الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

CCC Methodology and Mapping Annex

DRAFT VERSION

Sharing Indicator: White
Document Classification: Open

In the Name of Allah,
The Most Gracious,
The Most Merciful

Traffic Light Protocol (TLP):

This marking protocol is widely used around the world. It has four colors (traffic lights):

Red - Personal, Confidential and for Intended Recipient only

The recipient has no rights to share information classified in red with any person outside the defined range of recipients either inside or outside the organization.

Amber - Restricted Sharing

The recipient may share information classified in amber only with intended recipients inside the organization and with recipients who are required to take action related to the shared information.

Green - Sharing within the Same Community

The recipient may share information classified in green with other recipients inside the organization or outside it within the same sector or related to the organization. However, it is not allowed to exchange or publish this information on public channels.

White - No Restrictions

Table of Contents

Table of Figures

Table of Tables

Design principles of the CCC

The CCC was designed to provide controls to both CSPs and CSTs.

The CCC was designed as a modular extension to ECC. Both CSPs and CSTs shall comply with ECC controls first, and then the additional controls provided by the CCC. In other words, **compliance with ECC is required as a pre-requisite to compliance to CCC.**

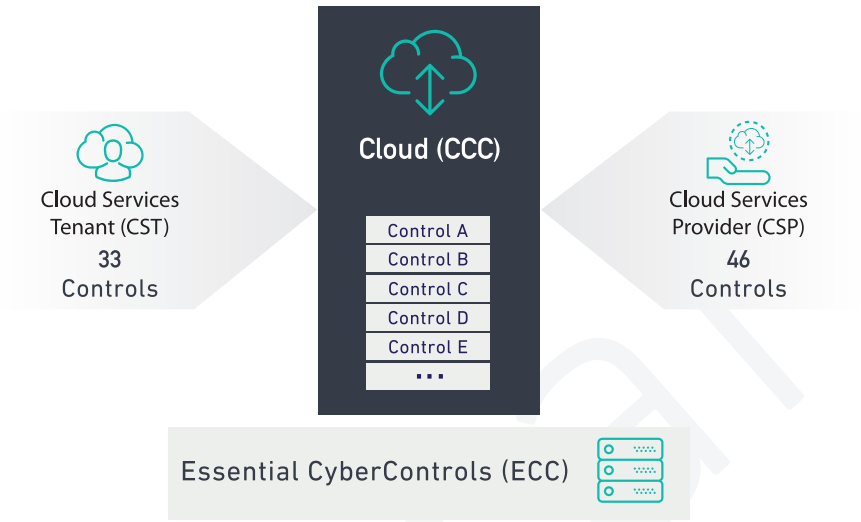

Figure 1: CCC as a modular extension of the ECC

For CSPs, the following principles were applied:

- High level cybersecurity leveraging other countries' cloud security standards (such as US FedRAMP. Singapore MTCS, Germany C5) or industry standards (CCM, ISO27000 series).

- The control/subcontrol catalogue has a reference to other standards, so that CSPs can leverage previous certifications from other countries. References are provided in section "Domain mapping to international standards" and section "Control mapping" .

For CSTs, the following principle was applied

- The security level of the controls in the CCC is additional to the security levels of the ECC

Relationship to other international standards

The international cloud computing standards and guideline formed the foundation for the CCC controls. The five leading standards used were:

- ISO/IEC 27000-series
- The Federal Risk and Authorization Management Program (FedRAMP (FR))
- The Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)
- German Government-backed Cloud Computing Compliance Controls Catalog (C5)
- The Multi-Tier Cloud Security (MTCS) Singapore standard

Design methodology of the CCC

To accomplish the CCC aims, the design methodology reviewed existing and anticipated data privacy and protection laws and regulations, national government managed cloud computing certifications and attestations, international cloud computing standards and guidelines. Informed by this baseline data, the NCA designed the CCC controls as an extension to the ECC in terms of both depth and outreach through the cloud computing sector.

