Course: Information Security Management in e-Governance

Day 3

Session 1: Information Security Audits

Agenda

- Need for information security audit and its objectives
- Categories of information security audit
- Scope of information security audit and expected outcomes
- Network security assessment
- Role of information security auditor

Security Audits - FAQ

- We already have firewalls in place. Isn't that enough?
- We did not realize we could get security audits. Can you really get security audits, just like financial audits?
- We have already had a security audit. Why do we need another one?

Answers

- Firewalls and other devices are simply tools to help provide security. They do not, by themselves, provide security.
- Using a castle as an analogy, think of firewalls and other such tools as simply the walls and watch towers. Without guards, reports, and policies and procedures in place, they provide little protection.
- Security audits, like financial audits should be performed on a regular basis.

Security Audit…

Business use of IT is involving more

- complex systems
- Networking
- Internet connectivity
- rapidly changing technology…..

Leads to

Ever increasing number of:

- gaps in the information security measures
- network & systems vulnerabilities
- hacking incidents…

Can be identified and addressed by

Testing/auditing security:

- periodically
- by validation of information security risks, mitigation measures, controls, polices and procedures in the organization
- Comparison with the industry best practices…

Audit forms an integral part of security monitoring processes

	Preventative	Detective
Physical	▪ locks and keys ▪ backup power ▪ biometric access controls ▪ site selection ▪ fire extinguishers	▪ motion detectors ▪ smoke and fire detectors ▪ CCTV monitors ▪ sensors and alarms
Technical	▪ authentication ▪ Firewalls & IPS ▪ anti-virus software ▪ encryption ▪ access control….. ▪ **Vulnerabilities assessment** ▪ **Diagnostic reviews…**	▪ audit trails ▪ intrusion detection ▪ **automated configuration monitoring** ▪ **penetration testing**
Administrative	▪ employment procedures ▪ supervision ▪ technical training ▪ separation of duties ▪ disaster recovery plans ▪ security awareness training ▪ **Diagnostic reviews…**	▪ security reviews and audits ▪ performance evaluations ▪ required vacations/rotation of duties ▪ **incident investigations**

Defining security audit

Security Audit :

- Identifying the information security risks to the organization and evaluation of Information security measures and effectiveness
- It is a systematic evaluation of the security of an organization Information systems by measuring how well it conforms to the best practices.
- an audit on the level of information security in an organization.
- auditing information security covers topics from auditing the physical security of data centers to the auditing logical security of databases and application..

Why do u need a Security Audit?

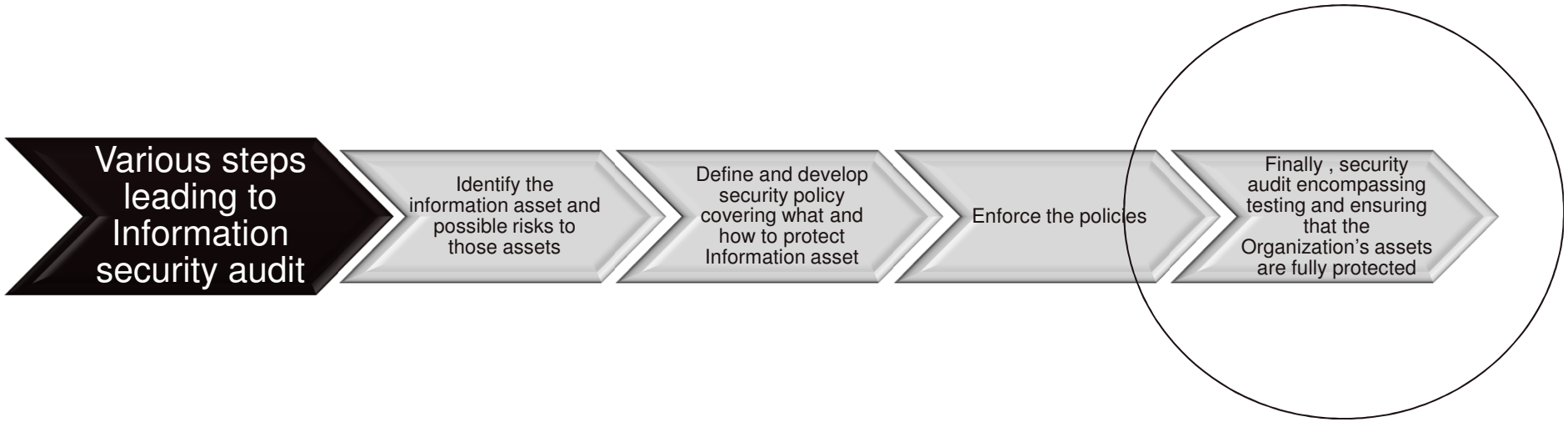
- Most businesses are connected to the Internet and have implemented measures (policies, systems) to protect themselves from unauthorised access/transactions
- IT can be at risk, even with all the right technology, if security policy and procedures are poorly implemented or outdated
- A few software vulnerabilities account for majority of successful attacks
- Hackers/attackers are opportunistic – taking the easiest and most convenient route.
- Hacking exploits the best-known flaws with the most effective and widely available attack tools
- It counts on organizations not fixing the problems, and they often attack indiscriminately, by scanning the Internet for vulnerable systems.

Need for IT Security Audit

- To ensure that the security is in order to ensure that organizations security systems and processes are working as intended
- To verify and ensure compliance with some the legislations and acts
- To identify the gaps in the existing defenses…

IT Security Audit – Where does it fall

Security audit is the final step in the implementation of an Organization's security defenses.



Types of Security Audit

External Audit Assessment

- Public information collection
- External Penetration
  - Non-destructive test
  - Destructive test

Internal Audit Assessment

- Confidential information collection
- Security policy reviewing
- Interviews
- Environment and Physical Security
- Internal Penetration
- Security and controls review of information systems and infrastructure

External Audit Assessment

- Hackers view of the network
- Simulate attacks from outside
- Point-in-time snapshots
- Can NEVER be 100%
- Ethical hacking
  - conducted to identify the gaps in the information security systems with a view to bridge these gaps for strengthening information security
  - Organizations get ethical hacking/external audit done through professional agencies to identify the gaps in the systems

External Audit-Public Information Gathering

This basically involves

- **Network Identification**
  - Identify IP addresses range owned/used by the organization/systems in target
- **Network Fingerprinting**
  - Try to map the network topology
  - Perimeter models identifications
- **OS & Application fingerprinting**
  - OS finger printing
  - Port scanning to define services and application
  - Banner grabbing

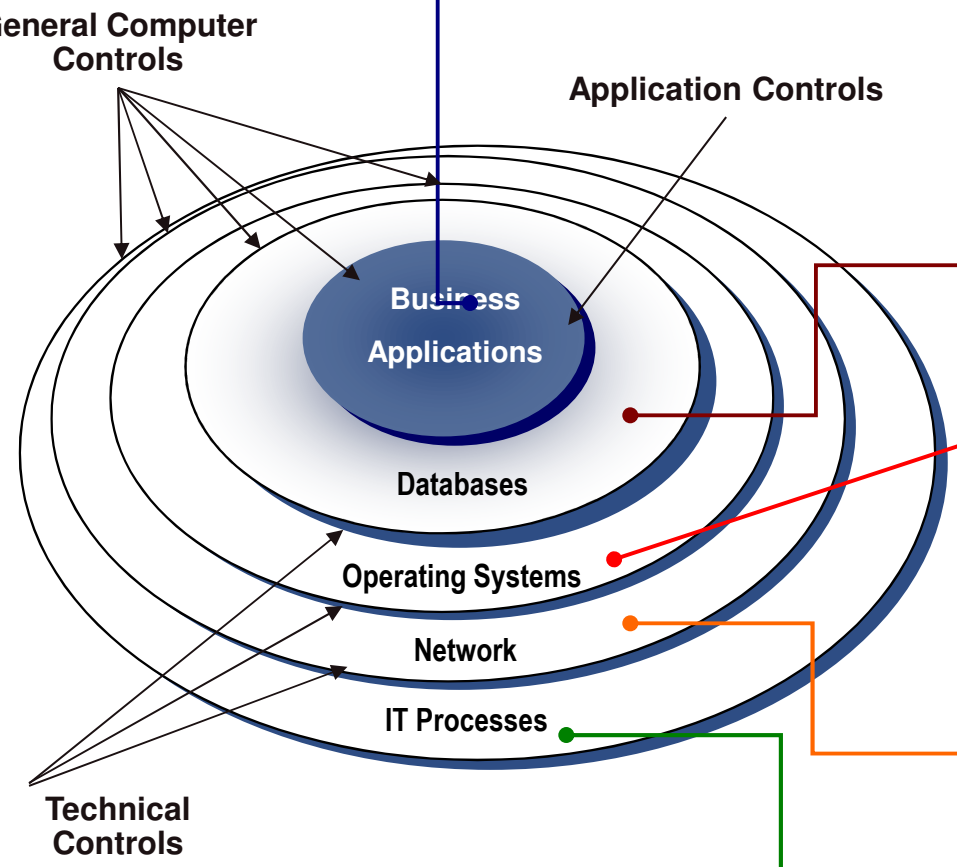
Internal Audit

- To assess the effectiveness of information security measures of the organization with a view to bridge the identified gaps
- Conducted at the premises
- A process of hacking with full knowledge of the network topology and other crucial information.
- Also to identify threats within the organization and surrounding the information systems

Focus of IT Security Audit (Illustrative)

- Information Security Policies and Procedures
- Information Security Architecture
- Business Applications
- Database systems and data sources
- Computing infrastructure (Servers, PCs..)
- Network infrastructure (Router, Switch, WAN, LAN, VPN..)
- Security Infrastructure (Firewall, IPS/IDS, Antivirus)
- Physical Security (physical access control systems to data center, end user environment i.e. bio-metric, CC TV..)
- Environmental controls (Power, cooling system, UPS etc)
- HR Awareness
- IT Systems Documentation

Security Audit Horizon…..



Business Applications for core and support functions of the Government

- Logical Access Controls
- Input/output Controls
- Configuration controls
- Procedural controls
- Audit trials

Databases supporting business applications

- Access Controls
- Data Integrity controls
- Configuration controls
- Audit & Accounting policies

Operating systems hosting business applications and databases

- User Management and Password policies
- Access Controls
- Accounting & Audit policies
- Service packs and security patches

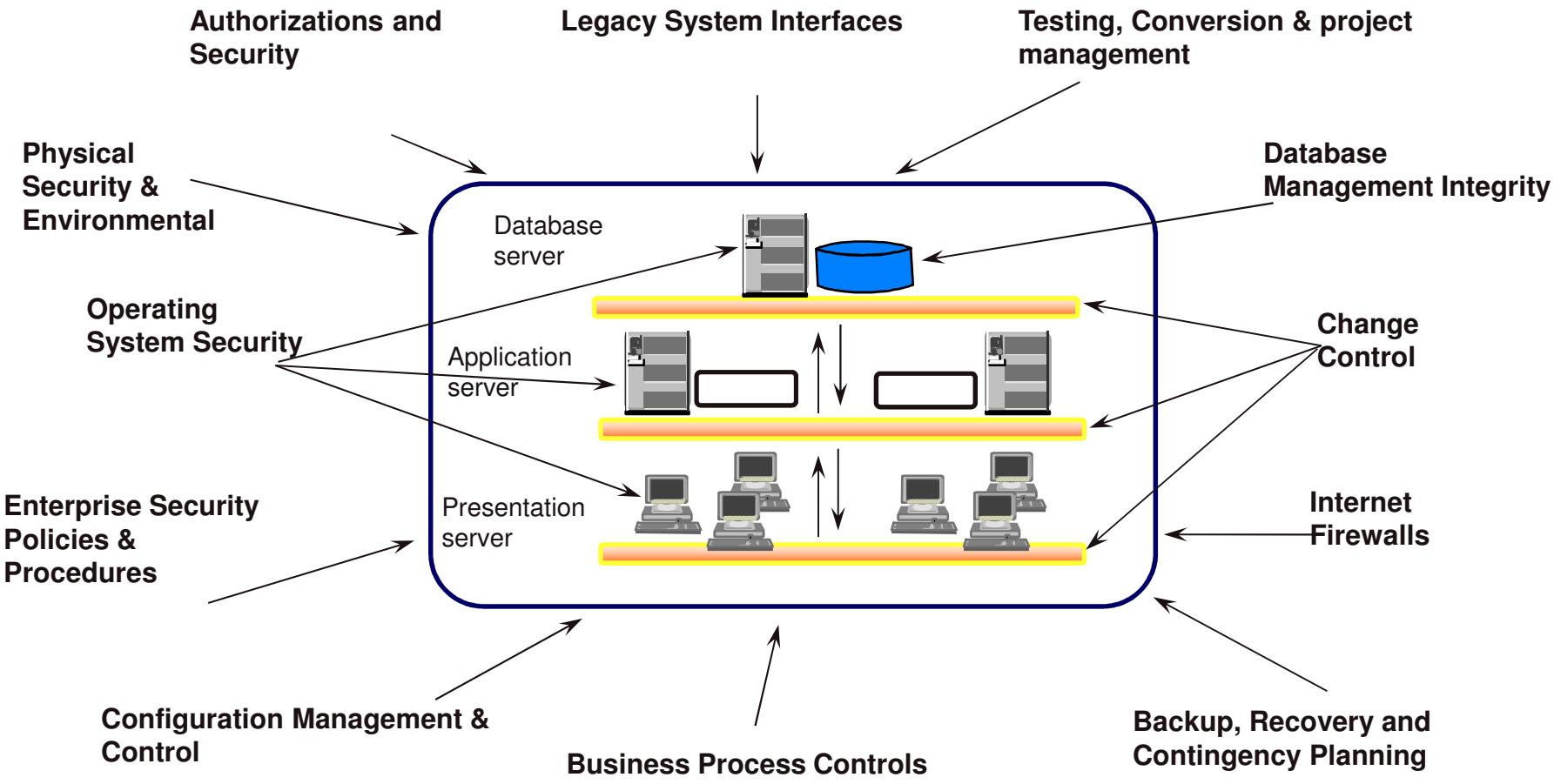
Network infrastructure comprising of LAN and Internet supporting administrative access

- Access controls
- Security policies
- Management and Monitoring controls

Architecture, Policy and Procedures

- Physical access Controls
- Environmental Controls
- Backup procedures
- Asset Management Processes
- Insurance Policies

Security Audit Horizon…..



What does IT Security Auditing involves..
Some standard techniques

IT security auditing to assess the security posture of systems and networks can include a combination of the following:

- Network Scanning
- Vulnerability Scanning
- Password Cracking
- Log Review
- Integrity Checkers
- Virus Detection
- Penetration Testing etc…

Network Scanning

- Involves using a port scanner to identify all hosts potentially connected to an organization's network, the network services operating on those hosts and specific application running the identified service.

- Provides a comprehensive list of all active hosts and services, printers, switches, and routers operating in the address space scanned by the port-scanning tool, i.e., any device that has a network address or is accessible to any other device.

- Port scanners first identify active hosts in the address range specified by the user using Transport Control Protocol/Internet Protocol (TCP/IP) Internet Control Message Protocol (ICMP) ECHO and ICMP ECHO_REPLY packets

Network Scanning (contd..)

Organizations should conduct Network scanning to

- Check for unauthorized hosts connected to the organization's network
- Identify vulnerable services
- Identify deviations from the allowed services defined in the organization's security policy
- Prepare for penetration testing
- Assist in the configuration of the intrusion detection system (IDS) and
- Collect forensics evidence.

Network Scanning (contd..)

The following corrective actions may be necessary as a result of network scanning:

- Investigate and disconnect unauthorized hosts,
- Disable or remove unnecessary and vulnerable services,
- Modify vulnerable hosts to restrict access to vulnerable services to a limited number of required hosts (e.g., host level firewall or TCP wrappers), and
- Modify enterprise firewalls to restrict outside access to known vulnerable services.

Vulnerability Scanning

- Vulnerability scanning identifies hosts and open ports, together with information on the associated vulnerabilities
- Different to port scanning as doesn't rely on human interpretation of the results
- Most vulnerability scanners also attempt to provide information on mitigating discovered vulnerabilities
- Vulnerability scanners provide system and network administrators with proactive tools that can be used to identify vulnerabilities before an adversary can find them
- A vulnerability scanner is a relatively fast and easy way to quantify an organization's exposure to surface vulnerabilities
- Vulnerability scanners can also help identify out-of-date software versions, applicable patches or system upgrades, and validate compliance with, or deviations from, the organization's security policy

Vulnerability Scanning (contd..)

Vulnerability scanners provide the following capabilities:

- Identifying active hosts on network
- Identifying active and vulnerable services (ports) on hosts.
- Identifying applications and banner grabbing.
- Identifying operating systems.
- Identifying vulnerabilities associated with discovered operating systems and applications.
- Identifying mis-configured settings.
- Testing compliance with host application usage/security policies.
- Establishing a foundation for penetration testing

Vulnerability Scanning (contd..)

The following corrective actions may be necessary as a result of vulnerability scanning:

- Upgrade or patch vulnerable systems to mitigate identified vulnerabilities as appropriate
- Deploy mitigating measures if the system cannot be immediately patched in order to minimize the probability of this system being compromised
- Improve configuration management program and procedures to ensure that systems are upgraded routinely
- Assign a staff member to monitor vulnerability alerts and mailing lists, examine their applicability to the organization's environment and initiate appropriate system changes
- Modify the organization's security policies, architecture, or other documentation to ensure that security practices include timely system updates and upgrades

Password Cracking

- Password cracking programs can be used to identify weak passwords.
- Password cracking verifies that users are employing sufficiently strong passwords.
- During a penetration test or a real attack, password cracking employs captured password hashes.
- Passwords hashes can be intercepted when they are transmitted across the network (using a network sniffer) or they can be retrieved from the targeted system.
- Once the hashes are obtained, an automated password cracker rapidly generates hashes until a match is found.

Log Reviews

- Various system logs can be used to identify deviations from the organization's security policy,
- Review focuses on firewall logs, IDS logs, server logs, and any other logs that are collecting audit data on systems and networks
- Log review and analysis can provide a dynamic picture of ongoing system activities that can be compared with the intent and content of the security policy.
- Essentially, audit logs can be used to validate that the system is operating according to policies.

Log Reviews (contd..)

The following actions can be taken if a system is not configured according to policies:

- Remove vulnerable services if they are not needed.
- Reconfigure the system as required to reduce the chance of compromise.
- Change firewall policy to limit access to the vulnerable system or service.
- Change firewall policy to limit accesses from the IP subnet that is the source of compromise.

Virus Detectors

- All organizations are at risk of “contracting” computer viruses, Trojans and worms if they are connected to the Internet, or use removable media (e.g., floppy disks and CD-ROMs), or use shareware/freeware software.

- The impact of a virus, Trojan, or worm can be as harmless as a pop-up message on a computer screen, or as destructive as deleting all the files on a hard drive.

- With any malicious code, there is also the risk of exposing or destroying sensitive or confidential information.

- Virus detectors support in identifying the existing virus programmes on the systems

Virus Detectors (contd..)

- The virus detector installed on the network infrastructure is usually installed on mail servers or in conjunction with firewalls at the network border of an organization.
- Server based virus detection programs can detect viruses before they enter the network or before users download their e-mail.
- The other type of virus detection software is installed on end-user machines.
- Software detects malicious code in e-mails, USB disks, hard disks, documents and the like but only for the local host
- The software also sometimes detects malicious code from web sites.
- This type of virus detection program has less impact on network performance but generally relies on end-users to update their signatures, a practice that is not always reliable.

Virus Detectors (contd..)

The following steps are recommended:

- Virus definition files should be updated at least weekly and whenever a major outbreak of a new virus occurs.
- The anti-virus software should be configured to run continuously in the background and use heuristics, if available to look for viruses.
- After the virus definition files are updated, a full system scan should be performed.

Penetration Testing

- Penetration testing is security testing in which evaluators attempt to circumvent the security features of a system based on their understanding of the system design and implementation.
- The purpose of penetration testing is to identify methods of gaining access to a system by using common tools and techniques used by attackers.
- However, it is a very labor-intensive activity and requires great expertise to minimize the risk to targeted systems.
- It may slow the organization's networks response time due to network scanning and vulnerability scanning.

Penetration Testing (contd..)

This rules of engagement, should include:

- Specific IP addresses/ranges to be tested
- Any restricted hosts (i.e., hosts, systems, subnets, not to be tested)
- A list of acceptable testing techniques (e.g. social engineering, DoS, etc.) and tools (password crackers, network sniffers, etc.)
- Times when testing is to be conducted (e.g., during business hours, after business hours, etc.)
- Identification of a finite period for testing
- IP addresses of the machines from which penetration testing will be conducted so that administrators can differentiate the legitimate penetration testing attacks from actual malicious attacks
- Points of contact for the penetration testing team, the targeted systems, and the networks
- Measures to prevent law enforcement being called with false alarms (created by the testing)
- Handling of information collected by penetration testing team.

Penetration Testing (contd..)

- To simulate an actual external attack, the testers are not provided with any real information about the target environment other than targeted IP address/ranges and they must covertly collect information before the attack.

- An internal penetration test is similar to an external except that the testers are now on the internal network (i.e., behind the firewall) and are granted some level of access to the network (generally as a user but sometimes at a higher level).

- The penetration testers will then try to gain a greater level of access to the network through privilege escalation

Internet Audit – Security Policy Review

- Understand and analyse the approach adopted by the organisation for Enterprise Security Architecture as compared with the standard approach to highlight any gaps
- Identify the gaps between corporate policies and security architecture
- Whether the Security Policy relate to the business requirements and meet the direction and expectations of senior management
- Perform Gap Analysis between Security Policies and Information Systems Strategic Plans
- Ensure that there are clearly defined expectations, roles and responsibilities amongst end users and administrators
- Ensure that detailed technical and security administration processes and procedures have been exhaustively elaborated in the administrative guidelines
- Ensure that there are sufficient compliance controls to ensure that the security policies and standards are being complied with
- Assess the adequacy of the Business Resumption/ Disaster Recovery Plan

Internal Audit-Information gathering

- Discussion of the network topology
- Placement of perimeter devices of routers and firewalls
- Placement of mission critical servers
- Existence of IDS
- Logging

Internal Audit-Environment & Physical Security

- Locked / combination / card swipe doors
- Temperature / humidity controls
- Neat and orderly computing rooms
- Fire suppression equipment
- UPS (Uninterruptible power supply)….

Internal Audit-Penetration

For Internal penetration test, it can divided to few categories

- Network
- Perimeter devices
- Servers and OS
- Application and services
- Monitor and response

Internal Audit-Network

- Location of devices on the network
- Redundancy and backup devices
- Staging network
- Management network
- Monitoring network
- Other network segmentation
- Cabling practices
- Remote access to the network

Internal Audit-Perimeter Devices

Involves of checking of configuration of perimeter devices like

- Routers
- Firewalls
- Wireless
- VPN servers

Test involves the followings

Test the ACL and filters like egress and ingress

Firewall rules

Configuration Access method

Logging methods

Internal Audit-Server & OS

- Identify mission critical servers like application, database, DNS, Email and others..
- Examine OS and the patch levels
- Examine the ACL on each servers
- Examine the management control-acct & password
- Placement of the servers
- Backup and redundancy

Internal Audit-Application & Services

Identify services and application running on the critical mission servers. Check vulnerabilities for the versions running. Remove unnecessary services/application.

This may include :

- DNS
  - Name services
- Email
  - Pop3,SMTP
- Web/Http
- SQL
- Others

Internal Audit-Monitor & Response

Audit should check for procedures on

Event Logging and Audit

- What are logged?
- How frequent logs are viewed?
- How long logs are kept?

Network monitoring

- What is monitored?
- Response Alert?

Intrusion Detection

- IDS in place?
- What rules and detection used?

Incident Response

- How is the response on the attack?
- What is recovery plan?
- Follow up?

Internal Audit-Analysis and Report

Analysis result

- Check compliance with security policy
- Identify weakness and vulnerabilities
- Cross check with external audit report

Report- key to realizing value

- Must be 2 parts
  - Not technical (for management use)
  - Technical (for IT staff)
- Methodology of the entire audit process
- Separate Internal and External
- State weakness/vulnerabilities
- Suggest solution to harden security

Guidelines for auditee organizations for Security Audit – Issues by Cert India

Guidelines for auditee organizations for Security Audit

Auditing contract should have the following :

Introduction – identifies the purpose, participants, and scope of audit

- Purpose
- Participants (auditee & auditor organization and any other)
- Audit scope definition

Audit Environment

- describes the environment in which the auditor will perform the audit including the physical location, hardware/software being used, policy and procedures the auditor will need to follow.
  - Entities and Locations
  - Facilities at each location
  - Equipment at each location
  - Policies, Procedures and Standards
  - Agreement and Licenses

Guidelines for auditee organisations for Security Audit

Roles and Responsibilities : describes the roles and responsibilities of all major participants.

- In case any of the activities to be audited in the auditee organsaition is outsourced, auditee must ensure that relevant personnel from outsourced organization are available at the time audit.

- The auditor's responsibilities need to articulate not just the audit tasks, but also the documentation of their activities, reporting their actions etc

Auditee roles and responsibilities for Security Audit

- Auditee refrains from carrying out any unusual or major network changes during auditing/testing.
- To prevent temporary raises in security only for the duration of the test, the auditee notifies only key people about the auditing/testing. It is the auditee's judgment, which discerns who the key people are, however it is assumed that they will be people at policy making level, managers of security processes, incident response, and security operations.
- If necessary for privileged testing, the auditee provides for necessary access tokens whether they be logins and passwords, certificates, secure ID numbers, etc. and they are typical to the users of the privileges being tested.

List of typical reviews and tests

- **Review of security policies and procedures**
  - Review of organization IT security policy and management system
  - Review of security procedures including
  - Incident response
  - Business continuity planning and disaster
- **Information Security Testing**
  - Information Integrity Review
  - Intelligence Survey
  - Human Resources Review
  - Competitive Intelligence Scouting
  - Privacy Controls Review
  - Information Controls Review

List of typical reviews and tests

Internet Technology Security Testing

1. Logistics and Controls
2. Posture Review
3. Intrusion Detection Review
4. Network Surveying
5. System Services Identification
6. Competitive Intelligence Scouting
7. Privacy Review
8. Document Grinding
9. Internet Application Testing
10. Exploit Research and Verification
11. Routing
12. Trusted Systems Testing
13. Access Control Testing
14. Password Cracking
15. Containment Measures Testing
16. Survivability Review
17. Denial of Service Testing
18. Security Policy Review
19. Alert and Log Review

Role of Auditors….

Role of Auditors

To determine whether

- Appropriate controls supporting integrity of business processes have been incorporated
- Appropriate security controls have been designed to minimise the risks of unauthorised access
- Appropriate controls exist surrounding the multi-platform Client server environment

Internal Auditors have to understand the objectives and implications of the Enterprise policies, procedures and standards, assess and control their compliance on a continued basis

Selecting external security consultants – Questions you need to ask !!

- Does the consultant organization offer a comprehensive suite of services , tailored to specific requirements ?
- Does the consulting organization have a quality certification ?
- Does the consulting organization have a track record of having handled a similar assignment for security consulting ?
- Are the organization's security professional having certificates like CISSP, CISA,CSM and CIPP?
- Does the Organization have sound methodology to follow ?
- Is the Organization recognized contributor within the security industry in terms of research and publication etc. ?

End of Session