI IT-Grundschutz, Behandlung von Risiken und Maßnahmen Abschnitt B 2.1.*
B 2.2	Elektrotechnische Verkabelung	X	*Siehe AWS Ausrichtung nach BSI IT-Grundschutz, Behandlung von Risiken und Maßnahmen Abschnitt B 2.2.*
B 2.9	Rechenzentrum	X	*Siehe AWS Ausrichtung nach BSI IT-Grundschutz, Behandlung von Risiken und Maßnahmen Abschnitt B 2.1.*
B 2.12	IT-Verkabelung	X	*Siehe AWS Ausrichtung nach BSI IT-Grundschutz, Behandlung von Risiken und Maßnahmen Abschnitt B 2.1.*
B 3 IT-Systeme			
B 3.101	Allgemeiner Server	X	*Siehe AWS Ausrichtung nach BSI IT-Grundschutz, Behandlung von Risiken und Maßnahmen Abschnitt B 3.101.*
B 3.302	Router und Switches	X	*Siehe AWS Ausrichtung nach BSI IT-Grundschutz, Behandlung von Risiken und Maßnahmen Abschnitt B 3.302.*
B 3.304	Virtualisierung	X	*Siehe AWS Ausrichtung nach BSI IT-Grundschutz, Behandlung von Risiken und Maßnahmen Abschnitt B 3.304.*
B 5 Anwendungen			
B 5.22	Protokollierung	X	*Siehe AWS Ausrichtung nach BSI IT-Grundschutz, Behandlung von Risiken und Maßnahmen Abschnitt B 5.22.*
B 5.23	Cloud Management	X	*Siehe AWS Ausrichtung nach BSI IT-Grundschutz, Behandlung von Risiken und Maßnahmen Abschnitt B 5.23.*

Baustein ID	Titel	Anwendung durch AWS	Zusatzinformation / Bemerkung
B 5.24	Web-Services	X	*Siehe AWS Ausrichtung nach BSI IT-Grundschutz, Behandlung von Risiken und Maßnahmen Abschnitt B 5.24.*

Abschnitt 2 – AWS Sicht:

Beschreibung, was durch den Kunden bereitgestellt werden muss

Sicherheit **IN DER** Cloud

Während AWS für die Sicherheit der Cloud-Infrastruktur selbst sorgt, liegt die Verantwortung für die Sicherheit der in der Cloud verarbeiteten Daten und Informationen beim Kunden. Kunden müssen daher selbst für ausreichende Informationssicherheits-Maßnahmen zum Schutz ihrer eigenen Inhalte, ihrer Plattform, Anwendungen, Systeme und Netzwerke sorgen, wie dies auch in einem Rechenzentrum vor Ort mit selbst betriebener IT-Infrastruktur der Fall wäre.

Kunden behalten bei der Nutzung der AWS-Services die volle Kontrolle über ihre eigenen Inhalte. Nicht AWS sondern die Kunden bestimmen, welche Daten und Informationen bei AWS verarbeitet und gespeichert werden, wie die Umgebungen konfiguriert und deren Inhalte gesichert werden sollen und welche Informationssicherheits-Funktionen und -tools sie einsetzen möchten und wie sie sie einsetzen. Aus diesem Grund sind die Kunden auch für die Sicherheit aller Daten und Informationen selbst verantwortlich, die ihr Unternehmen bei AWS verarbeitet und speichert sowie für alle Komponenten, die sie mit der AWS-Infrastruktur verbinden. Dazu gehören beispielsweise Gastbetriebssysteme, Anwendungen auf den Datenverarbeitungs-Instanzen der Kunden und Inhalte, die auf AWS-Speicher-, Plattform- und Datenbank-Services abgelegt und verarbeitet werden.

AWS bietet eine große Auswahl an Sicherheitsfunktionen, die Kunden zur Einrichtung, Implementierung und zum Betrieb ihrer eigenen sicheren AWS-Umgebung einsetzen können. Alternativ können Kunden ihre eigenen Sicherheitstools und -kontrollen verwenden. Die AWS-Services lassen sich nach Wunsch konfigurieren, damit Kunden diese Sicherheitsfunktionen nutzen und ihre Inhalte schützen können. Dazu gehören leistungsstarke Tools zur Identitäts- und Zugriffsverwaltung, Sicherheitsfunktionen, Verschlüsselung und Netzwerksicherheit. Folgende Maßnahmen können Kunden beispielsweise dabei helfen, ihre Inhalte schützen:

- Richtlinien für sichere Passwörter, individuelle Gewährung angemessener Zugriffsrechte und zuverlässiger Schutz von Zugriffsschlüsseln
- Angemessene Firewalls und Netzwerksegmentierung, Verschlüsselung von Inhalten und durchdachte Systemarchitektur, um Datenverlust und nicht autorisierten Zugriff zu verhindern

All diese Faktoren werden vom Kunden kontrolliert, nicht von AWS. AWS hat keine Informationen über die Inhalte, die vom Kunden bei AWS abgelegt werden, und ändert auch keine Konfigurationseinstellungen des Kunden. Diese werden vom Kunden festgelegt und gesteuert. Einzig und allein der Kunde kann entscheiden, welches Sicherheitsniveau für seine bei AWS verarbeiteten und gespeicherten Daten und Informationen angemessen ist.

AWS veröffentlicht verschiedene Whitepaper zu Datensicherheit, Organisation, Risiko und Compliance sowie diverse Checklisten und bewährte Methoden, mit deren Hilfe Kunden die AWS-Informationssicherheits-Maßnahmen in ihre vorhandenen Kontrollrahmen integrieren und Sicherheitsbewertungen zum Einsatz von AWS in ihren Unternehmen erstellen und durchführen können. Natürlich können Kunden auch ihre eigenen Sicherheitsbewertungen erstellen und durchführen und die Erlaubnis zur Durchführung eigener Scans in ihrer Cloud-Infrastruktur beantragen, solange sich diese Scans auf die Datenverarbeitungs-Instanzen des Kunden beschränken und nicht gegen die „AWS Acceptable Use Policy“ verstoßen.

Wie können Anforderungen aus Bausteinen mit bestehenden AWS Zertifizierungen oder Maßnahmen abgedeckt werden

Sicherheit **DER** Cloud

Sicherheit **DER** Cloud bezieht sich darauf, wie AWS die Informationssicherheit der zugrundeliegenden Cloud-Infrastruktur handhabt. Alle Komponenten, von Host-Betriebssystem und Virtualisierungsebene bis hin zur physischen Sicherheit der Anlagen, in denen die AWS-Services ausgeführt werden, werden von AWS betrieben, verwaltet und gesteuert.

Wie können Kunden die in der AWS-Umgebung eingesetzten Sicherheitsmaßnahmen nachprüfen?

Von externen AWS-Prüfern werden AWS-Zertifizierungen und -Berichte erstellt, die die konzeptionelle und operative Wirksamkeit der AWS-Umgebung bezeugen. Dazu gehören:

SOC 1/ ISAE 3402: AWS veröffentlicht den Bericht "Service Organization Controls 1 (SOC 1), Type II[46]". Diese Prüfung ersetzt den Prüfbericht "Statement on Auditing Standards Nr. 70 (SAS 70) Type II". Im SOC 1-Prüfbericht wird bestätigt, dass die AWS-Kontrollziele ihren Zweck erfüllen und die Maßnahmen zum Schutz von Kundendaten wirksam sind.

SOC 2 – Sicherheit: Zusätzlich zum SOC 1-Bericht veröffentlicht AWS den Bericht "Service Organization Controls 2 (SOC 2), Type II[47]". Wie bei SOC 1 werden auch im SOC 2-Bericht die Maßnahmen bewertet, allerdings erstreckt sich dieser Bericht darüber hinaus auf die in den American Institute of Certified Public Accountants (AICPA) Trust Services Principles[48] dargelegten Kriterien. Bei AWS SOC 2 wird die konzeptionelle und operative Wirksamkeit der Maßnahmen bewertet, die das Sicherheitsprinzip gemäß den AICPA Trust Services Principles erfüllen. Dieser Bericht bietet zusätzliche Transparenz hinsichtlich der AWS-Sicherheit basierend auf einer definierten Industrienorm und unterstreicht ferner das Bekenntnis von AWS, Kundendaten zu schützen.

SOC 3 – Sicherheit: AWS veröffentlicht den Bericht "Service Organization Controls 3 (SOC 3)[49] ". Der SOC 3-Bericht ist eine öffentlich zugängliche Zusammenfassung des SOC 2-Berichts und beinhaltet das Sicherheitssiegel AICPA SysTrust Security Seal[50].

Der Bericht umfasst das Gutachten des externen Auditors hinsichtlich der Umsetzung der Maßnahmen (basierend auf den im SOC 2-Bericht enthaltenen AICPA's Security Trust Principles[51]), eine Erklärung des AWS-Managements bezüglich der Wirksamkeit der Maßnahmen und einen Überblick über die AWS-Infrastruktur und –Services.

ISO/IEC 27001: AWS ist gemäß ISO/IEC 27001[52] (International Organization for Standardization) zertifiziert. ISO/IEC 27001 ist ein weit verbreiteter globaler Sicherheitsstandard, der Sicherheitsanforderungen für Informationssicherheits-Managementsysteme (ISMS) beschreibt. Der Standard bietet eine systematische, auf regelmäßigen Risikobewertungen basierende Vorgehensweise für den Umgang mit Unternehmens- und Kundendaten. Um die Zertifizierung zu erhalten, weist AWS nach, dass es über einen systematischen und kontinuierlichen Ansatz für den Umgang mit Informationssicherheitsrisiken verfügt, die die Vertraulichkeit, Integrität und Verfügbarkeit von Unternehmens- und Kundendaten bedrohen.

PCI – Sicherheit: AWS erfüllt die Anforderungen von "Level 1" des PCI (Payment Card Industry) DSS (Data Security Standard), dem Datensicherheitsstandard der Zahlungs- und Kreditkartenbranche. Kunden können ihre Anwendungen auf unserer PCI-konformen Technologieinfrastruktur für die Speicherung, Verarbeitung und Übermittlung von Kreditkartendaten in der Cloud ausführen. Im Februar 2013 hat das PCI Security Standards Council die PCI DSS Cloud Computing Guidelines[53] herausgegeben. Diese Leitlinien bieten Kunden, die eine Umgebung für Kreditkartendaten betreiben, Anleitungen zum Einrichten von PCI DSS-Kontrollen in der Cloud. AWS hat die PCI DSS Cloud Computing-Leitlinien in das AWS PCI-Compliance-Paket für Kunden integriert.

---

46 http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/AICPASOC1Report.aspx
47 http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/AICPASOC2Report.aspx
48 https://cert.webtrust.org/pdfs/Trust_Services_PC_latest.pdf
49 http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/AICPASOC3Report.aspx
50 https://cert.webtrust.org/soc3_amazon_web_services.html
51 https://cert.webtrust.org/pdfs/Trust_Services_PC_latest.pdf
52 http://www.27000.org/iso-27001.htm
53 https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Cloud_Guidelines.pdf

Compliance-Berichte und Zertifizierungen von AWS anfordern

Sie können die jeweiligen AWS-Compliance-Zertifizierungen und -Berichte unter https://aws.amazon.com/compliance/contact anfordern.

Weitere Informationen und Material zur AWS-Compliance-Umgebung

AWS verfügt über Whitepaper zur Compliance[54], die Informationen für AWS-Kunden enthalten, die AWS in ihre vorhandenen Kontrollrahmen integrieren und Sicherheitsbewertungen zum Einsatz von AWS durch ein Unternehmen erstellen und durchführen möchten.

Weitere Informationen zu AWS-Compliance-Zertifizierungen und -Berichten sowie zur Orientierung an bewährten Verfahren und Standards wie MPAA finden Sie auf der Compliance-Website[55] von AWS.

[54] http://aws.amazon.com/compliance/whitepapers
[55] http://aws.amazon.com/de/compliance/

Mapping der vorhandenen Zertifizierungen und Maßnahmen zu den Anforderungen der Grundschutz Bausteine

Die folgende Tabelle stellt eine Übersicht dar, wie die Anforderungen der BSI IT-Grundschutzkataloge durch AWS umgesetzt werden.

Baustein ID	Titel	Umsetzung durch AWS
B 1 Übergreifende Aspekte		
B 1.0	Sicherheitsmanagement	AWS hat einen Rahmen für die Informationssicherheit und Richtlinien festgelegt, die auf dem COBIT-Framework (Control Objectives for Information and related Technology) beruhen, und hat das zertifizierbare Framework ISO/IEC 27001 mithilfe der ISO/IEC 27002-Kontrollen, der American Institute of Certified Public Accountants (AICPA) Trust Services Principles, dem PCI DSS v2.0 und der Veröffentlichung 800-53 Rev 3 (Recommended Security Controls for Federal Information Systems) des National Institute of Standards and Technology (NIST) integriert. Die Kontrollumgebung beginnt bei Amazon auf höchster Unternehmensebene. Die Geschäftsführung sowie die Führungskräfte des oberen Managements spielen bei der Festlegung der Grundwerte des Unternehmens eine entscheidende Rolle. AWS verfügt über eine etablierte Informationssicherheits-Organisation, die durch das AWS-Sicherheitsteam gemanagt und durch den AWS Chief Information Security Officer (CISO, Beauftragter für die zentrale IT-Sicherheit) geleitet wird. AWS führt für alle Benutzer des Informationssystems, die AWS unterstützen, Schulungen zur Sensibilisierung durch. Diese jährliche Schulung zur Sicherheitssensibilisierung umfasst die folgenden Themen: Zielsetzung der Schulung über Sicherheit und Sensibilisierung, Ablageorte aller AWS-Richtlinien, AWS-Vorfallreaktionsprozesse (einschließlich Anweisungen darüber, wie interne und externe Sicherheitsvorfälle zu berichten sind). AWS hat Richtlinien zur Zertifizierung, Autorisierung und Sicherheitsbewertung erarbeitet, die die Zielsetzung, den Umfang, die Rollen, die Verantwortlichkeiten und das Engagement der Unternehmensleitung in Bezug darauf festlegt, wie AWS die Ausrichtung an durch Dritte geprüften Zertifizierungen/Akkreditierungen verwaltet, überwacht und kommuniziert. Das AWS Security Assurance-Team ist damit beauftragt, die Compliance-Frameworks einzuführen, zu verwalten, zu überwachen und zu bewerten. Dazu gehört auch die Verwaltung der Prüfgegenstände wie Dokumentationen zur Systemsicherheit, Prüfgegenstände, Prüfungsergebnisse und Abhilfemaßnahmen. AWS arbeitet mit externen Zertifizierungsstellen und unabhängigen Auditoren zusammen, um unsere Compliance mit allen Compliance-Frameworks im gesamten System zu überprüfen und zu validieren.
B 1.1	Organisation	AWS hat einen Rahmen für die Informationssicherheit und Richtlinien festgelegt, die auf dem COBIT-Framework (Control Objectives for Information and related Technology) beruhen, und hat das zertifizierbare Framework ISO/IEC 27001 mithilfe der ISO/IEC 27002-Kontrollen, der American Institute of Certified Public Accountants (AICPA) Trust Services Principles, dem PCI DSS v2.0 und der Veröffentlichung 800-53 Rev 3 (Recommended Security Controls for Federal Information Systems) des National Institute of Standards and Technology (NIST) integriert. AWS befolgt Sicherheitsrichtlinien, bietet Sicherheitsschulungen für Mitarbeiter an und führt Sicherheitsprüfungen für Anwendungen durch. Diese Prüfungen beurteilen die Vertraulichkeit, Integrität und Verfügbarkeit von Daten sowie die Einhaltung der Richtlinien zur Informationssicherheit. Die Kontrollumgebung beginnt bei Amazon auf höchster Unternehmensebene. Die Geschäftsführung sowie die Führungskräfte des oberen Managements spielen bei der