In developing the CCC controls, security controls across a consolidated domain list were distilled from the five cloud security reference standards described in section "Relationship to other international standards" into a consolidated stack of cloud controls. A comparison with the existing ECC controls provided the delta that will define the scope.

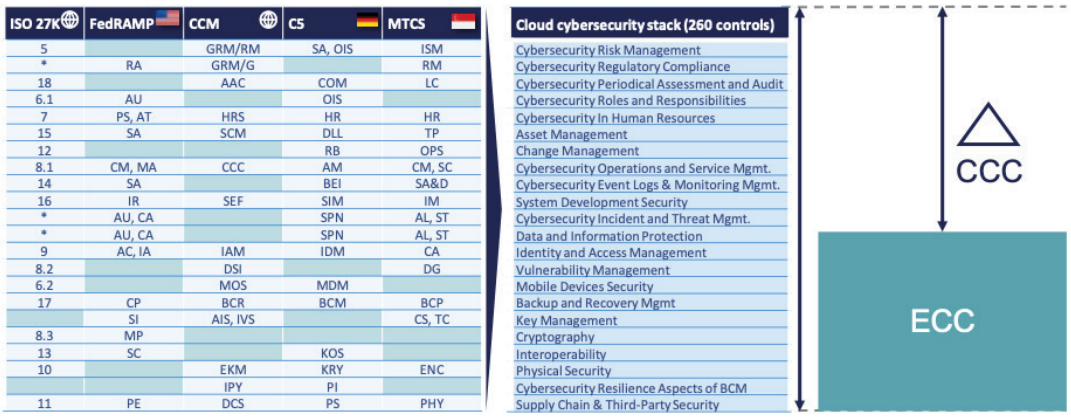

Figure 2: International cloud computing standards distilled to the consolidated control list

Main Domains and Subdomains structure of the CCC

Relationship to ECC:

The ECC and CCC main domains and sub domains are aligned in a structure. Four of the five ECC domains are in the CCC. In addition, 20 of the ECC subdomains are CCC subdomains (Shown in white in Figure 3). Six new subdomains were added as they were specific to cloud computing services (shown in dark blue in Figure 3). Eight ECC domains do not have specific controls for cloud and are not part of CCC (shown in grey in Figure 3).

