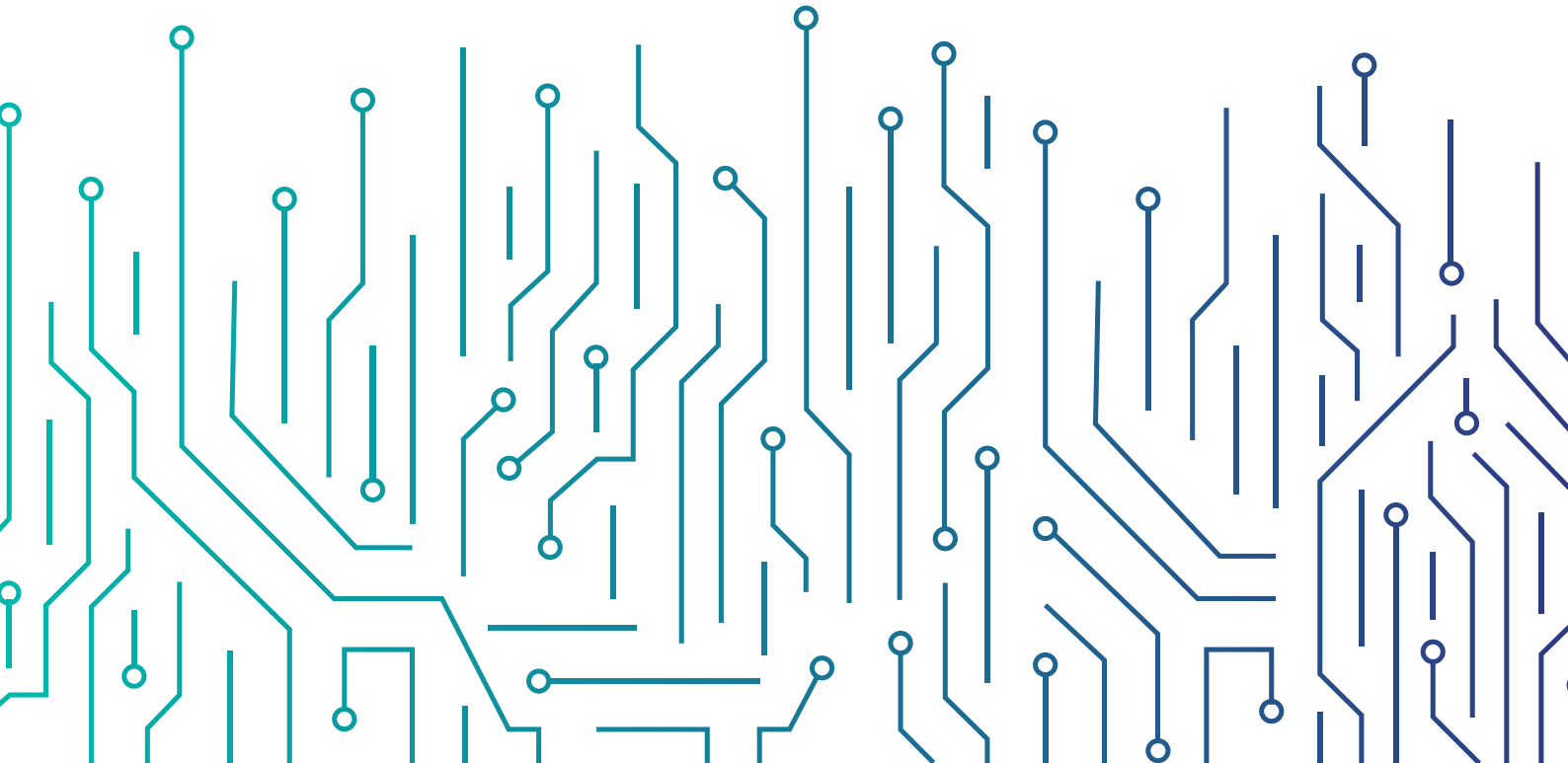
الهيئة الوطنية للأمن السيبـراني
National Cybersecurity Authority

Cloud Cybersecurity Controls

(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

List of the Figures and Illustrations

List of Tables

1. Executive Summary

NCA's mandates and duties fulfill the regulatory cybersecurity needs related to the development of cybersecurity national policies, governance mechanisms, frameworks, standards, controls and guidelines, 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 the Kingdom of Saudi Arabia which results in a new cybersecurity risks that require cybersecurity controls to transact with cloud services taking into consideration international common practices in this field; and to be an extension to the already published Essential Cybersecurity Controls (ECC-1: 2018).

As a result, the Cloud Cybersecurity Controls (CCC – 1: 2020) is developed to minimize the cybersecurity risks of Cloud Service Providers (CSPs), and Cloud Customers, also known as Cloud Service Tenants (CSTs). This document highlights the details of the cloud cybersecurity controls 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 (referred to in this document as "The Authority" or "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 and controls such as US FedRAMP (the number of FedRAMP requirements ranges from 125 to 421), Multi-Tier Cloud Security Standard for Singapore (MTCS SS) which contains 535 requirements, Germany C5 which contains 114 requirements, Cloud Controls Matrix (CCM) which contains 133 controls, and ISO/IEC 27001 which contains 114 controls. Details of this mapping is represented in a separate document extended to the CCC.

Cloud Cybersecurity Controls Components

The cloud cybersecurity controls consist of the following:

<table>
<tr><th>For CSPs</th><th>For CSTs</th></tr>
<tr><td colspan="2">4 Main Domains</td></tr>
<tr><td colspan="2">24 Subdomains</td></tr>
<tr><td>37 Main Controls</td><td>18 Main Controls</td></tr>
<tr><td>96 Subcontrols</td><td>26 Subcontrols</td></tr>
</table>

Figure 1: Cloud Cybersecurity Controls Components

3. Objectives

The Cloud Cybersecurity Controls (CCC – 1: 2020) is developed as an extension to the ECC; to achieve higher levels of national cybersecurity goals by focusing on cloud computing services from the perspective of Cloud Service Providers (CSPs) and Cloud Service Tenants (CSTs). Also, the CCC aims to set the minimum requirements for cybersecurity of cloud computing, for both CSPs and CSTs, to contribute to enable the CSPs and the CSTs to provide and use secure cloud computing services and mitigating cyber risks against them.

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 take into consideration the following four main cybersecurity pillars:

- Strategy
- People
- Procedures
- Technology

4. Scope of Work and Applicability

Scope of Work of the CCC

The cybersecurity controls shall apply to the CSPs and CSTs. These controls represent the minimum cybersecurity requirements for cloud computing.

CSPs within the scope of CCC are any CSP which provides cloud computing services to the CSTs within the scope of work. CSTs within the scope of CCC are any government organization in the Kingdom of Saudi Arabia inside or outside the Kingdom (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) that currently use or planning to use any cloud service.

The cybersecurity controls shall apply to the CSPs and CSTs. These controls represent the minimum cybersecurity requirements for cloud computing.

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

Examples of CSPs outside Scope of Work

- CSPs who provide cloud computing services for non-saudi organizations outside KSA, and not provided services to CSTs within scope of work.
- CSPs who provide cloud computing services for individuals, and private sector organizations not owning, operating or hosting Critical National Infrastructures (CNIs), and not provided services to CSTs within scope of work.

CCC Statement of Applicability

The ECC and the CCC have been developed after taking into consideration the cybersecurity needs of CSPs and CSTs, and every CSP and CST must comply with all applicable controls.

5. Implementation and Compliance

To comply with item 3 of article 10 of NCA's mandate and as per the Royal Decree number 57231, all CSPs and CSTs within the scope of these controls must implement whatever necessary to ensure continuous compliance with the CCC according to the levels shown in Table (2) and Table (3) in section "Annex No. (A): Cloud Cybersecurity Controls Levels" in this document, taking into account the following two rules:

1. CST's controls in the CCC are an extension and complement to the controls in the ECC; therefore the CSTs must ensure continuous compliance with the controls in both ECC and CCC.
2. CSP's controls in the CCC are an extension and complement to the controls in the ECC; therefore the CSPs – within or outside the scope of the ECC- must ensure continuous compliance with the controls in both ECC and CCC.

NCA will give CSPs and CSTs within the scope of work a compliance period to comply with the CCC (taking into account CSPs and CSTs who move from outside the scope to within the scope of work) as deemed appropriate by NCA. Also, NCA evaluates CSPs and CSTs compliance with the CCC in accordance with the mechanisms deemed appropriate by NCA; such as self-assessment of CSPs and CSTs, and/or external compliance assessment by NCA or designated third-parties.

6. Cloud Cybersecurity Controls 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 cloud cybersecurity controls methodology and mapping annex 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.
- Control Applicability on different Cloud Service Models (IaaS, PaaS, and SaaS).

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. Cloud Cybersecurity Controls Domains and Structure

