الهيئة الوطنية للأمن الـسيبـراني
National Cybersecurity Authority

Critical Systems Cybersecurity Controls

(CSCC – 1 : 2019)

Sharing Indicator: 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, Confidential and for Intended Recipient Only**

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

🟠 **Amber – Restricted Sharing**

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

🟢 **Green – Sharing within the Same Community**

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

⚪ **White - No Restrictions**

Table of Contents

Executive Summary 10

Introduction 12

Objectives 13

Definition and Identification Criteria of Critical Systems 14

Components of Critical Systems 15

Scope of Work and Applicability 16

Implementation and Compliance 17

Update and Review 17

CSCC Domains and Structure 18

Critical Systems Cybersecurity Controls (CSCC) 20

1- Cybersecurity Governance 20

2- Cybersecurity Defense 22

3- Cybersecurity Resilience 28

4- Third-Party and Cloud Computing Cybersecurity 29

Appendices 30

Appendix (A): Relationship between CSCC and ECC 30

Appendix (B): Terms and Definitions 32

Appendix (C): List of Abbreviations 34

List of the Tables

Table (1): CSCC Structure 19

Table (2): Terms and Definitions 32

Table (3): List of Abbreviations 34

List of the Figures and Illustrations

Figure (1): CSCC Main Domains and Subdomains 18

Figure (2): Controls Coding Scheme 19

Figure (3): CSCC Structure 19

Figure (4): Guide to Colors of Subdomains in Figure 5 30

Figure (5): ECC and CSCC Subdomains 31

Executive Summary

The Kingdom of Saudi Arabia's Vision 2030 aims for a comprehensive improvement of the nation and its security, economy and citizens' well-being. One of the essential goals of Vision 2030 is the continued transformation towards digitalization and the improvement of its infrastructure in order to keep up with the accelerated global progress in digital services, renewable global networks, IT/ OT systems and artificial intelligence and 4th industrial revolution transformations.

This transformation requires supporting the ease of information flow, securing that information and preserving the integrity of all systems. It also requires maintaining and supporting the cybersecurity of the Kingdom in order to protect its vital interests, national security, critical infrastructures, high priority sectors and governmental services and practices. To accomplish this objective, the National Cybersecurity Authority (NCA) was established, and its mandate was approved as per the Royal Decree number 6801, dated 11/2/1439H making it the national and specialized reference for matters related to cybersecurity in the Kingdom.

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

NCA's mandate also fulfill the need to continuously monitor the organizations' compliance as the importance of cybersecurity has significantly increased more than ever with the rise of security risks in the cyberspace.

NCA's mandate states that its responsibility for cybersecurity does not absolve any government or private organization from its own cybersecurity responsibilities as confirmed by the Royal Decree number 57231, dated 10/11/1439H, which states that "all government organizations must improve their cybersecurity level to protect their networks, systems and data, and comply with NCA's policies, frameworks, standards, controls and guidelines" and what the Royal Decree number 7732, dated 12/2/1440H has also confirmed.

From this perspective, NCA developed the Critical Systems Cybersecurity Controls (CSCC - 1 : 2019) to set the minimum cybersecurity requirements for critical systems in all organizations, in addition to the Essential Cybersecurity Controls (ECC - 1 : 2018). This document highlights the details of CSCC controls, goals, scope, statement of applicability, compliance and monitoring.

All organizations that own or operate critical systems must implement all necessary measures to ensure continuous compliance with the CSCC as per item 3 of article 10 of NCA’s mandate and as per the Royal Decree number 57231, dated 10/11/1439H, also as per the Royal Decree number 7732, dated 12/2/1440H.

Introduction

The National Cybersecurity Authority (referred to in this document as "NCA") developed the Essential Cybersecurity Controls (ECC - 1 : 2018) to set the minimum cybersecurity requirements for organizations. As an extension and a complement to ECC, the Critical Systems Cybersecurity Controls (CSCC - 1 : 2019) was developed to fit the cybersecurity needs for national critical systems.

The CSCC was developed after conducting a comprehensive study of multiple national and international cybersecurity frameworks and standards, studying related national decisions, law and regulatory requirements, reviewing and leveraging cybersecurity best practices, analyzing previous cybersecurity incidents and attacks on government and other critical organizations, and conducting public consultations.

