

bsi.

# ● CSA STAR Certificate ก้าการ ปรับเปลี่ยนข้อกำหนดใหม่

BSI Group (Thailand) Ltd.



# Discussion items

1. Background CSA STAR

2. สรุปข้อกำหนด CSA CCM version 4

3. การ transition จาก CSA CCM version 3  
ไปสู่ CSA CCM Version 4



# Background CSA STAR

# Who is the cloud security alliance?

Founded 2008

Support global policy makers

Currently 31 research initiatives and working groups

**CSA** *cloud security alliance*®



# STAR CERTIFICATION (ISO/IEC 27001)



Figure 3

# STAR CERTIFICATION (ISO/IEC 27001)

## Acquia

Acquia offers enterprises unparalleled freedom to innovate and increase business agility by creating extraordinary web experiences. The fastest growing open clo...

Listed Since: 01/13/2013



Submissions:



Submissions:



## Acronis

### Acronis International GmbH

Acronis sets the standard for cyber protection through its innovative backup, anti-ransomware, disaster recovery, storage, and enterprise file sync and share so...

Listed Since: 05/06/2020



Submissions:



# The CCM and maturity modelling

# Management capability score

1-3 No formal approach

4-6 Reactive approach

7-9 Proactive approach

10-12 Improvement based approach

13-15 Optimizing approach



# Reporting format and awards

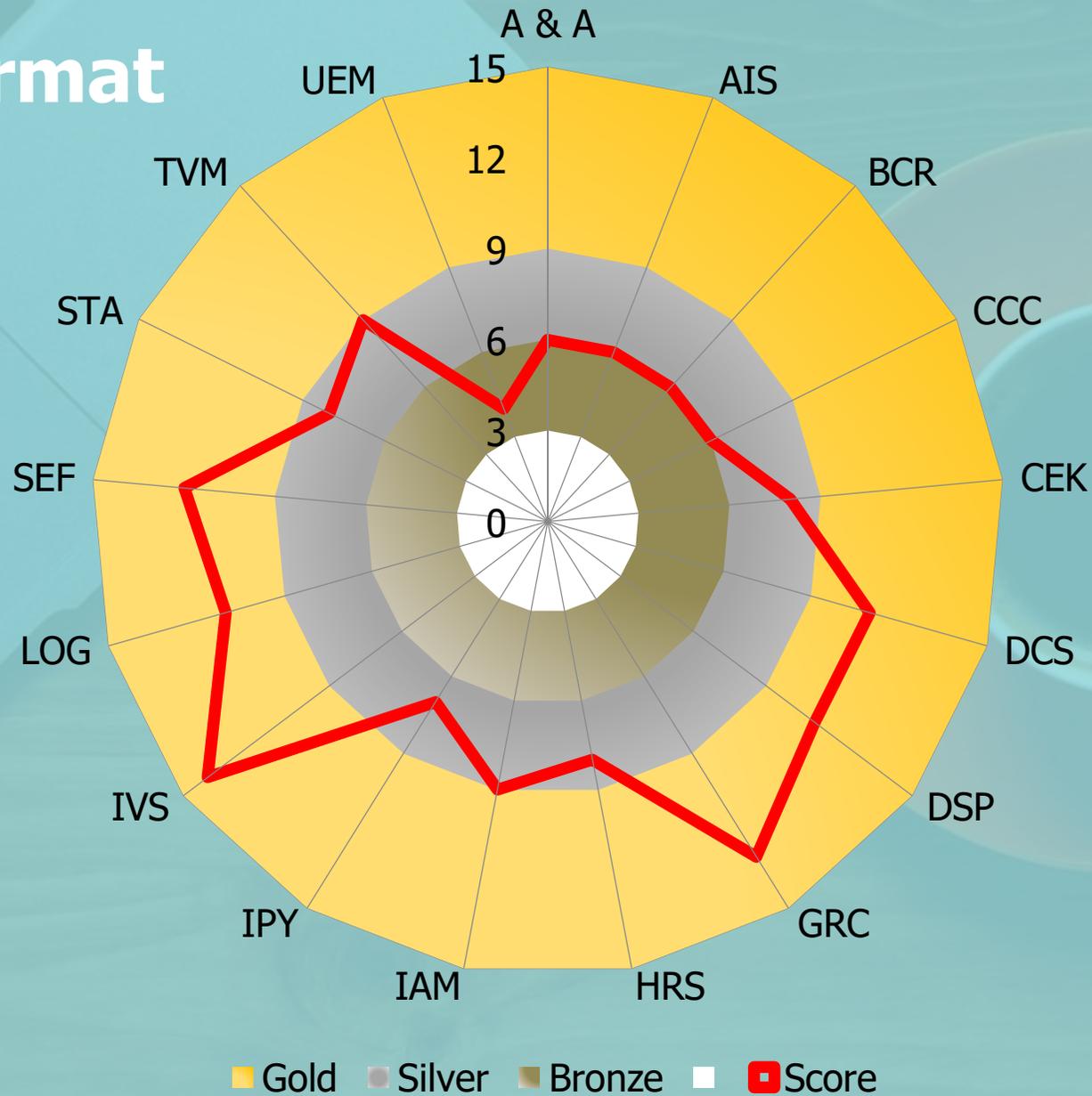
Control Domain	Control Title	Control ID	Control Specification	ISO/IEC 27001:2013 Control Mapping	Is the Control applicable?	Evidence the controls in place	Select NC status	Evidence of the maturity level	Select the Score	FINAL SCORE	ISO/IEC 27017:2015 and ISO/IEC 27018:2019 Control Mapping	
						Complete all the cells below						
Audit & Assurance	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.	9.2								
Audit & Assurance	Independent Assessments	A&A-02	Conduct independent audit and assurance assessments according to relevant standards at least annually.	A.18.2.1								
Audit & Assurance	Risk Based Planning Assessment	A&A-03	Perform independent audit and assurance assessments according to risk-based plans and policies.	A.18.2.1								27018: 18.2.1
Audit & Assurance	Requirements Compliance	A&A-04	Verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit.	A.18.2.2 A.18.2.3								
Audit & Assurance	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.	9.2.c A.18.2.2								
Audit & Assurance	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.	A.18.2.2								
<b>Audit &amp; Assurance - SCORE</b>									<b>0</b>	<b>0</b>		

