Vulnerability Management Process description

WIKI PAGE URL

https://pb-wiki.intra.loyaltypartner.com/display/SM/Vulnerability+Management+Process+description

CREATED BY	EXPORTED BY
Matthias Trampler	Matthias Trampler
CREATION DATE	EXPORT DATE
04.07.2022	16.08.2022
MODIFICATION DATE	VERSION OF WIKI PAGE
16.08.2022	6

Table of Content

Document history

Date	Author	Version	Changes	Status
			For details see Wiki source!	
04 Jul 2022	Matthias Trampler	0.1	First Draft	
16 Aug 2022	Matthias Trampler	0.2	Rework of the first draft	

1 Overview

1.1 Vulnerability Management

Vulnerability Management is the recurring process of identifying, classifying, prioritizing, mitigating, and remediating vulnerabilities. This overview will focus on infrastructure vulnerabilities and the operational vulnerability management process. This process is designed to provide insight into our environments, promote healthy patch management among other preventative best-practices, and remediate risk; all with the end goal to better secure our environments.

This process must meet the requirements resulting from PLP-IS06.03.01 Vulnerability Management Procedure (https://toolbox.loyaltypartner.com/fileadmin/Dateien/Office_IT/Security/PLP-IS06.03.01_Vulnerability_Management_Procedure.pdf).

The following general conditions apply to PAYBACK:

- The IT operating processes at PAYBACK are set up in accordance with ITIL V3 and cover important processes such as incident, problem and change management.
- Vulnerability management effectively and efficiently identifies and addresses vulnerabilities in the PAYBACK system with the aim of remedying them as quickly as possible.
- The vulnerability management process ensures compliance with the DSGVO protection goals of "availability" and "resilience".
- The responsibilities of the vulnerability management process can be divided into the areas of IT Security and IT Operations.

The entire vulnerability management process is documented in the Wiki (https://pb-wiki.intra.loyaltypartner.com/display/SM/Vulnerability+Management+Process).

Definition:

Vulnerability Management in Information Security is the continuous process of identifying, evaluating and remediating security vulnerabilities in PAYBACK systems.

2 Roles and responsibilities

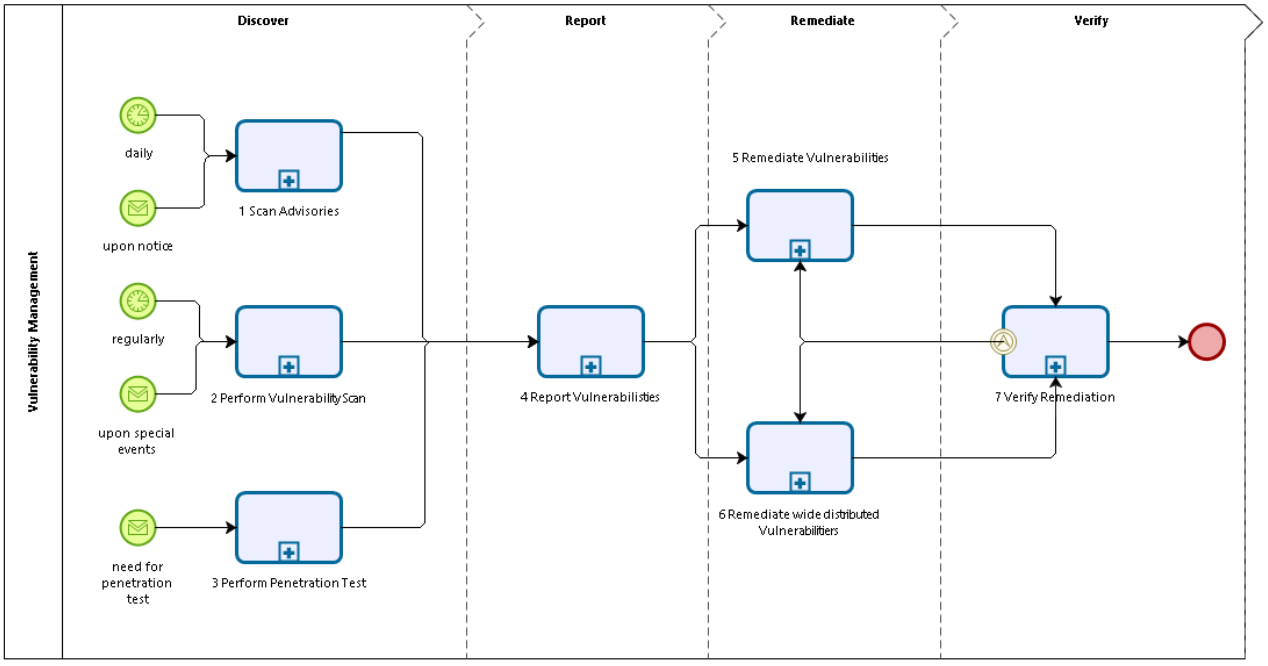
The following roles and groups are involved in handling the Vulnerability Management Process.

- **Information Security Team**
  - Checks third-party security advisories daily or upon notice.
  - Performs vulnerability scans on a regular basis or during special events.
  - Performs or orders (from AMEX or 3rd Party) penetration tests on a regular basis or in the case of special events
  - Prioritizes vulnerabilities and informs asset owners
  - Verifies the remediation of the vulnerabilities
- **AMEX**
  - Performs AMEX vulnerability scans.
  - Reports the test report to Information Security Team
- **Asset Owner**
  - Analyses the remediation options.
  - Develops remediation plan if necessary.
  - Remediate the vulnerability.
- **Procurement**
  - Validates the selected service provider,
  - negotiates a contract and
  - engages the service provider

3 Vulnerability Management Process

3.1 Overview

The following diagram shows the overview of the vulnerability management process:



The vulnerability management process consists of six different sub-processes, which are divided into four separate phases:

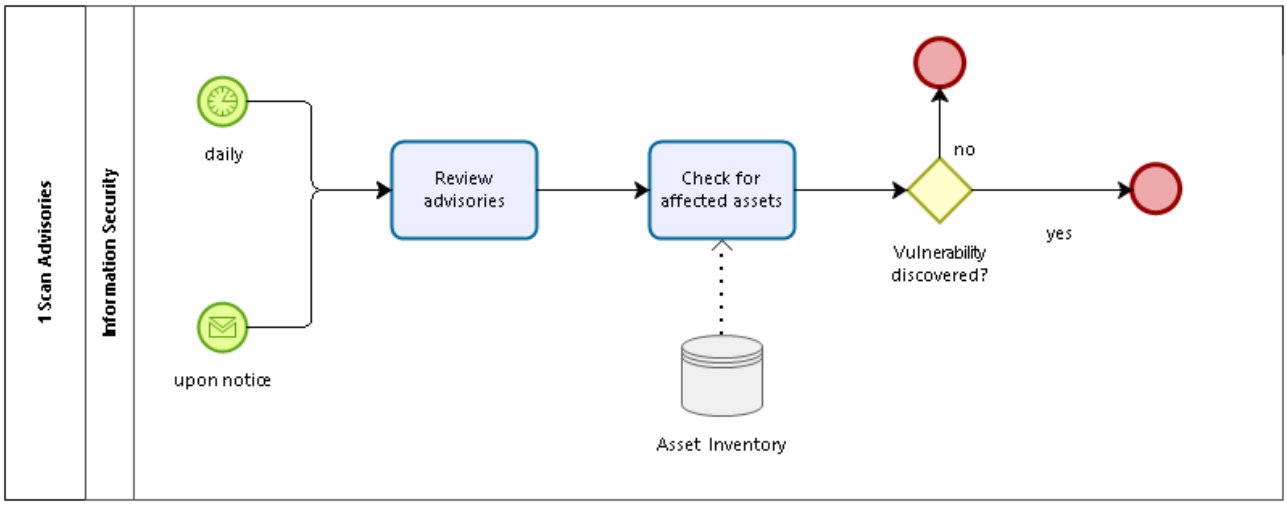
1. Discover Phase
   1. Subprocess - 1 Scan Advisories
   2. Subprocess - 2 Perform Vulnerability Scan
   3. Subprocess - 3 Perform Penetration Test
2. Report Phase

1. Subprocess - 4 Report Vulnerabilities

3. Remediation Phase
   1. Subprocess - 5 Remediate Vulnerabilities
   2. Subprocess - 6 Remediate wide distributed Vulnerabilities
4. Verify Phase
   1. Subprocess - 7 Verify Remediation

3.2 Discover Phase - Subprocess - 1 Scan Advisories

In the Scan Advisories subprocess, the third-party security advisories are checked daily or upon notice.



The process starts when the Information Security Team:

- receives or observes relevant security advisories by vendors, CERTs (Cyber Emergency Response Team) or news services daily;
- receives advisories e. g. from asset owners or vendors.

Review advisories

Information security reviews the advisories and communications to determine whether they are relevant to PAYBACK.

Check for affected assets

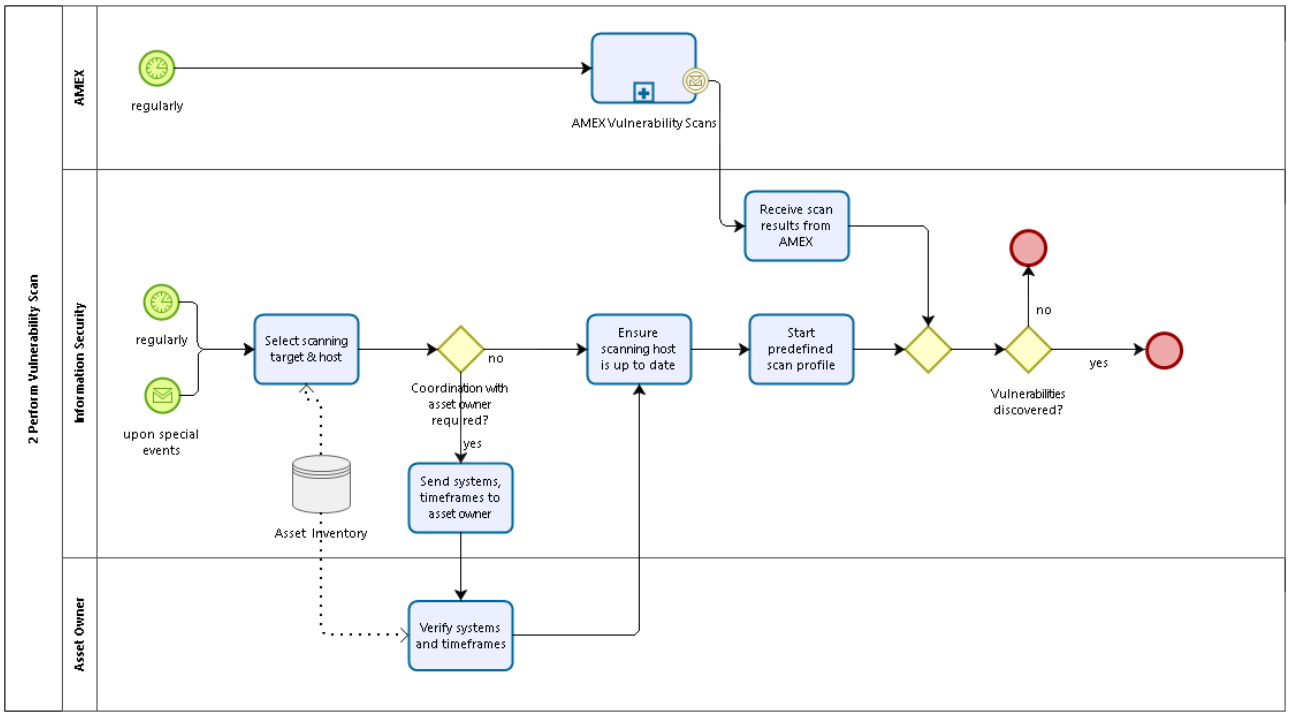
After the advisories have been checked, the asset inventory is used to search for affected assets. However, Information Security can currently not rely solely on the asset inventory. Therefore, asset owners and internal IT employees are consulted as well.

(The asset inventory servers as one point of information to identify assets affected by vulnerabilities as well as the asset owner. There are different sources to check: SREQ (Software Request) database, ITSM CMDB etc...)

If a vulnerability is discovered, then the Report Vulnerabilities subprocess is started, if none is discovered, then the process ends.

3.3 Discover Phase - Subprocess - 2 Perform Vulnerability Scan

In the "Perform vulnerability Scan" subprocess, vulnerability scans are performed by PAYBACK or AMEX.



The process starts:

- regularly configured by Information Security. Internet facing systems are scanned bi-weekly, intranet systems are scanned at least monthly;
- or regularly triggered by AMEX;
- triggered by special events such as newly discovered widespread security vulnerabilities.

Select scanning target & host

Information Security selects the scanning target. Depending on the scanning target the appropriate host is selected by using the information in the asset inventory.
Depending on the scanning target, it might be required to coordinate the timeframes for the planned scans with the asset owner.

Send systems, timeframes to asset owner

Information Security sends the scanning details including affected systems and planned timeframes for the scans.

Verify systems and timeframes

The asset owner verifies the details for the planned scan and checks for conflicts (e. g. planned downtimes). The asset owner rules out conflicts with Information Security.

Ensure scanning host is up to date

Before scanning, Information Security verifies that the scanning host is up to date and has the latest vulnerability patterns available.

Start predefined scan profile

Information Security starts the predefined scan profile matching the selected scanning target.

AMEX Vulnerability Scans

AMEX regularly performs vulnerability scans of PAYBACK websites.

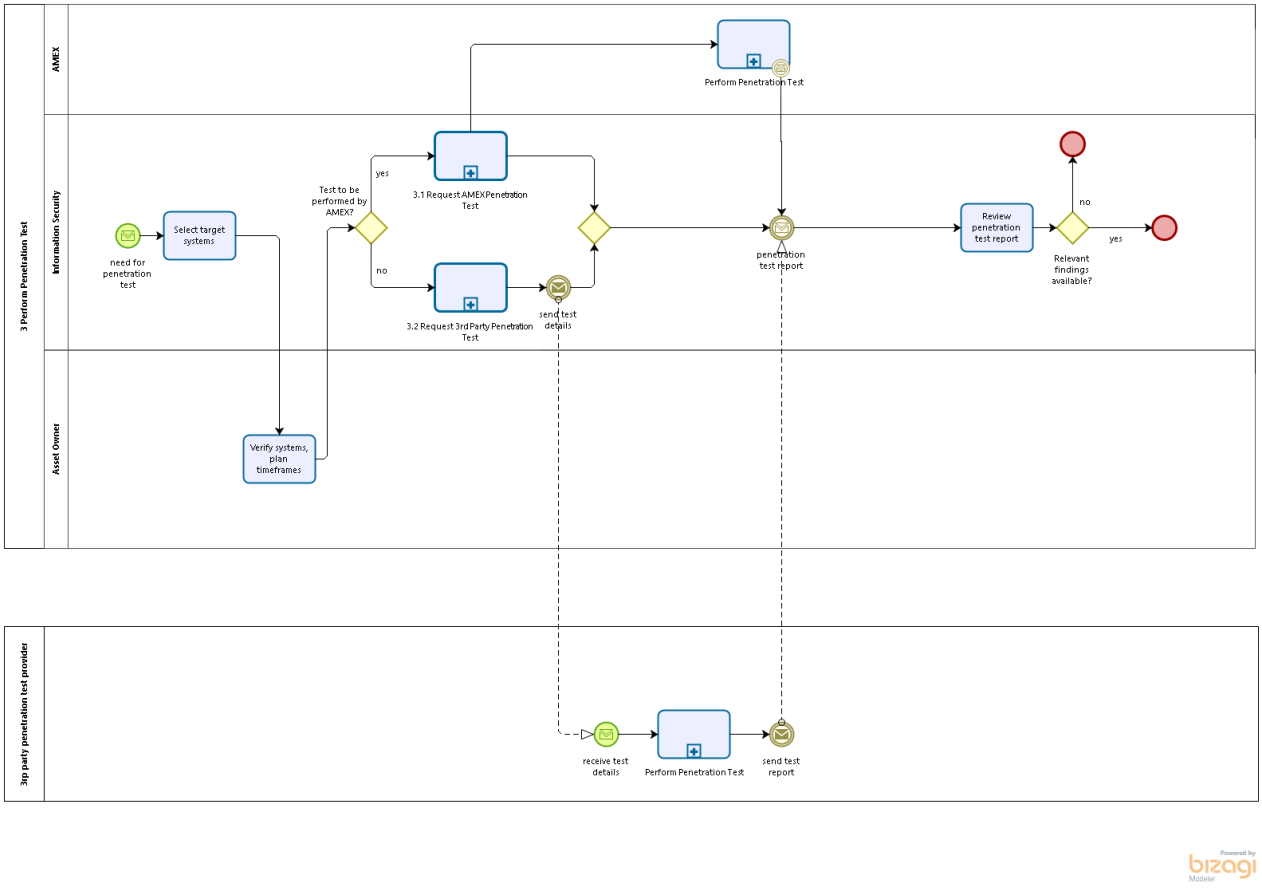
Receive scan results from AMEX

For vulnerability scans performed by AMEX, Information Security receives and reviews the scan results.

If a vulnerability is discovered, then the Report Vulnerabilities subprocess is started, if none is discovered, then the process ends.

3.4 Discover Phase - Subprocess - 3 Perform Penetration Test

In the "Perform Penetration Test" subprocess, penetration tests are requested by PAYBACK Information Security and performed by AMEX or a 3rd party penetration test provider.



The process starts when there is a need for a penetration test. Every internet-facing device shall be manually pen-tested by an external Tiger-Team at least once a year.

Select target systems

Information Security selects the target systems for the penetration test. According to the identified need for penetration testing, the target systems are defined within the scoping.

Depending on the target systems, it might be required to coordinate the timeframes for the planned scans with the asset owner.
Information Security sends the scanning details including affected systems and planned timeframes for the scans to the asset owner.

Verify systems, plan, timeframes

The Asset Owner(s) verifies the selected target systems as well as the timeframes for penetration testing to ensure penetration testing does not interfere with planned releases, system downtimes etc.

After the coordination with the Asset Owner(s), the Information Security checks if the penetration test is to be performed by AMEX or a 3rd party penetration test provider and requests the chosen penetration test.

Information Security checks if the penetration test can be performed by AMEX or a 3rd party penetration test provider.

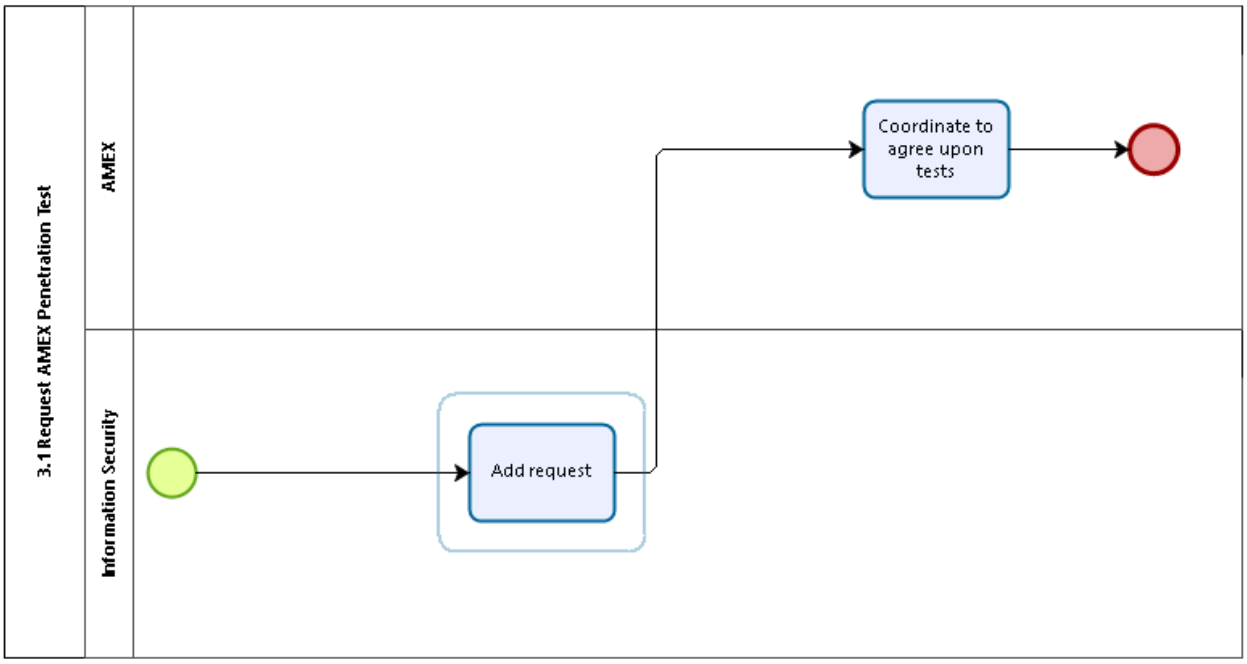
If AMEX can perform the penetration test the Subprocess 3.1 Request AMEX Penetration Test is started, if AMEX cannot perform it, the Subprocess 3.2 Request 3rd Party Penetration Test is started.

After commissioning the service provider, Information Security sends the test details to the service provider. The service provider carries out the test and sends back the test report. AMEX also sends back the test report.

The test report is checked by Information Security for relevant findings.

3.4.1 Subprocess 3.1 Request AMEX Penetration Test

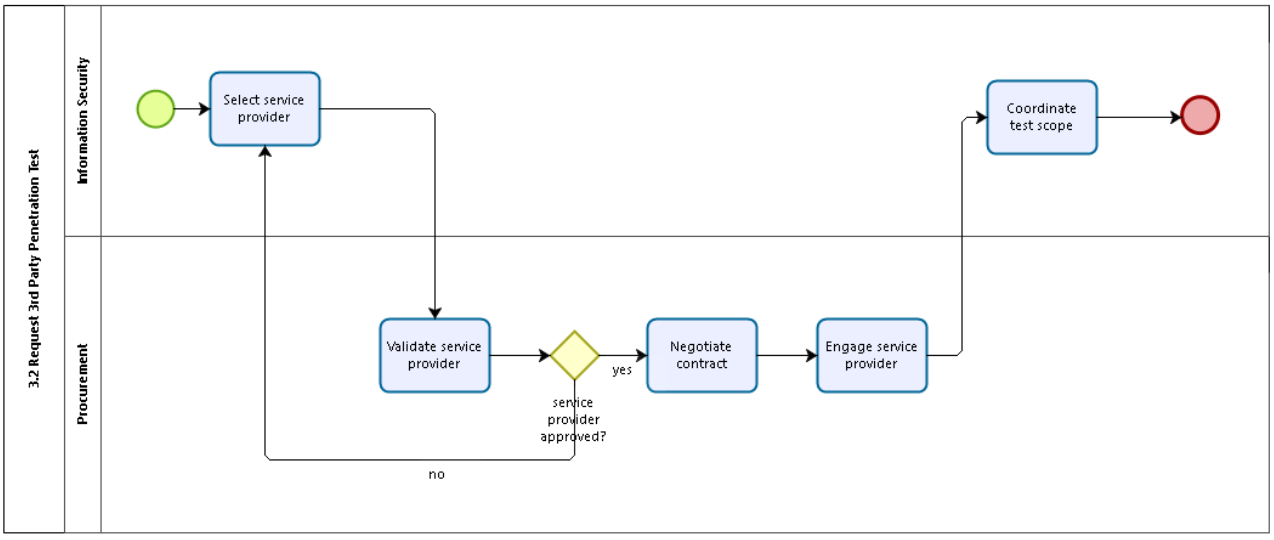
Information Security requests a penetration test with AMEX.



Information Security adds the request for penetration test in RSA Archer and after that, AMEX coordinates meetings to agree upon the scope and context of the planned penetration test.

Subprocess 3.2 Request 3rd Party Penetration Test

Information Security requests a penetration test with a 3rd party penetration test provider.

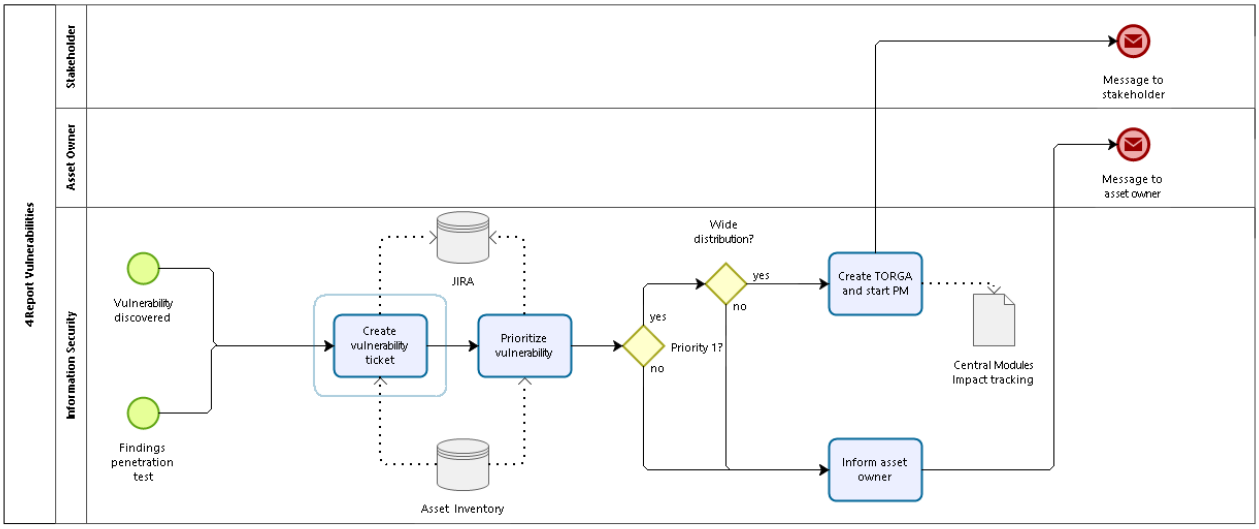


It is necessary, that Information Security selects a service provider who should conduct the penetration test. Once selected, procurement must verify that the service provider is validated, negotiate the contract and finalise it.
If the services provider is not approved, Information Security must select another service provider or start the onboarding of the vendor.

After engaging of the service provider, Information Security coordinates the kick-off meetings with the penetration test service provider and defines the test scope.

3.5 Report Phase - Subprocess - 4 Report Vulnerabilities

In the "Report vulnerabilities" subprocess, discovered vulnerabilities or findings from penetration tests are reported to the asset owner and the affected stakeholders.



Information Security creates a new JIRA ticket for each of the discovered vulnerabilities or penetration test findings. JIRA tickets are tracked in the Information Security (INFOSEC) project space. See https://pb-jira.intra.loyaltypartner.com/secure/RapidBoard.jspa?rapidView=14107&view=detail&quickFilter=24383

The asset inventory servers as one point of information to identify assets affected by vulnerabilities as well as the asset owner. There are different sources to check: SREQ database, ITSM CMDB etc...

Information Security prioritizes the detected vulnerabilities according to the relative CVSS score. Vulnerabilities of a CVSS score of 9.0 - 10.0 are rated critical with a priority of 1, vulnerabilities with a CVSS score of 7.0 - 8.9 are rated high with a priority of 2, vulnerabilities with a CVSS score of 4.0 - 6.9 are rated medium with a priority of 3, vulnerabilities with a CVSS score of 0.0 - 3.9 are rated low with a priority of 4.

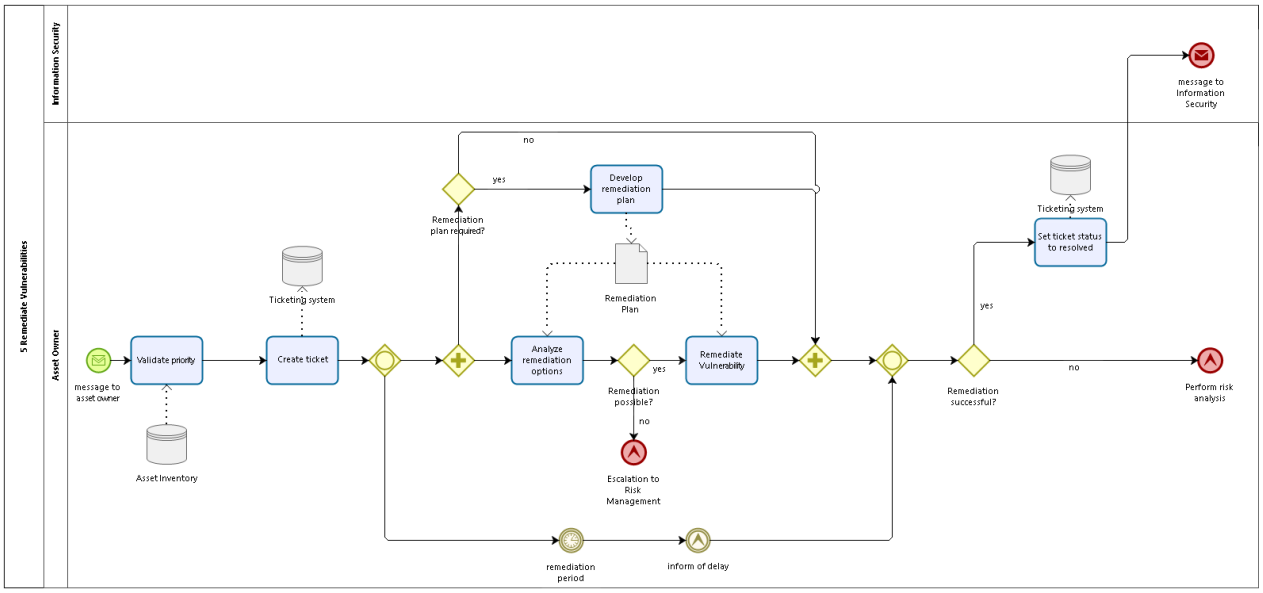
Information Security must check after priorization if it is a critical vulnerability with a CVSS score of 9.0 - 10.0 (classified as priority 1) according to the standard PLP-IS06.03.01 Vulnerability Management Procedure. If it is a priority 1 and the check for wide distribution is positive, Information Security creates a TORGA and designates in collaboration with PM (Project Management) Team a project manager who is responsible for tracking the remediation of the vulnerability. For tracking it is necessary to create a central modules impact tracking sheet (Excel). A message to the stakeholders (e.g. Technical Owner, TWG, Modul Owner, Core Technical Strategy Working Group Member, Order of Phoenix Group Member) is sent, containing:

- the problem statement (vulnerability description, the severity of the vulnerability);
- a due date until this vulnerability must be fixed
- PM/TORGA information's

If the vulnerability or penetration test finding does not have priority 1 and/or wide distribution, a message to the asset owner is sent, containing the vulnerability description, the affected assets, the severity of the vulnerability and the priority estimated by Information Security.

3.6 Remediate Phase - Subprocess - 5 Remediate Vulnerabilities

In the "Remediate Vulnerabilities" subprocess, discovered vulnerabilities or findings from penetration tests are remediated by the asset owner and the affected stakeholders.



Validate Priority

The Asset Owner validates the assigned severity and priority of the vulnerability by using the asset inventory servers as one point of information to identify assets. There are different sources to check: SREQ database, ITSM CMDB etc...

Create ticket

The Asset owner creates a ticket for the vulnerability in his ticketing system (asset owners do not necessarily use JIRA).

Analyse remediation options

The Asset Owner analyses remediation options and decides which one to choose. If necessary, Information Security can be consulted.

Develop remediation plan

The Asset Owner creates a remediation plan for the vulnerability.

Remediation possible

If the vulnerability cannot be remediated, this is escalated to Risk Management where further alternatives are evaluated.

Remediate Vulnerability

If the remediation is possible the Asset Owner takes necessary steps to remediate vulnerabilities.

Remediation period

Parallel to this depending on the assigned priority, the proper remediation period must be kept. These are as follows:
Prio 1: 48 hours
Prio 2: 8 days
Prio 3: 28 days
Prio 4: 3 months

Inform of delay

If the remediation period passes without the vulnerability being closed, the delay is escalated to Information Security.

Remediation successful

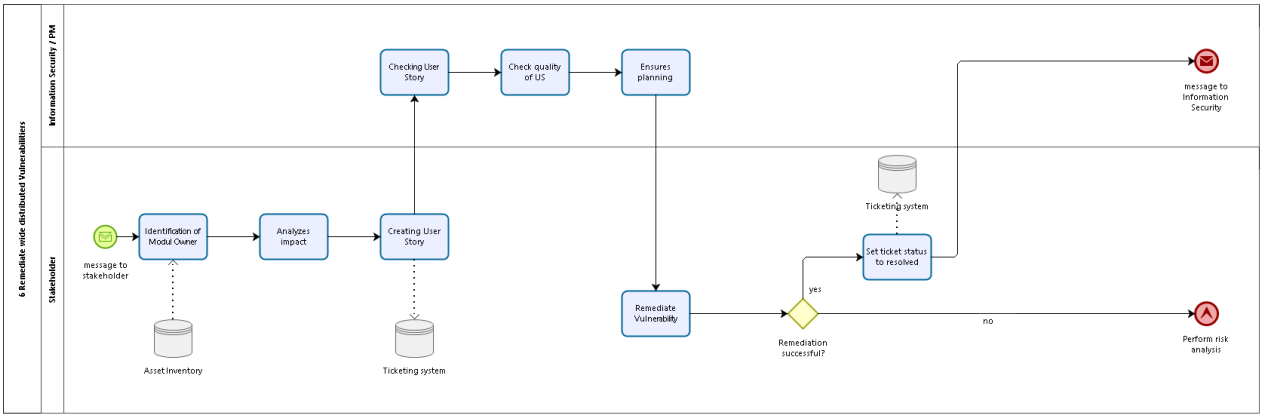
If the vulnerability cannot be remediated, this is escalated to Risk Management where further alternatives are evaluated.

Set ticket status to resolved

If the remediation effort was successful, the Asset Owner sets the status of his vulnerability ticket to resolved and informs Information Security.

3.7 Remediate Phase - Subprocess - 6 Remediate wide distributed Vulnerabilities

In the "Remediate wide distributed Vulnerabilities" subprocess, discovered vulnerabilities or findings from penetration tests are remediated by the asset owner and the affected stakeholders.



Identification of Modul Owner

Core Technical Strategy Working Group/ Order of Phoenix Member (Stakeholder) doing an initial check and identifies corresponding Modul Owner by using of the asset inventory servers as one point of information to identify assets affected by vulnerabilities as well as the asset owner. There are different sources to check: SREQ database, ITSM CMDB etc.

Analyses impact

The responsible Tech Owner / Module Owner identifies the impact for his modules that are affected by the vulnerability.

Creating User Story

Tech Owner / Modul Owner creates a User Story for the changes for the module. This US must contain following information:

- remediation option

Checking User Story

Information Security Team and Project Manager is checking the User Story in coordination with the Owner, advice the Owner about the User Story and gives feedback.

Check quality of US

The Project Manager / Information Security Team checks and ensures overall quality of the US and the linkage with the PM.

Ensures planning

The Project Manager / Information Security Team ensures the planning of the US with the SM and PO according to the timelines.

Remediate Vulnerability

The Owner takes necessary steps to remediate vulnerabilities.

Remediation successful

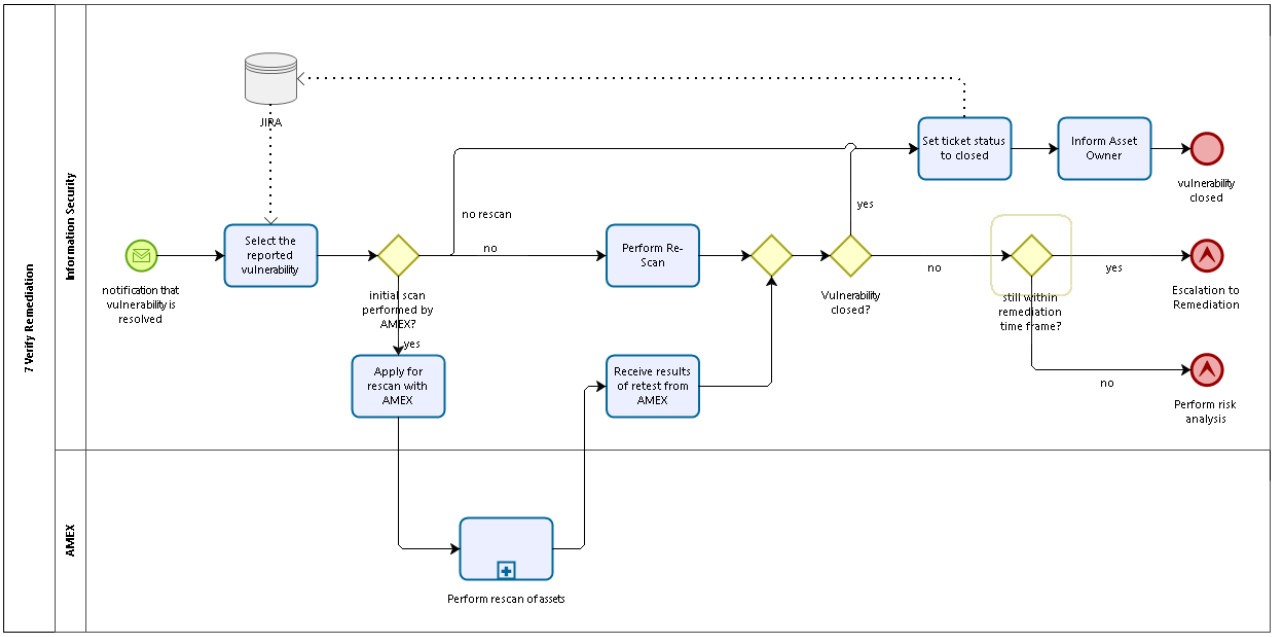
If the vulnerability cannot be remediated, this is escalated to Risk Management where further alternatives are evaluated.

Set ticket status to resolved

If the remediation effort was successful, the Asset Owner sets the status of his vulnerability ticket to resolved and informs Information Security.

3.8 Verify Phase - Subprocess - 7 Verify Remediation

In the "Verify Remediation" subprocess, discovered Information Security verifies if the remediation of the vulnerabilities or findings from penetration tests was successful.



Select the reported vulnerability

If the Asset Owner has resolved a vulnerability, a notification is sent to Information Security. Information Security selects the initial vulnerability from the JIRA issue and checks if the initial scan was performed by AMEX.

Apply for rescan with AMEX

If the scan was performed by AMEX, Information Security applies for a rescan with AMEX for vulnerabilities which were initially discovered by AMEX.

AMEX performs a rescan of the reported combinations of assets and vulnerabilities.

Receive results of retest from AMEX

Information Security receives the results of the performed rescans from AMEX and verifies whether the vulnerabilities were closed.

Perform rescan

For vulnerabilities that were initially discovered by Information Security, the rescan is performed by Information Security.

Vulnerability closed

If the rescan by AMEX or by Information Security shows that the vulnerability is closed or there is no rescan necessary Information Security closes the JIRA issue and informs the Asset Owner of the successfully performed retest.

If the rescan shows that the vulnerability is not closed and the remediation period has not expired, an escalation is sent to the asset owner for remediation. If the vulnerability is not remediated in the required period, this is escalated to Risk Management where further alternatives are evaluated.