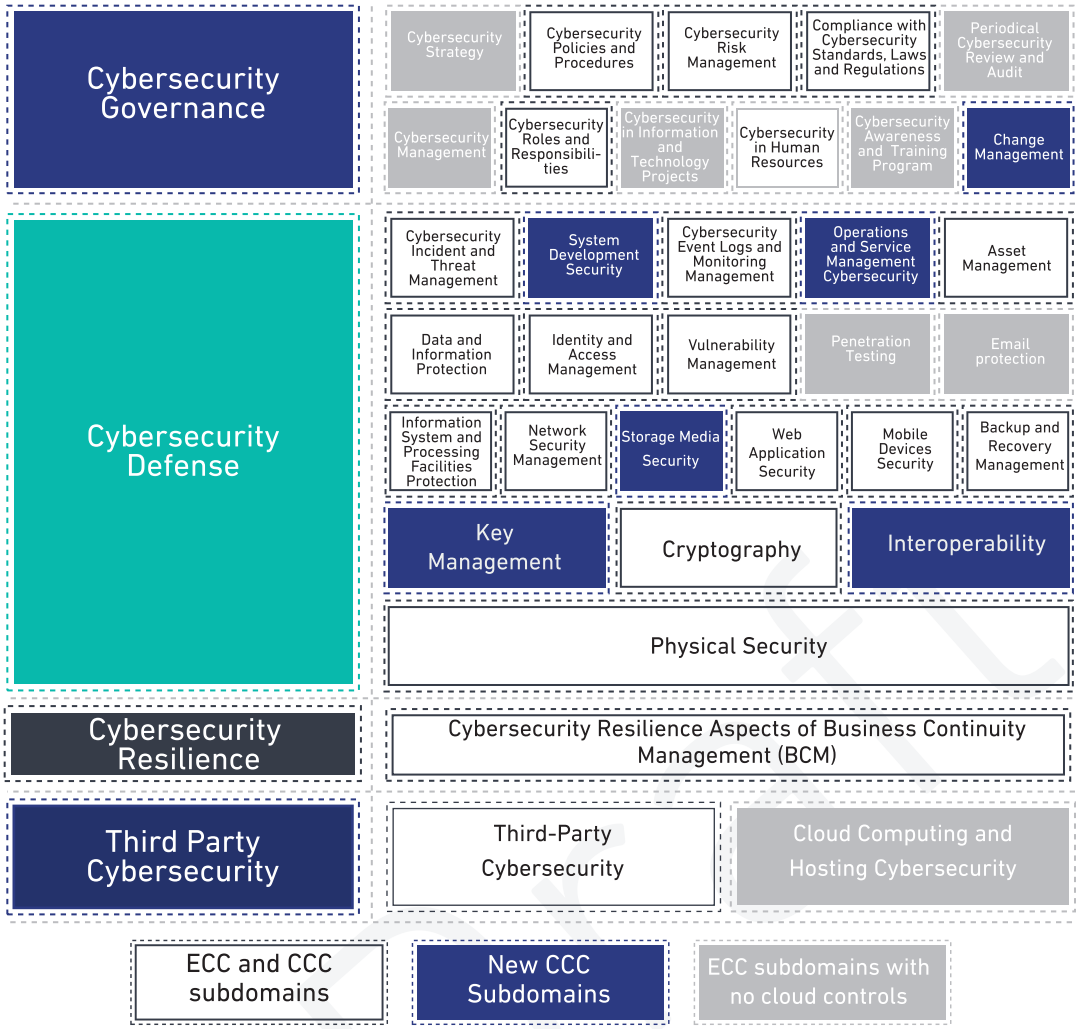

Figure 3: Main Domain and Subdomain basis of the CCC

Main Domains and Subdomains structure of the Cloud Cybersecurity Controls:

As a result of the above, the CCC is constituted by the following Main Domains and Subdomains:

