الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

Cloud Cybersecurity Controls

(CCC – 1 : 2020)

Draft

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):

A TLP was created for sharing the maximum amount of sensitive information, and it is widely used worldwide. There are four colors (traffic lights).

🔴 Red – Personal and Confidential to the Recipient only

The recipient is not allowed to share red-classified materials with any person, from within or outside the institution, beyond the scope specified for receipt.

🟠 Orange – Limited Sharing

The recipient of orange-classified materials may share the information contained therein with concerned personnel only in the same institution, and with those competent to take procedures with regard to the information.

🟢 Green – Sharing within the Same Community

Green-classified materials may be shared with others within the same institution or in other institutions that have relations with your institution or are operating in the same sector. However, such materials may not be shared or exchanged through public channels.

⚪ White – Unlimited

Table of Contents

Table of Figures

List of Tables

1. Executive Summary

NCA's mandates and duties fulfill the strategic and regulatory cybersecurity needs related to the development of cybersecurity national policies, governance mechanisms, frameworks, standards, controls and guidelines.

They also fulfill the need to continuously monitor the compliance of organizations to support the important role of cybersecurity which has increased with the rise of security risks in cyberspace more than any time before.

The cloud services subject is trending globally, and improves in a very fast pace in line with the trendy updates and the 4th industrial revolution transformations, which comes as a result of the reliance on the massive and supreme capabilities of the Cloud Service Providers (CSPs) to provide fast and affordable services (e.g., storage, databases, web software) and backup copies resistant to external impact factors, to both individuals and public organizations. For that, there is a current and pressing need to have cybersecurity controls to deal with cloud services that are considered as an extension to the already published Essential Cybersecurity Controls (ECC-1: 2018) and international common practices in this field.

The Cloud Cybersecurity Controls (CCC – 1: 2020) aim at minimizing the cybersecurity risks of Cloud Service Tenants (CSTs), also known as Cloud Customer, and Cloud Service Providers (CSPs).

This document highlights the details of the Cloud Cybersecurity Controls and cybersecurity obligations for cloud services, objectives, scope, statement of applicability, compliance approach and monitoring.

All CSPs and CSTs shall implement all necessary measures to ensure continuous compliance with the CCC as per Paragraph III of Article 10 of NCA's mandate and as per the Royal Decree number 57231, dated 10/11/1439AH.

2. Introduction

The National Cybersecurity Authority (Hereinafter referred to as the "Authority – NCA") developed the Cloud Cybersecurity Controls (CCC – 1: 2020) after conducting a comprehensive study of multiple national and international cybersecurity frameworks, standards and controls, and reviewing common industry practices and experiences in the field of cybersecurity. A mapping study is conducted with international cloud computing standards such as US FedRAMP, Singapore MTCS, Germany C5, Cloud Controls Matrix (CCM) and ISO/IEC 27000-series. This mapping is represented in a separate document extended to the CCC to make the compliance and mapping of the CCC controls easier for CSPs national and international companies and the CSTs. The CCC standard is constituted by the following elements:

For CSPs	For CSTs
4 Main Domains	
26 Subdomains	
46 Controls	33 Controls
189 Subcontrols	47 Subcontrols

Figure 1: Cloud Cybersecurity Control components

3. Objectives

As an extension to the ECC, the CCC objective is to define cybersecurity controls and obligations for cloud computing services, from the point of view of both the provider (CSP) and the consumer (CST). These requirements are based on industry leading practices which will help to minimize the cybersecurity risks that originate from internal and external threats. The cybersecurity of cloud computing services, for both CSPs and CSTs, must be able to protect the confidentiality, integrity and availability of the data and information within the cloud environment. To that aim, CCC shall address three of the four foundations upon which cybersecurity is based, namely:

- People;
- Processes; and
- Technology
- Strategy, is not specific to cloud and, as therefore it is already covered in the ECC.

4. Scope of Work and Applicability

Scope of Work of the CCC

The cybersecurity obligations and controls shall apply to the CSPs and CSTs.

CSTs within the scope of CCC are any organization (as defined in annex (A)) that currently use or planning to use any cloud service from CSPs.

CSPs within the scope of CCC are any CSP inside or outside KSA which provides cloud computing services to the CSTs withing the scope of work.

The NCA strongly encourages all other CSPs in the Kingdom to leverage these controls to implement best practices to improve and enhance their cybersecurity.

Examples of CSPs outside Scope of Work

- CSPs who provide cloud computing services for non-saudi organizations outside KSA.

- CSPs who provide cloud computing services for persons, small and medium enterprises, and private sector organizations not owning, operating or hosting Critical National Infrastructures

(CNIs).

5. Implementation and Compliance

To comply with item 3 of article 10 of NCAs mandate and as per the Royal Decree number 57231 dated 10/11/1439H, all CSPs and CSTs within the scope of these controls must implement whatever necessary to ensure continuous compliance with the obligations and controls.

Compliance with Essential Cybersecurity Controls (ECC) is a mandatory pre-requisite for CSTs and CSPs.

NCA evaluates CSPs and CSTs compliance with the CCC through multiple means such as self-assessment of CSPs and CSTs, and/or audit field visits by NCA or designated third-parties, in accordance with the mechanisms approved by the NCA.

6. CCC Methodology and Mapping Annex

NCA developed cloud cybersecurity controls methodology and mapping annex document which is considered as a part of Cloud Cybersecurity Controls document. The CCC methodology and mapping document is constituted of the following:

- Design principles of the CCC.
- Relationship to other international standards.
- Design methodology of the CCC.
- Main domains and subdomains structure of the CCC.
- Domains mapping to international standards.
- Control mapping to international standards.
- ECC/CCC subdomain mapping.

7. Update and Review

NCA will periodically review and update the CCC (in addition to any supplement documents related to the CCC) as per the cybersecurity requirements and related industry updates. NCA will communicate and publish the updated version of CCC for implementation and compliance.

8. Cybersecurity Obligations for Cloud Services

Cybersecurity obligations for cloud services are divided into four levels using a top down approach, level 1, level 2, level 3, and level 4:

- Level 1: A classification level applies to data classified as a (top secret) based on what is issued by the competent organization.

- Level 2: A classification level applies to data classified as a (secret) based on what is issued by the competent organization.

- Level 3: A classification level applies to data classified as a (restricted) based on what is issued by the competent organization, and level 3 is the lowest level for hosting sensitive systems and the data it contains.

- Level 4: classification level applies to data classified as a (open) based on what is issued by the competent organization.

8.1 The CSP is committed to achieving a constant and continuous commitment to the cybersecurity obligations in the cloud computing mentioned below, and to the cybersecurity of cloud computing (section no. 11 “Cloud Cybersecurity Controls”) by levels as shown in Table (1).

Table 1. CSP’s commitments to cybersecurity controls for cloud computing

CCC Subdomains and Controls	Level 1	Level 2	Level 3	Level 4
1-1-P-1	✓	✓	✓	✓
1-2-P-1	✓	✓	✓	✓
1-3-P-1	✣	✓	✓	✓
1-4-P-1	✓	✓	✓	✓
1-4-P-2	✓	✓	✓	✓
1-5-P-1	✣	✓	✓	✓
1-5-P-2	✣	✓	✓	✓
1-6-P	✓	✓	✓	✓
2-1-P-1	✓	✓	✓	✓
2-2-P	✓	✓	✓	✓

2-3-P-1	✣	✓	✓	✓
2-4-P	✓	✓	✓	✓
2-5-P-1	✓	✓	✓	✓
2-6-P-1	✓	✓	✓	✓
2-7-P-1	✓[1]	✓	✓	✓
2-8-P-1	✓	✓	✓	✓
2-9-P-1	✓	✓	✓	✓
2-10-P-1	✓	✓	✓	✓
2-11-P	✓	✓	✓	✓
2-12-P-1	✓	✓	✓	✓
2-13-P-1	✓	✓	✓	✓
2-14-P-1	✓	✓	✓	✓
2-15-P	✓	✓	✓	✓
2-16-P-1	✓	✓	✓	✓
2-17-P	✓	✓	✓	✓
2-18-P-1	✓	✓	✓	✓
3-1-P-1	✓	✓	✓	✓
4-1-P-1	✓	✓	✓	✓

✓ Mandatory ✣ Optional (recommended)

[1] With exception of subcontrols 2-7-P-1-15 and 2-7-P-1-16 that are considered as optional

8.2 The CST is committed to achieving a constant and continuous commitment to the cybersecurity obligations in the cloud computing mentioned below, and to the cybersecurity of cloud computing (section no. 11 “Cloud Cybersecurity Controls”) by levels as shown in Table (2).

Table 2. CST’s commitments to cybersecurity controls for cloud computing

CCC Subdomains and Controls	Level 1	Level 2	Level 3	Level 4
1-2-T-1	✓	✓	✓	✓
1-3-T-1	✓	✓	✓	✓
1-4-T-1	✓	✓	✓	✓
1-5-T-1	✣	✓	✓	✓
1-6-T	✓	✓	✓	✓
2-2-T	✓	✓	✓	✓
2-5-T-1	✣	✓	✓	✓
2-6-T-1	✣	✓	✓	✓
2-7-T-1	✓	✓	✓	✓
2-8-T-1	✓	✓	✓	✓
2-13-T-1	✣	✓	✓	✓
2-15-T	✓	✓	✓	✓
2-16-T-1	✓	✓	✓	✓
2-17-T	✓	✓	✓	✓
3-1-T-1	✓	✓	✓	✓
4-1-T-1	✓	✓	✓	✓

✓ Mandatory ✣ Optional (recommended)

8.3 Cybersecurity obligations for level 4:

8.3.1 The CST shall comply with the following obligations:

8.3.1.1 The CST shall comply with what is issued by the National Data Management Office or related laws regarding data classification, and in case there is any inquiry, the

CST should refer to the office.

