Information Technology Vulnerability Assessment and Penetration Testing Policy

Control Information

Version	Drafting	Review	Approval
1.0	Mr. Bijay Kumar Swain B.Com, MCA, LLM, CISA, PMP Information System Auditor	Department of Information Technology Balasore Bhadrak Central Co-operative Bank Ltd.	Board of Directors Balasore Bhadrak Central Co-operative Bank Ltd.

Change Control

Version	Change	Date	Comments
1.0	First Draft	16-08-2024	Submitted 12-08-2024 Reviewed 14-08-2024 Approved 16-08-2024

1. Introduction

Purpose

The purpose of this Vulnerability Assessment and Penetration Testing (VAPT) Policy is to define the process and responsibilities for identifying, assessing, and mitigating vulnerabilities within the organisation's information systems, networks, and applications. This policy is crucial to ensure that security weaknesses are identified and addressed before they can be exploited by malicious actors, thereby protecting the organisation's assets, data, and reputation.

Scope

This policy applies to all organisational assets, including but not limited to information systems, networks, applications, cloud services, and any other related services. The policy is applicable to all internal staff, contractors, and third-party vendors involved in the VAPT process.

Audience

This policy is intended for all members of the IT and security teams, system and application owners, management, and any third-party vendors who may be involved in the VAPT process. It is essential for anyone responsible for maintaining the security posture of the organisation's assets.

2. Objectives

Identify Vulnerabilities

The primary objective of this policy is to systematically identify vulnerabilities across the organisation's IT infrastructure. This includes discovering weaknesses in systems, networks, and applications that could be exploited by unauthorised parties.

Assess Security Posture

The policy aims to provide a clear understanding of the current security posture of the organisation by assessing the severity of identified vulnerabilities and determining the associated risks.

Improve Security

Based on the findings from VAPT activities, the organisation aims to strengthen its defences by implementing appropriate remediation measures. Continuous improvement in security practices is a key objective.

Compliance

The policy ensures that the organisation remains compliant with relevant security standards, regulations, and industry best practices, thereby minimizing legal and financial risks.

3. Definitions and Terms

- **Vulnerability**: A flaw or weakness in a system, network, or application that can be exploited by a threat actor to gain unauthorised access or cause harm.
- **Penetration Testing**: A simulated cyberattack conducted by security professionals to identify and exploit vulnerabilities in systems, networks, or applications to understand the impact of potential threats.
- **Threat**: Any circumstance or event with the potential to adversely impact organisational operations, assets, or individuals by exploiting vulnerabilities.
- **Risk**: The potential for loss or damage to an asset, calculated as a function of the likelihood of a threat exploiting a vulnerability and the resulting impact.
- **Asset**: Any resource, process, product, or component that has value to the organisation and requires protection.
- **CVE:** The Common Vulnerabilities and Exposures (CVE) system provides a reference-method for publicly known information-security vulnerabilities and exposures.

4. Roles and Responsibilities

VAPT Team

- **Composition**: The VAPT team is composed of cybersecurity experts with experience in vulnerability assessment and penetration testing.
- **Responsibilities**:
  - Conduct VAPT activities as per the defined scope and methodology.
  - Report findings in a clear, actionable manner.
  - Maintain confidentiality of all information discovered during testing.
  - Provide guidance on remediation of identified vulnerabilities.

Management

- **Responsibilities**:
  - Approve the VAPT policy and ensure that it is implemented.
  - Oversee the allocation of resources required for VAPT activities.
  - Review and approve the final VAPT reports.
  - Ensure that remediation actions are prioritised and implemented.

System Owners

- **Responsibilities**:
  - Facilitate access to systems, networks, and applications within the scope of VAPT.
  - Work with the VAPT team to understand identified vulnerabilities.
  - Implement recommended remediation actions in a timely manner.

Third-Party Vendors

- **Responsibilities**:
  - Adhere to the organisation's VAPT policy when conducting testing.
  - Ensure all testing activities are authorised and within the defined scope.
  - Sign a Non- Disclosure Agreement.
  - Maintain the confidentiality of all data accessed during VAPT activities.

5. VAPT Process Overview

Pre-Engagement

- **Scope Definition**: Clearly define the scope of the VAPT, including the systems, networks, and applications to be tested. Obtain necessary approvals and legal agreements.
- **Risk Assessment**: Conduct a preliminary risk assessment to understand potential impacts and prepare for any contingencies.
- **Authorisation**: A written permission by management to conduct VAPT.

Assessment Phase I

- **Vulnerability Scanning**: Use automated tools to scan for known vulnerabilities across in-scope assets.

- **Penetration Testing**: Conduct manual testing to identify and exploit vulnerabilities that automated tools may miss. Testing should be conducted with care to avoid disruption of services.
- **Exploitation**: If vulnerabilities are identified, attempt to exploit them to understand their impact. This helps in determining the real-world risk associated with the vulnerability.

Intermediate Report Submission:

- **Report all vulnerabilities discovered.**

Assessment Phase II

- **Revalidation Test**: Retesting all the vulnerabilities discovered in Phase I, post application of patches.

Final Reporting

- **Documentation**: Document all findings in a structured report. Include details of each vulnerability, its risk level, and recommended remediation.
- **Risk Levels**: Categorize findings based on severity (e.g., Low, Medium, High, Critical).
- **Recommendations**: Provide clear, actionable recommendations for mitigating identified vulnerabilities.
- **Report Acceptance**: IT Team to discuss the report with VAPT Team and Accept the Report.

Post-Engagement

- **Retesting**: After remediation, conduct a follow-up test to ensure that vulnerabilities have been successfully addressed.
- **Debriefing**: Hold a debriefing session with relevant stakeholders to discuss findings, remediation efforts, and lessons learned.
- **Knowledge Sharing**: Share insights gained during VAPT activities with the broader security team to enhance overall security practices.

6. Scope of Testing

In-Scope Assets

- **Systems**: All critical systems including servers, databases, and storage systems.

- **Networks**: Internal and external networks, including firewalls, routers, and switches.
- **Applications**: Web, mobile and thick client applications.
- **Cloud Services**: Public, private, and hybrid cloud environments.
- **IoT Devices**: Any Internet of Things (IoT) devices used within the organisation.
- **OT Systems**: Operational technology systems used in industrial control processes.

Out-of-Scope Assets

- **Legacy Systems**: Certain legacy systems may be excluded if testing poses a risk of disruption.
- **Third-Party Systems**: Systems managed by third parties, unless explicitly authorised.

Testing Frequency

- **Critical Systems**: Quarterly testing.
- **Non-Critical Systems**: Semi-annual testing.
- **New Systems**: Testing before deployment into production.

Depth of Testing

- **Full Network**: Comprehensive testing of all in-scope networks.
- **Application-Specific**: Targeted testing on high-risk applications.

7. Risk Assessment and Categorisation

Risk Levels

- **Low**: Minor vulnerabilities that pose little risk and can be addressed during regular maintenance.
- **Medium**: Vulnerabilities that could lead to unauthorised access or data leakage but are difficult to exploit.
- **High**: Vulnerabilities that could result in significant impact, such as data breaches or system compromise.
- **Critical**: Vulnerabilities that could cause catastrophic damage to the organisation, requiring immediate attention.

Risk Assessment Matrix

Likelihood	Impact	Risk Level
Low	Low	Low
Low	Medium	Medium
Low	High	High
Medium	Low	Medium
Medium	Medium	High
Medium	High	Critical
High	Low	High
High	Medium	Critical
High	High	Critical

Impact Analysis

- **Business Impact**: Consider the potential loss of revenue, reputation damage, and regulatory penalties.
- **Operational Impact**: Assess the potential disruption to operations, including downtime and productivity loss.

Risk Mitigation

- **Immediate Actions**: Address critical vulnerabilities immediately. (CVSS Score 7.0-10.0 within 30 days)
- **Scheduled Remediation**: Plan and prioritize remediation of high and medium-risk vulnerabilities. (CVSS Score 4.0-6.9 within 120 days)
- **Monitoring**: Implement continuous monitoring for low-risk vulnerabilities.

8. Legal and Compliance Considerations

Legal Requirements

- **Data Protection Laws**: Ensure VAPT activities comply with data protection regulations such as DPDP, IT Act, etc.
- **Authorisation**: Obtain written authorisation before conducting VAPT activities to avoid legal repercussions.

Compliance Standards

- **ISO 27001**: Align VAPT processes with the ISO 27001 standard for information security management.

- **PCI-DSS**: Ensure compliance with the Payment Card Industry Data Security Standard (PCI-DSS) for any systems processing payment information.

Data Privacy

- **Data Handling**: Ensure that all data accessed during VAPT activities is handled securely and in accordance with privacy regulations.
- **Confidentiality Agreements**: Require all personnel involved in VAPT to sign confidentiality agreements.

Third-Party Agreements

- **Contracts**: Include specific clauses in contracts with third-party vendors regarding the scope, confidentiality, and reporting of VAPT activities.
- **Liability**: Define liability in case of data breaches or disruptions caused by VAPT activities.

9. VAPT Tools and Methodologies

Tools

- **Nessus**: Used for vulnerability scanning across networks and systems.
- **Burp Suite**: Employed for web application security testing.
- **Metasploit**: Used for penetration testing and exploiting vulnerabilities.
- **Wireshark**: Network protocol analyzer used to capture and analyze network traffic.
- **OWASP ZAP**: An open-source tool for finding vulnerabilities in web applications.
- Any other tool approved by the IT Team.

Methodologies

- **OWASP**: Follow the Open Web Application Security Project (OWASP) methodology for web application security.
- **NIST SP 800-115**: Adhere to the NIST Special Publication 800-115 for technical guide to information security testing and assessment.

- **Custom Frameworks**: Use custom-built frameworks for specific environments where standard methodologies may not apply.

Tool Selection Criteria

- **Relevance**: Choose tools that are relevant to the specific systems or applications under test.
- **Accuracy**: Ensure the tools are known for high accuracy in identifying vulnerabilities.
- **Ease of Use**: Prefer tools that integrate well with the organisation's existing security infrastructure.

Custom Scripts

- **In-House Development**: Develop custom scripts to address specific testing needs or to automate repetitive tasks.

10. Reporting and Documentation

Report Structure

- **Executive Summary**: Provide an overview of the testing process, key findings, and overall security posture.
- **Detailed Findings**: Document each vulnerability, including the location, description, impact, and risk level.
- **Risk Levels in Reports**: Categorize vulnerabilities by their risk level (Low, Medium, High, Critical) and explain the criteria used.
- **Actionable Recommendations**: Provide specific, actionable recommendations for each vulnerability, prioritizing critical and high-risk issues.

Distribution

- **Report Recipients**: Distribute the final report to relevant stakeholders, including system owners, management, and the security team.
- **Secure Distribution**: Ensure that reports are distributed securely, using encryption and access controls to prevent unauthorised access.

11. Remediation and Follow-Up

Remediation Planning

- **Prioritisation**: Develop a remediation plan that prioritizes vulnerabilities based on their risk level and potential impact.
- **Resource Allocation**: Ensure that adequate resources are allocated to address the identified vulnerabilities.

Tracking

- **Progress Tracking**: Use a tracking system to monitor the progress of remediation efforts.
- **Accountability**: Assign responsibility for each remediation task to ensure accountability.

Retesting

- **Validation**: Conduct retesting to validate that vulnerabilities have been successfully remediated and no new issues have been introduced.
- **Documentation**: Update the documentation to reflect the results of the retesting and any additional findings.

Validation

- **Independent Review**: Consider an independent review of the remediation efforts to ensure that all vulnerabilities have been adequately addressed.
- **Final Report**: Provide a final report on the status of remediation, including any remaining vulnerabilities and recommendations for ongoing monitoring.

12. Policy Review and Updates

Exceptions: Exceptions to this policy will be handled in accordance with the IT & IS Policy.

Review Frequency

- **Annual Review**: Conduct a formal review of this policy at least once a year to ensure it remains current and effective.
- **Trigger-Based Review**: Perform additional reviews if there are significant changes to the IT environment, legal requirements, or threat landscape.

Change Control

- **Approval Process**: Implement a change control process for approving updates to the policy. Changes must be reviewed and approved by senior management.

- **Stakeholder Involvement**: Involve relevant stakeholders in the review process to ensure that all perspectives are considered.

Versioning

- **Version Control**: Maintain a version control system to track changes to the policy. Include a version history in the document, noting the date of each change and a brief description of what was updated.

Appendices

Acronyms

- **VAPT**: Vulnerability Assessment and Penetration Testing
- **OWASP**: Open Web Application Security Project
- **NIST**: National Institute of Standards and Technology
- **ISO**: International Organisation for Standardisation
- **PCI-DSS**: Payment Card Industry Data Security Standard

References

- **ISO 27001**: Information Security Management System (ISMS) Standard
- **NIST SP 800-115**: Technical Guide to Information Security Testing and Assessment
- **OWASP Top 10**: List of the most critical security risks to web applications

Templates

- **VAPT Scope Template**: A template to define the scope of VAPT activities, including in-scope and out-of-scope assets.

Reporting Template: A standardised template for documenting and reporting VAPT findings, including risk levels and recommendations.