الهيئة الوطنية للأمن السيبـراني
National Cybersecurity Authority

Cloud Cybersecurity Controls
Methodology and Mapping Annex

(CCC - 1 : 2020)

Sharing Notice: White
Document Classification: Open

Disclaimer: The following controls will be governed by and implemented in accordance with the laws of the Kingdom of Saudi Arabia, and must be subject to the exclusive jurisdiction of the courts of the Kingdom of Saudi Arabia. Therefore, the Arabic version will be the binding language for all matters relating to the meaning or interpretation of this document.

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 and Confidential to the 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 orange 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 Restriction

Table of Contents

Design Principles of the CCC 8

Relationship to other International Standards 9

Design Methodology of the CCC 10

Main Domains and Subdomains Structure of the CCC 11

Domain Mapping to International Standards 13

Control Mapping to International Standards 15

Essential Cybersecurity Controls and Cloud Cybersecurity Controls Subdomain Mapping 21

Control Applicability on Different Cloud Service Models (IaaS, PaaS, SaaS) 24

List of the Figures and Illustrations

Figure 1: CCC as a Modular Extension of the ECC 8

Figure 2: International Cloud Computing Standards Distilled to the Consolidated Control List 10

Figure 3: Main Domain and Subdomain Basis of the CCC Cloud Cybersecurity Controls 11

Figure 4: CCC Cloud Cybersecurity Controls Main Domain and Subdomain Stack 12

List of Tables

Table 1: CCC Domain Mapping to International Standards 14

Table 2: CCC Control Mapping 20

Table 3: ECC/CCC Subdomain Mapping 23

Table 4: CSP Controls Applicability on Different Cloud Service Models 31

Table 5: CST Controls Applicability on Different Cloud Service Models 33

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, to provide controls to both CSPs and CSTs. 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.

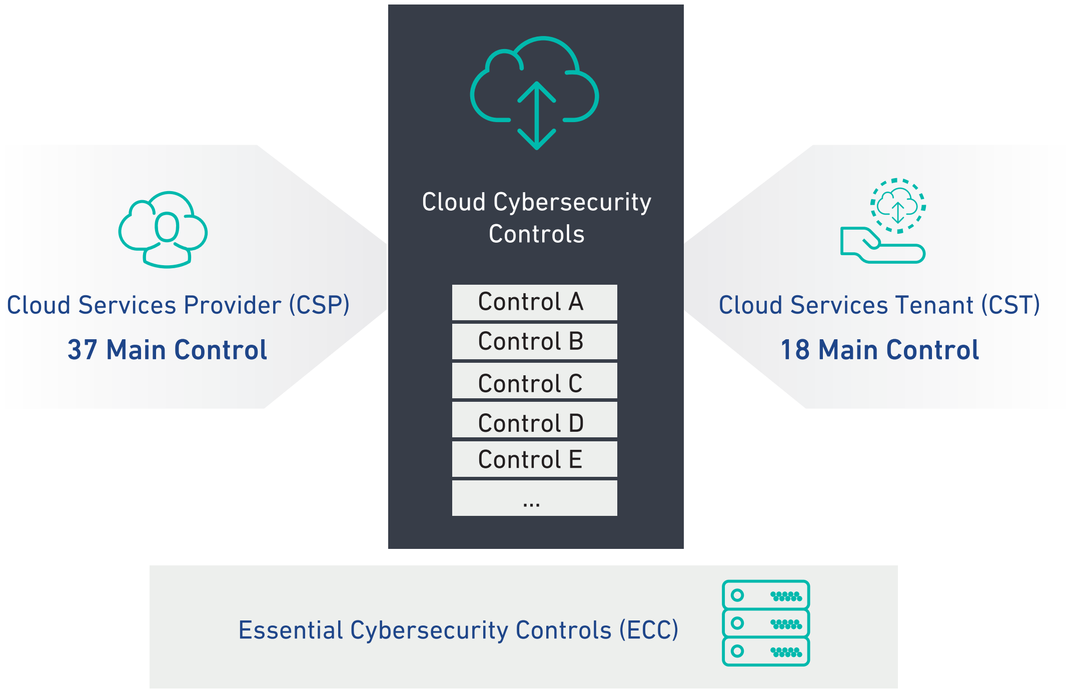

Cloud Services Provider (CSP)
37 Main Control
Cloud Cybersecurity Controls
Control A
Control B
Control C
Control D
Control E
...
Cloud Services Tenant (CST)
18 Main Control
Essential Cybersecurity Controls (ECC)

Figure 1: CCC as a Modular Extension of the ECC

For CSPs, the following principles were applied:

- The security level of the controls in the CCC is additional to the security levels of the ECC.
- High level cybersecurity leveraging other countries' cloud security standards (such as US FedRAMP. Singapore MTCS SS, Germany C5) or industry standards (CCM, ISO27001).
- The control/subcontrol catalogue has a reference to other standards.

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 cloud cybersecurity controls. The five leading standards used were:

- ISO/IEC 27001
- 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 SS) Singapore standard

Design Methodology of the CCC

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

In developing the cloud cybersecurity 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.