During the development of these controls, NCA considered the alignment between CSCC and ECC (which is a prerequisite for compliance with CSCC). The organizations must continuously comply with ECC in order to be fully compliant with the CSCC. for that, the CSCC consists of the following:

- 4 Main Domains
- 21 Subdomains
- 32 Main Controls
- 73 Subcontrols

Objectives

As an extension to ECC, the CSCC aims to enable organizations and build their protection and cyber resilience capabilities against cyber attacks, and sustain information technology assets for critical systems. The CSCC was developed based on international standards and best practices in order to meet the current security needs and raise organizations' preparedness to face the growing cybersecurity risks against their critical systems that may result in negative impacts and significant losses on the national level.

Definition and Identification Criteria of Critical Systems

Critical Systems Definition

Any system or network whose failure, unauthorized change to its operation, unauthorized access to it, or to the data stored or processed by it; may result in negative impact on the organization's businesses and services' availability, or cause negative economic, financial, security or social impacts on the national level.

Critical Systems Identification Criteria

The following are the criteria that may be used by organizations to identify critical systems they own:

1. Negative impact on national security.
2. Negative impact on the Kingdom's reputation and public image.
3. Significant financial losses (i.e., more than 0.01% of GDP).
4. Negative impact on the services provided to a large number of users (i.e., more than 5% of the population)
5. Loss of lives.
6. Unauthorized disclosure of data that is classified as Top Secret or Secret.
7. Negative impact on the operations of one (or more) vital sector(s).

Components of Critical Systems

Below is the list of critical systems' components (1 through 8 are the technical components):

1. Network, for example:

    1.1. Connecting devices, such as:

    - Router.
    - Switches.
    - Gateways.

    1.2 Firewall.

    1.3 Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).

    1.4 Advanced Persistent Threat (APT) protection devices.

2. Databases.
3. Storage Assets.
4. Middleware.
5. Servers and Operating Systems.
6. Applications.
7. Encryption Devices.
8. Critical systems' peripherals, (e.g., printers and scanners).
9. Individuals working in critical systems' supporting roles (e.g., users, technical staff with significant and sensitive privileges, operators and service providers).
10. Documents related to the components above.

Scope of Work and Applicability

CSCC Scope of Work

These controls are applicable to systems deemed critical (as per the criteria forementioned in this document) by the organizations who own or operate these systems, whether they are government organizations in the kingdom or abroad (e.g., ministries, authorities, establishments, embassies and others), subsidiaries of government or private organizations, which are all referred to herein as “Organization”.

CSCC Statement of Applicability

Every organization must comply with all applicable controls after assessing the extent of impact and conducting necessary checks before implementation. Some controls' applicability differs from one organization to another, for example:

- Controls in Subdomain 4-2 (Cloud Computing and Hosting Cybersecurity) are applicable and must be implemented by organizations currently using or planning to use cloud computing and hosting services.

Implementation and Compliance

In order to comply with item 3 of article 10 of NCA's mandate, and as per the Royal Decree number 57231, dated 10/11/1439H, and the Royal Decree number 7732, dated 12/2/1440H, all organizations within the scope of the CSCC must:

1. Identify the organization's critical systems using (Critical Systems Identification Criteria).
2. Implement all necessary measures to comply with these controls on the identified critical systems within the compliance period defined by NCA, provided that cybersecurity risks are assessed and managed to minimize potential risks during the defined compliance period.
3. Ensure the continuous compliance after the defined compliance period.

NCA evaluates the organizations' compliance with the CSCC through multiple means such as self-assessments by the organizations themselves, and/or on-site audits, in accordance with the mechanisms deemed appropriate by the NCA.

Update and Review

NCA will periodically review and update the CSCC as per the related industry cybersecurity updates. NCA will communicate and publish the updated version of CSCC for implementation and compliance.

CSCC Domains and Structure

Main Domains and Subdomains

Figure (1) below shows the main domains and subdomains of CSCC. Appendix (A) shows relationship between the CSCC and ECC.

1- Cybersecurity Governance	1-1	Cybersecurity Strategy	1-2	Cybersecurity Risk Management
	1-3	Cybersecurity in Information Technology Project Management	1-4	Periodical Cybersecurity Review and Audit
	1-5	Cybersecurity in Human Resources		
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	Web Application Security
	2-13	Application Security		
3- Cybersecurity Resilience	3-1	Cybersecurity Resilience Aspects of Business Continuity Management (BCM)		
4- Third-Party and Cloud Computing Cybersecurity	4-1	Third-Party Cybersecurity	4-2	Cloud Computing and Hosting Cybersecurity

Figure (1): CSCC Main Domains and Subdomains

Structure

Figures (2) and (3) below show the scheme and structure of CSCC codes.