Baustein ID	Titel	Umsetzung durch AWS
		Festlegung der Grundwerte des Unternehmens eine entscheidende Rolle. Die AWS-Organisationsstruktur bietet einen Rahmen für die Planung, Ausführung und Kontrolle der Geschäftstätigkeiten. Die Organisationsstruktur weist Rollen und Verantwortlichkeiten zu, um eine angemessene Personalausstattung, Betriebseffizienz und Aufgabenverteilung zu gewährleisten. Das Management hat auch leitendes Personal mit Kompetenzen ausgestattet und geeignete Berichtslinien eingerichtet. Die Überprüfung der Ausbildung, der vorherigen Beschäftigung und, in einzelnen Fällen und soweit rechtlich zulässig, der Hintergrundinformationen zählen zu den Bestandteilen des Einstellungsprozesses des Unternehmens, wobei diese Überprüfungen im angemessenen Verhältnis zur Position und zum Level der Zugriffsberechtigung des Mitarbeiters auf AWS-Einrichtungen durchgeführt werden müssen. Das Unternehmen befolgt einen strukturierten Onboarding-Prozess, um neue Mitarbeiter mit den Tools, Prozessen, Systemen, Richtlinien und Verfahren von Amazon vertraut zu machen. AWS hat die folgende Maßnahmenliste zusammengestellt, um Bedrohungen in der Lieferkette vorzubeugen, welche wiederum die Ressourcen beeinträchtigen könnten: Agile Beschaffung – Das obere Management von AWS hält eine wöchentliche Besprechung ab, in der festgelegt wird, welche Maßnahmen notwendig sind, um die Geschäftsanforderungen zu erfüllen. Die Einzelposten, die für die Abdeckung der Kapazitätsanforderungen ermittelt wurden, werden in RFQs (Requests for Quotation, Aufforderungen zur Angebotsabgabe) bekanntgegeben und anschließend erworben. Diese häufige Überprüfung der Anforderungen und der daraus erfolgende Angebots- und Akquisitionszyklus führen zu einem wesentlich agileren Akquisitionsprozess, als wenn die Ausgaben für die Einzelposten in einem Jahreszyklus eingeplant werden. Durch diesen Prozess ist es AWS möglich, schnell auf Geschäftsanforderungen zu reagieren. Einzelverträge – Die wöchentlichen Gespräche und häufigen RFQs erlauben eine größere Anzahl kleinerer Verträge, die bei Bedarf erneuert werden. Falls ein Anbieter aus welchem Grund auch immer nicht in der Lage ist, die Lieferung auszuführen, sind die Auswirkungen gering und für die Beschaffung kann leicht eine neue Quelle gefunden werden. Verwendung anerkannter, etablierter, diversifizierter Lieferanten – Dem Eingehen vertraglicher Vereinbarungen, um Hardware, Software, Firmware oder Services zu erwerben, muss eine Unternehmensprüfung (Due Diligence) der Lieferanten vorausgehen. Mehrere Anbieter – Eine Liste zugelassener Anbieter wird vom AWS-Team geführt, jeweils mit mehreren Anbietern zur Auswahl für jeden Komponententyp. Sollte ein Lieferant außerstande sein, die Lieferung auszuführen, kann ein anderer Anbieter für die nächsten Beschaffungsvorgänge verwendet werden. Obwohl ein Großteil des AWS-Systems unternehmensintern entwickelt wurde, um den besonderen AWS-Anforderungen gerecht zu werden, verwendet AWS soweit wie möglich auch standardmäßige, kommerziell erhältliche Informationssystemkonfigurationen und reduziert so die Möglichkeit, Systeme und Produkte zu erwerben, die während der Lieferkettenvorgänge beschädigt wurden. Beim Erwerb der AWS-Ressourcen werden diese mit einer Komponentenkennzeichnung versehen. AWS-

Baustein ID	Titel	Umsetzung durch AWS
		Komponentenkennzeichnungen sind kundenunabhängig und dienen der Inventarisierung der Hardware innerhalb des AWS-Tools zur Komponentenverwaltung. In den AWS-Rechenzentren wird die Hardware normalerweise nicht physisch speziellen Kunden oder den auf der Hardware gespeicherten Daten zugeordnet. Alle Kundendaten werden unabhängig von ihrer Quelle als kritisch angesehen und aus diesem Grund werden alle Medien vertraulich behandelt. Die Prozesse und Vorgänge der AWS-Komponentenverwaltung werden von unabhängigen, externen Auditoren während der Prüfungen bezüglich der Compliance mit PCI DSS, ISO 27001 und FedRAMP überprüft. AWS verwendet für den Zugang zu Rechenzentren nicht nur Multi-Factor Authentication-Mechanismen sondern auch zusätzliche Sicherheitsmechanismen, die so ausgelegt sind, dass nur autorisierte Personen Zugang zu einem AWS-Rechenzentrum erhalten. Die autorisierten Personen müssen ihren Zugangsausweis an einem Kartenleser verwenden und ihre individuelle PIN eingeben, um Zugang zur Einrichtung und den Räumen zu erhalten, für die sie autorisiert wurden. Der physische Zugang zu den Rechenzentren wird durch das elektronische AWS-Zugangskontrollsystem überwacht. Für den Zugang in das Gebäude und die Räume setzt sich das System aus Kartenlesern und PIN-Pads zusammen, für das Verlassen besteht es nur aus Kartenlesern. Durch die Verwendung von Kartenlesern beim Verlassen von Gebäuden und Räumen treten Doppelzutrittssperren in Kraft, die sicherstellen, dass autorisierte Personen nicht von unautorisierten Personen verfolgt werden, die sich so ohne Ausweis Zutritt verschaffen. Zusätzlich zum Zugangskontrollsystem sind alle Eingänge der AWS-Rechenzentren, einschließlich des Haupteingangs, der Laderampe und aller Dachausstiege/-luken, mit Einbruchmeldevorrichtungen versehen, die einen Alarm auslösen, sobald die Tür aufgebrochen oder aufgehalten wird. Neben den elektronischen Mechanismen verwenden die AWS-Rechenzentren rund um die Uhr auch ausgebildete Sicherheitskräfte, die sowohl innerhalb der Gebäude als auch in deren Umgebung stationiert sind. Innerhalb des Systems wird der Zugang zu den Rechenzentren nur nach Notwendigkeit erteilt; alle physischen Zugangsanfragen werden vom zuständigen AAM (Area Access Manager, Zutrittsmanager) überprüft und genehmigt. AWS-Rechenzentren sind in unauffälligen Anlagen untergebracht und sind nicht für die Öffentlichkeit zugänglich. Der physische Zugang wird sowohl in der Umgebung als auch an den Zutrittspunkten zum Gebäude streng kontrolliert. AWS gewährt nur solchen Anbietern, Auftragnehmern und Besuchern Zugang und Informationen zu den Rechenzentren, für die eine legitime geschäftliche Notwendigkeit besteht, wie Notfallreparaturen. Alle Besucher der Rechenzentren müssen vorab durch den zuständigen Zutrittsmanager (AAM) autorisiert worden sein und im AWS-Ticketmanagementsystem dokumentiert werden. Bei der Ankunft am Rechenzentrum müssen sie sich ausweisen und anmelden, bevor ihnen ein Besucherausweis ausgestellt wird. Während sie sich im Rechenzentrum befinden, werden sie ständig von autorisiertem Personal begleitet. Die physischen Sicherheitsmechanismen von AWS werden von unabhängigen, externen Auditoren während der Prüfungen bezüglich der Compliance mit SOC, PCI DSS, ISO/IEC 27001 und FedRAMP überprüft. AWS hat formale Richtlinien und Verfahren gemäß ISO/IEC 27001 erstellt, um Mindeststandards für den logischen Zugriff auf die AWS-Ressourcen festzulegen. Der Bericht AWS-SOC 1-Typ II und SOC 2-Typ II beschreibt die vorhandenen Kontrollen, um die Zugriffsberechtigungen von AWS-Ressourcen zu verwalten. Das AWS-Produktionsnetzwerk ist vom Amazon-Unternehmensnetzwerk getrennt und erfordert separate Anmeldeinformationen für den logischen Zugriff. Das Amazon-Unternehmensnetzwerk verwendet Benutzer-IDs, Passwörter und Kerberos, während das AWS-Produktionsnetzwerk eine Authentifizierung mit einem öffentlichen SSH-Schlüssel durch einen Bastion-Host erfordert. AWS-Entwickler und Administratoren des Amazon-Unternehmensnetzwerks, die Zugriff auf die AWS-Cloud-Komponenten benötigen, müssen ausdrücklich eine Anforderung auf Zugriff über das AWS-Zugriffsverwaltungssystem stellen. Alle Anforderungen werden vom entsprechenden Verantwortlichen oder Manager überprüft und genehmigt. Konten werden

Baustein ID	Titel	Umsetzung durch AWS
		alle 90 Tage überprüft; es ist eine ausdrückliche erneute Überprüfung erforderlich oder der Zugriff auf die Ressource wird automatisch widerrufen. Der Zugriff wird ebenfalls automatisch widerrufen, wenn ein Mitarbeiterdatensatz im Personalverwaltungssystem von Amazon geschlossen wird. Windows- und UNIX-Konten werden deaktiviert und das Zugriffsverwaltungssystem von Amazon entfernt den Benutzer aus allen Systemen. Anforderungen für Zugriffsänderungen werden im Auditprotokoll des Zugriffsverwaltungssystem von Amazon erfasst. Wenn sich die Funktion eines Mitarbeiters ändert, muss der kontinuierliche Zugriff ausdrücklich in der Ressource genehmigt werden, da dieser sonst automatisch widerrufen wird.
B 1.2	Personal	Die AWS-Organisationsstruktur bietet einen Rahmen für die Planung, Ausführung und Kontrolle der Geschäftstätigkeiten. Die Organisationsstruktur weist Rollen und Verantwortlichkeiten zu, um eine angemessene Personalausstattung, Betriebseffizienz und Aufgabenverteilung zu gewährleisten. Das Management hat auch leitendes Personal mit Kompetenzen ausgestattet und geeignete Berichtslinien eingerichtet. Die Überprüfung der Ausbildung, der vorherigen Beschäftigung und, in einzelnen Fällen und soweit rechtlich zulässig, der Hintergrundinformationen zählen zu den Bestandteilen des Einstellungsprozesses des Unternehmens, wobei diese Überprüfungen im angemessenen Verhältnis zur Position und Level der Zugriffsberechtigung des Mitarbeiters auf AWS-Einrichtungen durchgeführt werden müssen. Das Unternehmen befolgt einen strukturierten Onboarding-Prozess, um neue Mitarbeiter mit den Tools, Prozessen, Systemen, Richtlinien und Verfahren von Amazon vertraut zu machen. AWS hat verschiedene Methoden zur internen Kommunikation auf weltweiter Ebene implementiert, um Mitarbeiter dabei zu unterstützen, ihre jeweiligen Rollen und Verantwortlichkeiten zu verstehen und wichtige Vorfälle zeitgerecht zu kommunizieren. Diese Methoden umfassen Orientierungs- und Schulungsprogramme für neu eingestellte Mitarbeiter sowie E-Mail-Benachrichtigungen und das Posten von Informationen über das Amazon-Intranet. Die Rechtsberater von Amazon verwalten und überarbeiten regelmäßig die Geheimhaltungsvereinbarung von Amazon, um die Geschäftsbedürfnisse von AWS widerzuspiegeln. Die Geheimhaltungsvereinbarung von AWS wird von unabhängigen, externen Auditoren während der Prüfungen bezüglich der Compliance mit ISO 27001 und FedRAMP überprüft. AWS führt für alle Benutzer des Informationssystems, die AWS unterstützen, Schulungen zur Sensibilisierung durch. Diese jährliche Schulung zur Sicherheitssensibilisierung umfasst die folgenden Themen: - die Zielsetzung der Schulung über Sicherheit und Sensibilisierung, - die Ablageorte aller AWS-Richtlinien, - die AWS-Vorfallreaktionsprozesse (einschließlich Anweisungen darüber, wie interne und externe Sicherheitsvorfälle zu berichten sind). Das Onboarding von Auftragnehmern und Anbietern wird für Mitarbeiter und Auftragnehmer gleich gehandhabt, wobei die Verantwortung hierfür zwischen den Bereichen Personalverwaltung und Betriebsprozesse sowie den Service-Inhabern aufgeteilt wird. Die AWS-Richtlinien, Prozesse und relevanten Schulungsprogramme werden von unabhängigen, externen

