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 Audit Procedure 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

Purpose

This procedure aims to define the detailed step-by-step cybersecurity requirements related to the cybersecurity audit and review process for <organization name>. These requirements are aligned with international best practices and are based on the <organization name> 's Cybersecurity Review and Audit Policy. The ability of <organization name> to perform audits and reviews in accordance with this procedure will assist in preserving the availability, integrity and confidentiality of <organization name>'s assets and information.

The requirements in this procedure are aligned with the cybersecurity requirements issued by the National Cybersecurity Authority (NCA) in addition to other related cybersecurity legal and regulatory requirements.

Scope

This procedure covers <organization name>'s cybersecurity audit and review process in relation to all cybersecurity controls and applies to all personnel (employees and contractors) in <organization name>.

Overview of the cybersecurity audit and review process

According to <organization name> internal policies and applicable best practices, and standards, the Cybersecurity Audit and Review Process must be divided into the following phases:

1. Development of the audit plan,
2. Audit/review preparation,
3. Audit/review execution,
4. Reporting and documentation of cybersecurity audit/review findings,
5. Presentation of findings to the Cybersecurity Steering Committee and the organization head,
6. Monitoring and review.

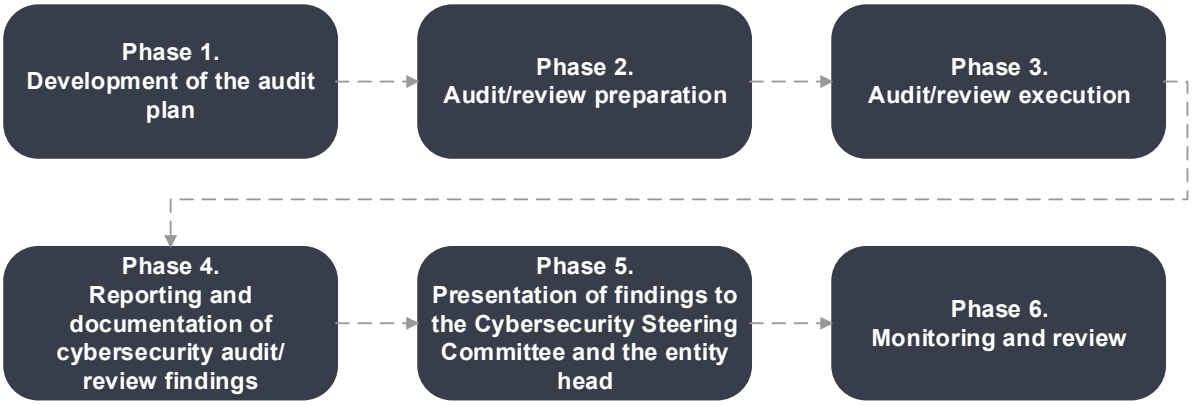

Figure 1 - Overview of the phases of the procedure

The audit or review may be performed either internally by personnel of Internal Audit Function (for audits) and Cybersecurity Function (reviews) or externally by an External Auditor from an independent third party.

Details of the cybersecurity audit process

Phase 1. Development of the audit plan

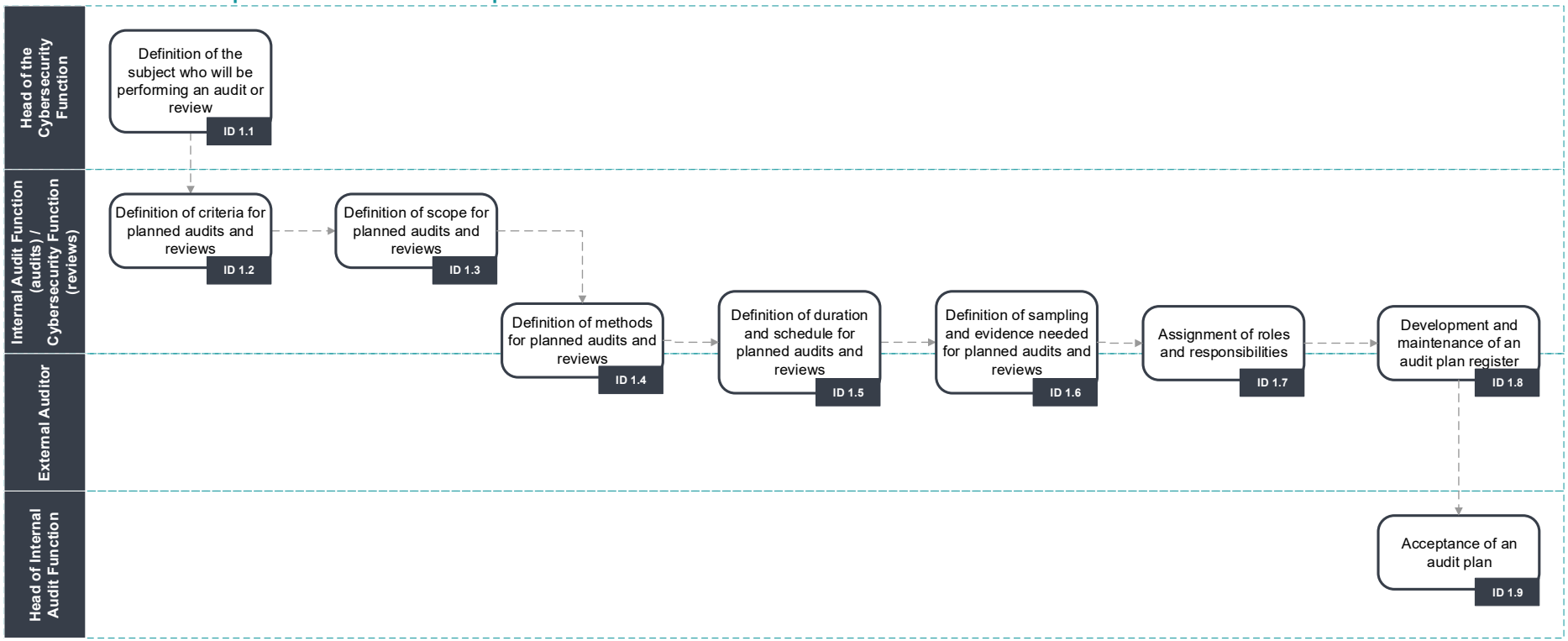

Figure 2 - Development of the audit plan phase workflow

No.	Step	Description	Owner/Responsible	Inputs	Outputs	Stakeholders
1.1	Definition of the subject who will be performing an audit or review	Subject who will be responsible for performing an audit have to be defined based on the Cybersecurity Review and Audit Policy requirements.	Head of the Cybersecurity Function	Decision to perform audit/review	Defined subject	Head of the Cybersecurity Function
1.2	Definition of criteria for planned audits and reviews	Criteria for the audit and review program must be defined. Cybersecurity controls issued by the National Cybersecurity Authority such as Essential Cybersecurity Controls (ECC-1:2018), Critical Systems Cybersecurity Controls (CSCC-1:2019), and any other applicable controls issued by the National Cybersecurity Authority should be used as the basis for criteria definition.	Internal Audit Function (audits), Cybersecurity Function (reviews)	Decision to perform audit/review	Defined criteria	Internal Audit Function (audits), Cybersecurity Function (reviews)

No.	Step	Description	Owner/Responsible	Inputs	Outputs	Stakeholders
1.3	Definition of scope for planned audits and reviews	Scope of planned audits and reviews must be defined based on the Cybersecurity Review and Audit Policy requirements.	Internal Audit Function (audits), Cybersecurity Function (reviews)	Decision to perform audit/review, Defined criteria	Defined scope	Internal Audit Function (audits), Cybersecurity Function (reviews)
1.4	Definition of methods for planned audits and reviews	Methods for audits and reviews have to be defined and should be based on internally developed methodology, best practices or international standards (e.g., ISO19011). Particular methodology should be based on risk assigned to the verified controls. Possible approaches are: 1. Inquiry – seeking information of knowledgeable persons. It may be used extensively throughout	Internal Audit Function (audits), Cybersecurity Function (reviews), External Auditor (audits and reviews)	Defined criteria, scope and type	Defined methods	Internal Audit Function (audits), Cybersecurity Function (reviews), External Auditor (audits and reviews)

No.	Step	Description	Owner/Responsible	Inputs	Outputs	Stakeholders
		the audit or review in addition to other audit or review procedures. 2. Observation - consists of looking at a process or procedure being performed by others. 3. Inspection - involves examining records or documents, whether internal or external, in paper form, electronic form, or other media, or a physical examination of an asset. 4. Reperformance - involves the auditor's independent execution of procedures or controls that were originally performed as part of the organization's internal control.				

No.	Step	Description	Owner/Responsible	Inputs	Outputs	Stakeholders
		Their combination can also be implemented.				
1.5	Definition of duration and schedule for planned audits and reviews	Duration and schedule for planned audits and reviews must be defined. Frequency of audits and reviews should be based on the Cybersecurity Review and Audit Policy requirements.	Internal Audit Function (audits), Cybersecurity Function (reviews), External Auditor (audits and reviews)	Defined criteria, scope, type and methods	Defined duration and schedule	Internal Audit Function (audits), Cybersecurity Function (reviews), External Auditor (audits and reviews)
1.6	Definition of sampling and evidence needed for planned	Sampling and evidence (e.g., procedures and policies, data and screenshots from IT (Information Technology) systems, configuration parameters) required for planned	Internal Audit Function (audits), Cybersecurity Function	Defined criteria, scope, type, methods, duration and	Defined needed sampling and evidence	Internal Audit Function (audits), Cybersecurity Function

No.	Step	Description	Owner/Responsible	Inputs	Outputs	Stakeholders
	audits and reviews	audits and reviews should be defined based on scope of audits and reviews. A risk based approach should be implemented.	(reviews), External Auditor (audits and reviews)	schedule		(reviews), External Auditor (audits and reviews)
1.7	Assignment of roles and responsibilities	Roles and responsibilities during the cybersecurity audits and reviews should be assigned in relation to the Responsibility Assignment Matrix from Cybersecurity Review and Audit Policy requirements.	Internal Audit Function (audits), Cybersecurity Function (reviews), External Auditor (audits and reviews)	Defined properties for planned audits/ reviews	Assigned roles and responsibilities	Internal Audit Function (audits), Cybersecurity Function (reviews), External Auditor (audits and reviews)

No.	Step	Description	Owner/Responsible	Inputs	Outputs	Stakeholders
1.8	Development and maintenance of an audit plan register	Audit plan register (list of planned audits and reviews) must be developed and maintained up to date. Audit plan register should cover at least the current calendar year and should include at least following information: 1. Audit ID 2. Audit name 3. Team responsible 4. Lead Auditor 5. Type of audit 6. Scope of audit (list of cybersecurity controls to be tested) 7. Methods	Internal Audit Function (audits), Cybersecurity Function (reviews), External Auditor (audits and reviews)	Defined properties for planned audits/ reviews	Audit plan register	Internal Audit Function (audits), Cybersecurity Function (reviews), External Auditor (audits and reviews)

No.	Step	Description	Owner/Responsible	Inputs	Outputs	Stakeholders
		8. Criteria 9. Sampling 10. Evidence needed 11. Duration and schedule, including planned start and end date of the audit 12. Cost of the audit.				
1.9	Acceptance of an audit plan	Prepared audit plan has to be approved.	Head of Internal Audit Function	Audit plan register	Approved audit plan register	Head of Internal Audit Function

Phase 2. Audit/review preparation

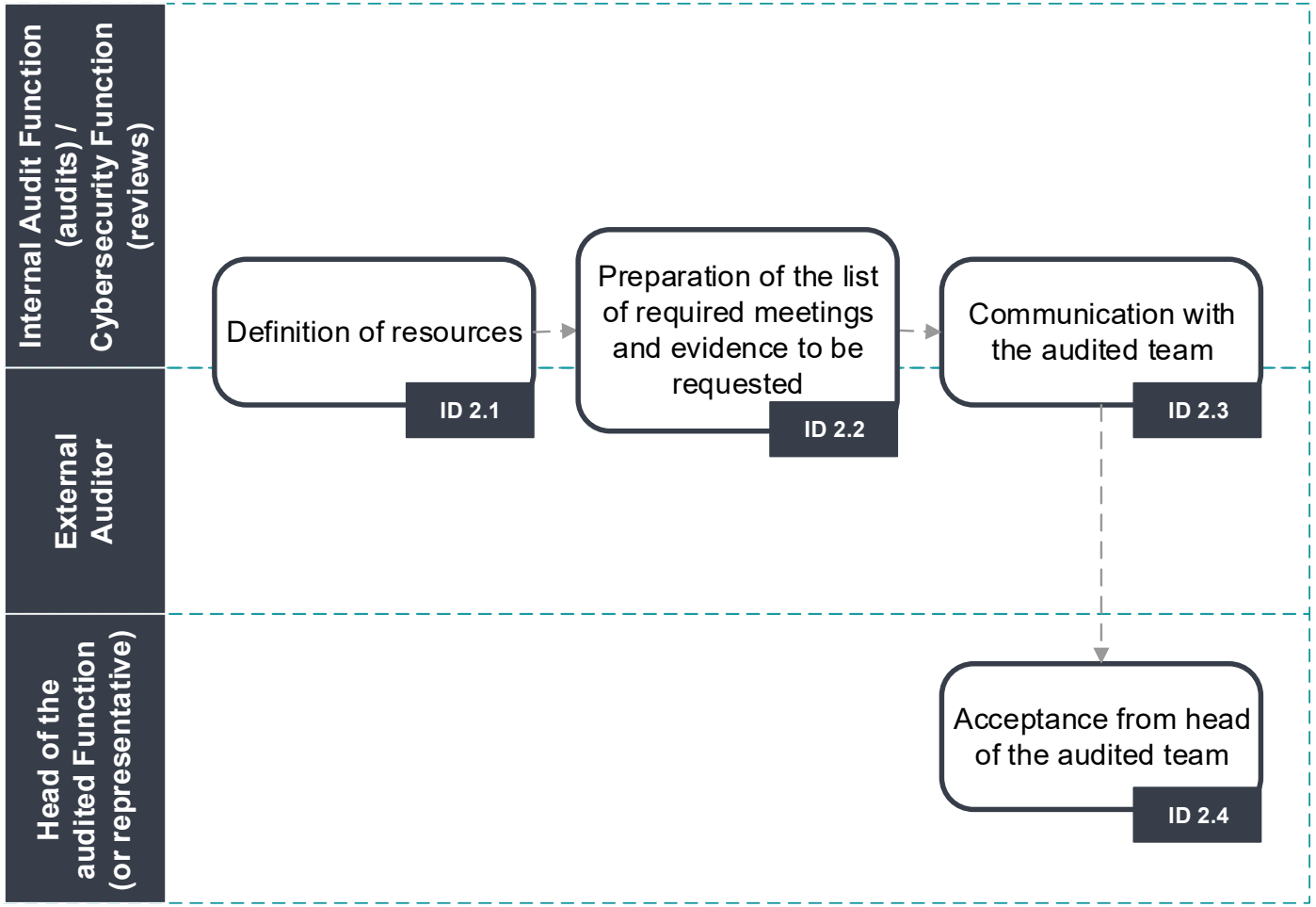

Figure 3 - Audit/review preparation phase workflow

No.	Step	Description	Owner/Responsible	Inputs	Outputs	Stakeholders
2.1	Definition of resources	During the preparation phase of an audit or review, resources needed for performing it have to be defined. Auditing team and participants from the audited function and their engagement have to be defined.	Internal Audit Function (audits), Cybersecurity Function (reviews), External Auditor (audits and reviews)	Defined properties for audit/ review	Defined resources	Internal Audit Function (audits), Cybersecurity Function (reviews), External Auditor (audits and reviews)
2.2	Preparation of the list of required meetings and evidence to be requested	List of required meetings, along with all the required attendees and evidence needed to perform audit or review, has to be defined.	Internal Audit Function (audits), Cybersecurity Function (reviews), External Auditor	Defined resources	List of required meetings and required evidence	Internal Audit Function (audits), Cybersecurity Function (reviews), External Auditor (audits

No.	Step	Description	Owner/Responsible	Inputs	Outputs	Stakeholders
			(audits and reviews)			and reviews)
2.3	Communication with the audited team	A month before the audit or review starts, information about the audit/review scope, schedule, resources that have to be engaged, the list of required meetings and evidence and have to be communicated to the head of the audited team, so the team can prepare for the audit or review.	Internal Audit Function (audits), Cybersecurity Function (reviews), External Auditor (audits and reviews)	Audit/review due in a month	Communication sent to the audited team	Internal Audit Function (audits), Cybersecurity Function (reviews), External Auditor (audits and reviews), Audited Function
2.4	Acceptance from head of the audited	Head of the audited function has to confirm that his/her team received all the information about the audit or review which will be performed and that	Head of the audited function or his representativ	Communication sent to the audited team	Confirmation of receival of communication and its	Head of the audited function or his

No.	Step	Description	Owner/Responsible	Inputs	Outputs	Stakeholders
	team	he/she accepts all the requirements and confirms availability of audit participants and meeting attendees.	e		acceptance	representative

Phase 3. Audit/review execution

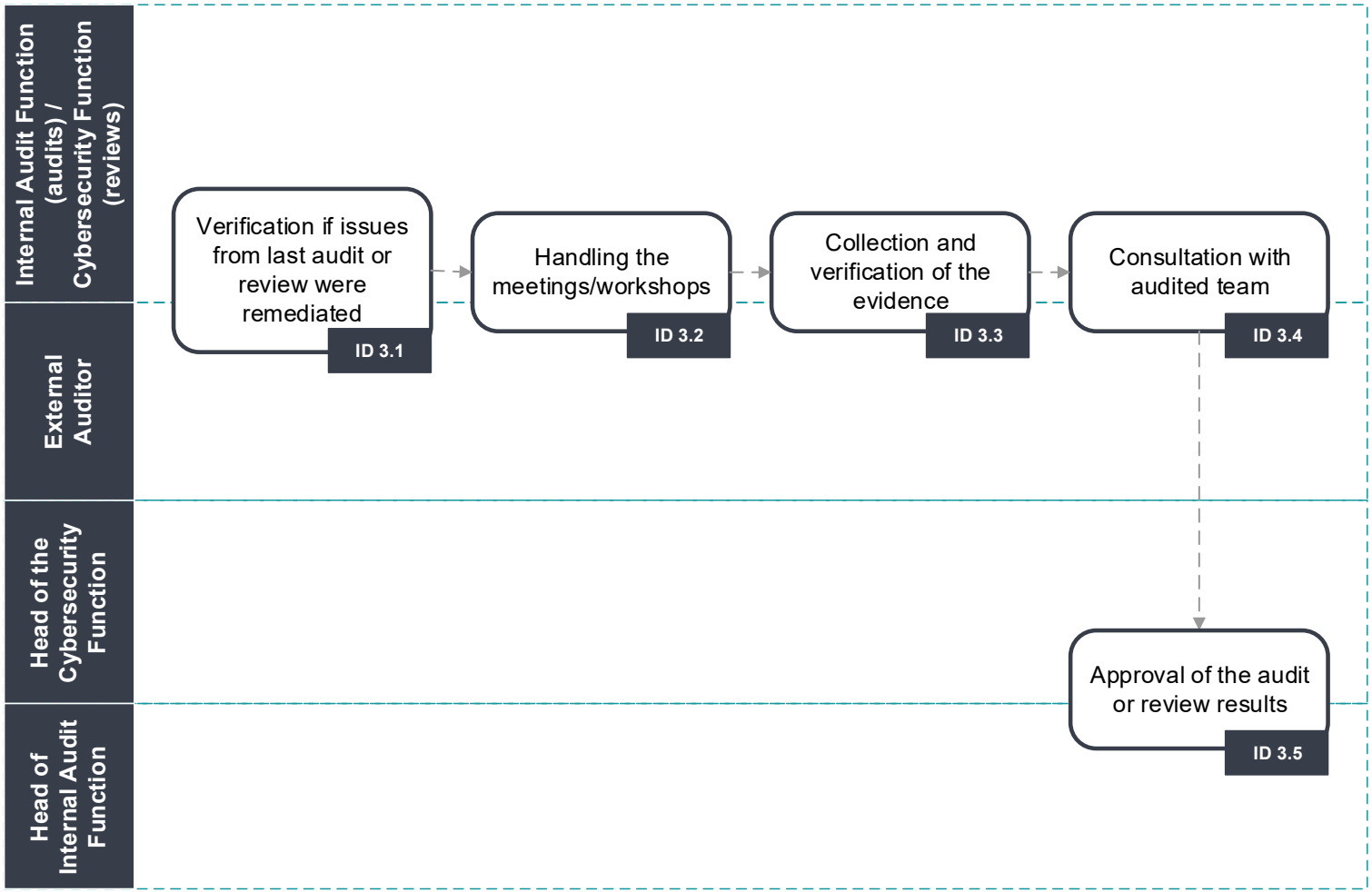

Figure 4 - Audit/review execution phase workflow

Choose Classification

No.	Step	Description	Owner/Responsible	Inputs	Outputs	Stakeholders
3.1	Verification if issues from last audit or review were remediated	Review of the findings from previous audits (based on the report) and verification of the status of remediation plan have to be done in order to ensure that all issues and corrective actions were addressed.	Internal Audit Function (audits), Cybersecurity Function (reviews), External Auditor (audits and reviews)	Reports from previous audits/ reviews	Completed verification of remediated issues from previous audits/ reviews	Internal Audit Function (audits), Cybersecurity Function (reviews), External Auditor (audits and reviews)
3.2	Handling the meetings/ workshops	All the required meetings/workshops have to be performed in order to gain an understanding of the processes and operating controls which will be subject to the audit or review.	Internal Audit Function (audits), Cybersecurity Function (reviews), External Auditor	Defined properties for audit/ review, List of required meetings	Understanding of the processes and controls that are subject of the audit/ review	Internal Audit Function (audits), Cybersecurity Function (reviews), External Auditor (audits

No.	Step	Description	Owner/Responsible	Inputs	Outputs	Stakeholders
			(audits and reviews)			and reviews), Audited Function
3.3	Collection and verification of the evidence	Evidence and samples required to perform audit or review have to be collected and verified. Evidence has to be securely transferred. Security of collected evidence in order to avoid data leakage has to be ensured.	Internal Audit Function (audits), Cybersecurity Function (reviews), External Auditor (audits and reviews)	Defined properties for audit/ review, List of required evidence	Collected and secured evidence and samples	Internal Audit Function (audits), Cybersecurity Function (reviews), External Auditor (audits and reviews), Audited Function
3.4	Consultation with audited	In order to attain a good understanding of the audited or reviewed process and	Internal Audit Function (audits),	Meetings and workshops	Confirmed understanding of the	Internal Audit Function (audits),

No.	Step	Description	Owner/Responsible	Inputs	Outputs	Stakeholders
	team	evidence, each unclear matter has to be consulted with the audited function.	Cybersecurity Function (reviews), External Auditor (audits and reviews)	completed	processes and controls that are subject of the audit/ review	Cybersecurity Function (reviews), External Auditor (audits and reviews), Audited Function
3.5	Approval of the audit or review results	Audit results: findings, recommendations and remediation plan should be approved.	Head of Cybersecurity Function and Head of Internal Audit Function	Results of the audit/ review	Approved results of the audit/ review	Head of Cybersecurity Function and Head of Internal Audit Function

Phase 4. Reporting and documentation of cybersecurity audit and review findings

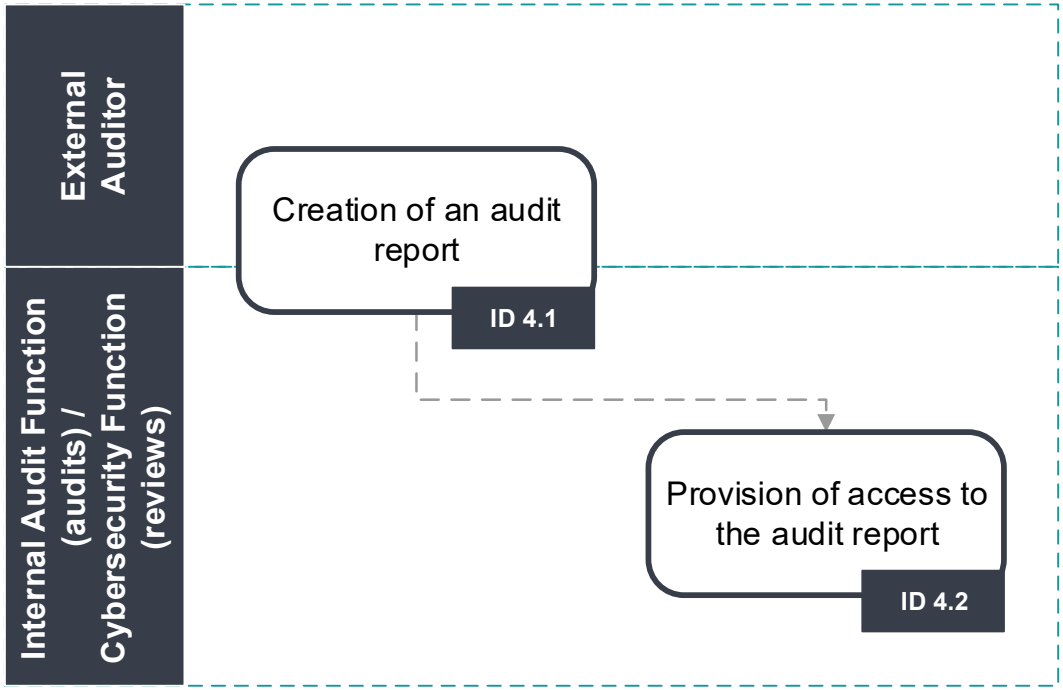

Figure 5 - Reporting and documentation phase workflow

No.	Step	Description	Owner/Responsible	Inputs	Outputs	Stakeholders
4.1	Creation of an	Audit report has to be created after every performed audit and review	Internal Audit Function	Audit/review activities	Audit report	Internal Audit Function

No.	Step	Description	Owner/Responsible	Inputs	Outputs	Stakeholders
	audit report	within two weeks after an audit or review ends. It should include at least following information: 1. Audit ID 2. Audit name 3. Team responsible 4. Lead Auditor 5. Type of audit 6. Scope of audit 7. Reference documents 8. Date of audit start 9. Date of audit end	(audits), Cybersecurity Function (reviews), External Auditor (audits and reviews)	ended		(audits), Cybersecurity Function (reviews), External Auditor (audits and reviews)

No.	Step	Description	Owner/Responsible	Inputs	Outputs	Stakeholders
		10. Summary of performed actions and procedures, and results of the review 11. Observations, including its description and criticality 12. Recommendations, including its priority 13. Remediation plan for recommendations, covering corrective actions, their implementation, owner and deadline				
4.2	Provision of access to the	Access to the audit report has to be provided to all relevant stakeholders: e.g., audited function, Internal Audit	Internal Audit Function (audits),	Audit report	Access to audit granted to relevant	Internal Audit Function (audits),

No.	Step	Description	Owner/Responsible	Inputs	Outputs	Stakeholders
	audit report	Function, Cybersecurity Steering Committee.	Cybersecurity Function (reviews)		stakeholders	Cybersecurity Function (reviews), Audited Function, Cybersecurity Steering Committee

Phase 5. Presentation of findings to the Cybersecurity Steering Committee and the organization head

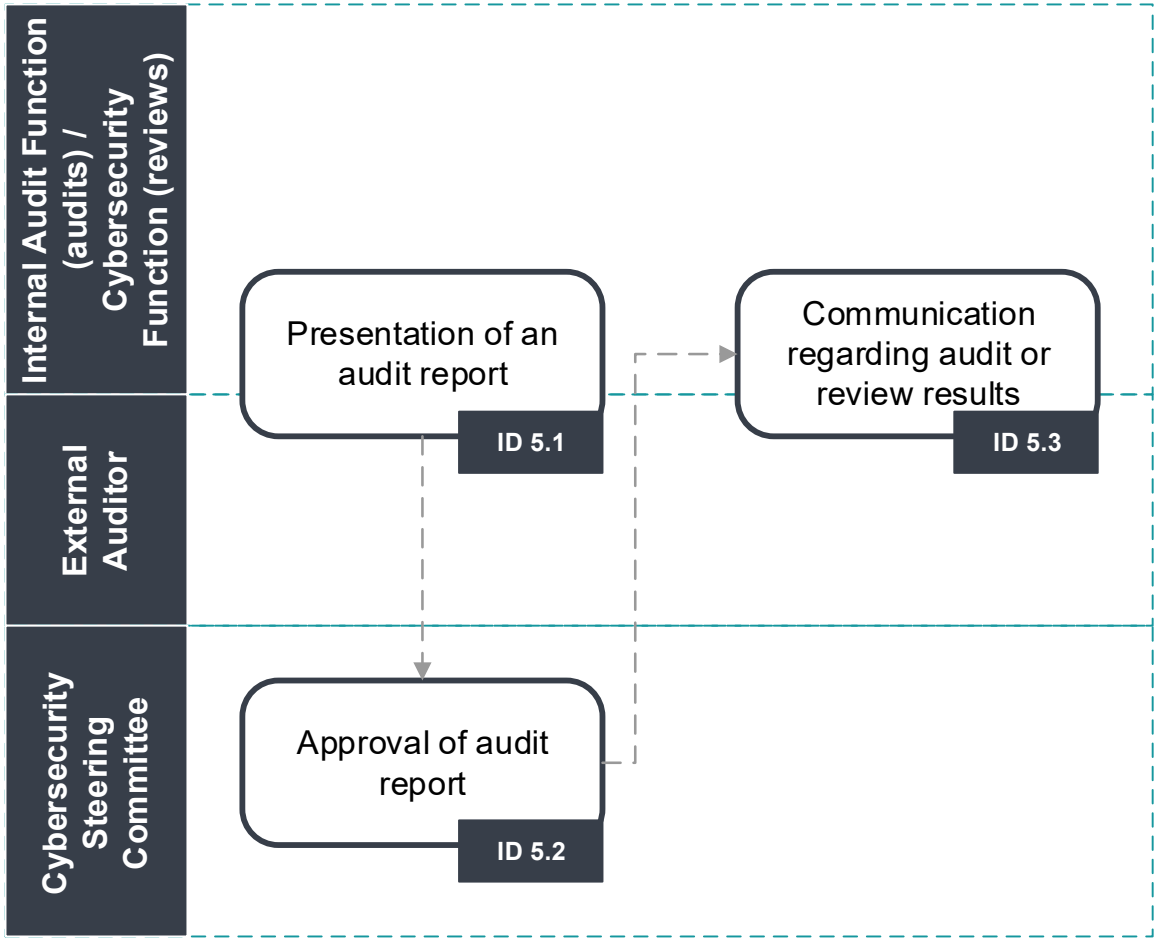

Figure 6 - Presentation of findings phase workflow

No.	Step	Description	Owner/Responsible	Inputs	Outputs	Stakeholders
5.1	Presentation of an audit report	Results of every performed audit or review have to be presented to the Cybersecurity Steering Committee at next Steering Committee meeting and to the organization head within 3 weeks after an audit or review ends. Presented report should include the scope of an audit/review, findings, recommendations as well as and remediation plan.	Internal Audit Function (audits), Cybersecurity Function (reviews), External Auditor (audits and reviews)	Audit report	Presented audit report	Internal Audit Function (audits), Cybersecurity Function (reviews), External Auditor (audits and reviews), Cybersecurity Steering Committee
5.2	Approval of audit report	Audit reports have to be approved.	Cybersecurity Steering Committee	Presented audit report	Approved audit report	Cybersecurity Steering Committee
5.3	Communication regarding	Audit reports have to be shared with the head of the audited function. Results of	Internal Audit Function	Approved	Audit/ review results are	Internal Audit Function

No.	Step	Description	Owner/Responsible	Inputs	Outputs	Stakeholders
	audit or review results	the audit or review, including findings, recommendations and remediation plan have to be agreed with the head of the audited function.	(audits), Cybersecurity Function (reviews), External Auditor (audits and reviews)	audit report	communicated	(audits), Cybersecurity Function (reviews), External Auditor (audits and reviews)

Phase 6. Monitoring and review

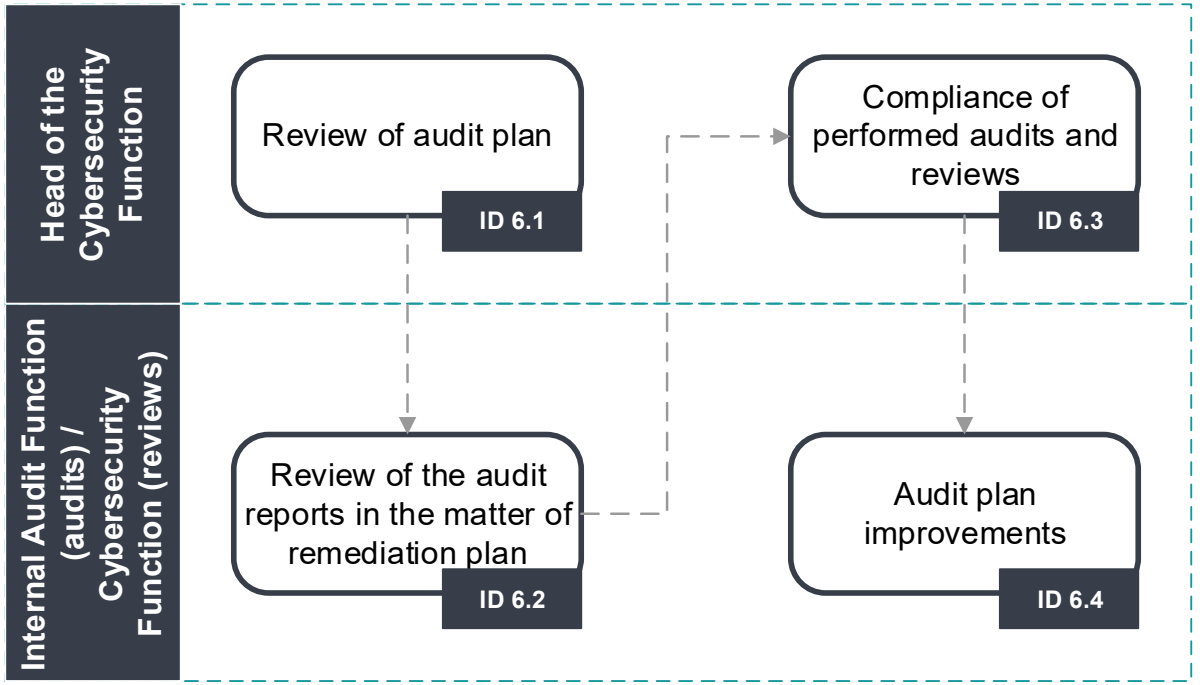

Figure 7 - Monitoring and review phase workflow

No.	Step	Description	Owner/Responsible	Inputs	Outputs	Stakeholders
6.1	Review of	Review of the audit plan has to be performed at least annually to verify	Head of Cybersecurity	Audit plan	Reviewed audit plan	Head of Cybersecurity

No.	Step	Description	Owner/Responsible	Inputs	Outputs	Stakeholders
	audit plan	whether all the required audits and reviews are planned and update it if necessary.	Function or his representative	register	register	Function or his representative
6.2	Review of the audit reports in the matter of remediation plan	Review of the remediation plan from audit reports have to be performed at least annually in order to verify if it is implemented accordingly.	Internal Audit Function (audits), Cybersecurity Function (reviews)	Audit reports from previous audits/ reviews	Reviewed of remediation plans from previous audits/ reviews	Internal Audit Function (audits), Cybersecurity Function (reviews)
6.3	Compliance of performed audits and reviews	Analysis of compliance of performed audit or review with current audit plan has to be performed within one month after an audit or review ends. The following aspects should be included in the review:	Head of Cybersecurity Function or his representative	Audit report from performed audit/review, audit plan register	Compliance of performed audit/review with audit plan register confirmed	Head of Cybersecurity Function or his representative

No.	Step	Description	Owner/Responsible	Inputs	Outputs	Stakeholders
		1. Whether planned scope of audit/review was covered. 2. The actual cost of an audit/review vs planned cost.				
6.4	Audit plan improvements	In case there are any possible improvements or lessons learned which can be beneficial for the future, they should be implemented to the audit plan.	Internal Audit Function (audits), Cybersecurity Function (reviews)	Audit plan register	Adjusted audit plan register	Internal Audit Function (audits), Cybersecurity Function (reviews)

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>, <internal audit 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 information assets including the workstation and servers in the <organization name> and applies to all personnel in the <organization name>.

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