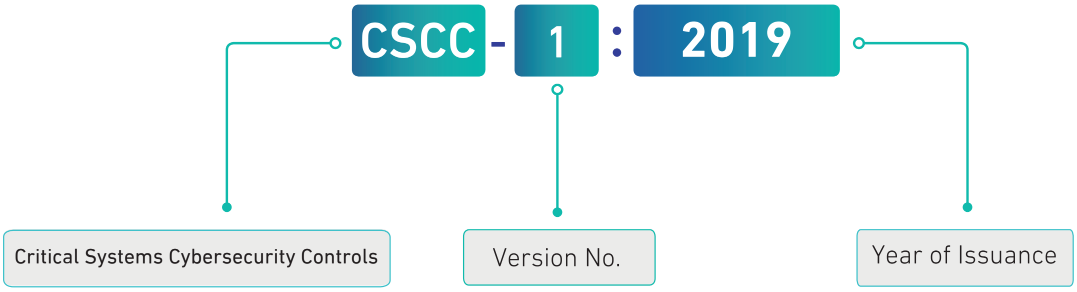


Figure 2. Controls Coding Scheme

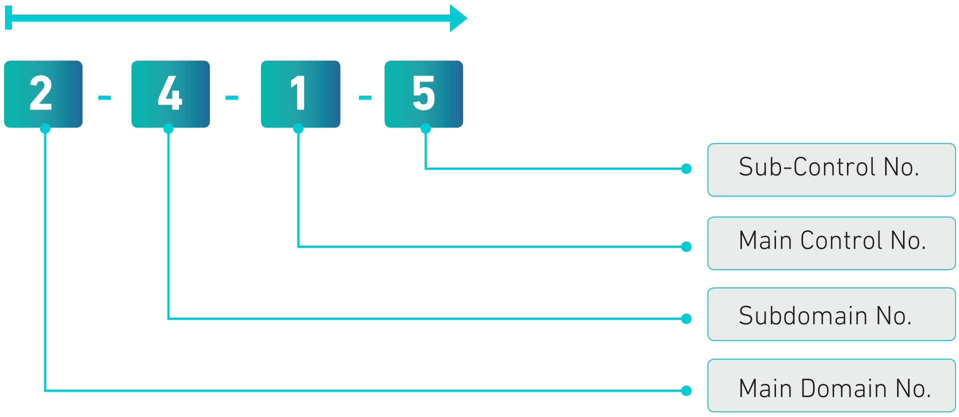


Figure 3. CSCC Structure

Please note that the green colored numbers (such as: 1-8-1), are reference numbers to related ECC subdomain or control.

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

Table 1. CSCC Structure

1	**Name of Main Domain**
Reference Number of the Main Domain	
Reference No. of the Subdomain	Name of the Subdomain
Objective	
Controls	
Control Reference Number	Control Clauses

Critical Systems Cybersecurity Controls (CSCC)

Details of the Critical Systems Cybersecurity Controls (CSCC)

1 Cybersecurity Governance

1-1	Cybersecurity Strategy
Objective	To ensure that cybersecurity plans, goals, initiatives and projects are contributing to compliance with related laws and regulations.
Controls	
1-1-1	In addition to the controls in ECC subdomain 1-1, the organization's cybersecurity strategy must prioritize the support of protecting its critical systems.
1-2	**Cybersecurity Risk Management**
Objective	To ensure managing cybersecurity risks in a methodological approach in order to protect the organization's information technology assets as per the organizational policies and procedures and related laws and regulations.
Controls	
1-2-1	In addition to the controls in ECC subdomain 1-5, cybersecurity risk management methodology must include at least the following: 1-2-1-1 Conducting a cybersecurity risk assessment on critical systems at least once annually. 1-2-1-2 Creating a cybersecurity risk register for critical systems, and reviewing it at least once every month.
1-3	**Cybersecurity in Information Technology Project Management**
Objective	To ensure that cybersecurity requirements are included in project management methodology and procedures in order to protect the confidentiality, integrity and availability of information technology assets as per organization policies, and procedures, and related laws and regulations.
Controls	
1-3-1	In addition to the subcontrols in ECC control 1-6-2, cybersecurity requirements of project management and asset (information technology) change management of the organization's critical systems must include at least the following: 1-3-1-1 Conducting a stress test to ensure the capacity of the various components. 1-3-1-2 Ensuring the implementation of business continuity requirements.