Baustein ID	Titel	Umsetzung durch AWS
		Auditoren während der Prüfungen bezüglich der Compliance mit SOC, PCI DSS, ISO/IEC 27001 und FedRAMP überprüft. Weitere Informationen finden Sie im AWS-Whitepaper "Übersicht über die Sicherheitsprozesse" unter http://aws.amazon.com/security. Das AWS-Personalverwaltungsteam definiert die internen Verwaltungsaufgaben, die im Falle einer Kündigung bzw. einer Rollenveränderung der Mitarbeiter und Anbieter befolgt werden müssen. Die Verantwortung für die Genehmigung/Entziehung der Zugangsrechte der Mitarbeiter und Auftragnehmer wird zwischen den Bereichen Personalverwaltung und Betriebsprozesse sowie den Service-Inhabern aufgeteilt. Weitere Informationen finden Sie im AWS-Whitepaper "Übersicht über die Sicherheitsprozesse" unter http://aws.amazon.com/security.
B 1.3	Notfallmanagement	Die AWS-Richtlinien und -Pläne zum Notfallmanagement wurden im Einklang mit ISO/IEC 27001 entwickelt und getestet und sind Teil des umfassenderen Ansatzes von AWS hinsichtlich der Entwicklung von Informationssicherheits-Richtlinien. Das Programm AWS Resilience umfasst die Verfahren und Vorgehensweisen, die die AWS-Komponenten zur Identifizierung und Behebung eines erheblichen Vorfalls einsetzen. Dieses Programm nimmt den traditionellen Ansatz des Contingency Managements mit Elementen herkömmlicher Betriebskontinuitäts- und Notfallwiederherstellungspläne zur Grundlage. Ergänzt werden diese jedoch um wichtige Elemente proaktiver Strategien zur Gefahreneindämmung, z. B. durch Schaffung physisch separater Availability Zones (AZ) und fortlaufende Infrastrukturkapazitätsplanung. Die Notfallpläne und Vorfallleitfäden von AWS werden ständig um neu erkannte Betriebsrisiken und durch Erkenntnisse aus vergangenen Störungen ergänzt. Die Handhabung von Störungen durch AWS wird regelmäßig getestet. Aus diesen Tests gewonnene Erkenntnisse werden umgesetzt und die Dokumentation wird entsprechend aktualisiert. AWS-Rechenzentren werden gruppenweise in verschiedenen Regionen der Welt errichtet. Alle Rechenzentren sind online und bedienen Kunden; kein Rechenzentrum ist abgeschaltet. Bei einem Ausfall verschieben automatische Prozesse den Kundendatenverkehr weg von den betroffenen Bereichen. Die Kernanwendungen werden in einer N+1-Konfiguration bereitgestellt, sodass im Falle eines Rechenzentrumsausfalls ausreichend Kapazität vorhanden ist, um den Datenverkehr lastverteilt an die verbleibenden Standorte zu verteilen. AWS bietet Kunden die Flexibilität, Instanzen zu platzieren und Daten innerhalb mehrerer geografischer Regionen sowie über mehrere Availability Zones innerhalb der einzelnen Regionen zu speichern. Jede Availability Zone wurde als unabhängige Ausfallszone entwickelt. Dies bedeutet, dass Availability Zones innerhalb einer typischen Stadtregion physisch verteilt sind und sich in Gebieten mit niedrigerem Überschwemmungsrisiko befinden (je nach Region gibt es unterschiedliche Überschwemmungszonen-Kategorisierungen). Zusätzlich zu einer eigenständigen unterbrechungsfreien Stromversorgung und Notstromgeneratoren vor Ort werden alle Availability Zones über unterschiedliche Stromnetze von unabhängigen Stromversorgern gespeist, um Einzelfehlerstellen zu minimieren. Sämtliche Availability Zones sind redundant mit mehreren Tier-1-Transit-Providern verbunden. Kunden sollten die Architektur ihrer AWS-Nutzung so erstellen, dass sie mehrere Regionen und Availability Zones umfasst. Durch das Verteilen von Anwendungen über mehrere Availability Zones bleibt die Architektur bei den meisten Ausfallarten, einschließlich Naturkatastrophen oder Systemausfällen, stabil. Weitere Details finden Sie im AWS-SOC 1-Typ II-Bericht. Außerdem enthält ISO/IEC 27001, Anhang A.11.2, zusätzliche Informationen. AWS wurde durch einen unabhängigen Auditor auf Erfüllung der ISO/IEC 27001-Zertifizierungsanforderungen geprüft. AWS bietet Kunden eine raschere Notfallwiederherstellung ihrer kritischen IT-Systeme, ohne dass ein kostspieliger zweiter

Baustein ID	Titel	Umsetzung durch AWS
		physischer Standort erforderlich ist. Die AWS Cloud unterstützt zahlreiche bekannte Notfallwiederherstellungs-Architekturen, von "Pilot-Light"-Umgebungen, die sich ohne Zeitverlust skalieren lassen, bis zu Hot-Standby-Umgebungen, die ein rasches Failover erlauben. Weitere Informationen zur Notfallwiederherstellung bei AWS finden sich unter http://media.amazonwebservices.com/AWS_Disaster_Recovery.pdf. Mit AWS können Kunden einen zuverlässigen Kontinuitätsplan implementieren, der häufige Server-Instanz-Backups, Datenredundanz-Replikation und Bereitstellungsarchitekturen für mehrere Regionen bzw. Availability Zones umfasst. AWS bietet Kunden die Flexibilität, Instanzen zu platzieren und Daten innerhalb mehrerer geografischer Regionen sowie über mehrere Availability Zones innerhalb der einzelnen Regionen zu speichern. Jede Availability Zone wurde als unabhängige Ausfallszone entwickelt. Bei einem Ausfall wird der Datenverkehr des Kunden durch automatische Prozesse von dem betroffenen Bereich ferngehalten.
B 1.6	Schutz vor Schadprogrammen	Das Programm, die Verfahren und die Vorgehensweisen von AWS zur Handhabung von Virenschutz bzw. Schadprogrammen entsprechen den ISO/IEC 27001-Standards. Weitere Informationen finden Sie im SOC 1-Typ II-Bericht für AWS. Das gesamte Konfigurationsmanagement und alle Nachbesserungsprozesse von AWS werden regelmäßig von unabhängigen Auditoren auf Erfüllung der Anforderungen von SOC, PCI DSS, ISO/IEC 27001 und FedRAMP geprüft. Ein Konfigurationsmanagementtool wird zur Verwaltung von bereitstellbarer Software in Paketen, Paketgruppen und Umgebungen verwendet. Bei einem Paket handelt es sich um eine Sammlung zusammenhängender Dateien, z. B. eng miteinander verknüpfte Software oder verknüpfter Content. Mehrere Pakete, die oft gemeinsam bereitgestellt werden, werden als Paketgruppe bezeichnet. Eine Umgebung schließlich ist eine Kombination von Paketen und Paketgruppen, die in einer Gruppe von Hostklassen (Hosts oder Servern mit derselben Funktion) bereitgestellt werden. Eine Umgebung stellt die Gesamtheit aller Pakete dar, die zur Ausführung einer bestimmten Funktion durch den Server erforderlich sind. Amazon-Geräte, z. B. Laptops, sind mit Virenschutzsoftware konfiguriert, die E-Mail-Filterung und Schadware-Erkennung umfasst.
B 1.7	Kryptokonzept	AWS gibt Kunden die Möglichkeit, für nahezu alle Services einschließlich S3, EBS und EC2 Ihren eigenen Verschlüsselungsmechanismus zu verwenden. VPC-Sitzungen sind ebenfalls verschlüsselt. Für AWS-Verbindungen stehen FIPS-zugelassene Hashes zur Verfügung. AWS nutzt kryptografische Module zur Benutzerauthentifizierung über folgende Zugriffsmethoden: API-Endpunkte, VPC IPSEC VPN, IAM, MFA-Hardware-Token, SSH. Intern erstellt und verwaltet AWS kryptografische Schlüssel zur Kryptografie, die innerhalb der AWS-Infrastruktur eingesetzt wird. AWS erstellt, steuert und verteilt symmetrische kryptografische Schlüssel mithilfe NIST-zugelassener Schlüsselverwaltungstechnologie und -prozesse im AWS-Informationssystem. Zur Erstellung, zum Schutz und zur Verteilung symmetrischer Schlüssel wird ein von AWS entwickelter Verschlüsselungs- und Anmeldungsmanager verwendet. Damit wird Folgendes gesichert und verteilt: AWS-Anmeldeinformationen, die für Hosts benötigt werden, öffentliche/private RSA-Schlüssel und X.509-Zertifizierungen. Die kryptografischen Prozesse von AWS werden regelmäßig von unabhängigen Auditoren auf Erfüllung der Anforderungen von SOC, PCI DSS, ISO/IEC 27001 und FedRAMP geprüft.

Baustein ID	Titel	Umsetzung durch AWS
		Darüber hinaus können Kunden mit dem AWS CloudHSM-Service Ihre Schlüssel zur Datenverschlüsselung innerhalb von HSMs schützen, die für die sichere Schlüsselverwaltung konzipiert und geprüft wurden. Sichere kryptografische Schlüssel für die Datenverschlüsselung lassen sich generieren und verwalten, auf die nur die jeweiligen Kunden zugreifen können. Dank AWS CloudHSM können die AWS Kunden strenge Schlüsselverwaltungsanforderungen erfüllen, ohne dafür die Anwendungsleistung zu opfern. Der AWS CloudHSM-Service wird mit der Amazon Virtual Private Cloud (VPC) zusammen eingesetzt. CloudHSMs werden mit einer von Ihnen angegebenen IP-Adresse in der VPC des Kunden bereitgestellt und bieten somit eine problemlose und private Netzwerkkonnektivität mit den Amazon Elastic Compute Cloud (EC2)-Instanzen des Kunen. Die Platzierung von CloudHSMs in der Nähe der EC2-Instanzen verringert die Netzwerklatenz. Das kann die Anwendungsleistung erhöhen. AWS bietet den Kunden dedizierten, exklusiven Zugriff auf CloudHSMs. AWS CloudHSMs sind in verschiedenen Regionen und Availability Zones (AZs) verfügbar. Den Amazon EC2-Anwendungen kann eine langfristige und sichere Schlüsselspeicherung hinzugefügt werden.
B 1.8	Behandlung von Sicherheitsvorfällen	AWS hat eine formale, dokumentierte Richtlinie und ein Programm zur Vorfallhandhabung implementiert. Diese Richtlinie beschreibt die Zielsetzung, den Umfang, die Rollen, die Verantwortlichkeiten und das Engagement der Unternehmensleitung. AWS führt außerdem für alle Benutzer des Informationssystems, die AWS unterstützen, Schulungen zur Sicherheitssensibilisierung durch. Diese jährliche Schulung zur Sicherheitssensibilisierung umfasst die folgenden Themen: - die Zielsetzung der Schulung über Sicherheit und Sensibilisierung, - die Ablageorte aller AWS-Richtlinien, - die AWS-Vorfallreaktionsprozesse (einschließlich Anweisungen darüber, wie interne und externe Sicherheitsvorfälle zu berichten sind). Systeme innerhalb von AWS sind umfassend zur Überwachung von wichtigen Betriebs- und Datensicherheitsmetriken ausgestattet. Alarme sind so konfiguriert, dass sie automatisch das Betriebs- und Verwaltungspersonal benachrichtigen, wenn die Frühwarnschwellen von wichtigen Betriebsmetriken überschritten werden. Wird eine Frühwarnschwelle überschritten, wird der AWS-Vorfallreaktionsprozess gestartet. Das Amazon-Team zur Behebung von Vorfällen wendet branchenübliche diagnostische Verfahren an, um die Behebung unternehmenskritischer Vorfälle zu beschleunigen. Das Betriebspersonal bietet eine kontinuierliche Besetzung rund um die Uhr, sieben Tage die Woche und an 365 Tagen im Jahr, um Störfälle zu erkennen und deren Auswirkungen und Behebung zu verwalten. AWS nutzt zum Umgang mit Sicherheitsvorfällen einen Drei-Phasen-Ansatz: 1. Aktivierungs- und Benachrichtigungsphase: Ein Vorfall beginnt laut AWS-Definition mit dem Feststellen eines

Baustein ID	Titel	Umsetzung durch AWS
		Ereignisses. Die Information kann aus unterschiedlichen Quellen stammen, z. B.: a. Metriken und Alarme – Probleme werden von AWS extrem schnell ermittelt, da eine Überwachung rund um die Uhr stattfindet und Echtzeit-Metriken sowie Service-Dashboards sofort Alarme auslösen. Die Mehrheit aller Störfälle wird auf diese Weise festgestellt. AWS nutzt Alarme bei frühzeitigen Anzeichen, um Probleme zu erkennen, die letztendlich Auswirkungen auf die Kunden haben können. b. Durch einen AWS-Mitarbeiter erstelltes Fehlertickets. c. Anrufe bei der allzeit verfügbaren technischen Support-Hotline. Erfüllt das Ereignis die Kriterien für einen Vorfall, leitet der relevante Support-Techniker mithilfe des AWS Event Management Tool-Systems die erforderlichen Schritte ein und benachrichtigt die jeweiligen Experten für die Behebung des Problems (z. B. das Sicherheitsteam). Diese analysieren den Vorfall, um zu ermitteln, ob weitere Hilfe benötigt wird und was die wahrscheinliche Ursache des Vorfalls sein könnte. 2. Wiederherstellungsphase – die Verantwortlichen führen eine Break-/Fix-Behebung der Störung durch. Nachdem Fehlersuche, Break/Fix und Feststellung betroffener Komponenten durchgeführt wurden, weist der Verantwortliche die weiteren Schritte hinsichtlich Dokumentation und anderer Maßnahmen entsprechend zu und schließt den Fall ab. 3. Nachbereitungsphase – Sobald die erforderlichen Schritte zur Fehlerbehebung durchgeführt wurden, wird die Wiederherstellungsphase als abgeschlossen erklärt. Nachbesprechungen und umfassende Ursachenforschung werden dem relevanten Team aufgetragen. Die daraus gewonnenen Erkenntnisse werden von den verantwortlichen Führungskräften geprüft und Maßnahmen, die sich daraus ergeben, z. B. Design-Änderungen, werden in einem Correction of Errors-Dokument (COE, Fehlerbehebungsdokument) erfasst und bis zur Durchführung nachverfolgt. Zusätzlich zu den oben beschriebenen internen Kommunikationsmechanismen hat AWS ebenfalls verschiedene Methoden der externen Kommunikation implementiert, um den Kundenkreis und die Community zu unterstützen. Es wurden Mechanismen eingerichtet, die das Kunden-Support-Team über Betriebsprobleme benachrichtigen, wenn durch diese die Nutzererfahrung der Kunden beeinträchtigt wird. Eine "Übersicht zum Servicestatus" (Service Health Dashboard) steht zur Verfügung, die vom Kunden-Support-Team verwaltet wird und in der Kunden auf Probleme hingewiesen werden, die größere Auswirkungen haben könnten.
B 1.9	Hard- und Software-Management	Entsprechend den ISO/IEC 27001-Standards werden die AWS-Hardware-Komponenten einem Verantwortlichen zugewiesen und von den AWS-Mitarbeitern mithilfe AWS-eigener Bestandsverwaltungstools nachverfolgt und überwacht. AWS hat die folgende Maßnahmenliste zusammengestellt, um Bedrohungen in der Lieferkette vorzubeugen, welche wiederum die Ressourcen beeinträchtigen könnten:

Baustein ID	Titel	Umsetzung durch AWS
		Agile Beschaffung – Das obere Management von AWS hält eine wöchentliche Besprechung ab, in der festgelegt wird, welche Maßnahmen notwendig sind, um die Geschäftsanforderungen zu erfüllen. Die Einzelposten, die für die Abdeckung der Kapazitätsanforderungen ermittelt wurden, werden in RFQs (Requests for Quotation, Aufforderungen zur Angebotsabgabe) bekanntgegeben und anschließend erworben. Diese häufige Überprüfung der Anforderungen und der daraus erfolgende Angebots- und Akquisitionszyklus führen zu einem wesentlich agileren Akquisitionsprozess, als wenn die Ausgaben für die Einzelposten in einem Jahreszyklus eingeplant werden. Durch diesen Prozess ist es AWS möglich, schnell auf Geschäftsanforderungen zu reagieren. Einzelverträge – Die wöchentlichen Gespräche und häufigen RFQs erlauben eine größere Anzahl kleinerer Verträge, die bei Bedarf erneuert werden. Falls ein Anbieter aus welchem Grund auch immer nicht in der Lage ist, die Lieferung auszuführen, sind die Auswirkungen gering und für die Beschaffung kann leicht eine neue Quelle gefunden werden. Verwendung anerkannter, etablierter, diversifizierter Lieferanten – Dem Eingehen vertraglicher Vereinbarungen, um Hardware, Software, Firmware oder Services zu erwerben, muss eine Unternehmensprüfung (Due Diligence) der Lieferanten vorausgehen. Mehrere Anbieter – Eine Liste zugelassener Anbieter wird vom AWS-Team geführt, jeweils mit mehreren Anbietern zur Auswahl für jeden Komponententyp. Sollte ein Lieferant außerstande sein, die Lieferung auszuführen, kann ein anderer Anbieter für die nächsten Beschaffungsvorgänge verwendet werden. Obwohl ein Großteil des AWS-Systems unternehmensintern entwickelt wurde, um den besonderen AWS-Anforderungen gerecht zu werden, verwendet AWS soweit wie möglich auch standardmäßige, kommerziell erhältliche Informationssystemkonfigurationen und reduziert so die Möglichkeit, Systeme und Produkte zu erwerben, die während der Lieferkettenvorgänge beschädigt wurden. Alle neuen Informationssystemkomponenten für AWS-Rechenzentren erfordern Autorisierung durch die und Benachrichtigung der Rechenzentrumsleitung. Dazu zählen unter anderem Server, Racks, Netzwerkgeräte, Festplatten, Systemhardware-Komponenten und Baustoffe, die an Rechenzentren geliefert und von Rechenzentren in Empfang genommen werden. Die Artikel werden an die Laderampe der einzelnen AWS-Rechenzentren geliefert und dort auf Beschädigungen an Artikel oder Verpackung geprüft sowie von einem Vollzeitmitarbeiter von AWS gegengezeichnet. Jede Lieferung wird gescannt und in das Komponentenverwaltungs- und Inventarsystem von AWS aufgenommen. Eingegangene Artikel werden vor der endgültigen Installation im Rechenzentrum zunächst in einem Lagerraum innerhalb des Rechenzentrums gelagert, zu dem der Zugang nur über Magnetstreifenkarte und PIN-Eingabe möglich ist. Bevor Artikel das Rechenzentrum verlassen können, werden sie gescannt, dokumentiert und bereinigt. Wenn die Lebensdauer eines Speichergeräts zu Ende geht, führt AWS einen Prozess zur Außerbetriebnahme durch, der entwickelt wurde, damit Kundendaten nicht an unautorisierte Personen offengelegt werden. AWS wendet die in DoD 5220.22-M ("Betriebshandbuch zum nationalen Branchensicherheitsprogramm") oder NIST 800-88 ("Richtlinien zur Medienbereinigung") beschriebenen Techniken an, um Daten im Rahmen des Prozesses zur Außerbetriebnahme zu zerstören. Wenn ein Hardware-Gerät nicht mithilfe dieser Prozesse außer Betrieb genommen werden kann, dann wird das Gerät entmagnetisiert und physisch den branchenüblichen Vorgehensweisen entsprechend zerstört. Weitere

Baustein ID	Titel	Umsetzung durch AWS
		Informationen finden Sie im AWS-Whitepaper "Übersicht über die Sicherheitsprozesse" unter http://aws.amazon.com/security. AWS hat für alle Systeme und Geräte innerhalb des AWS-Systems auditierbare Ereigniskategorien ermittelt. Service-Teams konfigurieren die Auditfunktionen so, dass sicherheitsrelevante Ereignisse fortlaufend gemäß den Anforderungen aufgezeichnet werden. Das Protokollspeichersystem ist dafür ausgelegt, einen hoch skalierbaren und hoch verfügbaren Service zu bieten, dessen Kapazität bei steigendem Protokollspeicherbedarf automatisch erweitert wird. Die Auditdaten enthalten eine Gruppe von Datenelementen, die die erforderlichen Analyseanforderungen unterstützen. Zusätzlich stehen sie dem AWS-Sicherheitsteam oder anderen relevanten Teams bei Bedarf zur Prüfung oder Analyse und für die Behebung sicherheitsrelevanter oder geschäftsschädigender Ereignisse zur Verfügung. Mitarbeiter des AWS-Teams erhalten automatisierte Benachrichtigungen, wenn Fehler in überwachten Prozessen auftreten. Dazu gehören unter anderem Software- oder Hardwarefehler. Nach Erhalt einer Fehlermeldung stellen die benachrichtigten Mitarbeiter ein Fehlerticket aus und behandeln das Problem, bis es gelöst ist. Der AWS-SOC 1-Typ II-Bericht bietet einen Überblick der zur Änderungsverwaltung in der physischen und logischen AWS-Umgebung verfügbaren Kontrollen. Bei jeder Änderung, die in den Systemen und Geräten innerhalb des AWS-Systems vorgenommen wird, wird ein Change Management-Ticket (CM, Änderungsverwaltung) erstellt. In diesem CM-Ticket werden alle Details der Änderung festgehalten. Dazu gehören eine Beschreibung der Änderung, Auswirkungsanalyse, ggf. Sicherheitsüberlegungen, Änderungszeitraum und erforderliche Genehmigungen. AWS hat formale Richtlinien und Verfahren gemäß ISO/IEC 27001 erstellt, um Mindeststandards für den logischen Zugriff auf die AWS-Ressourcen festzulegen. Der Bericht AWS-SOC 1-Typ II und SOC 2-Typ II beschreibt die vorhandenen Kontrollen, um die Zugriffsberechtigungen von AWS-Ressourcen zu verwalten. Das AWS-Produktionsnetzwerk ist vom Amazon-Unternehmensnetzwerk getrennt und erfordert separate Anmeldeinformationen für den logischen Zugriff. Das Amazon-Unternehmensnetzwerk verwendet Benutzer-IDs, Passwörter und Kerberos, während das AWS-Produktionsnetzwerk eine Authentifizierung mit einem öffentlichen SSH-Schlüssel durch einen Bastion-Host erfordert. AWS-Entwickler und Administratoren des Amazon-Unternehmensnetzwerks, die Zugriff auf die AWS-Cloud-Komponenten benötigen, müssen ausdrücklich eine Anforderung auf Zugriff über das AWS-Zugriffsverwaltungssystem stellen. Alle Anforderungen werden vom entsprechenden Verantwortlichen oder Manager überprüft und genehmigt. Konten werden alle 90 Tage überprüft; es ist eine ausdrückliche erneute Überprüfung erforderlich oder der Zugriff auf die Ressource wird automatisch widerrufen. Der Zugriff wird ebenfalls automatisch widerrufen, wenn ein Mitarbeiterdatensatz im Personalverwaltungssystem von Amazon geschlossen wird. Windows- und UNIX-Konten werden deaktiviert und das Zugriffsverwaltungssystem von Amazon entfernt den Benutzer aus allen Systemen. Anforderungen für Zugriffsänderungen werden im Auditprotokoll des Zugriffsverwaltungssystems von Amazon erfasst. Wenn sich die Funktion eines Mitarbeiters ändert, muss der kontinuierliche Zugriff ausdrücklich in der Ressource genehmigt werden, da dieser sonst automatisch widerrufen wird.
B 1.14	Patch- und Änderungsmanagement	AWS hat eine formale, dokumentierte Richtlinie zur Konfigurationsverwaltung implementiert. Diese Richtlinie beschreibt die Zielsetzung, den Umfang, die Rollen, die Verantwortlichkeiten und das Engagement der Unternehmensleitung im Hinblick auf die Konfigurations- und Änderungsverwaltung. Bei jeder Änderung, die an den Systemen und Geräten vorgenommen wird, wird ein Change Management-Ticket (CM, Änderungsverwaltung) erstellt. In diesem CM-Ticket

Baustein ID	Titel	Umsetzung durch AWS
		werden alle Details der Änderung festgehalten. Dazu gehören eine Beschreibung der Änderung, Auswirkungsanalyse, ggf. Sicherheitsüberlegungen, Änderungszeitraum und erforderliche Genehmigungen. Der Änderungsverwaltungsprozess wird von externen Dritten während der Tests für AWS SOC, PCI DSS, ISO 27001 und FedRAMP überprüft und bewertet. AWS ist für das Patchen von Systemen verantwortlich, die das Erbringen des Services für die Kunden unterstützen, wie zum Beispiel die Hypervisoren und Netzwerkdienste. Dies wird entsprechend den AWS-Richtlinien und gemäß den Anforderungen von ISO 27001, NIST und PCI durchgeführt. Die Kunden kontrollieren ihre eigenen Gastbetriebssysteme, -software und -anwendungen und sind aus diesem Grund dafür verantwortlich, ihre eigenen Systeme zu patchen. AWS erfordert kein Abschalten der Systeme, um regelmäßige Wartungsarbeiten und Patch-Vorgänge am System durchzuführen. Die eigenen Wartungsarbeiten und Patch-Vorgänge von AWS bringen in der Regel keine Beeinträchtigungen für die Kunden mit sich. Die Wartung der Instanzen selbst wird vom Kunden kontrolliert. AWS implementiert das Prinzip der geringsten Rechte innerhalb der Infrastrukturkomponenten. AWS unterbindet die Verwendung aller Ports und Protokolle, die keinen speziellen geschäftlichen Zweck erfüllen. AWS verfolgt konsequent den Ansatz der minimalen Implementierung ausschließlich der Merkmale und Funktionen, die für die Verwendung des Geräts notwendig sind. Netzwerkscans werden durchgeführt und unnötige Ports oder Protokolle deaktiviert. Es werden regelmäßig mit verschiedenen Tools interne und externe Schwachstellen-Scans auf dem Host-Betriebssystem, der Webanwendung und den Datenbanken in der AWS-Umgebung vollzogen. Die Schwachstellen-Scans und Wiederherstellungsverfahren von AWS werden regelmäßig auf die Erfüllung der Anforderungen mit PCI DSS und FedRAMP geprüft. Das Amazon-Team für Informationssicherheit und die AWS-Sicherheitsteams abonnieren des Weiteren Newsfeeds zu den entsprechenden Anbieterfehlern von Secunia und TELUS Security Labs. Das Amazon-Team für Informationssicherheit überwacht proaktiv die Websites der Anbieter und andere relevante Quellen für neue Patches. Vor der Implementierung werden die Patches hinsichtlich ihrer Auswirkungen auf die Sicherheit und den Geschäftsbetrieb bewertet und entsprechend der Bewertung zeitgerecht angewendet. Die Kunden kontrollieren ihre eigenen Gastbetriebssysteme, -software und -anwendungen und sind aus diesem Grund dafür verantwortlich, ihre eigenen Schwachstellen-Scans durchzuführen und ihre eigenen Systeme zu patchen. Kunden können eine Genehmigung zur Durchführung von Scans ihrer Cloud-Infrastruktur anfordern, solange diese sich auf die Instanzen des Kunden beschränken und nicht gegen die „AWS Acceptable Use Policy“ von verstoßen.
B 1.15	Löschen und Vernichten von Daten	Wenn die Lebensdauer eines Speichergeräts zu Ende geht, führt AWS einen Prozess zur Außerbetriebnahme durch, der entwickelt wurde, damit Kundendaten nicht an unautorisierte Personen offengelegt werden. AWS wendet die in DoD 5220.22-M ("Betriebshandbuch zum nationalen Branchensicherheitsprogramm") oder NIST 800-88 ("Richtlinien zur Medienbereinigung") beschriebenen Techniken an, um Daten im Rahmen des Prozesses zur Außerbetriebnahme zu zerstören. Wenn ein Hardware-Gerät nicht mithilfe dieser Prozesse außer Betrieb genommen werden kann, dann wird das Gerät entmagnetisiert und physisch den branchenüblichen Vorgehensweisen entsprechend zerstört. Weitere Informationen finden Sie im AWS-Whitepaper "Übersicht über die Sicherheitsprozesse" unter http://aws.amazon.com/security.