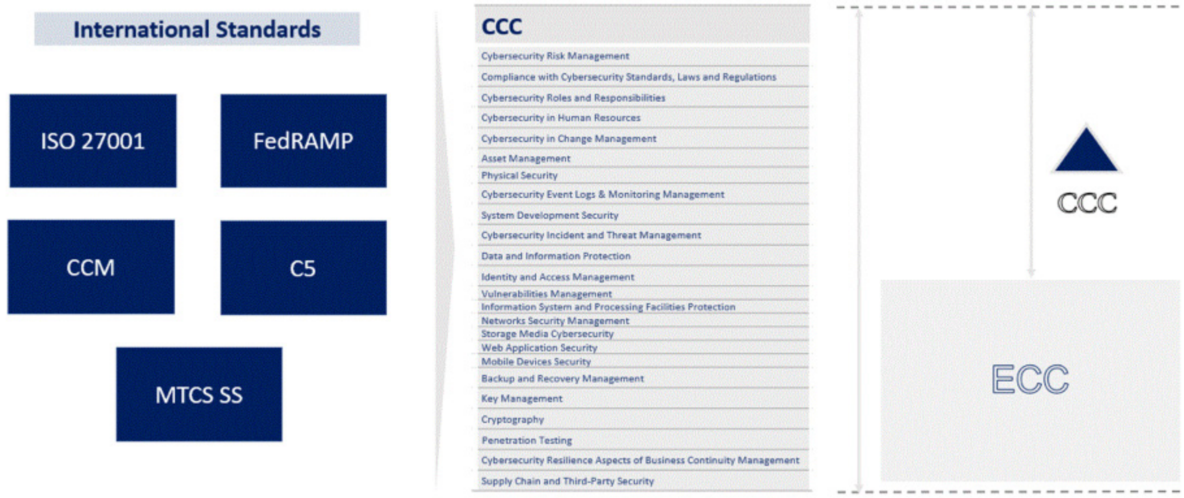
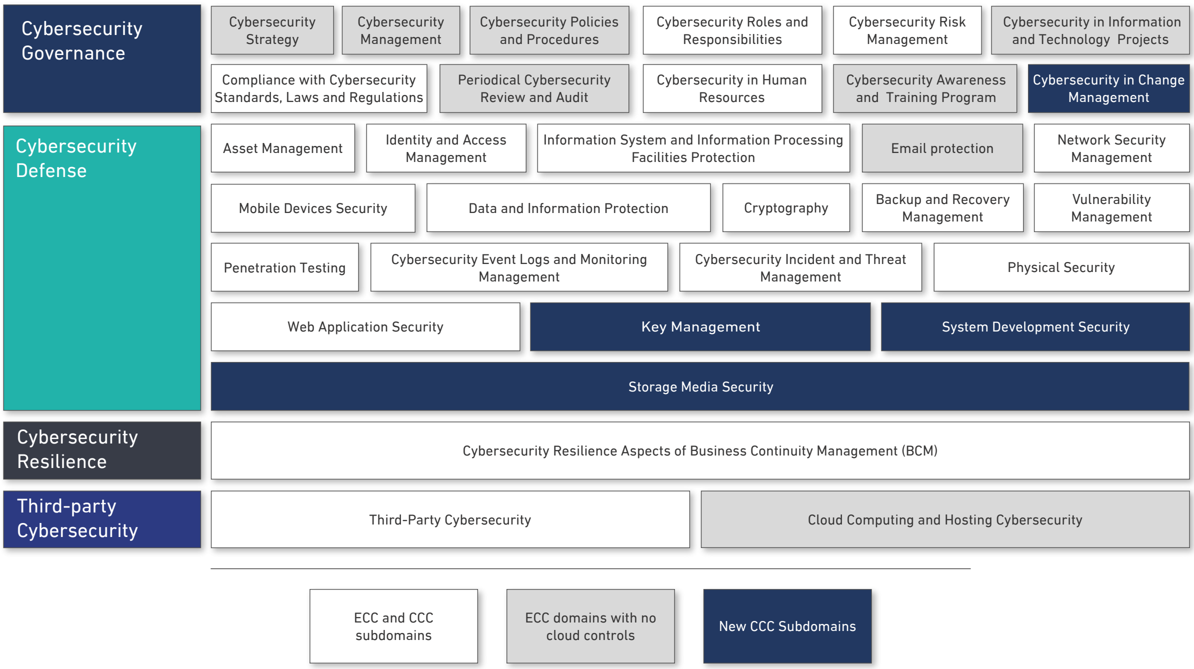

International Standards
ISO 27001
FedRAMP
CCM
C5
MTCS SS
CCC
Cybersecurity Risk Management
Compliance with Cybersecurity Standards, Laws and Regulations
Cybersecurity Roles and Responsibilities
Cybersecurity in Human Resources
Cybersecurity in Change Management
Asset Management
Physical Security
Cybersecurity Event Logs & Monitoring Management
System Development Security
Cybersecurity Incident and Threat Management
Data and Information Protection
Identity and Access Management
Vulnerabilities Management
Information System and Processing Facilities Protection
Networks Security Management
Storage Media Cybersecurity
Web Application Security
Mobile Devices Security
Backup and Recovery Management
Key Management
Cryptography
Penetration Testing
Cybersecurity Resilience Aspects of Business Continuity Management
Supply Chain and Third-Party Security
CCC
ECC

Figure 2: International Cloud Computing Standards Distilled to the Consolidated Control List

Main Domains and Subdomains Structure of the CCC

Relationship to ECC

Main domains and subdomains of the ECC and the cloud cybersecurity controls in the CCC 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). Four 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).