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

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

Figure 2: Main Domains and Subdomains of Cloud Cybersecurity Controls

9. CCC Documentation Structure

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

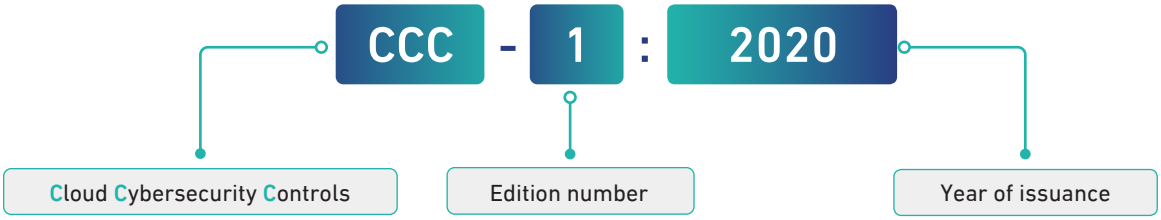


Figure 3: CCC Identification Notation

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

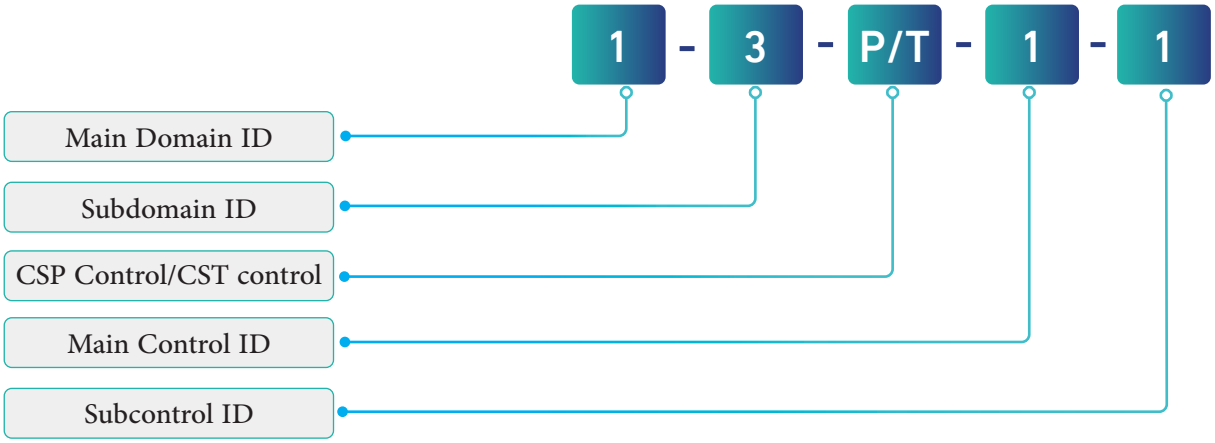


Figure 4: Controls Unique Identifier Structure

CSP and CST controls have common main domains and subdomains, that are differentiated on the third identification tier, and have their own main control and subcontrol identification notation sequences. CSPs will have an identification notation structure like '1-3-P-1-1' in the figure. CSTs will have an identification notation structure like '1-3-T-1-1'. CCC uses the following:

- 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").
- The green coloured numbers (such as: **1-3-2**) are reference numbers to subdomains or controls of ECC.

Cloud Cybersecurity Controls Documentation

Table (1) below shows the methodological structure of the controls.

	Name of Main Domain
Reference number of the Main Domain	
Reference number of the Subdomain	Name of Subdomain
Objective	
Controls	
Conrol Reference Number	Control clauses

Table 1. CCC Structure

10 Cloud Cybersecurity Controls

Details of Cloud Cybersecurity Controls:

1 Cybersecurity Governance

1-1	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	
1-1-P-1	In addition to the ECC control 1-4-1, the Authorizing Official shall also identify, document and approve: 1-1-P-1-1 Cybersecurity roles and RACI assignment for all stakeholders of the cloud services including Authorizing Official's roles and responsibilities.
1-1-T-1	In addition to the ECC control 1-4-1, the Authorizing Official shall also identify, document and approve: 1-1-T-1-1 Cybersecurity roles and RACI assignment for all stakeholders of the cloud services including Authorizing Official's roles and responsibilities.
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 Defining acceptable risk levels for the cloud services, and clarifying them to the CST if they are related to the CST. 1-2-P-1-2 Considering data and information classification in cybersecurity risk management methodology. 1-2-P-1-3 Developing cybersecurity risk register for cloud services, and monitoring it periodically according to the risks.

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 Defining acceptable risk levels for the cloud services. 1-2-T-1-2 Considering data and information classification accredited by CST in cybersecurity risk management methodology. 1-2-T-1-3 Developing cybersecurity risk register for cloud services, and monitoring it periodically according to the risks.
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 Continuous compliance with all laws, regulations, instructions, decisions, regulatory frameworks and controls, and mandates regarding cybersecurity in KSA.
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 Continuous or real-time compliance monitoring of the CSP with relevant cybersecurity legislation and contract clauses.
1-4	**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	
1-4-P-1	In addition to subcontrols in the ECC controls 1-9-3 and 1-9-4, the following requirements should be covered prior and during the professional relationship of personnel with the CSP as a minimum: 1-4-P-1-1 Positions of cybersecurity functions in CSP's data centers within the KSA must be filled with qualified and suitable Saudi nationals. 1-4-P-1-2 Screening or vetting candidates of personnel working inside KSA who have access to Cloud Technology Stack, periodically.