1-3-2	In addition to the subcontrols in ECC control 1-6-3, cybersecurity requirements related to software and application development projects of the organization's critical systems must include at least the following: 1-3-2-1 Conducting a security source code review before the critical system release. 1-3-2-2 Securing the access, storage, documentation and releases of source code. 1-3-2-3 Securing the authenticated Application Programming Interface (API). 1-3-2-4 Secure and trusted migration of applications from testing environments to production environments, along with deletion of any data, IDs or passwords related to the testing environment before the migration.
1-4	Periodical Cybersecurity Review and Audit
Objective	To ensure that cybersecurity controls are implemented and in compliance with organizational policies and procedures, as well as related national and international laws, regulations and agreements.
Controls	
1-4-1	With reference to ECC control 1-8-1, the organization's cybersecurity function must review the implementation of CSCC at least once annually.
1-4-2	With reference to ECC control 1-8-2, the implementation of CSCC must be reviewed by independent parties within the organization, outside the cybersecurity function at least once every three years.
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	
1-5-1	In addition to the subcontrols in ECC control 1-9-3, personnel cybersecurity requirements prior to employment must include at least the following: 1-5-1-1 Screening or vetting candidates for working on critical systems. 1-5-1-2 The technical support and development positions for critical systems, must be filled with experienced Saudi professionals.

2 Cybersecurity Defense

2-1	Asset Management
Objective	To ensure that the organization has an accurate and detailed inventory of information technology assets in order to support the organization's cybersecurity and operational requirements to maintain the confidentiality, integrity and availability of information technical assets.
Controls	
2-1-1	In addition to the controls in ECC subdomain 2-1, cybersecurity requirements for managing information technology assets must include at least the following: 2-1-1-1 Maintaining an annually-updated inventory of critical systems' assets. 2-1-1-2 Identifying assets owners and involving them in the asset management lifecycle for critical systems.
2-2	Identity and Access Management
Objective	To ensure the secure and restricted logical access to information technology assets in order to prevent unauthorized access and allow only authorized access for users which are necessary to accomplish assigned tasks.
Controls	
2-2-1	In addition to the subcontrols in ECC control 2-2-3, cybersecurity requirements for identity and access management of critical systems must include at least the following: 2-2-1-1 Prohibiting remote access from outside the Kingdom of Saudi Arabia. 2-2-1-2 Restricting remote access from inside the Kingdom of Saudi Arabia and verifying each access attempt by the organization's security operations center, and continuously monitoring activities related to remote access. 2-2-1-3 Using multi-factor authentication for all users. 2-2-1-4 Using multi-factor authentication for privileged users, and on systems utilized for managing critical systems stated in control 2-3-1-4. 2-2-1-5 Developing and implementing a high-standard and secure password policy. 2-2-1-6 Utilizing secure methods and algorithms for storing and processing passwords, such as: Hashing functions. 2-2-1-7 Securely managing service accounts for applications and systems, and disabling interactive login from these accounts. 2-2-1-8 Prohibiting direct access and interaction with databases for all users except for database administrators. Users' access and interaction with databases must be through applications only, with consideration given to applying security solutions that limit or prohibit visibility of classified data to database administrators.

2-2-2	With reference to ECC subcontrol 2-2-3-5, user identities and access rights to critical systems must be reviewed at least once every three months.
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	
2-3-1	In addition to the subcontrols in ECC control 2-3-3, cybersecurity requirements for protecting critical systems and information processing facilities must include at least the following: 2-3-1-1 Whitelisting of application and software operation files that are allowed to execute on servers hosting critical systems. 2-3-1-2 Protecting servers hosting critical systems using end-point protection solutions that are approved by the organization. 2-3-1-3 Applying security patches and updates at least once every month for external and internet-connected critical systems and at least once every three months for internal critical systems, in line with the organization's approved change managmenet mechanisms. 2-3-1-4 Allocating specific workstations in an isolated network (Management Network), that is isolated from other networks or services (e.g., email service or internet), to be used by highly privileged accounts. 2-3-1-5 Encrypting the network traffic of non-console administrative access for all technical components of critical systems using secure encryption algorithms and protocols. 2-3-1-6 Reviewing critical systems' configurations and hardening at least once every six months. 2-3-1-7 Reviewing and changing default configurations, and ensuring the removal of hard-coded, backdoor and/or default passwords, where applicable. 2-3-1-8 Protecting systems' logs and critical files from unauthorized access, tampering, illegitimate modification and/or deletion.