# Reporting and format awards

<b>AIS-01</b>	<b>9</b>	
<b>AIS-02</b>	<b>7</b>	
<b>AIS-03</b>	<b>8</b>	
<b>AIS-04</b>	<b>8</b>	
<b>AIS-05</b>	<b>7</b>	
<b>AIS-06</b>	<b>3</b>	
<b>AIS-07</b>	<b>8</b>	
	<b>3</b>	<b>3</b>



# Reporting format and awards



Gold Silver Bronze Score

# Maturity model

Score	1 to 3	4 to 6	7 to 9	10 to 12	13 to 15
	No Formal Approach	Reactive	Proactive	Improving	Optimizing
Evidence/ Definition	1. There is no evidence or a system in place to manage the control area	4. There is evidence of a system in place to cover key operations in the control area. Where required, the system is documented	7. There is evidence of a robust system in place that covers all routine operations in the control area	10. There is evidence the system for managing the control area is capable of managing contingency events as well as routine activity	13. Control area owners can demonstrate that they actively review best practice from their industry and across their organization and apply it to the control area
Managed	2. There is some evidence of either a documented system or an accepted way of working is in place	5. There is a clearly identified owner for the control area who understands their scope of responsibility	8. There is evidence that the control area is actively monitored and measured and action evaluated based on the evidence	11. Input from a variety of sources is considered to decide how to manage risk and improve operations in this control area	14. Control owners actively share best practice to support development in other areas of the organization based on their experience in this control area
Followed / Effective	3. There is some evidence of an accepted way of working that is broadly understood and followed	6. There is evidence the system is understood and routinely followed	9. There is evidence that critical people operating in the control area are appropriately trained / skilled to manage routine operations in the control area	12. There is evidence that inputs from a range of stakeholders and monitoring and measuring systems has been taken into account when improving operations in the control area	15. Changes in the control area are evaluated against the strategic objectives of the organization

# **CCM-version 4.0**

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

---

## Structure of CCM version 4

14

---

17 security domains and 197 controls

---

Security Shared Responsibility Model (SSRM)

---

Applicability with others internal standard (mapping)