8.3.1.2 The CST must contract with only licensed CSP.

8.3.1.3 KSA laws, regulations, regulatory frameworks and decisions shall govern the provision of all cloud services to CST.

8.3.1.4 The CST shall verify that the CSP shall comply with all controls, guidelines, frameworks and regulations for cybersecurity at level 4.

8.3.2 The CSP shall comply with the following obligations:

8.3.2.1 Consider all laws, regulations and mandates regarding cybersecurity in KSA.

8.3.2.2 CSPs must, to the extent required under the laws of the KSA, use telecommunication infrastructure, including international connectivity points through operators licensed in KSA.

8.3.2.3 With respect to actions taken by or on behalf of the CSP in the KSA:

8.3.2.3.1 Shall not copy or retain any CST's data unless the consent of the CST (data owner) or at the request of the competent authorities in the KSA.

8.3.2.3.2 CSP shall not comply with any laws other than KSA laws that would result in violation of the requirements specified in this document or any subsequent amendment. With respect to actions taken by or on behalf of the CSP outside the KSA that would result in access to data within the KSA, CSP shall not violate any applicable cybersecurity laws or regulations in KSA unless compelled by law, and then only after making all reasonable efforts to contest such compulsion by law. Any conflicts shall be brought without undue delay to the attention of appropriate Saudi authorities to the fullest extent permitted by law.

8.3.2.4 CSP must submit the following to NCA:

8.3.2.4.1 Disclosure of (by providing a detailed report at least once a year) the technology, features, controls, and available mitigations related to the CSP's ability to access or decrypt, or to assist or allow a third party to access or decrypt, any data stored, processed, or transmitted in or through the KSA.

8.3.2.4.2 Without undue delay, updates to such reports following any material adverse change to the security of the Saudi government data stored, processed, or transmitted in or through the KSA as a result of changes or updates to CSP's ability described in this clause.

8.3.2.5 Provide cloud computing services from within the KSA, including all systems used including storage, processing, monitoring, support, and disaster recovery centers.

8.3.2.6 KSA laws, regulations, regulatory frameworks and decisions shall govern the provision of all cloud services to KSA organizations.

8.3.2.7 The CSP shall comply with all controls, guidelines, frameworks and regulations for cybersecurity at level 4.

8.4 Cybersecurity obligations for level 3:

The CST and CSP shall comply with the specific obligations for cybersecurity at level 4, mentioned in paragraph 8.3, except for paragraph 8.3.2.3.2, in addition to the following obligations:

8.4.1 The CST shall verify that the CSP complies with all controls, guidelines, frameworks and regulations for cybersecurity at level 3.

8.4.2 The CSP shall comply with the following obligations:

8.4.2.1 For CSP's data centers within the KSA, CSPs shall provide a mutually reasonable agreed time plan that describes the eventual transition of all critical technical and operational functions performed on-site, including cybersecurity functions to qualified and suitable Saudi nationals.

8.4.2.2 CSP shall provide to the relevant competent authorities the general description, location and main features of connections, whether wired or wireless, between the telecommunications infrastructure and their Cloud ecosystem in the KSA.

8.4.2.3 CSPs will work with the competent Saudi authorities to develop a technical solution that shall ensure that any third-party providers in the Cloud ecosystem comply with all KSA data classification and protection requirements and regulations. Both parties will work together to develop a technical solution that will allow the Saudi Government to whitelist suppliers in the ecosystem that want to offer their services to the Saudi Government organizations.

8.4.2.4 With regard to the actions taken by the CSP or his representative in the KSA:

8.4.2.4.1 CSP shall not violate any applicable laws or security regulations in KSA, and shall not comply with any other laws, regulations, or requests that would conflict with the applicable laws or security regulations in KSA to the fullest extent permitted by law. Any conflicts shall be brought to the immediate attention of appropriate KSA authorities.

8.4.2.4.2 By using a detailed document, CSP shall disclose any and all capabilities CSP has to access or decrypt, or to assist or allow a third party to access or decrypt, any data stored, processed, or transmitted in or through the KSA, and CSP shall not implement any new capabilities in this regard without the NCA's prior express written consent.

8.4.2.5 The CSP shall comply with all controls, guidelines, frameworks and regulations for cybersecurity at level 3.

8.5 Cybersecurity obligations for level 2 and level 1:

The CSP and CST shall comply with the specific obligations for cybersecurity at level 3, mentioned in paragraph 8.4, in addition to the following obligations:

8.5.1 The CST shall comply with the following obligations:

8.5.1.1 The CST shall verify the CSP is isolating the cloud assigned to this level from other classification levels.

8.5.1.2 The CST shall verify that the CSP complies with all controls, guidelines, frameworks and regulations for cybersecurity at level 2 and level 1.

8.5.2 The CSP shall comply with the following obligations:

8.5.2.1 Isolate the cloud assigned to this level from other classification levels.

8.5.2.2 Ensure that third party apply all of the applicable obligations and controls.

8.5.2.3 The CSP shall comply with all controls, guidelines, frameworks and regulations for cybersecurity at level 2 and level 1.

9. CCC Domains and Structure

Figure (2) below shows the Main Domains and Subdomains of controls.

1- Cybersecurity Governance	1-1	Cybersecurity Policies and Procedures	1-4	Cybersecurity Roles and Responsibilities
	1-2	Cybersecurity Risk Management	1-5	Cybersecurity in Human Resources
	1-3	Compliance with Cybersecurity Standards, Laws and Regulations	1-6	Change Management
2- Cybersecurity Defense	2-1	Asset Management	2-10	Networks Security Management
	2-2	Operations and Service Management Cybersecurity	2-11	Storage Media Cybersecurity
	2-3	Cybersecurity Event Logs and Monitoring Management	2-12	Web application security
	2-4	System Development Security	2-13	Mobile Devices Security
	2-5	Cybersecurity Incident and Threat Management	2-14	Backup and Recovery Management
	2-6	Data and Information Protection	2-15	Key Management
	2-7	Identity and Access Management	2-16	Cryptography
	2-8	Vulnerability Management	2-17	Interoperability
	2-9	Information System and Processing Facilities Protection	2-18	Physical Security
3- Cybersecurity Resilience	3-1	Cybersecurity Resilience Aspects of Business Continuity Management (BCM)		
4- Third party Cybersecurity	4-1	Supply Chain & Third-Party Cybercecurity		

Figure 2: Main Domains and Subdomains of CCC

10 CCC Documentation Structure

CCC notation

The CCC itself is referred as described in Figure (3).

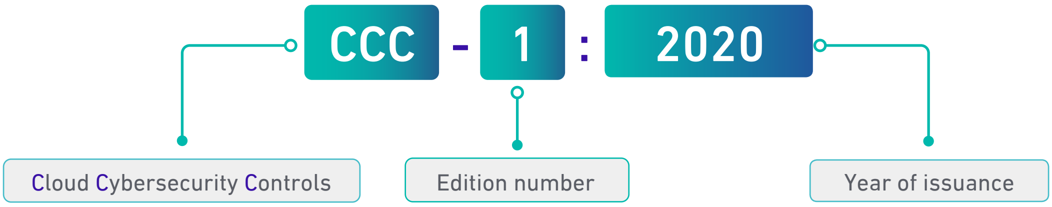

Figure 3: CCC identification notation

The CCC uses a notation providing a unique identifier for each element (Main Domain, Subdomain, Controls and Sub controls). The unique identifier is defined following the rules described in Figure (4)

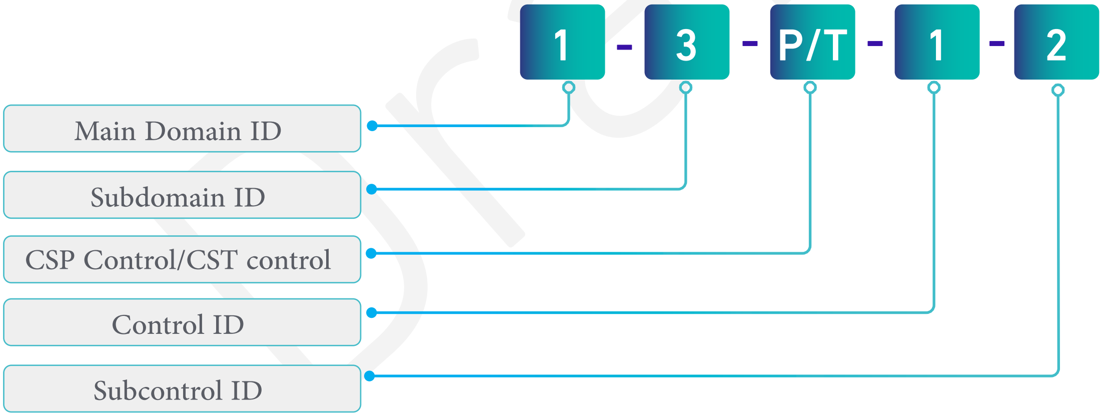

Figure 4: Controls Unique Identifier Structure

CST and CSP controls have common Main Domains and Subdomains, that are differentiated on the third identification tier, and have their own control and subcontrol identification notation sequences. CSPs will have an identification notation structure like ‘1-3-P-1-2’ in the figure. CSTs will have an identification notation structure like ‘1-3-T-1-2’.

A control is either applicable to the Provider (P) or the Cloud Tenant (T) and this is indicated in the notation’s third tier (“P/T”).

Please note that the green coloured numbers (such as: **1-3-2**) are reference numbers to subdomains or controls of ECC.

CCC Documentation

The CCC constituent element will be describes as shown in Figure (5), indicating how Main Domains, Subdomains, controls and subcontrols are documented in the rest of the document.