2-4	Networks Security Management
Objective	To ensure the protection of the organization’s network from cyber risks.
Controls	
2-4-1	In addition to the subcontrols in ECC control 2-5-3, cybersecurity requirements of critical systems’ network security management must include at least the following: 2-4-1-1 Logically and/or physically segregating and isolating critical systems' networks. 2-4-1-2 Reviewing firewall rules and access lists, at least once every six months. 2-4-1-3 Prohibiting direct connection between local network devices and critical systems, unless those devices are scanned to ensure they have security controls that meet the acceptable security levels for critical systems. 2-4-1-4 Prohibiting critical systems from connecting to a wireless network. 2-4-1-5 Protecting against Advanced Persistent Threats (APT) at the network layer. 2-4-1-6 Prohibiting connection to the internet for critical systems that provide internal services to the organization and have no strong need to be accessed from outside the organization. 2-4-1-7 Critical systems that provide services to a limited number of organizations (not individuals), shall use networks isolated from the Internet. 2-4-1-8 Protecting against Distributed Denial of Service (DDoS) attacks to limit risks arising from these attacks. 2-4-1-9 Allowing only whitelisting for critical systems’ firewall access lists.
2-5	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 organization’s information (including sensitive information) while utilizing Bring Your Own Device (BYOD) policy.
Controls	
2-5-1	In addition to the subcontrols in ECC control 2-6-3, cybersecurity requirements for mobile devices security and BYOD in the organization must include at least the following: 2-5-1-1 Prohibting access to critical systems from mobile devices except for a temporary period only, after assessing the risks and obtaining the necessary approvals from the cybersecurity function in the organization. 2-5-1-2 Implementing full disk encryption for mobile devices with access to critical systems.
2-6	Data and Information Protection
Objective	To Ensure the confidentiality, integrity and availability of the organization’s data and information as per organizational policies and procedures, and related laws and regulations.

Controls	
2-6-1	In addition to the subcontrols in ECC control 2-7-3, cybersecurity requirements for protecting and handling data and information must include at least the following: 2-6-1-1 Prohibting the use of critical systems' 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. 2-6-1-2 Classifying all data within critical systems. 2-6-1-3 Protecting classified data of critical systems using data leakage prevention techniques. 2-6-1-4 Identifying retention period for critical systems-associated data, in accordance with relevant legislations. Only required data must be retained in critical systems' production environments. 2-6-1-5 Prohibting the transfer of any critical systems' data from production environment to any other environment.
2-7	Cryptography
Objective	To ensure the proper and efficient use of cryptography to protect information assets as per organizational policies and procedures, and related laws and regulations.
Controls	
2-7-1	In addition to the subcontrols in ECC control 2-8-3, cybersecurity requirements for cryptography must include at least the following: 2-7-1-1 Encrypting all critical systems' data-in-transit. 2-7-1-2 Encrypting all critical systems' data-at-rest at the level of files, database or certain columns within database. 2-7-1-3 Using secure and up-to-date methods, algorithms, keys and devices in accordance with what NCA issues in this regard.
2-8	Backup and Recovery Management
Objective	To ensure the protection of the organization's data and information, including information systems and software configurations from cyber risks as per organizational policies and procedures, and related laws and regulations.
Controls	
2-8-1	In addition to the subcontrols in ECC control 2-9-3, cybersecurity requirements for backup and recovery management must include at least the following: 2-8-1-1 Scope and coverage of online and offline backups shall cover all critical systems. 2-8-1-2 Performing backup within planned intervals, according to the organization's risk assessment. NCA recommends performing backup for critical systems on a daily basis. 2-8-1-3 Securing access, storage and transfer of critical systems' backups and storage media, and protecting it from destruction, unauthorized access or modification.

2-8-2	With reference to ECC subcontrol 2-9-3-3, a periodical test must be conducted at least once every three months in order to determine the efficiency of recovering critical systems backups.
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 organization.
Controls	
2-9-1	In addition to the subcontrols in ECC control 2-10-3, cybersecurity requirements for technical vulnerabilities management of critical systems must include at least the following: 2-9-1-1 Utilizing trusted methods and tools for vulnerabilities assessments. 2-9-1-2 Assessing and remediating vulnerabilities (by installing security updates and patches) on technical components of critical systems at least once every month for external and internet-connected critical systems, and at least once every three months for internal critical systems. 2-9-1-3 Immediately remediating for critical vulnerabilities, in line with change management processes approved by the organization.
2-9-2	With reference to ECC subcontrol 2-10-3-1, vulnerabilities assessments must be conducted on critical systems' technical components at least once every month.
2-10	Penetration Testing
Objective	To assess and evaluate the efficiency of the organization's cybersecurity defense capabilities through simulated cyber attacks to discover unknown weaknesses within the technical infrastructure that may lead to a cyber breach.
Controls	
2-10-1	In addition to the subcontrols in ECC control 2-11-3, cybersecurity requirements for penetration testing on critical systems must include at least the following: 2-10-1-1 Scope of penetration tests must cover all of the critical systems' technical components and all its internal and external services. 2-10-1-2 Conducting penetration tests by a qualified team.
2-10-2	With reference to ECC subcontrol 2-11-3-2, penetration tests must be conducted on critical systems at least once every six months.
2-11	Cybersecurity Event Logs and Monitoring Management
Objective	To ensure timely collection, analysis and monitoring of cybersecurity events for early detection of potential cyber-attacks in order to prevent or minimize the negative impacts on the organization's operations.