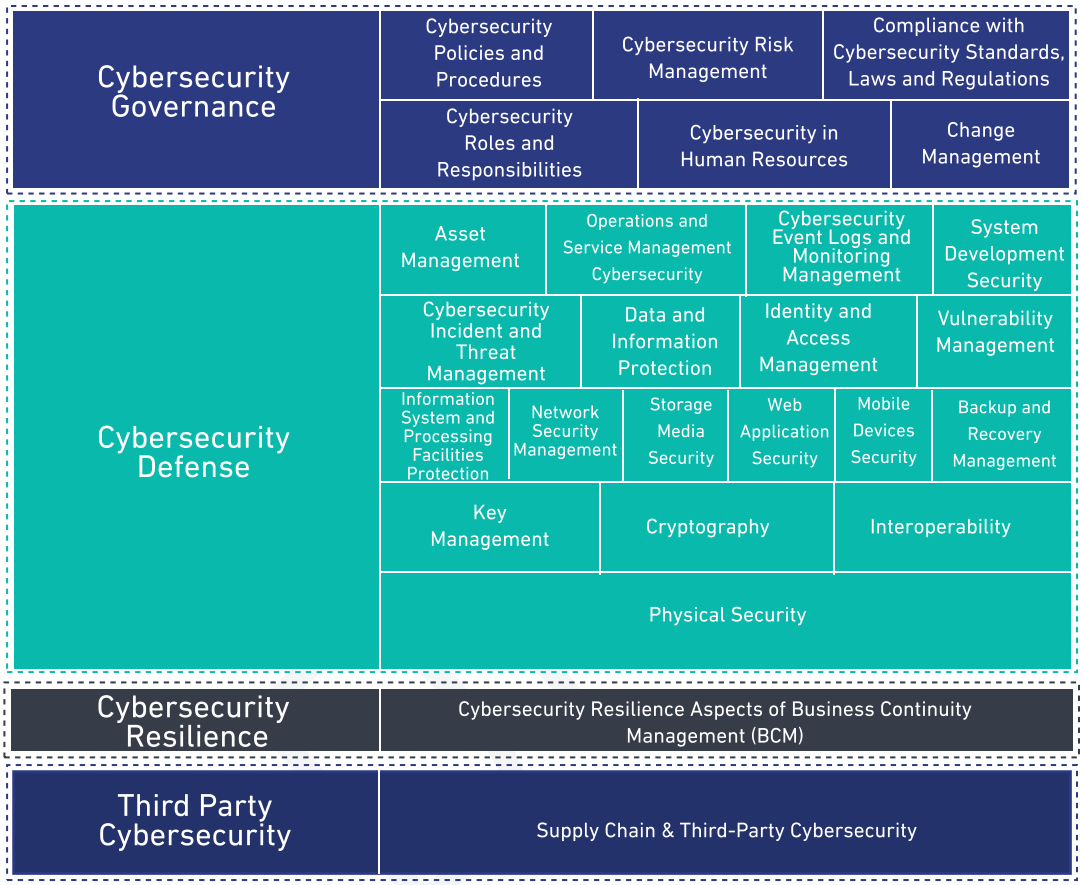

Figure 4: CCC Main Domain and Subdomain stack

Domain mapping to international standards

In case of a discrepancy between the CCC domain and the five international standards referenced, the CCC description shall take precedence.

Main Domains	CCC Domains		Standard Domain Comparison				
			ISO 27K	FEDRamp (US)	CCM	C5 (DE)	MTCS (SGP)
Cybersecurity Governance	1-1	Cybersecurity Policies and Procedures	A.5		GRM/ RM	2 - SA	6
	1-2	Cybersecurity Risk Management	6.1	RA	GRM/G		8
	1-3	Compliance with Cybersecurity Standards, Laws and Regulations	A.18		AAC	16 - COM	10
	1-4	Cybersecurity Roles and Responsibilities	A.6.1	AU		1 - OIS	
	1-5	Cybersecurity in Human Resources	A.7	PS	HRS	3 - HR	7
				AT			
	1-6	Change Management	A.12			6 - RB	19
Cybersecurity Defense	2-1	Asset Management	A.8.1	CM	CCC	4 -AM	20
				MA			14
	2-2	Operations and Service Management Cybersecurity	A.12	MA		6 - RB	19
	2-3	Cybersecurity Event Logs and Monitoring Management		AU			13
				CA		15- SPN	15
	2-4	System Development Security	A.14	SA		11- BEI	16
	2-5	Cybersecurity Incident and Threat Management	A.16	IR	SEF	13 - SIM	11
	2-6	Data and Information Protection	A.8.2		DSI		12

	2-7	Identity and Access Management	A.9	AC	IAM		23
				IA		7 - IDM	
	2-8	Vulnerability Management			TVM		
	2-9	Information System and Processing Facilities Protection		SC	AIS		22
				SI	IVS		4
	2-10	Networks Security Management	A.13	SC		9 - KOS	
			A.13	SC			
	2-11	Storage Media Security	A.8.3	MP			
	2-12	Web Application security					
	2-13	Mobile Devices Security	A.6.2		MOS	17 – MDM	
	2-14	Backup and Recovery Management					
	2-15	Key Management	A.10		EKM	8 - KRY	17
	2-16	Cryptography	A.10		EKM	8 - KRY	17
	2-17	Interoperability			IPY	10 - PI	
	2-18	Physical Security	A.11	PE	DCS	5 - PS	
Cybersecurity Resilience	3-1	BC/DR	A.17	CP	BCR	14 - BCM	21
Third-party Cybersecurity	4-1	Supply Chain & Third-Party Security	A.15	SA	SCM	12 - DLL	9

Table 1: CCC Domain Mapping to International Standards

Control Mapping

In case of a discrepancy between the CCC controls and the five international standards referenced, the CCC control description shall take precedence.

Please note that Standard reference 'original' implies that it was not mentioned in the five international standards.

1 Cybersecurity Governance

Subdomain ID	Subdomain	CSP Control ID	CST Control ID	Standard reference	Other standard references
CCC-1-1	Cybersecurity Policies and Procedures	1-1-P-1-1		C5 SA-03	
CCC-1-2	Cybersecurity Risk Management	1-2-P-1-1	1-2-T-1-1	CCM GRM-11	
		1-2-P-1-2	1-2-T-1-2	CCM GRM-02	
		1-2-P-1-3	1-2-T-1-3	MTCS 8.4	
		1-2-P-1-4	1-2-T-1-4	CCM GRM-08	
CCC-1-3	Compliance with Cybersecurity Standards, Laws and Regulations	1-3-P-1-1		ISO27K A.18.1.1	ISISO27K A.18.1.1, MTCS 10.1, C5 COM-01, CCM-BCR-11, CCM-AAC-03
			1-3-T-1-1	ISO27K A.18.1.2	
		1-3-P-1-2		ISO27K A.18.1.3	
		1-3-P-1-3		ISO27K A.18.1.4	
		1-3-P-1-4		MTCS 10.4	ISO27K A.18.1.5
		1-3-P-1-5		MTCS 10.5	
			1-3-T-1-2	MTCS 10.6	

CCC-1-4	Cybersecurity Roles and Responsibilities	1-4-P-1-1	1-4-T-1-1	C5-OIS-02, C5 OIS-03	ISO27K - A.6.1.1
		1-4-P-2-1		C5-OIS-05	ISO27K - A.6.1.4
		1-4-P-2-2		ISO27K - A.6.1.3	
CCC-1-5	Cybersecurity in Human Resources	1-5-P-1-1		FR PS-2	
		1-5-P-1-2	1-5-T-1-1	MTCS 7.2	
		1-5-P-1-3		MTCS 7.4	C5 HR-04; ISO27K A.7.1.5; FR PS-8
		1-5-P-1-4		FR PS-6	
		1-5-P-2-1		FR PS-4	
		1-5-P-2-2		MTCS 7.5	CCM HRS-01
CCC-1-6	Change Management	1-6-P-3-1		FR-CM-3	CCM- CCC-05
		1-6-P-3-2		C5- BEI-07, C5-BEI-08, C5-BEI-09	
		1-6-P-3-3		C5- BEI-10	
		1-6-P-3-4	1-6-T-3-1	FR-CM-4	
		1-6-P-3-5		FR-CM-7	
		1-6-P-3-6		CCM- CCC-04	

2 Cybersecurity Defense

Subdomain ID	Subdomain	CSP Control ID	CST Control ID	Standard reference	Other standard references
CCC-2-1	Asset Management	2-1-P-1-1		ISO27K A.8.1.1	
		2-1-P-1-2		ISO27K A.8.1.2	
CCC-2-2	Operations and Service Management Cybersecurity	2-2-P-1		MTCS-19.3	
		2-2-P-3-1		MTCS-19.3	
		2-2-P-3-2	2-2-T-3-1	MTCS-19.1, MTCS-19.2	
		2-2-P-3-3		FR-CM-2	
		2-2-P-3-4		MTCS-19.4	
		2-2-P-3-5		FR PL-8	
CCC-2-3	Cybersecurity Event Logs and Monitoring Management	2-3-P-1-1		MTCS 13.3	
		2-3-P-1-2		MTCS 13.4	
		2-3-P-1-3		C5-RB-15	MTCS 13.2
		2-3-P-1-4		MTCS 13.4	
		2-3-P-1-5		FR- SI-04	
		2-3-P-1-6		MTCS 13.2	
		2-3-P-1-7		C5-RB-16	
		2-3-P-1-8		C5-RB-11	
		2-3-P-1-9		FR AC-17 (1)	
		2-3-P-1-10	2-3-T-1-3	ISO27K A.12.4.3	
CCC-2-4	System Development Security	2-4-P-3-1		FR-SA-03	
		2-4-P-3-2		C5-BEI-01	
		2-4-P-3-3	2-4-T-3-1	ISO27K A.14.1.1	
		2-4-P-3-4	2-4-T-3-2	ISO27K A.14.2.8	
		2-4-P-3-5		FR-SA-05	
		2-4-P-3-6		ISO27K A.14.2.6	

		2-4-P-3-7		MTCS 16.4	
		2-4-P-3-8		CCM-CCC-02	
		2-4-P-3-9		MTCS-16.5	
		2-4-P-3-10		ISO27K A.14.3.1	
CCC-2-5	Cybersecurity Incident and Threat Management		2-5-T-1-1	FR-IR-06	MTCS-11.3
		2-5-P-1-1		MTCS-11.1	FR-IR-08
		2-5-P-1-2		FR-IR-02	
		2-5-P-1-3		FR-IR-09	
		2-5-P-1-4		MTCS-11.4	
		2-5-P-1-5		CCM-SEF-04	
		2-5-P-1-6	2-5-T-1-4	C5-SIM-06	
		2-5-P-1-7	2-5-T-1-2	FR-IR-07	
		2-5-P-1-8	2-5-T-1-3	CCM-SEF-05	
		2-5-P-1-9	2-5-T-1-5	MTCS-11.2	
CCC-2-6	Data and Information Protection	2-6-P-1-1	2-6-T-1-1	CCM-DSI-02	
		2-6-P-1-2	2-6-T-1-2	MTCS-12.10	
		2-6-P-1-3		CCM-DSI-05	
		2-6-P-1-4		MTCS-12.6	
		2-6-P-1-5		Original	
		2-6-P-1-6	2-6-T-1-3	Original	
		2-6-P-1-7		FR SA-09 (5)	
CCC-2-7	Identity and Access Management	2-7-P-1-1		C5-IDM-08	
		2-7-P-1-2	2-7-T-1-1	CCM- IAM-12	
		2-7-P-1-3	2-7-T-1-2	C5- IDM-07	
		2-7-P-1-4	2-7-T-1-3	C5-IDM- 08	
		2-7-P-1-5	2-7-T-1-4	FR IA-2 (1)	
		2-7-P-1-6	2-7-T-1-5	MTCS-23.4	FR-AC-7
		2-7-P-1-7		FR-AC-18	
		2-7-P-1-8		CCM-IAM-07	
		2-7-P-1-9		CCM-DCS-03	
		2-7-P-1-10		C5-IAM-12	
		2-7-P-1-11		FR IA-06	
		2-7-P-1-12		FR AC-08	
		2-7-P-1-13		FR AC-17 (9)	
		2-7-P-1-14		FR IA-05 (2)	
CCC-2-8	Vulnerability Management	2-8-P-1-3		MTCS-24.4	CCM-IVS-05
		2-8-P-1-4	2-8-T-1-1	MTCS-15.1	
		2-8-P-1-5	2-8-T-1-2	C5-RB-20	

CCC-2-9	Information System and Processing Facilities Protection	2-9-P-1-1		FR- SI-01, FR-SC-01	
		2-9-P-1-2		CCM- IVS-02	
		2-9-P-1-3		MTCS-14.9	
		2-9-P-1-4		FR-SC-02	
		2-9-P-1-5		FR-SI-02	CCM-IVS-09
		2-9-P-1-6		FR SC-24, FR-SI-10, FR- SI-11, FR- SI-16	
		2-9-P-1-7		CCM- IVS-04	
		2-9-P-1-8		MTCS-19.5	ISO27K A.17.2.1
		2-9-P-1-9		FR-SC-06	
		2-9-P-1-10		FR SC-03	
		2-9-P-1-11		FR-SI-06	
		2-9-P-1-12		FC- SC-18	CCM-TVM-03
		2-9-P-1-13		FR- SI-7	
		2-9-P-1-14		MTCS-24.1	
		2-9-P-1-15		FR- SC-39	C5-KOS-05
		2-9-P-1-16		FR- SC-6 (for computing systems only)	
		2-9-P-1-17		MTCS-24.6	
		2-9-P-1-18		MTCS-24.5	
CCC-2-10	Networks Security Management	2-10-P-1-1		CCM IVS-13	C5 KOS-06
		2-10-P-1-2		FR SC-07	
		2-10-P-1-3		FR SC-05	
		2-10-P-1-4		FR SC-08	
		2-10-P-1-5		C5 KOS-03	
		2-10-P-1-6		FR SC-06 (communications only)	
		2-10-P-1-7		Original	Original
		2-10-P-1-8		C5-KOS-05	ISO27K A.13.1.3
		2-10-P-1-9		MTCS-24.2	C5-KOS-04
		2-10-P-1-10			FR SI-4 (11) (18) (22)
		2-10-P-1-11		FR- SI-04 (1)	
CCC-2-11	Storage Media Security	2-11-P-3-1		FR-MP-6	
		2-11-P-3-2		MTCS-12.8	CCM-DSI-07
		2-11-P-3-3		ISO27K A.8.3.1	
		2-11-P-3-4		FR-MP-3	

		2-11-P-3-5		FR-MP-4	
		2-11-P-3-6		FR MP-7	
CCC-2-12	Web application security	2-12-P-1-1		ISO27K A.14.1.2, ISO27K A.14.1.3	
CCC-2-13	Mobile Devices Security	2-13-P-1-1		CCM, MOS-09	
		2-13-P-1-2		CCM, MOS-10	
		2-13-P-1-3		CCM, MOS-16	
		2-13-P-1-4		CCM, MOS-19	
		2-13-P-1-5		Original	
		2-13-P-1-6	2-13-T-1-1	Original	
		2-13-P-1-7	2-13-T-1-2	Original	
		2-13-P-1-8		FR SC-15	
		2-13-P-1-9		FR MA-3	
CCC-2-14	Backup and Recovery Management	2-14-P-1-1		FR CP-10 (4)	CCM BCR-11
CCC-2-15	Key Management	2-15-P-3-1	2-15-T-3-1	CCM-EKM-01	
		2-15-P-3-2	2-15-T-3-2	CCM-EKM-04	
		2-15-P-3-3	2-15-T-3-3	Original	
		2-15-P-3-4	2-15-T-3-4	FR SC-12 (1)	
CCC-2-16	Cryptography	2-16-P-1-1	2-16-T-1-1	C5 KRY-02 (Basic requirement only)	MTCS 17.2
		2-16-P-1-2		FR SC-17	
			2-16-T-1-2	FC- SC-28 (1)	
CCC-2-17	Interoperability	2-17-P-3-1	2-17-T-3-1	C5-PI-03	
		2-17-P-3-2	2-17-T-3-2	CCM-IPY-01	C5-PI-01
		2-17-P-3-3	2-17-T-3-3	CCM-IPY-04	
		2-17-P-3-4	2-17-T-3-4	CCM-IPY-02	
		2-17-P-3-5		CCM-IPY-05	
CCC-2-18	Physical Security	2-18-P-1-1		FR-PE-06	
		2-18-P-1-2		FR-PE-08	MTCS-18,4
		2-18-P-1-3		FR-PE-04	
		2-18-P-1-4		FR-PE-05	
		2-18-P-1-5		CCM-DCS-01	
		2-18-P-1-6		FR-PE-12	
		2-18-P-1-7		FR-PE-10	
		2-18-P-1-8		FR-PE-13	
		2-18-P-1-9		C5-PS-03	

		2-18-P-1-10		FR PE-15	
		2-18-P-1-11		C5-PS-04	
		2-18-P-1-12		FR-PE-11 (1)	
		2-18-P-1-13		FR CP-8	
		2-18-P-1-14		CCM BCR-06	
		2-18-P-1-15		CCM BCR-07	C5-PS-05
		2-18-P-1-16		Original	
		2-18-P-1-17		CCM-DCS-01	
		2-18-P-1-18		MTCS-18.2	CCM-DCS-04
		2-18-P-1-19		ISO27K A.11.1.6	
		2-18-P-1-20		CCM-DCS-05	
		2-18-P-1-21		FR-PR 14 (1) (2)	CCM BCR-03
		2-18-P-1-22		FR-PE-09	

3 Cybersecurity Resilience

Subdomain ID	Subdomain	CSP Control ID	CST Control ID	Standard reference	Other standard references
CCC-3-1	Cybersecurity Resilience Aspects of Business Continuity Management (BCM)	3-1-P-1-1	3-1-T-1-1	FR CP-2 (4)	
		3-1-P-1-2		C5 BCM-02	
		3-1-P-1-3	3-1-T-1-2	FR CP-3	
		3-1-P-1-4		FR CP-4	
		3-1-P-1-5		FR CP-7 (1) (2) (3) (4)	
		3-1-P-1-6		FR PE-17	
		3-1-P-1-7		FR CP-6	

4 Third-party Cybersecurity

Subdomain ID	Subdomain	CSP Control ID	CST Control ID	Standard reference	Other standard references
CCC-4-1	Supply Chain & Third-Party Security	4-1-P-1-1		MTCS-9.1, MTCS-9.2 CCM-STA-06, CCM-STA-08, CCM-STA-09	
		4-1-P-1-2		FR-SA-05	
		4-1-P-1-3	4-1-T-1-1	CCM-STA-01	
		4-1-P-1-4		C5-DDL-02	
		4-1-P-1-5		CCM-STA-06	

Table 2: CCC Control Mapping

ECC/CCC Subdomain Mapping

Main Domains	ECC Consolidated Sub-domains		CCC Sub-domains	
Cybersecurity Governance	1-1	Cybersecurity Strategy		
	1-2	Cybersecurity Management		
	1-3	Cybersecurity Policies and Procedures	1-1	Cybersecurity Policies and Procedures
	1-4	Cybersecurity Roles and Responsibilities	1-4	Cybersecurity Roles and Responsibilities
	1-5	Cybersecurity Risk Management	1-2	Cybersecurity Risk Management
	1-6	Cybersecurity in Information Technology Projects		
	1-7	Compliance with Cybersecurity Standards, Laws and Regulations	1-3	Compliance with Cybersecurity Standards, Laws and Regulations
	1-8	Cybersecurity Periodical Assessment and Audit		
	1-9	Cybersecurity in Human Resources	1-5	Cybersecurity in Human Resources
	1-10	Cybersecurity Awareness and Training Program		
			1-6	Change management
Cybersecurity Defense	2-1	Asset Management	2-1	Asset Management
			2-2	Operations and Service Management Cybersecurity
	2-2	Identity and Access Management	2-7	Identity and Access Management
	2-3	Information System and Information Processing Facilities Protection	2-9	Information System and Processing Facilities Protection
	2-4	Email Protection		
	2-5	Network Security Management	2-10	Network Security Management
	2-6	Mobile Device Security	2-13	Mobile Device Security
			2-11	Storage Media Security
	2-7	Data and Information Protection	2-6	Data and Information Protection
			2-4	System Development Security
	2-8	Cryptography	2-16	Cryptography

	2-9	Backup and Recovery Management	2-14	Backup and Recovery Management
	2-10	Vulnerability Management	2-8	Vulnerability Management
	2-11	Penetration Testing		
	2-12	Cybersecurity Event Logs and Monitoring Management	2-3	Cybersecurity Event Logs and Monitoring Management
	2-13	Cybersecurity Incident and Threat Management	2-5	Cybersecurity Incident and Threat Management
	2-14	Physical Security	2-18	Physical Security
	2-15	Web Application Security	2-12	Web Application Security
			2-15	Key Management
			2-17	Interoperability
Cybersecurity Resilience	3-1	Cybersecurity Resilience Aspects of Business Continuity Management (BCM)	3-1	Cybersecurity Resilience Aspects of Business Continuity Management (BCM)
Third-party cybersecurity	4-1	Third-Party Cybersecurity	4-1	Supply Chain & Third-Party Security

Table 3: ECC/CCC Subdomain Mapping

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority