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

Vulnerability Assessment 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 aims to define detailed step-by-step cybersecurity requirements to asses vulnerabilities and protect <organization name>'s information technology assets against threats and cybersecurity vulnerabilities.

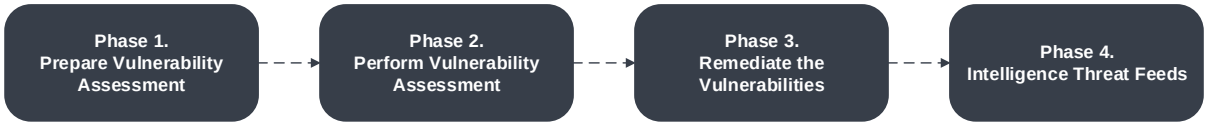
The requirements in this procedure are aligned with the cybersecurity requirements issued by the National Cybersecurity Authority (NCA), including but not limited to (ECC-1:2018), (DCC-1:2022), (CSCC-1:2019) and (CCC-1:2020), in addition to other related cybersecurity legal and regulatory requirements.

Scope

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

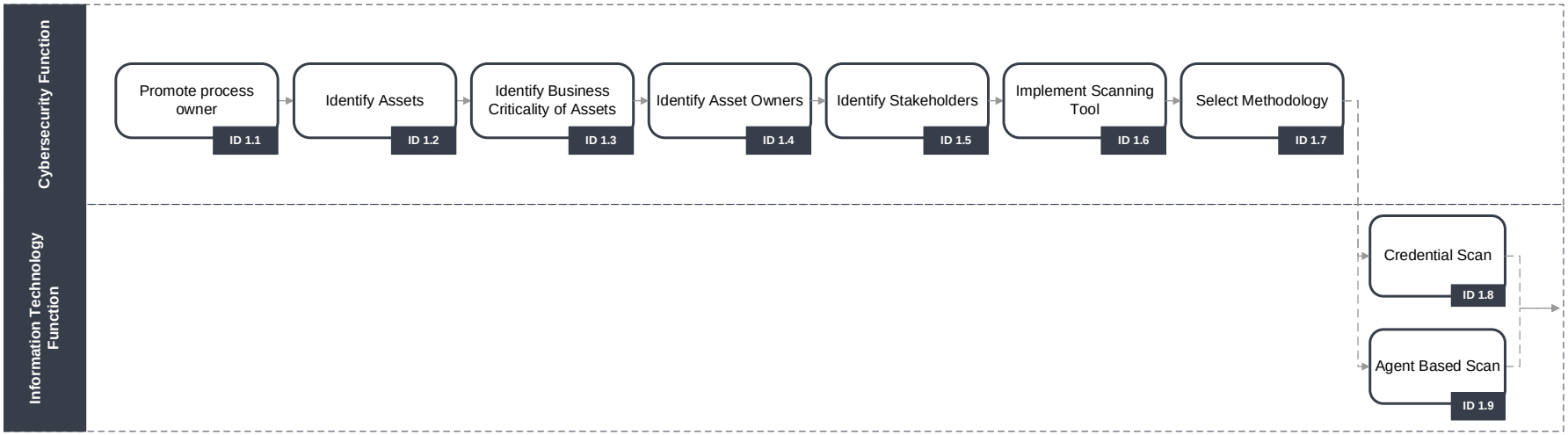
Overview of the Vulnerability Management Process

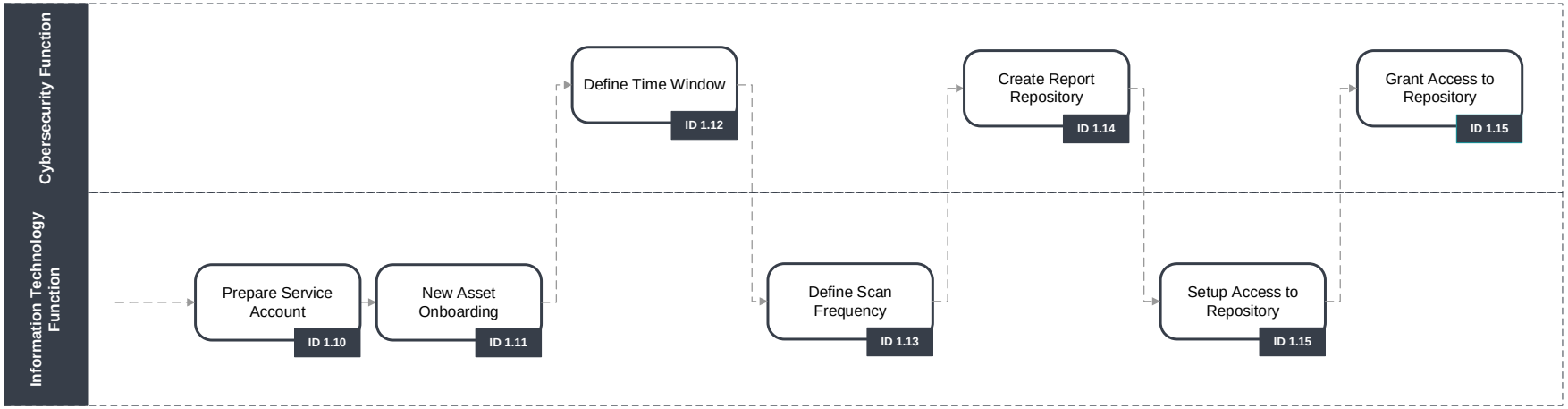
The Vulnerability Management Process must be divided into the following phases:



- Prepare Vulnerability Assessment
- Perform Vulnerability Assessment
- Remediate the Vulnerabilities
- Intelligence Threat Feeds

Phase 1. Prepare Vulnerability Assessment





No.	Step	Description	Owner/Responsible	Inputs	Outputs	Stakeholders
1-1	Promote Process Owner	Promote a dedicated Process Owner who will be responsible for the implementation and the management of the <organization name>'s Vulnerability Management Program.	<cybersecurity function>	Criteria for the process owner selection	Dedicated process owner has been nominated	<cybersecurity function>
1-2	Identify Assets	Identify all assets which are in scope of vulnerability management. The authorized hardware and software are documented in the <organization name>'s Asset Management Policy and Standard.	<cybersecurity function>	Information and technology asset register	Identified assets in scope of vulnerability management	<cybersecurity function> <Information Technology function>
1-3	Identify Business Criticality of Assets	Verify the business criticality of all assets which are in scope of vulnerability management.	<cybersecurity function>	Identified assets in scope of vulnerability	Verified business criticality of assets	<all departments of organization>

No.	Step	Description	Owner/Responsible	Inputs	Outputs	Stakeholders
				management		
1-4	Identify Asset Owners	Identify business and system owners of assets who are responsible for remediating identified vulnerabilities based on agreed KPIs as described in the <organization name>'s Key Performance Indicators for Vulnerability Management.	<cybersecurity function>	Verified business criticality of assets	Identified business and system owners of assets	<cybersecurity function>
1-5	Identify Stakeholders	Document the identified stakeholders in the <organization name>'s Vulnerability Management Process.	<cybersecurity function>	Identified business and system owners of assets	Documented stakeholders	<cybersecurity function>
1-6	Implement the Scanning	Implement vulnerability scanning tool suitable for the <organization name>'s	<cybersecurity	Low level design of the	Implemented vulnerability	<cybersecurity

No.	Step	Description	Owner/Responsible	Inputs	Outputs	Stakeholders
	Tool	network infrastructure, so it is able to scan all assets which are in scope of vulnerability management	function>	solution	scan solution	function> <Information Technology function>
1-7	Select Methodology	Selecting suitable scanning methodology, by performing authenticated scan either using credential based or agent-based scanning methodology (in case the uncredentialed scan is not suitable and credentialed scan cannot be used due to technical or other limitations), for the identified Critical Assets	<cybersecurity function>	Low level design of the solution	Selected scanning methodology for identified critical assets	<cybersecurity function> <Information Technology function>
1-8	Prepare credentialed	Create the accounts used for Credentialed Scan, following the	<Information Technology	Selected scanning	List of critical assets	<cybersecurity function>

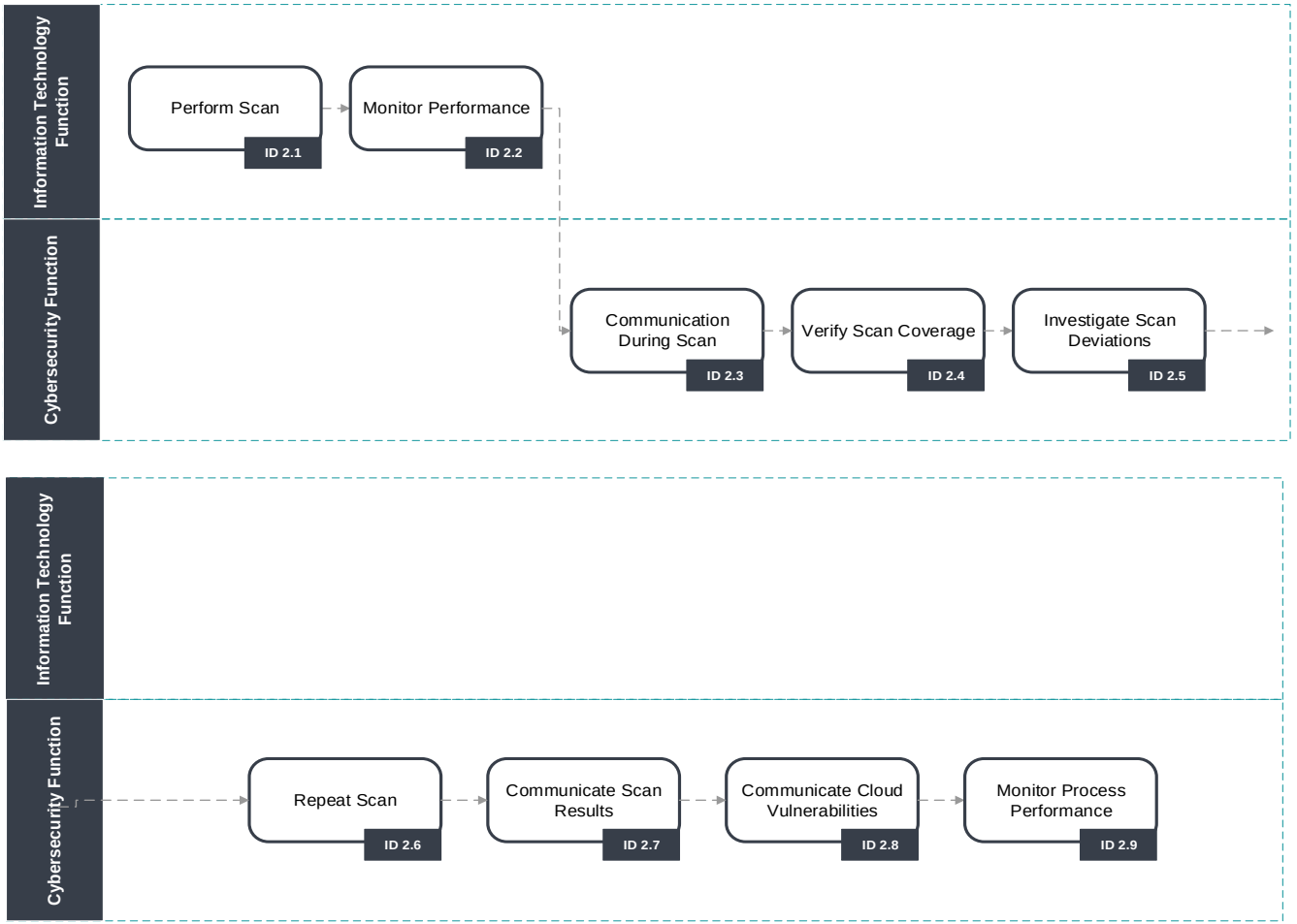
No.	Step	Description	Owner/Responsible	Inputs	Outputs	Stakeholders
	scan	<organization name>'s Privileged Access Management Policy.	function>	methodology for identified critical assets	accessible through credential scan	<Information Technology function>
1-9	Perform credentialed scan	Perform test credentialed scan (also known as an authenticated scan) to provide a definitive list of required patches and misconfigurations by using credentials to log into systems and applications.	<Information Technology function>	Account created for credential scan for identified critical assets	List of required patches and misconfiguration	<cybersecurity function> <Information Technology function>
1-10	Prepare agent based scan	Implement local scan agent (lightweight, low-footprint programs) on the host.	<Information Technology function>	Selected scanning methodology for identified critical assets	List of critical assets, with implemented local scan agent	<cybersecurity function> <Information Technology function>

No.	Step	Description	Owner/Responsible	Inputs	Outputs	Stakeholders
1-11	Perform agent based scan	Perform agent based test scan in order to collect vulnerability, compliance, and system data, and report that information back to the central scan server for analysis.	<Information Technology function>	Implemented local scan agent	List of required patches and misconfiguration	<cybersecurity function> <Information Technology function>
1-12	New Asset Onboarding	Ensure the onboarding of new assets in the vulnerability management program in a timely manner, by the necessary processes.	<cybersecurity function>	Updated asset register	New assets onboarded	<Information Technology function>
1-13	Define Time Window	Verify that the vulnerability scan does not interfere with any other scheduled activities, i.e., Backup, Scheduled Maintenance, etc.	<Information Technology function>	Selected scanning methodology for identified critical assets	Verification of scan interference with other activities	<cybersecurity function> <Information Technology function>

No.	Step	Description	Owner/Responsible	Inputs	Outputs	Stakeholders
1-14	Define Scan Frequency	Define the frequency of the vulnerability scan as described in the <organization name> Vulnerability Management Policy and Standard.	<cybersecurity function>	Selected scanning methodology for identified critical assets	Defined vulnerability scan frequency	<cybersecurity function>
1-15	Create Report Repository	Creating a central location to store the vulnerability scan reports and the <organization name>'s Vulnerability Register.	<Information Technology function>	Selected scanning methodology for identified critical assets	Central location to store reports	<cybersecurity function> <Information Technology function>
1-16	Grant Access to Repository	Ensure that only employee with valid need to know are granted access to this central location as listed in the <organization name>'s Vulnerability Management Policy.	<cybersecurity function>	List of employees with access to central location	Role based access model dedicated for the central repository	<cybersecurity function> <Information Technology

No.	Step	Description	Owner/Responsible	Inputs	Outputs	Stakeholders
						function>

Phase 2. Perform Vulnerability Assessment

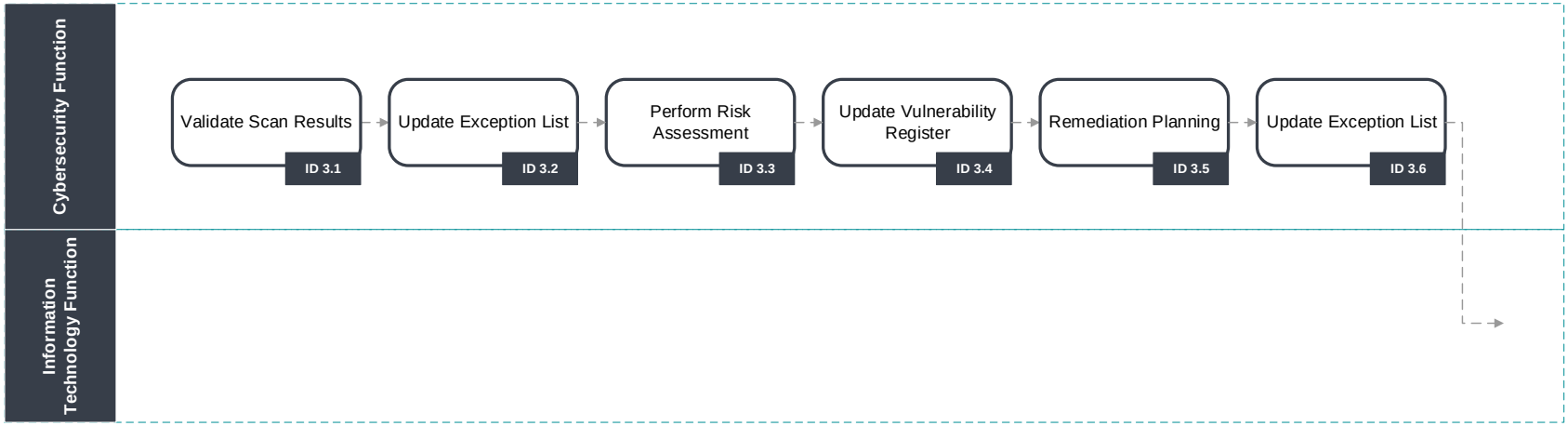


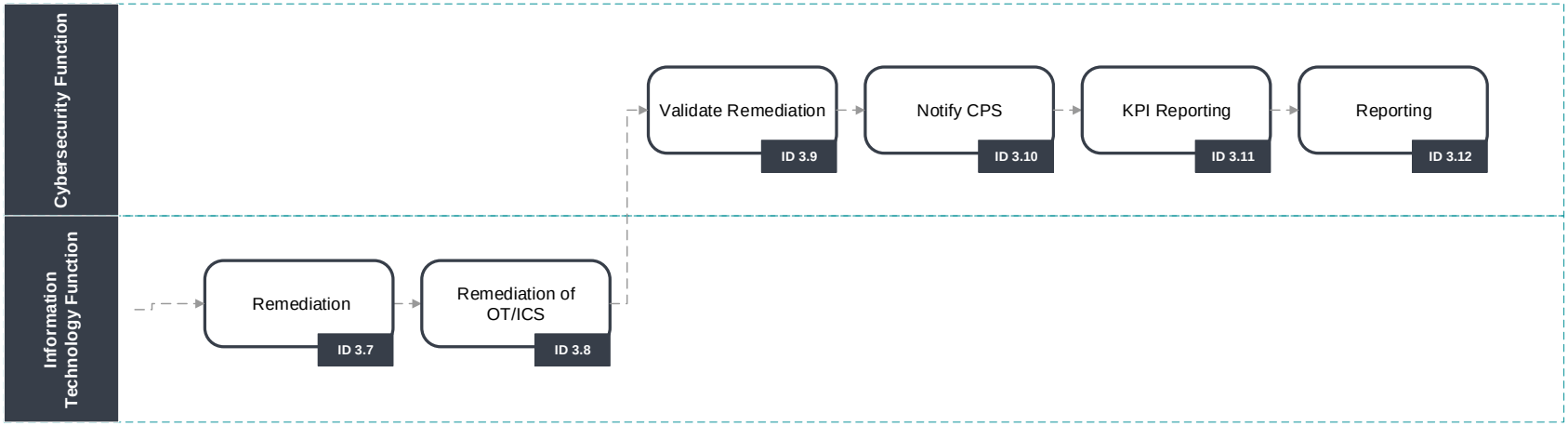
No.	Step	Description	Owner/Responsible	Inputs	Outputs	Stakeholders
2-1	Perform Scan	Execute the vulnerability scan as it was documented in the approved change record.	<Information Technology function>	Approved change record	Vulnerability scan report	<cybersecurity function> <Information Technology function>
2-2	Monitor Performance	Monitor the performance of both of the vulnerability scan environment as well as the assets being scanned, for the duration of the scan.	<Information Technology function>	Identified critical assets in scope for vulnerability scan	Assets negatively impacted by the scan	<cybersecurity function> <Information Technology function>
2-3	Communication During Scan	Communicate any issue with the appropriate stakeholders as described in the change record.	<cybersecurity function>	Assets negatively impacted by the scan	Issue communicated to stakeholders	<all departments of organization>

No.	Step	Description	Owner/Responsible	Inputs	Outputs	Stakeholders
2-4	Verify Scan Coverage	Verify that all assets in scope of vulnerability management were scanned successfully	<cybersecurity function>	Vulnerability scan report Asset register	List of assets missed by the vulnerability scan	<cybersecurity function> <Information Technology function>
2-5	Investigate Deviations	Investigate any deviation in a timely manner based on agreed KPIs.	<cybersecurity function>	List of assets missed by the vulnerability scan	Investigated deviation	<cybersecurity function>
2-6	Repeat Scan	Repeat the vulnerability on the assets, where the scan failed during the previous attempt.	<cybersecurity function>	List of assets missed by the vulnerability scan	Repeated scan	<cybersecurity function> <Information Technology function>

No.	Step	Description	Owner/Responsible	Inputs	Outputs	Stakeholders
2-7	Communicate Scan Results	Communicate the end-result of the scan to the relevant stakeholders	<cybersecurity function>	Vulnerability scan report	Scan result made available at central repository	<cybersecurity function>
2-8	Communicate cloud vulnerabilities	Notify the CSTs (Cloud Service Team) of identified vulnerabilities that may be affecting them and put safeguards in place.	<cybersecurity function>	Scan result made available at central repository	Cloud vulnerabilities communicated	<cybersecurity function>
2-9	Monitor Process Performance	Measure key performance indicators (KPI) to ensure the continuous improvement of vulnerability management.	<cybersecurity function>	Vulnerability scan report	KPI report	<cybersecurity function>

Phase 3. Remediate the Vulnerabilities





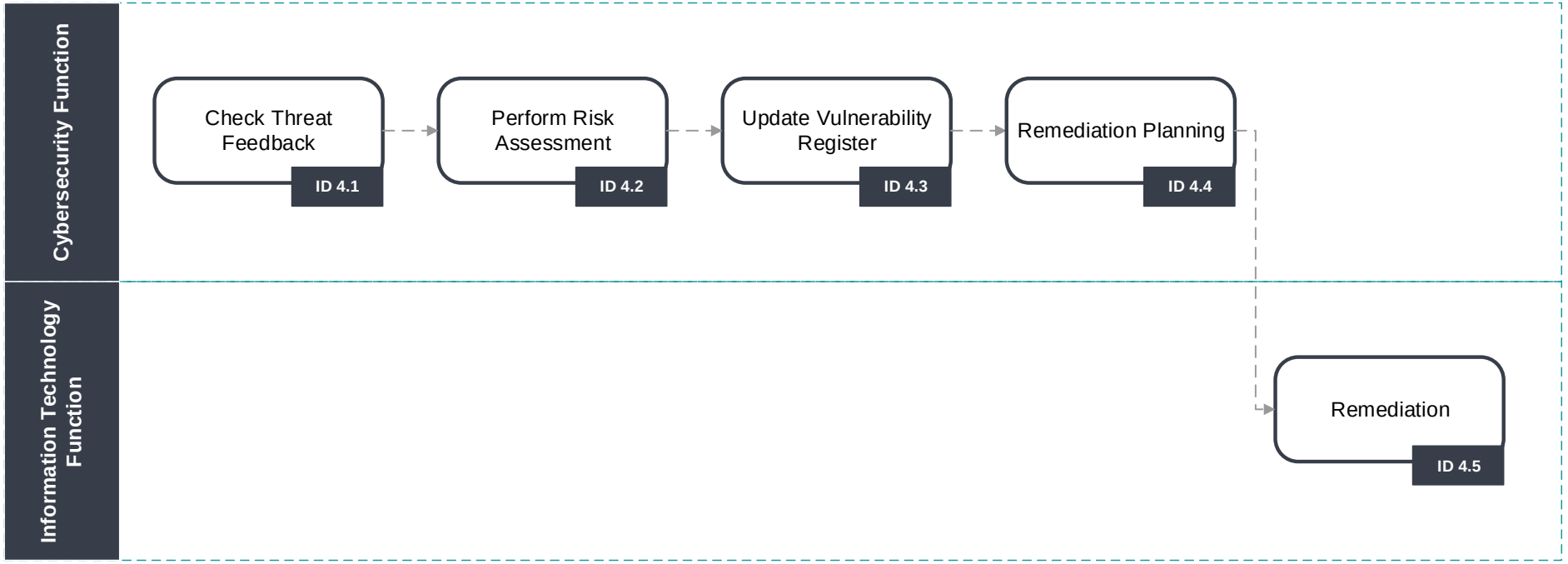
No.	Task	Description	Owner/Responsible	Inputs	Outputs	Stakeholders
3-1	Validate Scan Results	Validate the result of the vulnerability scan.	<cybersecurity function>	Vulnerability scan report	Validated end results	<cybersecurity function>
3-2	Update Exception List	Add false alerts to the exception list.	<cybersecurity function>	Validated end results	False alerts added to exception list	<cybersecurity function> <Information Technology function>
3-3	Perform Risk Assessment	Analyze vulnerabilities and their associated risks based on the <organization name>'s Risk Management Policy.	<cybersecurity function>	Validated end results	Analyzed vulnerabilities and risks	<cybersecurity function>
3-4	Update Vulnerability	Document all identified vulnerabilities in the <organization name>'s Vulnerability	<cybersecurity	Analyzed vulnerabilities	Updated vulnerability	<cybersecurity

No.	Task	Description	Owner/Responsible	Inputs	Outputs	Stakeholders
	Register	Register.	function>	and risks	register	function>
3-5	Remediation Planning	Defined corrective actions for each identified vulnerability based on their risk level.	<cybersecurity function>	Updated vulnerability register	Defined action plan to assess vulnerability	<cybersecurity function>
3-6	Update Exception List	Add vulnerabilities with tolerable risk level to the exception list.	<cybersecurity function>	Updated vulnerability register	Updated exception list	<cybersecurity function>
3-7	Remediation	Implement corrective actions in accordance with the <organization name>'s Patch Management Policy and Standard.	<Information Technology function>	Defined action plan to assess vulnerability	Implemented corrective actions	<cybersecurity function> <Information Technology function>

No.	Task	Description	Owner/Responsible	Inputs	Outputs	Stakeholders
3-8	Remediation of OT/ICS	Remediate the newly discovered critical vulnerabilities presenting significant risks to the OT/ICS environment in a safe manner.	<Information Technology function>	Defined action plan to assess vulnerability	Implemented corrective actions	<cybersecurity function> <Information Technology function>
3-9	Validate Remediation	Verify the success of the implementation of the corrective actions by rerunning the vulnerability scan on the relevant assets.	<cybersecurity function>	Implemented corrective actions	Verification of implementation	<cybersecurity function> <Information Technology function>
3-10	Notify CSP	Notify the management of CSP (Content Security Policy), that the safeguards in relation to cloud-based	<cybersecurity function>	Verification of implementation	Result of implementation communicated	<cybersecurity function>

No.	Task	Description	Owner/Responsible	Inputs	Outputs	Stakeholders
		vulnerabilities are in place.				
3-11	KPI reporting	Measure key performance indicators (KPI) described in the Key Performance Indicators section of the document to ensure the continuous improvement of vulnerability management.	<cybersecurity function>	Verification of implementation	KPI report	<cybersecurity function>
3-12	Reporting	Provide regular reporting for the <organization name>'s senior management about the vulnerabilities and subsequent risks as described in the <organization name>'s Risk Management Policy.	<cybersecurity function>	KPI report	Regular reporting to senior management	<cybersecurity function>

Phase 4. Intelligence Threat feeds



No.	Task	Description	Owner/Responsible	Inputs	Outputs	Stakeholders
4-1	Check Threat Feeds	Daily review of potential technical vulnerabilities coming from trusted authorized sources.	<cybersecurity function>	Information from trusted sources	Validated end results	<cybersecurity function>
4-2	Perform Risk Assessment	Analyze vulnerabilities and their associated risks based on the <organization name>'s Risk Management Policy.	<cybersecurity function>	Validated end results	Analyzed vulnerabilities and risks	<cybersecurity function>
4-3	Update Vulnerability Register	Document all identified vulnerabilities in the <organization name>'s Vulnerability Register.	<cybersecurity function>	Analyzed vulnerabilities and risks	Updated vulnerability register	<cybersecurity function>
4-4	Remediation Planning	Define corrective actions for each identified vulnerability based on their risk level.	<cybersecurity function>	Updated vulnerability register	Defined action plan to assess vulnerability	<cybersecurity function>

No.	Task	Description	Owner/Responsible	Inputs	Outputs	Stakeholders
4-5	Remediation	Implement the corrective actions based on the <organization name>'s Patch Management Policy and Standard.	<Information Technology function>	Defined action plan to assess vulnerability	Implemented corrective actions	<Information Technology function>

Roles and Responsibilities

1- **Procedure Owner:** <head of the cybersecurity function>

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

3- **Procedure Implementation and Execution:** <information technology 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- All personnel (employees and contractors) at <organization name> must comply with this procedure.

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