1 Reference number of the Main Domain	Name of Main Domain
Reference number of the Subdomain	Name of Subdomain
Objective	
Controls	
Reference number of the control	Control clauses

Figure 5: Documentation of controls, structures.

11. Cloud Cybersecurity Controls

Details of Cloud Cybersecurity Controls

1 Cybersecurity Governance

1-1	Cybersecurity Policies and Procedures
Objective	To ensure that cybersecurity requirements are documented, communicated and complied with by the CSPs and CSTs as per related laws and regulations, and organizational requirements.
Controls	
1-1-P-1	Referring to the ECC control 1-3-2 on implementation of security policies, the CSP shall also implement: 1-1-P-1-1 Obtaining the Authorizing Official's approval based on cybersecurity organizational structure, roles and responsibilities for actions that deviate from security policy, processes or procedures
1-2	**Cybersecurity Risk Management**
Objective	To ensure managing cybersecurity risks in a methodological approach in order to protect the CSP's and CST's information and technology assets as per organizational policies and procedures, and related laws and regulations.
Controls	
1-2-P-1	Cybersecurity Risk Management methodology mentioned in the ECC Subdomain 1-5, shall also include for the CSP, as a minimum: 1-2-P-1-1 Define acceptable risk levels for the cloud service. 1-2-P-1-2 Provision for data and information-focused risk management. 1-2-P-1-3 Risk register for cloud service and operation developed and maintained. 1-2-P-1-4 Cybersecurity policies updated based on outcome of risk assessment for the cloud service.

1-2-T-1	Cybersecurity Risk Management methodology mentioned in the ECC Subdomain 1-5 shall also include for the CST, as a minimum: 1-2-T-1-1 Define acceptable risk levels for the cloud service. 1-2-T-1-2 Provision for data and information-focused risk management. 1-2-T-1-3 Risk register for cloud service and operation developed and maintained. 1-2-T-1-4 Risk assessment performed on a regular basis and cybersecurity policy updated with the outcome for the cloud service.
1-3	**Compliance with Cybersecurity Standards, Laws and Regulations**
Objective	To ensure that the CSPs' and CSTs' cybersecurity program is in compliance with related laws and regulations.
Controls	
1-3-P-1	In addition to the ECC control 1-7-1, the CSP legislative and regulatory compliance should include as a minimum with the following requirements: 1-3-P-1-1 Legislation, regulation and contract terms that may create legal liabilities and obligations identified and continually monitored 1-3-P-1-2 Records protected from alteration, disclosure, destruction and unauthorized access and unauthorized release, in accordance with legal, regulatory, or contractual requirements 1-3-P-1-3 Privacy and protection of personal information, provided as per legal, regulatory, and contractual requirements 1-3-P-1-4 Cryptographic controls compliant with legal and regulatory requirements, PLAs (privacy level agreements) and common industry practice 1-3-P-1-5 Third party providers compliant with legal and regulatory requirements relevant to their scope
1-3-T-1	In addition to the ECC control 1-7-1, the CST legislative and regulatory compliance should include as a minimum with the following requirements: 1-3-T-1-1 Procedures to ensure compliance of CSP infrastructure service consumption (especially software products) with intellectual property laws. 1-3-T-1-2 Continuous or real-time compliance monitoring of the CSP.

1-4	Cybersecurity Roles and Responsibilities
Objective	To ensure that roles and responsibilities are defined for all parties participating in implementing the cloud cybersecurity controls, including the roles and responsibilities of the head of the CSP and CST or his/her delegate, referred to in this controls as “Authorizing Official”.
Controls	
1-4-P-1	In addition to the ECC control 1-4-1, the Authorizing Official shall also identify, document and approve: 1-4-P-1-1 Cybersecurity roles and RACI assignment for all stakeholders of the cloud service assigned, and communicated including Authorizing Official's roles and responsibilities.
1-4-P-2	In addition to the internal roles and responsibilities for the CSP defined in the ECC control 1-4-1, the the Authorizing Official shall also define the following external organizational interfaces: 1-4-P-2-1 CSP participation in authorized and specialized organizations and groups to stay up-to-date on Cybersecurity common practices and key know-how. 1-4-P-2-2 Communication with regulators.
1-4-T-1	In addition to the ECC control 1-4-1, the Authorizing Official shall also identify, document and approve: 1-4-T-1-1 Cybersecurity roles and RACI assignment for all stakeholders of the cloud service defined, documented, assigned, and communicated depending on the respective cloud service model.
1-5	**Cybersecurity in Human Resources**
Objective	To ensure that cybersecurity risks and requirements related to personnel (employees and contractors) are managed efficiently prior to employment, during employment and after termination/separation as per organizational policies and procedures, and related laws and regulations.
Controls	
1-5-P-1	In addition to subcontrols in the ECC control 1-9-4, the following requirements should be covered during the professional relationship of personnel with the CSP as a minimum: 1-5-P-1-1 Organizational roles and positions defined with a risk designation and personnel criteria for each designation

	1-5-P-1-2 Personnel with access to Cloud Technology Stack background-checked on defined intervals
	1-5-P-1-3 Disciplinary measures and processes for personnel who have violated the cybersecurity policy or processes and procedures
	1-5-P-1-4 Access agreements as a prerequisite to access to Cloud Technology Stack, signed and appropriately approved
1-5-P-2	In addition to subcontrols in the ECC control 1-9-5, the following controls should be in place, as a minimum, for the termination/completion of a human resource's professional relationship with the CSP: 1-5-P-2-1 Cybersecurity common practices for personnel contract termination, including: • Exit interviews for key cybersecurity personnel • Access retention (handover of credentials and passwords) to systems formerly controlled by terminated personnel/ third-party • Notification of cessation to all CSP staff for key cybersecurity personnel 1-5-P-2-2 Assurance that assets owned by the organization (especially those with security exposure) are accounted for and returned upon termination
1-5-T-1	In addition to subcontrols in the ECC control 1-9-3, the following requirements should be covered during the professional relationship of staff with the CST shall cover, at a minimum: 1-5-T-1-1 Background-checks at defined intervals on personnel with access to Cloud Service sensitive functions (Key Management, Service Administration, Access Control)
1-6	**Change Management**
Objective	Ensure cybersecurity levels are not affected by change requests introduced in the cloud stack and operation by exercising due diligence analysis and control of the changes
Controls	
1-6-P-1	Cybersecurity requirements for change management within the CSP shall be identified, documented and approved.

1-6-P-2	Cybersecurity requirements for change management within the CSP shall be applied
1-6-P-3	Cybersecurity for Change Management in the CSP shall cover, as a minimum: 1-6-P-3-1 Processes and procedures to orderly implement changes planned works in production systems. 1-6-P-3-2 Common practices for testing and rollback in planned works 1-6-P-3-3 Processes for the implementation of exceptional changes (e.g.: changes during incident restoration) 1-6-P-3-4 Analysis of security impact from all change requests implemented in the Cloud Technology Stack 1-6-P-3-5 Technical system configurations adhering to the Minimum Functionality Principle 1-6-P-3-6 Whitelisted software only allowed on systems
1-6-P-4	Cybersecurity requirements for change management within the CSP shall be applied and reviewed periodically
1-6-T-1	Cybersecurity requirements for change management within the CST shall be identified, documented and approved.
1-6-T-2	Cybersecurity requirements for change management within the CST shall be applied
1-6-T-3	Cybersecurity Change Management in the CST shall cover, as a minimum: 1-6-T-3-1 Analysis of security impact from all change requests and planned works related to the cloud computing service
1-6-T-4	Cybersecurity requirements for change management within the CST shall be applied and reviewed periodically

2 Cybersecurity defense

2-1	Asset Management
Objective	To ensure that the CSP and CST has an accurate and detailed inventory of information and technology assets in order to support the organization's cybersecurity and operational requirements to maintain the confidentiality, integrity and availability of information and technology assets.
Controls	
2-1-P-1	In addition to controls in the ECC control 2-1, the CSP shall cover the following additional controls for cybersecurity requirements for cybersecurity event logs and monitoring management, as a minimum: 2-1-P-1-1 Inventory of all information and technology assets using suitable techniques such as Configuration Management Database (CMDB) or similar capability containing an inventory of all technical assets 2-1-P-1-2 Appointment of owners for each technical asset
2-2	Operations and Service Management Cybersecurity
Objective	Ensure all operations are conducted in a manner that safeguards the confidentiality, integrity, and availability of the CSPs' and CSTs' technical and information assets
Controls	
2-2-P-1	Cybersecurity requirements for operations and service management within the CSP shall be identified, documented and approved.
2-2-P-2	Cybersecurity requirements for operations and service management within the CSP shall be applied.
2-2-P-3	Operations and Service Management Cybersecurity within the CSP shall cover, at a minimum, the following: 2-2-P-3-1 A procedure to monitor technical resource load and utilization and to plan for capacity provisioning 2-2-P-3-2 Documentation of the procedures required for the operation of the cloud stack, and security classification thereof 2-2-P-3-3 Management and maintenance of a Cloud Technology Stack configuration

	2-2-P-3-4 Contractual SLA clauses compliance between CSP and CST continually monitored 2-2-P-3-5 Cybersecurity architecture for the Cloud Computing Service that addresses approach, structure, support of the enterprise architecture and operating model and external interfaces and dependencies
2-2-P-4	Cybersecurity requirements for cybersecurity operations and service management within the CSP shall be applied and reviewed periodically.
2-2-T-1	Cybersecurity requirements for cybersecurity operations and service management within the CST shall be identified, documented and approved.
2-2-T-2	Cybersecurity requirements for cybersecurity operations and service management within the CST shall be applied.
2-2-T-3	Cybersecurity operations and service management within CST shall cover, at a minimum, the following: 2-2-T-3-1 Documentation (and security classification thereof) of procedures required for the operation of the Cloud Technology Stack
2-2-T-4	Cybersecurity requirements for security operations and service management within the CST shall be applied and reviewed periodically.
2-3	**Cybersecurity Event Logs and Monitoring Management**
Objective	Ensure timely collection, analysis and monitoring of cybersecurity event logs for the proactive detection and effective management of cyber-attacks to prevent or minimize the impact on the CSPs' and CSTs' business.
Controls	
2-3-P-1	In addition to subcontrols in the ECC control 2-12-3, the CSP shall cover the following additional subcontrols for cybersecurity requirements for cybersecurity event logs and monitoring management, as a minimum: 2-3-P-1-1 Capture of all audit trails from all systems in the Cloud Technology Stack 2-3-P-1-2 Protection of all audit trails from all systems in the Cloud Technology Stack 2-3-P-1-3 Protect and capture all logs of clear identification of user activity at the tenant level in order to support forensic analysis

	2-3-P-1-4 Referring to the ECC control 2-12-3-5, all logs must be retained (for at least 18 months) and backed up 2-3-P-1-5 Continuous cybersecurity events monitoring using SIEM technique (Real-time, consolidated monitoring of security events) covering the full Cloud Technology Stack 2-3-P-1-6 Periodical, in-depth, back office (tier 2) cybersecurity log review, covering all logs and audit trails in the Cloud Technology Stack 2-3-P-1-7 Availability SLAs enforced for the SIEM system 2-3-P-1-8 Technical and organizational safeguards for the secure handling of user-related data found in the audit trails and the cybersecurity logs 2-3-P-1-9 Automated Monitoring and logging of remote access sessions 2-3-P-1-10 Enablement and collection of login history
2-3-T-1	In addition to subcontrols in the ECC control 2-12-3, the CST shall cover the following additional subcontrols for cybersecurity requirements for cybersecurity event logs and monitoring management, as a minimum: 2-3-T-1-1 Ensure that CSP capture all event logs of user activities at the tenant level. 2-3-T-1-2 Monitoring shall include all captured logs on the cloud service of the CST. 2-3-T-1-3 Collection of login history from the cloud service
2-4	**System Development Security**
Objective	Ensure applications are developed, integrated and deployed in a secure manner
Controls	
2-4-P-1	Cybersecurity requirements for software and application development within the CSP shall be identified, documented and approved.
2-4-P-2	Cybersecurity requirements for software and application development within the CSP shall be applied

2-4-P-3	Cybersecurity requirements for software and application development within the CSP shall include as a minimum the following controls along the development lifecycle: 2-4-P-3-1 Well-defined system development lifecycle (SDLC) to facilitate security controls and a secure systems development lifecycle (SSDLC). This is also applicable to agile approaches. 2-4-P-3-2 Technical and organizational safeguards for the proper implementation and integration of applications 2-4-P-3-3 Cybersecurity requirements of the Cloud Technology Stack in the design and specification of the cloud computing services 2-4-P-3-4 The inclusion of security test cases for all systems, in the Cloud Technology Stack, in system testing and evaluation 2-4-P-3-5 The exhaustive inclusion of cybersecurity on technical system documentation and manuals 2-4-P-3-6 Protection of system development environments, testing environments and integration platforms 2-4-P-3-7 Restriction of access to secure application code 2-4-P-3-8 Enforcement of adoption by outsourcing third-party developers and vendors of cybersecurity standards consistent with those of the CSP 2-4-P-3-9 Ensure that the security of the software developed by third-parties is monitored and controlled 2-4-P-3-10 Protection of test data
2-4-P-4	Cybersecurity requirements for software and application development within the CSP shall be applied and reviewed periodically
2-4-T-1	Cybersecurity requirements for software and application development on services consumed by the CST within the cloud shall be identified, documented and approved by the CST
2-4-T-2	Cybersecurity requirements for software and application development within the cloud shall be applied by the CST

2-4-T-3	Cybersecurity requirements for software and application development for applications shall include as a minimum the following controls along the development lifecycle: 2-4-T-3-1 Cybersecurity requirements on the specification of all cloud computing services consumed by the CST 2-4-T-3-2 The inclusion of security test cases in system testing and evaluation, for all cloud computing services consumed by the CST
2-4-T-4	Cybersecurity requirements for software and application development of services consumed by the CST shall be applied and reviewed
2-5	**Cybersecurity Incident and Threat Management**
Objective	Ensure timely identification and detection of cybersecurity incidents and their effective management and proactive response to cybersecurity threats to prevent or minimize the impact of the impacts resulting on the business of the CSP and CST, alongside observance of the provisions of Royal Decree No. 37140 of 14/08/1438 AH.
Controls	
2-5-P-1	In addition to subcontrols in the ECC control 2-13-3, the CSP shall cover the following additional subcontrols for cybersecurity requirements for cybersecurity incident and threat management, as a minimum: 2-5-P-1-1 Implementation of processes and procedures to respond to security incidents in a timely and efficient manner 2-5-P-1-2 Training for employees to respond to incidents, in line with their roles and responsibilities 2-5-P-1-3 Response to (and containment of) Information Spillage incidents 2-5-P-1-4 Clear and structured processes and procedures for Root Cause Analysis (i.e.: identification and handling of the root causes of security incidents) 2-5-P-1-5 Mechanisms to support legal proceedings and forensics, protecting the chain of custody provided to CST 2-5-P-1-6 Information and contractual requirement for employees and third-party personnel to report security events to their knowledge 2-5-P-1-7 Support for CSTs to handle security incidents 2-5-P-1-8 Mechanisms to measure cybersecurity incident metrics and monitor compliance with contract and guidelines

	2-5-P-1-9 Periodically testing the incident response capability 2-5-P-1-10 Real-time reporting of incidents to CSTs.
2-5-T-1	In addition to subcontrols in the ECC control 2-13-3, the CST shall cover the following additional subcontrols for cybersecurity requirements for cybersecurity incident and threat management, as a minimum: 2-5-T-1-1 Handling of reported cybersecurity incidents from CSP 2-5-T-1-2 Interface with CSP to get support on cloud-related incident management, when required 2-5-T-1-3 Mechanisms to measure security incident Key Performance Indicators (KPIs) (frequency, impact, response time, etc.…) and monitor compliance with SLAs, contract, and guidelines 2-5-T-1-4 Information and contractual requirement for employees and external parties to report security events to their knowledge 2-5-T-1-5 Testing the incident response capability of the CSP and the CST security operation
2-6	**Data and Information Protection**
Objective	To ensure the confidentiality, integrity and availability of CSPs' and CSTs' data and information as per organizational policies and procedures, and related laws and regulations.
Controls	
2-6-P-1	In addition to subcontrols in the ECC control 2-7-3, the CSP shall cover the following additional subcontrols for cybersecurity requirements for data and information protection requirements, as a minimum: 2-6-P-1-1 Assurance of data flows being contained within the tenancy, geography and access boundaries required by contract and by regulation 2-6-P-1-2 Provision to CSTs (and administrators) of the capability to identify the physical location for all data 2-6-P-1-3 Prevention of the use of unsanitized production data in non-production environments, such as test or development environments 2-6-P-1-4 Provision to CSTs of data storage processes, procedures, and technology to comply with legal, regulatory and contractual requirements 2-6-P-1-5 Provision to CSTs a mechanism for the management of privacy and security metadata

	2-6-P-1-6	Provision of metadata labelling mechanism to meet all applicable data privacy, data sovereignty, and data protection laws and regulations
	2-6-P-1-7	Restriction of data processing location based on cybersecurity policy and data privacy, protection and sovereignty regulations
	2-6-P-1-8	Disposal of tenant’s data should be performed in a secure manner that guarntees the disposed data cannt be recovered
2-6-T-1	In addition to subcontrols in the ECC control 2-7-3, the CST shall cover the following additional subcontrols for cybersecurity requirements for data and information protection requirements, as a minimum:	
	2-6-T-1-1	Assurance of data flows being contained within the tenancy, geography and access boundaries required by contract and by regulation.
	2-6-T-1-2	Operational capability (with support from CSP) for CST administrators and data controller to identify the physical location for all data.
	2-6-T-1-3	Provision of metadata labelling mechanism to prevent violation of data privacy, data sovereignty, and data protection laws, statutes or directives.
	2-6-T-1-4	Exit Strategy to ensure means for secure disposal of data.
2-7	**Identity and Access Management**	
Objective	To ensure the secure and restricted logical access to information and technology assets in order to prevent unauthorized access and allow only authorized access for users which are necessary to accomplish assigned tasks.	
Controls		
2-7-P-1	In addition to subcontrols in the ECC control 2-2-3, the CSP shall cover the following additional subcontrols for cybersecurity requirements for identity and access management requirements, as a minimum:	
	2-7-P-1-1	Identity and Access Management of credentials for which a personalized account cannot be created
	2-7-P-1-2	Identity and access management for all credentials along their full lifecycle
	2-7-P-1-3	Confidentiality of user identification and access rights information, including the requirement on users to keep them private (for employed, third party and CST personnel)

	2-7-P-1-4	Secure session management, including session authenticity, session lockout, session timeout termination
	2-7-P-1-5	Multi-factor authentication for all accounts
	2-7-P-1-6	Formal process to detect and prevent unauthorized access (e.g. unsuccessful login attempt threshold)
	2-7-P-1-7	Prevention of access from wireless networks for the Controlled Area Network of the Cloud Technology Stack
	2-7-P-1-8	Provision for third party access control, to minimize risk of unauthorized or inappropriate access
	2-7-P-1-9	Location-aware technologies to validate access authentication to the Cloud Technology Stack
	2-7-P-1-10	Access control enforced to management systems, administrative consoles (whether for hardware, hypervisor, VM or OS)
	2-7-P-1-11	Masking of displayed authentication inputs, especially passwords, to prevent shoulder surfing
	2-7-P-1-12	Notification to user when opening the session of access to a controlled system, that session may be monitored, that only authorized users are permitted to log in and the legal liabilities derived from the use of the system
	2-7-P-1-13	Capability to immediately interrupt a remote access session and prevent any future access for a user
	2-7-P-1-14	PKI-based authentication capability that validates certifications with trusted certification authority and enforces individual ownership of authenticated identity
	2-7-P-1-15	Notification to CST when CST-related asset is accessed by the CSP.
	2-7-P-1-16	Getting CST approval before accessing any CST-related asset.
	2-7-P-1-17	Utilizing secure methods and algorithms for saving and processing passwords, such as: Hashing functions.

2-7-T-1	In addition to subcontrols in the ECC control 2-2-3, the CST shall cover the following additional subcontrols for cybersecurity requirements for identity and access management requirements, as a minimum: 2-7-T-1-1 Identity and access management for all cloud credentials along their full lifecycle. 2-7-T-1-2 Confidentiality of cloud user identification, cloud credential and cloud access rights information, including the requirement on users to keep them private (for employed, third party and CST personnel). 2-7-T-1-3 Secure session management, including session authenticity, session lockout, session timeout termination on the cloud. 2-7-T-1-4 Multi-factor authentication for privileged cloud accounts.
	2-7-T-1-5 Formal process to detect and prevent unauthorized access to cloud through a threshold of unsuccessful login attempts.
2-8	**Vulnerability Management**
Objective	To ensure timely detection and effective remediation of technical vulnerabilities to prevent or minimize the probability of exploiting these vulnerabilities to launch cyber attacks against the CSP and CST.
Controls	
2-8-P-1	In addition to subcontrols in the ECC control 2-10-3, the CSP shall cover the following additional subcontrols for cybersecurity requirements for vulnerability management requirements, as a minimum: 2-8-P-1-1 Provision for minimal impact on the services provided to CSTs in the patching process 2-8-P-1-2 Provision for immediate patching of critical vulnerabilities identified on the Cloud Technology Stack 2-8-P-1-3 Provision for vulnerability assessment on the Cloud Technology Stack 2-8-P-1-4 External (once every month) and internal (once every three months) vulnerability assessment and management 2-8-P-1-5 Notification to CST of identified vulnerabilities and safeguards in place

2-8-T-1	In addition to subcontrols in the ECC control 2-10-3, the CST shall cover the following additional subcontrols for cybersecurity requirements for vulnerability management requirements, as a minimum: 2-8-T-1-1 Vulnerability assessment and management for the cloud service one every three months 2-8-T-1-2 Management of CSP-notified vulnerabilities in the cloud service and safeguards in place
2-9	**Information System and Information Processing Facilities Protection**
Objective	To ensure the protection of information systems and information processing facilities (including workstations and infrastructures) against cyber risks.
Controls	
2-9-P-1	In addition to subcontrols in the ECC control 2-3-3, the CSP shall cover the following additional subcontrols for cybersecurity requirements for information system and processing facilities protection requirements, as a minimum: 2-9-P-1-1 Protection of the integrity of the Cloud Technology Stack 2-9-P-1-2 Integrity and tampering prevention of virtual machines, containers, and any other virtualization appliance 2-9-P-1-3 Compliance checks to ensure all configurations are applied in accordance to Configuration Management 2-9-P-1-4 Isolation of application and user functionality from system-level functionality (OS, hypervisor, CMP…) 2-9-P-1-5 Management of security controls and control of adherence to the minimum functionality principle 2-9-P-1-6 Robustness of the Cloud Technology Stacks to handle malicious or corrupt inputs (information input validation, memory protection) and exceptions and fail in a controlled manner (i.e.: fail in known state, exception handling) 2-9-P-1-7 Detailed and complete documentation of Cloud Technology Stack architecture, indicating redundancy 2-9-P-1-8 Right level of redundancy, capacity and availability on the Cloud Technology Stack's compute and storage to meet SLAs

	2-9-P-1-9	Documented dynamic resource management process
	2-9-P-1-10	Full isolation of security function from non-security functions in the Cloud Technology Stack
	2-9-P-1-11	Maximize the automated reporting of security control metrics and KPIs.
	2-9-P-1-12	Prevention of execution of unauthorized mobile code (Java, JavaScript, ActiveX, VBScript, Flash, etc.…)
	2-9-P-1-13	Detection and prevention of unauthorized changes to software, firmware and systems
	2-9-P-1-14	Complete isolation and protection of multiple guest environments in a common shared virtualization infrastructure
	2-9-P-1-15	Provision for process isolation within the Cloud Technology Stack
	2-9-P-1-16	Commitment of a pre-determined minimum available resource capacity to CSTs
	2-9-P-1-17	Assurance of separation and isolation of data, environments and information systems across CSTs, to prevent data commingling
	2-9-P-1-18	Assurance of restricted and controlled access to storage arrays and total isolation between guest environments in the SAN
2-10	**Networks Security Management**	
Objective	To ensure the protection of CSP's and CST's network from cyber risks.	
Controls		
2-10-P-1	In addition to subcontrols in the ECC control 2-5-3, the CSP shall cover the following additional subcontrols for cybersecurity requirements for networks security management requirements, as a minimum:	
	2-10-P-1-1	Detailed documentation of network architecture and topology for all areas at high risk, detailing safeguards and countermeasures
	2-10-P-1-2	Network isolation and protection of the Controlled Area Network of the Cloud Technology Stack (e.g.: gateways to communication service provider, internet access, DMZs…), as well as at key internal boundaries (e.g.: subnets, Data Center Interconnect gateways...)

	2-10-P-1-3 Protection from denial of service attacks (including DDoS) 2-10-P-1-4 Protection of data transmitted within the Cloud Technology Stack outside the Controlled Area Network through standard-prescribed cryptography primitives or full network isolation 2-10-P-1-5 Access control between different network segments 2-10-P-1-6 Commitment to a predefined level of bandwidth and latency for guest environments, services and CSTs, based on priority, to prevent crowding out from bandwidth-demanding connections 2-10-P-1-7 Isolation of the Cloud Technology Stack from Wireless networks. 2-10-P-1-8 Multi-tenant segregation in network connectivity and data flows across the communications network 2-10-P-1-9 Isolation between cloud service delivery network, cloud management network and CSP enterprise network 2-10-P-1-10 Monitoring of traffic across the Controlled Area Network and across internal boundaries, with detection capabilities for anomalies, covert information and unauthorized network services 2-10-P-1-11 End-to-end IDS/IPS capability across all the Cloud Technology Stack and the wider CSP enterprise
2-11	**Storage Media Security**
Objective	Ensure secure handling of information and data on physical media.
Controls	
2-11-P-1	Cybersecurity requirements for usage of information and data media within the CSP shall be identified, documented and approved.
2-11-P-2	Cybersecurity requirements for usage of information and data media within the CSP shall be applied.

2-11-P-3	Cybersecurity requirements for usage of information and data media within the CSP shall cover, at minimum, the following: 2-11-P-3-1 Enforcement of sanitization of media, prior to disposal or reuse 2-11-P-3-2 Enforcement of media clearing and data remanence practice 2-11-P-3-3 Provision to maintain confidentiality and integrity of data on removable media 2-11-P-3-4 Human readable marking of media, including control restriction and caveats for management and control of media 2-11-P-3-5 Controlled and physically secure storage of removable media
	2-11-P-3-6 Restriction and control of usage of portable media inside the Controlled Area Network of the cloud technology stack
2-11-P-4	Cybersecurity requirements for usage of information and data media within the CSP shall be applied and reviewed periodically.
2-12	**Web application security**
Objective	Ensure the protection of external web applications of the CSP and CST from cyber risks.
Controls	
2-12-P-1	In addition to subcontrols in the ECC control 2-15-3, the CSP shall cover the following additional subcontrols for cybersecurity requirements for web application security, as a minimum: 2-12-P-1-1 Information involved in application service transactions shall be protected against possible risks (e.g.: incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure….).
2-13	**Mobile Devices Security**
Objective	To ensure the protection of mobile devices (including laptops, smartphones, tablets) from cyber risks and to ensure the secure handling of the CSPs' and CSTs' information (including sensitive information) while utilizing Bring Your Own Device (BYOD) policy.

Controls	
2-13-P-1	In addition to subcontrols in the ECC control 2-6-3, the CSP shall cover the following additional subcontrols for cybersecurity requirements for mobile device security, as a minimum:
	2-13-P-1-1 Inventory of all end user and mobile devices 2-13-P-1-2 Centralized mobile device management and laptop/desktop software, release and configuration management 2-13-P-1-3 Screen locking for end user devices 2-13-P-1-4 Latest level of patching for all mobile devices 2-13-P-1-5 Endpoint IDS/IPS capability on laptops, desktops and workstations
	2-13-P-1-6 End user asset return and verification for those assets with exposure to the Cloud Technology Stack Controlled Area Network 2-13-P-1-7 Data sanitation and disposal for end-user devices, especially for those with exposure to the Cloud Technology Stack Controlled Area Network 2-13-P-1-8 Disablement of cameras, microphones and other media devices on laptops that may be used within the Cloud Technology Stack Controlled Area Network and data center facilities 2-13-P-1-9 Monitor, control and management of portable maintenance tools that can access data and have exposure to the Controlled Area Network of the Cloud Technology Stack
2-13-T-1	In addition to subcontrols in the ECC control 2-6-3, the CST shall cover the following additional subcontrols for cybersecurity requirements for mobile device security, as a minimum: 2-13-T-1-1 End user asset return and verification for those assets with access to the cloud service 2-13-T-1-2 Data sanitation and disposal for end-user devices with access to the cloud service
2-14	**Backup and Recovery Management**
Objective	To ensure the protection of CSPs' and CSTs' data and information including information systems and software configurations from cyber risks as per organizational policies and procedures, and related laws and regulations.
Controls	

2-14-P-1	In addition to subcontrols in the ECC control 2-9-3, the CSP shall cover the following additional subcontrols for cybersecurity requirements for backup and recovery management, as a minimum: 2-14-P-1-1 Online and offline backup of CST’s data according to planned intervals with the ablitiy of recover the CST's virtual appliances, snapshots, images, containers and any service metadata within a time period specified in the services SLAs. 2-14-P-1-2 Scope and coverage of online and offline backups to cover Cloud Technology Stack. 2-14-P-1-3 Securing access, storage and transfer of CST’s data backups and its mediums, and protecting it against damage, amendment or unauthorized access. 2-14-P-1-4 Securing access, storage and transfer of Cloud Technology Stack backups and its mediums, and protecting it against damage, amendment or unauthorized access.
2-15	**Key Management**
Objective	Ensure secure management of cryptographic keys to protect confidentiality, integrity and availability of information and technical assets.
Controls	
2-15-P-1	Cybersecurity requirements for key management process within the CSP shall be identified, documented and approved.
2-15-P-2	Cybersecurity requirements for key management process within the CSP shall be identified, documented and approved.
2-15-P-3	In addition to the ECC subcontrol 2-8-3-2, cybersecurity requirements for key management within the CSP shall cover, at minimum, the following: 2-15-P-3-1 Ensure well-defined ownership and non-disclosure for every encryption key, to allow for responsibility and accountability. 2-15-P-3-2 Backup of keys and enforcement of trusted key storage, strictly external to cloud 2-15-P-3-3 Capability to revoke keys and certificates from users and information systems. 2-15-P-3-4 Availability of information in case of key loss. 2-15-P-3-5 Capturing and monitoring of all audit trails of keys.

2-15-P-4	Cybersecurity requirements for key management within the CSP shall be reviewed periodically.
2-15-T-1	Cybersecurity requirements for key management within the CST shall be identified, documented and approved.
2-15-T-2	Cybersecurity requirements for key management within the CST shall applied.
2-15-T-3	In addition to the ECC subcontrol 2-8-3-2, cybersecurity requirements for key management within the CST shall cover, at minimum, the following: 2-15-T-3-1 Ensure well-defined ownership and non-disclosure for every encryption key used for the cloud service, to allow for responsibility and accountability. 2-15-T-3-2 Trusted key storage for the cloud service, strictly external to cloud. 2-15-T-3-3 Capability to revoke keys for the cloud service and certificates from users and information systems. 2-15-T-3-4 Assurance for availability of information in all cases.
2-15-T-4	Cybersecurity requirements for key management within the CST shall be reviewed periodically.
2-16	**Cryptography**
Objective	To ensure the proper and efficient use of cryptography to protect information assets as per CSPs and CSTs policies and procedures, and related laws and regulations.
Controls	
2-16-P-1	In addition to subcontrols in the ECC control 2-8-3, the CSP shall cover the following additional subcontrols for cryptography, as a minimum: 2-16-P-1-1 Technical mechanisms and cryptographic primitives for strong encryption. 2-16-P-1-2 Certification authority and issuance capability, or usage of certificates from a trusted certification authority.
2-16-T-1	In addition to subcontrols in the ECC control 2-8-3, the CST shall cover the following additional subcontrols for cryptography, as a minimum: 2-16-T-1-1 Technical mechanisms and cryptographic primitives for strong encryption.

	2-16-P-1-2 Certification authority and issuance capability, or usage of certificates from a trusted certification authority
2-17	**Interoperability**
Objective	Ensure minimal operational and economic restrictions caused by the usage of proprietary or non-interoperable technical assets and information storage formats.
Controls	
2-17-P-1	Cybersecurity requirements for interoperability within the CSP shall be identified, documented and approved.
2-17-P-2	Cybersecurity requirements for interoperability within the CSP shall be applied.
2-17-P-3	Cybersecurity requirements for interoperability within the CSP shall cover, at minimum, the following: 2-17-P-3-1 Interoperable and portable services available to CST. 2-17-P-3-2 Provision of open and published APIs to CSTs. 2-17-P-3-3 Provision of standard network protocols to CSTs, for the transfer of data and management of the cloud service. 2-17-P-3-4 Provision of standard data formats to CSTs. 2-17-P-3-5 Provision of standard formats to CSTs, for images and virtual appliance storage (e.g. OVF).
2-17-P-4	Cybersecurity requirements for interoperability within the CSP shall be reviewed periodically.
2-17-T-1	Cybersecurity requirements for interoperability within the CST shall be identified, documented and approved.
2-17-T-2	Cybersecurity requirements for interoperability within the CST shall be applied.
2-17-T-3	Cybersecurity requirements for interoperability within the CST shall cover, at minimum, the following: 2-17-T-3-1 Interoperable and portable services in contract between CST and CSP. 2-17-T-3-2 Preferred use of standard and published APIs, to ensure support for interoperability between components and to facilitate migrating applications.

	2-17-T-3-3 Preferred use of standard network protocols, for the transfer of data and management of the cloud service. 2-17-T-3-4 Preferred use of standard data formats to be able to export and move data to and from a CSP. 2-17-T-3-5 Exit strategy to ensure means for data export and transfer .
2-17-T-4	Cybersecurity requirements for interoperability within the CST shall be reviewed periodically.
2-18	**Physical Security**
Objective	To ensure the protection of information and technology assets from unauthorized physical access, loss, theft and damage.
Controls	
2-18-P-1	In addition to subcontrols in the ECC control **2-14-3**, the CSP shall cover the following additional subcontrols for cybersecurity requirements for physical security, as a minimum: 2-18-P-1-1 Continual monitoring of access to cloud hosting or cloud management facilities, with detection and response of unauthorized access incidents. 2-18-P-1-2 Procedures to ensure that only authorized personnel are allowed access to the data center, cloud hosting or cloud management facilities. 2-18-P-1-3 Provision to prevent unauthorized access, eavesdropping and damage of the transmission medium part of the Cloud Technology Stack. 2-18-P-1-4 Provision to prevent unauthorized access to input/output and management devices in the Cloud Technology Stack. 2-18-P-1-5 Provision for implementing a safe working environment in the Data Centre/cloud collocation facility and cloud management facility. 2-18-P-1-6 Lighting in the event of blackout in the working Data Centre facility, as well as lighting of emergency exits and evacuation route. 2-18-P-1-7 Capability to immediately shut off power information systems or components securely thereof in case of emergency.

	2-18-P-1-8	Fire detection and suppression systems that are fed from an autonomous power source.
	2-18-P-1-9	Provision to protect facility and cloud technology infrastructure from earthquakes, explosions, civil disturbances and other forms of natural threats and threats caused by humans.
	2-18-P-1-10	Protection from water leakage.
	2-18-P-1-11	Prevention of outages caused by power supply blackouts or electrical failures.
	2-18-P-1-12	Utilization of utility services from redundant sources, and ensuring of utility services continuity in case of interruption, and periodically testing of it.
	2-18-P-1-13	Utilization of two different and fully redundant telecommunication networks between CSTs, cloud and internet.
	2-18-P-1-14	Prevention of equipment/information system collocation in building areas where hazard may be more likely.
	2-18-P-1-15	Regular execution of equipment maintenance routines.
	2-18-P-1-16	Caged collocation infrastructure to host higher classification information assets optionally offered in the service portfolio.
	2-18-P-1-17	Physical asset classification and labelling in terms of security sensitivity, business criticality and operational availability requirements.
	2-18-P-1-18	Ensure that only authorized equipment is moved securely onsite or offsite.
	2-18-P-1-19	Provision in the data center/collocation facility of access points and packing/unpacking areas, isolated with access control from the rest of the facility.
	2-18-P-1-20	Secure disposal of cloud infrastructure hardware, in particular, storage equipment (external or internal), addressing the clearing, wiping and destruction of stored data.
	2-18-P-1-21	Provision of automated temperature, ventilation and humidity controls in the data center/cloud collocation facility.
	2-18-P-1-22	Provision of redundant electrical cabling in data center/cloud hosting facility.

3 Cybersecurity Resilience

3-1	Cybersecurity Resilience Aspects of Business Continuity Management (BCM)
Objective	To ensure the inclusion of the cybersecurity resiliency requirements within the CSPs' and CSTs' business continuity management and to remediate and minimize the impacts on systems, information processing facilities and critical e-services from disasters caused by cybersecurity incidents.
Controls	
3-1-P-1	In addition to subcontrols in the ECC control 3-1-3, the CSP shall cover the following additional subcontrols for cybersecurity requirements for cybersecurity resilience aspects of business continuity management, as a minimum: 3-1-P-1-1 Resumption of business functions in a well specified period defined as SLA. 3-1-P-1-2 Assessing and handling risks of potential malfunctions or disasters. 3-1-P-1-3 Raise awareness and training of staff through rehearsal and drill of disaster recovery plans. 3-1-P-1-4 Testing and simulation of the disaster recovery plan. 3-1-P-1-5 Geographically redundant (separated 50 km. or more) second data center facility to hold compute and processing to ensure the continuioty in case a disaster or incident renders the main site inoperative provided that these two data centers do not share potential risks. 3-1-P-1-6 Geographically redundant second data center facility (separated 50 km. or more) to hold vaulted storage and data in case a disaster or incident renders the main site inoperative provided that these two data centers do not share potential risks. 3-1-P-1-7 Geographically redundant second site (separated 100 km. or more) to host command center and workforce to ensure the continuiot , in case the main center is rendered inoperative provided that these two sites do not share potential risks. 3-1-P-1-8 Identifying roles and responsibilities related to business continuity management and disaster recovery.