Cybersecurity Governance

Cybersecurity Strategy

Cybersecurity Management

Cybersecurity Policies and Procedures

Cybersecurity Roles and Responsibilities

Cybersecurity Risk Management

Cybersecurity in Information and Technology Projects

Compliance with Cybersecurity Standards, Laws and Regulations

Periodical Cybersecurity Review and Audit

Cybersecurity in Human Resources

Cybersecurity Awareness and Training Program

Cybersecurity in Change Management

Cybersecurity Defense

Asset Management

Identity and Access Management

Information System and Information Processing Facilities Protection

Email protection

Network Security Management

Mobile Devices Security

Data and Information Protection

Cryptography

Backup and Recovery Management

Vulnerability Management

Penetration Testing

Cybersecurity Event Logs and Monitoring Management

Cybersecurity Incident and Threat Management

Physical Security

Web Application Security

Key Management

System Development Security

Storage Media Security

Cybersecurity Resilience

Cybersecurity Resilience Aspects of Business Continuity Management (BCM)

Third-party Cybersecurity

Third-Party Cybersecurity

Cloud Computing and Hosting Cybersecurity

ECC and CCC subdomains

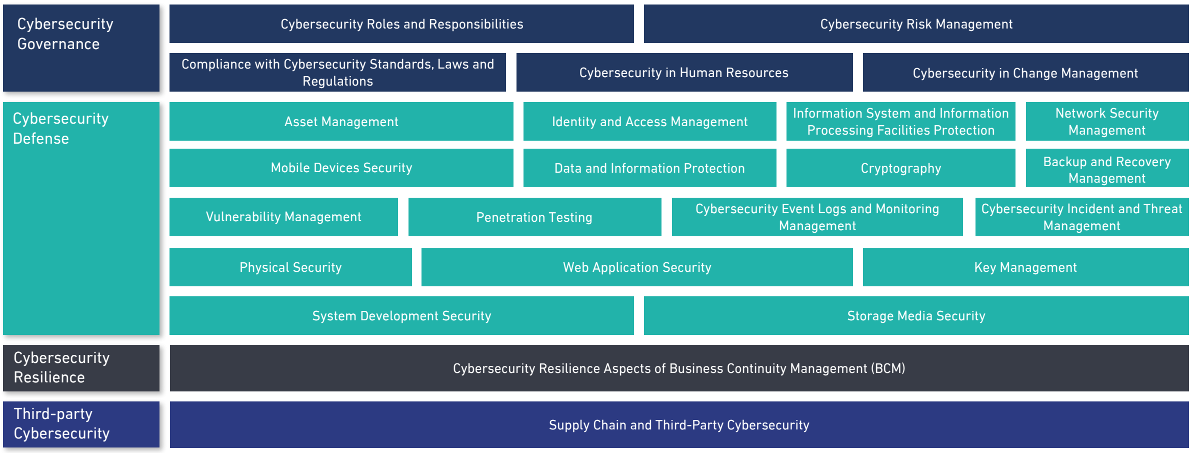
ECC domains with no cloud controls

New CCC Subdomains

Figure 3: Main Domain and Subdomain Basis of the CCC Cloud Cybersecurity Controls

Main Domains and Subdomains Structure of the Cloud Cybersecurity Controls

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



Cybersecurity Governance
Cybersecurity Roles and Responsibilities
Cybersecurity Risk Management
Compliance with Cybersecurity Standards, Laws and Regulations
Cybersecurity in Human Resources
Cybersecurity in Change Management

Cybersecurity Defense
Asset Management
Identity and Access Management
Information System and Information Processing Facilities Protection
Network Security Management
Mobile Devices Security
Data and Information Protection
Cryptography
Backup and Recovery Management
Vulnerability Management
Penetration Testing
Cybersecurity Event Logs and Monitoring Management
Cybersecurity Incident and Threat Management
Physical Security
Web Application Security
Key Management
System Development Security
Storage Media Security

Cybersecurity Resilience
Cybersecurity Resilience Aspects of Business Continuity Management (BCM)

Third-party Cybersecurity
Supply Chain and Third-Party Cybersecurity

Figure 4: CCC Cloud Cybersecurity Controls Main Domain and Subdomain Stack

Domain Mapping to International Standards

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

Main Domains	CCC		Standard Domain Comparison				
	Domains		ISO 27001	FedRAMP (FR)	CCM	C5	MTCS SS
Cybersecurity Governance	1-1	Cybersecurity Roles and Responsibilities	A.6.1	AU		1 - OIS	
	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 in Human Resources	A.7	PS	HRS	3 - HR	7
				AT			
	1-5	Cybersecurity in Change Management	A.12			6 - RB	19
Cybersecurity Defense	2-1	Asset Management	A.8.1	CM		4 - AM	20
				MA			14
	2-2	Identity and Access Management	A.9	AC	IAM		23
				IA		7 - IDM	
	2-3	Information System and Information Processing Facilities Protection		SC	AIS		22
				SI	IVS		4
	2-4	Networks Security Management	A.13	SC		9 - KOS	
	2-5	Mobile Devices Security	A.6.2		MOS	17 - MDM	
	2-6	Data and Information Protection	A.8.2		DSI		12
	2-7	Cryptography	A.10		EKM	8 - KRY	17
	2-8	Backup and Recovery Management					
	2-9	Vulnerabilities Management			TVM		
	2-10	Penetration Testing		CA		18 - RB	15
	2-11	Cybersecurity Event Logs and Monitoring Management	A.12.4	AU			13
				CA		15 - SPN	15
	2-12	Cybersecurity Incident and Threat Management	A.16	IR	SEF	13 - SIM	11
	2-13	Physical Security	A.11	PE	DCS	5 - PS	18
	2-14	Web Application Security					
	2-15	Key Management	A.10		EKM	8 - KRY	17
	2-16	System Development Security	A.14	SA		11- BEI	16
	2-17	Storage Media Security	A.8.3	MP			

