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

Insert organization logo by clicking on the outlined image.

Cybersecurity Risk Management Policy 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 legal 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

Purpose

This policy aims to define the cybersecurity requirements related to <organization name>'s cybersecurity risk management to achieve the main objective of this policy which is minimizing cybersecurity risks resulting from internal and external threats at <organization's name>.

The requirements in this policy are aligned with the cybersecurity requirements issued by the National Cybersecurity Authority (NCA) including but not limited to (ECC-1:2018) and (CSCC-1:2019), in addition to other related legal and regulatory requirements.

Scope

This policy covers all information and technology assets and systems in the <organization name> in addition to its work procedures in <organization name> and applies to all personnel (employees and contractors) in the <organization name>.

Policy Statements

1- General Requirements

1-1 Cybersecurity Risk Management Methodology and cybersecurity risk management procedures in <organization name> must be defined, documented and approved, while ensuring its alignment with the National Cybersecurity Risk Management Framework, which has already been aligned with internationally approved standards and guidelines (e.g. ISO27005, ISO31000, NIST).

1-2 The Cybersecurity Risk Management Methodology must serve the following purposes:

1-2-1 Define, collect, and list assets, then classify and prioritize them based on the level of protection required.

1-2-2 Define and evaluate risks to the business, assets, or personnel of <organization name> (e.g. cybersecurity risks on <organization name>).

1-2-3 Evaluate cybersecurity risks in planning and before approving use of social media as well as telework for any service or system.

1-2-4 Define and evaluate information and technology assets vulnerability to specific threats.

1-2-5 Define decisions to respond to such risks.

1-2-6 Prioritize risk response plans based on specific procedures.

1-2-7 Classify and define risk levels based on the risk probability and impact on <organization name>.

1-2-8 Define the roles and responsibilities to manage and deal with cybersecurity risk.

1-3 A periodic risk assessment must be conducted to ensure security of information and technology assets and prioritization of risk levels.

1-4 Cybersecurity risks must be managed in a methodological approach to protect information and technology assets in <organization name>.

1-5 Cybersecurity risks in <organization name> must be managed and overseen on a continuous basis.

1-6 Cybersecurity Risk Management must be aligned with the Enterprise Risk Management “ERM” in <organization name>.

1-7 Risk management related recommendations, issued by NCA, must be applied.

1-8 Key performance indicators (KPI) must be used to ensure the continuous improvement and effective and efficient use of Cybersecurity Risk Management requirements.

2- Main Stages for Cybersecurity Risks Management

2-1 **Risk Identification**:

This process must cover the following:

2-1-1 Assets must be identified and an inventory list must be prepared with prioritized list and classifications.

2-1-2 Potential vulnerabilities and threats on assets must be identified.

2-1-3 Current risks on assets must be identified through:

2-1-3-1 Developing potential risks scenarios as per the identified vulnerabilities, threats and attacks.

2-1-3-2 Identifying currently applied cybersecurity controls to counter identified risks.

2-2 **Risk Assessment:**

2-2-1 The <cybersecurity function> must implement cybersecurity risk assessment procedures as a minimum in the following cases:

2-2-1-1 Every 3 years at least for all information and technology assets, and at least once a year for critical systems, telework systems, and social media accounts.

2-2-1-2 At early stages of technology projects.

2-2-1-3 Before making major changes to infrastructure.

2-2-1-4 When planning to acquire new services from a third party.

2-2-1-5 At the planning stage and before the launch of new technology products and services.

2-2-2 Risks must be re-assessed and updated as follows:

2-2-2-1 After a cybersecurity incident that compromises information and technology asset integrity, availability, or confidentiality.

2-2-2-2 After a significant audit findings or proactive data.

2-2-2-3 Whenever information and technology assets experience significant enhancement or modification.

2-2-3 Current risks assessment process must cover the following:

2-2-3-1 **Risk Analysis:** The <organization name> must assess the likelihood of threats, assess their consequences

and use results to determine the overall risk level. The <organization name> must adopt a Quantitative or Qualitative methodology to conduct risk analysis.

2-2-3-2 **Risk Evaluation**: The <organization name> must evaluate cybersecurity risk against its adopted enterprise risk evaluation criteria in the <organization name> to prioritize such risks.

2-3 **Risk Response:**

2-3-1 The <organization name> must select the risk response decision based on the following:

2-3-1-1 **Risk Mitigation**: Mitigate or reduce risk degree by applying the necessary security controls to reduce the likelihood or impact or both, which help control risks and bring them to a level that could be accepted. The organization must do the following:

- Identifying, documenting and prioritizing risk response plans to deal with current risks.
- Executing risk response plans based on priority.
- Calculating residual risks after conducting risk response plans.

2-3-1-2 **Risk Avoidance**: Remove risk by avoiding the conditions that create it.

2-3-1-2-1 Risk Transfer: Pass the risk to a third party that has better capabilities to deal with it or insure information and technology assets against cybersecurity risks.

2-3-1-2-2 Risk Acceptance: Risk level is acceptable but in <organization name> continuous monitoring is required in case of any change.

2-3-2 Risk treatment options must be selected and documented based on the outcomes of risk assessment, cost of implementation and expected benefits.

2-4 Risk Oversight:

2-4-1 To oversee risks, <organization name> must develop and maintain a risk register to document outcomes of risk management process. This must include at a minimum the following information:

2-4-1-1 Risk identifier.

2-4-1-2 Scope of risks.

2-4-1-3 Risk Owner.

2-4-1-4 Description of risks including their causes and impacts.

2-4-1-5 Risk analysis highlighting risk consequences and their timescale.

2-4-1-6 Risk evaluation and rating covering risk likelihood and magnitude and overall risk rating if the risk occurs.

2-4-1-7 Risk treatment plan covering risk treatment action, owner, timeline.

2-4-1-8 Residual risk description.

2-4-2 Cybersecurity risk register must be created for operations, cloud computing services, and critical systems and periodically oversee it in alignment with the risk profile.

2-4-3 Cybersecurity risks related to telework systems, services and systems allowed to work remotely, social media accounts, and the services and systems used must be included in the organization cybersecurity risk register and oversee them at least once a year.

2-4-4 The <organization name> must collect and review guides related to cybersecurity risks state on an annual basis.

2-4-5 Risk management reports must be developed.

3- Risk Appetite:

3-1 Criteria for risk appetite must be defined and documented as per risk level and cost of treatment compared to impact.

3-2 Risk appetite level must be defined for cloud computing services.

3-3 If a residual risk does not match the criteria of risk appetite, further controls to reduce risks to an acceptable level must be applied.

3-4 If a residual risk does not match the criteria of risk appetite, further controls to reduce risks to an acceptable level must be applied.

4- Cybersecurity risks in OT/ICS

4-1 OT/ICS cybersecurity risk methodology must be developed as part of risk management methodology and safety risk management and procedures adopted in <organization name>.

4-2 OT/ICS cybersecurity risks must be evaluated periodically along with the risks of signing contracts and agreements with external parties concerned with OT/ICS and /or when changes to relevant legal and regulatory requirements occur , as part of the assessment.

4-3 A cybersecurity risk register related to OT/ICS must be included in the risk register of <organization name>.

4-4 Appropriate levels of areas and facilities containing OT/ICS must be defined based on an approved methodology.

4-5 A qualitative analysis of cybersecurity risks must be included in the Process Hazard Analysis procedures, which applies to any change in processes, procedures, or factories.

4-6 In the event that the cybersecurity requirements cannot be met within the OT/ICS environment, the necessary justifications must be clarified and documented, approved by the <cybersecurity function> and also approved by the representative.

4-7 If cybersecurity risk appetite is approved, alternative controls must be identified, documented and approved by the representative and reviewed by the <cybersecurity function> to make sure they are effectively and timely implemented, while assessing and reviewing those risks on a continuous basis.

Roles and Responsibilities

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

Update and Review

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

Compliance

1- The <head of the cybersecurity function> will ensure compliance of <organization name> with this policy on a regular basis.
2- All personnel at <organization name> must comply with this policy.
3- Any violation of this policy may be subject to disciplinary action as per <organization name>'s procedures.