This is a guidance box. Remove all guidance boxes after filling out the template. Items highlighted in turquoise should be edited appropriately. After all edits have been made, all highlights should be cleared.

Insert organization logo by clicking on the outlined image.

Cybersecurity Steering Committee Regulating Document Template

Replace <organization name> with the name of the organization for the entire document. To do so, perform the following

- Press “Ctrl” + “H” keys simultaneously
- Enter “<organization name>” in the Find text box
- Enter your organization’s full name in the “Replace” text box
- Click “More”, and make sure “Match case” is ticked
- Click “Replace All”
- Close the dialog box.

Choose Classification

DATE	Click here to add date
VERSION	Click here to add text
REF	Click here to add text

Disclaimer

This template has been developed by the National Cybersecurity Authority (NCA) as an illustrative example that can be used by organizations as a reference and guide. This template must be customized and aligned with the <organization name>'s business and relevant legislative and regulatory requirements. This template must be approved by the head of the organization (Authorizing official) or his/her delegate. The NCA is not responsible for any use of this template as is, and it affirms that this template is solely an illustrative example.

Document Approval

Role	Job Title	Name	Date	Signature
Choose Role	<Insert job title>	<Insert individual's full personnel name>	Click here to add date	<Insert signature>

Version Control

Version	Date	Updated by	Version Details
<Insert version number>	Click here to add date	<Insert individual's full personnel name>	<Insert description of the version>

Review Table

Periodical Review Rate	Last Review Date	Upcoming Review Date
<Once a year>	Click here to add date	Click here to add date

Table of Contents

Introduction 4
Mandate 4
Purpose 4
Scope 4
Controls 5
Composition 6
General Rules 8
Roles and Responsibilities 10
Update and Review 10
Compliance 10

Introduction

Cybersecurity Steering Committee (CSC) is a specialized committee to ensure the alignment of the <cybersecurity function>'s strategy with the strategic objectives of the <organization name>, in addition to its objectives stated in this document. It is comprised of stakeholders and owners of <organization name>'s business who are responsible for guidance, support and prioritization of cybersecurity strategy objectives.

Mandate

The Cybersecurity Steering Committee (CSC) was established by the <authorization official> and mandated in accordance with the relevant legal and regulatory requirements (such as: Essential Cybersecurity Controls "ECC-1:2018"). It is a regulatory requirement as stated in the control 1-2-3 of the Essential Cybersecurity Controls (ECC-1:2018) issued by the National Cybersecurity Authority (NCA).

CSC provides the organization a framework for the governance of cybersecurity. Additional responsibilities may be delegated to the CSC by the <authorization official>.

Purpose

This document aims to define the Cybersecurity Steering Committee at <organization name> to ensure compliance to the implementation, support, and follow-up of <organization name>'s cybersecurity programs, legislations and strategy. These requirements are aligned with the National Cybersecurity Authority's (NCA) cybersecurity requirements including but not limited to Essential Cybersecurity Controls (ECC - 1:2018) and other relevant legal and regulatory requirements.

Scope

This document covers all information and technology assets in the <organization name> and applies to all personnel (employees and contractors) in <organization name>.

Controls

CSC acts as a forum where cybersecurity directions, decisions, and performance are discussed. CSC will also follow-up on the cybersecurity programs execution, ensure internal commitment to the cybersecurity strategy, policies, and legislations, and provide adequate support, where necessary. CSC responsibilities are defined as follows, as an example but not limited to:

1- Follow up the operating principles and requirements as per the Cybersecurity Steering Committee Charter.

2- Establish accountability, responsibility, and authority by setting the roles and responsibilities for the protection of the <organization name>'s information and technology assets.

3- Set an approved methodology for cybersecurity risks management and assessment and the risk appetite for <organization name>.

4- Approve, support and monitor cybersecurity risk procedures.

5- Approve, support and monitor cybersecurity governance.

6- Review cybersecurity strategy before approval to ensure its alignment <organization name>'s strategic objectives.

7- Approve, support and monitor cybersecurity strategy execution.

8- Approve, support and monitor cybersecurity policies implementation.

9- Approve, support and monitor cybersecurity programs and initiatives (such as: cybersecurity and data protection awareness programs, etc.).

10- Approve the key performance indicators (KPIs), monitor their impact on <cybersecurity function>'s business and improve the level of performance.

11- Monitor patch management reports periodically.

12- Monitor and support cybersecurity incidents management.

13- Review the periodic reports of <cybersecurity function> that includes cybersecurity projects, the overall cybersecurity status, residual risks of risk appetite, and cybersecurity risks that may directly or indirectly affect <organization name>'s business and provide the necessary support.

14- Review cybersecurity-risks reports and follow up and support treatment or mitigation.

15- Review security reports of cybersecurity incidents and make recommendations.

16- Review exception requests of cybersecurity incidents and make recommendations.

17- Review security patches reports and assess and fix vulnerabilities of all information and technology assets.

18- Review the results of internal and external cybersecurity audit, and ensure setting a plan to fix, follow up and support the findings.

19- Present periodic reports of cybersecurity status and the required support to the <authorization official>.

20- Review compliance with internal requirements of <organization name> and the legal requirements of the National Cybersecurity Authority.

Composition

1- CSC is chaired by the <organization head or deputy>, provided there is no conflict of interest.

2- CSC includes permanent members, as well as guest members (that attend on an as-needed basis). CSC must include members affected or members whose business is affected by <organization name>'s cybersecurity. Such members include without limitation:

2-1 <organization head or deputy>

2-2 <head of cybersecurity function>

2-3 <head information technology function>

2-4 <head of risk function>

2-5 <head of compliance function>

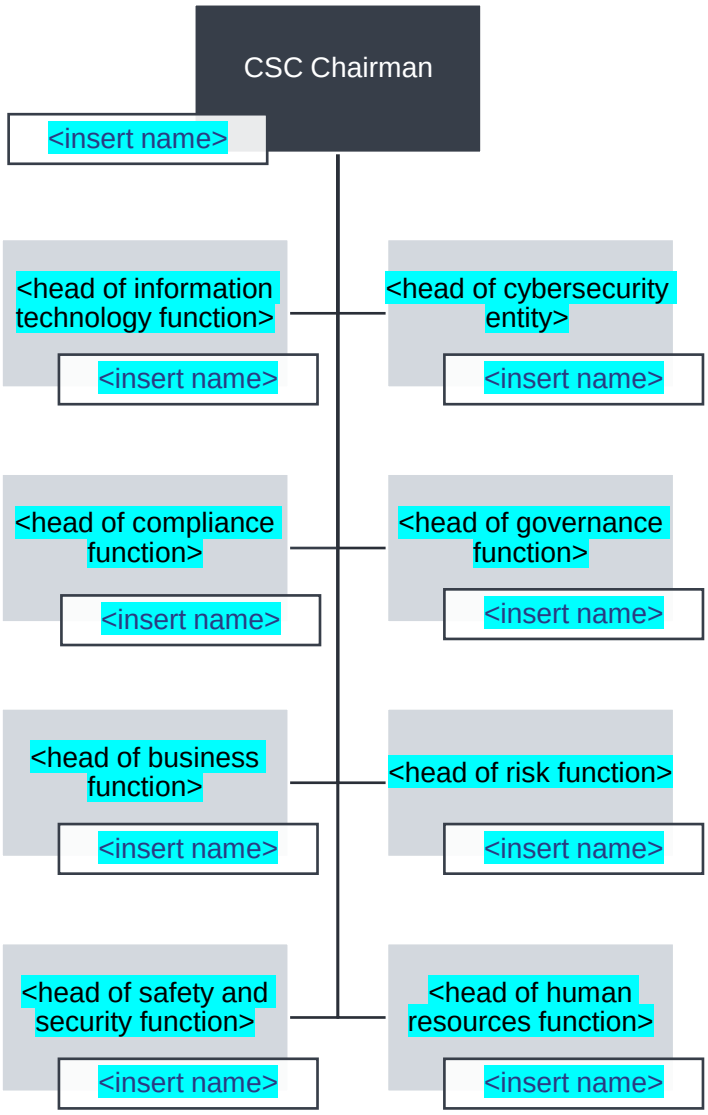
2-6 <head of business function>

2-7 <head of human resources function>

2-8 <head of safety and security function>

3- CSC includes the following members:

Full name	Job Description	Position
<insert name>	<organization head or deputy>	CSC Chairman
<insert name>	<head of cybersecurity function>	Permanent member and secretary of CSC
<insert name>	<head of information technology function>	Permanent member
<insert name>	<head of corporate governance function>	Permanent member
<insert name>	<head of compliance function>	Permanent member
<insert name>	<head of risk function>	Permanent member
<insert name>	<head of business function>	Guest member
<insert name>	<head of human resources function>	Guest member
<insert name>	<head of safety and security function>	Guest member



General Rules

1- CSC meetings is held at least 4 times a year (quarterly). Additional emergency meetings may be scheduled as necessary.

2- CSC meeting cannot be held without the attendance of CSC chairman (or vice-chairman) or without the attendance of at least half of the permanent members.

3- If the meeting requires the attendance of an expert or consultant, CSC secretary may invite such person after the approval of CSC chairman.

4- CSC secretary may request unscheduled emergency meetings after the approval of CSC chairman.

5- CSC secretary records the minutes of meeting, provided that such minutes are official and approved.

6- Information among CSC members is shared using a traffic light protocol (TLP) in order to enable secure information governance. All information shared in CSC must be classified and clearly marked in accordance with the following color-coded levels:

6-1 Information classified as **RED** can only be discussed by the members of CSC.

6-2 Information classified as **AMBER** can be shared by CSC members with their direct reports on a need-to-know basis to address the specific topic or risk.

6-3 Information classified as **GREEN** is internal information that can be shared with all employees of the <organization name>.

Roles and Responsibilities

1- **Document Owner:** <head of cybersecurity function>

2- **Document Review and Update:** <cybersecurity function>

3- **Document Implementation and Execution:** <steering committee members> and <cybersecurity function>

4- **Document Compliance Measurement**: <cybersecurity function>

Update and Review

<cybersecurity function> must review this document at least once a year or in case any significant changes happen to the policy or the regulatory procedures in <organization name> or the relevant legislative and regulatory requirements.

Compliance

1- The <head of cybersecurity function> will ensure the compliance of <organization name> with this document on a regular basis.

2- All personnel at <organization function> must comply with this document.

3- Any violation of this document may be subject to disciplinary action according to <organization name>'s procedures.