Main Domains	CCC Domains		Standard Domain Comparison				
			ISO 27001	FedRAMP (FR)	CCM	C5	MTCS SS
Cybersecurity Resilience	3-1	Cybersecurity Resilience Aspects of Business Continuity Management (BCM)	A.17	CP	BCR	14 - BCM	21
Third-party Cybersecurity	4-1	Supply Chain and Third-Party Security	A.15	SA	SCM	12 - DLL	9

Table 1: CCC Domain Mapping to International Standards

Control Mapping to International Standards

In case of a discrepancy between the cloud cybersecurity controls in the CCC and the five international standards referenced, the CCC controls shall take precedence.

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

1 Cybersecurity Governance

Subdomain ID	Subdomain	CSP Control ID	CST Control ID	Standard reference	Other standard references
1-1	Cybersecurity Roles and Responsibilities	1-1-P-1-1	1-1-T-1-1	C5-OIS-02, C5-OIS-03	ISO27001 - A.6.1.1
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 SS 8.4	
1-3	Compliance with Cybersecurity Standards, Laws and Regulations	1-3-P-1-1		ISO27001 A.18.1.1	MTCS SS 10.1, C5 COM-01, CCM-BCR-11, CCM-AAC-03
			1-3-T-1-1	MTCS SS 10.6	
1-4	Cybersecurity in Human Resources	1-4-P-1-1		original	
		1-4-P-1-2	1-4-T-1-1	MTCS SS 7.2	
		1-4-P-1-3		FR PS-6	
		1-4-P-2-1		MTCS SS 7.5	CCM HRS-01
1-5	Cybersecurity in Change Management	1-5-P-3-1		FR-CM-3	CCM- CCC-05
		1-5-P-3-2		C5- BEI-10	

2 Cybersecurity Defense

Subdomain ID	Subdomain	CSP Control ID	CST Control ID	Standard reference	Other standard references
2-1	Asset Management	2-1-P-1-1	2-1-T-1-1	ISO27001 A.8.1.1	
		2-1-P-1-2		ISO27001 A.8.1.2	
2-2	Identity and Access Management	2-2-P-1-1		C5-IDM-08	
			2-2-T-1-1	CCM- IAM-12	
			2-2-T-1-2	C5-IDM-07	
		2-2-P-1-2	2-2-T-1-3	C5-IDM- 08	
		2-2-P-1-3	2-2-T-1-4	FR IA-2 (1)	
		2-2-P-1-4	2-2-T-1-5	MTCS SS-23.4	FR-AC-7
		2-2-P-1-5		C5-IDM-11	FR-IA-5 (1)
		2-2-P-1-6		CCM-IAM-07	
		2-2-P-1-7		C5-IAM-12	
		2-2-P-1-8		FR IA-06	
		2-2-P-1-9		C5-IDM-03	
		2-2-P-1-10		FR AC-17 (9)	
		2-2-P-1-11		FR IA-2 (1)	
		2-2-P-1-12		MTCS SS-24.5	
2-3	Information System and Information Processing Facilities Protection	2-3-P-1-1		MTCS SS-14.9	
		2-3-P-1-2		MTCS SS-24.6	
		2-3-P-1-3		FR-CM-7	
		2-3-P-1-4		FR SC-24, FR- SI-10, FR- SI-11, FR-SI-16	
		2-3-P-1-5		FR SC-03	
		2-3-P-1-6		original	
		2-3-P-1-7		FR- SI-7	
		2-3-P-1-8		MTCS SS-24.1	
		2-3-P-1-9	2-3-T-1-1	original	
		2-3-P-1-10		original	
		2-3-P-1-11		original	
		2-3-P-1-12		original	

Subdomain ID	Subdomain	CSP Control ID	CST Control ID	Standard reference	Other standard references
2-4	Networks Security Management	2-4-P-1-1		FR SI-4 (11) (18) (22)	
		2-4-P-1-2		FR SC-07	
		2-4-P-1-3		FR SC-05	
		2-4-P-1-4		FR SC-08 (1)	
		2-4-P-1-5		C5 KOS-03	
		2-4-P-1-6		MTCS SS-24.2	C5-KOS-04
			2-4-T-1-1	FR SC-08	
2-5	Mobile Devices Security	2-5-P-1-1		CCM, MOS-09	
		2-5-P-1-2		CCM, MOS-10	
		2-5-P-1-3		CCM, MOS-16	
		2-5-P-1-4	2-5-T-1-1	original	
2-6	Data and Information Protection	2-6-P-1-1		CCM-DSI-05	
		2-6-P-1-2		MTCS SS-12.6	
		2-6-P-1-3		MTCS SS-12.6	
		2-6-P-1-4	2-6-T-1-1	ISO27001 A.18.1.4	
		2-6-P-1-5	2-6-T-1-2	C5-PI-03	
2-7	Cryptography	2-7-P-1-1	2-7-T-1-1	original	
		2-7-P-1-2		FR SC-17	
			2-7-T-1-2	FR- SC-28 (1)	
2-8	Backup and Recovery Management	2-8-P-1-1		FR CP-10 (4)	CCM BCR-11
		2-8-P-1-2		FR CP-10 (4)	CCM BCR-11
2-9	Vulnerabilities Management	2-9-P-1-1	2-9-T-1-1	MTCS SS-24.4	CCM-IVS-05, MTCS SS-15.1
		2-9-P-1-2	2-9-T-1-2	C5-RB-20	
2-10	Penetration Testing	2-10-P-1-1		FR-CA-08	
2-11	Cybersecurity Event Logs and Monitoring Management	2-11-P-1-1		MTCS SS 13.3	MTCS SS 13.4
		2-11-P-1-2	2-11-T-1-1	ISO27001 A.12.4.3	
		2-11-P-1-3		C5-RB-15	
		2-11-P-1-4		ISO27001 A.18.1.3	
		2-11-P-1-5		FR- SI-04	MTCS SS 13.2

