Vulnerability Management Process

Doc. Control Number	Version
SNL-71	0.3

Document Reference

Item	Description
Title	Vulnerability Management Policy
Department	Cybersecurity Department
Version No	0.2
Status	Draft
Type	DOCX
Publish-Date	13 March 2024
Revision-Date	13 March 2025

Authors		
Name	Department	Signature/Date
Muhaned Kamal Ali	Cybersecurity - I. S Specialist	13/3/2024

Reviewed by		
Name	Department	Signature/Date
Yasir Awad	Head of Cyber Security Department	13/3/2024

Approved by		
Name	Department	Signature/Date
Abdullah Al Shuhail	V.P	13/3/2024

Control-Page

Document Amendment Record			
Version-No	Date	Prepared-by	Explanation
0.1	13 Jan	Muhaned Ali	First Release
0.2	13 March 2024	Muhaned Ali	The document has been reviewed
0.2	11 Aug 2024	Muhaned Ali	The document has been reviewed

Contents

1. Purpose

Vulnerability management is the process in which vulnerabilities in IT are identified and the risks of these vulnerabilities are evaluated. This evaluation leads to correcting the vulnerabilities and removing the risk or a formal risk acceptance by the management of an organization.

2. Scope

All SNLC network infrastructure, servers, operating systems on virtual machines, cloud-hosted server operating systems, database servers, databases, and applications.

3. Roles and responsibilities

When building a vulnerability management process, the following roles should be identified within the SNLC:

3.1 GRC Team: The GRC Team is the owner of the vulnerability management process. This person designs the process and ensures it is implemented as designed.

3.2 Vulnerability Engineer: The vulnerability engineer role is responsible for configuring the vulnerability scanner and scheduling the various vulnerability scans.

3.3 Asset Owner: The asset owner is responsible for the IT asset that is scanned by the vulnerability management process. This role should decide whether identified vulnerabilities are mitigated or their associated risks are accepted.

3.4 IT System Engineer: The IT system engineer role is typically responsible for implementing remediating actions defined because of detected vulnerabilities.

4 Vulnerability Management Process

4.1 Scanning

a) The GRC Team Must conduct vulnerability scans on all information assets listed in the Asset Inventory using relevant tools.

b) Frequency of scans should adhere to the defined requirements, such as monthly for critical systems, quarterly for medium systems, and annually for low-risk systems.

c) Scans should cover operating systems, applications, network devices, and other critical components to identify potential vulnerabilities.

d) Utilize specialized vulnerability scanning tools tailored to specific environments, such as dedicated tools for web servers, mobile apps, databases, etc., to ensure comprehensive coverage.

4.2 Analyzing

a) Upon completion of vulnerability scans, The GRC Team must analyze the impact of identified vulnerabilities on critical information assets.

b) The GRC Team must assign a criticality level to each vulnerability based on its severity and potential impact on the Company.

c) Define timeframes for remediation based on the criticality level:
- Critical vulnerabilities: Remediate within 24 to 48 hours.
- High-severity vulnerabilities: Remediate within 7 to 14 days.
- Medium-severity vulnerabilities: Remediate within 30 to 60 days.
- Low-severity vulnerabilities: Remediate within 90 to 120 days.

d) Prioritize vulnerabilities based on their criticality level to ensure timely remediation of high-risk issues.

4.3 Reporting

a) Generate a Vulnerabilities Report containing details of identified vulnerabilities, including their criticality levels, and affected assets.

b) Share the Vulnerabilities Report with the respective departments responsible for managing the affected assets.

c) Define recommended actions for remediation, such as applying patches, implementing workarounds, or updating configurations.
d) Ensure that Patch Management processes are aligned with the Vulnerability Management process to facilitate timely deployment of patches and updates.
e) Monitor the progress of remediation efforts and provide regular updates to stakeholders until all vulnerabilities are resolved.

4.4 Patch Management Integration

a) Integrate Vulnerability Management with Patch Management processes to ensure timely deployment of patches and updates in response to identified vulnerabilities.
b) Develop automated workflows and procedures to streamline the patch deployment process, minimizing manual intervention and reducing the time to remediation.
c) Prioritize patch deployment based on the criticality of vulnerabilities and their potential impact on the Company.
d) Test patches in a controlled environment before deployment to minimize the risk of unintended consequences.
e) Develop rollback procedures to address any issues that may arise from patch deployment.
f) Maintain an inventory of patches and updates to ensure all systems are up to date with the latest security fixes.

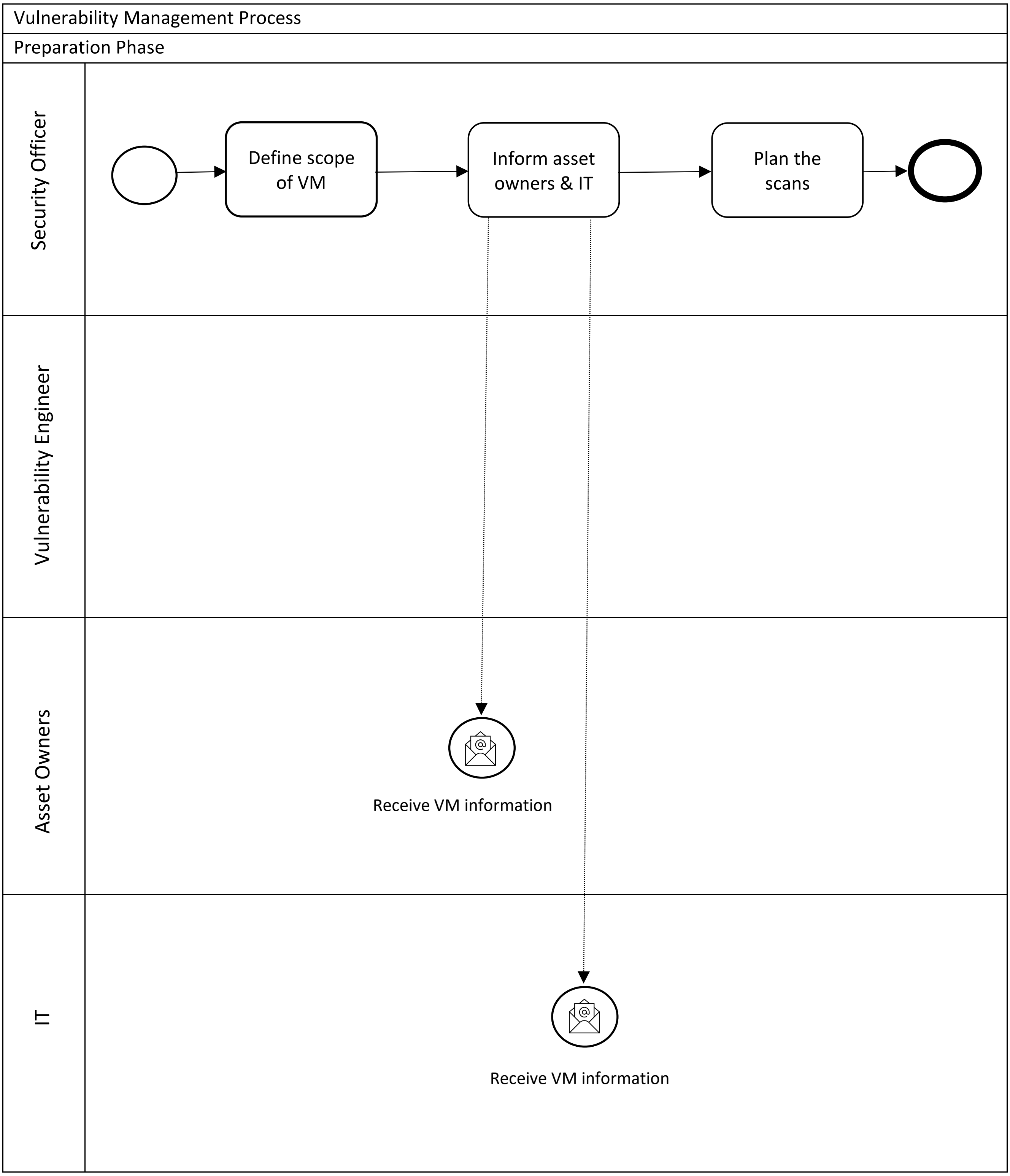
4.5 Continuous Improvement

a) Continuously evaluate and refine the Vulnerability Management process based on lessons learned, emerging threats, and changes in the company's infrastructure.
b) Conduct regular reviews of vulnerability data, trends, and remediation efforts to identify areas for improvement and optimization.
c) Provide ongoing training and awareness programs to educate personnel on the importance of vulnerability management and their roles and responsibilities in the process.

4.6 A vulnerability management process consists of five phases:

a) Preparation
b) Vulnerability scan
c) Define remediating actions
d) Implement remediating actions
e) Rescan

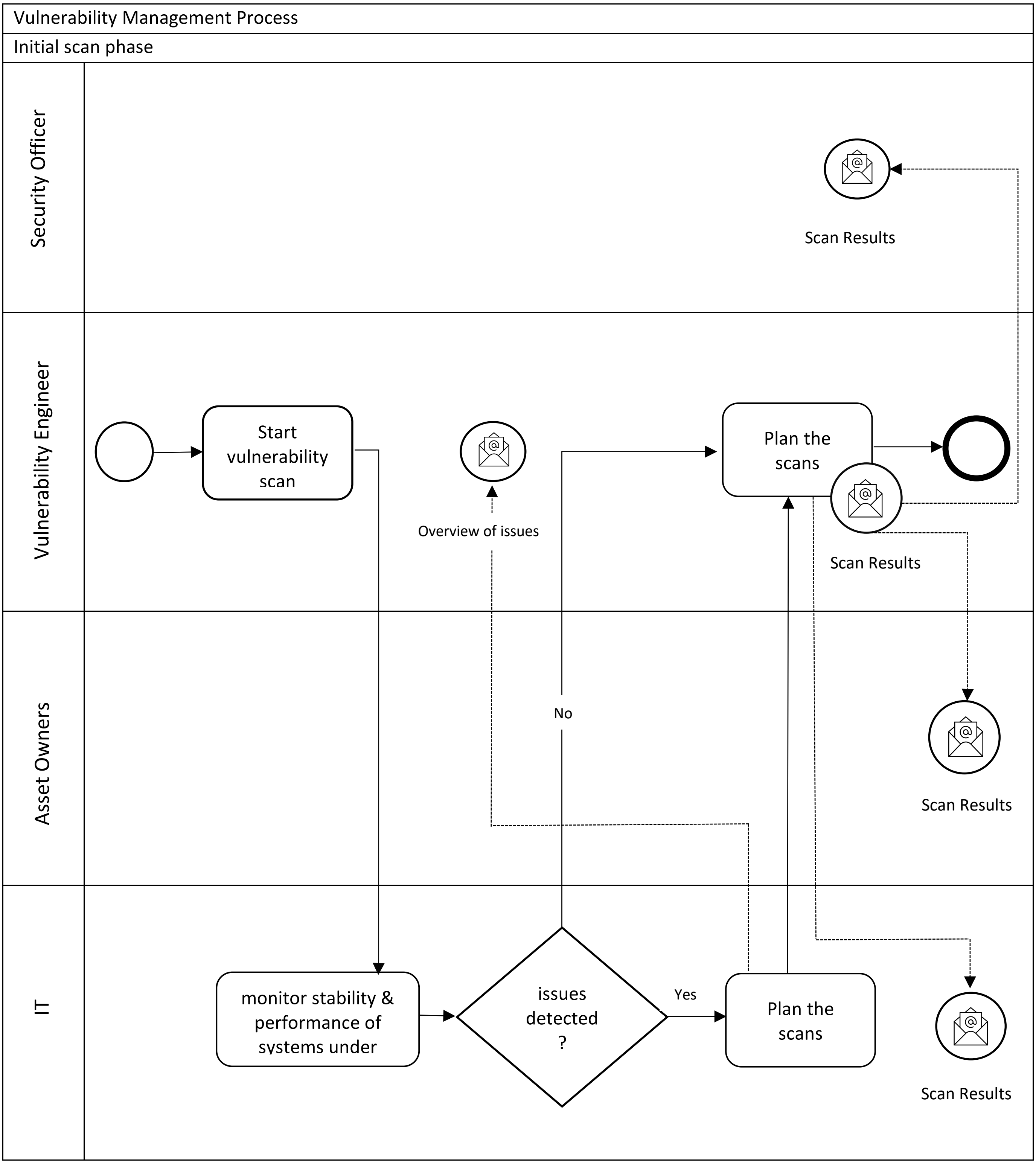
a) Preparation



The preparation phase is the first phase in a vulnerability management process. To prevent being overwhelmed by thousands of vulnerabilities identified in the first scans, starting with a small scope is recommended. This can be achieved by starting out with a small number of systems or by limiting the number of vulnerabilities identified by the vulnerability scanner.

The preparation phase is mainly the responsibility of the GRC Team in the company. The first step is to define the scope of the vulnerability management process. It is important to obtain an agreement on which systems will be included or excluded from the vulnerability management process. Besides the in-scope systems, SNLC should also determine the type of scans. Possibilities can include either an external scan performed from the perspective of an external attacker on the internet or an internal scan from the perspective of an attacker on the internal network. Both types of scans can be either unauthenticated or authenticated scanning.

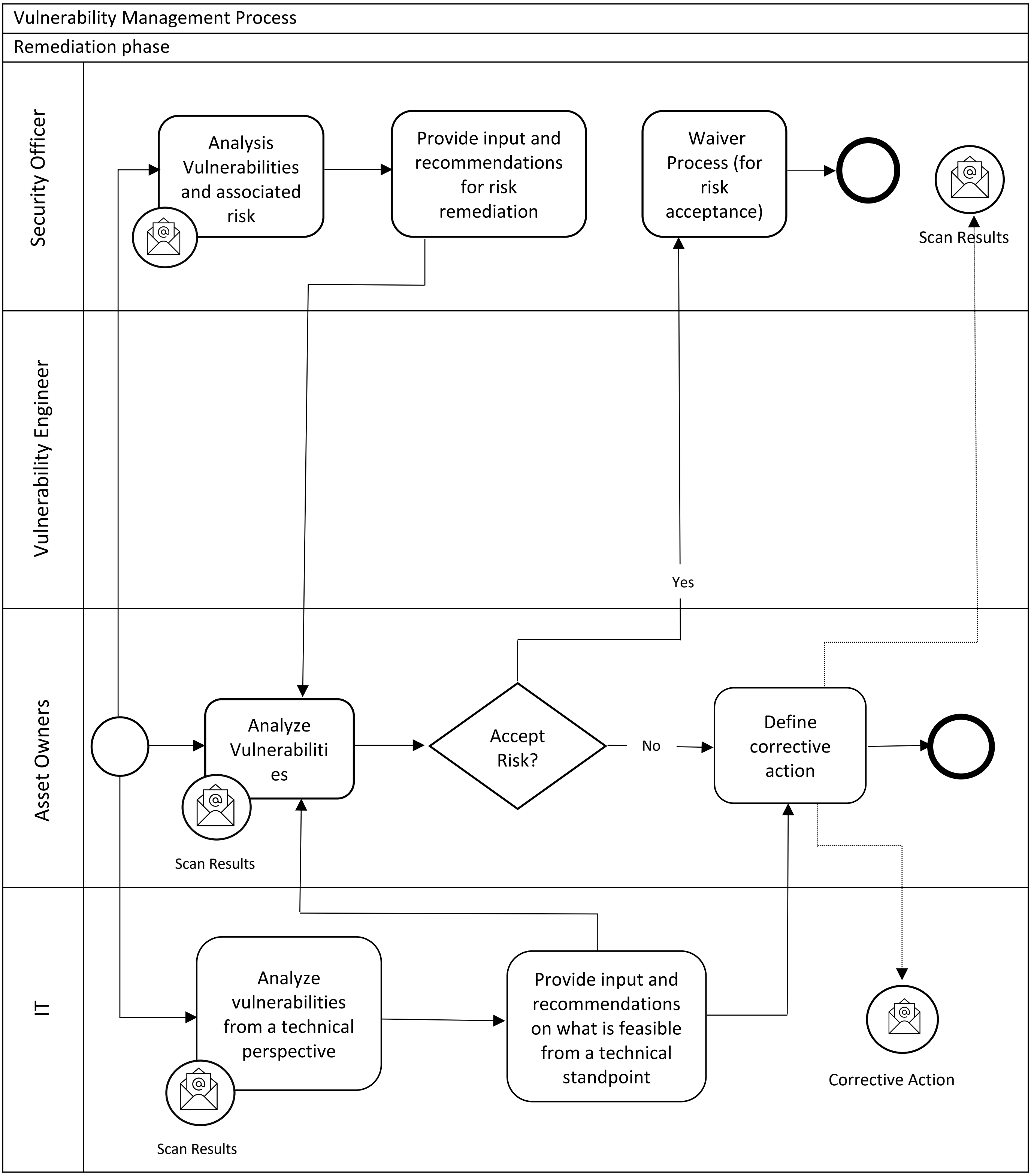
b) **Vulnerability scan**



Once the preparation phase is complete, the next phase of the process begins, and the initial vulnerability scans are performed. Most vulnerability scanning tools offer a wide range of reporting options to visualize scan results. It is necessary to use them to create various reports. Management and the security officer will be interested in the risk the organization is currently facing, this risk includes several vulnerabilities detected and the severity/risk rating of the identified vulnerabilities.

Asset owners will want to obtain an overview of vulnerabilities in the systems they are responsible for. The IT department will want an overview (per technology) of technical information about detected vulnerabilities as well as recommendations for mitigation and improvement.

c) **Remediation phase**


Vulnerability Management Process
Remediation phase
Security Officer
Vulnerability Engineer
Asset Owners
IT
Analysis Vulnerabilities and associated risk
Provide input and recommendations for risk remediation
Waiver Process (for risk acceptance)
Scan Results
Yes
Analyze Vulnerabiliti es
Accept Risk?
No
Define corrective action
Scan Results
Analyze vulnerabilities from a technical perspective
Provide input and recommendations on what is feasible from a technical standpoint
Corrective Action
Scan Results

In the next phase, the asset owners, with the cooperation of the GRC Team and the IT department, will define remediating actions. The GRC Team will analyze the vulnerabilities, determine the associated risks, and will provide input on risk remediation. The IT department will analyze the vulnerabilities from a technical. perspective and answer questions such as if patches are available or whether the configuration can be hardened. The IT department recommendation also includes the feasibility of the possible remediating action such as whether installing a certain patch will result in the application no longer being supported by the vendor. To ensure remediation is given sufficient priority the security officer should set clear deadlines for when the remediating actions will be implemented. Asset owners should include a timeline in their action plan indicating when these remediating actions will be implemented. The remediation timeframe should be in line with the level of risk detected. This timeframe will be different for each organization since the reaction speed will depend greatly on the risk appetite of the organization. For example:

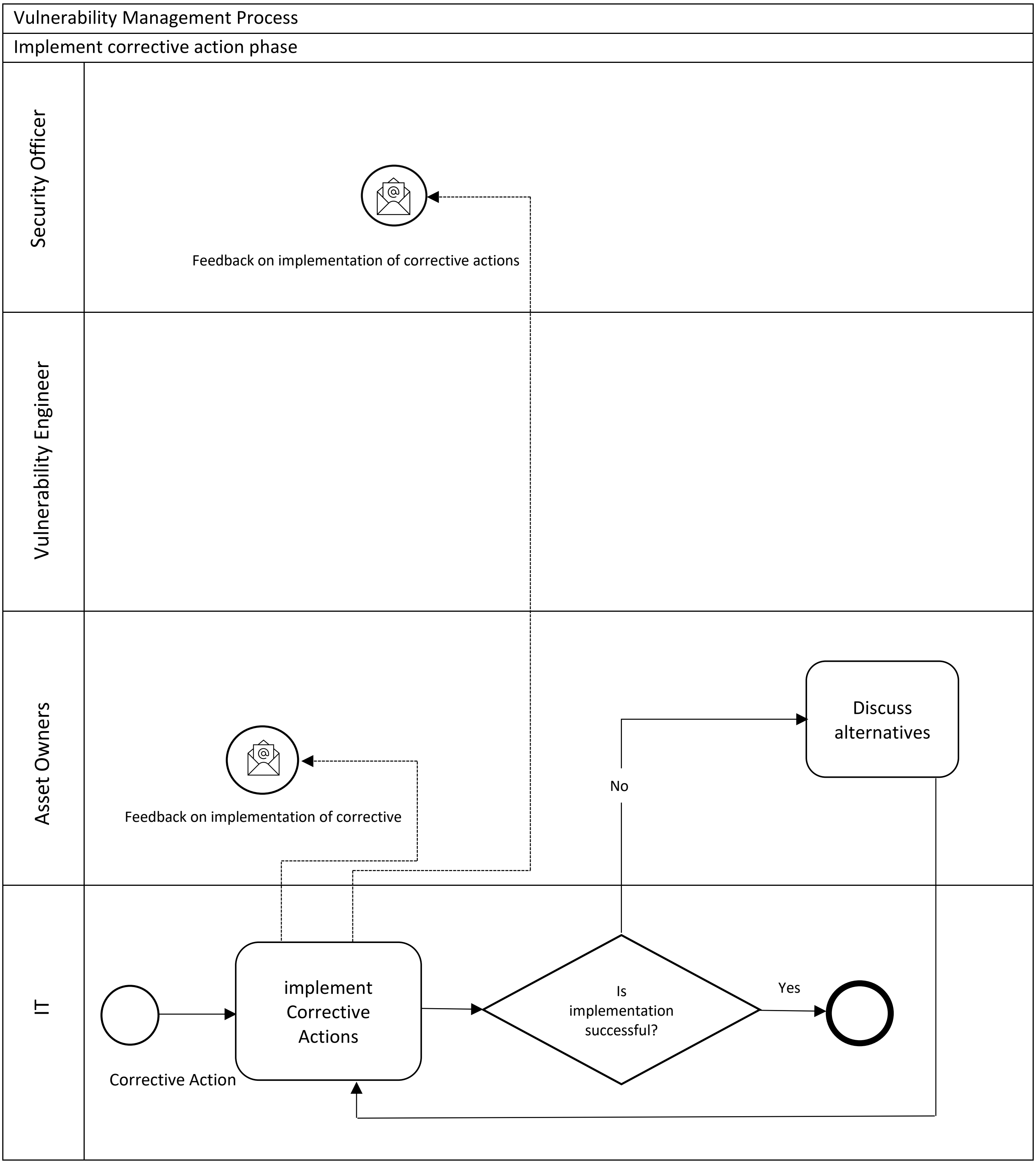
IP address	Scan Date	Vulnerability Detected	Risk Rating	Corrective Action	Implementation Date

The GRC Team keeps track of planned remediating actions to follow up on their implementation. This can be done by using a simple spreadsheet.

If short-term remediation is not possible, compensating controls should be identified to mitigate/remove the risk without correcting the vulnerability. Such compensating controls could include restricting network access to the vulnerable service, virtual patching, etc.

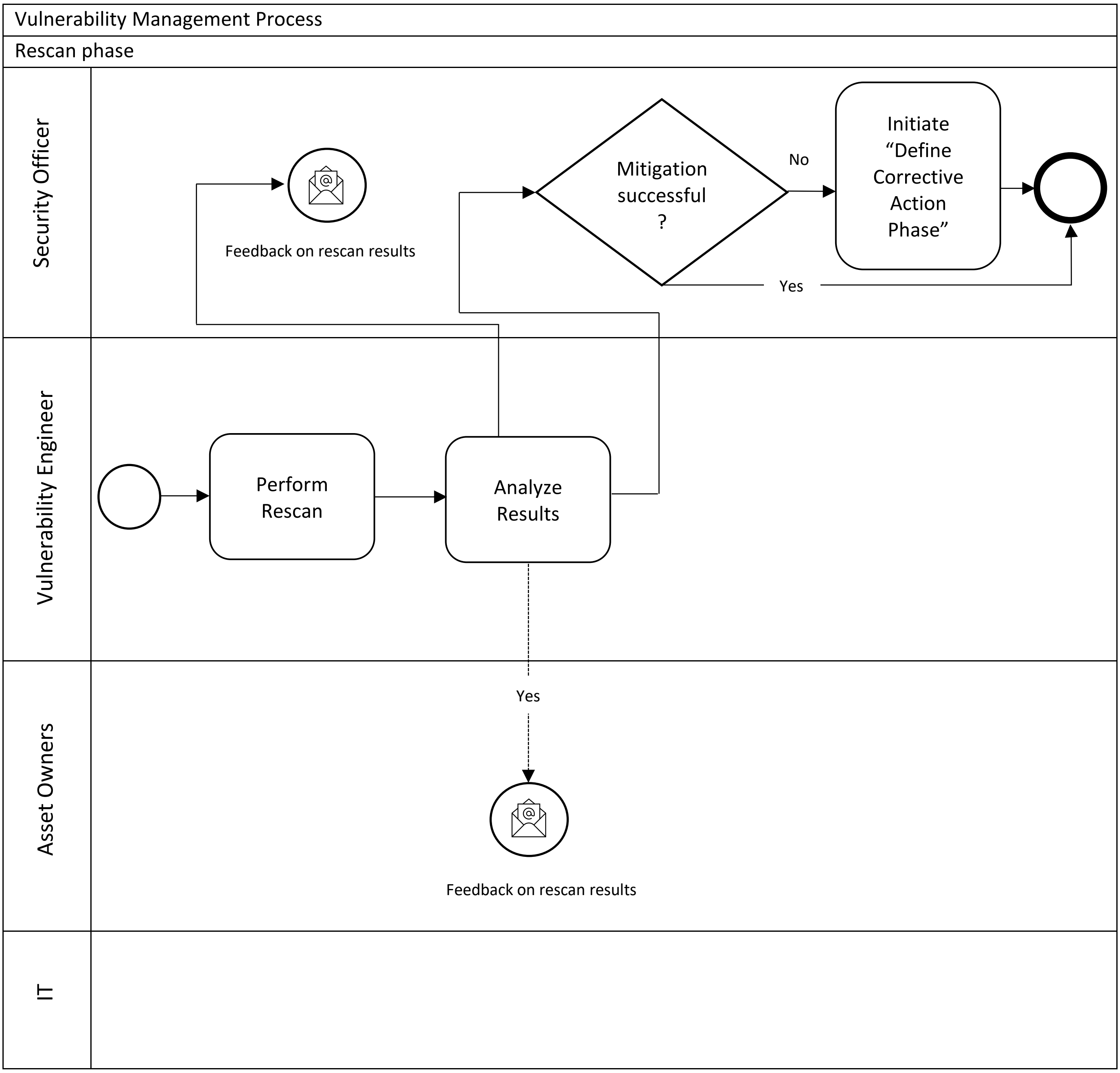
In case asset owners decide to accept the risk, it should be documented through a risk acceptance process. A risk acceptance or waiver process is a formal process in which an exception to the security policies can be requested.

d) Implement remediating actions


Vulnerability Management Process
Implement corrective action phase
Security Officer
Vulnerability Engineer
Asset Owners
IT
Feedback on implementation of corrective actions
Feedback on implementation of corrective
Discuss alternatives
No
Yes
implement Corrective Actions
Is implementation successful?
Corrective Action

The planned remediating actions should be executed in line with the agreed timeframes. If a problem occurs with implemented remediation, it should be recorded. Alternative actions should be defined by the asset owner based on recommendations by the GRC Team and the IT department. These new or other remediating actions should then be implemented. The GRC Team should track the status of the remediating actions.

e) Rescan


Vulnerability Management Process
Rescan phase
Security Officer
Vulnerability Engineer
Asset Owners
IT
Feedback on rescan results
Mitigation successful ?
No
Initiate "Define Corrective Action Phase"
Yes
Perform Rescan
Analyze Results
Yes
Feedback on rescan results

Once a vulnerability is remediated, a rescan must be scheduled to verify the remediating actions have been implemented. This scan will be performed using the same vulnerability scanning tools and identical configuration settings as the initial scan. This step is very important to prevent inaccurate results due to configuration errors. Typically, a rescan is scheduled after the deadline for implementing remediating actions.

The next step is an agreement between asset owners and the GRC Team on how often such scans will be scheduled. This timeframe should consider the risk appetite of the company, as well as the capability of the company to remediate identified vulnerabilities. To establish a mature vulnerability management process, it is recommended to schedule scans frequently, typically monthly. This will ensure rapid detection of vulnerabilities, allowing the company to determine and deploy mitigating controls in a timely fashion.

Correcting vulnerabilities from the initial scan provides good insight into the ability of the (IT) company to handle requests. Furthermore, lessons learned during the execution of the process should be used to reevaluate and improve the vulnerability management process.