---

Implement guideline

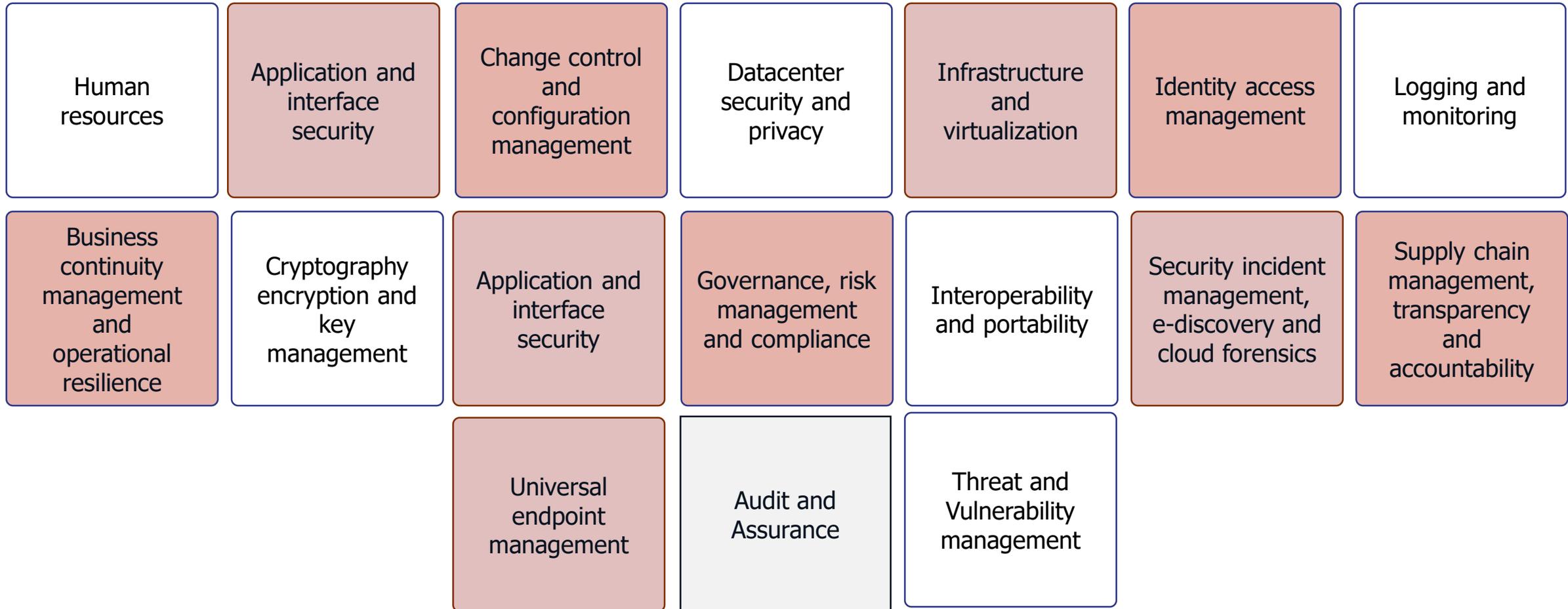
---

Auditing guideline

---

All above in one Excel file.

# Cloud Controls Matrix CCM V. 4 – 197 controls



These 17 domains contain a total of 197 Cloud Security Controls. Each control can have multiple relationships with the mapping frameworks. By mapping the Cloud Security Controls to the ISO/IEC 27001 clauses and controls, we can start to understand the management system structure of the CCM controls put in place by an organization.

As a framework, the CSA CCM provides organizations with the needed structure, detail and clarity relating to information security tailored to the cloud industry.

# Map CCM controls to ISO/IEC 27001

CCM™ CLOUD CONTROLS MATRIX v4.0.5				ISO/IEC 27001/02/17/18		
Control Domain	Control Title	Control ID	Control Specification	Control Mapping	Gap Level	Addendum
Audit & Assurance	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.	27001: 9.2	Partial Gap	Missing specification(s) in ISOs: Requirement of 'at least annually' in last sentence.
Audit & Assurance	Independent Assessments	A&A-02	Conduct independent audit and assurance assessments according to relevant standards at least annually.	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.
Audit & Assurance	Risk Based Planning Assessment	A&A-03	Perform independent audit and assurance assessments according to risk-based plans and policies.	27001: A.18.2.1 27002: 18.2.1 27018: 18.2.1	No Gap	N/A
Audit & Assurance	Requirements Compliance	A&A-04	Verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit.	27001: A.18.2.2 27002: 18.2.2 27001: A.18.2.3 27002: 18.2.3	No Gap	N/A

# CCM version 4 - Share responsibility model

				Typical Control Applicability and Ownership			Architectural Relevance – Cloud Stack Components						
Control Domain	Control Title	Control ID	Control Specification	IaaS	PaaS	SaaS	Phys	Network	Compute	Storage	App	Data	Cy
<b>Audit &amp; Assurance – A&amp;A</b>													
Audit & Assurance	Audit and Assurance Policy and Procedures	<b>A&amp;A-01</b>	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.	Shared	Shared	Shared	TRUE	FALSE	FALSE	FALSE	TRUE	TRUE	
Audit & Assurance	Independent Assessments	<b>A&amp;A-02</b>	Conduct independent audit and assurance assessments according to relevant standards at least annually.	Shared	Shared	Shared	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	
Audit & Assurance	Risk Based Planning Assessment	<b>A&amp;A-03</b>	Perform independent audit and assurance assessments according to risk-based plans and policies.	Shared	Shared	Shared	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	
Audit & Assurance	Requirements Compliance	<b>A&amp;A-04</b>	Verify compliance with all relevant standards, regulations, legal/contractual and statutory requirements applicable to the audit.	Shared	Shared	Shared	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	
Audit & Assurance	Audit Management Process	<b>A&amp;A-05</b>	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	Shared	Shared	Shared	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	
Audit & Assurance	Remediation	<b>A&amp;A-06</b>	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.	Shared	Shared	Shared	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	
<b>Application &amp; Interface Security – AIS</b>													