	1-4-P-1-3 Cybersecurity policies as a prerequisite to access to Cloud Technology Stack, signed and appropriately approved.
1-4-P-2	In addition to subcontrols in the ECC control 1-9-5, the following requirements should be in place, as a minimum, for the termination/completion of a human resource's professional relationship with the CSP: 1-4-P-2-1 Assurance that assets owned by the organization (especially those with security exposure) are accounted for and returned upon termination.
1-4-T-1	In addition to subcontrols in the ECC control 1-9-3, the following requirements should be covered prior the professional relationship of staff with the CST shall cover, at a minimum: 1-4-T-1-1 Screening or vetting candidates of personnel with access to Cloud Service sensitive functions (Key Management, Service Administration, Access Control).
1-5	**Cybersecurity in Change Management**
Objective	To ensure that cybersecurity requirements are included in change management methodology and procedures in order to protect the confidentiality, integrity and availability of information and technology assets as per CSPs policies and procedures, and related laws and regulations.
Controls	
1-5-P-1	Cybersecurity requirements for change management within the CSP shall be identified, documented and approved.
1-5-P-2	Cybersecurity requirements for change management within the CSP shall be applied.
1-5-P-3	Cybersecurity for change management in the CSP shall cover, as a minimum: 1-5-P-3-1 Processes and procedures to securely implement changes (planned works) in production systems, with priority given to cybersecurity observations. 1-5-P-3-2 Process for the implementation of cybersecurity exceptional changes (e.g.: changes during incident restoration).
1-5-P-4	Cybersecurity requirements for change management within the CSP 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 Identifying assets owners and involving them in the asset management lifecycle.
2-1-T-1	In addition to controls in the ECC control 2-1, the CST shall cover the following additional controls for cybersecurity requirements for cybersecurity event logs and monitoring management, as a minimum: 2-1-T-1-1 Inventory of all cloud services and information and technology assets related to the cloud services.
2-2	**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	
2-2-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: 2-2-P-1-1 Identity and access management of generic accounts credentials for accountability cannot be assigned for a specific individual. 2-2-P-1-2 Secure session management, including session authenticity, session lockout, and session timeout termination.

	2-2-P-1-3	Multi-factor authentication for privileged users, and candidates of personnel with access to Cloud Technology Stack.
	2-2-P-1-4	Formal process to detect and prevent unauthorized access (e.g. unsuccessful login attempt threshold).
	2-2-P-1-5	Utilizing secure methods and algorithms for saving and processing passwords, such as: Secure Hashing functions.
	2-2-P-1-6	Secure management of third party personnel's accounts.
	2-2-P-1-7	Access control enforced to management systems, administrative consoles.
	2-2-P-1-8	Masking of displayed authentication inputs, especially passwords, to prevent shoulder surfing.
	2-2-P-1-9	Getting CST's approval before accessing any CST-related asset by the CSP or CSP's third parties.
	2-2-P-1-10	Capability to immediately interrupt a remote access session and prevent any future access for a user.
	2-2-P-1-11	Provision to CSTs of Multi-factor authentication services for privileged cloud users.
	2-2-P-1-12	Assurance of restricted and controlled access to storage systems and means (such as Storage Area Network (SAN)).
2-2-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:	
	2-2-T-1-1	Identity and access management for all cloud credentials along their full lifecycle.
	2-2-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).
	2-2-T-1-3	Secure session management, including session authenticity, session lockout, and session timeout termination on the cloud.
	2-2-T-1-4	Multi-factor authentication for privileged cloud users.
	2-2-T-1-5	Formal process to detect and prevent unauthorized access to cloud (such as a threshold of unsuccessful login attempts).

2-3	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	
2-3-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: 2-3-P-1-1 Ensuring that all configurations are applied in accordance to CSP's cybersecurity standards. 2-3-P-1-2 Assurance of separation and isolation of data, environments and information systems across CSTs, to prevent data commingling. 2-3-P-1-3 Adopting of cybersecurity principles for technical system configurations adhering to the minimum functionality principle. 2-3-P-1-4 Ability of the Cloud Technology Stacks to securely handle input validation, exceptions and failure. 2-3-P-1-5 Full isolation of security functions and applications from other functions and applications in the Cloud Technology Stack. 2-3-P-1-6 Notification to CSTs with cybersecurity requirements provided by the CSP that are useable by the CST. 2-3-P-1-7 Detection and prevention of unauthorized changes to softwares, and systems. 2-3-P-1-8 Complete isolation and protection of multiple guest environments. 2-3-P-1-9 The community cloud services provided to CSTs (government organizations and CNI organizations) shall be isolated from any other cloud computing provided to organizations outside the scope of work. 2-3-P-1-10 Provide cloud computing services from within the KSA, including systems used for storage, processing, and disaster recovery centers. 2-3-P-1-11 Provide cloud computing services from within the KSA, including systems used for monitoring, and support. 2-3-P-1-12 Modern technologies, such as Endpoint Detection and Response (EDR) technologies, to ensure that the information servers and devices of CSP's information processing systems and devices of are ready for rapid response to incidents.

2-3-T-1	In addition to subcontrols in the ECC control 2-3-3, the CST shall cover the following additional subcontrols for cybersecurity requirements for information system and processing facilities protection requirements, as a minimum: 2-3-T-1-1 Verifying that the CSP isolates the community cloud services provided to CSTs (government organizations and CNI organizations) from any other cloud computing provided to organizations outside the scope of work.
2-4	**Networks Security Management**
Objective	To ensure the protection of CSP's and CST's network from cyber risks.
Controls	
2-4-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: 2-4-P-1-1 Monitoring of traffic across the external and internal networks to detect anomalies. 2-4-P-1-2 Network isolation and protection of Cloud Technology Stack network from other internal and external networks. 2-4-P-1-3 Protection from denial of service attacks (including Distributed Denial of Service (DDoS)). 2-4-P-1-4 Protection of data transmitted through the network; from and to the Cloud Technology Stack network using cryptography primitives; for management and administrative access. 2-4-P-1-5 Access control between different network segments. 2-4-P-1-6 Isolation between cloud service delivery network, cloud management network and CSP enterprise network.
2-4-T-1	In addition to subcontrols in the ECC control 2-5-3, the CST shall cover the following additional subcontrols for cybersecurity requirements for networks security management requirements, as a minimum: 2-4-T-1-1 Protecting the connection channel with CSP.
2-5	**Mobile Devices Security**
Objective	To ensure the protection of mobile devices (including laptops, smartphones, and tablets) from cyber risks and to ensure the secure handling of the CSPs' and CSTs' information (including sensitive information) while utilizing mobile devices.
Controls	