Baustein ID	Titel	Umsetzung durch AWS
B 1.16	Anforderungsmanagement	Entsprechend den ISO/IEC 27001-Standards werden die AWS-Hardware-Komponenten einem Verantwortlichen zugewiesen und von den AWS-Mitarbeitern mithilfe AWS-eigener Bestandsverwaltungstools nachverfolgt und überwacht. AWS hat die folgende Maßnahmenliste zusammengestellt, um Bedrohungen in der Lieferkette vorzubeugen, welche wiederum die Ressourcen beeinträchtigen könnten: Agile Beschaffung – Das obere Management von AWS hält eine wöchentliche Besprechung ab, in der festgelegt wird, welche Maßnahmen notwendig sind, um die Geschäftsanforderungen zu erfüllen. Die Einzelposten, die für die Abdeckung der Kapazitätsanforderungen ermittelt wurden, werden in RFQs (Requests for Quotation, Aufforderungen zur Angebotsabgabe) bekanntgegeben und anschließend erworben. Diese häufige Überprüfung der Anforderungen und der daraus erfolgende Angebots- und Akquisitionszyklus führen zu einem wesentlich agileren Akquisitionsprozess, als wenn die Ausgaben für die Einzelposten in einem Jahreszyklus eingeplant werden. Durch diesen Prozess ist es AWS möglich, schnell auf Geschäftsanforderungen zu reagieren. Einzelverträge – Die wöchentlichen Gespräche und häufigen RFQs erlauben eine größere Anzahl kleinerer Verträge, die bei Bedarf erneuert werden. Falls ein Anbieter aus welchem Grund auch immer nicht in der Lage ist, die Lieferung auszuführen, sind die Auswirkungen gering und für die Beschaffung kann leicht eine neue Quelle gefunden werden. Verwendung anerkannter, etablierter, diversifizierter Lieferanten – Dem Eingehen vertraglicher Vereinbarungen, um Hardware, Software, Firmware oder Services zu erwerben, muss eine Unternehmensprüfung (Due Diligence) der Lieferanten vorausgehen. Mehrere Anbieter – Eine Liste zugelassener Anbieter wird vom AWS-Team geführt, jeweils mit mehreren Anbietern zur Auswahl für jeden Komponententyp. Sollte ein Lieferant außerstande sein, die Lieferung auszuführen, kann ein anderer Anbieter für die nächsten Beschaffungsvorgänge verwendet werden. Obwohl ein Großteil des AWS-Systems unternehmensintern entwickelt wurde, um den besonderen AWS-Anforderungen gerecht zu werden, verwendet AWS soweit wie möglich auch standardmäßige, kommerziell erhältliche Informationssystemkonfigurationen und reduziert so die Möglichkeit, Systeme und Produkte zu erwerben, die während der Lieferkettenvorgänge beschädigt wurden. Alle neuen Informationssystemkomponenten für AWS-Rechenzentren erfordern Autorisierung durch die und Benachrichtigung der Rechenzentrumsleitung. Dazu zählen unter anderem Server, Racks, Netzwerkgeräte, Festplatten, Systemhardware-Komponenten und Baustoffe, die an Rechenzentren geliefert und von Rechenzentren in Empfang genommen werden. Die Artikel werden an die Laderampe der einzelnen AWS-Rechenzentren geliefert und dort auf Beschädigungen an Artikel oder Verpackung geprüft sowie von einem Vollzeitmitarbeiter von AWS gegengezeichnet. Jede Lieferung wird gescannt und in das Komponentenverwaltungs- und Inventarsystem von AWS aufgenommen. Eingegangene Artikel werden vor der endgültigen Installation im Rechenzentrum zunächst in einem Lagerraum innerhalb des Rechenzentrums gelagert, zu dem der Zugang nur über Magnetstreifenkarte und PIN-Eingabe möglich ist. Bevor Artikel das Rechenzentrum verlassen können, werden sie gescannt, dokumentiert und bereinigt.

Baustein ID	Titel	Umsetzung durch AWS
B2 Infrastruktur		
B 2.1	Allgemeines Gebäude	AWS-Rechenzentren sind in unauffälligen Anlagen untergebracht und sind nicht für die Öffentlichkeit zugänglich. Die AWS-Rechenzentren sind mit physischen Schutzmaßnahmen gegen Umweltrisiken ausgerüstet. Die von AWS implementierten physischen Schutzmaßnahmen gegen Umweltrisiken wurden von einem unabhängigen Auditor geprüft und es wurde zertifiziert, dass sie mit den in ISO/IEC 27002 aufgelisteten bewährten Methoden übereinstimmen. Die Rechenzentren verfügen über Branderkennungs- und Brandbekämpfungsmechanismen. Die Branderkennungs- sowie Brandbekämpfungssysteme in den Rechenzentren bestehen aus Feuerlöschgeräten und VESDA-Rauchmeldern (Very Early Smoke Detection Apparatus, Brandfrühesterkennungs-Systeme). Die Branderkennungs- und Brandbekämpfungssysteme werden im Fall eines Stromausfalls durch eine unabhängige Notstromversorgung gespeist. Sollte ein Brandbekämpfungssystem eingesetzt werden, verfügt AWS über die notwendigen Kapazitäten, um den Betrieb in ein anderes Rechenzentrum umzuleiten. Die Verfahren, die bei der Schließung eines Rechenzentrums zur Anwendung kommen, umfassen auch ausführliche Informationen darüber, wie ein Rechenzentrum zu schließen und der Verkehr zu einem anderen Rechenzentrumcluster oder einer anderen Region umzuleiten ist. AWS verwendet für das Informationssystem Branderkennungsgeräte/-systeme, die automatisch aktiviert werden und im Falle eines Feuers die Organisation und die Notfall-Einsatzkräfte benachrichtigen. AWS-Rechenzentren werden gruppenweise in verschiedenen Regionen der Welt errichtet. Alle Rechenzentren sind online und bedienen Kunden; kein Rechenzentrum ist abgeschaltet. Bei einem Ausfall verschieben automatische Prozesse den Kundendatenverkehr weg von den betroffenen Bereichen. Die Kernanwendungen werden in einer N+1-Konfiguration bereitgestellt, sodass im Falle eines Rechenzentrumsausfalls ausreichend Kapazität vorhanden ist, um den Datenverkehr lastverteilt an die verbleibenden Standorte zu verteilen. AWS bietet Kunden die Flexibilität, Instanzen zu platzieren und Daten innerhalb mehrerer geografischer Regionen sowie über mehrere Availability Zones innerhalb der einzelnen Regionen zu speichern. Jede Availability Zone wurde als unabhängige Ausfallszone entwickelt. Dies bedeutet, dass Availability Zones innerhalb einer typischen Stadtregion physisch verteilt sind und sich in Gebieten mit niedrigerem Überschwemmungsrisiko befinden (je nach Region gibt es unterschiedliche Überschwemmungszonen-Kategorisierungen). Zusätzlich zu einer eigenständigen unterbrechungsfreien Stromversorgung und Notstromgeneratoren vor Ort werden alle Availability Zones über unterschiedliche Stromnetze von unabhängigen Stromversorgern gespeist, um Einzelfehlerstellen zu minimieren. Sämtliche Availability Zones sind redundant mit mehreren Tier-1-Transit-Providern verbunden. Kunden sollten die Architektur ihrer AWS-Nutzung so erstellen, dass sie mehrere Regionen und Availability Zones umfasst. Durch das Verteilen von Anwendungen über mehrere Availability Zones bleibt die Architektur bei den meisten Ausfallarten, einschließlich Naturkatastrophen oder Systemausfällen, stabil. Der physische Zugang zu den Rechenzentren wird durch das elektronische AWS-Zugangskontrollsystem überwacht. Für den Zugang in das Gebäude und die Räume setzt sich das System aus Kartenlesern und PIN-Pads zusammen, für das Verlassen besteht es nur aus Kartenlesern. Durch die Verwendung von Kartenlesern beim Verlassen von Gebäuden und Räumen treten Doppelzutrittssperren in Kraft, die sicherstellen, dass autorisierte Personen nicht von unautorisierten Personen verfolgt werden, die sich so ohne Ausweis Zutritt verschaffen. Zusätzlich zum Zugangskontrollsystem sind alle Eingänge der AWS-Rechenzentren, einschließlich des Haupteingangs, der Laderampe und aller Dachausstiege/-luken, mit Einbruchmeldevorrichtungen versehen, die einen Alarm auslösen, sobald die Tür aufgebrochen oder aufgehalten wird. Neben den elektronischen Mechanismen verwenden die AWS-Rechenzentren rund um die Uhr auch ausgebildete

Baustein ID	Titel	Umsetzung durch AWS
		Sicherheitskräfte, die sowohl innerhalb der Gebäude als auch in deren Umgebung stationiert sind. Innerhalb des Systems wird der Zugang zu den Rechenzentren nur nach Notwendigkeit erteilt; alle physischen Zugangsanfragen werden vom zuständigen AAM (Area Access Manager, Zutrittsmanager) überprüft und genehmigt. AWS-Rechenzentren sind in unauffälligen Anlagen untergebracht und sind nicht für die Öffentlichkeit zugänglich. Der physische Zugang wird sowohl in der Umgebung als auch an den Zutrittspunkten zum Gebäude streng kontrolliert. AWS gewährt nur solchen Anbietern, Auftragnehmern und Besuchern Zugang und Informationen zu den Rechenzentren, für die eine legitime geschäftliche Notwendigkeit besteht, wie Notfallreparaturen. Alle Besucher der Rechenzentren müssen vorab durch den zuständigen Zutrittsmanager (AAM) autorisiert worden sein und im AWS-Ticketmanagementsystem dokumentiert werden. Bei der Ankunft am Rechenzentrum müssen sie sich ausweisen und anmelden, bevor ihnen ein Besucherausweis ausgestellt wird. Während sie sich im Rechenzentrum befinden, werden sie beständig von autorisiertem Personal begleitet. Weitere Informationen finden Sie in den Berichten AWS SOC 1-Typ II und SOC 2-Typ II – Sicherheit. Außerdem enthält ISO/IEC 27001, Anhang A.11.2, zusätzliche Informationen. AWS wurde durch einen unabhängigen Auditor auf Erfüllung der ISO/IEC 27001-Zertifizierungsanforderungen geprüft.
B 2.2	Elektrotechnische Verkabelung	Die internen AWS-Verkabelungsverfahren regeln, wie AWS die Verkabelungsanforderungen kategorisiert, implementiert und verwaltet. AWS-Komponentenkennzeichnungen sind kundenunabhängig und dienen der Inventarisierung der Hardware innerhalb des AWS-Tools zur Komponentenverwaltung. In den AWS-Rechenzentren wird die Hardware normalerweise nicht physisch speziellen Kunden oder den auf der Hardware gespeicherten Daten zugeordnet. Alle Kundendaten werden unabhängig von ihrer Quelle als kritisch angesehen und aus diesem Grund werden alle Medien vertraulich behandelt. Die Prozesse und Vorgänge der AWS-Komponentenverwaltung werden von unabhängigen, externen Auditoren während der Prüfungen bezüglich der Compliance mit PCI DSS, ISO/IEC 27001 und FedRAMP überprüft.
B 2.9	Rechenzentrum	AWS-Rechenzentren sind in unauffälligen Anlagen untergebracht und sind nicht für die Öffentlichkeit zugänglich. Die AWS-Rechenzentren sind mit physischen Schutzmaßnahmen gegen Umweltrisiken ausgerüstet. Die von AWS implementierten physischen Schutzmaßnahmen gegen Umweltrisiken wurden von einem unabhängigen Auditor geprüft und es wurde zertifiziert, dass sie mit den in ISO/IEC 27002 aufgelisteten bewährten Methoden übereinstimmen. Die Rechenzentren verfügen über Branderkennungs- und Brandbekämpfungsmechanismen. Die Branderkennungs- sowie Brandbekämpfungssysteme in den Rechenzentren bestehen aus Feuerlöschgeräten und VESDA-Rauchmeldern (Very Early Smoke Detection Apparatus, Brandfrühesterkennungs-Systeme). Die Branderkennungs- und Brandbekämpfungssysteme werden im Fall eines Stromausfalls durch eine unabhängige Notstromversorgung gespeist. Sollte ein Brandbekämpfungssystem eingesetzt werden, verfügt AWS über die notwendigen Kapazitäten, um den Betrieb in ein anderes Rechenzentrum umzuleiten. Die Verfahren, die bei der Schließung eines Rechenzentrums zur Anwendung kommen, umfassen auch ausführliche Informationen darüber, wie ein Rechenzentrum zu schließen und der Verkehr zu einem anderen Rechenzentrumcluster oder einer anderen Region umzuleiten ist. AWS verwendet für das Informationssystem Branderkennungsgeräte/-systeme, die automatisch aktiviert werden und im Falle eines Feuers die Organisation und die Notfall-Einsatzkräfte benachrichtigen. AWS-Rechenzentren werden gruppenweise in verschiedenen Regionen der Welt errichtet. Alle Rechenzentren sind online

Baustein ID	Titel	Umsetzung durch AWS
		und bedienen Kunden; kein Rechenzentrum ist abgeschaltet. Bei einem Ausfall verschieben automatische Prozesse den Kundendatenverkehr weg von den betroffenen Bereichen. Die Kernanwendungen werden in einer N+1-Konfiguration bereitgestellt, sodass im Falle eines Rechenzentrumsausfalls ausreichend Kapazität vorhanden ist, um den Datenverkehr lastverteilt an die verbleibenden Standorte zu verteilen. AWS bietet Kunden die Flexibilität, Instanzen zu platzieren und Daten innerhalb mehrerer geografischer Regionen sowie über mehrere Availability Zones innerhalb der einzelnen Regionen zu speichern. Jede Availability Zone wurde als unabhängige Ausfallszone entwickelt. Dies bedeutet, dass Availability Zones innerhalb einer typischen Stadtregion physisch verteilt sind und sich in Gebieten mit niedrigerem Überschwemmungsrisiko befinden (je nach Region gibt es unterschiedliche Überschwemmungszonen-Kategorisierungen). Zusätzlich zu einer eigenständigen unterbrechungsfreien Stromversorgung und Notstromgeneratoren vor Ort werden alle Availability Zones über unterschiedliche Stromnetze von unabhängigen Stromversorgern gespeist, um Einzelfehlerstellen zu minimieren. Sämtliche Availability Zones sind redundant mit mehreren Tier-1-Transit-Providern verbunden. Kunden sollten die Architektur ihrer AWS-Nutzung so erstellen, dass sie mehrere Regionen und Availability Zones umfasst. Durch das Verteilen von Anwendungen über mehrere Availability Zones bleibt die Architektur bei den meisten Ausfallarten, einschließlich Naturkatastrophen oder Systemausfällen, stabil. Der physische Zugang zu den Rechenzentren wird durch das elektronische AWS-Zugangskontrollsystem überwacht. Für den Zugang in das Gebäude und die Räume setzt sich das System aus Kartenlesern und PIN-Pads zusammen, für das Verlassen besteht es nur aus Kartenlesern. Durch die Verwendung von Kartenlesern beim Verlassen von Gebäuden und Räumen treten Doppelzutrittssperren in Kraft, die sicherstellen, dass autorisierte Personen nicht von unautorisierten Personen verfolgt werden, die sich so ohne Ausweis Zutritt verschaffen. Zusätzlich zum Zugangskontrollsystem sind alle Eingänge der AWS-Rechenzentren, einschließlich des Haupteingangs, der Laderampe und aller Dachausstiege/-luken, mit Einbruchmeldevorrichtungen versehen, die einen Alarm auslösen, sobald die Tür aufgebrochen oder aufgehalten wird. Neben den elektronischen Mechanismen verwenden die AWS-Rechenzentren rund um die Uhr auch ausgebildete Sicherheitskräfte, die sowohl innerhalb der Gebäude als auch in deren Umgebung stationiert sind. Innerhalb des Systems wird der Zugang zu den Rechenzentren nur nach Notwendigkeit erteilt; alle physischen Zugangsanfragen werden vom zuständigen AAM (Area Access Manager, Zutrittsmanager) überprüft und genehmigt. AWS-Rechenzentren sind in unauffälligen Anlagen untergebracht und sind nicht für die Öffentlichkeit zugänglich. Der physische Zugang wird sowohl in der Umgebung als auch an den Zutrittspunkten zum Gebäude streng kontrolliert. AWS gewährt nur solchen Anbietern, Auftragnehmern und Besuchern Zugang und Informationen zu den Rechenzentren, für die eine legitime geschäftliche Notwendigkeit besteht, wie Notfallreparaturen. Alle Besucher der Rechenzentren müssen vorab durch den zuständigen Zutrittsmanager (AAM) autorisiert worden sein und im AWS-Ticketmanagementsystem dokumentiert werden. Bei der Ankunft am Rechenzentrum müssen sie sich ausweisen und anmelden, bevor ihnen ein Besucherausweis ausgestellt wird. Während sie sich im Rechenzentrum befinden, werden sie beständig von autorisiertem Personal begleitet. Weitere Informationen finden Sie in den Berichten AWS SOC 1-Typ II und SOC 2-Typ II – Sicherheit. Außerdem enthält ISO/IEC 27001, Anhang A.11.2, zusätzliche Informationen. AWS wurde durch einen unabhängigen Auditor auf Erfüllung der ISO/IEC 27001-Zertifizierungsanforderungen geprüft.
B 2.12	IT-Verkabelung	Die internen AWS-Verkabelungsverfahren regeln, wie AWS die Verkabelungsanforderungen kategorisiert, implementiert und verwaltet.

Baustein ID	Titel	Umsetzung durch AWS
		AWS-Komponentenkennzeichnungen sind kundenunabhängig und dienen der Inventarisierung der Hardware innerhalb des AWS-Tools zur Komponentenverwaltung. In den AWS-Rechenzentren wird die Hardware normalerweise nicht physisch speziellen Kunden oder den auf der Hardware gespeicherten Daten zugeordnet. Alle Kundendaten werden unabhängig von ihrer Quelle als kritisch angesehen und aus diesem Grund werden alle Medien vertraulich behandelt. Die Prozesse und Vorgänge der AWS-Komponentenverwaltung werden von unabhängigen, externen Auditoren während der Prüfungen bezüglich der Compliance mit PCI DSS, ISO/IEC 27001 und FedRAMP überprüft.
B 3 IT-Systeme		
B 3.101	Allgemeiner Server	AWS hat eine formale, dokumentierte Richtlinie zur Konfigurationsverwaltung implementiert. Diese Richtlinie beschreibt die Zielsetzung, den Umfang, die Rollen, die Verantwortlichkeiten und das Engagement der Unternehmensleitung. Ein Konfigurationsverwaltungs-Tool wird zur Verwaltung von bereitstellbarer Software in Paketen, Paketgruppen und Umgebungen verwendet. Bei einem Paket handelt es sich um eine Sammlung zusammenhängender Dateien, z. B. eng miteinander verknüpfte Software oder verknüpfter Content. Mehrere Pakete, die oft gemeinsam bereitgestellt werden, werden als Paketgruppe bezeichnet. Eine Umgebung schließlich ist eine Kombination von Paketen und Paketgruppen, die in einer Gruppe von Hostklassen (Hosts oder Servern mit derselben Funktion) bereitgestellt werden. Eine Umgebung stellt die Gesamtheit aller Pakete dar, die zur Ausführung einer bestimmten Funktion durch den Server erforderlich sind. AWS sorgt für die die Verteilung des Basis-OS, das auf den Hosts verwendet wird. Ports, Protokolle und Services, die nicht benötigt werden, sind in den Basis-Builds deaktiviert. Mithilfe der Build-Tools fügen die Serviceteams nur die zugelassenen Softwarepakete hinzu, die zur Serverfunktion gemäß den Basiskonfigurationen notwendig sind. Die Server werden regelmäßig gescannt und unnötige Ports oder Protokolle werden mithilfe des Nachbesserungsprozesses behoben. Bereitgestellte Software durchläuft wiederholte Penetrationstests, die durch ausgewählte Branchenexperten ausgeführt werden. Die aus den jährlichen Penetrationstests resultierenden Nachbesserungen werden über den Nachbesserungsprozess ebenfalls in die Basiskonfiguration aufgenommen. AWS implementiert das Prinzip der geringsten Rechte innerhalb der Infrastrukturkomponenten. AWS unterbindet die Verwendung aller Ports und Protokolle, die keinen speziellen geschäftlichen Zweck erfüllen. AWS verfolgt konsequent den Ansatz der minimalen Implementierung ausschließlich der Merkmale und Funktionen, die für die Verwendung des Geräts notwendig sind. Es werden Netzwerk-Scans durchgeführt und unnötige Ports oder Protokolle deaktiviert. Administratoren, die aus geschäftlichen Gründen Zugriff auf die Verwaltungsebene benötigen, müssen die Multi-Factor Authentication verwenden, um Zugriff auf speziell erstellte administrative Hosts zu erhalten. Diese administrativen Hosts sind Systeme, die speziell zum Schutz der Verwaltungsebene der Cloud entwickelt, erstellt, konfiguriert und gehärtet wurden. Jeder Zugriff wird protokolliert und geprüft. Sobald für einen Mitarbeiter keine geschäftliche Notwendigkeit mehr für den Zugriff auf die Verwaltungsebene besteht, werden die Privilegien und die Zugriffsberechtigung für diese Hosts und relevante Systeme widerrufen.
B 3.302	Router und Switches	AWS-Systeme befinden sich in einem Sicherheitsbereich innerhalb von AWS-gesteuerten Rechenzentren. Der Zugriff auf diese Systeme ist nur über SSH und Multi-Factor Authentication möglich. AWS verwendet Bastion-Hosts, um den Zugriff

Baustein ID	Titel	Umsetzung durch AWS
		auf Netzwerkgeräte und andere Komponenten der Infrastruktur zu beschränken. Zusätzlich zu den Bastion-Hosts enthalten alle Netzwerkgeräte ACLs, und ein SSH-Zugriff ist nur auf Netzwerkgeräte bestimmter Bastion-Hosts möglich. AWS isoliert Netzwerke logisch mithilfe von Boundary Devices, die die ein- und ausgehende Kommunikation auf einen autorisierten Verkehrsfluss begrenzen. AWS isoliert Informationssicherheits-Tools, Sicherheitsmechanismen und Unterstützungskomponenten von anderen internen Komponenten des Informationssystems über logisch getrennte Teilnetze, die von den Instanzen und dem Datenverkehr des Kunden getrennt sind. Alle Hosts, die Informationssicherheits-Tools, Sicherheitsmechanismen und Unterstützungskomponenten enthalten, gehören zu separaten Sicherheits-Host-Klassen, die Zugriffs- und andere Berechtigungen auf Sicherheits-Hosts von denen auf andere Arten von Produktions-Servern isolieren. Der Zugriffs und die Berechtigungen auf Sicherheit-Hosts werden vom AWS-Sicherheitsteam strikt überwacht. AWS verfügt nur über eine begrenzte Anzahl von Zugriffspunkten auf das Informationssystem, um eine möglichst umfassende Überwachung des eingehenden und ausgehenden Netzwerkverkehrs und der Kommunikation zu ermöglichen. Diese Zugriffspunkte für Kunden werden API-Endpunkte genannt. Sie ermöglichen dem Kunden den Aufbau sicherer Kommunikationssitzungen mit ihren Speicher- oder Datenverarbeitungs-Instanzen innerhalb von AWS. In diesen Zugriffspunkten wird der eingehende und ausgehende Datenverkehr überwacht, um die Service-Verfügbarkeit sicherzustellen. AWS hat Netzwerkgeräte implementiert, die für die Verwaltung der Schnittstellenkommunikation mit Internetdienstanbietern (Internet Service Provider, ISPs) vorgesehen sind. AWS verwendet eine redundante Verbindung zu mehr als einem Kommunikations-Service an jeder mit dem Internet verbundenen Stelle des AWS-Netzwerks. Jede dieser Verbindungen verfügt über eigene Netzwerkgeräte. Die nachstehend aufgeführten Sicherheitskontrollen dienen zum Schutz der Vertraulichkeit und Integrität der übertragenen Informationen. Diese Sicherheitskontrollen werden alle 6 Monate auf operative Wirksamkeit hin überprüft. - Firewall-Geräte sind so konfiguriert, dass sie den Zugriff auf die Computerumgebung beschränken und die Abgrenzung der Computing-Cluster verstärken. - Firewall-Richtlinien (Konfigurationsdateien) werden automatisch alle 24 Stunden in das Netzwerk übertragen. - Die Aktualisierungen der Firewall-Richtlinien werden überprüft und genehmigt. - Netzwerkgeräte werden von AWS so konfiguriert, dass ein Zugriff nur auf bestimmte Ports auf anderen Systemen innerhalb von AWS möglich ist. AWS hat eine Konfigurationsverwaltung entwickelt und dokumentiert. AWS implementiert den AWS Configuration Management-Plan für Systeme und Geräte innerhalb der AWS- Systemgrenze. Der AWS Configuration Management-Plan beschreibt die Rollen, die Verantwortlichkeiten sowie die Prozesse und Prozeduren der Konfigurationsverwaltung. Der

Baustein ID	Titel	Umsetzung durch AWS
		AWS CM-Plan definiert detailliert das Verfahren zur Verwaltung der Konfigurationselemente von Produktionssystemen. AWS identifiziert Konfigurationselemente nach einer Änderung bezüglich System, Service, DB-Schema oder Umgebung, die Einfluss auf ein anderes Team, Service oder Website haben kann, oder wenn andere Gruppen innerhalb von AWS die Änderung kennen müssen. Zu solchen Änderungen gehören Modifikationen an Konfigurationseinstellungen, Paketen, Paketgruppen oder Umgebungen auf Systemen oder Geräten innerhalb der Systemgrenze. Alle Änderungsarten werden im AWS Configuration Management-Plan berücksichtigt.
B 3.304	Virtualisierung	AWS verwendet Virtualisierungstechniken zur Bereitstellung von Informationssystemkomponenten anstelle anderer Arten von Komponenten oder von Komponenten mit unterschiedlichen Konfigurationen. Dazu gehören virtuelle Netzwerkgeräte und Host-basierte Firewalls, die Verkehrsflusseinschränkungen über ACLs in EC2 und VPC steuern (und in EC2-Instanzen, die eine Vielzahl von Betriebssystemen umfassen). Wo virtuelle Compute-Instanzen mehrerer Kunden auf einem Host vorhanden sind, werden Systemressourcen für jeden Kunden entsprechend seiner ursprünglichen Einrichtung zugeordnet. Die Zuordnung von Systemressourcen erfolgt mittels Virtualisierungssoftware, wobei der Umfang der Systemressourcen, die jeden Kunden zugewiesen werden, abhängig ist von den Parametern, die der Kunde bei der ursprünglichen Einrichtung der Systemressourcen verwendet hat. Ein zentraler Region-by-Region-Server ermöglicht Aggregation und Verkehrslenkung pro Kunde. Wenn ein Kunde so viele Netzwerkgeräte belegt, dass dies Auswirkungen auf andere Kunden hat, drosselt AWS den Netzwerkverkehr dieses Kunden. Der Service überwacht und aggregiert Daten pro Minute. Die Drossel wird jede Minute zurückgesetzt, bis der Durchsatz wieder einen akzeptablen Wert erreicht.
B 5 Anwendungen		
B 5.22	Protokollierung	AWS hat für alle Systeme und Geräte innerhalb des AWS-Systems, für die AWS zuständig ist, auditierbare Ereigniskategorien ermittelt. Service-Teams konfigurieren die Auditfunktionen so, dass sicherheitsrelevante Ereignisse fortlaufend gemäß den Anforderungen aufgezeichnet werden. Das Protokollspeichersystem ist dafür ausgelegt, einen hoch skalierbaren und hoch verfügbaren Service zu bieten, dessen Kapazität bei steigendem Protokollspeicherbedarf automatisch erweitert wird. Die Auditdaten enthalten eine Gruppe von Datenelementen, die die erforderlichen Analyseanforderungen unterstützen. Zusätzlich stehen sie dem AWS-Sicherheitsteam oder anderen relevanten Teams bei Bedarf zur Prüfung oder Analyse und für die Behebung sicherheitsrelevanter oder geschäftsschädigender Ereignisse zur Verfügung. Mitarbeiter des AWS-Teams erhalten automatisierte Benachrichtigungen, wenn Fehler in überwachten Prozessen auftreten. Dazu gehören unter anderem Software- oder Hardwarefehler. Nach Erhalt einer Fehlermeldung stellen die benachrichtigten Mitarbeiter ein Fehlerticket aus und behandeln das Problem, bis es gelöst ist. Die Kunden kontrollieren ihre eigenen Gastbetriebssysteme, ihre Software und ihre Anwendungen und sind aus diesem Grund dafür verantwortlich, eine Überwachung der logischen Zustände dieser Systeme zu entwickeln. In Übereinstimmung mit ISO/IEC 27001-Standards verwenden AWS-Informationssysteme interne, über NTP (Network Time Protocol) synchronisierte Systemuhren. AWS CloudTrail bietet eine einfache Lösung, um Benutzeraktivitäten aufzuzeichnen, sodass möglicherweise kein

Baustein ID	Titel	Umsetzung durch AWS
		komplexes Logging-System erforderlich ist. Weitere Informationen finden sich unter "aws.amazon.com/cloudtrail". AWS Cloudwatch ermöglicht die Überwachung von Ressourcen in der AWS-Cloud und von Anwendungen, die Benutzer auf AWS ausführen. Weitere Informationen finden sich unter "aws.amazon.com/cloudwatch". AWS veröffentlicht aktuelle Informationen über Service-Verfügbarkeit in der Übersicht zum Servicestatus. Weitere Informationen finden Sie unter "http://status.aws.amazon.com/".
B 5.23	Cloud Management	AWS Services umfasst AWS Regions, Availability Zones (AZs) und Dienste, die die Anwendungsarchitektur des Kunden unterstützen. Die Services sind in allen Availability Zones gleichartig vorhanden. Dienste können für Wiederherstellungs- und Verfügbarkeitszwecke zwischen AZs und Regionen kommunizieren. Kundenanwendungen setzen auf die Standard AWS Services auf und werden als außerhalb des Sicherheitsbereichs von AWS liegend betrachtet. Kunden sind dafür verantwortlich die Sicherheitsmaßnahmen innerhalb ihrer Anwendungen zu verwalten. Kunden, die Verbindungen zu AWS Webseiten und API Schnittstellen aufbauen, die als Teil von der Webseiten von AWS Anwendungen zu betrachten sind, sowie die Inhaber von Webseiteninhalten, gelten als außerhalb des Sicherheitsbereichs von AWS liegend. AWS Administratoren sind ebenfalls außerhalb des Sicherheitsbereichs, und verwenden sichere Fernzugangsmethoden um AWS Systeme zu betreiben und zu warten. **AWS Regions** Ein benannter Satz von AWS-Ressourcen im gleichen geografischen Gebiet. Jede Region enthält mehrere Availability Zones. **Availability Zones** Amazon EC2-Standorte bestehen aus Regionen und Availability Zones. Availability Zones sind eigenständige Standorte, die so konzipiert sind, dass sie vor Ausfällen in anderen Availability Zones geschützt sind, und eine kostengünstige Netzwerkkonnektivität mit geringer Latenz zu anderen Availability Zones in der gleichen Region bereitstellen. **AWS Services** Jede Availability Zone bietet eine identische IaaS Cloud-Plattform, die Rechenleistung (Elastic Compute Cloud), Speicherplatz (Elastic Block Storage, Simple Storage Service), sichere Kommunikation (Virtual Private Cloud) und weitere Funktionen zur Verfügung stellen, womit es Kunden ermöglicht wird, kosteneffizient Anwendungen und Services mit hoher Flexibilität, Skalierbarkeit und Zuverlässigkeit einzusetzen. Durch den AWS Self Service können Kunden proaktiv interne Planungen umsetzen und schnell auf externe Anforderungen reagieren. Dadurch bietet AWS den Kunden die Option, nur die benötigten Services zu nutzen, sowie die Möglichkeit, genutzte Services nach Bedarf vorzuhalten oder aufzulösen. **AWS Infrastruktur** AWS bietet Einrichtungen, Hardware und Sicherheitsfunktionen auf Infrastrukturebene. Im IaaS-Modell ist AWS

Baustein ID	Titel	Umsetzung durch AWS
		verantwortlich für relevante Schichten der Servicebereitstellung, darunter Infrastruktur (d.h. Hardware und Software, die Teil der Infrastruktur ist) und Service Management Prozesse (d.h. Betrieb und Management der Infrastruktur und die System- und Softwareentwicklungszyklen). Kunden können darauf vertrauen, dass AWS die Cloud Infrastruktur verwaltet, einschließlich Netzwerk, Datenspeicher, Systemressourcen, Rechenzentren, Sicherheit, Verfügbarkeit und unterstützender Hard- und Software. **Simple Storage Service (S3)** Bei Amazon S3 handelt es sich um Speicher für das Internet. S3 ist ein hochskalierbar, dauerhafter und verfügbarer verteilter Objektspeicher für geschäftskritische und primäre Speicheranwendungen. S3 speichert Daten redundant in mehreren Systemen und auf mehreren Geräten in jedem System. S3 bietet Schutz sowohl vor logischen als auch vor physischen Ausfällen und schützt so vor Datenverlusten durch unbeabsichtigte Benutzeraktionen, Anwendungsfehler und Infrastrukturausfälle. Die Versionierung ermöglicht es, früherer Versionen aller Objekte in Ihrem Amazon S3 Bucket zu speichern, abzurufen oder wiederherzustellen. Auf diese Weise ist die Wiederherstellung nach unbeabsichtigten Nutzeraktionen oder Anwendungsausfällen problemlos möglich. Die Versionierung kann für jeden S3 Bucket aktiviert werden. **Elastic Compute Cloud (EC2)** EC2 ist ein Web-Service, der anpassbare Rechenkapazität in der Cloud bietet. Dabei handelt es sich im Kern um Serverinstanzen zum Erstellen und Betreiben von Anwendungssystemen. EC2 ist darauf ausgelegt, Entwicklern und Kunden das Aufspielen virtueller Maschinen zu erleichtern. Mit der einfachen Web-Service-Oberfläche von EC2 können Kunden mühelos Kapazität erhalten und konfigurieren. Sie ermöglicht die vollständige Kontrolle über Rechenressourcen. EC2 ermöglicht Unternehmen, große Ausgaben zu vermeiden, indem nur für die tatsächlich genutzten Kapazitäten gezalt wird. **Elastic Block Store (EBS)** EBS bietet Volumes auf Blockebene zur Verwendung mit EC2 Instanzen. Daten auf einem Amazon EBS-Volume werden unabhängig von der Nutzungsdauer der Instanz dauerhaft gespeichert. EBS bietet hochverfügbare, zuverlässige Speichervolumes die mit laufenden EC2 Instanzen verbunden oder als Laufwerk innerhalb von Instanzen verfügbar gemacht werden können. EBS ist besonders für Anwendungen geeignet, die eine Datenbank, ein Dateisystem, oder Zugriff auf Speicher auf Blockebene erfordern. EBS Volumes speichern Informationen redundant, womit sie robuster sind als typische Festplatten. Die jährliche Fehlerrate für ein EBS Volume liegt bei 0,1% bis 0,5%, verglichen mit 4% für eine gängige Festplatte. EBS und EC2 werden häufig gemeinsam verwendet, wenn eine Anwendung auf der AWS Plattform erstellt wird. Informationen, die persistent sein müssen, können auf EBS Volumes gespeichert werden, und nicht auf dem flüchtigen Speicher, der EC2 Instanzen zugeordnet ist. Falls die EC2 Instanz ausfällt und ersetzt werden muss, kann das EBS Volume einfach der neuen EC2 Instanz zugeordnet werden. Da die neue Instanz ein Duplikat des Originals ist, gehen weder

Baustein ID	Titel	Umsetzung durch AWS
		Informationen noch Funktionalitäten verloren. EBS Volumes sind hochzuverlässig, aber um die Möglichkeit eines Ausfalls weiter zu verringern, können Datensicherungen (sog. Snapshots) dieser Volumes erstellt werden. Eine zuverlässige Backupstrategie würde Backups, Aufbewahrungsfristen und Wiederherstellungspläne umfassen. Snapshots können für hohe Dauerhaftigkeit in Simple Storage Service (S3) gespeichert werden. Snapshots können verwendet werden, um neue EBS Volumes zu erstellen, die eine exakte Kopie des Originals zu dem Zeitpunkt sind, an dem der Snapshot erstellt wurde. Diese EBS Transaktionen können durch API Calls abgewickelt werden. **Virtual Private Cloud (VPC)** Amazon Virtual Private Cloud (Amazon VPC) ermöglicht die Bereitstellung eines logisch isolierten Bereichs der AWS-Cloud, in dem Rechen- und Speicherressourcen betrieben werden, die mit einer bestehenden Kundeninfrastruktur durch ein Virtuelles Privates Netzwerk (VPN) oder das Internet verbunden werden können. VPC ermöglicht es, bestehende Verwaltungsressourcen und Dienste wie DNS, LDAP, Active Directory, Firewalls und Intrusion Detection Systeme auf private AWS Ressourcen auszudehnen, und so einheitliche Schutzmaßnahmen zu gewährleisten, unabhängig davon, ob Informationen auf internen IT Ressourcen oder in der AWS-Cloud liegen. Die Nutzung von VPC ermöglicht die Transition in die Cloud, unter Nutzung des kundenspezifischen Rechenzentrumsmodells und Managementsystems. VPC erlaubt es, AWS Ressourcen als virtuelles Rechenzentrum zu nutzen, das sich an die existierenden IP-Adressräume und Infrastrukturen des Kunden anlehnt. Der Kunde kontrolliert die private Cloud, einschließlich IP Adressen, Subnetzen, Firewallregeln, VPN und/oder Internet Gateways, Zugangskontrolllisten und Routing.
B 5.24	Web-Services	EC2, EBS und VPC Hosts und Laufwerke befinden sich im EC2 Netzwerk. API Endpunkte und S3 Hosts und Laufwerke befinden sich im Prod Netzwerk. Der Internetzugang erfolgt über das Border/LBE Netzwerk. Das NAP Netzwerk bietet Konnektivität zwischen Rechenzentren sowie den Zugangspfad für AWS Administratoren. Alle diese Netzwerke befinden sich innerhalb der Autorisierungsgrenzen. Jede Region ist mit den Border und NAP Netzwerken verbunden, um Internet- und auch AWS Administrationsverbindungen herstellen zu können. Jeder erlaubte Datenverkehr wird spezifisch autorisiert und mittels Zugangskontrolllisten überprüft. Regionen werden mittels mehrerer Rechenzentren umgesetzt nd die verschiedenen Netzwerke verbinden sich zu ihren Gegenstellen in den anderen Rechenzentren. Beispielsweise verbindet sich das EC2 Netzwerk eines Rechenzentrums zu den EC2 Netzwerken der anderen Rechenzentren. **Datenfluss** Kunden senden API Aufrufe an AWS API Endpunkte, um Speicherplatz (Buckets, Objekte und Volumes), Recheninstanzen und VPC Umgebungen zu schaffen und zu verwalten. API Endpunkte können mittels http und https erreicht werden. Verbindungen, die https verwenden, sind auf jeder Art von API Endpunkt verfügbar. S3 Endpunkte bieten darüber hinaus die Möglichkeit, nichtvertrauliche Informationen mittels http zu übertragen. Dies kann beispielsweise genutzt werden, um Informationen zu speichern, die auf öffentlichen Webseiten dargestellt werden sollen. Kunden können VPC Umgebungen zu ihren existierenden Netzwerk-Infrastrukturen verbinden, indem eine site-to-site IPSEC VPN Verbindung genutzt wird. Da Kunden für ihre VPC Umgebungen die IP-Adressen, VLANs und Zugangskontrolllisten definieren, kann dadurch ein zulässiger Kommunikationsfluss zwischen dem Kundennetzwerk und ihrer VPC mittels eines sicheren Übertragungsweges

aufgebaut werden. Kunden können darüber hinaus eine Internetverbindung für ihre VPC Umgebung festlegen. Der Kunde legt die internen IP-Adressen, VLANs und Zugangskontrolllisten für seine VPC-Umgebungen fest, womit eine Festlegung der zulässigen Kommunikation vom Internet zu den Kundenressourcen möglich wird.

Ports, Protokolle und Dienste

Die untenstehende Tabelle listet die Ports, Protokolle und Dienste auf, die in diesem Informationssystem aktiv sind. TCP Ports werden mit einem T ausgewiesen, während UDP Ports anhand eines U kenntlich sind.

Ports (T or U)	Protokolle	Dienste	Zweck	genutzt von
80, 443 T	HTTP und HTTPS	Kommunikation mit API Endpunkten	Erstellen und Verwalten von IaaS-Implementierungen	S3,EC2, EBS, VPC Administratoren, Kunden
22 T	SSH	Fernzugang	Verwaltung von Hosts und NetzlaufwerkenVerwaltung von EC Instanzen	S3,EC2, EBS, VPC Administratoren, Kunden
53 U	DNS	Domain Name Services	Namensauflösung zu IP-Adressen	S3,EC2, EBS, VPC Alle Benutzer
N/A	AH und ESP (dies sind Transportprotokolle ohne Ports)	IPSEC VPN	Site to Site VPN-Verbindungen des Kunden zu VPC-Umgebungen des Kunden	VPC Kunden

AWS Referenz Architekturen

Durch die Flexibilität von AWS können Kunden ihre Anwendungsarchitekturen so gestalten, wie es erforderlich ist. AWS-Referenzarchitekturen bieten den Kunden die architektonische Orientierung, die sie benötigen, um eine Anwendung aufzubauen, die alle Vorteile der AWS-Services nutzt und gleichzeitig die unterschiedlichen Sicherheits- und Compliance-Anforderungen der Kunden erfüllen. Nachfolgend sind drei Anwendungsfälle beschrieben und die Empfehlung, welche Grundschutzkataloge für den speziellen Anwendungsfall modelliert werden sollten.

Eine Aussage darüber, wie jeder einzelne Service zur Erlangung einer Zertifizierbarkeit nach ISO 27001 auf der Basis von IT-Grundschutz konfiguriert werden muss, kann an dieser Stelle aufgrund der komplexen, unterschiedlichen und nicht bekannten Kundenanforderungen und Kundenumgebungen an dieser Stelle nicht gegeben werden.

Architekturübersicht und Anwendung der IT-Grundschutz Kataloge

Web Application Hosting
Hochverfügbares und skalierbares Web-Hosting kann komplex und teuer sein, Lastspitzen und starke Schwankungen im Datenfluss können zu geringe Auslastung der teuren Hardware führen. AWS bietet die für Web-Anwendungen benötigte und skalierbare, sichere und leistungsfähige Infrastruktur in Echtzeit, die die Schwankungen im Datenverkehr durch „elastic scale-out and scale-down Infrastruktur“ berücksichtigt.

AWS Service	Beschreibung	Anwendung IT-Grundschutz Kataloge
Amazon Route 53	Amazon Route 53 ist ein hochverfügbarer und skalierbarer DNS-Webservice (Domain Name System). Entwickler und Unternehmen bietet es eine außerordentlich zuverlässige und kostengünstige Möglichkeit, Endbenutzer zu Internetanwendungen zu routen. Dazu werden Namen wie www.beispiel.de in numerische IP-Adressen wie 192.0.2.1 übersetzt, die Computer zur gegenseitigen Vernetzung verwenden.	B 5.18 DNS-Server
Amazon CloudFront	Amazon CloudFront ist ein Web Service zur Bereitstellung von Inhalten. Der Service kann in andere Amazon Web Services-Produkte integriert werden und bietet Entwicklern und Unternehmen die Möglichkeit, Inhalte ganz einfach und mit geringer Latenz, hohen Datenübertragungsgeschwindigkeiten und ohne Mindestnutzung bereitzustellen.	B 1.17 Cloud-Nutzung B 3.304 Virtualisierung B 5.21 Webanwendungen B 5.23 Cloud Management
Amazon Simple Storage Service (Amazon S3)	Amazon Simple Storage Service (Amazon S3) bietet Entwicklern und IT-Teams sicheren, beständigen und hochgradig skalierbaren Objektspeicher. Amazon S3 ist bedienungsfreundlich und bietet eine einfache Schnittstelle für Webservices zum Speichern und Abrufen beliebiger Datenmengen von überall im Internet. Mit Amazon S3 zahlen Kunden nur für den Speicher, den Sie tatsächlich nutzen. Es gibt weder Mindest- noch Einrichtungsgebühr.	B 1.4 Datensicherungskonzept B 1.6 Schutz vor Schadprogrammen B 1.15 Löschen und Vernichten von Daten B 3.303 Speicherlösungen / Cloud Storage
Amazon Elastic Load Balancing	Elastic Load Balancing verteilt eingehenden Anwendungsverkehr automatisch auf mehrere EC2-Instances. Somit kann eine noch höhere Fehlertoleranz erreicht werden: Die Lastverteilungskapazität wird nahtlos an den Anwendungsverkehr angepasst.	B 3.302 Router und Switches B 4.1 Heterogene Netze

AWS Service	Beschreibung	Anwendung IT-Grundschutz Kataloge
Amazon Elastic Compute Cloud (Amazon EC2)	Amazon Elastic Compute Cloud (Amazon EC2) ist ein Web-Service, der anpassbare Rechenkapazität in der Cloud bietet. Der Service ist darauf ausgelegt, Cloud Computing für Entwickler zu erleichtern.	B 1.14 Patch- und Änderungsmanagement B 1.16 Anforderungsmanagement B 1.17 Cloud-Nutzung B 3.101 Allgemeiner Server B 3.102 Server unter Unix B 3.108 Windows Server 2003 B 3.109 Windows Server 2008 B 3.304 Virtualisierung B 5.3 Groupware B 5.4 Webserver B 5.5 Lotus Notes/Domino B 5.12 Microsoft Exchange/Outlook B 5.15 Allgemeiner Verzeichnisdienst B 5.16 Active Directory B 5.20 OpenLDAP B 5.21 Webanwendungen B 5.22 Protokollierung B 5.23 Cloud Management B 5.24 Web-Services B 5.25 Allgemeine Anwendungen
Amazon Machine Image (AMI)	Ein AMI ist eine besondere Art der virtuellen Appliance, die verwendet wird, um innerhalb von EC2 eine virtuelle Maschine zu instanziieren (erstellen). Es dient als Grundeinheit zur Bereitstellung von Dienstleistungen mit EC2.	B 1.17 Cloud-Nutzung B 3.304 Virtualisierung B 5.21 Webanwendungen
Auto Scaling	Mit Auto Scaling können Kunden ihre Amazon EC2-Kapazitäten entsprechend den von ihnen festgelegten Bedingungen nach oben oder nach unten anpassen. Wenn Auto Scaling angewendet wird, können wird dafür gesorgt, dass die Anzahl verwendeten Amazon EC2-Instances bei Anforderungsspitzen nahtlos nach oben skaliert wird, um die Leistung beizubehalten. Während eines Anforderungstiefs wird automatisch nach unten skaliert, um die Kosten gering zu halten. Auto Scaling eignet sich besonders für Anwendungen, bei denen es stündlich, täglich oder wöchentlich zu Unterschieden in der Verwendung kommt. Auto Scaling ist eine Funktion von Amazon CloudWatch, für die neben den normalen Gebühren für Amazon CloudWatch keine zusätzliche Gebühr anfällt.	B 1.17 Cloud-Nutzung B 3.304 Virtualisierung
Amazon Relational Database Service (Amazon RDS)	Amazon Relational Database Service (Amazon RDS) ist ein Web-Service zum einfachen Einrichten, Betreiben und Skalieren einer relationalen Datenbank in der Cloud. Dieser Service stellt kosteneffiziente und individuell anpassbare Kapazitäten zur Verfügung und erledigt gleichzeitig zeitraubende Datenbankverwaltungsaufgaben, sodass Sie sich stärker auf Ihre Anwendungen und Ihr Geschäft konzentrieren können.	B 5.7 Datenbanken

Fault tolerance and High Availability
Systeme, die im Fehlerfall schnell auf alternative Instanzen schwenken.

AWS Service	Beschreibung	Anwendung IT-Grundschutz Kataloge
Elastic Load Balancing	Elastic Load Balancing verteilt eingehenden Anwendungsverkehr automatisch auf mehrere EC2-Instances. Somit kann eine noch höhere Fehlertoleranz erreicht werden: Die Lastverteilungskapazität wird nahtlos an den Anwendungsverkehr angepasst.	B 3.302 Router und Switches B 4.1 Heterogene Netze
Availably Zones (AZs)	Amazon EC2 wird an mehreren Standorten weltweit betrieben. Diese Standorte bestehen aus Regionen und Verfügbarkeits-Zonen (Availability Zones – AZs). Jede *Region* ist ein separates geografisches Gebiet. Jede Region hat mehrere isolierte Standorte, die als Availability Zones bezeichnet werden. Amazon EC2 bietet Ihnen die Möglichkeit, Ressourcen, wie Instanzen und Daten an mehreren Standorten zu platzieren. Kundeninformationen werden nicht in allen Regionen repliziert, es sei denn der Kunde richtet die Replikation mit zwei AZs explizit ein.	B 2.1 Allgemeines Gebäude B 2.2 Elektrotechnische Verkabelung B 2.9 Rechenzentrum B 2.12 IT-Verkabelung
Elastic IP Addresses (EIP)	Eine Elastic IP-Adresse (EIP) ist eine statische IP-Adresse, die für das dynamische Cloud-Computing entwickelt wurde. Mit einer EIP, können Kunden den Ausfall einer Instanz oder Software durch schnelles Remapping der Adresse auf eine andere Instanz in ihrer Umgebung umgehen. Die EIP ist solange mit dem AWS-Konto des Kunden, nicht mit einer bestimmten Instanz verbunden, bis er beschließt, sie explizit freigeben.	B 3.302 Router und Switches B 4.1 Heterogene Netze
Elastic Block Store (EBS)	Amazon Elastic Block Store (Amazon EBS) bietet Volumes für persistente Speicherung auf Blockebene zur Verwendung mit Amazon EC2-Instances in der AWS-Cloud. Jedes Amazon EBS-Volume wird in seiner Availability Zone automatisch repliziert, um Schutz bei Ausfall von Komponenten zu bieten, was für hohe Verfügbarkeit und Beständigkeit sorgt. Amazon EBS-Volumes bieten die einheitliche Leistung und kurze Latenz, die Sie zum Bewältigen Ihrer Verarbeitungslasten benötigen. Bei Amazon EBS können Sie Ihre Nutzung binnen Minuten erweitern oder verringern und zahlen stets nur einen niedrigen Preis für die bereitgestellten Ressourcen.	B 1.4 Datensicherungskonzept B 1.6 Schutz vor Schadprogrammen B 1.15 Löschen und Vernichten von Daten B 3.303 Speicherlösungen / Cloud Storage
Amazon Simple Storage Service (Amazon S3)	Amazon Simple Storage Service (Amazon S3) bietet Entwicklern und IT-Teams sicheren, beständigen und hochgradig skalierbaren Objektspeicher. Amazon S3 ist bedienungsfreundlich und bietet eine einfache Schnittstelle für Webservices zum Speichern und Abrufen beliebiger Datenmengen von überall im Internet. Mit Amazon S3 zahlen Kunden nur für den Speicher, den Sie tatsächlich nutzen. Es gibt weder Mindest- noch Einrichtungsgebühr.	B 1.4 Datensicherungskonzept B 1.6 Schutz vor Schadprogrammen B 1.15 Löschen und Vernichten von Daten B 3.303 Speicherlösungen / Cloud Storage

Financial Services Grid Computing
Hoch skalierbare und flexible Netze für den Finanzdienstleistungssektor

AWS Service	Beschreibung	IT-Grundschutz Module Implementation
Amazon Simple Storage Service (Amazon S3)	Amazon Simple Storage Service (Amazon S3) bietet Entwicklern und IT-Teams sicheren, beständigen und hochgradig skalierbaren Objektspeicher. Amazon S3 ist bedienungsfreundlich und bietet eine einfache Schnittstelle für Webservices zum Speichern und Abrufen beliebiger Datenmengen von überall im Internet. Mit Amazon S3 zahlen Kunden nur für den Speicher, den Sie tatsächlich nutzen. Es gibt weder Mindest- noch Einrichtungsgebühr.	B 1.4 Datensicherungskonzept B 1.6 Schutz vor Schadprogrammen B 1.15 Löschen und Vernichten von Daten B 3.303 Speicherlösungen / Cloud Storage
AWS Direct Connect	Mit AWS Direct Connect ist es einfach, eine dedizierte Netzwerkverbindung zwischen einem Kundenstandort und AWS herzustellen. Mit AWS Direct Connect können Kunden eine private Verbindung zwischen AWS und ihrem Rechenzentrum, ihrer Niederlassung oder ihrer Colocation-Umgebung herstellen, wodurch sie in vielen Fällen ihre Netzwerkkosten senken, den Bandbreiten-Durchsatz erhöhen und eine konsistentere Netzwerkfunktion als mit internetbasierten Verbindungen herstellen können.	B 4.4 VPN
Amazon Relational Database Service (Amazon RDS)	Amazon Relational Database Service (Amazon RDS) ist ein Web-Service zum einfachen Einrichten, Betreiben und Skalieren einer relationalen Datenbank in der Cloud. Dieser Service stellt kosteneffiziente und individuell anpassbare Kapazitäten zur Verfügung und erledigt gleichzeitig zeitraubende Datenbankverwaltungsaufgaben, sodass Sie sich stärker auf Ihre Anwendungen und Ihr Geschäft konzentrieren können.	B 5.7 Datenbanken

AWS Service	Beschreibung	IT-Grundschutz Module Implementation
Amazon Elastic Compute Cloud (Amazon EC2)	Amazon Elastic Compute Cloud (Amazon EC2) ist ein Web-Service, der anpassbare Rechenkapazität in der Cloud bietet. Der Service ist darauf ausgelegt, Cloud Computing für Entwickler zu erleichtern	B 1.14 Patch- und Änderungsmanagement B 1.16 Anforderungsmanagement B 1.17 Cloud-Nutzung B 3.101 Allgemeiner Server B 3.102 Server unter Unix B 3.108 Windows Server 2003 B 3.109 Windows Server 2008 B 3.304 Virtualisierung B 5.3 Groupware B 5.4 Webserver B 5.5 Lotus Notes/Domino B 5.12 Microsoft Exchange/Outlook B 5.15 Allgemeiner Verzeichnisdienst B 5.16 Active Directory B 5.20 OpenLDAP B 5.21 Webanwendungen B 5.22 Protokollierung B 5.23 Cloud Management B 5.24 Web-Services B 5.25 Allgemeine Anwendungen
Amazon Machine Image (AMI)	Ein AMI ist eine besondere Art der virtuellen Appliance, die verwendet wird, um innerhalb von EC2 eine virtuelle Maschine zu instanziieren (erstellen). Es dient als Grundeinheit zur Bereitstellung von Dienstleistungen mit EC2.	B 1.17 Cloud-Nutzung B 3.304 Virtualisierung B 5.21 Webanwendungen
Amazon Simple Storage Service (Amazon S3)	Amazon Simple Storage Service (Amazon S3) bietet Entwicklern und IT-Teams sicheren, beständigen und hochgradig skalierbaren Objektspeicher. Amazon S3 ist bedienungsfreundlich und bietet eine einfache Schnittstelle für Webservices zum Speichern und Abrufen beliebiger Datenmengen von überall im Internet. Mit Amazon S3 zahlen Kunden nur für den Speicher, den Sie tatsächlich nutzen. Es gibt weder Mindest- noch Einrichtungsgebühr.	B 1.4 Datensicherungskonzept B 1.6 Schutz vor Schadprogrammen B 1.15 Löschen und Vernichten von Daten B 3.303 Speicherlösungen / Cloud Storage
Amazon DynamoDB	Amazon DynamoDB ist ein schneller, flexibler NoSQL-Datenbankservice für alle Anwendungen, die eine konsistente Latenz im einstelligen Millisekundenbereich für alle Größenordnungen benötigen. Es handelt sich um eine vollständig verwaltete Datenbank, die sowohl Dokument- als auch Schlüssel-Wert-Datenmodelle unterstützt. Aufgrund der Flexibilität des Datenmodells und der zuverlässigen Leistung eignet sich der Service hervorragend für mobile, Web-, Spiele-, Werbe-, IoT- und zahlreiche weitere Anwendungen.	B 5.7 Datenbanken

AWS Service	Beschreibung	IT-Grundschutz Module Implementation
Amazon Elastic MapReduce (Amazon EMR)	Amazon Elastic MapReduce (Amazon EMR) ist ein Web-Service, mit dem große Datenmengen schnell und kostengünstig verarbeitet werden können. Amazon EMR nutzt Hadoop, ein Open Source-Framework, für die Verteilung von Daten und die Verarbeitung auf einem skalierbaren Cluster aus Amazon EC2-Instances. Amazon EMR wird von einer Vielzahl von Anwendungen verwendet, darunter Anwendungen für Protokollanalyse, Web-Indizierung, Data Warehousing, maschinelles Lernen, Finanzanalyse, wissenschaftliche Simulationen und Bioinformatik. Unsere Kunden starten jährlich Millionen von EMR-Clustern.	B 5.21 Webanwendungen B 5.24 Web-Services B 5.25 Allgemeine Anwendungen
Amazon Glacier	Amazon Glacier ist ein äußerst kostengünstiger Archivspeicherservice in der Cloud, der sicheren und beständigen Speicher für die Datenarchivierung und Online-Sicherung bereitstellt. Um Kosten niedrig zu halten, ist Amazon Glacier für Daten, auf die selten zugegriffen wird und für die Abrufzeiten von mehreren Stunden angemessen sind, optimiert. Mit Amazon Glacier können Kunden große und kleine Datenmengen zuverlässig für nur 0,01 USD pro GB pro Monat speichern, was im Vergleich zu unternehmensinternen Lösungen ein erhebliches Kostenersparnis darstellt.	B 1.12 Archivierung