3-1-T-1	In addition to subcontrols in the ECC control 3-1-3, the CST shall cover the following additional subcontrols for cybersecurity requirements for cybersecurity resilience aspects of business continuity management, as a minimum: 3-1-T-1-1 Define SLAs in agreement with CSP for resumption 3-1-T-1-2 Provision for continuity of the operational interfaces with the CSP in case of a disaster, and training of staff on them

4 Third-party Cybersecurity

4-1	Supply Chain and Third-Party Cyberecurity
Objective	To ensure the protection of assets against the cybersecurity risks related to third-parties including outsourcing and managed services as per policies and procedures, and related laws and regulations.
Controls	
4-1-P-1	In addition to subcontrols in the ECC control 4-1-3, the CSP shall cover the following additional subcontrols for third-party cybercurity requirements, as a minimum: 4-1-P-1-1 Cybersecurity assessment and periodical audit of third-party providers, and handling the observations. 4-1-P-1-2 Requirement to provide security documentation for any equipment or services from suppliers and third-party providers. 4-1-P-1-3 Management of data integrity with third-party providers. 4-1-P-1-4 Continuous security monitoring on service delivery from suppliers and third-party providers. 4-1-P-1-5 Risk management and security governance on third-party providers as part of general cybersecurity risk management and governance . 4-1-P-1-6 Screening or vetting for outsourcing and managed services companies and personnel in association with Cloud Technology Stack.
4-1-T-1	In addition to subcontrols in the ECC control **4-1-3**, the CSP shall cover the following additional subcontrols for third-party cybercurity requirements, as a minimum: 4-1-T-1-1 Management of data integrity with third-party providers.

12. Annexes

Annex No. (A): Terminologies and Definitions

Annex A below shows some of the terminologies contained herein, and the meanings ascribed

Terminology	Definition
Advanced Persistent Threat (APT) Protection	Protection against Advanced Persistent Threats (APT Protection), which aim at unauthorized access to IT systems and networks and residing therein for the longest period possible through avoiding the detection and protection systems. Such means usually use viruses and malware not known before (Zero-Day Malware) to achieve their targets.
Asset	Anything tangible or intangible that has value to the Organization. There are many types of assets, and some of which include obvious things, such as: persons, machineries, utilities, patents, software and services. The term could also include less obvious things, such as: information and characteristics (for example, Organization's reputation and public image, as well as skill and knowledge).
Attack	Any kind of malicious activity that attempts to achieve unauthorized access, collection, disabling, prevention, destroy or sabotage of the information system resources or the information itself.
Audit	Independent review and examination of records and activities in order to assess the effectiveness of cybersecurity controls and to ensure adherence to policies, operational procedures, standards and relevant legislative and regulatory requirements.
Authentication	Ensure user›s identity, process or device, which is often a prerequisite for allowing access to resources in the system.
Authorization	Identification and verification of the rights/licenses of the user to access and allow him/her to view the information and technical resources of the Organization as defined in the rights/user licenses.
Availability	Ensure timely access to information, data, systems and applications.

Backup	Files, devices, data and procedures available for use in case of failure or loss, or in case of deletion or suspension of their original copies.
Bring Your Own Device (BYOD)	This term refers to the policy of the Organization that allows (in part or in whole) its employees to bring their personal devices (laptops, tablets and smartphones) to the premises of the Organization and use such devices to access the networks, information, applications and systems of the Organization which are access-restricted.
CCTV	CCTV, also known as video surveillance, uses video cameras to send a signal to a specific location on a limited set of screens. This term is often referred to as the surveillance technique in areas that may need to be monitored where physical security is an important requirement thereto.
Change Management	It is a service management system that ensures a systematic and proactive approach using effective standard methods and procedures (for example, change in infrastructure, networks, etc.). Change Management helps all stakeholders, including individuals and teams alike, move from their current state to the next desired state, and also helps reduce the impact of relevant incidents on service.
CMDB	Configuration Management DataBase, concept defined originally by the ITIL operations standard and consisting in database used to store configuration records of systems throughout their Lifecycle.
Cloud Technology Stack (CTS)	Disclosure of or obtaining information by unauthorized persons, which are unauthorized to be leaked or obtained, or violation of the cybersecurity policy of the Organization through disclosure, change, sabotage or loss of anything, either intentionally or unintentionally. The expression «security violation» means disclosure of, obtaining, leaking, altering or use of sensitive data without authorization (including cryptographic keys and other critical cybersecurity standards).

Confidentiality	Maintaining authorized restrictions on access to and disclosure of information, including means of protecting privacy/personal information.
Confidential Data/ Information	The information (or data) that is highly sensitive and important, according to the classification of the Organization, intended for use by a specific Organization/Organizations. One of the methods that can be used to classify this type of information is to measure the extent of the damage when it is disclosed, accessed in an unauthorized manner, damaged or sabotaged, as this may result in material or moral damage to the Organization or its clients, affecting the lives of persons related to that information or affecting and damaging the security of the state or its national economy or national capabilities. Sensitive information includes all information whose disclosure in unauthorized manner, loss or sabotage results in accountability or statutory penalties.
Controlled Area Network	Area of the network that supports the Cloud Technology Stack, isolated from the rest of the enterprise with controlled access
Critical National Infrastructure (CNI)	These are the assets (i.e. facilities, systems, networks, processes, and key operators who operate and process them), whose loss or vulnerability to security breaches may result in: • Significant negative impact on the availability, integration or delivery of basic services, including services that could result in serious loss of property and/or lives and/or injuries, alongside observance of significant economic and/or social impacts. • Significant impact on national security and/or national defense and/or state economy or national capacities.
Cryptography	These are the rules that include the principles, methods and means of storing and transmitting data or information in a particular form in order to conceal its semantic content, prevent unauthorized use or prevent undetected modification so that only the persons concerned can read and process the same.

Cyber-Attack	Intentional exploitation of computer systems and networks, and those organizations whose work depends on digital ICT, in order to cause damage.
Cyber Risks	Risks that harm the Organization's processes (including the Organization's vision, mission, management, image or reputation), assets, individuals, other organizations or the State due to unauthorized access, use, disclosure, disruption, modification or destruction of information and/or information systems.
Cybersecurity Resilience	Overall ability of the Organization to withstand cyber incidents and the causes of damage, and recovery therefrom.
Cybersecurity	Pursuant to the provisions of NCA's Regulation issued by virtue of the Royal Decree No. (6801) of (11/02/1439), cybersecurity is protection of networks, IT systems, operational technologies systems and their components of hardware and software, their services and the data they contain, from any penetration, disruption, modification, access, use or unauthorized exploitation. The concept of cybersecurity also includes information security, digital security, etc.
Cyberspace	The interconnected network of IT infrastructure, including the Internet, communications networks, computer systems and Internet-connected devices, as well as the associated hardware and control devices. The term can also refer to a virtual world or domain such as a simple concept.
Data and Information Classification	Setting the sensitivity level of data and information that results in security controls for each level of classification. Data and information sensitivity levels are set according to predefined categories where data and information is created, modified, improved, stored or transmitted. The classification level is an indication of the value or importance of the data and information of the Organization.

Data Archiving	The process of transmitting data that is no longer effectively used in a separate storage device for long-term preservation. Archived data consists of old data that is still relevant to the Organization and may be required for future reference thereto as well as data that must be retained to comply with relevant legislation and regulations.
Defense-in-Depth	This is a concept of information assurance where multiple levels of security controls are used (as a defense) within the IT/OT system.
Disaster Recovery	Programs and plans designed to restore the Organization's critical business functions and services to an acceptable situation, following exposure to cyber-attacks or disruption of such services.
Domain Name System (DNS)	A technical system that uses a database distributed over the network and/or the Internet that allows the transmitting of domain names to IP addresses, and vice-versa in order to identify service addresses such as web and e-mail servers.
Effectiveness	Effectiveness refers to the degree to which a planned impact is achieved. Planned activities are considered effective if these activities are already implemented, and the planned results are considered effective if the results are already achieved. KPIs can be used to measure and evaluate the level of effectiveness.
Efficiency	The relationship between the results achieved (outputs) and the resources used (inputs). The efficiency of the process or system can be enhanced by achieving more results using the same resources (inputs) or even less.
Event	Something that happens in a specific place (such as network, systems, applications, etc.) at a specific time.

FedRAMP	US Government assessment and authorization process for U.S. federal agencies designed to ensure security is in place when accessing cloud computing products and services. FedRAMP certifies cloud service providers to handle data in one of three impact levels: • FedRAMP Low - loss of confidentiality, integrity, and availability would result in limited adverse effects on an agency's operations, assets, or individuals. • FedRAMP Moderate - loss of confidentiality, integrity, and availability would result in serious adverse effects on an agency's operations, assets, or individuals. • FedRAMP High - Law Enforcement and Emergency Services systems, Financial systems, Health systems, and any other system where loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Hyper Text Transfer Protocol Secure (HTTPS)	A protocol that uses encryption to secure web pages and data when they are transmitted over the network. It is a secure version of the Hypertext Text Transfer Protocol (HTTP).
Identification	A means for identification of the identity of the user, process or device, which is usually a prerequisite for granting access to resources in the system.
Incident	A security breach through violation of cybersecurity policies, acceptable use policies, practices or cybersecurity controls or requirements.
Information Spillage	Information spillage refers to instances where either classified or sensitive information is inadvertently placed on information systems that are not authorized to process such information. Such information spills often occur when information that is initially thought to be of lower sensitivity is transmitted to an information system and then is subsequently determined to be of higher sensitivity. At that point, corrective action is required.
Integrity	Protection against unauthorized modification or destruction of information, including ensuring information non-repudiation and reliability.

(Inter)National Requirements	The international requirements are requirements developed by an international organization or organization, which are highly-used in a statutory manner all over the world (such as: PCI, SWIFT, etc.). The national requirements are requirements developed by a regulatory Organization within the KSA for statutory use (such as: the "ECC – 1: 2018".
Intrusion Prevention System (IPS)	A system with intrusion detection capabilities, as well as the ability to prevent and stop suspicious or potential incidents.
Key Performance Indicator (KPI)	A type of performance measurement tool that assesses the success of an activity or Organization towards achievement of specific objectives.
Labelling	Display of information (by specific and standard naming and coding) that is placed on the Organization's assets (such as devices, applications, documents, etc.) to be used to refer to some information related to the classification, ownership, type and other asset management information.
Least Privilege	A basic principle in cybersecurity that aims at giving users the powers of access they need to carry out their official responsibilities ONLY.
Malware	A program that infects systems in a hidden way (mostly) for violating the confidentiality, accuracy, or availability of data, applications or operating systems.
Multi-Factor Authentication (MFA)	A security system that verifies user identity, which requires the use of several separate elements of identity verification mechanisms. Verification mechanisms include several elements: • Knowledge: (something ONLY the user knows «like password»); • Possession: (something ONLY used by the user «such as a program or device generating random numbers or SMSs for login records, which are called: One-Time-Password); and • Inherent Characteristics: (a characteristic of the user ONLY, such as fingerprint).
Multi-tier Architecture	An architecture or structure to which a client-server approach is applied, in which the functional process logic, data access, data storage and user interface are developed and maintained as separate units on separate platforms.

Need-to-Know and Need-to-Use	Limitations on the data which are sensitive unless a person has a specific need to see the data for a purpose related to formal functions and tasks.
Offline/Offsite Backup	A backup database, system, application and hardware settings when the version is offline and not updatable. Tapes are usually used in the case of an offsite backup.
Online Backup	A method of storage that is regularly backed-up over a network on a distant server (either within the Organization's network or hosted by a CSP).
Organization Staff	Persons working in the Organization (including official and temporary staff and contractors).
Outsourcing	Obtaining (goods or services) by contracting with a supplier or service provider.
Update and Repair Patch	Supporting data patches for update, repair or improvement of the computer operating system, applications or software. This includes repairing security vulnerabilities and other errors. Such patches are usually called repairs or repairing of errors and improvement of usability or performance.
Penetration Testing	Testing a computer system, network, website application or smart phone application to look for the vulnerabilities that the attacker can exploit.
Phishing Emails	Attempting to obtain sensitive information such as usernames, passwords or credit card details, often for malicious reasons and intentions by disguising themselves as trustworthy organizations in email messages.
Physical Security	Physical security describes security measures designed to prevent unauthorized access to the Organization's facilities, equipment and resources, and to protect individuals and property from damage or harm (such as espionage, theft or terrorist attacks). Physical security involves the use of multiple-tier of interconnected systems, including CCTV, security guards, security limits, locks, access control systems and many other technologies.

Policy	A document whose clauses specify a general obligation, direction or intent as formally expressed by the Authorizing Official of the Organization. Cybersecurity Policy is a document whose clauses reflect official commitment of the Senior Management to implement and improve the cybersecurity program in the Organization, which includes the objectives of the Organization regarding the cybersecurity program, its controls and requirements, and the mechanism for improving and developing the same.
Privacy	Freedom from unauthorized interference or disclosure of personal information about an individual.
Privileged Access Management	The process of managing high-risk powers on Organization›s systems, which often require special treatment to minimize risks that may arise from misuse thereof.
Procedure	A document with a detailed description of the steps necessary to perform specific operations or activities in compliance with relevant standards and policies. Procedures are defined as part of operations.
Process	A set of interrelated or interactive activities that translated input into output. Such activities are influenced by the policies of the Organization.
RACI Matrix	Responsible, Accountable, Consulted, Informed Matrix. Matrix that maps each player in a process, capability or function with the degree of involvement and responsibility undertaken in the process.
Recovery	A procedure or process to restore or control something that is suspended, damaged, stolen or lost.
Retention	The length of time that information, data, event logs or backups shall be retained, regardless of the form (paper, electronic, etc.).
Secure Coding Standards	A practice for the development of computer software and applications in a way that protects against the unintended exposure to Cybersecurity vulnerabilities related to software and applications.

Secure Configuration and Hindering	Protecting, immunizing and adjusting computer settings, system, application, network device and security device for resisting cyber-attacks, such as: stopping or changing factory and default accounts, stopping of unused services and unused network ports.
Security Information and Event Management (SIEM)	A system that manages and analyses security events logs in real time in order to provide monitoring of threats, analysis of the results of interrelated rules for event logs and reports on logs data, and incident response.
Security Testing	A process designed to ensure that the system or the modified/ new application that includes appropriate security controls and protections and does not contain any security vulnerabilities that may damage other systems or applications, or lead to misuse of the system, application or information, as well as maintaining the function of the system or application as intended.
Security-by-Design	A methodology for developing systems and applications and designing of networks that seek to make them free of cyber vulnerabilities, and the ability to repel cybersecurity as much as possible through several measures, for example: continuous testing, protection of authentication and adherence to best programming and design practices, and others.
Segregation of Duties	A fundamental principle in cybersecurity aimed at reducing errors and fraud during the stages of the implementation of a specific operation by making sure that there is more than one person to complete such stages and with different powers.
Sender Policy Framework	A method to verify that the email server used to send email messages follows the domain of the sender.
System Development Security	Any application, platform, middleware, operating system, hypervisor, network stack and any other software that is part of the Cloud Technology Stack
Third-Party	Any Organization acting as a party in a contractual relationship to provide goods or services (this includes suppliers and service providers).

Threat	Any circumstance or events likely to adversely affect the business of the Organization (including its mission, functions, credibility or reputation), assets or employees, through exploiting an information system through unauthorized access to, destruction, disclosure, alteration or denial of services, in addition to the ability of the threat source to succeed in exploiting one of the vulnerabilities of a particular information system, which includes cyber threats.
Threat Intelligence	Provides organized information and analysis of recent, current and potential attacks that could pose a cyber threat to the Organization.
Vulnerability	Any kind of vulnerability in the computer system, its programs or applications, in a set of procedures or anything that makes cybersecurity vulnerable.
Web Application Firewall	A protection system that is developed before web applications in order to minimize the risks resulting from attacks on the web applications.
Zero-Day Malware	Malware is a previously unknown, newly produced or deployed software, which are usually difficult to detect by means of protection based on prior knowledge of malicious software (Signature-based Protection).
Person	Any natural or legal person(such as companies).
Organization	Any government organization in the Kingdom of Saudi Arabia (including ministries, authorities, establishments and others) and its companies and entities, as well as private sector organizations owning, operating or hosting Critical National Infrastructures (CNIs).
Cloud Customer	In this document reffered to as “Cloud Service Tenant (CST)”, is any person who subscribes to the cloud services provided by the service provider.
Cloud Service Provider	Anyone who provides cloud computing services to the public, either directly or indirectly through data centers (both inside and outside KSA) and manages them in whole or in part.
Data	Any information, records, statistics or documents that are photo-copied, recorded and stored electronically.

Cloud computing	Is a model which enables convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud models are composed of five Essential Characteristics: On-demand self-service, Broad network access, Resource pooling, Rapid elasticity, and Measured service. There are three types of cloud computing services delivery models: • Cloud Software as a Service (SaaS), • Cloud Platform as a Service (PaaS), • Cloud Infrastructure as a Service (IaaS). There are four deployment models: Private Cloud, Community Cloud, Public Cloud, and Hybrid Cloud.
Classification	Categorizing the data prepared, collected, processed, or exchanged by the public organizations for the provision of services or conduct of businesses, including data received from or exchanged with persons outside public organizations, and the data that is prepared for the interest of public organizations or related to the sensitive infrastructure. Data related to public organizations is classified, using a top down approach, level 1, level 2, level 3, or level 4.
Level 1	A classification level applies to data classified as a (top secret) based on what is issued by the competent organization.
Level 2	A classification level applies to data classified as a (secret) based on what is issued by the competent organization.
Level 3	A classification level applies to data classified as a (restricted) based on what is issued by the competent organization, and level 3 is the lowest level for hosting sensitive systems and the data it contains.
Level 4	A classification level applies to data classified as a (open) based on what is issued by the competent organization.
Classified Data	Any data classified at any of the following levels: level 1, level 2, level 3, or level 4.

Annex No. (B): List of the Abbreviations

Annex B below shows some of the abbreviations, and their meanings, used in the controls herein.

Abb.	Full Version
BCM	Business Continuity Management
BYOD	Bring Your Own Device
CCC	Cloud Cybersecurity Controls
CCTV	Closed-Circuit Television
CMDB	Configuration Management DataBase
CNI	Critical National Infrastructure
DNS	Domain Name System
ECC	Essential Cybersecurity Controls
HTTPS	Hyper Text Transfer Protocol Secure
ICS	Industrial Control System
ICT	Information and Communication Technology
IT	Information Technology
MFA	Multi-Factor Authentication
OT	Operational Technology
SIEM	Security Information and Event Management
SIS	Safety Instrumented System
SLA	Service Level Agreement
CTS	Cloud Technology Stack
CTS	Cloud Technology Stack

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority