TÜV
TRUST IT
TÜV AUSTRIA Group

IT Grundschutz Compliance on Amazon Web Services

Table of contents

Abstract

The Amazon Web Services (AWS) environment is a highly secured and audited cloud platform and may be utilized by customers to meet a wide range of regulatory and best practice security and compliance requirements, including the German Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik*, BSI) IT Baseline protection methodology (IT Grundschutz). AWS' secure infrastructure may be used by customers in the building of an Information Security Management System (ISMS) in alignment with IT Grundschutz best practice security recommendations.

This workbook provides information about implementing the requirements of the BSI Standards 100-1 and 100-2[1], as well as the requirements on IT-Grundschutz certifications of outsourced components[2]. The use of AWS Cloud Platform Services within the ISMS does not endanger existing certifications and enables smooth implementation of projected certifications.

For this, understanding the model of shared responsibility between the customer and AWS is prerequisite for effective administration and operation of a secure cloud computing environment. Customers can use a wide range of AWS security features and partner products to help meet relevant security requirements. The procedures and controls applied by AWS can be validated by the client using AWS certifications and reports. This document refers to these certifications and reports, which can be requested individually at AWS. The AWS websites also include further information on compliance programs. In addition, this document describes the technical and organizational information security measures implemented by AWS.

Customers that already operate an ISMS or are currently establishing ISMS structures can smoothly integrate the secure infrastructure of AWS into their own ISMS, thus still being compliant with the IT-Grundschutz approach and recommendations. This seamless integration enables customers to maintain an existing or keep working on a projected certification of the ISMS according to ISO 27001 on the basis of IT-Grundschutz. For this, customers must be aware of the outsourced procedures, including the information stored or processed therein, and must make sure these are properly protected. This requires the client to establish distinct measures, which need to be aligned with BSI IT-Grundschutz requirements. All measures, including those provided by AWS, must be evaluated in the customer's risk management process and complemented by additional customer measures, where necessary.

Despite existing information security measures implemented by AWS, the customer ultimately remains responsible for proper and secure processing and storage of all data and information.

Important: For an existing certification according to ISO 27001 on the basis of IT-Grundschutz, switching to AWS Cloud Platform Services may result in a change to the information domain, i.e. the scope, which must be reported to the BSI.

Basic remarks

This workbook was prepared by TÜV TRUST IT GmbH TÜV Austria Group at the request of Amazon Web Services. Requirements from the following documents were included:

- BSI Standard 100-1: Information Security Management Systems (ISMS), Version 1.5
- BSI Standard 100-2: IT-Grundschutz Methodology, Version 2.0
- Requirements on IT-Grundschutz certifications of outsourced components, Version 1.0 (currently only available in German)
- IT-Grundschutz catalogues, 14th supplemental 2014 (the 14th supplemental is currently only available in German)

All information in this workbook is based on the aforementioned requirements and the technical and organizational measures implemented by AWS and on grounds of many years of experience both companies have in the field of information security. This workbook serves as a means of orientation, but cannot guarantee that customers successfully complete a certification according to ISO 27001 on the basis of IT-Grundschutz without eventual amendments or additional claims by BSI, as customer requirements can differ greatly depending on protection requirements and criticality of their services. In any case, it is recommended to reconcile a planned

[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

information domain and questions on modeling with BSI before filing an application. If clients already implemented a certification, the ramifications on the existing certification should be clarified with BSI before carrying out the outsourcing endeavor.

Shared Responsibility of Security

As with any third party, utilizing AWS creates a shared responsibility model for the operation and management of security controls. This shared model can help relieve a layer of operational burden as both AWS and the customer operate, manage and control components of information security controls. Security controls are considered to be shared, inherited, or dual controls.

In terms of information security compliance in cloud computing there is a subtle but very important distinction in understanding and evaluating compliance of the cloud solution and understanding and evaluating your usage of the cloud solution. “Security **OF THE** cloud” pertains to the compliance programs and measures that the Cloud Service Provider (AWS) implements within the AWS Infrastructure; “Security **IN THE** cloud” relates to the implementation of security controls associated with workloads running on top of the AWS infrastructure.

Glossary of BSI IT-Grundschutz terminology

Information domain (German: IT-Verbund)

An information domain comprises the infrastructural, organizational, staff and technical objects that serve as means for accomplishing tasks in a specific scope of information processing. An information domain may include the entire institution or single areas that are classified through organizational structures (e.g. departments) or common business processes / applications (e.g. personnel information systems).

Modeling (German: Modellierung)

In the IT-Grundschutz methodology, an institution’s information domain is replicated using the modules found in the IT-Grundschutz catalogues. For every module, chapter 2.2 of the IT-Grundschutz catalogues contains instructions on the relevant targets (physical and logical objects), including specific requirements that may have to be observed.

Module (German: Baustein)

Modules are used for structuring the recommendations of the IT-Grundschutz catalogues. Modules are the units within a layer (e.g. IT systems, networks). They describe technical components (e.g. cabling), organizational measures (e.g. disaster recovery concepts) and special use cases (e.g. home office workplaces). Within every, module, the respective IT component and applied threats are described, with recommended organizational and technical security measures.

Please note that in the English version of the IT-Grundschutz catalogues, modules are referred to as “M x.x”, whereas the German version refers to them as “B x.x”.

Safeguard (German: Maßnahme)

In the English version, IT-Grundschutz refers to measures as “safeguards”. In this document, both terms are used synonymously.

Section 1 – Customer View

Description of the IT-Grundschutz catalogues to be modeled

IT-Grundschutz Framework Overview

The German Federal Office for Information Security known as 'BSI' developed a program to provide organizations with a methodology to build effective information security procedures. This IT Baseline Protection (IT-Grundschutz) methodology is supported by four standards documents that provide organizational guidance for building an Information Security Management System, the methodology for the implementation and evaluation of IT-Grundschutz, information on how to perform risk analysis against the IT-Grundschutz requirements, and business continuity management program development.

This methodology is supported by the IT-Baseline Protection Catalogues (IT-Grundschutz Catalogues), which include technical and organizational measures for protection against the most important threats to information and data security. The following picture shows the structure of the IT-Grundschutz framework:

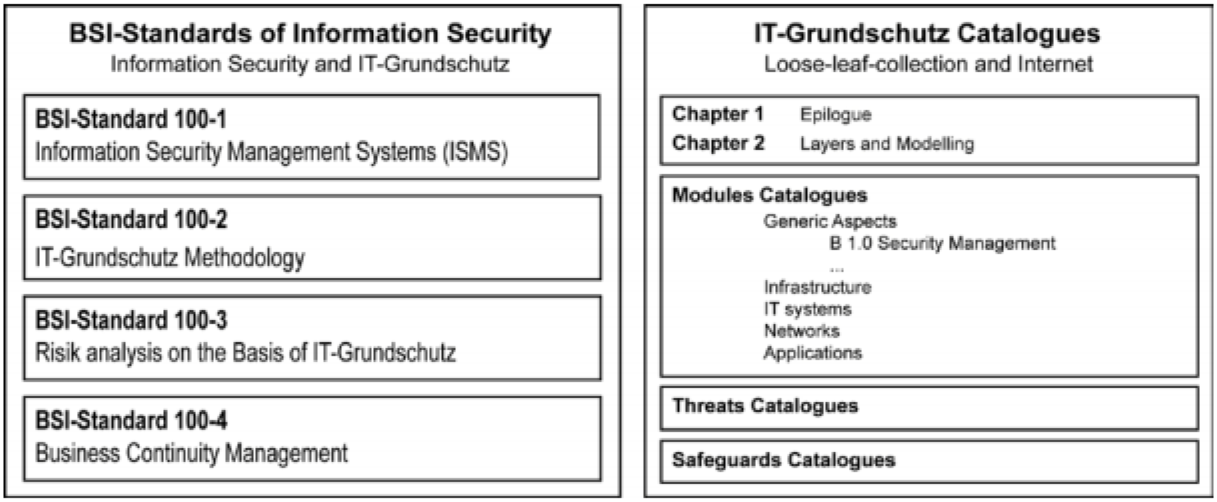
BSI-Standards of Information Security
Information Security and IT-Grundschutz
BSI-Standard 100-1
Information Security Management Systems (ISMS)
BSI-Standard 100-2
IT-Grundschutz Methodology
BSI-Standard 100-3
Risik analysis on the Basis of IT-Grundschutz
BSI-Standard 100-4
Business Continuity Management
IT-Grundschutz Catalogues
Loose-leaf-collection and Internet
Chapter 1 Epilogue
Chapter 2 Layers and Modelling
Modules Catalogues
Generic Aspects
B 1.0 Security Management
...
Infrastructure
IT systems
Networks
Applications
Threats Catalogues
Safeguards Catalogues

Figure 1: BSI-Standards and IT-Grundschutz Catalogues[3]

The Standard "100-1 Information Security Management Systems (ISMS)" defines general requirements on an ISMS. It is fully compatible to the ISO Standard 27001 and also includes the recommendations of the ISO-Standards 27000 and 27002.[4]

The Standard "100-2 IT-Grundschutz Methodology" interprets the very general requirements of the aforementioned ISO-Standards 27000, 27001 and 27002 and assists users by providing numerous directions, background information and examples.[5]

To implement these Standards and to define the measures for assuring information and data security measures relevant for the ISMS, the IT-Grundschutz approach describes the method of modeling modules. Herein, the defined information domain must be illustrated, i.e. modeled, using the modules provided by BSI. The respective modules are divided into five layers.

[3] Source: BSI-Standard 100-1, Information Security Management Systems (ISMS), Version 1.5, p. 10
[4] Source: BSI-Standard 100-1, Information Security Management Systems (ISMS), Version 1.5, p. 10 para. 3
[5] Source: BSI-Standard 100-1, Information Security Management Systems (ISMS), Version 1.5, p. 11 para. 2

These layers are:

- Layer 1: Generic aspects of information security
- Layer 2: Infrastructure security
- Layer 3: IT systems security
- Layer 4: Network security
- Layer 5: Security in applications

The respective modeling rules show how to model the existing modules and the associated measures within the information domain.[6] Modeling is carried out depending on the used products, technologies and existing processes, while also considering outsourcing measures within the organization.

This document describes the IT-Grundschutz modules that have to be modeled for the services provided by AWS and the technologies used therein. The "specifications for IT-Grundschutz certifications of outsourced components" are included in this description.

Relevant IT-Grundschutz modules

The modules that need to be modeled are based on the organization's defined information domain. When outsourcing services to AWS, the requirements set forth in the "specifications for IT-Grundschutz certifications of outsourced components" must be observed. Version 1.0 of these specifications offers mandatory regulations for outsourced components or services, since these are at least partially not controlled by the customer, but lie in the responsibility of AWS.

In general, outsourcing of components or services is only relevant for an ISO 27001 certification on the basis of IT-Grundschutz, if the following criteria[7] are met:

- IT systems, applications or business processes are outsourced to an external service provider, and
- the organization enters a long-term commitment with the service provider, and
- the service may have an impact on the organization's information security, and
- in the context of the services, the service provider regularly performs noteworthy activities in the area of information security management.

Performing "noteworthy activities in the area of information security management" includes any information security-related activity, like providing encryption services, failsafe connections or services or implementing security-related configurations.

Modeling the respective modules refers to one or all of the following three use cases:

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

[6] More details on proper modelling (German Website) https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/allgemein/modellierung/02001.html

[7] Source: IT-Grundschutz-Catalogues, 14. supplementary-2014, Chapter 2.1

The modeling includes the services and technologies described in the corresponding architecture overviews. In this document, referring to further modules that may have to be modeled in the customer's information domain is not possible, as the customers' environments are not known. The additional modules that need to be modeled by the customer for outsourcing to AWS are documented in the following chart.[8]

The modules marked with "X" should be modeled according to the specifications. Modules marked with "(X)" should be modeled depending on customer requirements, applied products as well as stored and processed data and information.

