

# CSA STAR: Cybersecurity for cloud computing Transition Training Course (CCM version 4.0)



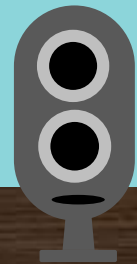
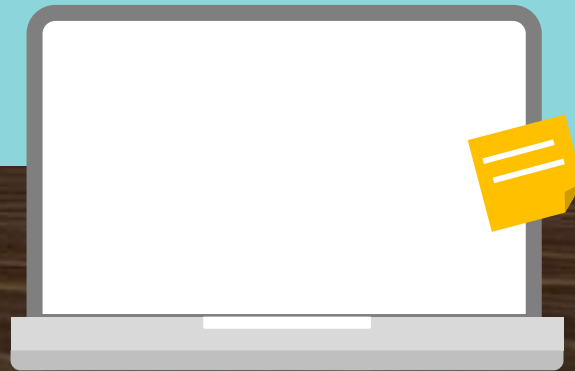
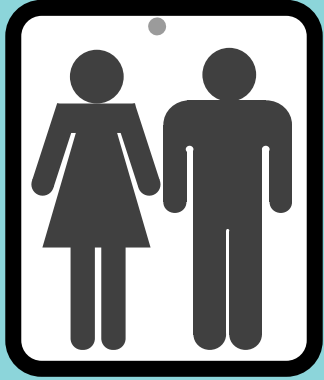
By Royal Charter

**bsi.**

# Benefits to you



Welcome



# Content of discussion

- Introduction of CSA and CSA STAR Certificate
- New version of CCM/CAIQ version 4.0 (4.0.1)
- Mapping for CCM version 4.0, CCM version 3.01 and ISO/IEC 27001 series

# Who is CSA



# Who are the Cloud Security Alliance?

comprehensive research program works in collaboration with industry, higher education and government on a global basis

Founded 2008

In 2009, CSA released the Security Guidance for Critical Areas of Focus In Cloud Computing



The world's leading organization to secure cloud computing environment best practices

The most popular cloud security provider certification Program (CSA STAR)

# What is

## Security, Trust, Assurance and Risk (STAR)

The industry's most powerful program for  
security assurance in the cloud.

[View the Registry](#)

[Submit to Registry](#)



# Levels of STAR





# Level 1: Self-Assessment



## Level 1: Self-Assessment

At level one organizations can submit one or both of the security and privacy self-assessments. For the security assessment, organizations use the [Cloud Controls Matrix](#) to evaluate and document their security controls. The privacy assessment submissions are based on the [GDPR Code of Conduct](#).

### Who should pursue level one?

Organizations should pursue this level if they are...

- Operating in a low-risk environment
- Wanting to offer increased transparency around the security controls they have in place.
- Looking for a cost-effective way to improve trust and transparency

# Level 2: Third-Party Audit



## Level 2: Third-Party Audit

Level 2 of STAR allows organizations to build off of other industry certifications and standards to make them specific for the cloud.

Organizations looking for a third-party audit can choose from one or more of the security and privacy audits and certifications. An organization's location, along with the regulations and standards it is subject to will have the greatest factor in determining which ones are appropriate to pursue.

## Which organizations should pursue level 2?

Organizations should pursue this level if they are...

- Operating in a medium to high risk environment
- Already hold or adhere to the following: ISO27001, SOC 2, GB/T 22080-2008, or GDPR
- Looking for a cost-effective way to increase assurance for cloud security and privacy.

**There are associated fees** for STAR Level 2. [CSA Corporate Members](#) receive a price reduction on STAR Level 2 certifications and attestations.

# CSA Trusted Cloud Providers



## CSA Trusted Cloud Providers

Organizations listed as CSA Trusted Cloud Providers in the registry are [CSA Corporate Members](#) that have also fulfilled additional training and volunteer requirements with CSA. Fulfilling these requirements demonstrates a commitment to the professional development of their employees to achieve cloud security competency, and a commitment to the industry at large.

[Read the FAQ →](#)

[Read the press release →](#)

[View trusted cloud providers →](#)

[Contact us to apply →](#)

# STAR Foundation Tools

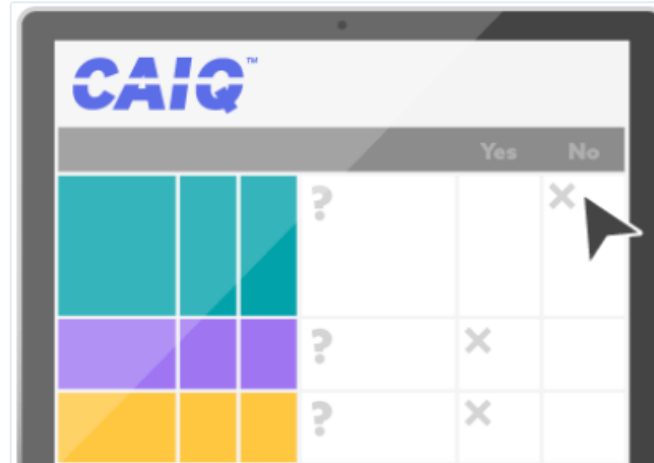
## Security



CCM				
Blue	Blue	-	x	x
Blue	Blue	-	x	x
Orange	Orange	-	x	x

### Cloud Controls Matrix

The only meta-framework of cloud-specific security controls, mapped to leading standards, best practices and regulations, CCM is currently considered a de-facto standard for cloud security assurance and compliance.



CAIQ			Yes	No
Teal	Teal	?		x
Purple	Purple	?	x	
Yellow	Yellow	?	x	

### CAIQ

CAIQ is a set of Yes/No questions for cloud consumers and auditors to assess the security capabilities of a cloud service provider. Cloud providers fill this in to complete the STAR Level 1 Self-Assessment.

## Privacy



### GDPR Code of Conduct

Contains all the necessary requirements a Cloud Service Provider has to satisfy in order to comply with the EU GDPR. Created in collaboration with representatives from the EU national data protection authorities, this code assists organizations in adhering to the European General Data Protection Regulation.

# New version of CCM, CIAQ version 4.0

The CSA Cloud Controls Matrix (CCM) is a cybersecurity control framework for cloud computing.



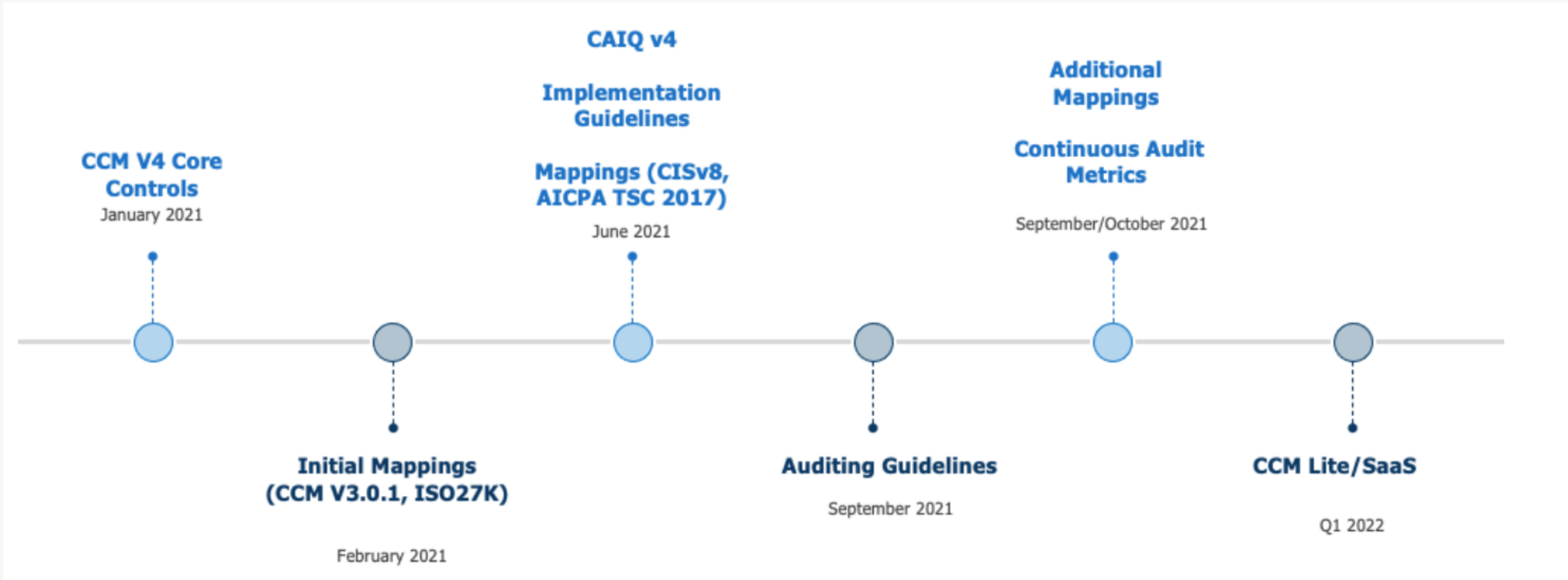
By Royal Charter

**bsi.**

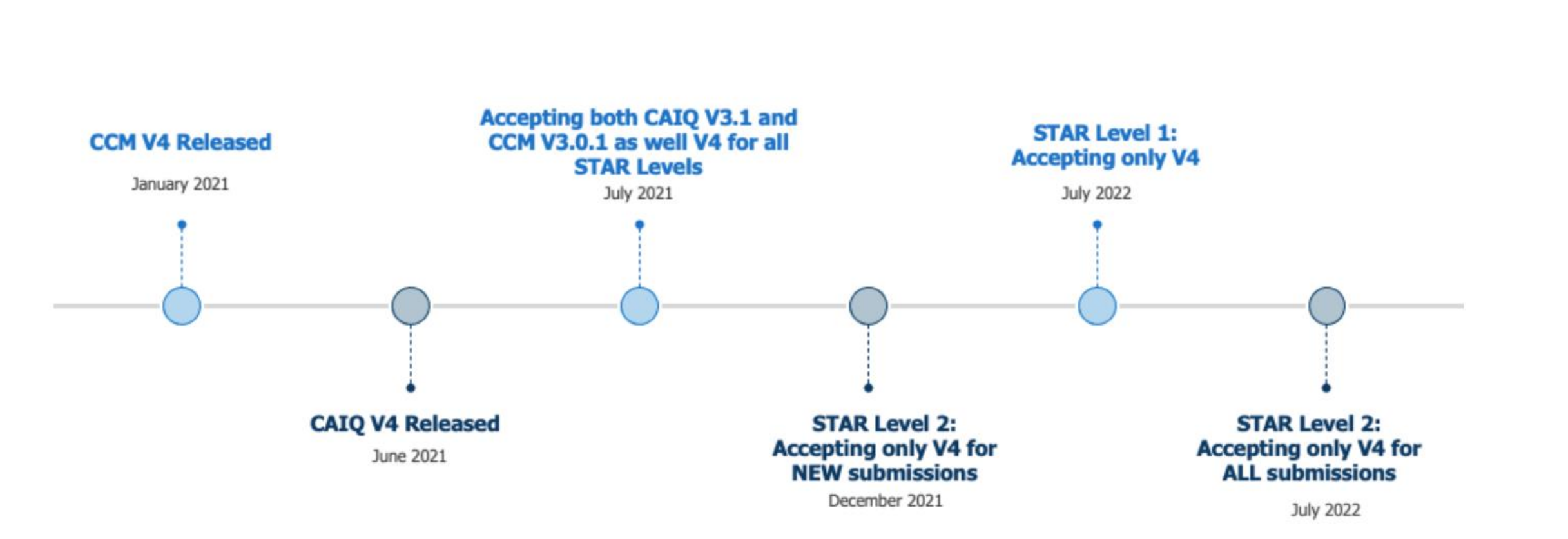
# CCM version 4.0

- On January 2021 CSA released version 4 of the Cloud Controls Matrix (CCM).
- The new version ensures coverage of requirements deriving from new cloud technologies, new controls and enhanced interoperability and compatibility with other standards

# CCM v4 Components Release Timeline (Ref. CSA Website)



# STAR Program Transition Timeline





# Changed in CCM Version 4.0

## Major improvement

- New structure that better reflects the cloud security and privacy requirements of modern cloud services
- New additional controls
- An improved language that favors the implementation and evaluation of the controls

## Adds new features

- CCM Implementation Guidelines (expected to be published in July),
- CCM Auditing Guidelines (expected to be published in September)
- CCM Metrics (expected to be published in September).

# What is changing in CAIQ v4?

- The number of questions 261 (compared to the 310 of the V3.1)
- The structure of the document used for the submissions for the STAR Level 1
- New columns for the Security Shared Responsibility Model (SSRM) were added to help address one of the biggest risks in the cloud ecosystem – Cloud Service Provider (CSP), Cloud Service Customer (CSC) -> csp-owned, csc-owned, share

# Changed in CCM Version 4.0

- Ensured coverage of requirements deriving from new cloud technologies.
- New controls and security responsibility matrix, improved auditability of the controls, and enhanced interoperability and compatibility with other standards.
- Changes in structure of the framework with a new domain dedicated to Log and Monitoring (LOG), and modifications in the existing ones (GRC, A&A, UEM, CEK, DSP).
- 197 control objectives that are structured in 17 domains

# Difference CCM V. 4.0 and V. 3.01 (In general)

## CCM version 4.0

- 197 Control Objectives and 17 Domains
- Audit & Assurance (A&A) / A&A-01 to A&A-06
- Cryptography, Encryption & Key Management (CEK)/ CEK-01 to CEK-21
- Governance, Risk Management & Compliance (GRC) / GRC-01 to GRC-08
- Universal Endpoint Management (UEM)/ UEM-01 to UEM-14
- Data Security and Privacy Lifecycle Management (DSP)/ DSP-01 to DSP-19
- New - Log and Monitoring (LOG) / LOG-01 to LOG-13

## CCM version 3.01

- 133 Controls Objective and 16 Domains
- Audit Assurance & Compliance (AAC) / AAC-01 to AAC-03
- Encryption & Key Management (EKM) / EKM-01 to EKM-04
- Governance and Risk Management (GRM) / GRM-01 to GRM-11
- Mobile Security (MOS) / MOS-01 to MOS-20
- Data Security & Information Lifecycle Management (DSI) / DSI-01 to DSI-07

# Difference CCM V. 4.0 and V. 3.01 (In general)

## CCM version 4.0

- Application & Interface Security (AIS) / AIS-01 to AIS-07
- Business Continuity Management and Operational Resilience (BCR) / BCR-01 to BCR-11
- Change Control and Configuration Management (CCC) / CCC-01 to CCC-09
- Datacenter Security (DCS) / DCS-01 to DCS-15
- Human Resources (HRS) / HRS-01 to HRS-13
- Identity & Access Management (IAM) / IAM-01 to IAM-16
- Interoperability & Portability (IPY) / IPY-01 to IPY-04
- Infrastructure & Virtualization Security (IVS) / IVS-01 to IVS-09

## CCM version 3.01

- Application & Interface Security (AIS) / AIS-01 to AIS-04
- Business Continuity Management & Operational Resilience (BCR) / BCR-01 to BCR-11
- Change Control & Configuration Management (CCC) / CCC-01 to CCC-05
- Datacenter Security (DCS) / DCS-01 to DCS-09
- Human Resources (HRS) / HRS-01 to HRS-11
- Identity & Access Management (IAM) / IAM-01 to IAM-13
- Interoperability & Portability (IPY) / IPY-01 to IPY-05
- Infrastructure & Virtualization Security (IVS) / IVS-01 to IVS-13

# Difference CCM V. 4.0 and V. 3.01 (In general)

- Security Incident Management, E-Discovery, & Cloud Forensics (SEF) / SEF-01 to SEF-08
  - Supply Chain Management, Transparency, and Accountability (STA) / STA-01 to STA-14
  - Threat & Vulnerability Management (TVM) / TVM-01 to TVM-10
- Security Incident Management, E-Discovery, & Cloud Forensics (SEF) / SEF-01 to SEF-05
  - Supply Chain Management, Transparency, and Accountability (STA) / STA-01 to STA-09
  - Threat & Vulnerability Management (TVM) / TVM-01 to TVM-03



# Course review & Final Questions

# Mapping

CSA-CCM V4.0 VS CSA-CCM V3.0.1  
and ISO/IEC 27001 series



By Royal Charter

**bsi.**





# Audit and Assurance - A&A

# Audit & Assurance - A&A

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
Audit and Assurance Policy and Procedures	A&A-01	Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually.	GRM-06 GRM-09	Partial Gap	Missing specification(s) in CCMv3.0.1: 'apply and evaluate audit and assurance policies, procedures and standards' Requirement of 'at least annually' in last sentence.	27001: 9.2	Partial Gap	Missing specification(s) in ISOs: Requirement of 'at least annually' in last sentence.
Independent Assessments	A&A-02	Conduct independent audit and assurance assessments according to relevant standards at least annually.	AAC-02	No Gap	N/A	27001: A.18.2.1 27002: 18.2.1	Partial Gap	Missing specification(s) in ISOs: Terms 'audit and assurance' and 'at least annually' are not specifically called out.
Risk Based Planning Assessment	A&A-03	Perform independent audit and assurance assessments according to risk-based plans and policies.	AAC-01 AAC-02	No Gap	N/A	27001: A.18.2.1 27002: 18.2.1 27018: 18.2.1	No Gap	N/A
Requirements Compliance	A&A-04	Verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit.	GRM-01 GRM-03	No Gap	N/A	27001: A.18.2.2 27002: 18.2.2 27001: A.18.2.3 27002: 18.2.3	No Gap	N/A
Audit Management Process	A&A-05	Define and implement an Audit Management process to support audit planning, risk analysis, security control assessment, conclusion, remediation schedules, report generation, and review of past reports and supporting evidence.	AAC-01	Partial Gap	Recommend the full V4 control specification to be used to close the gap. Portion in the mapped control(s) contributing to the partial gap, that is, covering in part the V4 control: (AAC-01) 'Audit plans shall be developed' and 'Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations'.	27001: 9.2.c 27001: A.18.2.2 27002: 18.2.2	No Gap	N/A
Remediation	A&A-06	Establish, document, approve, communicate, apply, evaluate and maintain a risk-based corrective action plan to remediate audit findings, review and report remediation status to relevant stakeholders.	GRM-10 GRM-11	Partial Gap	Missing specification(s) in CCMv3.0.1: 'Establish, document, approve, communicate, apply, evaluate and maintain a risk-based corrective action plan'	27001: A.18.2.2 27002: 18.2.2	Partial Gap	Missing specification(s) in ISOs: 'Establish, document, approve, communicate, apply, evaluate and maintain a risk-based corrective action plan to remediate audit findings'.



# Application and Interface Security - AIS

# Application & Interface Security – AIS (1)

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
Application and Interface Security Policy and Procedures	<b>AIS-01</b>	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for application security to provide guidance to the appropriate planning, delivery and support of the organization's application security capabilities. Review and update the policies and procedures at least annually.	<b>AIS-01 AIS-04</b>	<b>Partial Gap</b>	Missing specification(s) in CCMv3.0.1: 'apply, evaluate, maintain policies and procedures for application security' Requirement of 'at least annually' in last sentence.	<b>27001: A.14.2.1 27002: 14.2.1 27017: 14.2.1 27001: A.14.2.5 27001: 14.2.5 27017: 14.2.5</b>	<b>Partial Gap</b>	Missing specification(s) in ISOs: 'to review and update the policies and procedures at least annually.'
Application Security Baseline Requirements	<b>AIS-02</b>	Establish, document and maintain baseline requirements for securing different applications.	<b>AIS-01</b>	<b>No Gap</b>	N/A	<b>27001: A.5.1.1 27017: 5.1.1 27001: A.7.2.2 27002: 7.2.2</b>	<b>Partial Gap</b>	Missing specification(s) in ISOs: ISO does not explicitly stipulate baseline requirements for securing different applications.
Application Security Metrics	<b>AIS-03</b>	Define and implement technical and operational metrics in alignment with business objectives, security requirements, and compliance obligations.	<b>No Mapping</b>	<b>Full Gap</b>	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	<b>27001: 9.1 27001: A.18.2.2 27002: 18.2.2</b>	<b>Partial Gap</b>	Missing specification(s) in ISOs: ISO does not explicitly specify the need to implement technical and operational metrics in alignment with business objectives, security requirements, and compliance obligations.

# Application & Interface Security – AIS (2)

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
Secure Application Design and Development	AIS-04	Define and implement a SDLC process for application design, development, deployment, and operation in accordance with security requirements defined by the organization.	AIS-01 AIS-03	Partial Gap	Recommend the full V4 control specification to be used to close the gap.  Portion in the mapped control(s) contributing to the partial gap, that is, covering in part the V4 control: (AIS-01) 'Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards'	27001: A.14.1.1 27002: 14.1.1 27017: 14.1.1 27001: A.14.1.2 27002: 14.1.2 27017: 14.1.2 27001: A.14.2.1 27002: 14.2.1 27017: 14.2.1	No Gap	N/A
Automated Application Security Testing	AIS-05	Implement a testing strategy, including criteria for acceptance of new information systems, upgrades and new versions, which provides application security assurance and maintains compliance while enabling organizational speed of delivery goals. Automate when applicable and possible.	AIS-01 AIS-03	Partial Gap	Missing specification(s) in CCMv3.0.1: 'Automate when applicable and possible.'	27001: A.14.2.8 27001: A.14.2.9 27001: A.12.1.2 27002: 12.1.2 27001: A.14.1.1 27002: 14.1.1 27001: A.14.2.2 27002: 14.2.2	No Gap	N/A
Automated Secure Application Deployment	AIS-06	Establish and implement strategies and capabilities for secure, standardized, and compliant application deployment. Automate where possible.	AIS-01 AIS-03	Partial Gap	Missing specification(s) in CCMv3.0.1: 'Automate where possible.'	No mapping	Full Gap	The full V4 control specification is missing from the ISOs and has to be used to close the gap.
Application Vulnerability Remediation	AIS-07	Define and implement a process to remediate application security vulnerabilities, automating remediation when possible.	TVM-02	Partial Gap	Missing specification(s) in CCMv3.0.1: 'Automating remediation when possible.'	27001: A.16.1.5 27002: 16.1.5 27017: 16.1.5 27001: A.12.6.1 27002: 12.6.1 27017: 12.6.1 27018: 12.6.1	No Gap	N/A



# Business Continuity Management and Operational Resilience - BCR

# Business Continuity Management and Operational Resilience - BCR (1)

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
Business Continuity Management Policy and Procedures	BCR-01	Establish, document, approve, communicate, apply, evaluate and maintain business continuity management and operational resilience policies and procedures. Review and update the policies and procedures at least annually.	BCR-07 BCR-10 BCR-11 GRM-06 GRM-09	Partial Gap	Missing specification(s) in CCMv3.0.1: Requirement of 'at least annually' in last sentence.	27001: 5.2 27001: A.5.1 27001: A.7.2.1 27001: A.17.1.2	Partial Gap	Missing specification(s) in ISOs: The requirement to provide a framework for setting business continuity objectives.
Risk Assessment and Impact Analysis	BCR-02	Determine the impact of business disruptions and risks to establish criteria for developing business continuity and operational resilience strategies and capabilities.	BCR-09	No Gap	N/A	27001: 6.1.1 27001: 6.1.2 27001: 6.1.3 27001: 8.2 27001: 8.3 27001: A.16.1.6 27001: A.17.1	Partial Gap	Missing specification(s) in ISOs: The specific references to a BIA.
Business Continuity Strategy	BCR-03	Establish strategies to reduce the impact of, withstand, and recover from business disruptions within risk appetite.	BCR-04 BCR-06 BCR-08	No Gap	N/A	27001: A.17.1.1 27001: A.17.1.2	Partial Gap	Missing specification(s) in ISOs: No reference to Business Continuity Strategies
Business Continuity Planning	BCR-04	Establish, document, approve, communicate, apply, evaluate and maintain a business continuity plan based on the results of the operational resilience strategies and capabilities.	BCR-01	No Gap	N/A	27001: A.17.1.1 27001: A.17.1.3	Partial Gap	Missing specification(s) in ISOs: No reference to Business Continuity Strategies
Documentation	BCR-05	Develop, identify, and acquire documentation that is relevant to support the business continuity and operational resilience programs. Make the documentation available to authorized stakeholders and review periodically.	BCR-01 BCR-04	No Gap	N/A	27001: 7.5.1a	Partial Gap	Missing specification(s) in ISOs: No reference to Business Continuity Strategies

# Business Continuity Management and Operational Resilience - BCR (2)

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
Business Continuity Exercises	<b>BCR-06</b>	Exercise and test business continuity and operational resilience plans at least annually or upon significant changes.	<b>BCR-02</b>	<b>Partial Gap</b>	Missing specification(s) in CCMv3.0.1: 'at least annually'	<b>27001: A.17.1.3</b>	<b>Partial Gap</b>	Missing specification(s) in ISOs: 'Table Top Exercises'
Communication	<b>BCR-07</b>	Establish communication with stakeholders and participants in the course of business continuity and resilience procedures.	<b>BCR-01 BCR-02</b>	<b>No Gap</b>	N/A	<b>No Mapping</b>	<b>Full Gap</b>	The full V4 control specification is missing from the ISOs and has to be used to close the gap.
Backup	<b>BCR-08</b>	Periodically backup data stored in the cloud. Ensure the confidentiality, integrity and availability of the backup, and verify data restoration from backup for resiliency.	<b>BCR-11</b>	<b>Partial Gap</b>	Missing specification(s) in CCMv3.0.1: 'Ensure the confidentiality, integrity and availability of the backup'	<b>27001: A.12.3 27017: 12.3 27018: 12.3.1</b>	<b>Partial Gap</b>	Missing specification(s) in ISOs: ISO does not specify the need to verify data restoration from backup for resiliency.
Disaster Response Plan	<b>BCR-09</b>	Establish, document, approve, communicate, apply, evaluate and maintain a disaster response plan to recover from natural and man-made disasters. Update the plan at least annually or upon significant changes.	<b>No Mapping</b>	<b>Full Gap</b>	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	<b>No Mapping</b>	<b>Full Gap</b>	The full V4 control specification is missing from the ISOs and has to be used to close the gap.
Response Plan Exercise	<b>BCR-10</b>	Exercise the disaster response plan annually or upon significant changes, including if possible local emergency authorities.	<b>No Mapping</b>	<b>Full Gap</b>	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	<b>No Mapping</b>	<b>Full Gap</b>	The full V4 control specification is missing from the ISOs and has to be used to close the gap.
Equipment Redundancy	<b>BCR-11</b>	Supplement business-critical equipment with redundant equipment independently located at a reasonable minimum distance in accordance with applicable industry standards.	<b>BCR-06</b>	<b>No Gap</b>	N/A	<b>No Mapping</b>	<b>Full Gap</b>	The full V4 control specification is missing from the ISOs and has to be used to close the gap.





# Change Control and Configuration Management - CCC

# Change Control and Configuration Management - CCC (1)

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
Change Management Policy and Procedures	CCC-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for managing the risks associated with applying changes to organization assets, including application, systems, infrastructure, configuration, etc., regardless of whether the assets are managed internally or externally (i.e., outsourced). Review and update the policies and procedures at least annually.	CCC-05 GRM-06 GRM-09	Partial Gap	Missing specification(s) in CCMv3.0.1: 'apply, evaluate policies and procedures for managing the risks associated with applying changes to organization assets' 'regardless of whether the assets are managed internally or externally (i.e., outsourced)' Requirement of 'at least annually' in last sentence.	27001: A.12.1.1 27001: A.12.1.2 27002: 12.1.2 27017: 12.1.2 27001: A.14.2.2 27001: A.14.2.3	Partial Gap	Missing specification(s) in ISOs: 'Review and update the policies and procedures at least annually.'
Quality Testing	CCC-02	Follow a defined quality change control, approval and testing process with established baselines, testing, and release standards.	CCC-03	No Gap	N/A	27001: A.14.2.2 27002: 14.2.2 27017: 14.2.2	Partial Gap	Missing specification(s) in ISOs: 'Quality and baselines'
Change Management Technology	CCC-03	Manage the risks associated with applying changes to organization assets, including application, systems, infrastructure, configuration, etc., regardless of whether the assets are managed internally or externally (i.e., outsourced).	CCC-05	Partial Gap	Missing specification(s) in CCMv3.0.1: 'regardless of whether the assets are managed internally or externally (i.e., outsourced)'	27001:A.5.1.1 27017: 5.1.1 27001: A.12.1.2 27002: 12.1.2 27001: A.12.1.4 27001: A.14.2.3 27001: A.15.2.2 27002: 15.2.2 27001: A.14.2.6 27002: 14.2.6	No Gap	N/A

# Change Control and Configuration Management - CCC (2)

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
Unauthorized Change Protection	CCC-04	Restrict the unauthorized addition, removal, update, and management of organization assets.	CCC-04	Partial Gap	Missing specification(s) in CCMv3.0.1: 'removal, update, and management of organization assets'	27001: A.12.1.4 27002: 12.1.4 27001: A.12.4.2 27002: 12.4.2 27001: A.14.2.2 27017: 14.2.2	No Gap	N/A
Change Agreements	CCC-05	Include provisions limiting changes directly impacting CSCs owned environments/tenants to explicitly authorized requests within service level agreements between CSPs and CSCs.	CCC-05	No Gap	N/A	27001: A.15.2.2 27001: A.14.2.2 27002: 14.2.2 27001: A.12.1.2 27017: 12.1.2	No Gap	N/A
Change Management Baseline	CCC-06	Establish change management baselines for all relevant authorized changes on organization assets.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	27001: A.12.1.1 27002: 12.1.1 27001: 14.2.2 27002: 14.2.2	Partial Gap	Missing specification(s) in ISOs: 'Establish change management baselines'

# Change Control and Configuration Management - CCC (3)

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
Detection of Baseline Deviation	CCC-07	Implement detection measures with proactive notification in case of changes deviating from the established baseline.	GRM-01	Partial Gap	Missing specification(s) in CCMv3.0.1: 'detection measures with proactive notification'	27001: A.14.2.2 27001: A.14.2.4 27001: A.12.4.1 27002: 12.4.1 (g) 27001: A.5.1.1 27017: 5.1.1	No Gap	N/A
Exception Management	CCC-08	Implement a procedure for the management of exceptions, including emergencies, in the change and configuration process. Align the procedure with the requirements of GRC-04: Policy Exception Process.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	27001: A.12.1.2 27002: 12.1.2 (h) 27017: 12.1.2	No Gap	N/A
Change Restoration	CCC-09	Define and implement a process to proactively roll back changes to a previous known good state in case of errors or security concerns.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	27001: A.12.1.2 27002: 12.1.2 (g) 27001: A.12.5.1 27002: 12.5.1 (e) 27001: A.12.3.1 27017: 12.3.1	No Gap	N/A

# Cryptography, Encryption and Key Management - CEK

# Cryptography, Encryption & Key Management – CEK (1)

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
Encryption and Key Management Policy and Procedures	CEK-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Cryptography, Encryption and Key Management. Review and update the policies and procedures at least annually.	EKM-01 EKM-02 EKM-03 GRM-06 GRM-09	Partial Gap	Missing specification(s) in CCMv3.0.1: 'Apply and evaluate the policies and procedures for Cryptography, Encryption and Key Management' Requirement of 'at least annually' in last sentence.	27001: A.5 27002: 5 27001: 5.2 27001: 5.3 27001: A.6.1.1 27002 : 6.1.1 27001: A.6.1.2 27002: 6.1.2 27001: 8.2 27001: 8.3 27001: 9.1	No Gap	N/A
CEK Roles and Responsibilities	CEK-02	Define and implement cryptographic, encryption and key management roles and responsibilities.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	27001: 5.1 27001: 5.3 27001: A.5.1.1 27002: 5.1.1 27001: A.6.1.1 27002: 6.1.1 27017: 6.1.1 27001: A.6.1.2 27017: 6.1.2 27001: A.9.1 27002: 9.1 27001: A.10.1.1 27002: 10.1.1 27001: A.15.1.2 27017: 15.1.2 27001: A.13.1.3 27017: 13.1.3 27001: A.10.1.1 27017: 10.1.1 27001: A.10.1.2 27002: 10.1.2 27017: 10.1.2 27017: CLD 6.3	No Gap	N/A

# Cryptography, Encryption & Key Management – CEK (2)

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
Data Encryption	CEK-03	Provide cryptographic protection to data at-rest and in-transit, using cryptographic libraries certified to approved standards.	EKM-03 EKM-04	No Gap	N/A	27001: A.18.1.1 27001: A.18.1.2 27001: A.18.1.3 27001: A.18.1.4 27001: A.18.1.5 27001: A.10.1 27002: 10.1 27001: A.13.2.1 27002: 13.2.1 27001: A.18 27002: 18 27001: A.14.1.2 27002: 14.1.2 27001: A.14.1.3 27002 14.1.3 c) 27001 - A.10.1.1 27017 - 10.1.1 27001 - A.10.1.2 27017 - 10.1.2	No Gap	N/A
Encryption Algorithm	CEK-04	Use encryption algorithms that are appropriate for data protection, considering the classification of data, associated risks, and usability of the encryption technology.	EKM-04	Partial Gap	Missing specification(s) in CCMv3.0.1: 'considering the classification of data, associated risks, and usability of the encryption technology.'	27001: A.8.2 27002: 8.2 27001: A.8.3 27001: A.10.1.1 27002: 10.1.1 (b) 27001: A.10.1.2 27002: 10.1.2	No Gap	N/A
Encryption Change Management	CEK-05	Establish a standard change management procedure, to accommodate changes from internal and external sources, for review, approval, implementation and communication of cryptographic, encryption and key management technology changes.	EKM-02	Partial Gap	Recommend the full V4 control specification to be used to close the gap. Portion in the mapped control(s) contributing to the partial gap, that is, covering in part the V4 control: (EKM-02) 'lifecycle management/replacement' and 'changes within the cryptosystem'	27001: A.12.1.2 27002: 12.1.2 27017: 12.1.2 27001: A.10.1.2 27002: 10.1.2 e) 27001: A.14.2.2 27002: 14.2.2	No Gap	N/A

# Cryptography, Encryption & Key Management – CEK (3)

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
Encryption Change Cost Benefit Analysis	CEK-06	Manage and adopt changes to cryptography-, encryption-, and key management-related systems (including policies and procedures) that fully account for downstream effects of proposed changes, including residual risk, cost, and benefits analysis.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	27001: A.12.1.2 27002: 12.1.2 27001: A.10.1.2 27002: 10.1.2 e) 27017: 10.1.2 27001: A.10.1.1 27002: 10.1.1 27017: 10.1.1	No Gap	N/A
Encryption Risk Management	CEK-07	Establish and maintain an encryption and key management risk program that includes provisions for risk assessment, risk treatment, risk context, monitoring, and feedback.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	27001: 8.2 27001: 8.3 27001: A.10.1.1 27002: 10.1.1 27017: 10.1.1 27001: A.10.1.2 27017: 10.1.2	No Gap	N/A
CSC Key Management Capability	CEK-08	CSPs must provide the capability for CSCs to manage their own data encryption keys.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	27001: A.10.1 27017: 10.1 27001: A.10.1.1 27017: 10.1.1 27001: A.10.1.2 27017: 10.1.2	Partial Gap	Missing specification(s) in ISOs: 'The cloud service provider should provide capabilities to permit the cloud service customer to independently store and manage encryption keys used for protection of any data owned or managed by the cloud service customer'



# Cryptography, Encryption & Key Management – CEK (4)

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
Encryption and Key Management Audit	CEK-09	Audit encryption and key management systems, policies, and processes with a frequency that is proportional to the risk exposure of the system with audit occurring preferably continuously but at least annually and after any security event(s).	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	27001: 9.2 27001: A.18.2.1 27001: A.18.2.2 27001: A.12.7 27002: 12.7 27017: 12.7 27001: A.10.1.2 27001: A.10.1.2 27002: 10.1.2 k)	No Gap	N/A
Key Generation	CEK-10	Generate Cryptographic keys using industry accepted cryptographic libraries specifying the algorithm strength and the random number generator used.	EKM-04	Partial Gap	Recommend the full V4 control specification to be used to close the gap. Portion in the mapped control(s) contributing to the partial gap, that is, covering in part the V4 control: (EKM-04) 'open/validated formats and standard algorithms shall be required'.	27001: A.10.1.1 27002: 10.1.1 (e) 27017: 10.1.1 27001: A.10.1.2 27002: 10.1.2 27002: 10.1.2 (a) 27017: 10.1.2	No Gap	N/A
Key Purpose	CEK-11	Manage cryptographic secret and private keys that are provisioned for a unique purpose.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	27001: A.10.1.1 27017: 10.1.1 27001: A.10.1.2 27002: 10.1.2 (c) 27017: 10.1.2	No Gap	N/A

# Cryptography, Encryption & Key Management – CEK (5)

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
Key Rotation	CEK-12	Rotate cryptographic keys in accordance with the calculated cryptoperiod, which includes provisions for considering the risk of information disclosure and legal and regulatory requirements.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	27001: A.10.1.1 27017: 10.1.1 27001: A.10.1.2 27002: 10.1.2 e) 27017: 10.1.2	Partial Gap	Missing specification(s) in ISOs: 'Keys Rotation' requirement not mentioned
Key Revocation	CEK-13	Define, implement and evaluate processes, procedures and technical measures to revoke and remove cryptographic keys prior to the end of its established cryptoperiod, when a key is compromised, or an entity is no longer part of the organization, which include provisions for legal and regulatory requirements.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	27001: A.10.1.1 27017: 10.1.1 27001: A.10.1.2 27002: 10.1.2 (g),(f) 27017: 10.1.2	No Gap	N/A
Key Destruction	CEK-14	Define, implement and evaluate processes, procedures and technical measures to destroy keys stored outside a secure environment and revoke keys stored in Hardware Security Modules (HSMs) when they are no longer needed, which include provisions for legal and regulatory requirements.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	27001: A.10.1.1 27017: 10.1.1 27017: 10.1.2 27001: A.10.1.2 27002: 10.1.2 (j) 27001: A.18.1.3 27002: 18.1.3	No Gap	N/A
Key Activation	CEK-15	Define, implement and evaluate processes, procedures and technical measures to create keys in a pre-activated state when they have been generated but not authorized for use, which include provisions for legal and regulatory requirements.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	27001: A.10.1.1 27017: 10.1.1 27001: A.10.1.2 27002: 10.1.2 a) 27017: 10.1.2	Partial Gap	Missing specification(s) in ISOs: 'Keys Pre-Activation' requirement not mentioned

# Cryptography, Encryption & Key Management – CEK (6)

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
Key Suspension	<b>CEK-16</b>	Define, implement and evaluate processes, procedures and technical measures to monitor, review and approve key transitions from any state to/from suspension, which include provisions for legal and regulatory requirements.	<b>No Mapping</b>	<b>Full Gap</b>	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	<b>27001: A.10.1.1</b> <b>27017: 10.1.1</b> <b>27001: A.10.1.2</b> <b>27017: 10.1.2</b>	<b>Partial Gap</b>	Missing specification(s) in ISOs: 'Keys Suspension' requirement not mentioned
Key Deactivation	<b>CEK-17</b>	Define, implement and evaluate processes, procedures and technical measures to deactivate keys at the time of their expiration date, which include provisions for legal and regulatory requirements.	<b>No Mapping</b>	<b>Full Gap</b>	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	<b>27001: A.10.1.1</b> <b>27017: 10.1.1</b> <b>27001: A.10.1.2</b> <b>27002: 10.1.2</b> <b>27017: 10.1.2</b>	<b>No Gap</b>	N/A
Key Archival	<b>CEK-18</b>	Define, implement and evaluate processes, procedures and technical measures to manage archived keys in a secure repository requiring least privilege access, which include provisions for legal and regulatory requirements.	<b>No Mapping</b>	<b>Full Gap</b>	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	<b>27001: A.10.1.1</b> <b>27017: 10.1.1</b> <b>27001: A.10.1.2</b> <b>27017: 10.1.2</b> <b>27002: 10.1.2 (i)</b> <b>27001: 9.0</b> <b>27002: 9.0</b> <b>27017: 9.0</b>	<b>Partial Gap</b>	Missing specification(s) in ISOs: 'secure repository requiring least privileged access'

# Cryptography, Encryption & Key Management – CEK (7)

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
Key Compromise	CEK-19	Define, implement and evaluate processes, procedures and technical measures to use compromised keys to encrypt information only in controlled circumstances, and thereafter exclusively for decrypting data and never for encrypting data, which include provisions for legal and regulatory requirements.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	27001: A.10.1.1 27002: 10.1.1 (d) 27001: A.10.1.2 27002: 10.1.2 (f),(g) 27001: A.18.1.5 27001: A.18.1.3 27002: 18.1.3	No Gap	N/A
Key Recovery	CEK-20	Define, implement and evaluate processes, procedures and technical measures to assess the risk to operational continuity versus the risk of the keying material and the information it protects being exposed if control of the keying material is lost, which include provisions for legal and regulatory requirements.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	27001: 8.2 27001: 8.3 27001: A.10.1.2 27002: 10.1.2 (h) 27001: A.18.1.5	No Gap	N/A
Key Inventory Management	CEK-21	Define, implement and evaluate processes, procedures and technical measures in order for the key management system to track and report all cryptographic materials and changes in status, which include provisions for legal and regulatory requirements.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	27001: A.10.1.2 27002: 10.1.2 27017: 10.1.2 27001: A.18.1.5	No Gap	N/A

# Datacenter Security - DCS

# Datacenter Security - DCS(1)

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
Off-Site Equipment Disposal Policy and Procedures	DCS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure disposal of equipment used outside the organization's premises. If the equipment is not physically destroyed a data destruction procedure that renders recovery of information impossible must be applied. Review and update the policies and procedures at least annually.	DCS-05 GRM-06 GRM-09	Partial Gap	Missing specification(s) in CCMv3.0.1: 'apply and evaluate policies and procedures for the secure disposal of equipment used outside the organization's premises' Requirement of 'at least annually' in last sentence.	27001: A.11.2.7 27002: 11.2.7 27017: 11.2.7	No Gap	N/A
Off-Site Transfer Authorization Policy and Procedures	DCS-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location. The relocation or transfer request requires the written or cryptographically verifiable authorization. Review and update the policies and procedures at least annually.	DCS-04 GRM-06 GRM-09	Partial Gap	Missing specification(s) in CCMv3.0.1: 'apply and evaluate policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location' 'or cryptographically verifiable authorization' Requirement of 'at least annually' in last sentence.	27001: A.11.2.5	Partial Gap	Missing specification(s) in ISOs: 'Apply and maintain policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location' 'relocation requires the cryptographically verifiable authorization.'
Secure Area Policy and Procedures	DCS-03	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for maintaining a safe and secure working environment in offices, rooms, and facilities. Review and update the policies and procedures at least annually.	DCS-06 GRM-06 GRM-09	Partial Gap	Missing specification(s) in CCMv3.0.1: 'evaluate (implementation of) policies and procedures' Requirement of 'at least annually' in last sentence.	27001: A.11.1.3 27002: 11.1.3 27017: 11.1.3 27001: A.11.1.5 27002: 11.1.5 27017: 11.1.5	No Gap	N/A
Secure Media Transportation Policy and Procedures	DCS-04	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure transportation of physical media. Review and update the policies and procedures at least annually.	GRM-06 GRM-09	Partial Gap	Missing specification(s) in CCMv3.0.1: 'apply and evaluate policies and procedures for the secure transportation of physical media.' Requirement of 'at least annually' in last sentence.	27001: A.8.3.3 27007: 8.3.3 27017: 8.3.3	No Gap	N/A

# Datacenter Security - DCS(2)

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
Assets Classification	DCS-05	Classify and document the physical, and logical assets (e.g., applications) based on the organizational business risk.	DCS - 01	No Gap	N/A	27001: A.8.2.1 27002: 8.2.1 27017: 8.2.1	Partial Gap	Missing specification(s) in ISOs: 'classify physical assets'
Assets Cataloguing and Tracking	DCS-06	Catalogue and track all relevant physical and logical assets located at all of the CSP's sites within a secured system.	DCS - 01	No Gap	N/A	27001: A.8.1.1 27002: 8.1.1 27017: 8.1.1	Partial Gap	Missing specification(s) in ISOs: 'classify physical assets'
Controlled Access Points	DCS-07	Implement physical security perimeters to safeguard personnel, data, and information systems. Establish physical security perimeters between the administrative and business areas and the data storage and processing facilities areas.	DCS-02 DCS-08	No Gap	N/A	27001: A.11.1.1 27002: 11.1.1 27017: 11.1.1	No Gap	N/A
Equipment Identification	DCS-08	Use equipment identification as a method for connection authentication.	DCS - 03	No Gap	N/A	No Mapping	Full Gap	The full V4 control specification is missing from the ISOs and has to be used to close the gap.
Secure Area Authorization	DCS-09	Allow only authorized personnel access to secure areas, with all ingress and egress points restricted, documented, and monitored by physical access control mechanisms. Retain access control records on a periodic basis as deemed appropriate by the organization.	DCS-07 DCS-09	Partial Gap	Missing specification(s) in CCMv3.0.1: 'all ingress and egress points (are) documented' 'Retain access control records on a periodic basis as deemed appropriate by the organization.'	27001: A.11.1.2	No Gap	N/A
Surveillance System	DCS-10	Implement, maintain, and operate datacenter surveillance systems at the external perimeter and at all the ingress and egress points to detect unauthorized ingress and egress attempts.	DCS-02 DCS-07 DCS-08	Partial Gap	Missing specification(s) in CCMv3.0.1: 'maintain datacenter surveillance systems'	No Mapping	Full Gap	The full V4 control specification is missing from the ISOs and has to be used to close the gap.

# Datacenter Security - DCS(3)

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
Unauthorized Access Response Training	DCS-11	Train datacenter personnel to respond to unauthorized ingress or egress attempts.	HRS-09	Partial Gap	Recommend the full V4 control specification to be used to close the gap. Portion in the mapped control(s) contributing to the partial gap, that is, covering in part the V4 control: (HRS-09) 'All individuals with access to organizational data shall receive appropriate awareness training relating to their professional function relative to the organization.'	No Mapping	Full Gap	The full V4 control specification is missing from the ISOs and has to be used to close the gap.
Cabling Security	DCS-12	Define, implement and evaluate processes, procedures and technical measures that ensure a risk-based protection of power and telecommunication cables from a threat of interception, interference or damage at all facilities, offices and rooms.	BCR - 03	Partial Gap	Missing specification(s) in CCMv3.0.1: 'Define, implement and evaluate processes, procedures and technical measures that ensure a risk-based protection of telecommunication cables'	27001: A.11.2.3	No Gap	N/A
Environmental Systems	DCS-13	Implement and maintain data center environmental control systems that monitor, maintain and test for continual effectiveness the temperature and humidity conditions within accepted industry standards.	BCR - 03	Partial Gap	Missing specification(s) in CCMv3.0.1: 'within accepted industry standards'	27001: A.11	No Gap	N/A
Secure Utilities	DCS-14	Secure, monitor, maintain, and test utilities services for continual effectiveness at planned intervals.	BCR - 03	No Gap	N/A	27001: A.17.1.3 27001: A.11.2.1 27001: A.11.2.2	Partial Gap	Missing specification(s) in ISOs: No requirements to exercise environmental controls
Equipment Location	DCS-15	Keep business-critical equipment away from locations subject to high probability for environmental risk events.	BCR - 06	No Gap	N/A	27001: A.11.2.1 27002: 11.2.1	No Gap	N/A



# Data Security and Privacy Lifecycle Management - DSP

# Data Security and Privacy Lifecycle Management – DSP (1)

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
Security and Privacy Policy and Procedures	DSP-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the classification, protection and handling of data throughout its lifecycle, and according to all applicable laws and regulations, standards, and risk level. Review and update the policies and procedures at least annually.	DSI-04 GRM-06 GRM-09	Partial Gap	Missing specification(s) in CCMv3.0.1: 'apply and evaluate policies and procedures for the classification, protection and handling of data throughout its lifecycle and according to all applicable laws and regulations, standards, and risk level.' Requirement of 'at least annually' in last sentence.	27001: A.8.2.1 27001: A.5.1 27001: 5.2 27001: A.5.1.1 27002: 5.1.1 27001: A.5.1.2 27002: 5.1.2 27001: A.12.1 27002: 12.1	Partial Gap	Missing specification(s) in ISOs: Requirement to review and update the policies and procedures at least annually.
Secure Disposal	DSP-02	Apply industry accepted methods for the secure disposal of data from storage media such that data is not recoverable by any forensic means.	DSI-07	Partial Gap	Missing specification(s) in CCMv3.0.1: 'Apply industry accepted methods for the secure disposal of data'	27001: A.8.3.2 27002: 8.3.2 27001: A.11.2.7 27002: 11.2.7	Partial Gap	Missing specification(s) in ISOs: Requirement to ensure that data is not recoverable by any forensic means.
Data Inventory	DSP-03	Create and maintain a data inventory, at least for any sensitive data and personal data.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	27001: A.8.1.1 27002: 8.1.1	Partial Gap	Missing specification(s) in ISOs: Requirement for maintaining an inventory for personal data
Data Classification	DSP-04	Classify data according to its type and sensitivity level.	DSI-01	No Gap	N/A	27001: A.8.2.1 27002: 8.2.1	No Gap	N/A

# Data Security and Privacy Lifecycle Management – DSP (2)

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
Data Flow Documentation	DSP-05	Create data flow documentation to identify what data is processed, stored or transmitted where. Review data flow documentation at defined intervals, at least annually, and after any change.	DSI-02	Partial Gap	Missing specification(s) in CCMv3.0.1: 'Review data flow documentation at defined intervals, at least annually, and after any change.'	No Mapping	Full Gap	The full V4 control specification is missing from the ISOs and has to be used to close the gap.
Data Ownership and Stewardship	DSP-06	Document ownership and stewardship of all relevant documented personal and sensitive data. Perform review at least annually.	DSI-06	Partial Gap	Missing specification(s) in CCMv3.0.1: 'Document ownership' 'all relevant documented personal data' 'Perform review at least annually'	27001: A.8.1.2	Partial Gap	Missing specification(s) in ISOs: Requirement to perform a review at least annually.
Data Protection by Design and Default	DSP-07	Develop systems, products, and business practices based upon a principle of security by design and industry best practices.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	27001: A.14.1.1 27002:14.1.1 27001: A.14.2.5 27002:14.2.5	Partial Gap	Missing specification(s) in ISOs: incorporating security requirements at the design stage
Data Privacy by Design and Default	DSP-08	Develop systems, products, and business practices based upon a principle of privacy by design and industry best practices. Ensure that systems' privacy settings are configured by default, according to all applicable laws and regulations.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	No Mapping	Full Gap	The full V4 control specification is missing from the ISOs and has to be used to close the gap.
Data Protection Impact Assessment	DSP-09	Conduct a Data Protection Impact Assessment (DPIA) to evaluate the origin, nature, particularity and severity of the risks upon the processing of personal data, according to any applicable laws, regulations and industry best practices.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	No Mapping	Full Gap	The full V4 control specification is missing from the ISOs and has to be used to close the gap.
Sensitive Data Transfer	DSP-10	Define, implement and evaluate processes, procedures and technical measures that ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope as permitted by the respective laws and regulations.	GRM-02 EKM-03	Partial Gap	Missing specification(s) in CCMv3.0.1: The reference to personal data: 'transfer of personal data is protected from unauthorized access and only processed within scope as permitted by the respective laws and regulations'	27001: A.13.2.1 27002: 13.2.1 27001: A.8.3.3 27002: 8.3.3 27001: A.13.2.3 27002: 13.2.3	Partial Gap	Missing specification(s) in ISOs: Requirement to ensure information is only processed within scope as permitted by the respective laws and regulations.

# Data Security and Privacy Lifecycle Management – DSP (3)

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
Personal Data Access, Reversal, Rectification and Deletion	DSP-11	Define and implement, processes, procedures and technical measures to enable data subjects to request access to, modification, or deletion of their personal data, according to any applicable laws and regulations.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	No Mapping	Full Gap	The full V4 control specification is missing from the ISOs and has to be used to close the gap.
Limitation of Purpose in Personal Data Processing	DSP-12	Define, implement and evaluate processes, procedures and technical measures to ensure that personal data is processed according to any applicable laws and regulations and for the purposes declared to the data subject.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	27001: A.18.1.4 27002: 18.1.4	Partial Gap	Missing specification(s) in ISOs: Processing personal data as per the purpose declared to the data subject
Personal Data Sub-processing	DSP-13	Define, implement and evaluate processes, procedures and technical measures for the transfer and sub-processing of personal data within the service supply chain, according to any applicable laws and regulations.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	No Mapping	Full Gap	The full V4 control specification is missing from the ISOs and has to be used to close the gap.
Disclosure of Data Sub-processors	DSP-14	Define, implement and evaluate processes, procedures and technical measures to disclose the details of any personal or sensitive data access by sub-processors to the data owner prior to initiation of that processing.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	27018: A.6.2	Partial Gap	Missing specification(s) in ISOs: Requirement to disclose the details of any personal or sensitive data access by sub-processors to the data owner prior to initiation of that processing.
Limitation of Production Data Use	DSP-15	Obtain authorization from data owners, and manage associated risk before replicating or using production data in non-production environments.	DSI-05	No Gap	N/A	27001: A.14.3.1 27002: 14.3.1 27001: A.12.1.4 27002: 12.1.4	Partial Gap	Missing specification(s) in ISOs: Obtain explicit authorization from data owners

# Data Security and Privacy Lifecycle Management – DSP (4)

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
Data Retention and Deletion	DSP-16	Data retention, archiving and deletion is managed in accordance with business requirements, applicable laws and regulations.	GRM-02 BCR-11	No Gap	N/A	27001: A.18.1.3	No Gap	N/A
Sensitive Data Protection	DSP-17	Define and implement, processes, procedures and technical measures to protect sensitive data throughout it's lifecycle.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	27001: A.18.1.3 27002: 18.1.3 27001:A.18.1.4 27002:18.1.4	No Gap	N/A
Disclosure Notification	DSP-18	The CSP must have in place, and describe to CSCs the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations. The CSP must give special attention to the notification procedure to interested CSCs, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	27018: A.6.1	No Gap	N/A
Data Location	DSP-19	Define and implement, processes, procedures and technical measures to specify and document the physical locations of data, including any locations in which data is processed or backed up.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	27001: A.8.1.1 27002: 8.1.1 27017: 8.1.1	No Gap	N/A

# Governance, Risk and Compliance - GRC



# Governance, Risk and Compliance - GRC(1)

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
Governance Program Policy and Procedures	GRC-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for an information governance program, which is sponsored by the leadership of the organization. Review and update the policies and procedures at least annually.	GRM-06 GRM-09	Partial Gap	Missing specification(s) in CCMv3.0.1: 'apply and evaluate policies and procedures for an information governance program' Requirement of 'at least annually' in last sentence.	27001: 5.1 27001: 5.2 27001: 5.3	Partial Gap	Missing in the ISOs: "document, approve, apply, evaluate and maintain policies and procedures for an information governance program" "Review and update the policies and procedures at least annually."
Risk Management Program	GRC-02	Establish a formal, documented, and leadership-sponsored Enterprise Risk Management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of cloud security and privacy risks.	GRM-08 GRM-10 GRM-11	Partial Gap	Missing specification(s) in CCMv3.0.1: 'Enterprise Risk Management (ERM) program (as it includes information security risks but is not limited to only those)' '(ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of privacy risks' (focus is on missing req. for risk management on privacy)	27001: A.6.1.2 27001: 6.2	No Gap	N/A
Organizational Policy Reviews	GRC-03	Review all relevant organizational policies and associated procedures at least annually or when a substantial change occurs within the organization.	GRM-09	No Gap	N/A	27001:7.5.2 (c)	Partial Gap	Missing specification(s) in ISOs: Requirement of 'at least annually'
Policy Exception Process	GRC-04	Establish and follow an approved exception process as mandated by the governance program whenever a deviation from an established policy occurs.	GRM-01	Partial Gap	Missing specification(s) in CCMv3.0.1: 'deviation from an established policy'	27001: A.5.1.1 27002: 5.1.1 (c)	No Gap	N/A

# Governance, Risk and Compliance – GRC(2)

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
Information Security Program	<b>GRC-05</b>	Develop and implement an Information Security Program, which includes programs for all the relevant domains of the CCM.	<b>GRM-04</b>	<b>Partial Gap</b>	Missing specification(s) in CCMv3.0.1: 'all the domains of the CCM' (i.e., reference to CCMv4.0)	<b>27001: 1</b> <b>27001: 4.3</b>	<b>Partial Gap</b>	Missing specification(s) in ISOs: 'domains of the CCMv4.0' missing from ISOs
Governance Responsibility Model	<b>GRC-06</b>	Define and document roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs.	<b>No Mapping</b>	<b>Full Gap</b>	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	<b>27001: 5.3</b> <b>27001: A.6.1.1</b> <b>27002: 6.1.1</b> <b>27001: A.7.2.1</b> <b>27002: 7.2.1</b> <b>27018: 5.1.1</b>	<b>Partial Gap</b>	Missing in the ISOs: 'for planning, implementing, operating, assessing, and improving governance programs.' 'document roles and responsibilities'
Information System Regulatory Mapping	<b>GRC-07</b>	Identify and document all relevant standards, regulations, legal/contractual, and statutory requirements, which are applicable to your organization.	<b>AAC-03</b>	<b>No Gap</b>	N/A	<b>27001: A.18.1</b> <b>27001: A.18.2.2</b> <b>27018: A.18.1</b> <b>27018: A.18.2.2</b>	<b>No Gap</b>	N/A
Special Interest Groups	<b>GRC-08</b>	Establish and maintain contact with cloud-related special interest groups and other relevant entities in line with business context.	<b>No Mapping</b>	<b>Full Gap</b>	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	<b>27001: A.6.1.4</b>	<b>No Gap</b>	N/A



# Human Resources - HRS



# Human Resources – HRS(1)

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
Background Screening Policy and Procedures	HRS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for background verification of all new employees (including but not limited to remote employees, contractors, and third parties) according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, the business requirements, and acceptable risk. Review and update the policies and procedures at least annually.	HRS-02 GRM-06 GRM-09	Partial Gap	Missing specification(s) in CCMv3.0.1: 'apply, evaluate, policies and procedures for background verification of all new employees' Requirement of 'at least annually' in last sentence.	27001: A.7.1.1 27002: 7.1.1 27017: 7.1.1	Partial Gap	Missing specification(s) in ISOs: requirement to review and update the policies and procedures at least annually.
Acceptable Use of Technology Policy and Procedures	HRS-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets. Review and update the policies and procedures at least annually.	HRS-08 GRM-06 GRM-09	Partial Gap	Missing specification(s) in CCMv3.0.1: Requirement of 'at least annually' in last sentence.	27001: A.8.1.3 27002: 8.1.3 27017: 8.1.3	Partial Gap	Missing specification(s) in ISOs: requirement to review and update the policies and procedures at least annually.
Clean Desk Policy and Procedures	HRS-03	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures that require unattended workspaces to not have openly visible confidential data. Review and update the policies and procedures at least annually.	HRS-11 GRM-06 GRM-09	Partial Gap	Missing specification(s) in CCMv3.0.1: 'apply, evaluate, policies and procedures that require unattended workspaces to not have openly visible confidential data' Requirement of 'at least annually' in last sentence.	27001: A.11.2.8 27002: 11.2.8 27017: 11.2.8 27001: A.11.2.9 27002: 11.2.9 27017: 11.2.9	Partial Gap	Missing specification(s) in ISOs: requirement to review and update the policies and procedures at least annually.
Remote and Home Working Policy and Procedures	HRS-04	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect information accessed, processed or stored at remote sites and locations. Review and update the policies and procedures at least annually.	GRM-06 GRM-09	Partial Gap	Missing specification(s) in CCMv3.0.1: 'apply, evaluate, policies and procedures to protect information accessed, processed or stored at remote sites and locations' Requirement of 'at least annually' in last sentence.	27001: A.6.2.2 27002: 6.2.2 27001: A.11.2.6 27002: 11.2.6	Partial Gap	Missing specification(s) in ISOs: requirement to review and update the policies and procedures at least annually.
Asset returns	HRS-05	Establish and document procedures for the return of organization-owned assets by terminated employees.	HRS-01	Partial Gap	Missing specification(s) in CCMv3.0.1: 'Establish and document procedures'	27001: A.8.1.4 27002: 8.1.4 27017: 8.1.4	No Gap	N/A

# Human Resources – HRS(2)

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
Employment Termination	HRS-06	Establish, document, and communicate to all personnel the procedures outlining the roles and responsibilities concerning changes in employment.	HRS-04	No Gap	N/A	27001: A.7.3.1 27002: 7.3.1 27017: 7.3.1	No Gap	N/A
Employment Agreement Process	HRS-07	Employees sign the employee agreement prior to being granted access to organizational information systems, resources and assets.	HRS-03	No Gap	N/A	No Mapping	Full Gap	The full V4 control specification is missing from the ISOs and has to be used to close the gap.
Employment Agreement Content	HRS-08	The organization includes within the employment agreements provisions and/or terms for adherence to established information governance and security policies.	HRS-03	No Gap	N/A	27001: A.7.1.2 27002: 7.1.2 27017: 7.1.2	No Gap	N/A
Personnel Roles and Responsibilities	HRS-09	Document and communicate roles and responsibilities of employees, as they relate to information assets and security.	HRS-07 HRS-10	No Gap	N/A	27001: A.6.1.1 27002: 6.1.1 27017: 6.1.1	No Gap	N/A
Non-Disclosure Agreements	HRS-10	Identify, document, and review, at planned intervals, requirements for non-disclosure/confidentiality agreements reflecting the organization's needs for the protection of data and operational details.	HRS-06	No Gap	N/A	27001: A.7.1.2 27002: 7.1.2 27017: 7.1.2 27001: A.13.2.4	No Gap	N/A
Security Awareness Training	HRS-11	Establish, document, approve, communicate, apply, evaluate and maintain a security awareness training program for all employees of the organization and provide regular training updates.	HRS-09 HRS-10	Partial Gap	Missing specification(s) in CCMv3.0.1: 'approve, evaluate and maintain a security awareness training program'	27001: A.7.2.2 27002: 7.2.2 27017: 7.2.2	No Gap	N/A
Personal and Sensitive Data Awareness and Training	HRS-12	Provide all employees with access to sensitive organizational and personal data with appropriate security awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.	HRS-09 HRS-10	Partial Gap	Missing specification(s) in CCMv3.0.1: 'Provide all employees with access to sensitive organizational and personal data with appropriate security awareness training'	27001: A.7.2.2 27002: 7.2.2 27017: 7.2.2	Partial Gap	Missing specification(s) in ISOs: Requirement to focus training on "sensitive organizational and personal data"
Compliance Responsibility	HRS-13	Make employees aware of their roles and responsibilities for maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations.	HRS-10	No Gap	N/A	27001: A.7.2.1 27002: 7.2.1 27017: 7.2.1	Partial Gap	Missing specification(s) in ISOs: requirement to focus on "applicable legal, statutory, or regulatory compliance obligations"



# Identity and Access Management - IAM

# Identity & Access Management - IAM(1)

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
Identity and Access Management Policy and Procedures	IAM-01	Establish, document, approve, communicate, implement, apply, evaluate and maintain policies and procedures for identity and access management. Review and update the policies and procedures at least annually.	IAM-02 GRM-06 GRM-09	Partial Gap	Missing specification(s) in CCMv3.0.1: Requirement of 'at least annually' in last sentence.	27001: A.9.1.1 27002: 9.1.1 27001: A.5.1.2 27002: 5.1.2	No Gap	N/A
Strong Password Policy and Procedures	IAM-02	Establish, document, approve, communicate, implement, apply, evaluate and maintain strong password policies and procedures. Review and update the policies and procedures at least annually.	IAM-02 IAM-12 GRM-06 GRM-09	Partial Gap	(If Password is equal to "authentication secrets" then) Missing specification(s) in CCMv3.0.1: Requirement of 'at least annually' in last sentence.	27001: A.9.4.3 27002: 9.4.3 27017: 9.4.3 27018: 9.4.3 27001: A.9.2.4 27002: 9.2.4 27017: 9.2.4 27001: A.7.2.2 27002:7.2.2 27001: A.9.2.6 27002: 9.2.6 27001: A.9.2.3 27002: 9.2.3	Partial Gap	Missing specification(s) in ISOs: Requirement to review and update the policies and procedures at least annually.
Identity Inventory	IAM-03	Manage, store, and review the information of system identities, and level of access.	IAM-04 IAM-10	Partial Gap	Missing specification(s) in CCMv3.0.1: 'system identities'	27001: A.8.1.1 27002: 8.1.1 27001: A.9.4.1 27002: 9.4.1	Partial Gap	Missing specification(s) in ISOs: ISO partially addressed Identity Inventory under asset management
Separation of Duties	IAM-04	Employ the separation of duties principle when implementing information system access.	IAM-05	No Gap	N/A	27001: A.6.1.2 27002: 6.1.2	No Gap	N/A

# Identity & Access Management - IAM(2)

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
Least Privilege	IAM-05	Employ the least privilege principle when implementing information system access.	IAM-02 IAM-06	No Gap	N/A	27001: A.9.1.1 27002: 9.1.1 27001: A.9.1.2 27002: 9.1.2 27001: A.9.2.3 27002: 9.2.3	No Gap	N/A
User Access Provisioning	IAM-06	Define and implement a user access provisioning process which authorizes, records, and communicates access changes to data and assets.	IAM-09	No Gap	N/A	No Mapping	Full Gap	The full V4 control specification is missing from ISOs and has to be used to close the gap.
User Access Changes and Revocation	IAM-07	De-provision or respectively modify access of movers / leavers or system identity changes in a timely manner in order to effectively adopt and communicate identity and access management policies.	IAM-11	No Gap	N/A	No Mapping	Full Gap	The full V4 control specification is missing from ISOs and has to be used to close the gap.
User Access Review	IAM-08	Review and revalidate user access for least privilege and separation of duties with a frequency that is commensurate with organizational risk tolerance.	IAM-10	Partial Gap	Missing specification(s) in CCMv3.0.1: 'Review and revalidate user access for separation of duties' 'a frequency that is commensurate with organizational risk tolerance'	27001: A.9.2.5 27001: A.9.2.6 27001: A.9.4.1 27017: 9.4.1 27001: A.6.1.2	Partial Gap	Missing specification(s) in ISOs: Requirement of separation of duties in reviewing of user access rights.
Segregation of Privileged Access Roles	IAM-09	Define, implement and evaluate processes, procedures and technical measures for the segregation of privileged access roles such that administrative access to data, encryption and key management capabilities and logging capabilities are distinct and separated.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	27001: A.9.2.3 27002: 9.2.3 27017: 9.2.3 27018: 9.2.3	No Gap	N/A
Management of Privileged Access Roles	IAM-10	Define and implement an access process to ensure privileged access roles and rights are granted for a time limited period, and implement procedures to prevent the culmination of segregated privileged access.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	27001: A.9.2.3 27002: 9.2.3 27017: 9.2.3 27018: 9.2.3	Partial Gap	Missing specification(s) in ISOs: Requirement to prevent the culmination of segregated privileged access.

# Identity & Access Management - IAM(3)

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
CSCs Approval for Agreed Privileged Access Roles	IAM-11	Define, implement and evaluate processes and procedures for customers to participate, where applicable, in the granting of access for agreed, high risk (as defined by the organizational risk assessment) privileged access roles.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	No Mapping	Full Gap	N/A
Safeguard Logs Integrity	IAM-12	Define, implement and evaluate processes, procedures and technical measures to ensure the logging infrastructure is read-only for all with write access, including privileged access roles, and that the ability to disable it is controlled through a procedure that ensures the segregation of duties and break glass procedures.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	27001: A.12.4.1 27002: 12.4.1 27017: 12.4.1 27018: 12.4.1 27001: A.12.4.2 27002: 12.4.2 27017: 12.4.2 27018: 12.4.2 27001: A.12.4.3 27002: 12.4.3 27017: 12.4.3 27018: 12.4.3	Partial Gap	Missing specification(s) in ISOs: Requirement to control the ability to disable logs through a procedure that ensures the segregation of duties and break glass procedures.
Uniquely Identifiable Users	IAM-13	Define, implement and evaluate processes, procedures and technical measures that ensure users are identifiable through unique IDs or which can associate individuals to the usage of user IDs.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	27001: A.9.2.1 27002: 9.2.1	No Gap	N/A
Strong Authentication	IAM-14	Define, implement and evaluate processes, procedures and technical measures for authenticating access to systems, application and data assets, including multifactor authentication for at least privileged user and sensitive data access. Adopt digital certificates or alternatives which achieve an equivalent level of security for system identities.	IAM-02 IAM-05	Partial Gap	Missing specification(s) in CCMv3.0.1: 'Adopt digital certificates or alternatives which achieve an equivalent level of security for system identities'	27001: A.9.1.2 27002: 9.1.2 27017: 9.1.2 27001: A.9.2.4 27002: 9.2.4 27017: 9.2.4 27001: A.9.4.2 27002: 9.4.2 27017: 9.4.2 27018: 9.4.2	Partial Gap	Missing specification(s) in ISOs: Requirement to include multifactor authentication for at least privileged user and sensitive data access.

# Identity & Access Management - IAM(4)

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
CSCs Approval for Agreed Privileged Access Roles	IAM-11	Define, implement and evaluate processes and procedures for customers to participate, where applicable, in the granting of access for agreed, high risk (as defined by the organizational risk assessment) privileged access roles.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	No Mapping	Full Gap	N/A
Passwords Management	IAM-15	Define, implement and evaluate processes, procedures and technical measures for the secure management of passwords.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	27001: A.9.2.4 27002: 9.2.4 27017: 9.2.4 27018: 9.2.4 27001: A.9.3.1 27002: 9.3.1 27017: 9.3.1 27018: 9.3.1 27001: A.9.4.3 27002: 9.4.3 27017: 9.4.3 27018: 9.4.3	No Gap	N/A
Authorization Mechanisms	IAM-16	Define, implement and evaluate processes, procedures and technical measures to verify access to data and system functions is authorized.	IAM-02	No Gap	N/A	27001: A.9.2.5 27002: 9.2.5 27017: 9.2.5 27018: 9.2.5	No Gap	N/A





# Interoperability and Portability - IPY

# Interoperability & Portability - IPY

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
Interoperability and Portability Policy and Procedures	IPY-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for interoperability and portability including requirements for: a. Communications between application interfaces b. Information processing interoperability c. Application development portability d. Information/Data exchange, usage, portability, integrity, and persistence Review and update the policies and procedures at least annually.	IPY-03 GRM-06 GRM-09	Partial Gap	Missing specification(s) in CCMv3.0.1: 'apply and evaluate policies and procedures for interoperability and portability.' Requirement of 'at least annually' in last sentence.	27001: A.14.1.1 27017: 14.1.1 27001: A.14.1.2 27002: 14.1.2 27017: 14.1.2 27001: A.14.2 27002: 14.2 27001: A.14.2.1 27017: 14.2.1 27001: A.14.2.5	Partial Gap	Missing specification(s) in ISOs: Requirement of communications between application services (APIs)
Application Interface Availability	IPY-02	Provide application interface(s) to CSCs so that they programmatically retrieve their data to enable interoperability and portability.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	No Mapping	Full Gap	The full V4 control specification is missing from the ISOs and has to be used to close the gap.
Secure Interoperability and Portability Management	IPY-03	Implement cryptographically secure and standardized network protocols for the management, import and export of data.	IPY-04	No Gap	N/A	27001: A.18.1 27001: A.15.1.1 27002: 15.1.1 27017: 15.1.1	No Gap	N/A
Data Portability Contractual Obligations	IPY-04	Agreements must include provisions specifying CSCs access to data upon contract termination and will include: a. Data format b. Length of time the data will be stored c. Scope of the data retained and made available to the CSCs d. Data deletion policy	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	No Mapping	Full Gap	The full V4 control specification is missing from the ISOs and has to be used to close the gap.

# Infrastructure and Virtualization Security + IVS



# Infrastructure & Virtualization Security - IVS(1)

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
Infrastructure and Virtualization Security Policy and Procedures	IVS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for infrastructure and virtualization security. Review and update the policies and procedures at least annually.	GRM-06 GRM-09	Partial Gap	Missing specification(s) in CCMv3.0.1: 'apply and evaluate policies and procedures for infrastructure and virtualization security.' Requirement of 'at least annually' in last sentence.	27001: A.5 27002: 5 27017: 5 27018: 5	Partial Gap	Missing specification(s) in ISOs: Requirement of "Infrastructure & Virtualization Security"
Capacity and Resource Planning	IVS-02	Plan and monitor the availability, quality, and adequate capacity of resources in order to deliver the required system performance as determined by the business.	IVS-04	No Gap	N/A	27001: 5.3 27001: 6.1 27001: 9.1 27001: A.12.1.3 27002: 12.1.3	Partial Gap	Missing specification(s) in ISOs: Requirement of "Infrastructure & Virtualization Security"
Network Security	IVS-03	Monitor, encrypt and restrict communications between environments to only authenticated and authorized connections, as justified by the business. Review these configurations at least annually, and support them by a documented justification of all allowed services, protocols, ports, and compensating controls.	IVS-06	No Gap	N/A	27001: A.13.1.1 27002: 13.1.1 27001: A.13.1.2 27002: 13.1.2 27001: A.13.1.3 27002: 13.1.3	Partial Gap	Missing specification(s) in ISOs: Requirement of "Infrastructure & Virtualization Security"
OS Hardening and Base Controls	IVS-04	Harden host and guest OS, hypervisor or infrastructure control plane according to their respective best practices, and supported by technical controls, as part of a security baseline.	IVS-07	Partial Gap	Missing specification(s) in CCMv3.0.1: 'Host and guest OS', 'hypervisor', 'infrastructure control plane'.	27001: A.14.2.2 27002: 14.2.2 27001: A.14.2.3 27001 A.14.2.4 27018: 12.1.2	Partial Gap	Missing specification(s) in ISOs: Requirement of "Infrastructure & Virtualization Security"
Production and Non-Production Environments	IVS-05	Separate production and non-production environments.	IVS-08	No Gap	N/A	27001 A.12.1.4 27002 12.1.4 27017 12.1.4 27018 12.1.4	Partial Gap	Missing specification(s) in ISOs: Requirement of "Infrastructure & Virtualization Security"

# Infrastructure & Virtualization Security - IVS(2)

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
Segmentation and Segregation	IVS-06	Design, develop, deploy and configure applications and infrastructures such that CSP and CSC (tenant) user access and intra-tenant access is appropriately segmented and segregated, monitored and restricted from other tenants.	IVS-09	No Gap	N/A	27001: A.13.1.3 27002: 13.1.3 27017: 13.1.3	Partial Gap	Missing specification(s) in ISOs: 'Design, develop, deploy and configure applications and infrastructures' 'monitored and restricted from other tenants.'
Migration to Cloud Environments	IVS-07	Use secure and encrypted communication channels when migrating servers, services, applications, or data to cloud environments. Such channels must include only up-to-date and approved protocols.	IVS-10	Partial Gap	Missing specification(s) in CCMv3.0.1: 'Such channels must include only up-to-date and approved protocols'.	27001: 7.4 27001: A.13.1.1 27002: 13.1.1 27017: 13.1.1 27018: 13.1.1 27001: A.13.1.2 27002: 13.1.2 27017: 13.1.2 27018: 13.1.2 27001: A.13.1.3 27002: 13.1.3 27017: 13.1.3 27018: 13.1.3 27001: A.13.2.1 27002: 13.2.1 27017: 13.2.1 27018: 13.2.1 27001: A.13.2.2 27002: 13.2.2 27017: 13.2.2 27018: 13.2.2 27001: A.13.2.3 27002: 13.2.3 27017: 13.2.3 27018: 13.2.3	Partial Gap	Missing specification(s) in ISOs: Requirement of "Infrastructure & Virtualization Security"

# Infrastructure & Virtualization Security - IVS(3)

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
Network Architecture Documentation	IVS-08	Identify and document high-risk environments.	IVS-13	No Gap	N/A	27001: A.9.1.2 27002: 9.1.2 27017: 9.1.2 27001: A.9.4.2 27002: 9.4.2 27017: 9.4.2 27018: 9.4.2 27001: A.14.2.5 27002: 14.2.5 27017: 14.2.5	Partial Gap	Missing specification(s) in ISOs: Requirement of "Infrastructure & Virtualization Security"
Network Defense	IVS-09	Define, implement and evaluate processes, procedures and defense-in-depth techniques for protection, detection, and timely response to network-based attacks.	IVS-13	No Gap	N/A	27001: A.14.1.2 27002: 14.1.2 27017: 14.1.2 27001: A.11.1.4 27002: 11.1.4 27017: 11.1.4 27018: 16.1.1	Partial Gap	Missing specification(s) in ISOs: Requirement of Infrastructure & Virtualization Security Requirement for defense-in-depth approach

# Logging and Monitoring - LOG

# Logging and Monitoring - LOG(1)

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
Logging and Monitoring Policy and Procedures	LOG-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for logging and monitoring. Review and update the policies and procedures at least annually.	GRM-06 GRM-09	Partial Gap	Missing specification(s) in CCMv3.0.1: 'apply and evaluate policies and procedures for logging and monitoring' Requirement of 'at least annually' in last sentence.	No mapping	Full Gap	The full V4 control specification is missing from the ISOs and has to be used to close the gap.
Audit Logs Protection	LOG-02	Define, implement and evaluate processes, procedures and technical measures to ensure the security and retention of audit logs.	IVS-01	Partial Gap	Missing specification(s) in CCMv3.0.1: 'Define, implement and evaluate processes, procedures and technical measures'	27001: A.18.1.3 27002: 18.1.3	Partial Gap	Missing specification(s) in ISOs: Requirement for the review and update of policies and procedures.
Security Monitoring and Alerting	LOG-03	Identify and monitor security-related events within applications and the underlying infrastructure. Define and implement a system to generate alerts to responsible stakeholders based on such events and corresponding metrics.	SEF-03 SEF-05	Partial Gap	Missing specification(s) in CCMv3.0.1: 'Define and implement a system to generate alerts to responsible stakeholders based on such events and corresponding metrics.'	27001: A.12.4.1 27002: 12.4.1	Partial Gap	Missing specification(s) in ISOs: Requirement to generate alerts to responsible stakeholders.
Audit Logs Access and Accountability	LOG-04	Restrict audit logs access to authorized personnel and maintain records that provide unique access accountability.	IVS-01	Partial Gap	Missing specification(s) in CCMv3.0.1: 'Restrict audit logs access to authorized personnel'	27001: A.12.4.2 27001: A.12.4.1 27002: 12.4.2	No Gap	N/A
Audit Logs Monitoring and Response	LOG-05	Monitor security audit logs to detect activity outside of typical or expected patterns. Establish and follow a defined process to review and take appropriate and timely actions on detected anomalies.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	27001: A.12.4.3 27002: 12.4.3	No Gap	N/A
Clock Synchronization	LOG-06	Use a reliable time source across all relevant information processing systems.	IVS-03	No Gap	N/A	27001: A.12.4.4 27002: 12.4.4 27017: 12.4.4	No Gap	N/A
Logging Scope	LOG-07	Establish, document and implement which information meta/data system events should be logged. Review and update the scope at least annually or whenever there is a change in the threat environment.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	27001: A.12.4.1 27002: 12.4.1 27017: 12.4.1	No Gap	N/A



# Logging and Monitoring - LOG(2)

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
Log Records	LOG-08	Generate audit records containing relevant security information.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	27001: A.12.4.1 27002: 12.4.1 27017: 12.4.1	No Gap	N/A
Log Protection	LOG-09	The information system protects audit records from unauthorized access, modification, and deletion.	GRM-04 IVS-01	Partial Gap	Recommend the full V4 control specification to be used to close the gap.  Portion in the mapped control(s) contributing to the partial gap, that is, covering in part the V4 control: (IVS-01) 'Higher levels of assurance are required for protection of audit logs', (GRM-04) 'to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction'.	27001: A.12.4.2 27002: 12.4.2	No Gap	N/A
Encryption Monitoring and Reporting	LOG-10	Establish and maintain a monitoring and internal reporting capability over the operations of cryptographic, encryption and key management policies, processes, procedures, and controls.	EKM-02 EKM-03	Partial Gap	Recommend the full V4 control specification to be used to close the gap.  Portion in the mapped control(s) contributing to the partial gap, that is, covering in part the V4 control: (EKM-02) 'Policies and procedures shall be established for the management of cryptographic keys', (EKM-03) 'Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols'.	27001: A.10.1 27002: 10.1 27001: A.10.1.2 27017: 10.1.2	No Gap	N/A
Transaction/Activity Logging	LOG-11	Log and monitor key lifecycle management events to enable auditing and reporting on usage of cryptographic keys.	EKM-02	Partial Gap	Recommend the full V4 control specification to be used to close the gap.  Portion in the mapped control(s) contributing to the partial gap, that is, covering in part the V4 control: (EKM-02) 'management of cryptographic keys in the service's cryptosystem'.	27001: A.10.1.2 27017: 10.1.2	No Gap	N/A

# Logging and Monitoring - LOG(3)

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
Access Control Logs	LOG-12	Monitor and log physical access using an auditable access control system.	DCS-08	Partial Gap	Missing specification(s) in CCMv3.0.1: 'log physical access using an auditable access control system.'	27001: A.11.1.2 27002: 11.1.2	No Gap	N/A
Failures and Anomalies Reporting	LOG-13	Define, implement and evaluate processes, procedures and technical measures for the reporting of anomalies and failures of the monitoring system and provide immediate notification to the accountable party.	SEF-03	Partial Gap	Missing specification(s) in CCMv3.0.1: 'Define, implement and evaluate processes, procedures and technical measures for the reporting of anomalies and failures of the monitoring system'	27001: A.16.1.1 27002: 16.1.1 27001: A.16.1.2 27017: 16.1.2	No Gap	N/A



# Security Incident Management, E-Discovery, and Cloud Forensics - SEF

# Security Incident Management, E-Discovery, & Cloud Forensics – SEF(1)

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
Security Incident Management Policy and Procedures	SEF-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Security Incident Management, E-Discovery, and Cloud Forensics. Review and update the policies and procedures at least annually.	SEF-02 GRM-06 GRM-09	Partial Gap	Missing specification(s) in CCMv3.0.1: 'policies and procedures for E-Discovery and Cloud Forensics'. Requirement of 'at least annually' in last sentence.	27001: A.16.1 27002: 16.1 27017: 16.1 27018: 16.1	Partial Gap	Missing specification(s) in ISOs: Requirement to review and update the policies and procedures at least annually.
Service Management Policy and Procedures	SEF-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the timely management of security incidents. Review and update the policies and procedures at least annually.	SEF-02 GRM-06 GRM-09	Partial Gap	Missing specification(s) in CCMv3.0.1: Requirement of 'at least annually' in last sentence.	27001: A.16.1.2 27002: 16.1.2 27017: 16.1.2 27018: 16.1.2 27001: A.16.1.5 27002: 16.1.5 27017: 16.1.5 27018: 16.1.5	Partial Gap	Missing specification(s) in ISOs: Requirement to review and update the policies and procedures at least annually.
Incident Response Plans	SEF-03	Establish, document, approve, communicate, apply, evaluate and maintain a security incident response plan, which includes but is not limited to: relevant internal departments, impacted CSCs, and other business critical relationships (such as supply-chain) that may be impacted.	BCR-02	Partial Gap	Missing specification(s) in CCMv3.0.1: 'Establish, document, approve, communicate, apply, a security incident response plan, which include relevant internal departments'	27001: A.16.1.5 27002: 16.1.5 27017: 16.1.5 27017: CLD.12.1.5 27018: 16.1.5	No Gap	N/A

# Security Incident Management, E-Discovery, & Cloud Forensics – SEF(2)

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
Incident Response Testing	<b>SEF-04</b>	Test and update as necessary incident response plans at planned intervals or upon significant organizational or environmental changes for effectiveness.	<b>BCR-02</b>	<b>No Gap</b>	N/A	<b>No Mapping</b>	<b>Full Gap</b>	The full V4 control specification is missing from the ISOs and has to be used to close the gap.
Incident Response Metrics	<b>SEF-05</b>	Establish and monitor information security incident metrics.	<b>SEF-05</b>	<b>No Gap</b>	N/A	<b>No Mapping</b>	<b>Full Gap</b>	The full V4 control specification is missing from the ISOs and has to be used to close the gap.
Event Triage Processes	<b>SEF-06</b>	Define, implement and evaluate processes, procedures and technical measures supporting business processes to triage security-related events.	<b>SEF-02</b>	<b>No Gap</b>	N/A	<b>27001: A.16.1.4 27002: 16.1.4 27017: 16.1.4 27018: 16.1.4 27001: A.16.1.5 27002: 16.1.5 27017: 16.1.5 27018: 16.1.5</b>	<b>No Gap</b>	N/A

# Security Incident Management, E-Discovery, & Cloud Forensics – SEF(3)

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
Security Breach Notification	SEF-07	Define and implement, processes, procedures and technical measures for security breach notifications. Report security breaches and assumed security breaches including any relevant supply chain breaches, as per applicable SLAs, laws and regulations.	SEF-04 STA-05	Partial Gap	Missing specification(s) in CCMv3.0.1: 'Define and implement, processes, procedures and technical measures for security breach notifications' 'Report assumed security breaches'	27001: A.16.1.1 27002: 16.1.1 27017: 16.1.1 27018: 16.1.1 27001: A.16.1.2 27002: 16.1.2 27017: 16.1.2 27018: 16.1.2 27001: A.16.1.5 27002: 16.1.5 27017: 16.1.5 27018: 16.1.5	Partial Gap	Missing specification(s) in ISOs: Requirement to report relevant supply chain breaches. Requirement to report as per applicable SLAs, laws and regulations.
Points of Contact Maintenance	SEF-08	Maintain points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities.	SEF-01	No Gap	N/A	27001: 4.2 27001: A.6.1.3 27002: 6.1.3 27017: 6.1.3 27018: 6.1.3 27001: A.16.1.1 27002: 16.1.1 27001: A.18.1.1 27002: 18.1.1 27017: 18.1.1 27018: 18.1.1	No Gap	N/A

# Supply Chain Management, Transparency, and Accountability - STA



By Royal Charter

**bsi.**

# Supply Chain Management, Transparency, and Accountability – STA(1)

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
SSRM Policy and Procedures	STA-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the application of the Shared Security Responsibility Model (SSRM) within the organization. Review and update the policies and procedures at least annually.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	27001: 5.1a 27001: 5.2 27001: 6.2 27001: 9.1 27001: 9.3 27001: A.5.1 27001: A.5.2 27001: A.15.1.1	Partial Gap	Missing specification(s) in ISOs: Requirement of a Shared Security Responsibility Model (SSRM).
SSRM Supply Chain	STA-02	Apply, document, implement and manage the SSRM throughout the supply chain for the cloud service offering.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	27001: 6.2 27001: 7.1 27001: 8.1 27001: 8.2 27001: 9.1 27001: 9.3 27001: A.15.1 27001: A.15.2	Partial Gap	Missing specification(s) in ISOs: Requirement of a Shared Security Responsibility Model (SSRM).
SSRM Guidance	STA-03	Provide SSRM Guidance to the CSC detailing information about the SSRM applicability throughout the supply chain.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	27001: 6.2 27001: 7.4 27001: 9.1 27001: A.15.1.2 27001: A.15.1.3	Partial Gap	Missing specification(s) in ISOs: Requirement of a Shared Security Responsibility Model (SSRM).
SSRM Control Ownership	STA-04	Delineate the shared ownership and applicability of all CSA CCM controls according to the SSRM for the cloud service offering.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	27001: 6.2 27001: 7.4 27001: 9.1 27001: A.15.1.2 27001: A.15.2	Partial Gap	Missing specification(s) in ISOs: Requirement of a Shared Security Responsibility Model (SSRM).



# Supply Chain Management, Transparency, and Accountability – STA(2)

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
SSRM Documentation Review	STA-05	Review and validate SSRM documentation for all cloud service offerings the organization uses.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	27001: 6.2 27001: 7.4 27001: 9.1 27001: 9.3 27001: A.15.1.2 27001: A.15.1.3	Partial Gap	Missing specification(s) in ISOs: Requirement of a Shared Security Responsibility Model (SSRM).
SSRM Control Implementation	STA-06	Implement, operate, and audit or assess the portions of the SSRM which the organization is responsible for.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	27001: 8.1 27001: A.15.1.2 27001: A.15.1.3	Partial Gap	Missing specification(s) in ISOs: Requirement of a Shared Security Responsibility Model (SSRM).
Supply Chain Inventory	STA-07	Develop and maintain an inventory of all supply chain relationships.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	27001: 8.1 27001: A.15.1.2 27001: A.15.1.3	Partial Gap	Missing specification(s) in ISOs: Requirement of a Shared Security Responsibility Model (SSRM).
Supply Chain Risk Management	STA-08	CSPs periodically review risk factors associated with all organizations within their supply chain.	STA-06 STA-08	No Gap	N/A	27001: 8.1 27001: A.15.1.2 27001: A.15.1.3	Partial Gap	Missing specification(s) in ISOs: Requirement of a Shared Security Responsibility Model (SSRM).
Primary Service and Contractual Agreement	STA-09	Service agreements between CSPs and CSCs (tenants) must incorporate at least the following mutually-agreed upon provisions and/or terms: <ul style="list-style-type: none"> <li>• Scope, characteristics and location of business relationship and services offered</li> <li>• Information security requirements (including SSRM)</li> <li>• Change management process</li> <li>• Logging and monitoring capability</li> </ul>	STA-05	Partial Gap	Missing specification(s) in CCMv3.0.1: 'Logging and monitoring capability' 'Data Privacy'	27001: 8.1 27001: A.15.1.2 27001: A.15.1.3	Partial Gap	Missing specification(s) in ISOs: Requirement of a Shared Security Responsibility Model (SSRM).
Supply Chain Agreement Review	STA-10	Review supply chain agreements between CSPs and CSCs at least annually.	STA-07	No Gap	N/A	27001: A.15.1 27001: A.15.2	Partial Gap	Missing specification(s) in ISOs: Requirement of a Shared Security Responsibility Model (SSRM).

# Supply Chain Management, Transparency, and Accountability – STA(3)

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
Internal Compliance Testing	STA-11	Define and implement a process for conducting internal assessments to confirm conformance and effectiveness of standards, policies, procedures, and service level agreement activities at least annually.	STA-04	No Gap	N/A	27001: A.15.2	Partial Gap	Missing specification(s) in ISOs: Requirement of a Shared Security Responsibility Model (SSRM).
Supply Chain Service Agreement Compliance	STA-12	Implement policies requiring all CSPs throughout the supply chain to comply with information security, confidentiality, access control, privacy, audit, personnel policy and service level requirements and standards.	STA-09	Partial Gap	Missing specification(s) in CCMv3.0.1: 'to comply with privacy, personnel policy.'	27001: 5.2 27001: A.5.1 27001: A.5.2 27001: A.7.2.1 27001: A.15.1.2 27001: A.15.1.3	Partial Gap	Missing specification(s) in ISOs: Requirement of a Shared Security Responsibility Model (SSRM).
Supply Chain Governance Review	STA-13	Periodically review the organization's supply chain partners' IT governance policies and procedures.	STA-06	No Gap	N/A	27001: 8.1 27001: 9.1 27001: 9.2 27001: 9.3 27001: A.15.1.2 27001: A.15.1.3	Partial Gap	Missing specification(s) in ISOs: Requirement of a Shared Security Responsibility Model (SSRM).
Supply Chain Data Security Assessment	STA-14	Define and implement a process for conducting security assessments periodically for all organizations within the supply chain.	STA-08	No Gap	N/A	27001: 8.1 27001: 8.2 27001: 8.3 27001: A.15.1.2 27001: A.15.1.3	Partial Gap	Missing specification(s) in ISOs: Requirement of a Shared Security Responsibility Model (SSRM).

# Threat and Vulnerability Management - TVM



By Royal Charter

**bsi.**

# Threat & Vulnerability Management – TVM(1)

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
Threat and Vulnerability Management Policy and Procedures	<b>TVM-01</b>	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to identify, report and prioritize the remediation of vulnerabilities, in order to protect systems against vulnerability exploitation. Review and update the policies and procedures at least annually.	<b>TVM-02 GRM-06 GRM-09</b>	<b>Partial Gap</b>	Missing specification(s) in CCMv3.0.1: Requirement of 'at least annually' in last sentence.	<b>27001: 5.2 27001: A.5.1.1 27002: 5.1.1 (c), (h)</b>	<b>No Gap</b>	N/A
Malware Protection Policy and Procedures	<b>TVM-02</b>	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect against malware on managed assets. Review and update the policies and procedures at least annually.	<b>TVM-01 GRM-06 GRM-09</b>	<b>Partial Gap</b>	Missing specification(s) in CCMv3.0.1: Requirement of 'at least annually' in last sentence.	<b>27001: A.5.1.1 27002: 5.1.1 (g), (c) 27001: A.5.1.2 27002: 5.1.2</b>	<b>Partial Gap</b>	Missing specification(s) in ISOs: Requirement of 'malware policy and procedures'
Vulnerability Remediation Schedule	<b>TVM-03</b>	Define, implement and evaluate processes, procedures and technical measures to enable both scheduled and emergency responses to vulnerability identifications, based on the identified risk.	<b>TVM-02</b>	<b>No Gap</b>	N/A	<b>27001: A12.2.1 27001: A.12.6.1 27002: 12.6.1(c)(d)(j) 27018: 12.6.1(k)(i)</b>	<b>No Gap</b>	N/A
Detection Updates	<b>TVM-04</b>	Define, implement and evaluate processes, procedures and technical measures to update detection tools, threat signatures, and indicators of compromise on a weekly, or more frequent basis.	<b>No mapping</b>	<b>Full Gap</b>	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	<b>27001: A.5.1.1 27002: 5.1.1 (h) 27001: A.12.6.1 27002: 12.6.1 (b),(c)</b>	<b>Partial Gap</b>	Missing specification(s) in ISOs: Requirement of 'detection tools and or a specific time frame for updates as well as no mention of IOC's'
External Library Vulnerabilities	<b>TVM-05</b>	Define, implement and evaluate processes, procedures and technical measures to identify updates for applications which use third party or open source libraries according to the organization's vulnerability management policy.	<b>No mapping</b>	<b>Full Gap</b>	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	<b>27001: A.12.6.2 27002: 12.6.2</b>	<b>Partial Gap</b>	Missing specification(s) in ISOs: Requirement of 'for applications which use...open source libraries according to the organization's vulnerability management standard.'

# Threat & Vulnerability Management – TVM(2)

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
Penetration Testing	TVM-06	Define, implement and evaluate processes, procedures and technical measures for the periodic performance of penetration testing by independent third parties.	TVM-02	Partial Gap	Recommend the full V4 control specification to be used to close the gap.  Portion in the mapped control(s) contributing to the partial gap, that is, covering in part the V4 control: (TVM-02) 'supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g., penetration testing)'	No Mapping	Full Gap	The full V4 control specification is missing from the ISOs and has to be used to close the gap.
Vulnerability Identification	TVM-07	Define, implement and evaluate processes, procedures and technical measures for the detection of vulnerabilities on organizationally managed assets at least monthly.	TVM-02	Partial Gap	Missing specification(s) in CCMv3.0.1: Requirement of 'at least monthly'.	27001: A.12.6 27001: A.12.6.1 27002: 12.6.1	No Gap	N/A
Vulnerability Prioritization	TVM-08	Use a risk-based model for effective prioritization of vulnerability remediation using an industry recognized framework.	TVM-02	Partial Gap	Missing specification(s) in CCMv3.0.1: 'vulnerability remediation using an industry recognized framework'.	No Mapping	Full Gap	The full V4 control specification is missing from the ISOs and has to be used to close the gap.
Vulnerability Management Reporting	TVM-09	Define and implement a process for tracking and reporting vulnerability identification and remediation activities that includes stakeholder notification.	TVM-02	No Gap	N/A	27001: A.16.1.2 27002: 16.1.2 27001: A.16.1.3 27002: 16.1.3	No Gap	N/A
Vulnerability Management Metrics	TVM-10	Establish, monitor and report metrics for vulnerability identification and remediation at defined intervals.	No mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	27001: 9.1(a)(e)	Partial Gap	Missing specification(s) in ISOs: Requirement of 'vulnerability remediation'

# Universal Endpoint Management - UEM



# Universal Endpoint Management - UEM(1)

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
Endpoint Devices Policy and Procedures	UEM-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for all endpoints. Review and update the policies and procedures at least annually.	GRM-06 GRM-09 MOS-03 MOS-04 MOS-08 MOS-11 MOS-12 MOS-13	Partial Gap	Missing specification(s) in CCMv3.0.1: 'endpoints' (The term is missing from CCMv3.0.1 and MOS domain. Mobile device policies are a subset of endpoint devices policy). 'apply, evaluate policies and procedures for all endpoints'. Requirement of 'at least annually' in last sentence.	27001: A.6.2.1 27002: 6.2.1 27017: 6.2.1 27018: 6.2.1	Partial Gap	Missing specification(s) in ISOs: Term 'endpoint' device
Application and Service Approval	UEM-02	Define, document, apply and evaluate a list of approved services, applications and sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data.	MOS-02 MOS-03 MOS-04 MOS-06	Partial Gap	Missing specification(s) in CCMv3.0.1: 'endpoint'. 'Define, apply and evaluate a list'	27001: A.9.1.1 27002: 9.1.1 27001: A.9.2.2 27002: 9.2.2 27001: A.12.1.2 27002: 12.1.2 27001: A.12.5 27002: 12.5 27001: A.13.2.3 27002: 13.2.3 27001: A.14.2.2 27002:14.2.2	Partial Gap	Missing specification(s) in ISOs: Term 'endpoint' device
Compatibility	UEM-03	Define and implement a process for the validation of the endpoint device's compatibility with operating systems and applications.	MOS-07	Partial Gap	Missing specification(s) in CCMv3.0.1: 'endpoint'. 'Define and implement a process'.	27001: A.14.2.4 27002: 14.2.4	Partial Gap	Missing specification(s) in ISOs: Term 'endpoint' device
Endpoint Inventory	UEM-04	Maintain an inventory of all endpoints used to store and access company data.	MOS-09	Partial Gap	Missing specification(s) in CCMv3.0.1: 'endpoints'.	27001: A.8.1.1 27002: 8.1.1 27017: 8.1.1	Partial Gap	Missing specification(s) in ISOs: Term 'endpoint' device

# Universal Endpoint Management - UEM(2)

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
Endpoint Management	UEM-05	Define, implement and evaluate processes, procedures and technical measures to enforce policies and controls for all endpoints permitted to access systems and/or store, transmit, or process organizational data.	MOS-10	Partial Gap	Missing specification(s) in CCMv3.0.1: 'endpoints'. 'Define, implement and evaluate processes, procedures and technical measures to enforce policies and controls for all endpoints'.	27001: A.12.6.2 27002:12.6.2	Partial Gap	Missing specification(s) in ISOs: Term 'endpoint' device
Automatic Lock Screen	UEM-06	Configure all relevant interactive-use endpoints to require an automatic lock screen.	MOS-14	Partial Gap	Missing specification(s) in CCMv3.0.1: 'endpoint'.	No Mapping	Full Gap	The full V4 control specification is missing from the ISOs and has to be used to close the gap.
Operating Systems	UEM-07	Manage changes to endpoint operating systems, patch levels, and/or applications through the company's change management processes.	MOS-15	Partial Gap	Missing specification(s) in CCMv3.0.1: 'endpoint'.	27001: A.14.2 27001: A.14.2.2 27002: 14.2.2 27001: A.14.2.3 27001: A.14.2.4 27018: 12.1.2	Partial Gap	Missing specification(s) in ISOs: Term 'endpoint' device
Storage Encryption	UEM-08	Protect information from unauthorized disclosure on managed endpoint devices with storage encryption.	MOS-11	Partial Gap	Missing specification(s) in CCMv3.0.1: 'endpoint'.	27001: A.11.2.7 27002: 11.2.7 27001: A.18.1.1 27017: 18.1.1 27001: A.12.3.1 27017: 12.3.1 27018: A.11.4 27018: A.11.5	Partial Gap	Missing specification(s) in ISOs: Term 'endpoint' device
Anti-Malware Detection and Prevention	UEM-09	Configure managed endpoints with anti-malware detection and prevention technology and services.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	27001: A.12.2 27002: 12.2 27017: 12.2 27018: 12.2	Partial Gap	Missing specification(s) in ISOs: Term 'endpoint' device



# Universal Endpoint Management - UEM(3)

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
Software Firewall	UEM-10	Configure managed endpoints with properly configured software firewalls.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	27001: A.12.6.1 27002: 12.6.1 27001: A.13.1.2 27002: 13.1.2 27001: A.6.2.2 27002: 6.2.2 27018: 16.1	Partial Gap	Missing specification(s) in ISOs: Term 'endpoint' device
Data Loss Prevention	UEM-11	Configure managed endpoints with Data Loss Prevention (DLP) technologies and rules in accordance with a risk assessment.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	27001: A.12.3 27002: 12.3 27001: A.8.3.1 27002: 8.3.1 27001: A.12.2 27002: 12.2 27001: A.18.1.3 27002: 18.1.3 27001: A.3.2.2 27002: 3.2.2 27001: A.6.1.1 27017: 6.1.1 27018: 12.3.1 27018: 10.1	Partial Gap	Missing specification(s) in ISOs: Term 'endpoint' device
Remote Locate	UEM-12	Enable remote geo-location capabilities for all managed mobile endpoints.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	27001: A.6.2.1 27002: 6.2.1	Partial Gap	Missing specification(s) in ISOs: Term 'endpoint' device

# Universal Endpoint Management - UEM(4)

Control Title	Control ID	Updated Control Specification	CCM v3.0.1			ISO/IEC 27001/02/17/18		
			Controls Mapping	Gap Level	Addenda	Controls Mapping	Gap Level	Addenda
Remote Wipe	UEM-13	Define, implement and evaluate processes, procedures and technical measures to enable the deletion of company data remotely on managed endpoint devices.	MOS-18	Partial Gap	Missing specification(s) in CCMv3.0.1: 'endpoint'. 'Define, implement and evaluate processes, procedures and technical measures'.	27001: A.6.2.1 27002: 6.2.1	Partial Gap	Missing specification(s) in ISOs: Term 'endpoint' device
Third-Party Endpoint Security Posture	UEM-14	Define, implement and evaluate processes, procedures and technical and/or contractual measures to maintain proper security of third-party endpoints with access to organizational assets.	No Mapping	Full Gap	The full V4 control specification is missing from CCMv3.0.1 and has to be used to close the gap.	27001: A.15.1.1 27002: 15.1.1 27001: A.14.1.2 27002: 14.1.2 27001: A.6.1.1 27017: 6.1.1 27001: A.9.2.2 27017: 9.2.2 27001: A.9.2.4 27017: 9.2.4	Partial Gap	Missing specification(s) in ISOs: Term 'endpoint' device

**bsi.**

...making excellence a habit.<sup>™</sup>