2-5-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: 2-5-P-1-1 Inventory of all end user and mobile devices. 2-5-P-1-2 Centralized mobile device security management. 2-5-P-1-3 Screen locking for end user devices. 2-5-P-1-4 Data sanitation and secure disposal for end-user devices, especially for those with exposure to the Cloud Technology Stack.
2-5-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: 2-5-T-1-1 Data sanitation and secure disposal for end-user devices with access to the cloud services.
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 Prohibiting the use of Cloud Technology Stack's data in any environment other than production environment, except after applying strict controls for protecting that data, such as: data masking or data scrambling techniques. 2-6-P-1-2 Provision to CSTs of securely data storage processes, procedures, and technologies to comply with related legal and regulatory requirements. 2-6-P-1-3 Disposal of CST's data should be performed in a secure manner on termination or expiry of the contract with the CSP. 2-6-P-1-4 Commitment to maintain the confidentiality of the CST's data and information, according to related legal and regulatory requirements. 2-6-P-1-5 Providing CSTs with secure means to export and transfer data and virtual infrastructure
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 protecting CST's data and information in cloud computing , as a minimum:

	2-6-T-1-1	Exit Strategy to ensure means for secure disposal of data on termination or expiry of the contract with the CSP.
	2-6-T-1-2	Using secure means to export and transfer data and virtual infrastructure.
2-7	**Cryptography**	
Objective	To ensure the proper and efficient use of cryptography to protect information assets as per policies, procedures, and related laws and regulations.	
Controls		
2-7-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:	
	2-7-P-1-1	Technical mechanisms and cryptographic primitives for strong encryption, in according to the advanced level in the National Cryptographic Standards (NCS-1:2020).
	2-7-P-1-2	Certification authority and issuance capability in a secure manner, or usage of certificates from a trusted certification authority.
2-7-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:	
	2-7-T-1-1	Technical mechanisms and cryptographic primitives for strong encryption, in according to the advanced level in the National Cryptographic Standards (NCS-1:2020).
	2-7-T-1-2	Encryption of data and information transferred to or transferred out of the cloud according to the relevant law and regulatory requirements.
2-8	**Backup and Recovery Management**	
Objective	To ensure the protection of CSPs' data and information including information systems and software configurations from cyber risks as per organizational policies and procedures, and related laws and regulations.	
Controls		
2-8-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:	
	2-8-P-1-1	Securing access, storage and transfer of CST's data backups and its mediums, and protecting it against damage, amendment or unauthorized access.
	2-8-P-1-2	Securing access, storage and transfer of Cloud Technology Stack backups and its mediums, and protecting it against damage, amendment or unauthorized access.

2-9	Vulnerabilities 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	
2-9-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: 2-9-P-1-1 Assessing and remediating vulnerabilities on external components of Cloud Technology Stack at least once every month, and at least once every three months for internal components of Cloud Technology Stack. 2-9-P-1-2 Notification to CSTs of identified vulnerabilities that may affecting them, and safeguards in place.
2-9-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: 2-9-T-1-1 Assessing and remediating vulnerabilities cloud services and at least once every three months. 2-9-T-1-2 Management of CSP-notified vulnerabilities safeguards in place.
2-10	**Penetration Testing**
Objective	To assess and evaluate the efficiency of the CSP's cybersecurity defense capabilities through simulated cyber-attacks to discover unknown weaknesses within the technical infrastructure that may lead to a cyber breach.
Controls	
2-10-P-1	In addition to subcontrols in the ECC control 2-11-3, the CSP shall cover the following additional subcontrols for cybersecurity requirements for penetration testing, as a minimum: 2-10-P-1-1 Scope of penetration tests must cover Cloud Technology Stack and must be conducted at least once every six months.
2-11	**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	
2-11-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: 2-11-P-1-1 Activating and protecting event logs and audit trails of Cloud Technology Stack. 2-11-P-1-2 Activating and collecting of login attempts history. 2-11-P-1-3 Activating and protecting all event logs of activities and operations performed by the CSP at the tenant level in order to support forensic analysis. 2-11-P-1-4 Protecting cybersecurity event logs from alteration, disclosure, destruction and unauthorized access and unauthorized release, in accordance with regulatory, or law requirements. 2-11-P-1-5 Continuous cybersecurity events monitoring using SIEM technique covering the full Cloud Technology Stack. 2-11-P-1-6 Reviewing cybersecurity event logs and audit trails periodically, covering CSP events in the Cloud Technology Stack. 2-11-P-1-7 Automated monitoring and logging of remote access sessions event logs. 2-11-P-1-8 Secure handling of user-related data found in the audit trails and the cybersecurity event logs.
2-11-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: 2-11-T-1-1 Activating and collecting of login event logs, and cybersecurity event logs on assets related to cloud services. 2-11-T-1-2 Monitoring shall include all activated cybersecurity logs on the cloud services of the CST.
2-12	**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 CSPs.
Controls	
2-12-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:

	2-12-P-1-1	Subscribing in authorized and specialized organizations and groups to stay up-to-date on cybersecurity threats, common practices and key know-how.
	2-12-P-1-2	Training for employees and third-party personnel to respond to cybersecurity incidents, in line with their roles and responsibilities.
	2-12-P-1-3	Periodically testing the incident response capability.
	2-12-P-1-4	Root Cause Analysis of cybersecurity incidents and developing plans to address them.
	2-12-P-1-5	Support the CST in cases legal proceedings and forensics, protecting the chain of custody that falls under the management and responsibility of the CSP, in accordance with the related law and regulatory requirements.
	2-12-P-1-6	Real-time reporting to the CST of incidents that may affect CST; if the incident is discovered.
	2-12-P-1-7	Support for CSTs to handle security incidents according to the agreement between the CSP and CST.
	2-12-P-1-8	Measuring and monitoring cybersecurity incident metrics and monitor compliance with contracts and legislative requirements
2-13	**Physical Security**	
Objective	To ensure the protection of CSPs' information and technology assets from unauthorized physical access, loss, theft and damage.	
Controls		
2-13-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:	
	2-13-P-1-1	Continual monitoring of access to CSP's sites and buildings.
	2-13-P-1-2	Preventing unauthorized access to devices in the Cloud Technology Stack.
	2-13-P-1-3	Disposal of cloud infrastructure hardware, in particular, storage equipment (external or internal), by adopting relevant legislation and best practices.
2-14	**Web Application Security**	
Objective	Ensure the protection of external web applications of the CSP from cyber risks.	
Controls		
2-14-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:	

	2-14-P-1-1	Protecting information involved in application service transactions against possible risks (e.g.: incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure….).
2-15	**Key Management**	
Objective	Ensure secure management of CSPs' and CSTs' 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 applied.	
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 for cryptographic keys.
	2-15-P-3-2	A secure cryptographic key retrieval mechanism in case of cryptographic key lost (such as backup of keys and enforcement of trusted key storage, strictly external to cloud).
	2-15-P-3-3	Activating 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 for cryptographic keys.
	2-15-T-3-2	A secure data retrieval mechanism in case of cryptographic encryption key lost (such as backup of keys and enforcement of trusted key storage, strictly external to cloud).
2-15-T-4	Cybersecurity requirements for key management within the CST shall be applied and reviewed periodically.	
2-16	**System Development Security**	
Objective	Ensure CSPs' systems are developed, integrated and deployed in a secure manner.	
Controls		

2-16-P-1	Cybersecurity requirements for system development within the CSP shall be identified, documented and approved.
2-16-P-2	Cybersecurity requirements for system development within the CSP shall be applied.
2-16-P-3	Cybersecurity requirements for system development within the CSP shall include as a minimum the following controls along the development lifecycle: 2-16-P-3-1 Considering cybersecurity requirements of the Cloud Technology Stack and relevant systems in the design and implementation of the cloud computing services. 2-16-P-3-2 Protecting system development environments, testing environments (including data used in testing environment), and integration platforms.
2-16-P-4	Cybersecurity requirements for system development within the CSP shall be applied and reviewed periodically.
2-17	**Storage Media Security**
Objective	Ensure CSPs' secure handling of information and data on physical media.
Controls	
2-17-P-1	Cybersecurity requirements for usage of information and data media within the CSP shall be identified, documented and approved.
2-17-P-2	Cybersecurity requirements for usage of information and data media within the CSP shall be applied.
2-17-P-3	Cybersecurity requirements for usage of information and data media within the CSP shall cover, at minimum, the following: 2-17-P-3-1 Enforcement of sanitization of media, prior to disposal or reuse. 2-17-P-3-2 Using secure means when disposing of media. 2-17-P-3-3 Provision to maintain confidentiality and integrity of data on removable media. 2-17-P-3-4 Human readable labelling of media, to explain its classification and the sensitivity of the information it contains. 2-17-P-3-5 Controlled and physically secure storage of removable media. 2-17-P-3-6 Restriction and control of usage of portable media inside the Cloud Technology Stack.
2-17-P-4	Cybersecurity requirements for usage of information and data media within the CSP shall be applied and reviewed periodically.

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 Developing and implementing disaster recovery and business continuity procedures in a secure manner. 3-1-P-1-2 Developing and implementing procedures to ensure resilience and continuity of cybersecurity systems dedicated to the protection of Cloud Technology Stack.
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 Developing and implementing disaster recovery and business continuity procedures related to cloud computing, in a secure manner.