Controls	
2-11-1	In addition to the subcontrols in ECC control 2-12-3, cybersecurity requirements for event logs and monitoring management for critical systems must include at least the following: 2-11-1-1 Activating cybersecurity event logs on all technical components of critical systems. 2-11-1-2 Activating and monitoring of alerts and event logs related to file integrity management. 2-11-1-3 Monitoring and analyzing user behavior. 2-11-1-4 Monitoring critical systems security events around the clock. 2-11-1-5 Maintaining and protecting critical systems security events logs. The log shall include all details (e.g., time, date, ID and affected system).
2-11-2	With reference to ECC subcontrol 2-12-3-5, retention period of cybersecurity's critical systems event logs must be 18 months minimum, in accordance with relevant legislative and regulatory requirements.
2-12	Web Application Security
Objective	To ensure the protection of Internet-Facing web applications against cyber risk.
Controls	
2-12-1	In addition to the subcontrols in ECC control 2-15-3, cybersecurity requirements for external web applications for the organization's critical systems must include at least the following: 2-12-1-1 Secure session management, including session authenticity, session lockout and session timeout. 2-12-1-2 Applying the minimum standards of Open Web Application Security Project (OWASP) Top Ten.
2-12-2	With reference to ECC subcontrol 2-15-3-2, multi-tier architecture principle, with minimum 3 tiers, must be used.
2-13	Application Security
Objective	To ensure the protection of the critical systems' internal applications against cyber risks.
Controls	
2-13-1	Cybersecurity requirements for critical systems' internal applications must be defined, documented, and approved.
2-13-2	The cybersecurity requirements for critical systems' internal applications must be implemented.

2-13-3	The cybersecurity requirements for critical systems' internal applications must include at least the following: 2-13-3-1 Adopting multi-tier architecture principle, provided that number of tiers is not less than three. 2-13-3-2 Using secure protocols (e.g., HTTPS). 2-13-3-3 Outlining the acceptable use policy for users. 2-13-3-4 Secure session management, including session authenticity, session lockout and session timeout.
2-13-4	The cybersecurity requirements for critical systems' internal applications must be 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 organization’s 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	
3-1-1	In addition to the subcontrols in ECC control 3-1-3, cybersecurity requirements for business continuity management must include at least the following: 3-1-1-1 Establishing a disaster recovery center for critical systems. 3-1-1-2 Incorporating critical systems within disaster recovery plans. 3-1-1-3 Conducting periodical tests to ensure the efficiency of disaster recovery plans for critical systems, at least once annually. 3-1-1-4 NCA recommends conducting periodical live Disaster Recovery (DR) test for critical systems.

4 Third-Party and Cloud Computing Cybersecurity

4-1	Third-Party Cybersecurity
Objective	To ensure the protection of assets against cybersecurity risks related to third parties, including outsourcing and managed services as per organizational policies and procedures, and related laws and regulations.
Controls	
4-1-1	In addition to the controls in ECC subdomain 4-1, cybersecurity requirements for contracts and agreements with third-parties must include at least the following: 4-1-1-1 Screening or vetting of outsourcing and managed services companies and personnel who work on critical systems. 4-1-1-2 Outsourcing and managed services of critical systems must rely on Saudi companies and organizations, in accordance with the relevant legislative and regulatory requirements.
4-2	Cloud Computing and Hosting Cybersecurity
Objective	To ensure the proper and efficient remediation of cyber risks and the implementation of cybersecurity requirements related to hosting and cloud computing as per organizational policies and procedures, and related laws and regulations. It is also to ensure the protection of the organization's information technology assets hosted on the cloud or processed/ managed by third parties.
Controls	
4-2-1	In addition to the subcontrols in ECC control 4-2-3, cybersecurity requirements related to the use of hosting and cloud computing services must include at least the following: 4-2-1-1 Hosting of critical systems and any part of their technical components must be inside the organization or within cloud computing services provided by government organizations or Saudi companies that are in compliance with NCA's Cloud Cybersecurity Controls (CCC), taking into account the classification of the hosted data.

Appendices

Appendix (A): Relationship between CSCC and ECC

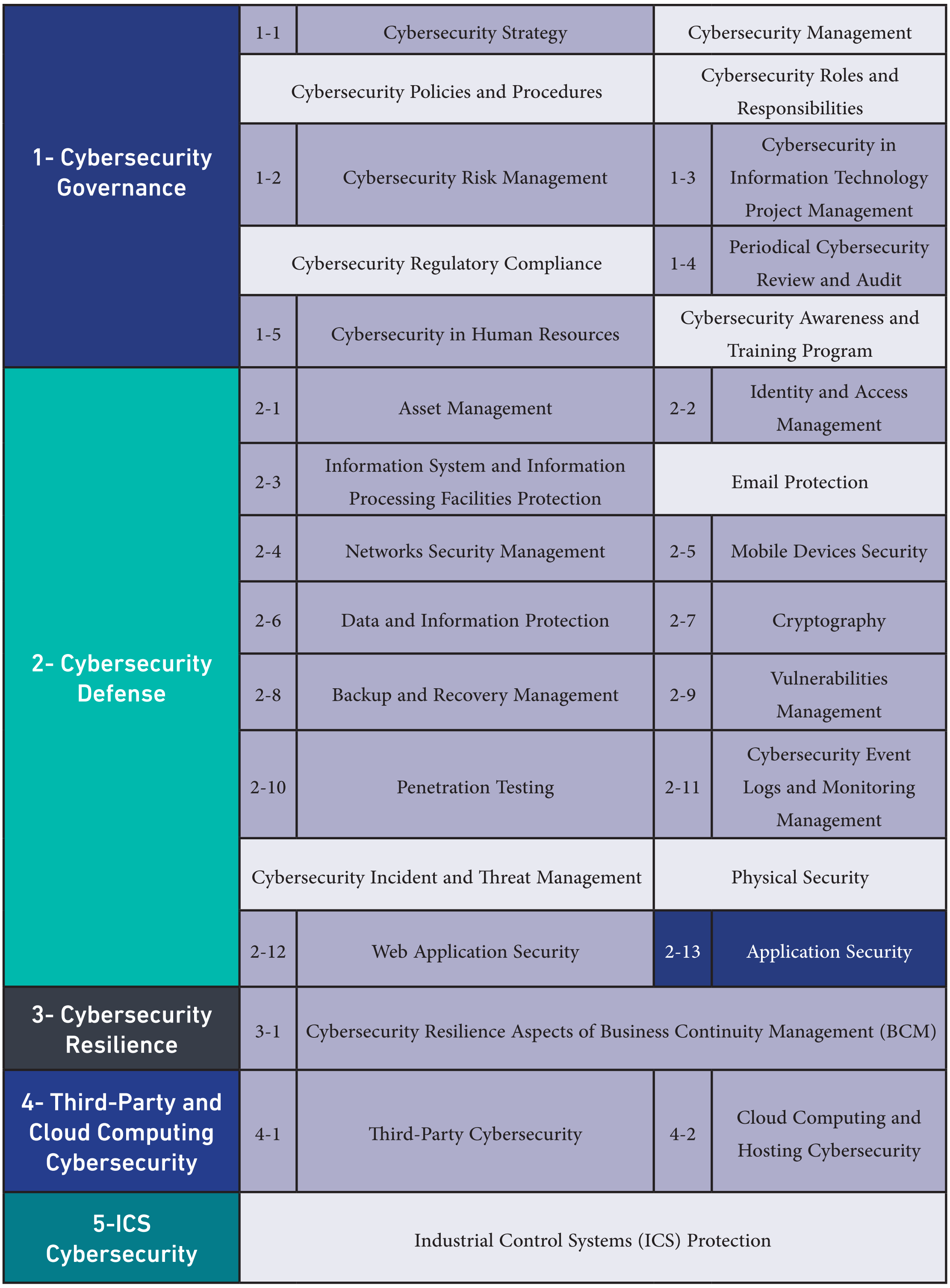
Critical Systems Cybersecurity Controls (CSCC – 1 : 2019) is an extension to Essential Cybersecurity Controls (ECC - 1 : 2018) as illustrated in figures (4) and (5) below, whereas the following items are added:

- New subdomain for critical systems cybersecurity controls.
- Cybersecurity controls for critical systems are added to twenty subdomains.

There are no controls for critical systems cybersecurity are added for nine subdomains.