Subdomain ID	Subdomain	CSP Control ID	CST Control ID	Standard reference	Other standard references
		2-11-P-1-6	2-11-T-1-2	MTCS SS 13.2	
		2-11-P-1-7		FR AC-17 (1)	
		2-11-P-1-8		C5-RB-11	
2-12	Cybersecurity Incident and Threat Management	2-12-P-1-1		C5-OIS-05	ISO27001 - A.6.1.4
		2-12-P-1-2		FR-IR-02	
		2-12-P-1-3		MTCS SS-11.2	
		2-12-P-1-4		MTCS SS-11.4	
		2-12-P-1-5		CCM-SEF-04	
		2-12-P-1-6		MTCS SS-11.3	
		2-12-P-1-7		FR-IR-07	
		2-12-P-1-8		CCM-SEF-05	
2-13	Physical Security	2-13-P-1-1		FR-PE-06	
		2-13-P-1-2		FR-PE-05	
		2-13-P-1-3		CCM-DCS-05	
2-14	Web Application Security	2-14-P-1-1		ISO27001 A.14.1.2, ISO27001 A.14.1.3	
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; FR SC-12 (1)	
		2-15-P-3-3		ISO27001 A.12.4.3	
2-16	System Development Security	2-16-P-3-1		ISO27001 A.14.1.1	
		2-16-P-3-2		ISO27001 A.14.2.6	
2-17	Storage Media Security	2-17-P-3-1		FR-MP-6	
		2-17-P-3-2		MTCS SS-12.8	CCM-DSI-07
		2-17-P-3-3		ISO27001 A.8.3.1	
		2-17-P-3-4		FR-MP-3	
		2-17-P-3-5		FR-MP-4	
		2-17-P-3-6		FR MP-7	

3 Cybersecurity Resilience

Subdomain ID	Subdomain	CSP Control ID	CST Control ID	Standard reference	Other standard references
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	

4 Third party Cybersecurity

Subdomain ID	Subdomain	CSP Control ID	CST Control ID	Standard reference	Other standard references
4-1	Supply Chain & Third-Party Security	4-1-P-1-1		original	
		4-1-P-1-2		FR-SA-05	
		4-1-P-1-3		MTCS SS 10.5	
		4-1-P-1-4		CCM-STA-06	

Table 2: CCC Control Mapping

Essential Cybersecurity Controls and Cloud Cybersecurity Controls Subdomain Mapping

Main Domains	ECC Consolidated Subdomains		Cloud Cybersecurity Controls Subdomains	
Cybersecurity Governance	1-1	Cybersecurity Strategy		
	1-2	Cybersecurity Management		
	1-3	Cybersecurity Policies and Procedures		
	1-4	Cybersecurity Roles and Responsibilities	1-1	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	Periodical Cybersecurity Review and Audit		
	1-9	Cybersecurity in Human Resources	1-4	Cybersecurity in Human Resources
	1-10	Cybersecurity Awareness and Training Program		
			1-5	Cybersecurity in Change Management

Main Domains	ECC Consolidated Subdomains		Cloud Cybersecurity Controls Subdomains	
Cybersecurity Defense	2-1	Asset Management	2-1	Asset Management
	2-2	Identity and Access Management	2-2	Identity and Access Management
	2-3	Information System and Information Processing Facilities Protection	2-3	Information System and Information Processing Facilities Protection
	2-4	Email Protection		
	2-5	Network Security Management	2-4	Network Security Management
	2-6	Mobile Device Security	2-5	Mobile Device Security
	2-7	Data and Information Protection	2-6	Data and Information Protection
	2-8	Cryptography	2-7	Cryptography
	2-9	Backup and Recovery Management	2-8	Backup and Recovery Management
	2-10	Vulnerabilities Management	2-9	Vulnerabilities Management
	2-11	Penetration Testing	2-10	Penetration Testing
	2-12	Cybersecurity Event Logs and Monitoring Management	2-11	Cybersecurity Event Logs and Monitoring Management
	2-13	Cybersecurity Incident and Threat Management	2-12	Cybersecurity Incident and Threat Management
	2-14	Physical Security	2-13	Physical Security
	2-15	Web Application Security	2-14	Web Application Security
			2-15	Key Management
			2-16	System Development Security
			2-17	Storage Media Security

Main Domains	ECC Consolidated Subdomains		Cloud Cybersecurity Controls Subdomains	
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	4-2	Third-Party Cybersecurity	4-1	Supply Chain and Third-Party Security

Table 3: ECC/CCC Subdomain Mapping

Control Applicability on different Cloud Service Models (IaaS, PaaS, SaaS)

This section shows a sample of the applicability of the CCC controls (for both the CSP and the CST) on different cloud service models (Software as a Service “SaaS”, Platform as a Service “PaaS”, Infrastructure as a service “IaaS”). The applicability of each control may differ from what is shown in this section as it depends on the type of the service and the relationship between CSP and CST.

for Cloud Service Provider (CSP):

Table 4 below shows the applicability of the CSP controls on different cloud service models (SaaS, PaaS, and IaaS).

Please note the following:

- **X** : means the control may not be applicable
- ✔ : means the control maybe applicable
- Resources: means the control may be applicable on the CSP especially on the CSP’s own resources
- Cloud Technology Stack: means the control may be applicable on the CSP especially on the CSP’s own cloud technology stack
- System development: means the control may be applicable on the CSP especially on the CSP’s own system development
- Physical Security: means the control may be applicable on the CSP especially on the CSP’s own physical security
- Business Continuity Management: means the control may be applicable on the CSP especially on the CSP’s own business continuity management
- Offerings: means the control may be applicable on the CSP especially on the CSP’s offerings

Main Control	Sub Control	IaaS	PaaS	SaaS
1-1-P-1				
	1-1-P-1-1	✓	✓	✓
1-2-P-1				
	1-2-P-1-1	✓	✓	✓
	1-2-P-1-2	✓	✓	✓
	1-2-P-1-3	✓	✓	✓
1-3-P-1				
	1-3-P-1-1	✓	✓	✓
1-4-P-1				
	1-4-P-1-1	✓	✓	✓
	1-4-P-1-2	✓	✓ (Resources and cloud technology stack)	✓ (Resources and cloud technology stack)
	1-4-P-1-3	✓	✓ (Resources and cloud technology stack)	✓ (Resources and cloud technology stack)
1-4-P-2				
	1-4-P-2-1	✓ (Resources and cloud technology stack)	✓ (Resources and cloud technology stack)	✓ (Resources and cloud technology stack)
1-5-P-1		✓	✓	✓
1-5-P-2		✓	✓	✓
1-5-P-3				
	1-5-P-3-1	✓ (Resources and cloud technology stack)	✓ (Resources and cloud technology stack)	✓ (Resources and cloud technology stack)
	1-5-P-3-2	✓ (Resources and cloud technology stack)	✓ (Resources and cloud technology stack)	✓ (Resources and cloud technology stack)
1-5-P-4		✓	✓	✓
2-1-P-1				
	2-1-P-1-1	✓ (Resources and cloud technology stack)	✓ (Resources and cloud technology stack)	✓ (Resources and cloud technology stack)
	2-1-P-1-2	✓ (Resources and cloud technology stack)	✓ (Resources and cloud technology stack)	✓ (Resources and cloud technology stack)
2-2-P-1				

Main Control	Sub Control	IaaS	PaaS	SaaS
	2-2-P-1-1	✓ (Offerings and cloud technology stack)	✓ (Offerings and cloud technology stack)	✓ (Offerings and cloud technology stack)
	2-2-P-1-2	✓ (Offerings and cloud technology stack)	✓ (Offerings and cloud technology stack)	✓ (Offerings and cloud technology stack)
	2-2-P-1-3	✓ (Offerings and cloud technology stack)	✓ (Offerings and cloud technology stack)	✓ (Offerings and cloud technology stack)
	2-2-P-1-4	✓ (Offerings and cloud technology stack)	✓ (Offerings and cloud technology stack)	✓ (Offerings and cloud technology stack)
	2-2-P-1-5	✓ (Offerings and cloud technology stack)	✓ (Offerings and cloud technology stack)	✓ (Offerings and cloud technology stack)
	2-2-P-1-6	✓ (Offerings and cloud technology stack)	✓ (Offerings and cloud technology stack)	✓ (Offerings and cloud technology stack)
	2-2-P-1-7	✓ (Offerings and cloud technology stack)	✓ (Offerings and cloud technology stack)	✓ (Offerings and cloud technology stack)
	2-2-P-1-8	✓ (Offerings and cloud technology stack)	✓ (Offerings and cloud technology stack)	✓ (Offerings and cloud technology stack)
	2-2-P-1-9	✓ (Offerings and cloud technology stack)	✓ (Offerings and cloud technology stack)	✓ (Offerings and cloud technology stack)
	2-2-P-1-10	✓ (Offerings and cloud technology stack)	✓ (Offerings and cloud technology stack)	✓ (Offerings and cloud technology stack)
	2-2-P-1-11	✓ (Offerings and cloud technology stack)	✓ (Offerings and cloud technology stack)	✓ (Offerings and cloud technology stack)
	2-2-P-1-12	✓ (Offerings and cloud technology stack)	✓ (Offerings and cloud technology stack)	✓ (Offerings and cloud technology stack)
2-3-P-1				
	2-3-P-1-1	✓ (Cloud technology stack)	✓ (Cloud technology stack)	✓ (Cloud technology stack)

