SECURITY VULNERABILITY TESTING SERVICE

EXECUTIVE SUMMARY

Security vulnerabilities are found in most systems, such as acquired systems and developed systems, due to the lack of patches, lack of security settings, lack of security coding, and lack of change management.

Therefore, most of the international standards or certification standards for security management system specifies periodic security vulnerability check as one of the essential requirements.

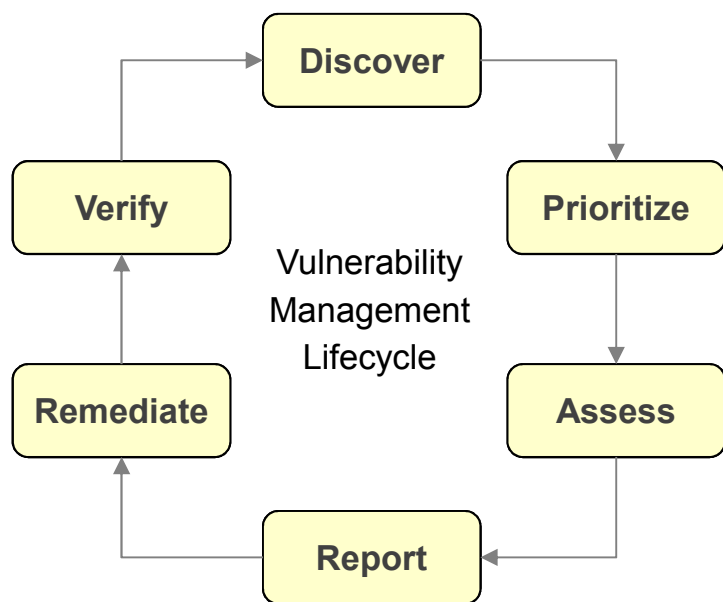Once the Security Vulnerability Test is completed, You will achieve the following goals:

- Identify where, and what information systems are present through information assets surveys
- Recognizing how many security vulnerabilities exist in which information systems
- Analyzing how dangerous a vulnerability is, and which vulnerability is important
- Selecting various methods to remedy found security vulnerabilities
- Enhancement of self-competence for periodic security vulnerability checks

Related international standards and regulations
- ISO/IEC 27002:2013 : A12.6 Technical Vulnerability Management
- PCI-DSS v3.2 Requirement 11.2 : External and Internal Network Vulnerability Scans
- EU GDPR Regulation: Article 32 Security of Processing
- Rwanda RURA Regulation: Article 21 Vulnerability Assessment (on all the plane twice a year)
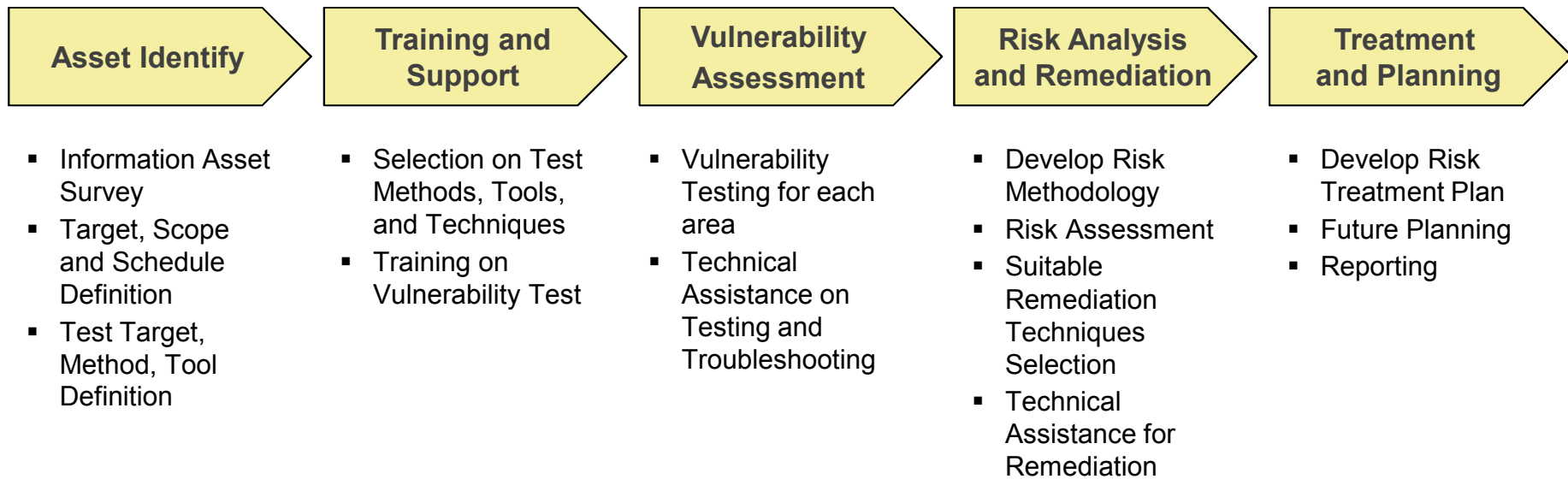
wiki

SERVICE STRATEGY

In order to achieve the ultimate goal of security vulnerability review, Vulnerability Management Lifecycle, which identifies existing information assets, prioritizes priorities, identifies existing vulnerabilities, analyzes them, measures them, It is necessary to consider all activities from the perspective.

- Providing all activities from technical to Managerial parts of Vulnerability Management Lifecycle
- Testing the Security Vulnerability Using the Updated Database with All the Latest Vulnerability Information
- Using Globally Verified Dedicated Vulnerability Testing Tool by Each Type of the System
- Professional Training for Practitioners to Build Self-vulnerability Test Capability
- Providing Technical Assistance Service for Risk Assessment and Treatment Base on Various Case-studies
- Providing related managerial policies, procedure, and standards of Vulnerability Management System

METHODOLOGY

Vulnerability Testing consists of 5 phases from Asset Identify to Treatment and Planning. Depending on the Target of Vulnerability Test, many testing techniques are used in the detailed steps of each phase.

Asset Identify	Training and Support	Vulnerability Assessment	Risk Analysis and Remediation	Treatment and Planning

- Information Asset Survey
- Target, Scope and Schedule Definition
- Test Target, Method, Tool Definition

- Selection on Test Methods, Tools, and Techniques
- Training on Vulnerability Test

- Vulnerability Testing for each area
- Technical Assistance on Testing and Troubleshooting

- Develop Risk Methodology
- Risk Assessment
- Suitable Remediation Techniques Selection
- Technical Assistance for Remediation

- Develop Risk Treatment Plan
- Future Planning
- Reporting

Types of Vulnerability Test Service

SC-NW	Network Vulnerability Test
SC-SS	Security System Vulnerability Test
SC-SV	Server/Web/Was System Vulnerability Test
SC-DB	Database Vulnerability Test
SC-PC	Person Computer Vulnerability Test
SC-AP	Application(Web, Mobile) Vulnerability Test

SC-CR	Application Source Code Review
SC-WR	Wireless Vulnerability Test
SC-PV	Personal Data Vulnerability Test
SC-US	Unmanned System Vulnerability Test
SC-SP	Specific Theme Vulnerability Test

WIKI

CASES

- **Client**: SK Group Company
- **Vulnerability Test Type**: Web Application/Mobile APP Source Code Review
- **Testing target**:
  Internal and external Web applications and Mobile APP on operating(by automated tools and manual test)

- **Testing Techniques**:
  - Dedicated automatic testing tools to match the type of information system
  - Manual testing of professional consultants

- **Testing Results**:
  Many vulnerabilities related to patches were found in security vulnerability testing using automation tools, but most security vulnerabilities related to business logic were found through manual testing rather than tools.

- **Peculiar Things**
  - Cross-checking with dynamic analysis of professional engineers based on static analysis results using automated testing tools
  - In the dynamic analysis of expert engineers, more security vulnerabilities with higher severity has been found.