Datasheet

IT Infrastructure Security Audit Service
(IT ISAS)

viettel security

Necessity of IT Infrastructure Security Audit

The fourth industrial revolution has brought about a great development of information technology, as a result, people increasingly depend on Information Technology (IT) software because every individual or organization needs to own and operate information systems (ICT) to run business activities, financial transactions, data analysis or other important operations, etc.

All information systems for production and business are built on IT infrastructure including network and security equipment, servers and terminals (user computers, printers, ...) and are always connected to the Internet to provide global service level.

Early detection of risks and vulnerabilities of the IT infrastructure will help the organization come up with a timely remedial plan, minimizing the risk of information security encountered in the operation and exploitation of information systems to help the organization devise a strategy to improve information system quality.

Viettel IT Infrastructure Security Audit Service

IT Infrastructure Security Audit service allows:

- Detecting problems that do not ensure information security in network planning and design.
- Identifying security weaknesses in device & system configuration.
- Scanning for vulnerabilities that exist in devices & systems.
- Evaluating the policy connected among system components.
- Conducting report on the risk and severity of information security problems.
- Providing remedial recommendations for problems identified during the audit.

Components in the system under the scope of implementation include:

- Network system design planning
- Connection policy on secure devices
- Security equipment, network equipment
- Server OS
- End-user computer operating system
- ADDS (Active Directory Domain Services) system
- Email System

Highlights

Network Infrastructure Assessment

- Security architecture assessment: ensuring availability and segregation of security levels of network areas.
- Security firewall policy assessment: Connecting in/out the Internet and partners, safely managing between network areas with different security levels.
- Information security assessment of network devices and security devices: scanning and detecting vulnerabilities of firmware versions; configure authentication, authorization, secure remote administration; logging and monitoring; time synchronization.

Security Assessment of Server OS & User Computer

- Vulnerabilities scan in operating system version.
- Status, patch installation update.
- Policies and operations of user accounts.
- Remote access configuration.
- Soft firewall policy.
- Logging, time synchronization configuration
- Other security configurations.

Assessment of Firmware Vulnerabilities on Devices & Server OS

- Scan for firmware vulnerabilities on devices & operating system with specialized tools.
- Assess the risks, the level of impact with the actual environment in the actual IT Infrastructure of the Client.

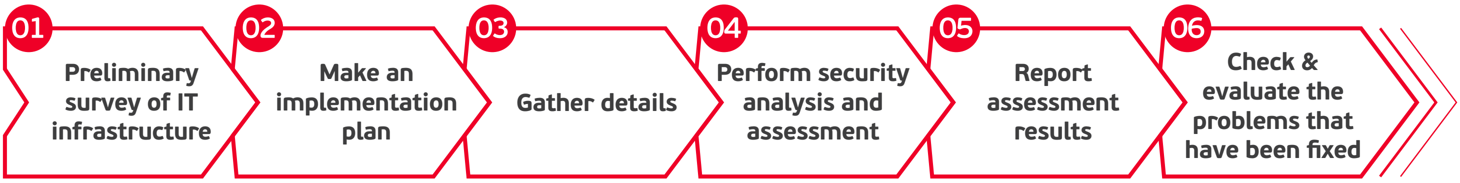
Security Assessment of Email Systems

- Email attack prevention:
  - Configure Email encryption for sending and receiving.
  - Configure Email anti-spoofing.
  - Configure Email anti-spam.
  - Configure anti-malware infection.
  - Configure password scanning protection.
- Assessments of preventing unauthorized access to the Email system:
  - Design a secure email system.
  - Secure an email server operating system.
  - Secure Mail Gateway device: scan for firmware version vulnerabilities; configure authentication, authorization, secure remote administration; logging and monitoring; time synchronization.

Security Assessment of Activedirectory Domain Services (Adds)

- Privilege Escalation Prevention:
  - Organize the user directory tree by Tier Model.
  - User account information.
  - Information about privileged groups.
  - Configure policy.
  - Configure Group Policy.
- Prevention of unauthorized access to the DC server:
  - Design safe ADDS system.
  - IT assessment of DC server operating system.

THE IT INFRASTRUCTURE SECURITY AUDIT PROCESS



01 Preliminary survey of IT infrastructure

02 Make an implementation plan

03 Gather details

04 Perform security analysis and assessment

05 Report assessment results

06 Check & evaluate the problems that have been fixed

1. Preliminary survey of IT infrastructure

- Communicate directly with customers.
- Collect preliminary information about IT infrastructure.

2. Make an implementation plan

- Scope & volume of equipment/systems to be performed.
- Content of performing specific assessments for devices/systems.
- Work coordination.
- Assessment method
- Asssessment conditions.
- Implementation timeframe.

3. Gather details

- Auditors collect equipment/systems directly.
- Interview to coordinate other necessary contents.
- Deploy specialized tools and perform scans.

Customers guarantee the conditions (connection, view accounts, deploying vulnerability scanning tools, etc.) which will be withdrawn after the evaluation process.

4. Perform security analysis and assessment

- Auditors conduct analysis and evaluation.
- Auditors can collect additional details.

5. Report assessment results

- Viettel provides the Information Security Assessment report of IT infrastructure with recommendations for customers to fix.

6. Check & evaluate the problems that have been fixed

- Customers handle and fix problems.
- The customer sends the corrected results back to Viettel.
- Viettel provides the second Information Security Assessment of IT Infrastructure.

The maximum time to conduct a re-assessment is within 45 days after Viettel submits the first Information Security Assessment report of the IT infrastructure. In case the customer's response time is more than 45 days, the evaluation will be carried out under the new contract.

BENEFITS

1. **Quick deployment time and cost effectiveness.**
2. **Comprehensive scanning and assessment of IT infrastructure of enterprises and organizations.**
3. **A team of leading experts with extensive experience in the field of information security.**
4. **Professional vulnerability scanning tools.**
5. **The assessment content is built on the key elements of international and domestic information security standards and guidelines such as:**
    - ISO/IEC 27001.
    - PCI DSS.
    - NIST SP800-53.
    - TCVN 11930:2017.
    - CIS Critical Security Controls and Benchmarks.
    - STIG - Security Technical Implementation Guides.