4 Third party Cybersecurity

4-1	Supply Chain and Third-Party Cybersecurity
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 implementing the ECC controls 4-1-2 and 4-1-3, the CSP shall cover the following additional subcontrols for third-party cybersecurity requirements, as a minimum: 4-1-P-1-1 Ensure that the CSP fulfills NCA's requests to remove software or services, provided by third-party providers that may be considered a cybersecurity threat to national organizations, from the marketplace provided to CSTs. 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 Third party providers compliant with law and regulatory requirements relevant to their scope. 4-1-P-1-4 Risk management and security governance on third-party providers as part of general cybersecurity risk management and governance.

11. Annexes

Annex No. (A): Cloud Cybersecurity Controls Levels

Cybersecurity controls 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 authority.
- **Level 2:** A classification level applies to data classified as a (secret) based on what is issued by the competent authority.
- **Level 3:** A classification level applies to data classified as a (confidential) based on what is issued by the competent authority.
- **Level 4:** classification level applies to data classified as a (public) based on what is issued by the competent authority.

Please note that the highest level of classification should be adopted when the content of an integrated set of data includes different levels.

CSP Controls:

Table (2) below shows CSP's commitments to cloud cybersecurity controls (section no. 10 «Cloud Cybersecurity Controls») by levels.

Table 2. CSP's commitments to cybersecurity controls for cloud computing

✣ Optional (Recommended) ✔ Mandatory

Subdomains and Controls	Level 1	Level 2	Level 3	Level 4
ECC Controls	✔	✔	✔	✔
1-1-P-1	✔	✔	✔	✔
1-2-P-1	✔	✔	✔	✔
1-3-P-1	✔	✔	✔	✣
1-4-P-1	✔	✔	✔	✣
1-4-P-2	✔	✔	✔	✣
1-5-P	✔	✔	✔	✔
2-1-P-1	✔	✔	✔	✔
2-2-P-1	✔	✔	✔	✔[1]
2-3-P-1	✔	✔	✔[2]	✔[3]
2-4-P-1	✔	✔	✔	✔
2-5-P-1	✔	✔	✔	✔[4]
2-6-P-1	✔	✔	✔	✔
2-7-P-1	✔	✔	✔	✔[5]
2-8-P-1	✔	✔	✔	✔
2-9-P-1	✔	✔	✔	✔
2-10-P-1	✔	✔	✔	✔
2-11-P-1	✔	✔	✔	✣
2-12-P-1	✔	✔	✔	✔[6]

[1] With exception of subcontrols 2-2-P-1-9 and 2-2-P-1-10 as they are considered as optional

[2] With exception of subcontrol 2-3-P-1-11 as it is considered as optional

[3] With exception of subcontrols 2-3-P-1-4 and 2-3-P-1-11 as they are considered as optional. Also, subcontrol 2-3-P-1-9 as it is not applicable

[4] With exception of subcontrol 2-5-P-1-2 as it is considered as optional

[5] With exception of subcontrol 2-7-P-1-1 as it is considered as optional

[6] With exception of subcontrols 2-12-P-1-2, 2-12-P-1-3, and 2-12-P-1-8 as they are considered as optional

Subdomains and Controls	Level 1	Level 2	Level 3	Level 4
2-13-P-1	✔	✔	✔	✔
2-14-P-1	✔	✔	✔	✔
2-15-P	✔	✔	✔	✔ [7]
2-16-P	✔	✔	✔	✔
2-17-P	✔	✔	✔	✔
3-1-P-1	✔	✔	✔	✔
4-1-P-1	✔	✔	✔	✔ [8]

CST Controls:

Table (3) below shows CST's commitments to cloud cybersecurity controls (section no. 10 «Cloud Cybersecurity Controls») by levels.

Table 3. CST's commitments to cybersecurity controls for cloud computing

✣ Optional (Recommended) ✔ Mandatory

Subdomains and Controls	Level 1	Level 2	Level 3	Level 4
1-1-T-1	✔	✔	✔	✔
1-2-T-1	✔	✔	✔	✔
1-3-T-1	✔	✔	✔	✔
1-4-T-1	✔	✔	✔	✣
2-1-T-1	✔	✔	✔	✔
2-2-T-1	✔	✔	✔	✔
2-3-T-1	✔	✔	✔	✔ [9]
2-4-T-1	✔	✔	✔	✔
2-5-T-1	✔	✔	✔	✣
2-6-T-1	✔	✔	✔	✣
2-7-T-1	✔	✔	✔	✔ [10]
2-9-T-1	✔	✔	✔	✔
2-11-T-1	✔	✔	✔	✣
2-15-T	✔	✔	✔	✔
3-1-T-1	✔	✔	✔	✔

[7] With exception of subcontrol 2-15-P-3-1 as it is considered as optional

[8] With exception of subcontrol 4-1-P-1-1 as it is considered as optional

[9] With exception of subcontrol 2-3-T-1-1 as it is not applicable

[10] With exception of subcontrol 2-7-T-1-1 as it is considered as optional

Annex No. (B): Terminologies and Definitions

Annex B below shows some of the terminologies contained herein, and the meanings ascribed thereto.

Table 4. Terms and Definitions

Terminology	Definition
Asset	Anything tangible or intangible that has value to the CSPs and CSTs. 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, CSP's and CST'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 CSPs and CSTs 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.
Closed-Circuit Television (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.

Terminology	Definition
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.
Classification	Categorizing the data prepared, collected, processed, or exchanged by the organizations for the provision of services or conduct of businesses, including data received from or exchanged with persons outside organizations, and the data that is prepared for the interest of organizations or related to the sensitive infrastructure. Data related to organizations is classified, using a top down approach, level 1, level 2, level 3, or level 4.
Classified Data	Any data classified at any of the following levels: level 1, level 2, level 3, or level 4.
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.

Terminology	Definition
Cloud Computing Compliance Control Catalogue (C5)	C5 is developed by the German Federal Office for Information Security (BSI) to set minimum requirements to secure cloud services in order to establish a framework of trust between cloud providers and their customers.
Cloud Computing Services	Is the delivery of various services via the Internet and can be accessible through different platforms (desktops, laptops, smart phones.. etc.). These services include applications and infrastructures such as servers, databases and networking to support, among other things, communication, data analysis, processing, sharing and storage.
Cloud Controls Matrix (CCM)	CCM is developed by the Cloud Security Alliance (CSA) to provide fundamental security principles to help the CSTs assessing the security risks of cloud services provided by the CSP.
Cloud Customer	In this document referred to as "Cloud Service Tenant (CST)", is any natural or legal person (such as companies) who subscribes to the cloud computing services provided by the service provider.
Cloud Service Provider (CSP)	Any natural or legal person (such as companies) 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.
Configuration Management DataBase (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)	Layered architecture of technologies that are essential to implement cloud computing services: (Data Center infrastructure, LAN, storage/ compute/ hyper convergence hardware, hypervisor, cloud management platform, virtual appliances, OSs, application software, O&M platforms, cloud security technologies etc.…)

Terminology	Definition
Compromise	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 CSPs and CSTs, intended for use by them. 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 CSPs and CSTs 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.
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.

Terminology	Definition
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 CSPs and CSTs whose work depends on digital ICT, in order to cause damage.
Cyber Risks	Risks that harm the CSPs' and CSTs' processes (including the CSPs' and CSTs' 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 CSPs and CSTs 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	Any information, records, statistics or documents that are photocopied, recorded and stored electronically.
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.

Terminology	Definition
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.
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.
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.
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.

Terminology	Definition
Incident	A security breach through violation of cybersecurity policies, acceptable use policies, practices or cybersecurity controls or requirements.
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»).
ISO/IEC 27000	This series developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) to provide best practice recommendations to establish, implement, maintain and continually improve information security management system (ISMS).
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 CSP's and CST'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.
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.

Terminology	Definition
Level 3	A classification level applies to data classified as a (confidential) based on what is issued by the competent organization.
Level 4	A classification level applies to data classified as a (public) based on what is issued by the competent organization.
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 Cloud Security Standard for Singapore (MTCS SS)	This standard aims to encourage the adoption of sound risk management and security practices for cloud computing. MTCS SS has three levels of security, Level 1 being the base and Level 3 being the most stringent: • Level 1 – Designed for non-business critical data and systems, with baseline security controls to address security risks and threats in potentially low impact information systems using cloud services. • Level 2 – Designed to address the need of most organizations running critical data and systems through a set of more stringent security controls. These address security risks and threats in potentially moderate impact information systems using cloud service. • Level 3 – Designed for regulated organizations with specific requirements, which supplement or address security risks and threats in high impact information systems using cloud services.

Terminology	Definition
Staff	Persons working with CSPs or CSTs (including official and temporary staff and contractors).
Outsourcing	Obtaining (goods or services) by contracting with a supplier or service provider.
Penetration Testing	Testing a computer system, network, website application or smart phone application to look for the vulnerabilities that the attacker can exploit.
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 CSPs and CSTs regarding the cybersecurity program, its controls and requirements, and the mechanism for improving and developing the same.
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 CSPs and CSTs.

Terminology	Definition
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.
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.
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 CSPs and CSTs (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.
Vulnerability	Any kind of vulnerability in the computer system, its programs or applications, in a set of procedures or anything that makes cybersecurity vulnerable.

Annex No. (C): List of the Abbreviations

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

Table 5. List of Abbreviations

Abb.	Full Version
BCM	Business Continuity Management
CCC	Cloud Cybersecurity Controls
CCTV	Closed-Circuit Television
CMDB	Configuration Management DataBase
CNI	Critical National Infrastructure
CSP	Cloud Service Provider
CST	Cloud Service Tenant
CTS	Cloud Technology Stack
DDoS	Distributed Denial of Service
ECC	Essential Cybersecurity Controls
IaaS	Infrastructure as a Service
MFA	Multi-Factor Authentication
PaaS	Platform as a Service
SAN	Storage Area Network
SaaS	Software as a Service
SIEM	Security Information and Event Management

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority