**Process Document - 4**

**Vulnerability Assessment Process**

|  |  |
| --- | --- |
| **Document Control Sheet** | |
| **For Airtel Money Environment only** | |
| Document Name | Vulnerability Assessment Process |
| Document Owner |  |
| Effective Date |  |
| Review Date |  |
| Review Remarks |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Document Version Control** | | | | |
| **Version** | **Date** | **Prepared By** | **Reviewed By** | **Approved By** |
|  |  |  |  |  |
|  |  |  |  |  |

**Table of contents**

[1.0 Introduction 3](#_Toc349291856)

[2.0 Scope 3](#_Toc349291857)

[3.0 Vulnerability Assessment Process 4](#_Toc349563918)

[4.0 Vulnerability Assessment Procedure 5](#_Toc349563919)

[5.0 Roles & Responsibilities 7](#_Toc349563920)

[6.0 Vulnerability Assessment Report 8](#_Toc349563921)

[7.0 Performance Metrics and Benchmarks 8](#_Toc349560309)

[7.1 KPI 8](#_Toc349560310)

[7.2 Vendor SLAs 8](#_Toc349560311)

1.0 Introduction

Vulnerability assessment is the process of identifying, quantifying, and prioritizing (or ranking) the weaknesses in a system, network or communications infrastructure. It is in fact a methodical evaluation of an organization’s IT weaknesses of infrastructure components and assets and how those weaknesses can be mitigated through proper security controls and recommendations to remediate exposure to risks, threats and vulnerabilities.

This process will run as per the following periodicity:

The vulnerability assessment for all online Servers/Networks/Security devices of Airtel Money environment will be conducted once in a Quarter.

Devices in Test and Development zone are not covered under the scope of Vulnerability Assessment process except the ones having customer data.

2.0 Scope

The scope of this process is to identify vulnerabilities in Servers, Endpoint devices, Network devices, with reference to Airtel Money environment by Mahindra Comviva and to close the high and medium hole of vulnerabilities. Low risk vulnerabilities are for information purposes only and not require any further calculation or migration

3.0 Vulnerability Assessment Process

A Vulnerability and Security Assessment is an excellent way to evaluate existing security posture and a great first step to take prior to making security improvements at Organization facility or when trying to solve a specific security problem.

During a Vulnerability and Security Assessment, all aspects of Organization facilities’ security are examined, any weaknesses are identified, and suggestions for security improvements are provided. In addition, opportunities where costs can be reduced or where security operations can be made more efficient are identified.

Vulnerability and Security Assessment process uses a structured, formal analysis process that allows us to gain a deep understanding of your business’ security requirements, operating conditions, policies and your surrounding community’s security risks and threats.

While client involvement is crucial to a successful assessment, our consultants facilitate the assessment every step of the way, keeping the project on track, and making sure that all important elements are examined

**Definitions**

Vulnerability: A flaw or weakness in system security procedures, design, implementation, or internal controls that may result in a security breach or a violation of the system's security policy.

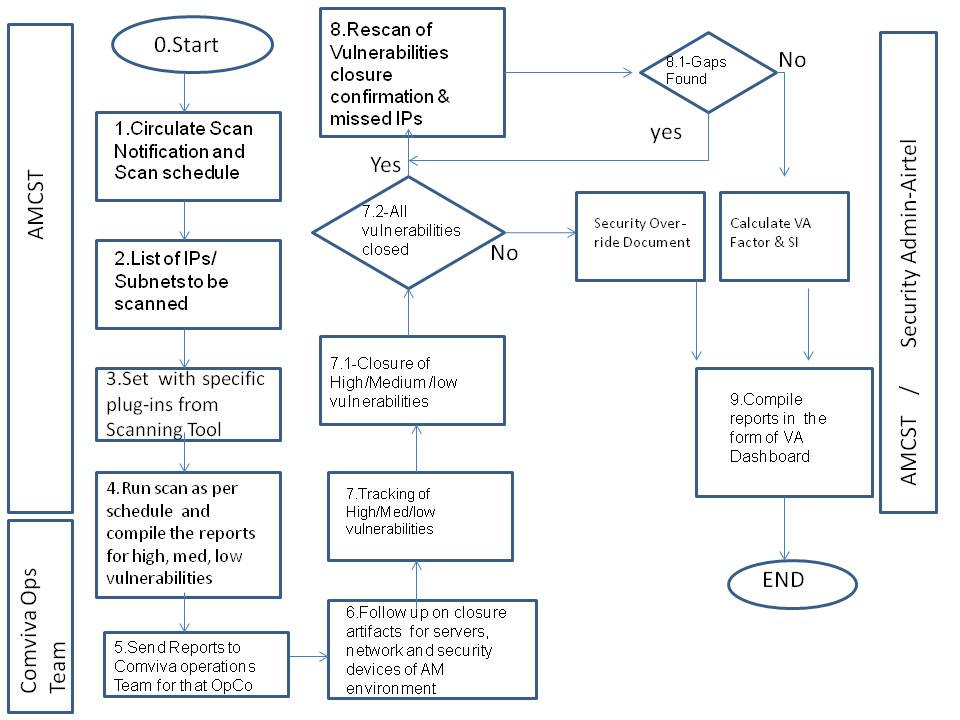
Threat: The potential for a specific vulnerability to be exercised either intentionally or accidentally

Control: measures taken to prevent, detect, minimize, or eliminate risk to protect the Integrity, Confidentiality, and Availability of information.

Vulnerability Assessment: The process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system.

4.0 Vulnerability Assessment Procedure

4.1 Process Flow diagram

****

4.2 VA Process Flow

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sl. No.** | **Activity** | **Responsibility** | **Output** | **Internal SLAs/ Performance Criteria** |
| 1 | Perform Vulnerability Scanning and Conduct Random Sample Checks | AMCST | List of systems vulnerabilities |  |
| 2 | Circulate Scan Notification and Scan schedule | AMCST | Scan notification | NIL |
| 3 | Set the baseline for scanning. | AMCST |  | NIL |
| 4 | Perform vulnerability scanning as per schedule and compile the reports for high and medium and low vulnerabilities. | AMCST | Vulnerability assessment scan reports |  |
| 5 | After scanning AMCST will send the list of high and medium, low vulnerabilities report to Comviva Operations Team. | AMCST | List of high and medium, low vulnerabilities report |  |
| 6 | Collect closure artifacts only for servers, network devices and security devices of Airtel Money environment. As soon as artifacts are uploaded VA Alert will be sent for closure artifacts validation | AMCST/ Comviva Ops Team | closure artifacts |  |
| 7 | Tracking of High/Medium/low vulnerabilities - AMCST will track all vulnerabilities closed/False Positives/Security Override Risk And will look for Closure of these vulnerabilities | AMCST/ Security Admin-Airtel | Gap analysis, checklist. Handling False Positive |  |
| 8 | Rescan for Vulnerabilities closure confirmation , And check for gaps; if found any will track those vulnerabilities for closure | AMCST | NIL |  |
| 9 | Compile reports VA Dashboard | AMCST | VA Dashboards |  |

5.0 Roles and Responsibilities

|  |  |
| --- | --- |
| **Role** | **Responsibility** |
| AMCST/ Comviva Operations Team | Responsibilities include: |
|          Maintaining VA and System Index measurements for reporting and forecasting. |
|          Analyze trends, service level commitments and thresholds. |
|          Establish thresholds and exception (alerts) reporting procedures |
|          Implement approved VA and SI changes according to requirement. |
|          Provide technical support and advise to address VA issues. |
|          Advise the Process analyst of any required system configuration or modifications to meet VA and SI targets |
|          Publish VA schedule |
|          Ensure the closure of high and medium vulnerabilities. |
|          Circulate notifications and schedule scan |
|          Run VA scan as per schedule. Rescan for missed IP and vulnerability closure confirmation. |
|          Calculate various security indices, such as VA Factor, System Index |
|          Compile Reports and share with stakeholders on the vulnerabilities and their potential solution options. |
|          Declare false positives. |
|          Analyzes the reports for vulnerability closure |
|          Work on the implementation of the solutions for vulnerabilities closure. |
| ·  Security Over-Ride Document to be prepared for vulnerabilities that couldn't be closed. |

1. Vulnerability Assessment **Reports**

* Vulnerability Assessment Scan report from Nessus scanning Tool
* VA Dashboard

1. **Performance Metrics and Benchmarks**
   1. **Key Performance Indicators**

|  |  |  |  |
| --- | --- | --- | --- |
| **KPI** | **Responsibility** | **Data Source** | **Periodicity** |
| VA for all online Servers/Network/Security Devices | AMCST | VA review report | Quarterly |
| Implementation of the solutions for vulnerabilities closure |  | False positive list/Audi report | Quarterly |

7.2 SLAs

|  |  |  |
| --- | --- | --- |
| **Service Provided** | **SLA parameter** | **Parameter Threshold** |
| Vulnerability assessment for systems | Time to perform vulnerability assessment on target systems and implement solutions for identified vulnerabilities | 100% of systems should be implemented with vulnerabilities of Medium and high risk |

Annexure :

1. Contact Details :

|  |  |  |
| --- | --- | --- |
|  | **Contact Person** | **Contact details** |
|  |  |  |
|  |  |  |
|  |  |  |