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 placeholder to the left.

Cybersecurity Risk Management Procedure 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 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 procedure defines the detailed step-by-step requirements for cybersecurity risk management for <organization name>. These requirements are aligned with best practices and the Risk Management Policy.

The requirements in this procedure are also 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 cybersecurity legal and regulatory requirements.

Scope

This procedure covers <organization name>'s cybersecurity risk management process and applies to all personnel (employees and contractors) in <organization name>.

Overview of the cybersecurity risk management process

The cybersecurity risk management process should be inclusive of the following steps:

1. Identifying scope, context, criteria
2. cybersecurity risk assessment process
   2.1 Risk identification
   2.2 Risk analysis
   2.3 Risk evaluation
3. cybersecurity risk treatment
4. Recording and reporting
5. Communication and Monitoring

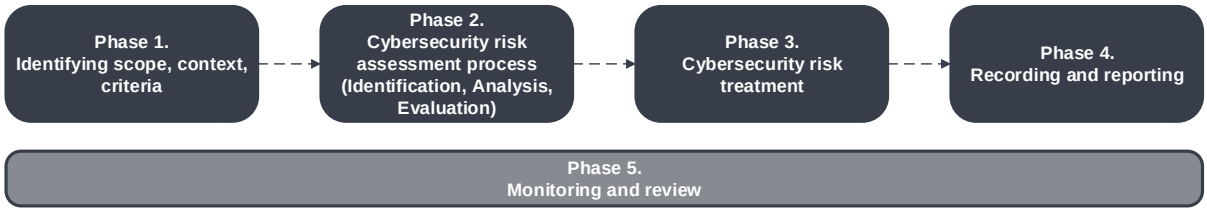

Figure 1 – Overview of the phases of the procedure

Details of the cybersecurity risk management process

Phase 1. Identifying scope, context, criteria

Figure 2 - Identifying scope, context, criteria phase workflow

Choose Classification

No.	Step	Description	Owner/ Responsible	Inputs	Outputs	Stakeholders
1.1	Process coordination	Coordination of the whole process of the cybersecurity risk management in the <organization name>.	Cybersecurity Function	Existing documentation regarding cybersecurity risk management	Coordinated steps of the process	Cybersecurity Function
1.2	Assets and processes identification	Assets and processes which are relevant for the <organization name> and the way they are used by the <organization name> have to be identified.	Cybersecurity Function, Head of Functions, Asset Owners, Process Owners	Assets and processes in the <organization name>	Identified relevant assets and processes in the <organization name>	Cybersecurity Function, Head of Functions, Asset Owners, Process Owners
1.3	Context	Internal and external context of the	Cybersecurity	Goals and	Identified	Cybersecurity

	identification	cybersecurity risk management process in which the <organization name> seeks to define and achieve its objectives have to be identified. The context of the cybersecurity risk management process has to be based on the understanding of the external and internal environment in which the <organization name> operates and should reflect the specific environment of the activity to which the cybersecurity risk management process is to be applied. Especially following factors have to be considered: 1. Cybersecurity risk assessment alignment with internal relations, objectives and policies. 2. Systems and technologies	Function	objectives of the <organization name>, existing assets, external factors	context of the cybersecurity risk management in the <organization name>	Function

		(infrastructure and assets) model. 3. Social, cultural, political, legal, regulatory, financial, technological and economic factors, whether international, national, regional or local that may affect the cybersecurity risk assessment. 4. External stakeholders' relationships, perceptions, values, needs and expectations. Contractual relationships and commitments and arrangements with third party vendors.				
1.4	Criteria	Criteria to evaluate the significance of the cybersecurity risk and to support	Cybersecurity	Identified context of the	Identified criteria for the	Cybersecurity

	identification	decision making processes have to be defined. Cybersecurity risk criteria should be aligned with the <organization name>'s cybersecurity risk management framework and customized to the specific purpose and scope of the activity under consideration. Cybersecurity risk criteria should reflect the <organization name>'s values, objectives and resources and be consistent with policies and statements about cybersecurity risk management. The criteria should be defined taking into consideration the <organization name>'s obligations and the views of stakeholders. To set criteria, the following should be considered; 1. The nature and type of uncertainties that can affect	Function	cybersecurity risk management	cybersecurity risk management	Function

		outcomes and objectives (both tangible and intangible) 2. How consequences (both positive and negative) and likelihood will be defined and measured 3. Time-related factors 4. Consistency in the use of measurements 5. How the level of cybersecurity risk is to be determined 6. How combinations and sequences of multiple cybersecurity risks will be taken into account The <organization name>'s capacity.				

1.5	Criteria review and update	While risk criteria should be established at the beginning of the cybersecurity risk assessment process, they are dynamic and should be continually reviewed and amended, if necessary.	Cybersecurity Function	Identified criteria for the cybersecurity risk management	Reviewed and updated criteria	Cybersecurity Function
1.6	Definition of risk appetite	Cybersecurity risk appetite has to be defined. Criteria for cybersecurity risk appetite definition have to be defined and documented as per cybersecurity risk level and cost of treatment compared to impact.	Cybersecurity Function, Risk Management Team	Identified scope, context and criteria	Defined cybersecurity risk appetite	Cybersecurity Function, Risk Management Team
1.7	Approval of scope, context, criteria and risk appetite	Identified scope, context, criteria and defined cybersecurity risk appetite have to be approved.	Head of the Cybersecurity Function	Identified scope, context, criteria and risk appetite	Approved scope, context, criteria and risk appetite	Head of the Cybersecurity Function

Phase 2. Cybersecurity risk assessment process

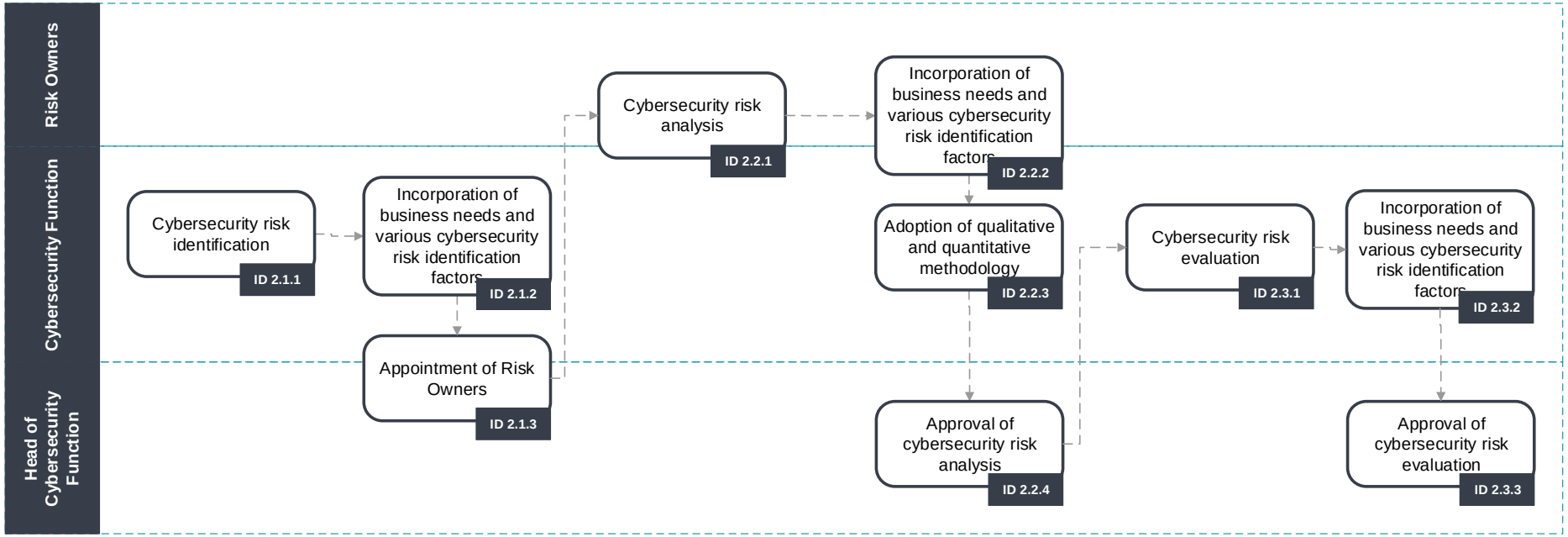

Figure 3 - Cybersecurity risk assessment phase workflow

Phase 2.1. Cybersecurity risk identification

No.	Step	Description	Owner/ Responsible	Inputs	Outputs	Stakeholders
2.1.1	Cybersecurity risk identification	Cybersecurity risks to <organization name>'s business, assets or personnel have to be identified. The purpose of cybersecurity risk identification is to find, recognize and describe cybersecurity risks that might help or prevent an organization achieving its objectives. All events and circumstances that could compromise the confidentiality, integrity and availability of information and technology assets have to be identified. In particular, this will involve identification of the information and technology assets, potential threats to those assets, relevant vulnerabilities	Cybersecurity Function	Information on <organization name>'s business, assets and personnel	Identified cybersecurity risks	Cybersecurity Function

No.	Step	Description	Owner/ Responsible	Inputs	Outputs	Stakeholders
		and existing controls and then identifying the consequences of loss of confidentiality, integrity and availability of those assets. Cybersecurity risks, whether or not their sources are under the control of risk owners but in their area of interests, have to be identified. Consideration has to be given that there may be more than one type of outcome, which may result in a variety of tangible or intangible consequences.				

No.	Step	Description	Owner/ Responsible	Inputs	Outputs	Stakeholders
2.1.2	Incorporation of business needs and various cybersecurity risk identification factors	During the cybersecurity risk identification process the following factors have to be considered: 1. Tangible and intangible sources of cybersecurity risk. 2. Causes and events. 3. Threats and opportunities. 4. Vulnerabilities and capabilities. 5. Changes in the external and internal context. 6. Indicators of emerging cybersecurity risks. 7. The nature and value of assets and resources.	Cybersecurity Function	Identified cybersecurity risks, Business needs	Adjusted list of cybersecurity risks	Cybersecurity Function

No.	Step	Description	Owner/ Responsible	Inputs	Outputs	Stakeholders
		8. Consequences and their impact on objectives. 9. Limitations of knowledge and reliability of information. 10. Time-related factors. 11. Biases, assumptions and beliefs of those involved.				
2.1.3	Appointment of risk owners	Risk Owners - heads of functions or asset and process owners who will be involved in the process of cybersecurity risk management have to be appointed.	Head of the Cybersecurity Function, Cybersecurity Function	List of cybersecurity risks	Risk Owners appointed for each of identified cybersecurity risks	Head of the Cybersecurity Function, Risk owners, Cybersecurity Function

Phase 2.2. Cybersecurity risk analysis

No.	Step	Description	Owner/ Responsible	Inputs	Outputs	Stakeholders
2.2.1	Cybersecurity risk analysis	The analysis of identified inherent cybersecurity risks have to be performed in coordination with all relevant stakeholders. Likelihood and magnitude/impact of the threats and their consequences should be assessed and based on that overall cybersecurity risk level should be estimated.	Cybersecurity Function, Risk Owners	List of cybersecurity risks	Estimated risk level for each of the cybersecurity risks	Cybersecurity Function, Risk Owners
2.2.2	Incorporation of business needs and various cybersecurity risk identification	While performing the analysis a detailed consideration of uncertainties, cybersecurity risk sources, consequences, likelihood, events, scenarios, controls and their effectiveness have to be involved.	Cybersecurity Function, Risk Owners	List of cybersecurity risks, Estimated risk level for each of the cybersecurity	Adjusted list of cybersecurity risks	Cybersecurity Function, Risk Owners

No.	Step	Description	Owner/ Responsible	Inputs	Outputs	Stakeholders
	factors	Divergence of opinions, biases, perceptions of cybersecurity risk, judgements, quality of the information used, the assumptions and exclusions made, any limitations of the techniques and how they are executed have to be taken under consideration as they may influence the cybersecurity risk analysis. These factors have to be documented and communicated to decision makers.		risks		
2.2.3	Adoption of qualitative and quantitative methodology	A qualitative and/or quantitative methodology might be adopted to conduct the inherent cybersecurity risk analysis based on ones using by risk management function.	Cybersecurity Function	List of cybersecurity risks	Calculated overall risk rating, evaluated criticality	Cybersecurity Function

No.	Step	Description	Owner/ Responsible	Inputs	Outputs	Stakeholders
		Quantitative methodology should be adopted for every cybersecurity risk analysis in order to calculate the overall risk rating and to evaluate it criticality and compare it against the risk appetite. Qualitative methodology should be used for assessment of very complex risks where many factors have to be considered. Qualitative methodology can also be good basis for the usage of quantitative methodology.			comparted against risk appetite	
2.2.4	Approval of cybersecurity risk analysis	Results of cybersecurity risk analysis have to be approved.	Head of the Cybersecurity Function	List of cybersecurity risks, calculated	Approved results of cybersecurity risks analysis	Head of the Cybersecurity Function

No.	Step	Description	Owner/ Responsible	Inputs	Outputs	Stakeholders
				overall risk rating, evaluated criticality comparted against risk appetite		

Phase 2.3. Cybersecurity risk evaluation

No.	Step	Description	Owner/ Responsible	Inputs	Outputs	Stakeholders
2.3.1	Cybersecurity risk evaluation	Cybersecurity risks have to be evaluated against <organization name>'s defined cybersecurity risk	Cybersecurity Function	List of cybersecurity risks	Cybersecurity risks evaluated	Cybersecurity Function

No.	Step	Description	Owner/ Responsible	Inputs	Outputs	Stakeholders
		evaluation criteria in order to determine next steps and assess the priority of the cybersecurity risk treatment actions. Following decisions are possible: 1. Consider cybersecurity risk treatment options. 2. Undertake further analysis to better understand the cybersecurity risk. 3. Reconsider objectives.			against defined criteria	
2.3.2	Incorporation of business needs and	Decisions have to take account of the wider context and the actual and perceived consequences to external	Cybersecurity Function	Cybersecurity risks evaluated	Adjusted list of	Cybersecurity Function

No.	Step	Description	Owner/ Responsible	Inputs	Outputs	Stakeholders
	various cybersecurity risk identification factors	and internal stakeholders.		against defined criteria, Business needs	cybersecurity risks	
2.3.3	Approval of cybersecurity risk evaluation	Performed cybersecurity risk evaluation have to be approved.	Head of the Cybersecurity Function	List of cybersecurity risks, Cybersecurity risks evaluated against defined criteria	Approved results of cybersecurity risks evaluation	Head of the Cybersecurity Function

Phase 3. Cybersecurity risk treatment

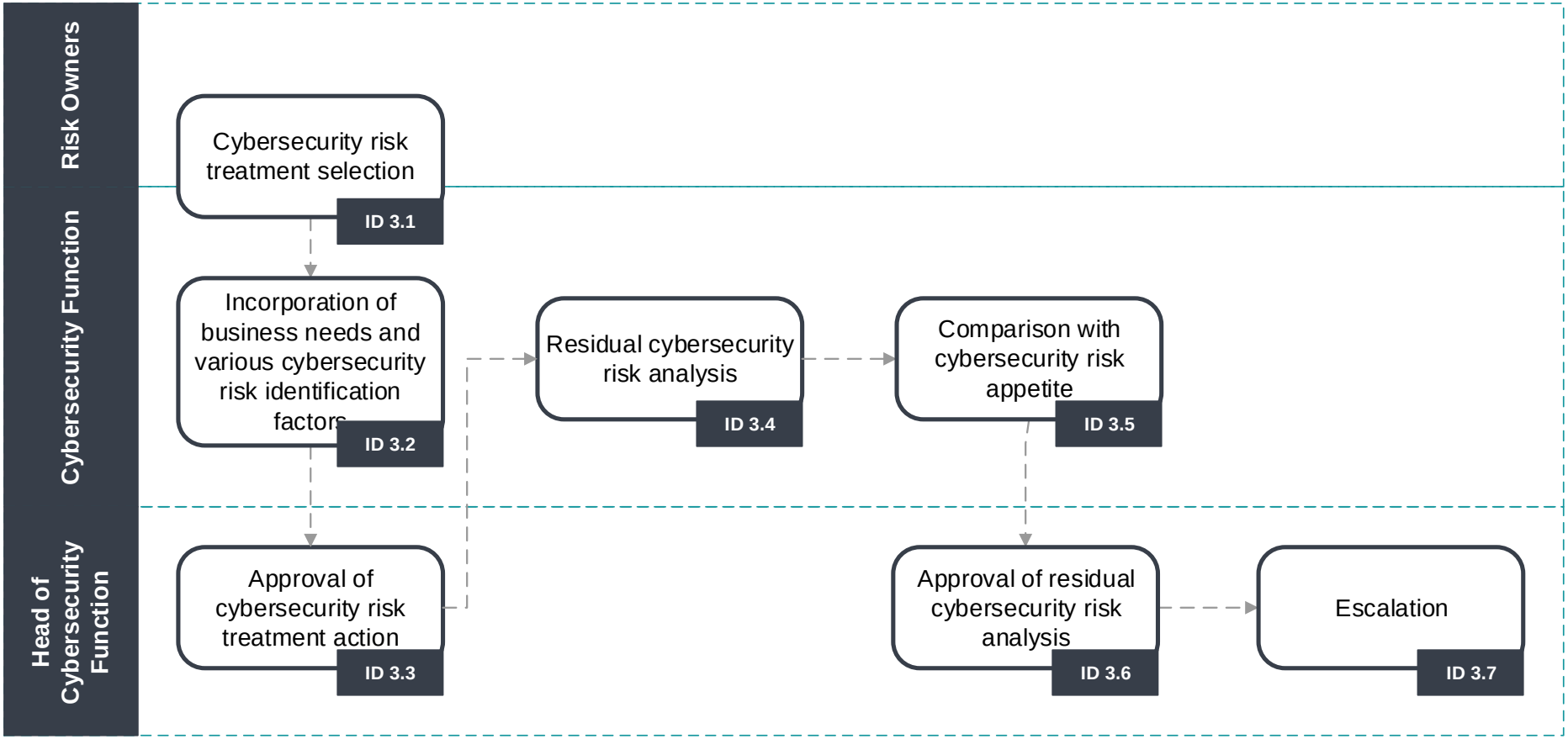

Figure 4 - Cybersecurity risk treatment phase workflow

No.	Step	Description	Owner/ Responsible	Inputs	Outputs	Stakeholders
3.1.	Cybersecurity risk treatment selection	Cybersecurity risk treatment options have to be selected out of the following: 1. Cybersecurity risk mitigation: mitigate cybersecurity risk by applying the required security controls to reduce the likelihood or magnitude/impact or both, and to bring the cybersecurity risk rating to a level that could be accepted. 2. Cybersecurity risk avoidance: avoid the circumstances and conditions that create the cybersecurity risk.	Cybersecurity Function, Risk Owners	List of cybersecurity risks	Selected cybersecurity risk treatment options	Cybersecurity Function, Risk Owners, Controls implementer

No.	Step	Description	Owner/ Responsible	Inputs	Outputs	Stakeholders
		3. Cybersecurity risk transfer: pass the cybersecurity risk to a third party that has better capabilities to deal with the cybersecurity risk or insure information and technology assets against cybersecurity risk. 4. Cybersecurity risk acceptance: cybersecurity risk level is acceptable but continuous monitoring is required in case of any change.				
3.2.	Incorporation of business needs and	Cybersecurity risk treatment has to be selected and documented based on the outcomes of the previously performed cybersecurity risk	Cybersecurity Function	Selected cybersecurity risk treatment	Adjusted cybersecurity risk treatment	Cybersecurity Function

No.	Step	Description	Owner/ Responsible	Inputs	Outputs	Stakeholders
	various cybersecurity risk identification factors	assessment, cost of implementation analysis and the expected benefits.		options, Business needs	options	
3.3.	Approval of cybersecurity risk treatment action	Selected cybersecurity risk treatment action has to be approved.	Head of the Cybersecurity Function	Adjusted cybersecurity risk treatment options	Approved cybersecurity risk treatment actions	Head of the Cybersecurity Function, Risk owners
3.4.	Residual cybersecurity risk analysis	Residual cybersecurity risk analysis has to be performed, particularly cybersecurity risk likelihood and magnitude/impact should be estimated.	Cybersecurity Function	Approved cybersecurity risk treatment actions	Analyzed residual cybersecurity risk	Cybersecurity Function

No.	Step	Description	Owner/ Responsible	Inputs	Outputs	Stakeholders
3.5.	Comparison with cybersecurity risk appetite	Residual cybersecurity risk rating should be compared with the cybersecurity risk appetite. In case residual cybersecurity risk exceeds risk appetite further controls to reduce cybersecurity risk to an acceptable level have to be applied.	Cybersecurity Function	Analyzed residual cybersecurity risk	Results of comparison of residual cybersecurity risk with risk appetite	Cybersecurity Function
3.6.	Approval of residual cybersecurity risk analysis	Residual cybersecurity risk analysis and the outcome of its comparison with cybersecurity risk appetite have to be approved.	Head of the Cybersecurity Function	Results of comparison of residual cybersecurity risk with risk appetite	Approved results of comparison of residual cybersecurity risk with risk appetite	Head of the Cybersecurity Function
3.7.	Escalation	If the residual cybersecurity risk	Head of the	Residual	Escalation to	Head of the

No.	Step	Description	Owner/ Responsible	Inputs	Outputs	Stakeholders
		cannot be reduced to the level of cybersecurity risk appetite or cost of it exceeds the profits, the matter has to be escalated to the <organization name> head to take the necessary actions or decisions.	Cybersecurity Function	cybersecurity risk exceeds risk appetite, or its cost exceeds the profits	the <organization name>'s head	Cybersecurity Function, Head of the <organization name>

Phase 4. Recording and reporting

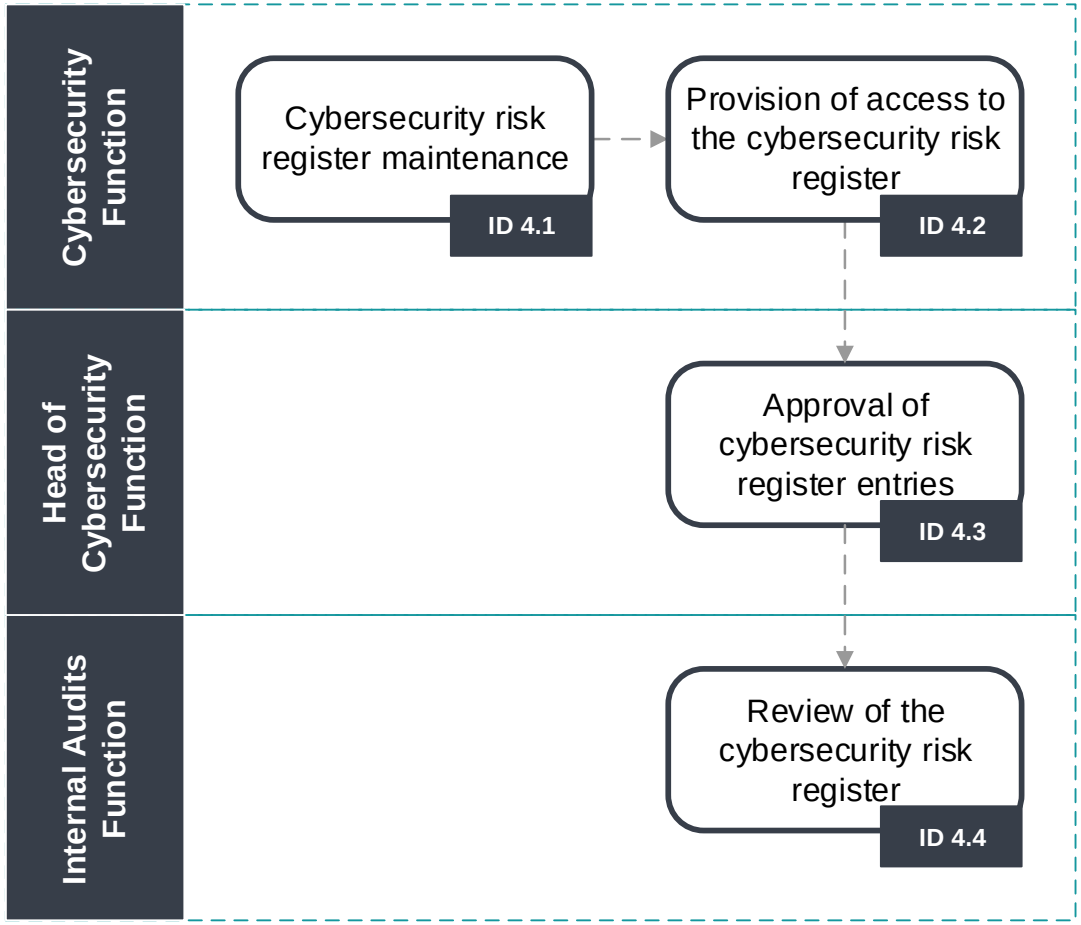

Figure 5 - Recording and reporting phase workflow

No.	Step	Description	Owner/ Responsible	Inputs	Outputs	Stakeholders
4.1	Cybersecurity risk register maintenance	Cybersecurity risk register has to be developed and maintained up to date in order to document the outcomes of the cybersecurity risk management process. Register should include at a minimum the following information: 1. Cybersecurity risk identifier 2. Scope of cybersecurity risk (area of cybersecurity risk) 3. Cybersecurity risk owner 4. Description of the cybersecurity risk including its cause and impact 5. Cybersecurity risk analysis highlighting the cybersecurity	Cybersecurity Function	List of cybersecurity risks, Risk owners, Cybersecurity risk treatment options, Analyzed residual cybersecurity risk	Cybersecurity risk register	Cybersecurity Function

No.	Step	Description	Owner/ Responsible	Inputs	Outputs	Stakeholders
		risk consequences and their timescale 6. Cybersecurity risk evaluation and rating covering the cybersecurity risk likelihood and magnitude/impact and overall cybersecurity risk rating if the cybersecurity risk materializes 7. Cybersecurity risk treatment plan covering the cybersecurity risk treatment action, owner and timeline 8. Residual cybersecurity risk description and analysis				

No.	Step	Description	Owner/ Responsible	Inputs	Outputs	Stakeholders
		9. Description of the following steps.				
4.2	Provision of access to the cybersecurity risk register	Access to the cybersecurity risk register has to be provided to all relevant stakeholders, based on the “Need-to-Know” principle.	Cybersecurity Function	Cybersecurity risk register	Access to cybersecurity risk register granted to relevant stakeholders	Cybersecurity Function
4.3	Approval of cybersecurity risk register entries	All newly added entries made to the cybersecurity risk register and provisions of access to it have to be approved.	Head of the Cybersecurity Function	Cybersecurity risk register	Approved cybersecurity risk register and granted access	Head of the Cybersecurity Function
4.4	Review of the	Cybersecurity risk register should be	Internal Audit	Cybersecurity	Reviewed	Internal Audit

No.	Step	Description	Owner/ Responsible	Inputs	Outputs	Stakeholders
	cybersecurity risk register	reviewed at least annually especially in the matter of cybersecurity risk treatment action implementation.	Functions	risk register	cybersecurity risk register	Functions

Phase 5. Communication and monitoring

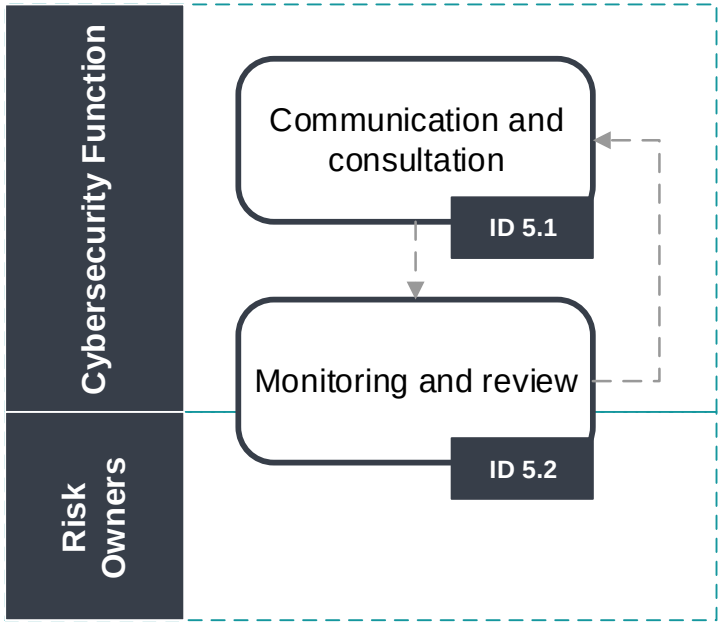

Figure 6 - Communication and monitoring phase workflow

No.	Step	Description	Owner/ Responsible	Inputs	Outputs	Stakeholders
5.1	Communication and	All steps and actions taken during the cybersecurity risk management	Cybersecurity	All steps in	Taken actions are clearly	Cybersecurity

No.	Step	Description	Owner/ Responsible	Inputs	Outputs	Stakeholders
	consultation	process have to be communicated and consulted with all relevant internal and external stakeholders. The purpose of this is to provide better understanding and rationale of all action taken with respect to the cybersecurity risk management process.	Function	the process	communicated to and consulted with relevant stakeholders	Function
5.2	Monitoring and review	All identified cybersecurity risks and applied cybersecurity risk treatment measures have to be continuously monitored and reviewed. Monitoring and review should take place in all stages of the process.	Cybersecurity Function, Risk Owners	Cybersecurity risk register	Cybersecurity risk register is monitored and reviewed	Cybersecurity Function, Risk Owners

Roles and Responsibilities

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

Update and Review

<cybersecurity function> must review the procedure 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 procedure on a regular basis.
2- This procedure covers all workstations and servers in the <organization name> and applies to all personnel at <organization name>.
3- Any violation of this procedure may be subject to disciplinary action according to <organization name>'s procedures.