Main Control	Sub Control	IaaS	PaaS	SaaS
	2-3-P-1-2	✓ (Cloud technology stack)	✓ (Cloud technology stack)	✓ (Cloud technology stack)
	2-3-P-1-3	✓ (Cloud technology stack)	✓ (Cloud technology stack)	✓ (Cloud technology stack)
	2-3-P-1-4	✓ (Cloud technology stack)	✓ (Cloud technology stack)	✓ (Cloud technology stack)
	2-3-P-1-5	✓ (Cloud technology stack)	✓ (Cloud technology stack)	✓ (Cloud technology stack)
	2-3-P-1-6	✓	✓	✓
	2-3-P-1-7	✓ (Cloud technology stack)	✓ (Cloud technology stack)	✓ (Cloud technology stack)
	2-3-P-1-8	✓ (Cloud technology stack)	X	X
	2-3-P-1-9	✓	✓	✓
	2-3-P-1-10	✓	✓	✓
	2-3-P-1-11	✓	✓	✓
	2-3-P-1-12	✓	✓	✓
2-4-P-1				
	2-4-P-1-1	✓ (Cloud technology stack)	✓ (Cloud technology stack)	✓ (Cloud technology stack)
	2-4-P-1-2	✓ (Cloud technology stack)	✓ (Cloud technology stack)	✓ (Cloud technology stack)
	2-4-P-1-3	✓ (Cloud technology stack)	✓ (Cloud technology stack)	✓ (Cloud technology stack)
	2-4-P-1-4	✓ (Cloud technology stack)	✓ (Cloud technology stack)	✓ (Cloud technology stack)
	2-4-P-1-5	✓ (Cloud technology stack)	✓ (Cloud technology stack)	✓ (Cloud technology stack)

Main Control	Sub Control	IaaS	PaaS	SaaS
	2-4-P-1-6	✓ (Cloud technology stack)	✓ (Cloud technology stack)	✓ (Cloud technology stack)
2-5-P-1				
	2-5-P-1-1	✓ (Cloud technology stack)	✓ (Cloud technology stack)	✓ (Cloud technology stack)
	2-5-P-1-2	✓ (Cloud technology stack)	✓ (Cloud technology stack)	✓ (Cloud technology stack)
	2-5-P-1-3	✓ (Cloud technology stack)	✓ (Cloud technology stack)	✓ (Cloud technology stack)
	2-5-P-1-4	✓ (Cloud technology stack)	✓ (Cloud technology stack)	✓ (Cloud technology stack)
2-6-P-1				
	2-6-P-1-1	✓ (Cloud technology stack)	✓ (Cloud technology stack)	✓ (Cloud technology stack)
	2-6-P-1-2	✓	✓ (Cloud technology stack)	✓ (Cloud technology stack)
	2-6-P-1-3	✓	✓	✓
	2-6-P-1-4	✓	✓	✓
	2-6-P-1-5	✓	✓	✓
2-7-P-1				
	2-7-P-1-1	✓ (Cloud technology stack)	✓ (Cloud technology stack)	✓ (Cloud technology stack)
	2-7-P-1-2	✓ (Cloud technology stack)	✓ (Cloud technology stack)	✓ (Cloud technology stack)
2-8-P-1				
	2-8-P-1-1	X	✓ (Cloud technology stack)	✓ (Cloud technology stack)
	2-8-P-1-2	✓ (Cloud technology stack)	✓ (Cloud technology stack)	✓ (Cloud technology stack)

Main Control	Sub Control	IaaS	PaaS	SaaS
2-9-P-1				
	2-9-P-1-1	✓ (Cloud technology stack)	✓ (Cloud technology stack)	✓ (Cloud technology stack)
	2-9-P-1-2	✓ (Cloud technology stack)	✓ (Cloud technology stack)	✓ (Cloud technology stack)
2-10-P-1				
	2-10-P-1-1	✓ (Cloud technology stack)	✓ (Cloud technology stack)	✓ (Cloud technology stack)
2-11-P-1				
	2-11-P-1-1	✓ (Resources and cloud technology stack)	✓ (Resources and cloud technology stack)	✓ (Resources and cloud technology stack)
	2-11-P-1-2	✓ (Resources and cloud technology stack)	✓ (Resources and cloud technology stack)	✓ (Resources and cloud technology stack)
	2-11-P-1-3	✓ (Resources and cloud technology stack)	✓ (Resources and cloud technology stack)	✓ (Resources and cloud technology stack)
	2-11-P-1-4	✓ (Resources and cloud technology stack)	✓ (Resources and cloud technology stack)	✓ (Resources, cloud technology stack, and CST related data managed by CSP)
	2-11-P-1-5	✓ (Resources and cloud technology stack)	✓ (Resources and cloud technology stack)	✓ (Resources and cloud technology stack)
	2-11-P-1-6	✓ (Resources and cloud technology stack)	✓ (Resources and cloud technology stack)	✓ (Resources and cloud technology stack)
	2-11-P-1-7	✓ (Resources and cloud technology stack)	✓ (Resources and cloud technology stack)	✓ (Resources and cloud technology stack)
	2-11-P-1-8	✓ (Resources and cloud technology stack)	✓ (Resources and cloud technology stack)	✓ (Resources and cloud technology stack)
2-12-P-1				
	2-12-P-1-1	✓	✓	✓