■	Subdomains for critical systems cybersecurity controls
▨	Subdomains which critical systems controls are added
□	Subdomains which no critical systems controls are added

Figure (4): Guide to Colors of Subdomains in Figure (5)



1- Cybersecurity Governance	1-1	Cybersecurity Strategy		Cybersecurity Management
		Cybersecurity Policies and Procedures		Cybersecurity Roles and Responsibilities
	1-2	Cybersecurity Risk Management	1-3	Cybersecurity in Information Technology Project Management
		Cybersecurity Regulatory Compliance	1-4	Periodical Cybersecurity Review and Audit
	1-5	Cybersecurity in Human Resources		Cybersecurity Awareness and Training Program
2- Cybersecurity Defense	2-1	Asset Management	2-2	Identity and Access Management
	2-3	Information System and Information Processing Facilities Protection		Email 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
		Cybersecurity Incident and Threat Management		Physical Security
	2-12	Web Application Security	2-13	Application Security
3- Cybersecurity Resilience	3-1	Cybersecurity Resilience Aspects of Business Continuity Management (BCM)		
4- Third-Party and Cloud Computing Cybersecurity	4-1	Third-Party Cybersecurity	4-2	Cloud Computing and Hosting Cybersecurity
5-ICS Cybersecurity		Industrial Control Systems (ICS) Protection		

Figure (5): ECC and CSCC Subdomains

Appendix (B): Terms and Definitions

Table (2) below highlights some of the terms and definitions which were used in this document.

Table (2): Terms and Definitions

Term	Definition
Application Program Interface (API)	Set of commands, functions, objects and protocols developed to be used by programmers for developing software or interacting with other systems and/or software.
Critical Vulnerabilities	Vulnerabilities that if exploited could lead to unauthorized access to data or information or devices and systems.
Data-At-Rest	Inactive data stored in permanent storage media, such as: (Databases, archivals, tapes, off-site back up, laptops and Disks).
Data-In-Transit	Data transmitted from one location to another, by any type of network; such as: Internet, private network, etc.
Data Leakage Prevention	Methods to keep important data from unauthorized individuals and prevent its circulation outside the confines of the organization regardless of its form or location, whether it be stored at-rest, or in-use in user PCs or central servers or in-transit through a network.
Data Masking	A technique based upon hiding part of the data to protect it by replacing some characters or values with certain symbols.
Data Scrambling	A method that relies on rearranging or replacing data in a data set; so that the data values remain but are inconsistent with the original records and cannot be restored.
Distributed Denial of Service Attack (DDoS)	An attempt to disable the system and make its services unavailable by sending many requests from more than one source at the same time.
End-point Protection	The actions and technology used for end-point protection against attcks, such as domains, computers and laptops (like anti-virus software, anti-spyware progams, personal fire walls and intrusion detection systems.
Hashing Functions	The process of applying a one-way algorithm upon data in order to obtain a numerical value expressing such data so that it is difficult (or almost impossible) to return to the original data from the numerical value.
Middleware	The software that helps programs and databases (which may be on different host) work together.
Remote Access	Users gain entry from outside the internal network or internal information system.
Screening or Vetting	The process of verifying the identity of persons, prior to employment, due to their expected association with a task related to sensitive systems.

Term	Definition
Secret	A classification level applies to data that the unauthorized disclosure of which results in a severe damage to the national security, national economy, KSA's international relationships or the investigation of major crimes.
Service Accounts	Account used for operating services or software, with access to data and resources.
Source Code	Set of commands and instructions written in one of programming languages.
Stress Testing	A form of deliberately intense or thorough testing used to determine the stability of a given system or entity. It involves overwhelming its resources and testing beyond normal operational capacity, often to a breaking point, in order to observe the results.
Top Secret	A classification level applies to data that the unauthorized disclosure of which results in a severe damage to the national security, national economy or KSA's international relationships and it is hardly possible to recover from such a damage.
User Behavior Analytics (UBA)	Track, collect and analyze user data, and identify patterns of user activities; in order to detect harmful or unusual behaviors.

Appendix (C): List of Abbreviations

Table (3) below shows some of the abbreviations and their meanings which are used in this document.

Table (3): List of Abbreviations

Abb.	Full Term
APT	Advanced Persistent Threat
API	Application Program Interface
BCM	Business Continuity Management
BYOD	Bring Your Own Device
CNI	Critical National Infrastructure
DDoS	Distributed Denial of Service
ECC	Essential Cybersecurity Controls
HTTPS	Hyper Text Transfer Protocol Secure
ICS	Industrial Control System
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
MFA	Multi-Factor Authentication
TLP	Traffic Light Protocol
UBA	User Behavior Analytics

الهيئة الوطنية للأمن الـسيبـراني
National Cybersecurity Authority