# Audit and Assurance - A&A



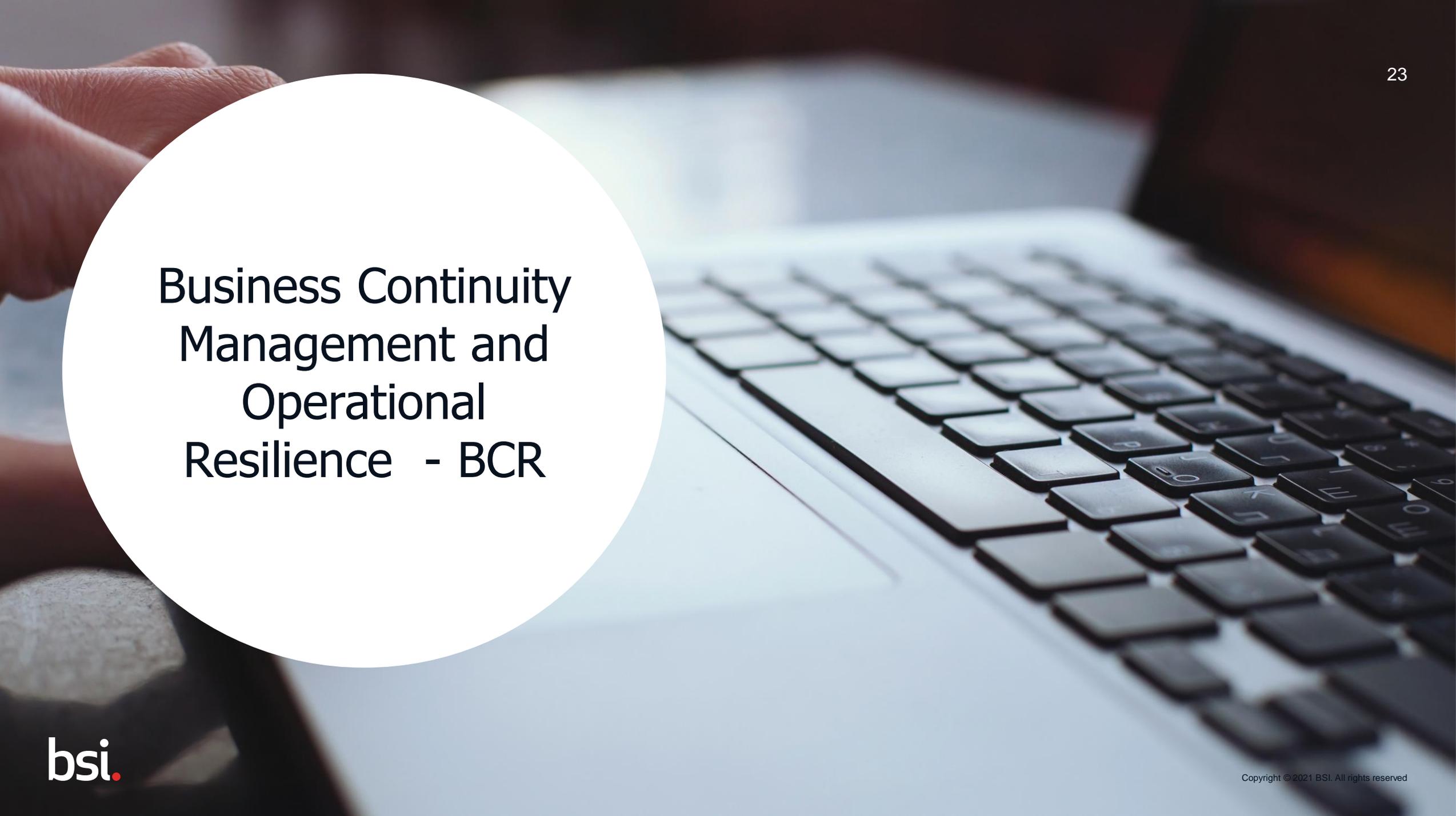
<b>Control ID</b>	<b>Control Title</b>	<b>Control ID</b>	<b>Control Title</b>
A&A-01	Audit and Assurance Policy and Procedures	A&A-04	Requirements Compliance
A&A-02	Independent Assessments	A&A-05	Audit Management Process
A&A-03	Risk Based Planning Assessment	A&A-06	Remediation



Application and  
Interface Security  
- AIS

# Application and Interface Security - AIS

<b>Control ID</b>	<b>Control Title</b>	<b>Control ID</b>	<b>Control Title</b>
AIS-01	Application and Interface Security Policy and Procedures	AIS-05	Automated Application Security Testing
AIS-02	Application Security Baseline Requirements	AIS-06	Automated Secure Application Deployment
AIS-03	Application Security Metrics	AIS-07	Application Vulnerability Remediation
AIS-04	Secure Application Design and Development		



**Business Continuity  
Management and  
Operational  
Resilience - BCR**

<b>Control ID</b>	<b>Control Title</b>	<b>Control ID</b>	<b>Control Title</b>
BCR-01	Business Continuity Management Policy and Procedures	BCR-07	Communication
BCR-02	Risk Assessment and Impact Analysis	BCR-08	Backup
BCR-03	Business Continuity Strategy	BCR-08	Disaster Response Plan
BCR-04	Business Continuity Planning	BCR-10	Response Plan Exercise
BCR-05	Documentation	BCR-11	Equipment Redundancy
BCR-06	Business Continuity Exercises		

# Change Control and Configuration Management - CCC

# Change Control and Configuration Management - CCC

<b>Control ID</b>	<b>Control Title</b>	<b>Control ID</b>	<b>Control Title</b>
CCC-01	Change Management Policy and Procedures	CCC-06	Change Management Baseline
CCC-02	Quality Testing	CCC-07	Detection of Baseline Deviation
CCC-03	Change Management Technology	CCC-08	Exception Management
CCC-04	Unauthorized Change Protection	CCC-09	Change Restoration
CCC-05	Change Agreements		

# Cryptography, Encryption and Key Management - CEK

# Cryptography, Encryption and Key Management - CEK

<b>Control ID</b>	<b>Control Title</b>	<b>Control ID</b>	<b>Control Title</b>
CEK-01	Encryption and Key Management Policy and Procedures	CEK-12	Key Rotation
CEK-02	CEK Roles and Responsibilities	CEK-13	Key Revocation
CEK-03	Data Encryption	CEK-14	Key Destruction
CEK-04	Encryption Algorithm	CEK-15	Key Activation
CEK-05	Encryption Change Management	CEK-16	Key Suspension
CEK-06	Encryption Change Cost Benefit Analysis	CEK-17	Key Deactivation
CEK-07	Encryption Risk Management	CEK-18	Key Archival
CEK-08	CSC Key Management Capability	CEK-19	Key Compromise
CEK-09	Encryption and Key Management Audit	CEK-20	Key Recovery
CEK-10	Key Generation	CEK-21	Key Inventory Management
CEK-11	Key Purpose		

# Datacenter Security - DCS

<b>Control ID</b>	<b>Control Title</b>	<b>Control ID</b>	<b>Control Title</b>
DCS-01	Off-Site Equipment Disposal Policy and Procedures	DCS-09	Secure Area Authorization
DCS-02	Off-Site Transfer Authorization Policy and Procedures	DCS-10	Surveillance System
DCS-03	Secure Area Policy and Procedures	DCS-11	Unauthorized Access Response Training
DCS-04	Secure Media Transportation Policy and Procedures	DCS-12	Cabling Security
DCS-05	Assets Classification	DCS-13	Environmental Systems
DCS-06	Assets Cataloguing and Tracking	DCS-14	Secure Utilities
DCS-07	Controlled Access Points	DCS-15	Equipment Location
DCS-08	Equipment Identification		



# Data Security and Privacy Lifecycle Management

# Data Security and Privacy Lifecycle Management - DSP

<b>Control ID</b>	<b>Control Title</b>	<b>Control ID</b>	<b>Control Title</b>
DSP-01	Security and Privacy Policy and Procedures	DSP-11	Personal Data Access, Reversal, Rectification and Deletion
DSP-02	Secure Disposal	DSP-12	Limitation of Purpose in Personal Data Processing
DSP-03	Data Inventory	DSP-13	Personal Data Sub-processing
DSP-04	Data Classification	DSP-14	Disclosure of Data Sub-processors
DSP-05	Data Flow Documentation	DSP-15	Limitation of Production Data Use
DSP-06	Data Ownership and Stewardship	DSP-16	Data Retention and Deletion
DSP-07	Data Protection by Design and Default	DSP-17	Sensitive Data Protection
DSP-08	Data Privacy by Design and Default	DSP-18	Disclosure Notification
DSP-09	Data Protection Impact Assessment	DSP-19	Data Location
DSP-10	Sensitive Data Transfer		



<b>Control ID</b>	<b>Control Title</b>	<b>Control ID</b>	<b>Control Title</b>
GRC-01	Governance Program Policy and Procedures	GRC-05	Information Security Program
GRC-02	Risk Management Program	GRC-06	Governance Responsibility Model
GRC-03	Organizational Policy Reviews	GRC-07	Information System Regulatory Mapping
GRC-04	Policy Exception Process	GRC-08	Special Interest Groups

A hand is holding a magnifying glass over a network diagram. The diagram consists of several stylized human figures connected by dashed lines, forming a web. Two of the figures are highlighted with a thick black circle. The magnifying glass is positioned over the central part of the diagram, focusing on the text.

# Human Resources - HRS

---

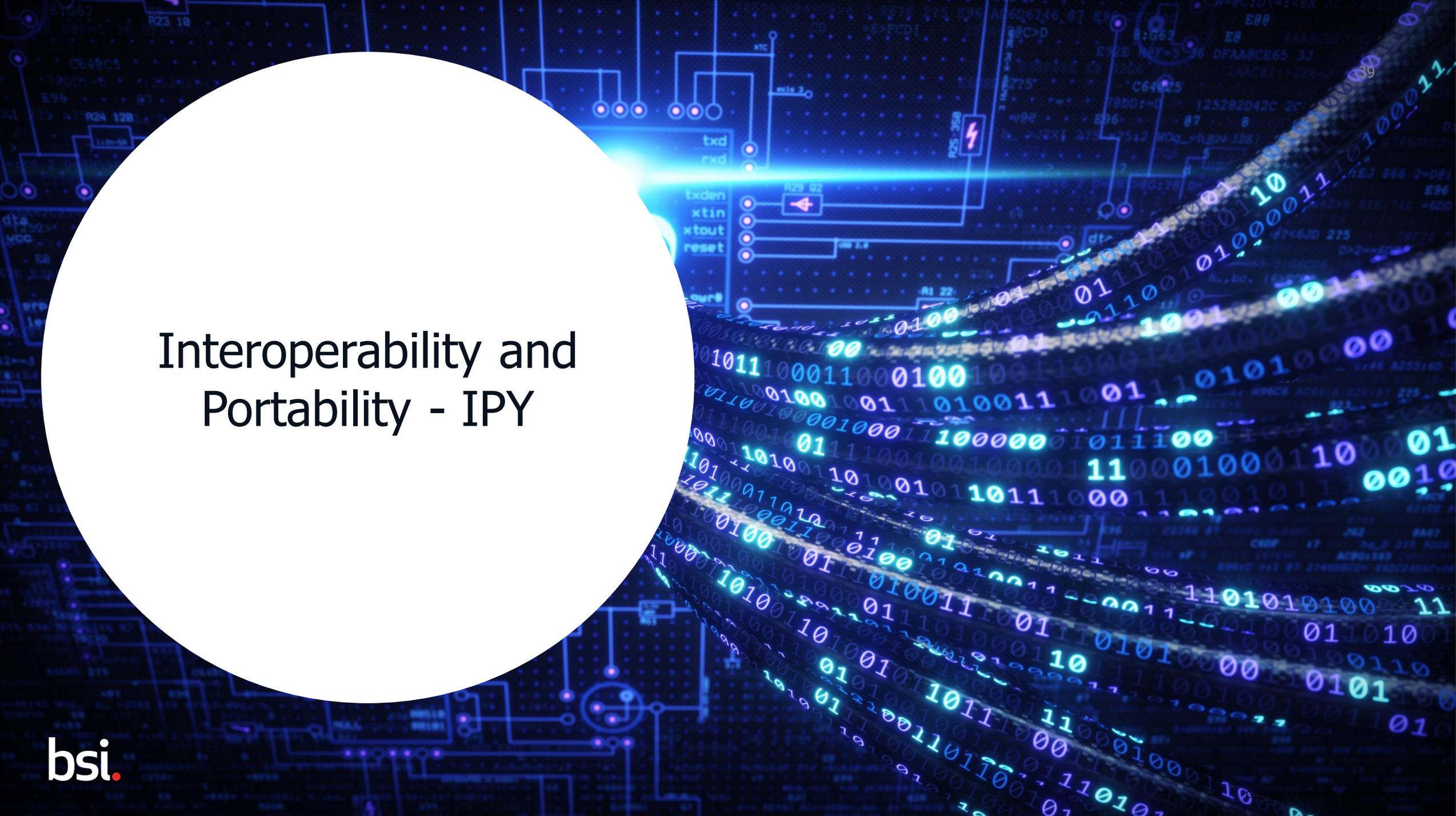
## Human Resources - HRS

<b>Control ID</b>	<b>Control Title</b>	<b>Control ID</b>	<b>Control Title</b>
HRS-01	Background Screening Policy and Procedures	HRS-08	Employment Agreement Content
HRS-02	Acceptable Use of Technology Policy and Procedures	HRS-09	Personnel Roles and Responsibilities
HRS-03	Clean Desk Policy and Procedures	HRS-10	Non-Disclosure Agreements
HRS-04	Remote and Home Working Policy and Procedures	HRS-11	Security Awareness Training
HRS-05	Asset returns	HRS-12	Personal and Sensitive Data Awareness and Training
HRS-06	Employment Termination	HRS-13	Compliance User Responsibility
HRS-07	Employment Agreement Process		



Identity and  
Access  
Management -  
IAM

<b>Control ID</b>	<b>Control Title</b>	<b>Control ID</b>	<b>Control Title</b>
IAM-01	Identity and Access Management Policy and Procedures	IAM-09	Segregation of Privileged Access Roles
IAM-02	Strong Password Policy and Procedures	IAM-10	Management of Privileged Access Roles
IAM-03	Identity Inventory	IAM-11	CSCs Approval for Agreed Privileged Access Roles
IAM-04	Separation of Duties	IAM-12	Safeguard Logs Integrity
IAM-05	Least Privilege	IAM-13	Uniquely Identifiable Users
IAM-06	User Access Provisioning	IAM-14	Strong Authentication
IAM-07	User Access Changes and Revocation	IAM-15	Passwords Management
IAM-08	User Access Review	IAM-16	Authorization Mechanisms



# Interoperability and Portability - IPY

<b>Control ID</b>	<b>Control Title</b>	<b>Control ID</b>	<b>Control Title</b>
IPY-01	Interoperability and Portability Policy and Procedures	IPY-03	Secure Interoperability and Portability Management
IPY-02	Application Interface Availability	IPY-04	Data Portability Contractual Obligations

Infrastructure and  
Virtualization Security  
- IVS



<b>Control ID</b>	<b>Control Title</b>	<b>Control ID</b>	<b>Control Title</b>
IVS-01	Infrastructure and Virtualization Security Policy and Procedures	IVS-06	Segmentation and Segregation
IVS-02	Capacity and Resource Planning	IVS-07	Migration to Cloud Environments
IVS-03	Network Security	IVS-08	Network Architecture Documentation
IVS-04	OS Hardening and Base Controls	IVS-09	Network Defense
IVS-05	Production and Non-Production Environments		



Logging and  
Monitoring - LOG

<b>Control ID</b>	<b>Control Title</b>	<b>Control ID</b>	<b>Control Title</b>
LOG-01	Logging and Monitoring Policy and Procedures	LOG-08	Log Records
LOG-02	Audit Logs Protection	LOG-09	Log Protection
LOG-03	Security Monitoring and Alerting	LOG-10	Encryption Monitoring and Reporting
LOG-04	Audit Logs Access and Accountability	LOG-11	Transaction/Activity Logging
LOG-05	Audit Logs Monitoring and Response	LOG-12	Access Control Logs
LOG-06	Clock Synchronization	LOG-13	Failures and Anomalies Reporting
LOG-07	Logging Scope		



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

<b>Control ID</b>	<b>Control Title</b>	<b>Control ID</b>	<b>Control Title</b>
SEF-01	Security Incident Management Policy and Procedures	SEF-05	Incident Response Metrics
SEF-02	Service Management Policy and Procedures	SEF-06	Event Triage Processes
SEF-03	Incident Response Plans	SEF-07	Security Breach Notification
SEF-04	Incident Response Testing	SEF-08	Points of Contact Maintenance

A white drone is flying in the upper right quadrant of the image, positioned against a bright, hazy sunset sky. Below the drone is a vast field of green crops, likely corn, which fills the lower two-thirds of the frame. The lighting is warm and golden, creating a soft glow over the entire scene. A large white circle is overlaid on the left side of the image, containing the main title text.

Supply Chain  
Management,  
Transparency, and  
Accountability - STA

# Supply Chain Management, Transparency, and Accountability - STA

<b>Control ID</b>	<b>Control Title</b>	<b>Control ID</b>	<b>Control Title</b>
STA-01	SSRM Policy and Procedures	STA-08	Supply Chain Risk Management
STA-02	SSRM Supply Chain	STA-09	Primary Service and Contractual Agreement
STA-03	SSRM Guidance	STA-10	Supply Chain Agreement Review
STA-04	SSRM Control Ownership	STA-11	Internal Compliance Testing
STA-05	SSRM Documentation Review	STA-12	Supply Chain Service Agreement Compliance
STA-06	SSRM Control Implementation	STA-13	Supply Chain Governance Review
STA-07	Supply Chain Inventory	STA-14	Supply Chain Data Security Assessment



# Threat and Vulnerability Management - TVM

# Threat and Vulnerability Management - TVM

<b>Control ID</b>	<b>Control Title</b>	<b>Control ID</b>	<b>Control Title</b>
TVM-01	Threat and Vulnerability Management Policy and Procedures	TVM-06	Penetration Testing
TVM-02	Malware Protection Policy and Procedures	TVM-07	Vulnerability Identification
TVM-03	Vulnerability Remediation Schedule	TVM-08	Vulnerability Prioritization
TVM-04	Detection Updates	TVM-09	Vulnerability Management Reporting
TVM-05	External Library Vulnerabilities	TVM-10	Vulnerability Management Metrics

The background features a complex digital interface with various data visualizations. On the left, a person's hand is shown using a stylus on a tablet. The interface includes several circular gauges with percentage values (25%, 50%, 75%, 55%, 75%, 35%, 65%, 70%, 25%, 50%), bar charts, and text labels such as 'SENSORS', 'LOCATION INTER...', 'SIBUS', and 'DETROIT'. A robotic arm is visible in the center-right, and the overall color scheme is a deep blue with glowing light effects.

# Universal Endpoint Management - UEM

<b>Control ID</b>	<b>Control Title</b>	<b>Control ID</b>	<b>Control Title</b>
UEM-01	Endpoint Devices Policy and Procedures	UEM-08	Storage Encryption
UEM-02	Application and Service Approval	UEM-09	Anti-Malware Detection and Prevention
UEM-03	Compatibility	UEM-10	Software Firewall
UEM-04	Endpoint Inventory	UEM-11	Data Loss Prevention
UEM-05	Endpoint Management	UEM-12	Remote Locate
UEM-06	Automatic Lock Screen	UEM-13	Remote Wipe
UEM-07	Operating Systems	UEM-14	Third-Party Endpoint Security Posture

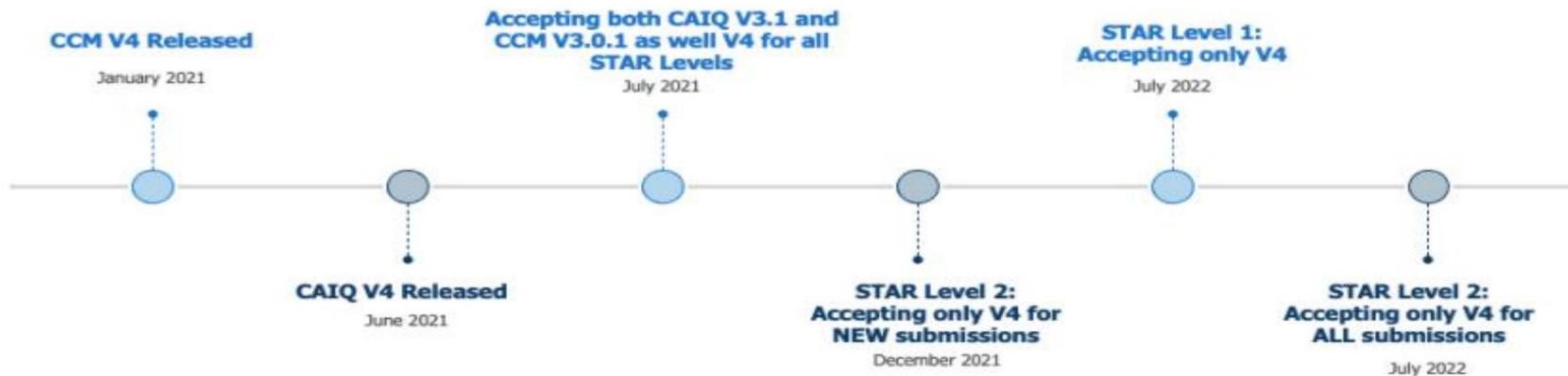
A woman with curly hair, wearing a red top, is shown in profile from the chest up, looking at a smartphone. The background is a stylized, light blue city map with white lines representing streets and buildings. Some street names like 'BANK', 'LONDON HOUSE', 'LONDON STREET', and 'MONUMENT' are visible. There are also numbered circles (1, 2, 3, 5, 6, 9, 10, 11, 13, 14, 16, 18, 20, 23, 25, 27, 28, 29, 30, 34, 35) scattered across the map. A large white circle is overlaid on the left side of the image, containing the text.

# Transition from CSA CCM version 3 to CSA CCM Version 4

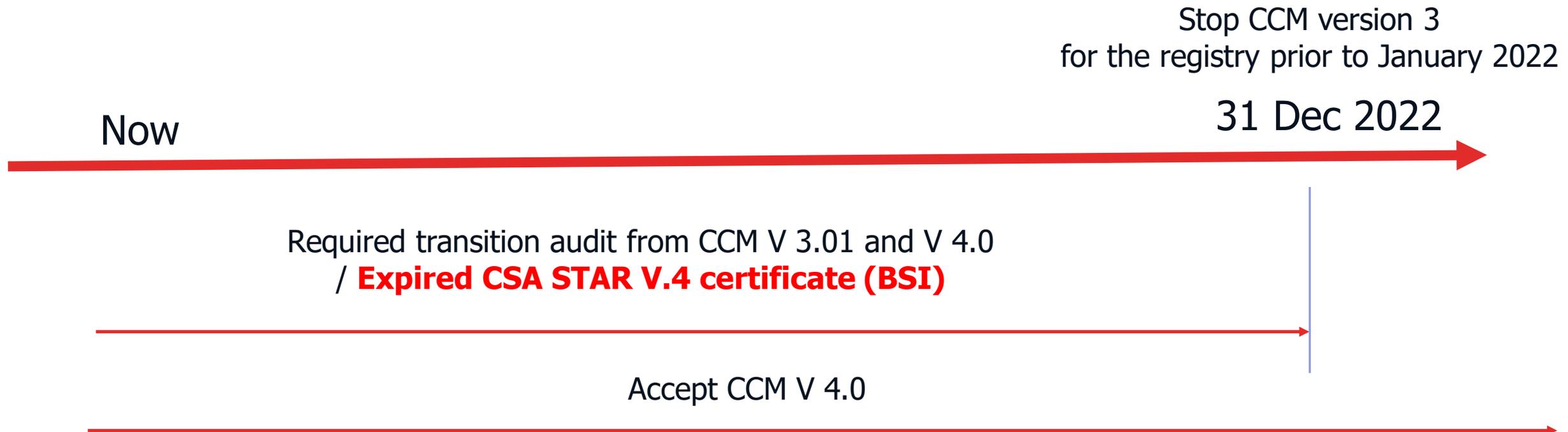
On January 21st CSA released version 4 of the Cloud Controls Matrix (CCM).

The new version ensures coverage of requirements deriving from new cloud technologies, new controls and enhanced interoperability and compatibility with other standards

## STAR Program Transition Timeline



# CCM Version 4 Transition Timeline (CSA Requirement)



## Prepare for Transition to CCM version 4

Study and implement CCM version 4 integrated to ISO/IEC 27001

Prepare CAIQ V4 and post to CSA Website

BSI audit CCM version 4 and issue certificate (CCM version 4)

Post certificate in CSA website

Note: all activities required to completed with in end of December 2022

# ● Thank you

## Further Information & Support

Address: BSI Group (Thailand) Co., Ltd.  
127/29 Panjathani Tower, 24<sup>th</sup> Fl. Nonsee  
Road, Chongnonsee, Yannawa, Bangkok  
10120

Tel: 02 294 4889-92

Fax: 02 294 4467

Email: [infothai@bsigroup.com](mailto:infothai@bsigroup.com)

Website: [www.bsigroup.com/en-th](http://www.bsigroup.com/en-th)