Module ID	Title	Modeling			
		General Application[9]	Fault Tolerance HA services[10]	FS Grid Computing	Web App Hosting
M 1 Common Aspects					
M 1.0	Security management	X			
M 1.1	Organization	X			
M 1.2	Personnel	X			
M 1.3	Business continuity management	X			
M 1.4	Data backup policy		X	X	X
M 1.5	Data protection[11]		(X)	(X)	(X)
M 1.6	Protection against malware		X	X	X
M 1.7	Crypto-concept[12]		(X)	(X)	(X)
M 1.8	Handling security incidents	X			
M 1.9	Hardware and software management	X			
M 1.10	Standard software		X	X	X
M 1.11	Outsourcing		X	X	X
M 1.12	Archiving			X	
M 1.13	Information security awareness and training				
M 1.14	Patch and change management		X	X	X
M 1.15	Deleting and destroying data		X	X	X
M 1.16	Compliance management		X	X	X
M 1.17	Cloud utilization		X	X	X
M 2 Infrastructure					
M 2.1	General building		X	X	X
M 2.2	Electrical Cabling		X	X	X
M 2.3	Office / local workplace				
M 2.4	Server room				
M 2.5	Data media archives				
M 2.6	Technical infrastructure room				
M 2.7	Protective cabinets				
M 2.8	Home workplace				
M 2.9	Computer center		X	X	X

[8] The listed modules refer to the 14th supplementary of the BSI IT-Grundschutz catalogues

[9] The selection of these modules is based on the "specifications for IT-Grundschutz certifications of outsourced components"; the modules need to be applied separately at the customer and AWS.

[10] The selection of these modules is based on the technologies of the use cases "Fault Tolerance HA services", "FS Grid Computing" und "Web App Hosting"

[11] Depending on the processing of PII

[12] Depending on the confidentiality of the processed information

Module ID	Title	Modeling			
		General Application[9]	Fault Tolerance HA services[10]	FS Grid Computing	Web App Hosting
M 2.10	Mobile workplace				
M 2.11	Meeting, event, and training rooms				
M 2.12	IT-Cabling		X	X	X
M 3 IT-Systems					
M 3.101	General server		X	X	X
M 3.102	Servers under Unix[13]		(X)	(X)	(X)
M 3.103	*Servers under Windows NT - not to apply*	*-/-*	*-/-*	*-/-*	*-/-*
M 3.104	*Servers under Novell Netware 3.x - not to apply*	*-/-*	*-/-*	*-/-*	*-/-*
M 3.105	*Servers under Novell Netware Version 4.x - not to apply*	*-/-*	*-/-*	*-/-*	*-/-*
M 3.106	*Server under Windows 2000 - not to apply*	*-/-*	*-/-*	*-/-*	*-/-*
M 3.107	S/390 and zSeries mainframes				
M 3.108	Windows Server 2003[14]		(X)	(X)	(X)
M 3.109	Windows Server 2008[15]		(X)	(X)	(X)
M 3.201	General client				
M 3.202	General stand-alone IT systems				
M 3.203	Laptop				
M 3.204	Unix client				
M 3.205	*Windows NT client - not to apply*	*-/-*	*-/-*	*-/-*	*-/-*
M 3.206	*Windows 95 client - not to apply*	*-/-*	*-/-*	*-/-*	*-/-*
M 3.207	*Client under Windows 2000 - not to apply*	*-/-*	*-/-*	*-/-*	*-/-*
M 3.208	Internet PCs				
M 3.209	Windows XP client				
M 3.210	Windows Vista client				
M 3.211	Client under Mac OS X				
M 3.212	Client under Windows 7				
M 3.301	Security gateway (firewall)				
M 3.302	Routers and switches		X	X	X
M 3.303	Storage systems / Cloud storage		X	X	X
M 3.304	Virtualization		X	X	X
M 3.305	Terminal servers				
M 3.401	Telecommunications system				
M 3.402	Fax machine				
M 3.403	*Answering machine - not to apply*	*-/-*	*-/-*	*-/-*	*-/-*
M 3.404	Mobile telephones				

[13] Depending on the operating system

[14] Depending on the operating system

[15] Depending on the operating system

Module ID	Title	Modeling			
		General Application[9]	Fault Tolerance HA services[10]	FS Grid Computing	Web App Hosting
M 3.405	PDA				
M 3.406	Printers, copiers, and all-in-one devices				
M 4 Networks					
M 4.1	Heterogeneous networks		X	X	X
M 4.2	Network- and System management				
M 4.3	Modem				
M 4.4	VPN[16]			(X)	
M 4.5	LAN connection of an IT system via ISDN				
M 4.6	WLAN				
M 4.7	VoIP				
M 4.8	Bluetooth				
M 5 Applications					
M 5.1	*Peer-to-peer services - not to apply*	*-/-*	*-/-*	*-/-*	*-/-*
M 5.2	Exchange of data media				
M 5.3	Groupware[17]		(X)	(X)	(X)
M 5.4	Web servers		X	X	X
M 5.5	Lotus Notes / Domino[18]		(X)	(X)	(X)
M 5.6	Fax servers				
M 5.7	Databases			X	X
M 5.8	Telecommuting				
M 5.9	Novell eDirectory				
M 5.10	*Internet Information Server - not to apply*	*-/-*	*-/-*	*-/-*	*-/-*
M 5.11	*Apache Webserver - not to apply*	*-/-*	*-/-*	*-/-*	*-/-*
M 5.12	Microsoft Exchange/Outlook[19]		(X)	(X)	(X)
M 5.13	SAP System				
M 5.14	Mobile data media				
M 5.15	General directory service[20]		(X)	(X)	(X)
M 5.16	Active Directory[21]		(X)	(X)	(X)
M 5.17	Samba				
M 5.18	DNS-Server[22]		(X)	(X)	X
M 5.19	Internet use				
M 5.20	OpenLDAP[23]		(X)	(X)	(X)

[16] Depending on the customer connection to AWS

[17] Depending on the services operated at AWS

[18] Depending on the services operated at AWS

[19] Depending on the services operated at AWS

[20] Depending on the technologies operated at AWS

[21] Depending on the technologies operated at AWS

[22] Depending on the technologies operated at AWS

[23] Depending on the technologies operated at AWS

Module ID	Title	Modeling			
		General Application[9]	Fault Tolerance HA services[10]	FS Grid Computing	Web App Hosting
M 5.21	Web applications		X	X	X
M 5.22	Logging		X	X	X
M 5.23	Cloud Management		X	X	X
M 5.24	Web services		X	X	X
M 5.25	General applications		X	X	X

Important: With regard to the customer’s definition of protection requirements, it may be necessary to model additional or develop customized modules to establish further security measures. This can be necessary if high or very high protection requirements exist, if special operating conditions need to be met or if the used components cannot be modeled with the available IT-Grundschutz modules.[24]

[24] Source: BSI Standard 100-2, Version 2.0, p. 35, Chapter. „Additional security safeguards“

Modules to be addressed by the customer

The modules shown in the following chart must be applied by the customer according to the information given in the chapter "Relevant IT-Grundschutz modules".

The modules marked with "X" should be modeled according to the specifications. Modules marked with "(X)" should be modeled depending on customer requirements, applied products as well as stored and processed data and information.

Module ID	Title	To be applied by AWS client	Additional information
M 1 Common aspects			
M 1.0	Security management	X	According to the „specifications for IT-Grundschutz certifications of outsourced components", this module needs to be applied separately by customers and providers.
M 1.1	Organization	X	According to the „specifications for IT-Grundschutz certifications of outsourced components", this module needs to be applied separately by customers and providers.
M 1.2	Personnel	X	According to the „specifications for IT-Grundschutz certifications of outsourced components", this module needs to be applied separately by customers and providers.
M 1.3	Business continuity management	X	According to the „specifications for IT-Grundschutz certifications of outsourced components", this module needs to be applied separately by customers and providers.
M 1.4	Data backup policy	X	Clients are responsible for their data and information and must apply appropriate measures for backup that are consistent with their security guidelines.
M 1.5	Data protection	(X)	Clients are responsible for their data and information and must apply appropriate data protection measures that are consistent with their security guidelines.
M 1.6	Protection against malware	X	Clients are responsible for their data and information and must apply appropriate malware protection measures that are consistent with their security guidelines.
M 1.7	Crypto-concept	(X)	Clients are responsible for their data and information and must apply appropriate cryptographic measures that are consistent with their security guidelines.
M 1.8	Handling security incidents	X	According to the „specifications for IT-Grundschutz certifications of outsourced components", this module needs to be applied separately by customers and providers.
M 1.9	Hardware and software management	X	According to the „specifications for IT-Grundschutz certifications of outsourced components", this module needs to be applied separately by customers and providers.
M 1.10	Standard software	X	Customers are responsible for evaluating standard software. Within the AWS environment, no standard software is used.
M 1.11	Outsourcing	X	Clients are responsible for their data and information and must apply appropriate outsourcing measures that are consistent with their security guidelines.

Module ID	Title	To be applied by AWS client	Additional information
M 1.12	Archiving	X	Clients are responsible for their data and information and must apply appropriate archiving measures that are consistent with their security guidelines.
M 1.14	Patch and change management	X	Clients are responsible for their data and information and must apply appropriate patch- and change management measures that are consistent with their security guidelines.
M 1.15	Deleting and destroying data	X	Clients are responsible for their data and information and must apply appropriate measures for deleting and destroying data that are consistent with their security guidelines.
M 1.16	Compliance management	X	Clients are responsible for their data and information and must apply appropriate compliance management measures that are consistent with their security guidelines.
M 1.17	Cloud utilization	X	Clients are responsible for their data and information and must apply appropriate measures for cloud utilization that are consistent with their security guidelines.
M 3 IT-Systems			
M 3.101	General server	X	Clients are responsible for their data and information and must apply appropriate measures for general servers that are consistent with their security guidelines.
M 3.102	Servers under Unix [25]	(X)	Clients are responsible for their data and information and must apply appropriate measures for Unix servers that are consistent with their security guidelines.
M 3.108	Windows Server 2003[26]	(X)	Clients are responsible for their data and information and must apply appropriate measures for Windows Server 2003 that are consistent with their security guidelines.
M 3.109	Windows Server 2008[27]	(X)	Clients are responsible for their data and information and must apply appropriate measures for Windows Server 2008 that are consistent with their security guidelines.
M 3.302	Routers und switches	X	Clients are responsible for their data and information and must apply appropriate measures for routers and switches that are consistent with their security guidelines.
M 3.303	Storage systems / Cloud Storage	X	Clients are responsible for their data and information and must apply appropriate measures for Storage Systems / Cloud Storage that are consistent with their security guidelines.
M 3.304	Virtualization	X	Clients are responsible for their data and information and must apply appropriate measures for virtualization that are consistent with their security guidelines.
M 4 Networks			

[25] Depending on the operating system

[26] Depending on the operating system

[27] Depending on the operating system

Module ID	Title	To be applied by AWS client	Additional information
M 4.1	Heterogeneous networks	X	Clients are responsible for their data and information and must apply appropriate measures for heterogeneous networks that are consistent with their security guidelines.
M 4.4	VPN[28]	(X)	Clients are responsible for their data and information and must apply appropriate measures for VPNs that are consistent with their security guidelines.
M 5 Applications			
M 5.3	Groupware[29]	(X)	Clients are responsible for their data and information and must apply appropriate measures for Groupware that are consistent with their security guidelines.
M 5.4	Web servers	X	Clients are responsible for their data and information and must apply appropriate measures for web servers that are consistent with their security guidelines.
M 5.5	Lotus Notes / Domino[30]	(X)	Clients are responsible for their data and information and must apply appropriate measures for Lotus Notes / Domino that are consistent with their security guidelines.
M 5.7	Databases	X	Clients are responsible for their data and information and must apply appropriate measures for databases that are consistent with their security guidelines.
M 5.12	Microsoft Exchange / Outlook[31]	(X)	Clients are responsible for their data and information and must apply appropriate measures for Microsoft Exchange / Outlook that are consistent with their security guidelines.
M 5.15	General directory service[32]	(X)	Clients are responsible for their data and information and must apply appropriate measures for general directory services that are consistent with their security guidelines.
M 5.16	Active Directory[33]	(X)	Clients are responsible for their data and information and must apply appropriate measures for Active Directory that are consistent with their security guidelines.
M 5.18	DNS-Server[34]	X	Clients are responsible for their data and information and must apply appropriate measures for the DNS-Server that are consistent with their security guidelines.
M 5.20	OpenLDAP[35]	(X)	Clients are responsible for their data and information and must apply appropriate measures for OpenLDAP that are consistent with their security guidelines.
M 5.21	Web applications	X	Clients are responsible for their data and information and must apply appropriate measures for web applications that are consistent with their security guidelines.

[28] Depending on the customer connection to AWS
[29] Depending on the services operated at AWS
[30] Depending on the services operated at AWS
[31] Depending on the services operated at AWS
[32] Depending on the technologies operated at AWS
[33] Depending on the technologies operated at AWS
[34] Depending on the technologies operated at AWS
[35] Depending on the technologies operated at AWS

Module ID	Title	To be applied by AWS client	Additional information
M 5.22	Logging	X	Clients are responsible for their data and information and must apply appropriate logging measures that are consistent with their security guidelines.
M 5.24	Web services	X	Clients are responsible for their data and information and must apply appropriate measures for web services that are consistent with their security guidelines.
M 5.25	General applications	X	Clients are responsible for their data and information and must apply appropriate measures for general applications that are consistent with their security guidelines.

Important: With regard to the customer's definition of protection requirements, it may be necessary to model additional or develop customized modules to establish further security measures. This can be necessary if high or very high protection requirements exist, if special operating conditions need to be met or if the used components cannot be modeled with the available IT-Grundschutz modules.[36]

[36] Source: BSI Standard 100-2, Version 2.0, p. 35, Chapter. „Additional security safeguards“

Implementing catalogue M 1.11 Outsourcing

If the outsourcing is relevant for a certification following the criteria described in the chapter Relevant IT-Grundschutz modules“, the following rules apply for implementing the module “M 1.11 Outsourcing”:

- 1st case: outsourcing poses an insignificant threat for the items in scope:

  The recommendations of the outsourcing modules are optional.

- 2nd case: outsourced components are subject to major threats:

  In this case, the outsourcing module must be applied.

- 3rd case: limited extent of damage (special case):

  In this case, the outsourcing module must be applied.

- 4th case: the outsourcing service provider possesses an IT-Grundschutz certification:

  In this case, the outsourcing module must be applied.

The remainder of this document is based on the assumption that the outsourcing is relevant for a certification, with the module “M 1.11 Outsourcing” being applicable according to the 2nd case.[37] The presence of “major threats” to outsourced components means that components of the outsourced information domain have high or even very high protection requirements or essential parts of the information domain are being outsourced.[38]

Within “M 1.11 Outsourcing”, as is the case for all modules of the IT-Grundschutz catalogues, BSI has already looked at major threats for outsourcing endeavors. Depending on the criticality of the outsourced systems or services, these threats can be very complex. The analysis differentiates between physical, technical and human aspects. The derived measures for planning and implementing an outsourcing endeavor are divided into the following seven phases:[39]

- Phase 1: strategic planning of the outsourcing endeavor
- Phase 2: defining material security requirements
- Phase 3: selecting the outsourcing service provider
- Phase 4: contract design
- Phase 5: preparing a security concept for the outsourced information domain
- Phase 6: migration phase
- Phase 7: planning and ensuring ongoing operations

According to the approach described in the BSI Standard 100, acquiring and maintaining a certification according to ISO 27001 on the basis of IT-Grundschutz requires reviewing and assessing all safeguards in the current module. This includes the qualification levels A (entry), B (secondary) and C (certificate). The existing safeguard “S 3.33 Security vetting of staff” has been classified at qualification level Z (additional) and usually is applied only if high or very protection requirements are determined for the outsourced services or processes.[40]

[37] Further details for the possible implementation scenarios can be found in the document “specifications for IT-Grundschutz certifications of outsourced components”

[38] Source: „specifications for IT-Grundschutz certifications of outsourced components“, Version 1, p. 3, 2nd case

[39] Source: BSI IT-Grundschutz catalogues, 14th supplementary, p. 143, chapter M 1.11 Outsourcing

[40] Further information on the qualification levels of safeguards can be found in the BSI-Standard 100-2

Modules to be delivered by AWS

The customer does not have to implement the respective modules if a task has been completely transferred to AWS. The modules shown in the following chart must be delivered by AWS according to the information given in the chapter "Relevant IT-Grundschutz modules".

The modules marked with "X" should be modeled according to the specifications. Modules marked with "(X)" should be modeled depending on customer requirements, applied products as well as stored and processed data and information.

Module ID	Title	To be delivered by AWS	Additional information
M 1 Common aspects			
M 1.0	Security management	X	According to the "specifications for IT-Grundschutz certifications of outsourced components", this module needs to be applied separately by customers and providers. *See AWS alignment to BSI IT-Grundschutz, Handling of risks and safeguards, section M 1.0.*
M 1.1	Organization	X	According to the "specifications for IT-Grundschutz certifications of outsourced components", this module needs to be applied separately by customers and providers. *See AWS alignment to BSI IT-Grundschutz, Handling of risks and safeguards, section M 1.1.*
M 1.2	Personnel	X	According to the "specifications for IT-Grundschutz certifications of outsourced components", this module needs to be applied separately by customers and providers. *See AWS alignment to BSI IT-Grundschutz, Handling of risks and safeguards, section M 1.2.*
M 1.3	Business continuity management	X	According to the "specifications for IT-Grundschutz certifications of outsourced components", this module needs to be applied separately by customers and providers. *See AWS alignment to BSI IT-Grundschutz, Handling of risks and safeguards, section M 1.3.*
M 1.6	Protection against malware	X	*See AWS alignment to BSI IT-Grundschutz, Handling of risks and safeguards, section M 1.6.*
M 1.7	Crypto-concept	(X)	*See AWS alignment to BSI IT-Grundschutz, Handling of risks and safeguards, section M 1.7.*
M 1.8	Handling security incidents	X	According to the "specifications for IT-Grundschutz certifications of outsourced components", this module needs to be applied separately by customers and providers. *See AWS alignment to BSI IT-Grundschutz, Handling of risks and safeguards, section M 1.8.*
M 1.9	Hardware and software management	X	According to the "specifications for IT-Grundschutz certifications of outsourced components", this module needs to be applied separately by customers and providers. *See AWS alignment to BSI IT-Grundschutz, Handling of risks and safeguards, section M 1.9.*
M 1.14	Patch and change management	X	*See AWS alignment to BSI IT-Grundschutz, Handling of risks and safeguards, section M 1.14.*

Module ID	Title	To be delivered by AWS	Additional information
M 1.15	Deleting and destroying data	X	*See AWS alignment to BSI IT-Grundschutz, Handling of risks and safeguards for the destruction of physical media.*
M 1.16	Compliance management	X	*See AWS alignment to BSI IT-Grundschutz, Handling of risks and safeguards, section M 1.16.*
M 2 Infrastructure			
M 2.1	General building	X	*See AWS alignment to BSI IT-Grundschutz, Handling of risks and safeguards, section M 2.1.*
M 2.2	Electrical cabling	X	*See AWS alignment to BSI IT-Grundschutz, Handling of risks and safeguards, section M 2.2*
M 2.9	Data center	X	*See AWS alignment to BSI IT-Grundschutz, Handling of risks and safeguards, section M 2.1.*
M 2.12	IT-cabling	X	*See AWS alignment to BSI IT-Grundschutz, Handling of risks and safeguards, section M 2.1.*
M 3 IT-Systems			
M 3.101	General server	X	*See AWS alignment to BSI IT-Grundschutz, Handling of risks and safeguards, section M 3.101.*
M 3.302	Routers and switches	X	*See AWS alignment to BSI IT-Grundschutz, Handling of risks and safeguards, section M 3.302.*
M 3.304	Virtualization	X	*See AWS alignment to BSI IT-Grundschutz, Handling of risks and safeguards, section M 3.304.*
M 5 Applications			
M 5.22	Logging	X	*See AWS alignment to BSI IT-Grundschutz, Handling of risks and safeguards, section M 5.22.*
M 5.23	Cloud Management	X	*See AWS alignment to BSI IT-Grundschutz, Handling of risks and safeguards, section M 5.23.*
M 5.24	Web services	X	*See AWS alignment to BSI IT-Grundschutz, Handling of risks and safeguards, section M 5.24.*

Section 2 – AWS View:

Description of what needs to be provided by the customer

Security **IN THE** Cloud

While AWS manages security of the cloud infrastructure, security in the cloud is the responsibility of the customer, as customers retain control of what security they choose to implement to protect their own content, platform, applications, systems and networks, no differently than they would for applications in an on-site datacenter.

Customers retain control of their content when using AWS services. Customers, rather than AWS, determine what content they store on AWS, control how they configure their environments and secure their content, what security features and tools they use and how they use them. For these reasons, customers also retain responsibility for the security of anything their organization puts on AWS, or that they connect to their AWS infrastructure. Examples include guest operating systems, applications on their compute instances, and content stored and processed in AWS storage, platform and database services.

To assist customers in designing, implementing and operating their own secure AWS environment, AWS provides a wide array of security features customers can use. Customers can also use their own security tools and controls. Customers can configure their AWS services to leverage a range of such security features, protect their content, including sophisticated identity and access management tools, security capabilities, encryption and network security. Examples of steps customers can take to help secure their content include implementing:

- Strong password policies, assigning appropriate permissions to users and taking robust steps to protect their access keys
- Appropriate firewalls and network segmentation, encrypting content, and properly architecting systems to decrease the risk of data loss and unauthorized access

All of these factors are within customer control, rather than AWS. AWS does not know what content customers are placing on AWS and does not change customer configuration settings; they are determined and controlled by the customer. Only the customer can determine what level of security is appropriate for the data they store and process using AWS.

To assist customers in integrating AWS security controls into their existing control frameworks and help customers design and execute security assessments of their organization’s use of AWS services, AWS publishes a number of whitepapers relating to security, governance, risk and compliance; and a number of checklists and best practices. Customers are also free to design and execute security assessments according to their own preferences, and can request permission to conduct scans of their cloud infrastructure as long as those scans are limited to the customer's compute instances and do not violate the AWS Acceptable Use Policy

Covering requirements with existing AWS certifications or measures

Security **OF THE** Cloud

Security **OF THE** Cloud refers to how AWS manages the security of the cloud's underlying infrastructure. AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the AWS services operate.

How can an organization validate the Security Controls in operation within the AWS Control environment?

AWS certifications and reports are produced by AWS third-party auditors and attest to the design and operating effectiveness of the AWS environment. These include:

SOC 1/ ISAE 3402: AWS publishes a "Service Organization Controls 1 (SOC 1), Type II report[41]". This audit is the replacement of the Statement on Auditing Standards No. 70 (SAS 70) Type II report. The SOC 1 report audit attests that the AWS control objectives are appropriately designed and that the controls safeguarding customer data are operating effectively.

SOC 2 - Security: In addition to the SOC 1 report, AWS publishes "Service Organization Controls 2 (SOC 2), Type II report[42]". Similar to the SOC 1 in the evaluation of controls, the SOC 2 report is an attestation report that expands the evaluation of controls to the criteria set forth by the American Institute of Certified Public Accountants (AICPA) Trust Services Principles[43]. The AWS SOC 2 is an evaluation of the design and operating effectiveness of controls that meet the criteria for the security principle set forth in the AICPA's Trust Services Principles criteria. This report provides additional transparency into AWS security based on a defined industry standard and further demonstrates AWS' commitment to protecting customer data.

SOC 3-Security: AWS publishes a Service Organization Controls 3 (SOC 3) report[44]. The SOC 3 report is a publically-available summary of the AWS SOC 2 report and provides the AICPA SysTrust Security Seal[45].

The report includes the external auditor's opinion of the operation of controls (based on the AICPA's Security Trust Principles[46] included in the SOC 2 report), the assertion from AWS management regarding the effectiveness of controls, and an overview of AWS Infrastructure and Services.

ISO 27001: AWS is certified under the International Organization for Standardization (ISO) 27001 standard[47]. ISO 27001 is a widely-adopted global security standard that outlines the requirements for information security management systems. It provides a systematic approach to managing company and customer information that's based on periodic risk assessments. In order to achieve the certification, a company must show it has a systematic and ongoing approach to managing information security risks that affect the confidentiality, integrity, and availability of company and customer information.

PCI – Security: AWS is Level 1 compliant under the Payment Card Industry (PCI) Data Security Standard (DSS). Customers can run applications on our PCI-compliant technology infrastructure for storing, processing, and transmitting credit card information in the cloud. In February 2013, the PCI Security Standards Council released PCI DSS Cloud Computing Guidelines[48]. These guidelines provide customers who are managing a cardholder data environment with considerations for maintaining PCI DSS controls in the cloud. AWS has incorporated the PCI DSS Cloud Computing Guidelines into the AWS PCI Compliance Package for customers.

[41] http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/AICPASOC1Report.aspx
[42] http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/AICPASOC2Report.aspx
[43] https://cert.webtrust.org/pdfs/Trust_Services_PC_latest.pdf
[44] http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/AICPASOC3Report.aspx
[45] https://cert.webtrust.org/soc3_amazon_web_services.html
[46] https://cert.webtrust.org/pdfs/Trust_Services_PC_latest.pdf
[47] http://www.27000.org/iso-27001.htm
[48] https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Cloud_Guidelines.pdf

Requesting AWS Compliance Certifications and reports

The applicable AWS compliance certifications and reports can be requested at https://aws.amazon.com/compliance/contact.

Additional information and resources that describe AWS Compliance environment.

AWS has Compliance Whitepapers[49], providing information to assist AWS customers with integrating AWS into their existing control frameworks and to help design and execute security assessments of an organization's use of AWS.

More information on AWS Compliance certifications, reports, alignment with best practices and standards (such as MPAA) can be found at AWS's Compliance website[50].

[49] http://aws.amazon.com/compliance/whitepapers
[50] http://aws.amazon.com/compliance/

AWS Alignment to BSI IT-Grundschutz

The following chart displays how AWS implements the BSI IT-Grundschutz catalogues.

Module ID	Title	AWS implementation
M 1 Common aspects		
M 1.0	Security management	AWS has established an information security framework and policies based on the Control Objectives for Information and related Technology (COBIT) framework and have effectively integrated the ISO 27001 certifiable framework based on ISO 27002 controls, American Institute of Certified Public Accountants (AICPA) Trust Services Principles, the PCI DSS v2.0 and the National Institute of Standards and Technology (NIST) Publication 800-53 Rev 3 (Recommended Security Controls for Federal Information Systems). The Control environment at Amazon begins at the highest level of the Company. Executive and senior leadership play important roles in establishing the Company's tone and core values. AWS has an established information security organization managed by the AWS Security team and is led by the AWS Chief Information Security Officer (CISO). AWS maintains and provides security awareness training to all information system users supporting AWS. This annual security awareness training includes the following topics; the purpose for security and awareness training, the location of all AWS policies, AWS incident response procedures (including instructions on how to report internal and external security incidents). AWS has an established Certification, Authorization, Security Assessment Policy which addresses the purpose, scope, roles, responsibilities and management commitment pertaining to how AWS manages, monitors and communicates alignment with third party audited Certifications / Accreditations. The AWS Security Assurance team is tasked with responsibility for onboarding, managing, monitoring and evaluating compliance frameworks. This includes managing audit artifacts such as system security plan documentation, audit artifacts, audit findings, audit remediation activities. AWS engages with external certifying bodies and independent auditors to review and validate our compliance with all compliance frameworks across the relevant system boundary.
M 1.1	Organization	AWS has established an information security framework and policies based on the Control Objectives for Information and related Technology (COBIT) framework and have effectively integrated the ISO 27001 certifiable framework based on ISO 27002 controls, American Institute of Certified Public Accountants (AICPA) Trust Services Principles, the PCI DSS v2.0 and the National Institute of Standards and Technology (NIST) Publication 800-53 Rev 3 (Recommended Security Controls for Federal Information Systems). AWS maintains the security policy, provides security training to employees, and performs application security reviews. These reviews assess the confidentiality, integrity, and availability of data, as well as conformance to the information security policy. The Control environment at Amazon begins at the highest level of the Company. Executive and senior leadership play important roles in establishing the Company's tone and core values. The AWS organizational structure provides a framework for planning, executing and controlling business operations. The organizational structure assigns roles and responsibilities to provide for adequate staffing, efficiency of operations, and the segregation of duties. Management has also established authority and appropriate lines of reporting for key personnel. Included as part of the Company’s hiring verification processes are educations, previous employment, and, in some cases, background checks as permitted by law and regulation for employees commensurate with the employee’s position and level of access to AWS facilities. The

Module ID	Title	AWS implementation
		Company follows a structured on-boarding process to familiarize new employees with Amazon tools, processes, systems, policies and procedures. AWS has defined the following list of measures to help protect against supply chain threats that could impact resources: Agile Acquisitions – AWS Senior Management holds a weekly meeting to determine what is required to meet business needs. The items identified to meet capacity needs are released in RFQs and subsequently acquired. This frequent review of needs and the resulting frequent bid and acquisition cycle results in a significantly more agile acquisition process than when items are budgeted on a yearly cycle. The process allows AWS to quickly acquire whatever is needed by the business. Small Contracts – The weekly discussion and frequent RFQs allow for multiple smaller contracts, recurring over time. If a vendor cannot deliver for whatever reason, the impact is small and the acquisition can be easily re-sourced. Use of Well Recognized, Established, Diverse Suppliers – Conduct due diligence review of suppliers prior to entering into contractual agreements to acquire hardware, software, firmware, or services. Multiple Vendors – The AWS team maintains a list of approved vendors with numerous vendors for each type of component needed. If a vendor is unable to deliver, another vendor can be used for the next round of acquisitions. While much of the AWS system has been designed in-house to meet AWS' unique needs, AWS uses standard, commercially available information system configurations to the maximum extent possible, thereby limiting the possibility of acquiring systems and products that have been corrupted via the supply chain actions. Upon acquisition, AWS resources are associated with an asset label. AWS Asset labels are customer agnostic and are utilized to maintain inventory of hardware within the AWS Asset Management Tool. Within AWS Data Centers hardware is not physically associated with a customer or the data stored on the hardware. All customer data, regardless of source is considered to be Critical, in turn, all media is treated as sensitive. Independent external auditors review AWS Asset Management processes and procedures during audits for our PCI DSS, ISO 27001 and FedRAMP compliance. AWS utilizes multi-factor authentication mechanisms for data center access as well as additional security mechanisms designed to ensure that only authorized individuals enter an AWS data center. Authorized individuals must use their badge on the card reader and enter their unique PIN to gain access to the facility and rooms for which they are authorized. Physical access to data centers is enforced by AWS's electronic access control system, which is comprised of card readers and PIN pads for building and room ingress and card readers only for building and room egress. Enforcing the use of card readers for building and room egress provides anti-pass back functionality to help ensure that unauthorized individuals do not tailgate authorized Persons and get in without a badge. In addition to the access control system, all entrances to AWS data centers, including the main entrance, the loading dock, and any roof doors/hatches, are secured with intrusion detection devices that sound alarms if the door is forced open or held open. In addition to electronic mechanisms, AWS data centers utilize trained security guards 24x7, which are stationed in and around the building. Access to data centers within the system boundary is granted on a need-to-know basis only, with all physical access requests being reviewed and

Module ID	Title	AWS implementation
		approved by the appropriate Area Access Manager (AAM). AWS data centers are housed in nondescript facilities and are not open to the public. Physical access is strictly controlled both at the perimeter and at building ingress points. AWS only provides data center access and information to vendors, contractors, and visitors who have a legitimate business need for such privileges, such as emergency repairs. All visitors to data centers must be pre-authorized by the applicable Area Access Manager (AAM) and documented in AWS ticket management system. When they arrive at the data center, they must present identification and sign in before they are issued a visitor badge. Authorized staff while in the data center continually escorts them. Independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP compliance review AWS Physical Security Mechanisms. In alignment with ISO 27001 standards, AWS has established formal policies, procedures to delineate the minimum standards for logical access to AWS resources. AWS SOC 1 Type 2 and SOC 2 Type 2 report outlines the controls in place to manage access provisioning to AWS resources. The AWS Production network is segregated from the Amazon Corporate network and requires a separate set of credentials for logical access. The Amazon Corporate network relies on user IDs, passwords, and Kerberos, while the AWS Production network requires SSH public-key authentication through a bastion host. AWS developers and administrators on the Amazon Corporate network who need to access AWS cloud components must explicitly request access through the AWS access management system. All requests are reviewed and approved by the appropriate owner or manager. Accounts are reviewed every 90 days; explicit re-approval is required or access to the resource is automatically revoked. Access is also automatically revoked when an employee's record is terminated in Amazon's Human Resources system. Windows and UNIX accounts are disabled and Amazon's permission management system removes the user from all systems. Requests for changes in access are captured in the Amazon permissions management tool audit log. When changes in an employee's job function occur, continued access must be explicitly approved to the resource or it will be automatically revoked. When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual ") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. If a hardware device is unable to be decommissioned using these procedures, the device will be degaussed or physically destroyed in accordance with industry-standard practices.
M 1.2	Personnel	The AWS organizational structure provides a framework for planning, executing and controlling business operations. The organizational structure assigns roles and responsibilities to provide for adequate staffing, efficiency of operations, and the segregation of duties. Management has also established authority and appropriate lines of reporting for key personnel. Included as part of the Company's hiring verification processes are educated, previous employments, and, in some cases, background checks as permitted by law and regulation for employees commensurate with the employee's position and level of access to AWS facilities. The Company follows a structured on-boarding process to familiarize new employees with Amazon tools, processes, systems, policies and procedures. AWS has implemented various methods of internal communication at a global level to help employees understand their individual roles and responsibilities and to communicate significant events in a timely manner. These methods include

Module ID	Title	AWS implementation
		orientation and training programs for newly hired employee as well as electronic mail messages and the posting of information via the Amazon intranet. Amazon Legal Counsel manages and periodically revises the Amazon Non-Disclosure Agreement (NDA) to reflect AWS business needs. Independent external auditors review AWS usage of Non-Disclosure Agreements (NDA) during audits for our ISO 27001 and FedRAMP compliance. AWS maintains and provides security awareness training to all information system users supporting AWS. This annual security awareness training includes the following topics: • The purpose for security and awareness training, • The location of all AWS policies, • AWS incident response procedures (including instructions on how to report internal and external security incidents). Contractor / vendor onboarding is managed the same for both employees and contractors, with responsibility shared across Human Resources (HR), Corporate Operations and Service Owners. Independent external auditors review AWS policies, procedures and relevant training programs during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP compliance. In addition the AWS Overview of Security Processes Whitepaper provides further details - available at http://aws.amazon.com/security. AWS Human Resources team defines internal management responsibilities to be followed for termination and role change of employees and vendors. The responsibility for provisioning /de-provisioning employee and contractor access is shared across Human Resources (HR), Corporate Operations and Service Owners. Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security.
M 1.3	Business continuity management	AWS Business Continuity Policies and Plans have been developed and tested in alignment with ISO 27001 standards and developed as a part of AWS overall approach to Information Security Policy development. AWS Resiliency program encompasses the processes and procedures by which AWS assets identify, respond to and recover from a major event or incident within our environment. This program builds upon the traditional approach of addressing Contingency Management which incorporates elements of a traditional Business Continuity and Disaster Recovery Plans and expands this to consider critical elements of proactive risk mitigation strategies such as engineering physically separate Availability Zones (AZ's) and continuous infrastructure capacity planning. AWS contingency plans and incident response playbooks are maintained and updated to reflect emerging continuity risks and lessons learned from past incidents. Testing of AWS capability to respond to events occurs regularly with lessons learnt captured and processes and documentation updated appropriately. AWS data centers are built in clusters in various global regions. All data centers are online and serving customers; no data center is “cold”. In case of failure, automated processes move customer data traffic away from the affected area. Core applications are deployed in an N+1 configuration, so that in the event of a data center failure, there is sufficient capacity

Module ID	Title	AWS implementation
		to enable traffic to be load-balanced to the remaining sites. AWS provides customers the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Each Availability Zone is designed as an independent failure zone. This means that Availability Zones are physically separated within a typical metropolitan region and are located in lower risk flood plains (specific flood zone categorization varies by Region). In addition to discrete uninterruptable power supply (UPS) and onsite backup generation facilities, they are each fed via different grids from independent utilities to further reduce single points of failure. Availability Zones are all redundantly connected to multiple tier-1 transit providers. Customers should architect their AWS usage to take advantage of multiple Regions and Availability Zones. Distributing applications across multiple Availability Zones provides the ability to remain resilient in the face of most failure modes including natural disasters or system failures. AWS SOC 1 Type 2 report provides further details. ISO 27001 standard Annex A, domain 11. 2 provide additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification.
M 1.6	Protection against malware	AWS's program, processes and procedures to managing antivirus / malicious software is in alignment with ISO 27001 standards. Refer to AWS SOC 1 Type II reports provides further details. Independent third party auditors for our continued compliance with SOC, PCI DSS, ISO 27001 and FedRAMP review all AWS Configuration Management and Flaw Remediation Process. A configuration management tool used to manage deployable software in packages, package groups, and environments. A package is a collection of related files, such as software, content, etc., that are tightly coupled to one another. A package group is a set of packages that are often deployed together. An environment is the combination of a set of packages and package groups which are deployed to a set of host classes (hosts or servers that serve the same function). An environment represents the complete set of packages required for a server to fulfill a particular function. Amazon assets (e.g. laptops) are configured with anti-virus software that includes e-mail filtering and malware detection. When changes are deployed to systems and devices within the system boundary, a Change Management (CM) ticket is submitted. This CM ticket captures all change details, including a change description, impact analysis, security considerations (if any), change timeframe, and required approvals. AWS maintains the baseline OS distribution used on hosts. AWS utilizes a customized version of RHEL with minimum base functionality. All unneeded ports; protocols and services are disabled in the base builds. Service teams use the build tools to add only approved software packages necessary for the server's function per the configuration baselines maintained in the tools. Servers are regularly scanned and any unnecessary ports or protocols in use are corrected using the flaw remediation process. Deployed software undergoes recurring penetration testing performed by carefully selected industry experts. Remediation of the annual penetration testing exercise is also incorporated into the baseline through the flaw remediation process.
M 1.7	Crypto-concept	AWS provides customers the ability to use their own encryption mechanism for nearly all services including S3, EBS and EC2. VPC sessions are also encrypted. For AWS connections, FIPS-approved hashes are available. AWS utilizes cryptographic modules for user authentication through the following access methods; API Endpoints, VPC IPSEC VPN, IAM, MFA Hardware Token, SSH.

Module ID	Title	AWS implementation
		Internally, AWS establishes and manages cryptographic keys for required cryptography employed within the AWS infrastructure. AWS produces, controls and distributes symmetric cryptographic keys using NIST approved key management technology and processes in the AWS information system. An AWS developed secure key and credential manager is used to create, protect and distribute symmetric keys and is used to secure and distribute: AWS credentials needed on hosts, RSA public/private keys and X.509 Certifications. Independent third party auditors for our continued compliance with SOC, PCI DSS, ISO 27001 and FedRAMP review AWS cryptographic processes.
M 1.8	Handling security incidents	AWS has implemented a formal, documented incident response policy and program. The policy addresses purpose, scope, roles, responsibilities, and management commitment. AWS also maintains and provides security awareness training to all information system users supporting AWS. This annual security awareness training includes the following topics: • The purpose for security and awareness training, • The location of all AWS policies, • AWS incident response procedures (including instructions on how to report internal and external security incidents). Systems within AWS are extensively instrumented to monitor key operational and security metrics. Alarms are configured to automatically notify operations and management personnel when early warning thresholds are crossed on key metrics. When a threshold is crossed, the AWS incident response process is initiated. The Amazon Incident Response team employs industry-standard diagnostic procedures to drive resolution during business-impacting events. Staff operates 24x7x365 coverage to detect incidents and manage the impact to resolution. AWS utilizes a three-phased approach to manage incidents: 1. Activation and Notification Phase: Incidents for AWS begin with the detection of an event. This can come from several sources including: a. Metrics and alarms - AWS maintains an exceptional situational awareness capability, most issues are rapidly detected from 24x7x365 monitoring and alarming of real time metrics and service dashboards. The majority of incidents are detected in this manner. AWS utilizes early indicator alarms to proactively identify issues that may ultimately impact Customers. b. b. Trouble ticket entered by an AWS employee c. Calls to the 24X7X365 technical support hotline.

Module ID	Title	AWS implementation
		If the event meets incident criteria, then the relevant on-call support engineer will start an engagement utilizing AWS Event Management Tool system to start the engagement and page relevant program resolvers (e.g. Security team). The resolvers will perform an analysis of the incident to determine if additional resolvers should be engaged and to determine the approximate root cause. 2. Recovery Phase - the relevant resolvers will perform break fix to address the incident. Once troubleshooting, break fix and affected components are addressed, the call leader will assign next steps in terms of follow-up documentation and follow-up actions and end the call engagement. 3. Reconstitution Phase - Once the relevant fix activities are complete the call leader will declare that the recovery phase is complete. Post mortem and deep root cause analysis of the incident will be assigned to the relevant team. The results of the post mortem will be reviewed by relevant senior management and relevant actions such as design changes etc. will be captured in a Correction of Errors (COE) document and tracked to completion. In addition to the internal communication mechanisms detailed above, AWS has also implemented various methods of external communication to support its customer base and community. Mechanisms are in place to allow the customer support team to be notified of operational issues that impact the customer experience. A "Service Health Dashboard" is available and maintained by the customer support team to alert customers to any issues that may be of broad impact.
M 1.9	Hardware and software management	In alignment with ISO 27001 standards, AWS Hardware assets are assigned an owner, tracked and monitored by the AWS personnel with AWS proprietary inventory management tools. AWS has defined the following list of measures to help protect against supply chain threats that could impact resources. Agile Acquisitions – AWS Senior Management holds a weekly meeting to determine what is required to meet business needs. The items identified to meet capacity needs are released in RFQs and subsequently acquired. This frequent review of needs and the resulting frequent bid and acquisition cycle results in a significantly more agile acquisition process than when items are budgeted on a yearly cycle. The process allows AWS to quickly acquire whatever is needed by the business. Small Contracts – The weekly discussion and frequent RFQs allow for multiple smaller contracts, recurring over time. If a vendor cannot deliver for whatever reason, the impact is small and the acquisition can be easily re-sourced. Use of Well Recognized, Established, Diverse Suppliers – Conduct due diligence review of suppliers prior to entering into contractual agreements to acquire hardware, software, firmware, or services. Multiple Vendors – The AWS team maintains a list of approved vendors with numerous vendors for each type of component needed. If a vendor is unable to deliver, another vendor can be used for the next round of acquisitions.

Module ID	Title	AWS implementation
		While much of the AWS system has been designed in-house to meet AWS' unique needs, AWS uses standard, commercially available information system configurations to the maximum extent possible, thereby limiting the possibility of acquiring systems and products that have been corrupted via the supply chain actions For AWS Data Center Environments, all new information system components, which include, but are not limited to, servers, racks, network devices, hard drives, system hardware components, and building materials that are shipped to and received by data centers require prior authorization by and notification to the Data Center Manager. Items are delivered to the loading dock of each AWS Data Center and are inspected for any damages or tampering with the packaging and signed for by a full-time employee of AWS. Upon shipment arrival, items are scanned and captured within the AWS Asset management system and device inventory tracking system. Once items are received, they are placed in an equipment storage room within the data center that requires the swipe badge and PIN combination for access until they are installed on the data center floor. Prior to exiting the data center, items are scanned, tracked, and sanitized before authorization to leave the data center. When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual ") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. If a hardware device is unable to be decommissioned using these procedures, the device will be degaussed or physically destroyed in accordance with industry-standard practices. AWS has identified auditable event categories across systems and devices within the AWS system. Service teams configure the auditing features to record continuously the security-related events in accordance with requirements. The log storage system is designed to provide a highly scalable, highly available service that automatically increases capacity as the ensuing need for log storage grows. Audit records contain a set of data elements in order to support necessary analysis requirements. In addition, audit records are available for AWS Security team or other appropriate teams to perform inspection or analysis on demand, and in response to security-related or business-impacting events. Designated personnel on AWS teams receive automated alerts in the event of an audit processing failure. Audit processing failures include, for example, software/hardware errors. When alerted, on-call personnel issue a trouble ticket and track the event until it is resolved. AWS SOC 1 Type II report provides an overview of the controls in place to manage change management in the physical and logical AWS environment. When changes are deployed to systems and devices within the system boundary, a Change Management (CM) ticket is submitted. This CM ticket captures all change details, including a change description, impact analysis, security considerations (if any), change timeframe, and required approvals. In alignment with ISO 27001 standards, AWS has established formal policies, procedures to delineate the minimum standards for logical access to AWS resources. AWS SOC 1 Type 2 and SOC 2 Type 2 report outlines the controls in place to manage access provisioning to AWS resources. The AWS Production network is segregated from the Amazon Corporate network and requires a separate set of credentials for logical access. The Amazon Corporate network relies on user IDs, passwords, and Kerberos, while the AWS Production network requires SSH public-key authentication through a bastion host. AWS developers and administrators on the Amazon Corporate network who need to access AWS cloud components

Module ID	Title	AWS implementation
		must explicitly request access through the AWS access management system. All requests are reviewed and approved by the appropriate owner or manager. Accounts are reviewed every 90 days; explicit re-approval is required or access to the resource is automatically revoked. Access is also automatically revoked when an employee's record is terminated in Amazon's Human Resources system. Windows and UNIX accounts are disabled and Amazon's permission management system removes the user from all systems. Requests for changes in access are captured in the Amazon permissions management tool audit log. When changes in an employee's job function occur, continued access must be explicitly approved to the resource or it will be automatically revoked.
M 1.14	Patch and change management	AWS has implemented a formal, documented configuration management policy. This policy addresses purpose, scope, roles, responsibilities, and management commitment as it pertains to configuration and change management. When changes are deployed to systems and devices a Change Management (CM) ticket is submitted. This CM ticket captures all change details, including a change description, impact analysis, security considerations (if any), change timeframe, and required approvals. The change management process is reviewed and assessed by external third partied during AWS SOC, PCI DSS, ISO 27001 and FedRAMP testing. AWS is responsible for patching systems supporting the delivery of service to customers, such as the hypervisor and networking services. This is done as required per AWS policy and in accordance with ISO 27001, NIST, and PCI requirements. Customers control their own guest operating systems, software and applications and are therefore responsible for patching their own systems. AWS does not require systems to be brought offline to perform regular maintenance and system patching. AWS implements least privilege throughout its infrastructure components. AWS prohibits all ports and protocols that do not have a specific business purpose. AWS follows a rigorous approach to minimal implementation of only those features and functions that are essential to use of the device. Network scanning is performed and any unnecessary ports or protocols in use are corrected. Regular internal and external vulnerability scans are performed on the host operating system, web application and databases in the AWS environment utilizing a variety of tools. Vulnerability scanning and remediation practices are regularly reviewed as a part of AWS continued compliance with PCI DSS and FedRAMP. Amazon Information Security and AWS Security teams subscribe to newsfeeds for applicable vendor flaws from Secunia and TELUS Security Labs. Amazon Information Security proactively monitors vendor's websites and other relevant outlets for new patches. Prior to implementation Patches are evaluated for security and operational impact and applied in timely manner based upon assessment.
M 1.15	Deleting and destroying data	When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual ") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. All decommissioned magnetic storage devices are

Module ID	Title	AWS implementation
		degaussed and physically destroyed in accordance with industry-standard practices. Further information can be found in the AWS Whitepaper “AWS Security Overview” at https://aws.amazon.com/security/
M 1.16	Compliance management	AWS has an established Certification, Authorization, Security Assessment Policy which addresses the purpose, scope, roles, responsibilities and management commitment pertaining to how AWS manages, monitors and communicates alignment with third party audited Certifications / Accreditations. The AWS Security Assurance team is tasked with responsibility for onboarding, managing, monitoring and evaluating compliance frameworks. This includes managing audit artifacts such as system security plan documentation, audit artifacts, audit findings, audit remediation activities. AWS engages with external certifying bodies and independent auditors to review and validate our compliance with all compliance frameworks across the relevant system boundary. Customers using AWS maintain and do not release effective control over their content. Customers control their content from the time of creation. Customers can: • Determine where content will be located, for example the type of storage and geographic location of that storage • Control over the format of that content, for example plain text, masked, anonymized or encrypted • Manage other access controls, such as identity, access management and security credentials This allows AWS customers to control the entire life-cycle of their content on AWS, and manage their content in accordance with their own specific needs, including content classification, access control, retention and disposal. AWS has an established information security organization managed by the AWS Security team and is led by the AWS Chief Information Security Officer (CISO). AWS maintains and provides security awareness training to all information system users supporting AWS. This annual security awareness training includes the following topics; the purpose for security and awareness training, the location of all AWS policies, AWS incident response procedures (including instructions on how to report internal and external security incidents).
M 2 Infrastructure		
M 2.1	General building	AWS data centers are housed in nondescript facilities and are not open to the public. AWS data centers incorporate physical protection against environmental risks. AWS's physical protection against environmental risks has been validated by an independent auditor and has been certified as being in alignment with ISO 27002 best practices. Data centers have both fire suppression and fire detection mechanisms. Fire suppression and detection systems within the data centers consist of fire extinguishers and VESDA smoke detectors. Fire suppression and detection systems are powered by a standalone backup power supply (UPS) in the event of power outage. In the event that a fire suppression system is deployed, AWS has the capacity to switch over operations to an alternate data center. Procedures for shutting down a data center include detailed information on how to shut down a data center and re-direct traffic to another data center cluster or region. AWS employs fire detection devices/systems for the information system that activate automatically and notify the organization and emergency responders in the event of a fire.

Module ID	Title	AWS implementation
		AWS data centers are built in clusters in various global regions. All data centers are online and serving customers; no data center is "cold." In case of failure, automated processes move customer data traffic away from the affected area. Core applications are deployed in an N+1 configuration, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites. AWS provides customers the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Each Availability Zone is designed as an independent failure zone. This means that Availability Zones are physically separated within a typical metropolitan region and are located in lower risk flood plains (specific flood zone categorization varies by Region). In addition to discrete uninterruptable power supply (UPS) and onsite backup generation facilities, they are each fed via different grids from independent utilities to further reduce single points of failure. Availability Zones are all redundantly connected to multiple tier-1 transit providers. Customers should architect their AWS usage to take advantage of multiple Regions and Availability Zones. Distributing applications across multiple Availability Zones provides the ability to remain resilient in the face of most failure modes including natural disasters or system failures. Physical access to data centers is enforced by AWS's electronic access control system, which is comprised of card readers and PIN pads for building and room ingress and card readers only for building and room egress. Enforcing the use of card readers for building and room egress provides anti-pass back functionality to help ensure that unauthorized individuals do not tailgate authorized Persons and get in without a badge. In addition to the access control system, all entrances to AWS data centers, including the main entrance, the loading dock, and any roof doors/hatches, are secured with intrusion detection devices that sound alarms if the door is forced open or held open. In addition to electronic mechanisms, AWS data centers utilize trained security guards 24x7, who are stationed in and around the building. Access to data centers within the system boundary is granted on a need-to-know basis only, with all physical access requests being reviewed and approved by the appropriate Area Access Manager (AAM). AWS data centers are housed in nondescript facilities and are not open to the public. Physical access is strictly controlled both at the perimeter and at building ingress points. AWS only provides data center access and information to vendors, contractors, and visitors who have a legitimate business need for such privileges, such as emergency repairs. All visitors to data centers must be pre-authorized by the applicable Area Access Manager (AAM) and documented in AWS ticket management system. When they arrive at the data center, they must present identification and sign in before they are issued a visitor badge. Authorized staff while in the data center continually escorts them. AWS SOC 1 Type 2 report and SOC 2 Type 2 Security provides further details. ISO 27001 standard Annex A, domain 11. 2 provide additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification.
M 2.2	Electrical Cabling	The AWS internal cabling procedures, sets forth the precedent by which AWS categorizes, implements and manages cabling requirements. AWS Asset labels are customer agnostic and are utilized to maintain inventory of hardware within the AWS Asset Management Tool. Within AWS Data Centers hardware is not physically associated with a customer or the data stored on the hardware. All customer data, regardless of source is considered to be Critical, in turn, all media is treated as sensitive.

Module ID	Title	AWS implementation
		Independent external auditors review AWS Asset Management processes and procedures during audits for our PCI DSS, ISO 27001 and FedRAMP compliance.
M 2.9	Data centers	AWS data centers are housed in nondescript facilities and are not open to the public. AWS data centers incorporate physical protection against environmental risks. AWS's physical protection against environmental risks has been validated by an independent auditor and has been certified as being in alignment with ISO 27002 best practices. Data centers have both fire suppression and fire detection mechanisms. Fire suppression and detection systems within the data centers consist of fire extinguishers and VESDA smoke detectors. Fire suppression and detection systems are powered by a standalone backup power supply (UPS) in the event of power outage. In the event that a fire suppression system is deployed, AWS has the capacity to switch over operations to an alternate data center. Procedures for shutting down a data center include detailed information on how to shut down a data center and re-direct traffic to another data center cluster or region. AWS employs fire detection devices/systems for the information system that activate automatically and notify the organization and emergency responders in the event of a fire. AWS data centers are built in clusters in various global regions. All data centers are online and serving customers; no data center is “cold.” In case of failure, automated processes move customer data traffic away from the affected area. Core applications are deployed in an N+1 configuration, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites. AWS provides customers the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Each Availability Zone is designed as an independent failure zone. This means that Availability Zones are physically separated within a typical metropolitan region and are located in lower risk flood plains (specific flood zone categorization varies by Region). In addition to discrete uninterruptable power supply (UPS) and onsite backup generation facilities, they are each fed via different grids from independent utilities to further reduce single points of failure. Availability Zones are all redundantly connected to multiple tier-1 transit providers. Customers should architect their AWS usage to take advantage of multiple Regions and Availability Zones. Distributing applications across multiple Availability Zones provides the ability to remain resilient in the face of most failure modes including natural disasters or system failures. Physical access to data centers is enforced by AWS’s electronic access control system, which is comprised of card readers and PIN pads for building and room ingress and card readers only for building and room egress. Enforcing the use of card readers for building and room egress provides anti-pass back functionality to help ensure that unauthorized individuals do not tailgate authorized Persons and get in without a badge. In addition to the access control system, all entrances to AWS data centers, including the main entrance, the loading dock, and any roof doors/hatches, are secured with intrusion detection devices that sound alarms if the door is forced open or held open. In addition to electronic mechanisms, AWS data centers utilize trained security guards 24x7, who are stationed in and around the building. Access to data centers within the system boundary is granted on a need-to-know basis only, with all physical access requests being reviewed and approved by the appropriate Area Access Manager (AAM). AWS data centers are housed in nondescript facilities and are not open to the public. Physical access is strictly controlled both at the perimeter and at building ingress points. AWS only provides data center access and information to vendors, contractors, and visitors who have a legitimate business need for such privileges, such as emergency repairs. All visitors to data centers must be pre-authorized by the applicable Area

Module ID	Title	AWS implementation
		Access Manager (AAM) and documented in AWS ticket management system. When they arrive at the data center, they must present identification and sign in before they are issued a visitor badge. Authorized staff while in the data center continually escorts them. AWS SOC 1 Type 2 report and SOC 2 Type 2 Security provides further details. ISO 27001 standard Annex A, domain 11. 2 provide additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification.
M 2.12	IT-cabling	The AWS internal cabling procedures, sets forth the precedent by which AWS categorizes, implements and manages cabling requirements. AWS Asset labels are customer agnostic and are utilized to maintain inventory of hardware within the AWS Asset Management Tool. Within AWS Data Centers hardware is not physically associated with a customer or the data stored on the hardware. All customer data, regardless of source is considered to be Critical, in turn, all media is treated as sensitive. Independent external auditors review AWS Asset Management processes and procedures during audits for our PCI DSS, ISO 27001 and FedRAMP compliance.
M 3 IT-Systems		
M 3.101	General Server	AWS has implemented a formal, documented configuration management policy, which is applicable to AWS, titled "AWS Configuration Management Policy". The AWS Configuration Management Policy is disseminated via the internal AWS Compliance web portal to all employees, vendors, and contractors. The AWS Compliance team reviews this policy annually, with approval by the AWS Chief Information Security Officer. This policy addresses purpose, scope, roles, responsibilities, and management commitment. Configuration management procedures are disseminated via the AWS internal wiki to all employees, vendors, and contractors. These procedures specify the outline for implementing changes to hosts within the system boundary. AWS offers two types of AMIs for the use of customers to create EC2 instances: **Amazon Linux** - The Amazon Linux AMI includes packages and configurations that provide tight integration with AWS. This allows the Amazon Linux AMI to launch and work correctly within Amazon EC2 as supplied. The Amazon Linux AMI comes pre-installed with most AWS API tools and CloudInit. AWS API tools enable scripting of important provisioning tasks from within an Amazon EC2 instance. CloudInit allows passing instance configuration actions to instances at launch time via the EC2 user-data fields, enabling remote configuration of Amazon EC2 instances. The configuration of the Amazon Linux AMI enhances security by focusing on two main security goals: limiting access and reducing software vulnerabilities. The Amazon Linux AMI limits remote access capabilities by using SSH key pairs and by disabling remote root login. Additionally, the Amazon Linux AMI minimizes the number of non-critical packages which are installed on the instance, limiting exposure to potential security vulnerabilities. Security updates are automatically applied

Module ID	Title	AWS implementation
		on the initial boot of the AMI. Upon login, the Message of the Day (/etc/motd) indicates whether or not any additional updates are available. The Amazon Linux AMI is built as a minimal Linux installation, including only the most essential Linux services. Rather than having to strip out components after installation, the Amazon Linux AMI is designed to provide a minimal and functional base. Starting with a minimal base of packages means there are fewer components to maintain, as well as less surface area for security exploits. **Vendor OS** – This consists of OS implementations of AMIs based on the vendors current software release. These AMIs contain standard releases from OS vendors such as Windows Server, RHEL, SUSE Linux and Ubuntu Linux. These AMIs are as supplied by the vendor without additional configuration. It is the customer's responsibility to patch and securely configure any AMIs that employ a vendor OS. **Logical Access** AWS defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the AWS information system in the following ways: Logical access to deploy or enact changes to systems and devices within the system boundary are limited to personnel with administrative or system management permissions. Requests for access, along with approval or denial are tracked in the Permissions tool. Access to network devices is then authenticated via TACACS+, while access to hosts is via certificate-based SSH v2 access. User functions on systems and devices within the system boundary are separated from administrative, or system management functions. The systems enforce this via permissions established in the sudoers files of hosts within the system boundary. Administrative or system management functions on hosts cannot be executed unless the authenticated user is a part of the sudoers file of that host.
M 3.302	Routers and switches	AWS systems reside in a secure perimeter within AWS-controlled data centers. Access to these systems is only via SSH and multifactor authentication. AWS has bastion hosts to restrict access to network devices and other components of the infrastructure. In addition to the bastion hosts, control-plane ACLs have been applied on all network devices and SSH access has been restricted to the network devices from only specific bastion hosts. AWS logically isolates networks by using boundary devices, which limit ingress and egress of communication to only authorized traffic flow. AWS isolates information security tools, mechanisms, and support components from other internal information system components via logically separate subnets, which are isolated from customer instances and traffic. All hosts that house information security tools, mechanisms and support components reside in separate security host classes, which isolate

Module ID	Title	AWS implementation
		access and permissions on security hosts from those on other types of production servers. The AWS Security team strictly controls the access and permissions on security hosts. AWS has a limited number of access points to the information system to allow for a more comprehensive monitoring of inbound and outbound communications and network traffic. These customer access points are called API end-points, which allow customers to establish a secure communication session with their storage or compute instances within AWS. These access points are monitored for inbound and outbound traffic in order to help ensure availability of service. AWS has implemented network devices that are dedicated to manage interfacing communications with Internet service providers (ISPs). AWS employs a redundant connection to more than one communication service at each internet-facing edge of the AWS network. These connections each have dedicated network devices. Security controls listed below are in place to help protect the confidentiality and integrity of information being transmitted. These security controls are assessed for operational effectiveness every 6 months. Firewall devices are configured to restrict access to the computing environment and enforce boundaries of computing clusters Firewall policies (configuration files) are automatically pushed to the network every 24 hours. Firewall policy updates are reviewed and approved. Network devices are configured by AWS to only allow access to specific ports on other systems within AWS. AWS has developed and has documented a configuration management. AWS implements the AWS Configuration Management Plan for systems and devices within the AWS system boundary. The AWS Configuration Management Plan addresses roles, responsibilities, and configuration management processes and procedures. The AWS CM Plan details the process for managing the configuration of production system configuration items. AWS identifies configuration items as a change to a system, service, db schema or environment, which could cause an impact to another team, service or site, or if other groups within AWS need to be aware of your change. These types of changes include configuration setting alternations, changes to packages, package groups or environments that exist on systems or devices within the system boundary. Change types are maintained within the AWS Configuration Management Plan.
M 3.304	Virtualization	Throughout AWS, AWS employs virtualization techniques to present information system components as other types of components, or components with differing configurations. This includes virtual networking devices and host based firewalls which control traffic flow restrictions via ACLs in EC2 and VPC and as EC2 instances which present a variety of operating systems. Where multiple customer virtual compute instances exist on a single host, system resources are allocated to each customer as initially setup by the customer. System resource allocation is managed via virtualization software, and the amount of system resource allocated to each customer is dependent on and enforced to adhere to the customer system

Module ID	Title	AWS implementation
		resource parameters established upon initial setup. A centralized region-by-region server provides per-customer aggregation and traffic direction. When a customer is consuming network devices to a point that would impact other customers, AWS applies per-customer network traffic throttles. The service monitors and aggregates data per minute and the throttle is reset each minute until the throughput returns to acceptable levels.
M 5 Applications		
M 5.22	Logging	For AWS assets, that AWS is responsible for, AWS has identified auditable event categories across systems and devices within the AWS system. Service teams configure the auditing features to record continuously the security-related events in accordance with requirements. The log storage system is designed to provide a highly scalable, highly available service that automatically increases capacity as the ensuing need for log storage grows. Audit records contain a set of data elements in order to support necessary analysis requirements. In addition, audit records are available for AWS Security team or other appropriate teams to perform inspection or analysis on demand, and in response to security-related or business-impacting events. Designated personnel on AWS teams receive automated alerts in the event of an audit processing failure. Audit processing failures include, for example, software/hardware errors. When alerted, on-call personnel issue a trouble ticket and track the event until it is resolved. Customers control their own Guest OS, their software and their applications and are therefore responsible for developing a monitoring of these systems' logic states. In compliance with ISO/IEC 27001-Standards, AWS information systems use internal NTP (Network Time Protocol) based system clocks. AWS CloudTrail provides a simple solution for logging user activities, so that a complex logging system may not be required. Further information can be found at aws.amazon.com/cloudtrail. AWS Cloudwatch allows monitoring of resources in the AWS Cloud and of applications users execute on AWS. Further information can be found at aws.amazon.com/cloudwatch. AWS publishes current information on service availability in the service state overview. Further information can be found at http://status.aws.amazon.com.
B 5.23	Cloud Management	AWS services includes AWS Regions, Availability Zones (AZs), and services that support the customer's application architecture. Identical sets of the various services are contained within each Availability Zone. Services may communicate between AZs and Regions for disaster recovery or availability purposes. Customer applications are built upon the standard AWS services, and are considered outside of the AWS security boundary. Customers are responsible for managing the security controls within their application. Customers initiating connections to AWS websites and API endpoints considered being AWS application websites, and owners of website content are considered outside the boundary. AWS administration personnel also are outside of the boundary, and use secure remote access methods to operate and maintain AWS system.

Module ID	Title	AWS implementation
		AWS Regions A Region is a collection of AWS resources in the same geographical area. It includes multiple Availability Zones (AZs). **Availability Zones** An Availability Zone (AZ) is a distinct location within a Region that is insulated from failures in other Availability Zones, and provides inexpensive, low-latency network connectivity to other Availability Zones in the same Region. A Region comprises at least two Availability Zones. By launching service instances in separate Availability Zones, applications can be protected from the failure of a single physical location. **AWS Services** Each AZ offers an identical IaaS cloud services platform, offering computing power (Elastic Compute Cloud), storage (Elastic Block Store, Simple Storage Service), secure communications (Virtual Private Cloud), and other functionality that enables customers to cost-effectively deploy applications and services with great flexibility, scalability, and reliability. The power of self-service through AWS means customers can proactively address internal plans and quickly react to external demands. In doing so, AWS provides customers with the option to choose only the services they require and the ability to provision or release them as needed. **AWS Infrastructure** AWS provides facilities, hardware and security features controlled by AWS at the infrastructure level. In the IaaS model, AWS is responsible for applicable service delivery layers including: infrastructure (i.e., hardware and software that comprise the infrastructure); and service management processes (i.e. the operation and management of the infrastructure and the system and software engineering lifecycles). Customers rely on AWS to manage the cloud infrastructure including the network, data storage, system resources, data centers, security, reliability, and supporting hardware and software. **Simple Storage Service (S3)** S3 is storage for the Internet. S3 is a highly scalable, durable, and available distributed object store designed for mission-critical and primary data storage. S3 stores objects redundantly on multiple devices across multiple facilities. S3 is designed to protect data and allow access to it even in the case of a failure of a data center. S3's versioning feature allows the retention of prior versions of objects stored in S3 and also protects against accidental deletions initiated by staff or software error. Versioning can be enabled on any S3 bucket. **Elastic Compute Cloud (EC2)** EC2 is a web service that provides resizable compute capacity in the cloud, which is essentially server instances used to build and host software systems. EC2 is designed to make web-scale computing easier for developers and customers to deploy virtual machines on demand. The simple web service interface allows customers to obtain and configure capacity

Module ID	Title	AWS implementation
		with minimal friction and provides complete control of their computing resources. EC2 changes the economics of computing by allowing enterprises to avoid large capital expenditures by paying only for capacity that is actually used. **Elastic Block Store (EBS)** EBS provides block level storage volumes for use with EC2 instances. EBS volumes are off-instance storage that persists independently from the life of an instance. Elastic Block Store provides highly available, highly reliable storage volumes that can be attached to a running EC2 instance and exposed as a device within the instance. EBS is particularly suited for applications that require a database, file system, or access to raw block level storage. EBS volumes store data redundantly, making them more durable than a typical hard drive. The annual failure rate for an EBS volume is 0.1% to 0.5%, compared to 4% for a commodity hard drive. EBS and EC2 are often used in conjunction with one another when building an application on the AWS platform. Any data that needs to persist can be stored on EBS volumes, not on the ephemeral storage associated with each EC2 instance. If the EC2 instance fails and needs to be replaced, the EBS volume can simply be attached to the new EC2 instance. Since this new instance is a duplicate of the original, there is no loss of data or functionality. EBS volumes are highly reliable, but to further mitigate the possibility of a failure, backups of these volumes can be created using a feature called snapshots. A robust backup strategy will include an interval between backups, a retention period and a recovery plan. Snapshots are stored for high-durability in Simple Storage Service (S3). Snapshots can be used to create new EBS volumes, which are an exact copy of the original volume at the time the snapshot was taken. These EBS operations can be performed through API calls. **Virtual Private Cloud (VPC)** VPC enables the creation of a logically separate space within AWS that can house compute resources and storage resources that can be connected to a customer's existing infrastructure through a virtual private network (VPN) connection or the internet. With VPC, it is possible to extend existing management capabilities and security services such as DNS, LDAP, Active Directory, firewalls, and intrusion detection systems to include private AWS resources, maintaining a consistent means of protecting information whether residing on internal IT resources or on AWS. Use of VPC allows a transition to the cloud using a customer's existing data center model and management scheme. It allows for the use of AWS resources as a virtual data center or site aligned with the customer's existing IP space and infrastructure. The customer controls the private cloud including IP addresses, subnets, firewall rules, VPN and/or Internet gateways, Access Control Lists and routing.
B 5.24	Web-Services	EC2, EBS and VPC hosts and devices reside on the EC2 network. API endpoints and S3 hosts and devices reside on the Prod network. Internet ingress and egress is through the Border/LBE network. The NAP network provides inter-Data Center connectivity along with the access path for AWS administrators. All of these networks reside within the authorization boundary. For both internet and AWS administrative connectivity, each Region connects to the Border and NAP networks. All allowed traffic flows are specifically authorized and controlled by access control lists. Regions are implemented using multiple data centers and the various networks connect to their peers at the other data centers. The EC2 network at one data center connects to the EC2 networks at the other data centers, for instance.

<table>
<tr><th>Module ID</th><th>Title</th><th>AWS implementation</th></tr>
<tr><td></td><td></td><td>
<p><b>Data Flow</b></p>
<p>Customers send API calls to AWS API endpoints to create and manage their storage (buckets, objects and volumes), compute instances and VPC environments. API endpoints can be accessed via http and https. Connections utilizing https are available on each type of API endpoint. S3 endpoints also offer the capability to connect and transfer data via http where non-sensitive data is being handled. This could be used to store data for public facing websites, for instance. Customers can connect their VPC environment to their existing network infrastructure using a site-to-site IPSEC VPN connection. Since the customer defines the IP addresses, VLANs and access control lists in use within their VPC environment, this would allow approved communication flows between the customer’s network and their VPC over a secure channel. Customers can also define a connection to the Internet for their VPC environment. The customer defines the internal IP addresses, VLANs and access control lists in use within their VPC environment. This provides the customer with the means to define the allowed communication flows from the internet to the customer’s resources.</p>
<p><b>Ports, Protocols and Services</b></p>
<p>The table below lists the Ports, Protocols, and Services enabled in this information system. TCP ports are indicated with a T and UDP ports are indicated with a U.</p>
<table>
<tr><th>Ports (T or U)</th><th>Protocols</th><th>Services</th><th>Purpose</th><th>Used By</th></tr>
<tr><td>80, 443 T</td><td>HTTP and HTTPS</td><td>Communication with API endpoints</td><td>Create and manage IaaS implementations</td><td>S3,EC2, EBS, VPC Administrators, Customers</td></tr>
<tr><td>22 T</td><td>SSH</td><td>Remote access</td><td>Manage hosts and network devices, manage EC2 instances</td><td>S3,EC2, EBS, VPC Administrators, Customers</td></tr>
<tr><td>53 U</td><td>DNS</td><td>Domain Name Services</td><td>Resolve names to IP addresses</td><td>S3,EC2, EBS, VPC
All users</td></tr>
<tr><td>N/A</td><td>AH and ESP (These are transport protocols with no concept of ports)</td><td>IPSEC VPN</td><td>Site to Site customer VPN connections to customer VPC environments</td><td>VPC
Customers</td></tr>
</table>
</td></tr>
</table>

AWS Reference Architectures

The flexibility of AWS allows customers to design application architectures according to their requirements. AWS Reference architectures provide customers with the architectural guidance they need in order to build an application that takes full advantage of the AWS services as well as supports the various security and compliance elements customers have to meet and maintain. Below are three use cases and recommendations, which Grundschutz catalogues should be modeled for the specific use case.

Information on how to configure each individual service in order to be able to be certified according to ISO 27001 on the basis of IT-Grundschutz cannot be provided due to the complex, diverse and unknown customer requirements and environments.

Architecture overview and IT-Grundschutz module alignment

Web Application Hosting

Highly available and scalable web hosting can be complex and expensive. Dense peak periods and wild swings in traffic patterns result in low utilization of expensive hardware. Amazon Web Services provides the reliable scalable, secure and high-performance infrastructure required for web applications, while enabling an elastic scale-out and scale-down infrastructure to match IT costs in real time as customer traffic fluctuates.

AWS Service	Description	IT-Grundschutz module implementation
Amazon Route 53	A highly available and scalable cloud Domain Name System (DNS) web service. It is designed to give developers and businesses an extremely reliable and cost effective way to route end users to Internet applications by translating names like www.example.com into the numeric IP addresses like 192.0.2.1 that computers use to connect to each other.	M 5.18 DNS-Server
Amazon CloudFront	A content delivery web service. Which, integrates with other Amazon Web Services products to give developers and businesses an easy way to distribute content to end users with low latency, high data transfer speeds, and no minimum usage commitments.	M 1.17 Cloud utilization M 3.304 Virtualization M 5.21 Web applications M 5.23 Cloud Management
Amazon Simple Storage Service (Amazon S3)	S3 provides developers and IT teams with secure, durable, highly scalable object storage. S3 stores data as objects within resources called "buckets." You can store as many objects as you want within a bucket, and write, read, and delete objects in your bucket. Objects can be up to 5 terabytes in size.	M 1.4 Data backup policy M 1.6 Protection against malware M 1.15 Deleting and destroying data M 3.303 Storage systems / Cloud Storage
Amazon Elastic Load Balancing	Automatically distributes incoming application traffic across multiple Amazon EC2 instances in the cloud. It enables you to achieve greater levels of fault tolerance in your applications, seamlessly providing the required amount of load balancing capacity needed to distribute application traffic.	M 3.302 Routers and switches M 4.1 Heterogeneous networks

AWS Service	Description	IT-Grundschutz module implementation
Amazon Elastic Compute Cloud (Amazon EC2)	EC2 presents a true virtual computing environment, allowing you to use web service interfaces to launch instances with a variety of operating systems, load them with your custom application environment, manage your network's access permissions, and run your image using as many or few systems as you desire.	M 1.14 Patch and change management M 1.16 Compliance management M 1.17 Cloud-utilization M 3.101 General server M 3.102 Servers under Unix M 3.108 Windows Server 2003 M 3.109 Windows Server 2008 M 3.304 Virtualization M 5.3 Groupware M 5.4 Web servers M 5.5 Lotus Notes / Domino M 5.12 Microsoft Exchange/Outlook M 5.15 General directory service M 5.16 Active Directory M 5.20 OpenLDAP M 5.21 Web applications M 5.22 Logging M 5.23 Cloud management M 5.24 Web services M 5.25 General applications
Amazon Machine Image (AMI)	AN AMI is a special type of virtual appliance that is used to instantiate (create) a virtual machine within EC2. It serves as the basic unit of deployment for services delivered using EC2.	M 1.17 Cloud utilization M 3.304 Virtualization M 5.21 Web applications
Auto Scaling	Auto Scaling helps you maintain application availability and allows you to scale your Amazon EC2 capacity up or down automatically according to conditions you define. Auto Scaling can also automatically increase the number of Amazon EC2 instances during demand spikes to maintain performance and decrease capacity during lulls to reduce costs.	M 1.17 Cloud utilization M 3.304 Virtualization
Amazon Relational Database Service (Amazon RDS)	A web service that makes it easy to set up, operates, and scales a relational database in the cloud. RDS gives you access to the capabilities of a MySQL, Oracle, SQL Server, PostgreSQL, or Amazon Aurora database engine running on your own Amazon RDS cloud-based database instance.	M 5.7 databases

Fault tolerance and High Availability

Systems that quickly failover to new instances in an event of failure

AWS Service	Description	IT-Grundschutz Module Implementation
Elastic Load Balancing	Automatically distributes incoming application traffic across multiple Amazon EC2 instances in the cloud. It enables you to achieve greater levels of fault tolerance in your applications, seamlessly providing the required amount of load balancing capacity needed to distribute application traffic.	M 3.302 Routers and switches M 4.1 Heterogene Netze
Availably Zones (AZs)	Amazon EC2 is hosted in multiple locations worldwide. These locations are composed of regions and Availability Zones. Each region is a separate geographic area. Each region has multiple, isolated locations known as Availability Zones. Amazon EC2 provides you the ability to place resources, such as instances, and data in multiple locations. Customer Resources aren't replicated across regions unless the customer specifically designs the replication using two AZs.	M 2.1 Allgemeines Gebäude M 2.2 Elektrotechnische Verkabelung M 2.9 Rechenzentrum M 2.12 IT-Verkabelung
Elastic IP Addresses (EIP)	An *Elastic IP address* (EIP) is a static IP address designed for dynamic cloud computing. With an EIP, you can mask the failure of an instance or software by rapidly remapping the address to another instance in your account. Your EIP is associated with your AWS account, not a particular instance, and it remains associated with your account until you choose to explicitly release it.	M 3.302 Router und Switches M 4.1 Heterogeneous networks
Elastic Block Store (EBS)	Amazon EBS allows you to create storage volumes and attach them to Amazon EC2 instances. Once attached, you can create a file system on top of these volumes, run a database, or use them in any other way you would use a block device. Amazon EBS volumes are placed in a specific Availability Zone, where they are automatically replicated to protect you from the failure of a single component.	M 1.4 Data backup policy M 1.6 Protection against malware M 1.15 Deleting and destroying data M 3.303 Storage systems / Cloud Storage
Amazon Simple Storage Service (Amazon S3)	S3 provides developers and IT teams with secure, durable, highly scalable object storage. S3 stores data as objects within resources called "buckets." You can store as many objects as you want within a bucket, and write, read, and delete objects in your bucket. Objects can be up to 5 terabytes in size.	M 1.4 Data backup policy M 1.6 Protection against malware M 1.15 Deleting and destroying data M 3.303 Storage systems / Cloud Storage

Financial Services Grid Computing

Highly scalable and elastic grids for the Financial Services Sector

AWS Service	Description	IT-Grundschutz Module Implementation
Amazon Simple Storage Service (Amazon S3)	S3 provides developers and IT teams with secure, durable, highly scalable object storage. S3 stores data as objects within resources called "buckets." You can store as many objects as you want within a bucket, and write, read, and delete objects in your bucket. Objects can be up to 5 terabytes in size.	M 1.4 Data backup policy M 1.6 Protection against malware M 1.15 Deleting and destroying data M 3.303 Storage systems / Cloud Storage

AWS Service	Description	IT-Grundschutz Module Implementation
AWS Direct Connect	AWS Direct Connect lets you establish a dedicated network connection between your network and one of the AWS Direct Connect locations. Using industry standard 802.1q VLANs, this dedicated connection can be partitioned into multiple virtual interfaces.	M 4.4 VPN
Amazon Relational Database Service (Amazon RDS)	Amazon RDS is designed for developers or businesses who require the full features and capabilities of a relational database, or who wish to migrate existing applications and tools that utilize a relational database. It gives you access to the capabilities of a MySQL, Oracle, SQL Server, PostgreSQL, or Amazon Aurora database engine running on your own Amazon RDS cloud-based database instance.	M 5.7 Databases
Amazon Elastic Compute Cloud (Amazon EC2)	EC2 presents a true virtual computing environment, allowing you to use web service interfaces to launch instances with a variety of operating systems, load them with your custom application environment, manage your network's access permissions, and run your image using as many or few systems as you desire.	M 1.14 Patch and change management M 1.16 Compliance management M 1.17 Cloud-utilization M 3.101 General server M 3.102 Servers under Unix M 3.108 Windows Server 2003 M 3.109 Windows Server 2008 M 3.304 Virtualization M 5.3 Groupware M 5.4 Web servers M 5.5 Lotus Notes / Domino M 5.12 Microsoft Exchange/Outlook M 5.15 General directory service M 5.16 Active Directory M 5.20 OpenLDAP M 5.21 Web applications M 5.22 Logging M 5.23 Cloud management M 5.24 Web services M 5.25 General applications
Amazon Machine Image (AMI)	AN AMI is a special type of virtual appliance that is used to instantiate (create) a virtual machine within EC2. It serves as the basic unit of deployment for services delivered using EC2.	M 1.17 Cloud utilization M 3.304 Virtualization M 5.21 Web applications
Amazon Simple Storage Service (Amazon S3)	S3 provides developers and IT teams with secure, durable, highly scalable object storage. S3 stores data as objects within resources called "buckets." You can store as many objects as you want within a bucket, and write, read, and delete objects in your bucket. Objects can be up to 5 terabytes in size.	M 1.4 Data backup policy M 1.6 Protection against malware M 1.15 Deleting and destroying data M 3.303 Storage systems / Cloud Storage

AWS Service	Description	IT-Grundschutz Module Implementation
Amazon DynamoDB	Is a fast and flexible NoSQL database service for all applications that need consistent, single-digit millisecond latency at any scale. It is a fully managed database and supports both document and key-value data models. Its flexible data model and reliable performance make it a great fit for mobile, web, gaming, ad-tech, IoT, and many other applications.	M 5.7 Databases
Amazon Elastic MapReduce (Amazon EMR)	Is a web service that makes it easy to quickly and cost-effectively process vast amounts of data. Amazon EMR uses Hadoop, an open source framework, to distribute your data and processing across a resizable cluster of Amazon EC2 instances. It can also run other distributed frameworks such as Spark and Presto. Amazon EMR is used in a variety of applications, including log analysis, web indexing, data warehousing, machine learning, financial analysis, scientific simulation, and bioinformatics. Customers launch millions of Amazon EMR clusters every year.	M 5.21 Web applications M 5.24 Web services M 5.25 General applications
Amazon Glacier	Data is stored in Amazon Glacier in "archives." An archive can be any data such as a photo, video, or document. You can upload a single file as an archive or aggregate multiple files into a TAR or ZIP file and upload as one archive. A single archive can be as large as 40 terabytes. You can store an unlimited number of archives and an unlimited amount of data in Amazon Glacier. Each archive is assigned a unique archive ID at the time of creation, and the content of the archive is immutable, meaning that after an archive is created it cannot be updated.	M 1.12 Archiving