Main Control	Sub Control	IaaS	PaaS	SaaS
	2-12-P-1-2	✓	✓	✓
	2-12-P-1-3	✓	✓	✓
	2-12-P-1-4	✓	✓	✓
	2-12-P-1-5	✓	✓	✓
	2-12-P-1-6	✓	✓	✓
	2-12-P-1-7	✓	✓	✓
	2-12-P-1-8	✓	✓	✓
2-13-P-1				
	2-13-P-1-1	✓ (Physical Security)	✓ (Physical Security)	✓ (Physical Security)
	2-13-P-1-2	✓ (Physical Security)	✓ (Physical Security)	✓ (Physical Security)
	2-13-P-1-3	✓ (Physical Security)	✓ (Physical Security)	✓ (Physical Security)
2-14-P-1				
	2-14-P-1-1	✓ (Cloud technology stack)	✓ (Cloud technology stack)	✓ (Cloud technology stack)
2-15-P-1		✓	✓	✓
2-15-P-2		✓	✓	✓
2-15-P-3				
	2-15-P-3-1	✓ (Cloud technology stack)	✓ (Cloud technology stack)	✓ (Cloud technology stack)
	2-15-P-3-2	✓ (Cloud technology stack)	✓ (Cloud technology stack)	✓ (Cloud technology stack)
	2-15-P-3-3	✓ (Cloud technology stack)	✓ (Cloud technology stack)	✓ (Cloud technology stack)
2-15-P-4		✓	✓	✓
2-16-P-1		✓	✓	✓
2-16-P-2		✓	✓	✓
2-16-P-3				
	2-16-P-3-1	✓ (System development and cloud technology stack)	✓ (System development and cloud technology stack)	✓ (System development and cloud technology stack)
	2-16-P-3-2	✓ (System development and cloud technology stack)	✓ (System development and cloud technology stack)	✓ (System development and cloud technology stack)
2-16-P-4		✓	✓	✓

Main Control	Sub Control	IaaS	PaaS	SaaS
2-17-P-1		✓	✓	✓
2-17-P-2		✓	✓	✓
2-17-P-3				
	2-17-P-3-1	✓ (Cloud technology stack)	✓ (Cloud technology stack)	✓ (Cloud technology stack)
	2-17-P-3-2	✓ (Cloud technology stack)	✓ (Cloud technology stack)	✓ (Cloud technology stack)
	2-17-P-3-3	✓	✓	✓
	2-17-P-3-4	✓ (Cloud technology stack)	✓ (Cloud technology stack)	✓ (Cloud technology stack)
	2-17-P-3-5	✓ (Cloud technology stack)	✓ (Cloud technology stack)	✓ (Cloud technology stack)
	2-17-P-3-6	✓ (Cloud technology stack)	✓ (Cloud technology stack)	✓ (Cloud technology stack)
3-1-P-1		✓	✓	✓
	3-1-P-1-1	✓ (Cloud technology stack and business continuity management)	✓ (Cloud technology stack and business continuity management)	✓ (Cloud technology stack and business continuity management)
	3-1-P-1-2	✓ (Cloud technology stack and business continuity management)	✓ (Cloud technology stack and business continuity management)	✓ (Cloud technology stack and business continuity management)
4-1-P-1				
	4-1-P-1-1	✓	✓	✓
	4-1-P-1-2	✓	✓	✓
	4-1-P-1-3	✓	✓	✓
	4-1-P-1-4	✓	✓	✓

Table 4: CSP Controls Applicability on Different Cloud Service Models

for Cloud Service Tenant (CST):

Table 5 below shows applicability of the CST controls on different cloud service models (SaaS, PaaS, and IaaS).

Please note the following:

- **X** : means the control may not be applicable
- ✓ : means the control maybe applicable
- Cryptographic keys: means the control may be applicable on the CST especially on the CST's own cryptographic keys

Main Control	Sub Control	IaaS	PaaS	SaaS
1-1-T-1				
	1-1-T-1-1	✓	✓	✓
1-2-T-1				
	1-2-T-1-1	✓	✓	✓
	1-2-T-1-2	✓	✓	✓
	1-2-T-1-3	✓	✓	✓
1-3-T-1				
	1-3-T-1-1	✓	✓	✓
1-4-T-1				
	1-4-T-1-1	✓	✓	✓
2-1-T-1				
	2-1-T-1-1	✓	✓	✓
2-2-T-1				
	2-2-T-1-1	✓	✓	✓
	2-2-T-1-2	✓	✓	✓
	2-2-T-1-3	✓	✓	✓
	2-2-T-1-4	✓	✓	✓
	2-2-T-1-5	✓	✓	✓
2-3-T-1				
	2-3-T-1-1	✓	✓	✓
2-4-T-1				
	2-4-T-1-1	✓	✓	✓
2-5-T-1				
	2-5-T-1-1	✓	✓	✓
2-6-T-1				
	2-6-T-1-1	✓	✓	✓
	2-6-T-1-2	✓	✓	✓

Main Control	Sub Control	IaaS	PaaS	SaaS
2-7-T-1				
	2-7-T-1-1	✓	✓	X
	2-7-T-1-2	✓	✓	✓
2-9-T-1				
	2-9-T-1-1	✓	✓	X
	2-9-T-1-2	✓	✓	X
2-11-T-1				
	2-11-T-1-1	✓	✓	✓
	2-11-T-1-2	✓	✓	✓
2-15-T-1		✓	✓	✓
2-15-T-2		✓	✓	✓
2-15-T-3				
	2-15-T-3-1	✓ (Cryptographic keys)	✓ (Cryptographic keys)	✓ (Cryptographic keys)
	2-15-T-3-2	✓ (Cryptographic keys)	✓ (Cryptographic keys)	✓ (Cryptographic keys)
2-15-T-4		✓	✓	✓
3-1-T-1				
	3-1-T-1-1	✓	✓	✓

Table 5: CST Controls Applicability on Different Cloud Service Models

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority