TRIANZ℠

Vulnerability and Penetration Testing Procedure

TRIANZ INTERNAL

trianz.com

Statement of Confidentiality

The information contained in this document is internal to Trianz. It shall not be disclosed, duplicated, or used for any purpose other than that stated herein, in whole or in part, without the express written consent of Trianz.

Information Classification

☐	Public
☒	Internal
☐	Confidential
☐	Restricted

Table of Contents

1. Introduction

Vulnerability Assessment and Penetration Testing is an integral part of information security best practices. It provides the organization with a comprehensive infrastructure and application evaluation.

2. Objective(s)

- Evaluate the weaknesses in Trianz managed Infrastructure and Information Assets that can be exploited by external and internal attackers
- Evaluate the effectiveness and ineffectiveness of Trianz security infrastructure & applications implemented by both Trianz and third-party vendors.

3. Scope

- The scope includes all Infrastructure, systems, applications and Information Assets that are owned, operated, maintained, and controlled by Trianz internally and externally either on premises or on cloud.

4. Entry Criteria

- All critical Projects, Products and functions identified for VAPT.

5. Input

- As per MSA/SOW
- Requirement from the Projects/Products
- As per business criticality of the application

6. Process Description (Procedure)

6.1 Vulnerability Assessment and Penetration Testing Process

The responsibility of carrying out vulnerability assessments has been assigned to Information Systems Team, Project Team, corporate functions team, product teams and/or an external party. The broad sets of responsibilities are as per the following listing

Sl. No.	Responsibility	Process Name	Process Description
1.	IS Team / Project Team/Product team	Initiate assessment planning	Initiate formulation of the Assessment Plan.
2	IS Team/ Project Team/Product team	Check latest asset inventory	Check the latest inventory for newly included servers/applications etc. in the setup which were not included in the last VA scan
3	IS Team/ Project Team/Product team	Prepare list of assets in scope	Prepare list of assets to be included and send an email to application/database owners to finalize devices and seeking their inputs or any other relevant information.
4	IS Team/ Project Team/Product team	Finalize list of assets in scope	Prepare final list of devices after taking input/feedback from other stakeholders
5	IS Team/ Project Team/Product team	Finalize dates of assessment	Send email communication to application/database teams to finalize schedule for assessment.
6	IS Team/Internal Apps/ Project Team/Product team	Confirm VA/PT assessment calendar	Cross check the dates given by InfoSec Team with calendar and inform the InfoSec Team regarding approval or modification in the dates.
7	Application/ Database Owner/Product team	Confirm VA/PT assessment calendar	Provide any relevant information required by InfoSec Team prior to starting of VA / PT assessment. Cross check the dates communicated by the InfoSec Team with calendar and inform the InfoSec Team regarding approval/rejection
8	IS Team/ Project Team/Product team	Communicate the assessment dates	Send an email communication to relevant stakeholders on receipt of a sign-off on dates
9	IS Team/ Project Team/Product team	Prepare plan for the assessment	Prepare a day wise plan for the Vulnerability Assessment and ensure readiness of following resources • Availability of relevant team members on respective dates

Sl. No.	Responsibility	Process Name	Process Description
			• Availability of VA/PT admin user-IDs on all target servers. All other aspects related to starting the VA/PT assessment as per the plan.

6.2 Vulnerability Assessment

- Vulnerabilities are identified at infrastructure and network level by running tools viz., Nessus and Burpsuite with latest versions.
- For PCI-specific environments, perform vulnerability scans on internal/external IP addresses; use an Approved Scanning Vendor (ASV) and track findings through remediation.
- Alerts and threats published by OEMs and certified agencies.
- Alerts and threats published by SANS, OWASP, NVD and CVSS is helpful to find vulnerability.
- Before proceeding with Vulnerability Assessment, the scope of the assessment to be clearly defined. The scope is based on the asset inventory to be assessed.
- The Vulnerability Assessment process is divided into three phases:
  - Pre-Assessment Phase (Information Gathering)
  - Assessment Phase (Detection, Analysis and Remediation)
  - Post Assessment Phase (Reporting and Monitor)

6.3 Pre- Assessment Phase (Information Gathering)

- VA team should gather information about the asset inventory as pre-requisites. The following information to be collected as minimum.
- Network architecture view e.g. MPLS, VLAN.
- Security appliance configuration like IDS, IPS, and UTM
- Switches, Routers, Web proxies and Firewall configurations.
- IP addresses of on premises and on cloud appliances
- Operating System version.
- Identify the critical assets

- Application details in case of Projects
- Roles and Responsibilities of Associates
- Security configuration of Website (e.g. security certificate, services running)

6.4 Assessment Phase (Detection, Analysis and Remediation)

Detection: After the finalization of devices and assets are to be assessed for the existence of vulnerabilities; the next step is to execute the selected tool.

- The actual execution of the tool shall be done as per the 'day-wise' and 'resource-wise' plan detailed in the asset inventory.
- Further to the above, the tool like Nessus, Burp Suite is used to find the vulnerabilities of assets as per in the asset inventory.
- The vulnerability like misconfiguration of patches, OS version and configuration of network architecture is to be segregated as per asset inventory.
- On the VA scanner ensure that discovery scanning is enabled to identify the new Information Assets connected to the Trianz network
- Mandatory VA scanning shall be conducted for all the information Assets before accessing the Trianz network.
- Associates travelling from high-risk geo locations with the Trianz Informational Assets (e.g. Laptop), ensure mandatory VA scanning shall be conducted post travel on the information Assets before connecting to the Trianz network.

Analysis: Analyze and prioritize the activity as per the criticality and impact of the vulnerability. The analysis of vulnerability is to be calculated based on the CVSS score.

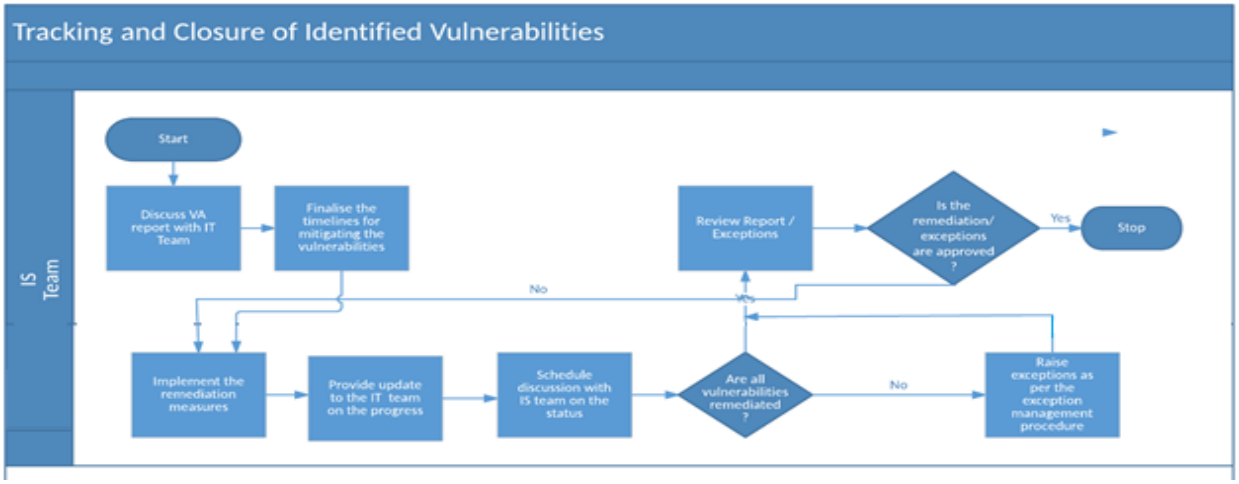
Analyze the vulnerabilities as per the best practice:

- Common Vulnerability Scoring System (CVSS)
- Common Vulnerabilities and Exposure (CVE)

Vulnerability Severity Rating: The severity of vulnerability is to be checked as per the asset inventory in risk register. Refer to Risk Management Procedure

Remediation: Vulnerabilities are remediated in accordance with calendar and further revalidations are done to ensure closure. Remediation will be done by Assets owner and review will be carried out by CIO/CISO prior to approval.

Tracking Closure of Identified Vulnerabilities



The above Flow Chart (FC) is described in the following table.

Ref. to FC	Responsibility	Process Name	Process Description
1.	IS Team/ Project Team	Discuss the VA Report	Recommendations with the IS Operation
2	IS Team/ Project Team	Finalize timelines	Agree on the timelines for fixing the vulnerabilities
3	IS Team/ Project Team /Internal Apps	Share reports	Share the report with application and database team Fix timelines for closure
4	IS Operations/Internal Apps	Implement the recommendations	Implement the recommendations provided for the vulnerabilities which can be closed
5	IS Operations/Internal Apps	Update on implementation status	Provide update to the IS and application/database team

Ref. to FC	Responsibility	Process Name	Process Description
6	IS Operations/Internal Apps	Discussion with InfoSec Team on remediation status	Schedule a discussion with the InfoSec Team and document the vulnerabilities with reasons for non-closure
7	IS Operations/Internal Apps	Remediation Status	If all the vulnerabilities have been remediated, then submit the report to the InfoSec Team for review else the exception management procedure needs to be followed.
8	IS Team/ Project Team	Exception	Initiate the Exception Management Process in case there is a vulnerability that cannot be fixed due to a valid requirement
9	InfoSec Team	Review Reports / Exceptions	CIO/CISO to review the final remediation report and the exceptions raised and approve. If unsatisfied, the InfoSec Team will ask the concerned team to further mitigate the vulnerability.

Timeline for fixing the vulnerability.

Sl. No	Vulnerability Severity	Time for mitigation
1	Critical	01 day
2	High	07 days
3	Medium	15 days
4	Low	30 days

Subject to approval from the business functions and approved downtime

6.5 Post Assessment Phase (Reporting and Monitor):

Reporting: Convert the final list of rated vulnerabilities into a separate VA report. This report should include vulnerabilities, affected assets, server details, vulnerability ratings, recommendations for fixes, best practices.

Prepare a management summary report of vulnerability assessment

Share the report with respective teams.

A management report containing the server details, vulnerabilities, rating and recommendations. It should also contain management summary for the findings in the VA assessment

Monitoring: The Vulnerability assessment must be monitored continuously as per the VAPT Report evaluation checklist.

6.6 Penetration Testing

Penetration testing checks the system's ability to protect its networks, applications, endpoints and users from external or internal threats based on vulnerabilities. It also protects the security controls and ensures only authorized access as per rule set.

Penetration testing is essential because:

- Check the infrastructure before the hacker attacks the infrastructure.
- Evaluate the efficiency of network security devices such as firewalls, routers, and Web servers
- To ensure the applications, products are not released with Vulnerabilities

In addition to this, Penetration Testing should be performed once in a year by a third party or whenever:

- Security system discovers new threats by attackers.
- Upgradation to the new system or install new software or set up a new end-user program/policy
- Any system or software before it is deployed to production.

6.7 Process of Penetration Testing

- Planning & Preparation: Planning and preparation starts with defining the goals and objectives of the penetration testing. Penetration testing has been assigned to IS Team/ Project Team and/or an external party. The broad sets of responsibilities are as defined in Table –Section" Vulnerability Assessment and Penetration Testing Process."
- **Reconnaissance:** Reconnaissance includes an Assessment of the preliminary information and obtain a complete and detailed information of the systems.

- Discovery: use automated tools to scan target assets for discovering vulnerabilities.

  - Network Discovery: Such as discovery of additional systems, servers, and other devices (core servers, domain controllers, e-mail platforms, ERP, and ERM systems, etc.)
  - Host Discovery: It discovers open ports on these devices
  - Service Running: It probes ports to discover actual services which are running on them.

- **Analyzing Information and Risks:** Analyzes and assesses the information gathered before the test steps for dynamically penetrating the system. Based on the Information and risk assessment, assess the following points.
  - The defined goals of the penetration test
  - The potential risks to the system

- **Active Intrusion Attempts**: This is the most important step that must be performed with due care. This step must be performed when a verification of potential vulnerabilities is needed.

- **Final Assessment**: This step primarily considers all the steps conducted (discussed above) till that time and an evaluation of the vulnerabilities present in the form of potential risks.

- **Report Preparation**: Report preparation must start with overall testing procedures, followed by an Assessment of vulnerabilities and risks. The high risks and critical vulnerabilities must have priorities and then followed by the lower order.

6.8 Phases of Penetration Testing Methodology

- Before proceeding to the phases, all parties should be aware of the scope, types of testing (internal or external), rules of engagement, documentation, success criteria, review of past threats and vulnerabilities, awareness and education, tools to be used and avoid scan on security appliances.
- The phases of Penetration testing methodology are divided in three steps:

Pre- Attack Phase

- Information gathering of all the Physical and logical infrastructure of the organization, Analog connections including phone lines, fax lines, dialup lines, and other out-of-band connectivity, other information that has the potential to result in a possible exploitation.

Passive Reconnaissance

- Finding the directory structures of Web servers and services
- Gathering competitive intelligence over social media.
- Social engineering about the Infrastructure.

Active Reconnaissance

- **Network mapping**: Find the network architecture through server domain or by directory structure.
- **Perimeter mapping**: Traceroute the Network gateway to define the outer network layer and switches, routers and firewall configuration.
- **System and service identification through port scans**: identify live systems and IP addresses, port states (open, closed, or filtered), protocols used (routing or tunneled), active services and service types, OS fingerprinting, version identification, internal IP addressing, etc.
- **Web profiling**: All Web-based forms, types of user input, and form-submission destinations, comments field etc.

6.9 Attack Phase

Compromise the target system, by using various tools and techniques to exploit the logical and physical vulnerabilities exposed in the pre- attack phase.

- **Network security**: Penetration testers should check for the following things to secure a network:
  - Testing for Port scanning
  - Testing for System Identification
  - Testing for Services Identification
  - Testing for Application testing and code review
  - Testing for Router Configuration
  - Testing for Firewall Configuration
  - Testing for IDS Configuration
  - Testing for Password Cracking
  - Testing for DoS and DDoS

- **Wireless security**: Penetration testers should check for the following things to secure a Wireless network:
  - Testing for AP SSID, radio configuration, encryption-type, rate, mode of operation, VLAN, rf-mgmt, etc.
  - Privacy review

- **Application security**

Penetration testers should check for the following things to secure an Application architecture:

- Testing for SSL/TLS
- Input validation
- Testing for buffer overflow
- Test for Hidden fields and sensitive information
- Testing for file extensions
- Testing for HTTP methods

- Testing for Business Logic
- Testing for the business logic of the application
- Testing for Cross-site scripting (XSS)
- Testing for SQL injection
- Authentication Testing
- Credentials transport over an encrypted channel- Check for SSL(https)
- Testing for Guessable User Account
- Brute Force Testing
- Testing for bypassing authentication schema
- Testing for vulnerable remember password and password reset
- Testing for Logout and Browser Cache Management
- Testing for backdoors
- Testing Multiple Factors Authentication
- Authorization Testing
- Testing for bypassing authorization CAPTCHA schema
- Testing for Privilege Escalation
- Testing for Session Management
- Testing for Session Management Schema
- Testing for Cookies attributes- http only, secure and time validity
- Testing for Session Fixation
- Testing for CSRF

- **Physical security**

Security of the organization against physical attacks shall be ensured by implementing the following procedures:

- Access-controls testing
- Perimeter review
- Monitoring review
- Alarm-response testing
- Location review

- Environment review

- **Social engineering**

Security of the organization against social-engineering attacks may be ensured by:

- Request testing
- Guided suggestion testing
- Trust testing

6.1 Post Attack Phase

- Removing all files uploaded to the system
- Cleaning all registry entries and removing any vulnerabilities created
- Reversing all file and settings manipulations done during the test
- Reversing all changes in privileges and user settings
- Removing all tools and exploits from the tested systems
- Restoring the network to the pretest stage by removing shares
- Mapping the network state

6.10 Post Attack Phase

- Thorough investigation and validation of the entire test results
- Documentation and Reporting of all the test finding and a mitigation plan.
- Mitigation plan which holds suggestion for remediation of identified vulnerabilities and exploits.
- Final report is confidential hence the report will be delivered only to authorized people.

6.11 Specific Risk of VAPT

- Technical Risk: Some of the major technical risks are Failure of the target system or interconnected system, Disruptions of Service, Reduced Performance, Modification or Contamination of data and disclosure of data.

- Organizational Risk: Organizational risks like Unnecessary triggering incident handling process, disruption of business processes, loss of Reputation if third party are affected.
- Legal Risks: Chances of violating legal and contractual obligations and mistakably committing punishable acts.

6.12 Specific Risk of VAPT

- OWASP Testing Guide
- National Vulnerability Database (NVD)
- Common Vulnerability Scoring System (CVSS)
- Common Vulnerabilities and Exposure (CVE)

6.13 List of Tools for Vulnerability Assessment and penetration Testing

Sl. No.	Name	License	Platform
1	Burp suite	Commercial/Free Limited Function	Windows/Linux/Mac
2	Nessus Pro	Commercial/Free Limited Function	Windows/Linux

7. Exit Criteria and Output

- VAPT Report
- Remediation Plan and Closure report

8. Roles and Responsibilities

Roles	Responsibilities	External/Internal
IS Operations /Cloud Service Customer/Product Security Team	• To provide all the IT infrastructure details related to design, implementation and operation of the Trianz network. • Perform VA for All IT security & Trianz critical devices	Internal

	• Remediate the identified vulnerabilities as per the VA Report • Conduct VA as per the Trianz Vulnerability Management policy once in three months/ Based on the Project requirements and • PT for critical systems, once in a year	
External Party	• Conduct penetration testing	External
Internal Apps Team/Delivery Teams	• To provide all the Internal and external application details related to design, implementation and operation of the Trianz Applications, Client Applications (wherever applicable) to IS & InfoSec team • Remediate the identified vulnerabilities as per the VAPT Report	Internal
InfoSec & Dataprivacy Assurance Team	• Review the VAPT scan report • Track the closure report	Internal
CIO/CISO	• Review and approve the final VAPT report.	Internal

9. Prerequisites

9.1 Resource

- VAPT Tools

9.2 Training

- VAPT assessment Training

9.3 Reference Policy, Process, Procedure, Templates, Checklist

- Vulnerability Management and Penetration Testing Policy
- Network Security Management Procedure
- Prevention and Detection of Malicious attack Procedure
- Risk and Opportunity Management Procedure
- Anti-Malware Policy

9.4 Acronyms/Abbreviations

Acronym/Abbreviation	Expansion
VA/PT	**Vulnerability Assessment/Penetration Test**
OEM	**Original Equipment Manufacturer**
SANS	**SysAdmin, Audit, Network and Security**
OWASP	**Open Web Application Security Project**
NVD	**National Vulnerability Database**
CVSS	**Common Vulnerability Scoring System**
MPLS	**Multi-Protocol Label Switching**
VLAN.	**Virtual local area networks**
IDS	**Intrusion Detection System**
IPS	**Intrusion Prevention System**
UTM	**Unified Threat Management**
OS	**Operating System**
CVE	**Common Vulnerabilities and Exposure**
CIO/CISO	**Chief Information Officer/Chief Information Security Officer**
ERP	**Enterprise Resource Planning**
ERM	**Enterprise Risk Management**
FTP	File Transfer Protocol
DoS and DDoS	**Denial of Service and Distributed Denial of Service**
AP SSID	Access Point, Service Set IDentifier
SSL/TLS	Secure Sockets Layer /Transport Layer Security
HTTP	HyperText Transfer Protocol
XSS	Cross site scripting (XSS) is a common attack vector that injects malicious code into a vulnerable web application
SQLi	Structured Query Language, injection

CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
CSRF	Cross Site Request Forgery

10. Measurement

Refer to VAPT reports

11. Standards Addressed

ISO 27001:2022

ISO 27701:2019

12.ISO Control Mapping(s)

Category of Control	**ISO 27001:2022 Control**	**Document Name as per ISO 27001:2022**
Technological	8.8 Management of technical vulnerabilities Control Information about technical vulnerabilities of information systerns in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken.	Vulnerability Assessment and Penetration Testing Procedure

For Trianz Process Improvement Group (TPIG) Purpose Only

Version History

Ver. No.	Author	Reviewer	Approver	Date	Reason for Change	Change Description
0.00	Jyotessh G Nair			19-Feb07	Initial Draft	None
1.00	Jyotessh G Nair			26-Feb-07	Baseline is approved by Zulfikar Deen	Approved Baseline.
1.01	Bharateesha B R			24-Feb-09	New Asset Management Framework	Formatted the document to incorporate the new asset management framework
1.02	Bharateesha B R			11- Mar-09	New Asset Management Framework	Included Records in the scope of section Labeling Of Information – Soft Copy. Made changes to the Guidelines for each classification.
2.00	Balu Nair			28-Apr-09	Approved for Baseline	Baselined
2.01	Bharateesha B R			23-June-09	2nd Surveillance audit	Removed “Hard Copy” for the control area “ Labeling of Information (documents and Records – soft copy) Changed the point 3 of the guidelines for control area “Dispatch and Distribution of

						Information (Electronic Mail) for the classification " Confidential"
3.00	Bharateesha B R			23-June-09	Approval for Baseline	Baselined
3.01	Chakravarthi			30-Dec-10	QMG review	Formatted entire document
4.00	Chakravarthi			31-Dec-10	Request for approval	Baselined
4.01	Srilakshmi			24-May-11	QMG Review	Modified release id in header and cover page
5.00	Srilakshmi			24-May-11	Approval for Baseline	Baselined
5.01	Sudharsana			3-Aug-11	QMG review	Replace Owner with Management Representative in place of CIO Removed Retention period in Document Classification scheme section
6.00	Sudharsana			3-Aug-11	Request for Approval	Approved and Base lined
7.00	Balu Nair			08-Nov-12	Standardization of Blue Book Process Assets	Modified the template format Changed the Logo

7.01	Paramita Ghosh and Balu Nair			25-Jan-16	Client Audit and alignment with shared assessment checklist.	Handling of information based on the type of Information Asset Classification. Updated control areas to include below points
						Added identification of data owners, criteria of accessing the data based on confidentiality, labelling mechanism for the sensitive documents, validation of data classification which needs to be verified on a periodic basis, data retention period based on regulatory, sensitivity and information, appropriate encryption methodologies for data in transit and documentation of securely disposal of data All the confidential/sensitive data shall be encrypted. data. Added separate "REFERENCES" sections
8.00	Balu Nair			08-Feb-16	Approved by Mahesh (CISO)	Baselined

8.1	Karthik N			3-Jan-22	For Review	Migrated to new template
9.0	Karthik N	Siva N	Siva N	3-Jan-22	For Approval	Approved and Baselined
9.0	Kruti	Vijaya		3-June-24	Annual Review	No Changes
9.1	Vijaya	Balu		28-May-25	For Annual Review	Migrated to a new template
10.0	Vijaya	Balu	Srikanth M	29-May-25	For Approval	Approved and Baselined

TRIANZ℠

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com