This is a guidance box. Remove all guidance boxes after filling out the template. Items highlighted in turquoiseshould be edited appropriately. Items highlighted in green are examples and should be removed. After all edits have been made, all highlights should be cleared. Remove items highlighted in yellow if the organization does not intend to add any subsidiaries to the cybersecurity strategy.

Insert organization logo by clicking on the outlined image.

Cybersecurity Strategy and Roadmap Template

Choose Classification

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

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.

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 shall not be 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

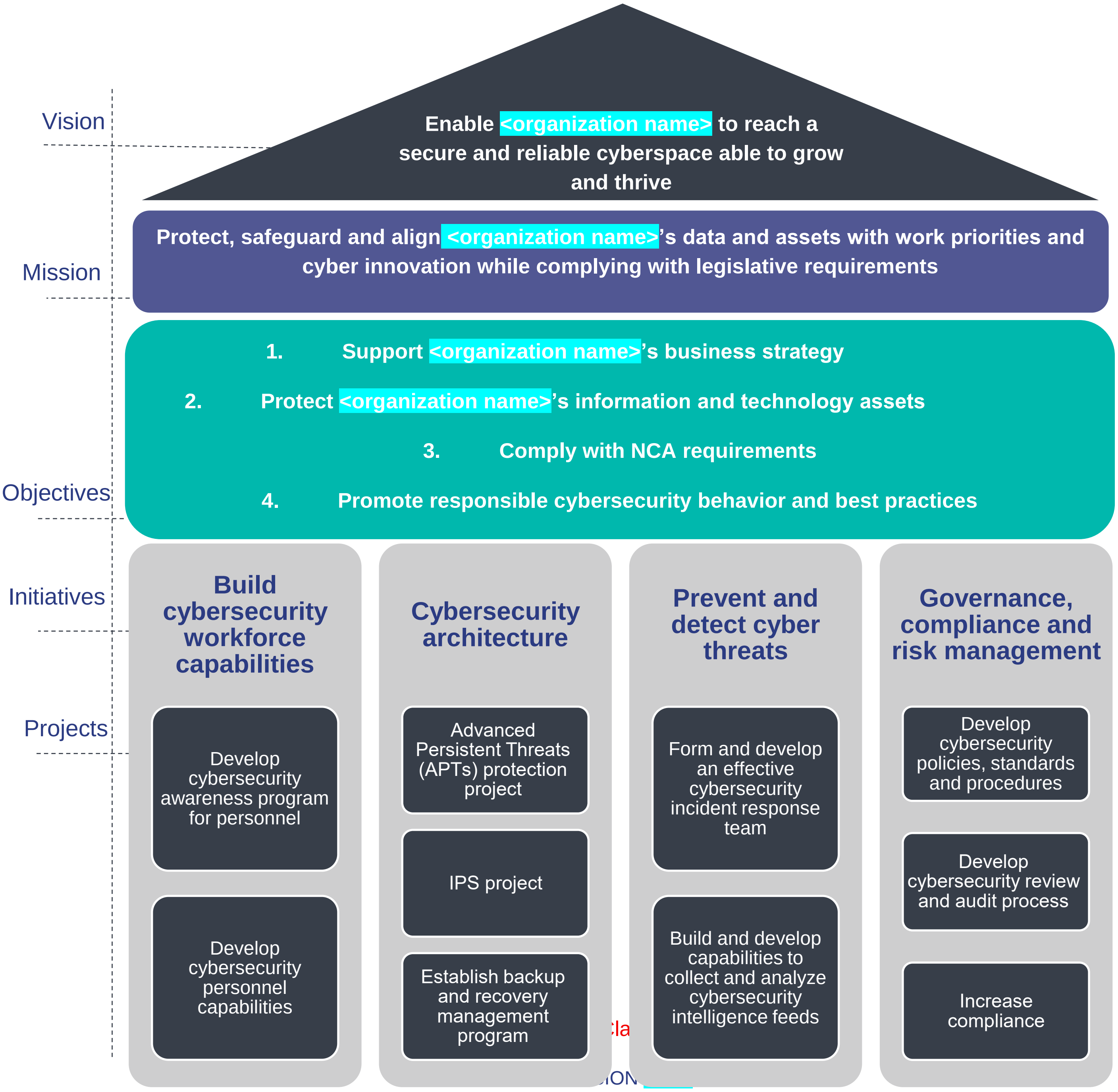
Periodical Review Rate	Last Review Date	Upcoming Review Date
Once a year	Click here to add date	Click here to add date

Table of Contents

Cybersecurity Strategy

Executive Summary

<Organization name> seeks to develop, maintain and enhance its cybersecurity capabilities and protecting same against internal and external cybersecurity risks. <Organization name> has developed this cybersecurity strategy in order to address threats, mitigate cyber risks and support <organization name>'s three-year business strategy.



Vision

Enable <organization name> to reach a secure and reliable cyberspace able to grow and thrive

Mission

Protect, safeguard and align <organization name>'s data and assets with work priorities and cyber innovation while complying with legislative requirements

Objectives

1. Support <organization name>'s business strategy
2. Protect <organization name>'s information and technology assets
3. Comply with NCA requirements
4. Promote responsible cybersecurity behavior and best practices

Initiatives

Projects

Build cybersecurity workforce capabilities

- Develop cybersecurity awareness program for personnel
- Develop cybersecurity personnel capabilities

Cybersecurity architecture

- Advanced Persistent Threats (APTs) protection project
- IPS project
- Establish backup and recovery management program

Prevent and detect cyber threats

- Form and develop an effective cybersecurity incident response team
- Build and develop capabilities to collect and analyze cybersecurity intelligence feeds

Governance, compliance and risk management

- Develop cybersecurity policies, standards and procedures
- Develop cybersecurity review and audit process
- Increase compliance

FIGURE 1 1: CYBERSECURITY STRATEGY EXECUTIVE SUMMARY

Introduction

<Organization name> seeks to develop, maintain and strengthen its cybersecurity capabilities in order to protect itself against internal and external cybersecurity risks. <Organization name> has developed this cybersecurity strategy to support <organization name>'s business strategy, address threats and mitigate cyber risks.

<Head of cybersecurity function>, CSC members, cybersecurity administers and other cybersecurity professionals in <organization name> are the primary target audience for this strategy. Cybersecurity is the responsibility of all personnel of <organization name>, including third parties.

This cybersecurity strategy is intended to make recommendations related to <organization name>’s cybersecurity activities in alignment with business nature to enable business initiatives, and share a clear, compelling, and unified vision among <organization name>’s functions and subsidiaries.

These requirements have been aligned with the cybersecurity requirements issued by NCA, including: Essential Cybersecurity Controls (ECC – 1: 2018), and other relevant legislative and regulatory requirements.

Scope of work and Applicability

This cybersecurity strategy covers all of <organization name>’s business. <Organization name> and its subsidiaries will ensure that this strategy is implemented.

The cybersecurity strategy applies to the following organizations and subsidiaries:

1- <organization name 1>.
2- <organization name 2>.
3- ...

Since initiatives set out in the strategy apply to and affect organizations and subsidiaries, their implementation will be agreed upon in coordination with these subsidiaries.

Cybersecurity Vision

1- The cybersecurity vision provides a short description of the<organization name> desired position in terms of cybersecurity status in the next 3 years. It also describes the future target state of cybersecurity at<organization name>.

2- <Cybersecurity function> took <organization name>'s objectives into consideration to ensure alignment with cybersecurity vision.

Cybersecurity Vision

Enable <organization name> to reach a secure and reliable cyberspace able to grow and thrive.

Cybersecurity Objectives

The cybersecurity objectives were defined according to the cybersecurity vision and the outcome of cybersecurity current state analysis, as follows:

1- **Support <organization name>'s business strategy:** Ensure that cybersecurity plans, objectives, initiatives and projects within<organization name> are contributing to achieve relevant legislative and regulatory objectives and requirements.
2- **Protect <organization name>'s information and technology assets:** Provide the required technology solutions to protect the <organization name> information and technology assets.
3- **Promote responsible cybersecurity behavior and best practices:** Provide personnel with cybersecurity skills and qualifications, promote cybersecurity awareness through multiple channels and build a positive cybersecurity culture.

Cybersecurity Initiatives and Projects

1- Cybersecurity initiatives include all the projects and programs required to achieve cybersecurity strategy objectives. Such initiatives shall be developed based on the cybersecurity vision and objectives:

- **Governance, compliance and risk management:**The initiative includes governance, risk and compliance-related projects and programs aiming to enhance cybersecurity in <organization name> and develop cybersecurity strategic plans. This includes, but is not limited to: Project of compliance with NCA controls and guidelines, including: Essential Cybersecurity Controls (ECC), Critical Systems Cybersecurity Controls (CSCC) and other controls.
- **Prevent and detect cyber threats:**The initiative includes projects and programs that help <organization name> to detect and prevent internal and external threats. This includes, but is not limited to: A project to purchase and run systems for detecting and preventing internal and external threats, including EDR or SIEM and others.
- **Cybersecurity architecture:** The initiative includes projects and programs aiming at helping <organization name> boost its cybersecurity maturity level and protect <organization name> from cyber risks. This includes, but is not limited to: Build and implement networks security architecture and other.
- **Build cybersecurity workforce capabilities:**This initiative includes projects and programs aiming at raising cybersecurity awareness and providing <cybersecurity function>'s personnel with cybersecurity skills and qualifications . This includes, but is not limited to: A project to develop a cybersecurity awareness program related to the organization's personnel, which covers several topics, including warning against email phishing and information sharing on social media.

Key Performance Indicators (KPIs)

In order to measure the strategy's efficiency in achieving its objectives, a number of KPIs have been created to measure the progress of each objective. A baseline and an annual target were set for each indicator based on the results of the current state study, international experiences and workshops with specialists and consultants. The indicators were linked to three strategic results that can be reached by calculating the indicators in order to achieve the strategy's vision, knowing that KSA seeks to achieve this vision within five years. These strategic results consist of:

1. Mitigating risks
2. Promoting trust

3. Enabling growth

The implementation impact will be evident through contributing to growth, risk mitigation and promoting trust with the development of strategy implementation, and the compliance of national entities with the assigned roles, responsibilities, frameworks and standards. Thus, the national deliverables will reflect a significant improvement on the long term.

Cybersecurity roadmap

Introduction

<Organization name> seeks to develop, maintain and strengthen its cybersecurity capabilities in order to protect itself against internal and external cybersecurity risks. <Organization name> has developed this cybersecurity strategy to support <organization name>'s business strategy, address threats and mitigate cyber risks.

This document aims to comply with cybersecurity requirements as well as the relevant legislative and regulatory requirements. This is a regulatory requirement stated in control no. 1-1-1 of the Essential Cybersecurity Controls (ECC-1: 2018) issued by NCA.

Scope of work and Applicability

This cybersecurity roadmap covers all of <organization name>'s business. <Organization name>and its subsidiaries will ensure that this roadmap is implemented.

The cybersecurity roadmap applies to the following organizations and subsidiaries:

4- <organization name 1>.
5- <organization name 2>.
6- ...

Since initiatives set out in the roadmap apply to and affect the organizations and the subsidiaries, their implementation will be agreed upon in coordination with these subsidiaries.

Cybersecurity Roadmap

1- Set an action plan to achieve the cybersecurity strategy objectives.

2- The strategy provides the key elements for an action plan comprised of cybersecurity initiatives that, if implemented, achieve the cybersecurity objectives (detailed in Cybersecurity Objectives Section).

3- The strategy action plan shall be formulated based on regulatory policies and procedures of <organization name> as well as the relevant legislative and regulatory requirements.

4- The strategy action plan includes items related to monitoring and KPIs in order to measure success level, enabling feedback to be submitted to the <head of the cybersecurity function> and the CSC. This would allow to introduce amendments to the plan and ensure that cybersecurity initiatives are properly implemented to achieve the defined objectives.

5- The cybersecurity roadmap reflects the distribution of the initiatives to be implemented over the next three years. Priority will be given to cybersecurity initiatives based on the following:

5-1 The results of the risk analysis and business impact analysis (BIA) described in the Risk Assessment and Business Impact Analysis section, while prioritizing higher risks.

5-2 Results of shortlisting critical systems, while prioritizing relevant initiatives.

Cybersecurity roadmap

Cybersecurity Roadmap.xlsx

Projects and Initiatives List

1- <Organization name> has developed detailed cybersecurity initiatives and projects profiles as per the following sheet:

Cybersecurity Programs and Initiatives Profiles

Cybersecurity Initiative and Project F

Cybersecurity Budget

The cybersecurity budget aims to determine the required budget to implement cybersecurity action plan and initiatives, and to obtain the necessary funds from <finance function>.

Budget Characteristics

1- The <cybersecurity function> is responsible for determining the cybersecurity budget as the best way to ensure the availability of cybersecurity technologies and tools. The <head of cybersecurity function> shall provide a summary of the cybersecurity budget to the <Authorizing Official>.

2- Cybersecurity budget shall be allocated to cover all costs of cybersecurity action plan. It should be accurate, rational and inclusive of all expected expenses.

3- Cybersecurity budget should be compliant with the relevant policies, legislative and regulatory requirements, orders, and decisions.

4- Cybersecurity budget shall be based on the yearly budget cycle of <organization name>.

5- Cybersecurity budget shall be subject to regular revision according to <organization name>'s policies and procedures.

Budget Components

1- The cybersecurity budget comprises of the following components:

1-1 Budget for operating the cybersecurity function, including:

1-1-1 Human resources costs.

1-1-2 Consulting services costs.

1-1-3 Technology costs.

1-1-4 Other costs.

1-2 Budget for the cybersecurity initiatives, including:

1-2-1 One-off costs to setup the cybersecurity function and related processes to implement the cybersecurity strategy.

1-2-2 Recurring costs covering cybersecurity measures (e.g. cybersecurity management, monitoring, reporting, compliance, etc.)

1-2-3 Cost of specialized skills development programs and required trainings for cybersecurity personnel, such as training courses and conferences.

1-2-4 Outsourcing costs.

Cybersecurity budget calculation

1- The <organization name> cybersecurity budget has been calculated according to the following sheet:

Cybersecurity budget calculation

Cybersecurity Budget.xlsx

2- The cybersecurity budget allocated by <organization name> for the cybersecurity strategy for the next three years amounts to: <determined by the organization> SAR.

RFPs

1- <Organization name> has set detailed data for RFPs regarding the cybersecurity strategy and roadmap according to the following templates adopted by MoF and the Center of Spending Efficiency, such as (but not limited to), kindly click on the below links:

RFP template (consulting services)

RFP template (IT services)

Other
(such as templates submitted by the Center of Spending Efficiency, etc.)

Roles and Responsibilities

1. **Document Owner:** <head of cybersecurity function>.
2. **Document Review and Update:** <cybersecurity function>
3. **Document Implementation and Execution:** <cybersecurity function>.
4. **Document Compliance Measurement:** <cybersecurity function>.

Update and Review

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