Introduction to Information Security and Audit-Veegent

Introduction to Information Security and Audit

1.3.1 Information Systems Audit versus Information Security Audit:

Information System Audit or **Application Security Audit** and Information Security Audit are two such tools that are used to ensure the safety and integrity of information and sensitive data. People are often confused by the difference between these two tools and feel they are the same. But there are differences that will be highlighted in this article.

“Information systems audit is a large, broad term that encompasses demarcation of responsibilities, server and equipment management, problem and incident management, network division, safety, security, and privacy assurance, etc. On the other hand, as the name implies, information security audit has a one-point agenda and that is the security of data and information when it is in the process of storage and transmission.”

Here data must not be confused with only electronic data as print data is equally important and its security is covered in this audit. Both audits have many overlapping areas which are what confuses many people. However, from a physical point of view, an information system audit is related to the core, whereas an information security audit is related to the outer circles. Here core can be taken as a system, servers, storage, and even printouts and pen drives, whereas outer circles mean network, firewalls, internet, etc. If one were to look from a logical point of view, it would emerge that an information systems audit deals with operations, and infrastructure whereas an information security audit deals with data on the whole.

Note: Do prepare a table of differences between both of them as an assignment

In brief:

- Information systems audit is a broader term that includes an information security audit
- System audit includes operations, network segmentation, server, device management, etc., whereas security audit focuses on the security of data and information.

What is an Information Security Audit?

A security audit is a systematic evaluation of the security of a company's information system by measuring how well it conforms to a set of established criteria. A thorough audit typically assesses the security of the system's physical configuration and environment, software, information handling processes, and user practices. **Application Security Assessments** are often used to determine regulatory compliance, in the wake of legislation that specifies how organizations must deal with information.

Some of the purposes of audits are listed below:

1. a) Build awareness of current practices and risks
2. b) Reducing risk, by evaluating, planning, and supplementing security efforts
3. c) Strengthening controls including both automated and human
4. d) Compliance with the customer and regulatory requirements and expectations
5. e) Building awareness and interaction between technology and business teams
6. f) Improving overall IT governance in the organization

An information security audit is an audit on the level of information security in an organization. Within the broad scope of auditing information security there are multiple types of audits, multiple objectives for different audits, etc. Most commonly the controls being audited can be categorized to technical, physical and administrative. According to Ira Winkler, president of the Internet Security Advisors Group, there are three main types of security diagnostics, namely:

- Security Audits
- Vulnerability Assessments
- Penetration Testing

Security Audits measure an information system's performance against a list of criteria. A vulnerability assessment, on the other hand, involves a comprehensive study of an entire information system, seeking potential security weaknesses.
Penetration testing is a covert operation, in which a security expert tries a number of attacks to ascertain whether or not a system could withstand the same types of attacks from a malicious hacker. In penetration testing, the feigned (insincere/manmade) attack can include anything a real attacker might try, such as social engineering. Each of the approaches has inherent strengths, and using two or more of them in conjunction may be the most effective approach of all.

1.3.2 Scope of the Audit

As with any Audit, a risk assessment should be one of the first steps to be completed when examining a new process. The risk assessment will help determine whether the process warrants expending a significant amount of audit resources on the project. The scope of the audit depends on the risk. But even for the high-risk systems, the scope should be limited to testing the critical internal controls upon which the security of the process depends.
The scope of the audit depends upon:

1. Site business plan
2. Type of data assets to be protected
3. Value of importance of the data and relative priority
4. Previous security incidents

5. Time available
6. Auditors experience and expertise

What should be covered in audits? (Given just for reference only)

1.3.4 What makes a good security audit?

The development and dissemination of the IS Auditing Standards by the Information Systems Audit and Control Association (ISACA) is already in circulation for further information. A good security audit is part of a regular and comprehensive framework of information security.
A good security audit may likely include the following:

- Clearly defined objectives
- Coverage of security is comprehensive and cross-cutting audit across the entire organization. Partial audits may be done for specific purposes.
- The audit team is experienced, independent ,and objective. Every audit team should consist of at least two auditors to guarantee the independence and objectivity of the audit (”two-person rule”). There is an unrestricted right to obtain and view information.
- Important IS audit meetings such as the opening and the closing meetings as well as the interviews should be conducted as a team. This procedure ensures objectivity, thoroughness, and impartiality. No member of the audit team should have participated directly in supporting or managing the areas to be audited, e.g. they must not have been involved in the development of concepts or the configuration of the IT systems.
- It should be ensured that actual operations in the organization are not significantly disrupted by the audit when initiating the audit. The auditors never actively intervene in systems, and therefore should not provide any instructions for making changes to the objects being audited. It is the management’s responsibility for supporting the conduct of fair and comprehensive audits.
- Appropriate communication and appointment of ca central point of contact and other support for the auditors.
- The execution is planned and carried out in a phase-wise manner

1.3.5 Constraints of a security audit: Time constraints

- Third-party access constraints
- Business operations continuity constraints
- Scope of the audit engagement
- Technology tools constraints

1.4 Information Security Methodologies (Black-box, White-box, Grey-box)

1.4.1 Need for a Methodology

Audits need to be planned and have a certain methodology to cover the total material risks of an organization. A planned methodology is also important as this clarifies the way forward to all in the organisation and the audit teams. Which methodology and techniques is used is less important than having all the participants within the audit approach the subject in the same manner.

Audit methodologies

There are two primary methods by which audits are performed. Start with the overall view of the corporate structure and drill down to the minutiae; or begin with a discovery process that builds up a view of the organization. Audit methods may also be classified according to the type of activity. These include three types

1. **Testing** – Pen tests and other testing methodologies are used to explore vulnerabilities. In other words, exercising one or more assessment objects to compare actual and expected behaviors.
2. **Examination and Review** – This include reviewing policies, processes, logs, other documents, practices, briefings, situation handling, etc. In other words checking, inspecting, reviewing, observing, studying, or analyzing assessment objects
3. **Interviews and Discussion** – This involves group discussions, individual interviews, etc. The three methods combine together to form an effective methodology for an overall audit.

1.4.2 Auditing techniques:

There are various Auditing techniques used: Examination Techniques, are generally conducted manually to evaluate systems, applications, networks, policies, and procedures to discover vulnerabilities. These techniques include • Documentation review • Log review • Ruleset and system configuration review • Network sniffing • File integrity checking Target Identification and Analysis Techniques Testing techniques are generally performed using automated tools used to identify systems, ports, services, and potential vulnerabilities. The techniques include • Network discovery • Network port and service identification • Vulnerability scanning • Wireless scanning • Application security examination Page | 5 Target Vulnerability Validation Techniques Testing techniques that corroborate the existence of vulnerabilities, these may be performed manually or with automated tools. These techniques include • Password cracking • Penetration testing • Social engineering • Application security testing Organisations use a combination of these techniques to ensure effectiveness and meeting the objectives of the audit.

1.4.3 Security Testing Frameworks:

There are numerous security testing methodologies being used today by security auditors for technical control assessment.
Four of the most common are as follows:

1. Open Source Security Testing Methodology Manual (OSSTMM)
2. Information Systems Security Assessment Framework (ISSAF)
3. NIST 800 - 115
4. Open Web Application Security Project (OWASP)

1.4.4 Audit Process:
A successful audit will minimally:

1. Establish a prioritized list of risks to an organization.
2. Delineate a plan to alleviate those risks.
3. Validate that the risks have been mitigated.
4. Develop an ongoing process to minimize risk.
5. Establish a cycle of reviews to validate the process on a perpetual basis.

Every successful audit has common properties:

- Define the security perimeter – what is being examined?
- Describe the components – and be detailed about it.
- Determine threats – what kinds of damage could be done to the systems
- Delineate the available tools – what documents and tools are in use or need to be created?
- Reporting mechanism – how will you show progress and achieve validation in all areas?
- Review history – is there institutional knowledge about existing threats?
- Determine Network Access Control list – who really needs access to this?
- Prioritize risk – calculate risk as Risk = probability * harm
- Delineate mitigation plan – what are the exact steps required to minimize the threats?
- Implement procedures – start making changes.
- Review results – perform an AAR on the audit process.
- Rinse and repeat – schedule the next iteration of the process.

Auditing Security Practices (Reference)
The first step for evaluating security controls is to examine the organization’s policies, security governance structure, and security objectives because these three areas encompass the business practices of security. Security controls are selected and implemented because of security policies or security requirements mandated by law.
Some criteria you can use to compare the service of security against are:

- Evaluation against the organization's own security policy and security baselines
- Regulatory/industry compliance—Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act (SOX), Grahmm-Leach-Bliley Act (GLBA), and Payment Card Industry (PCI)
- Evaluation against standards such as NIST 800 or ISO 27002
- Governance frameworks such as COBIT or COSO

After you have identified the security audit criteria that the organization needs to comply with, the next phase is to perform assessments to determine how well they achieve their goals. A number of assessments are usually required to determine appropriate means for referring back to the scope, which defines the boundaries of the audit.
The following are types of assessments that might be performed to test security controls:

- **Risk assessments:** This type of assessment examines potential threats to the organization by listing areas that could be sources of loss such as corporate espionage, service outages, disasters, and data theft. Each is prioritized by severity, matched to the identified vulnerabilities, and used to determine whether the organization has adequate controls to minimize the impact.
- **Policy assessment:** This assessment reviews policy to determine whether the policy meets best practices, is unambiguous, and accomplishes the business objectives of the organization.
- **Social engineering:** This involves penetration testing against people to identify whether security awareness training, physical security, and facilities are properly protected.
- **Security design review:** The security design review is conducted to assess the deployment of technology for compliance with policy and best practices. These types of tests involve reviewing network architecture and design and monitoring and alerting capabilities.
- **Security process review:** The security process review identifies weaknesses in the execution of security procedures and activities. All security activities should have written processes that are communicated and consistently followed. The two most common methods for assessing security processes are interviews and observation:
- **Interviews:** Talking to the actual people responsible for maintaining security, from users to systems administrators, provides a wealth of evidence about the people aspect of security. How do they feel about corporate security methods? Can they answer basic security policy questions? Do they feel that security is effective? The kind of information gathered helps identify any weakness in training and the organization's commitment to adhering to policy.
- **Observation:** Physical security can be tested by walking around the office and observing how employees conduct themselves from a security perspective. Do they walk away

without locking their workstations or have sensitive documents sitting on their desks? Do they leave the data centre door propped open, or do they not have a sign-out procedure for taking equipment out of the building? It is amazing what a stroll through the cubicles of a company can reveal about the security posture of an organization.

- **Document review:** Checking the effectiveness and compliance of the policy, procedure, and standards documents is one of the primary ways an auditor can gather evidence. Checking logs, incident reports, and trouble tickets can also provide data about how IT operates on a daily basis.
- **Technical review:** This is where penetration testing and technical vulnerability testing come into play. One of the most important services an auditor offers is to evaluate the competence and effectiveness of the technologies relied upon to protect a corporation's assets.

1.4.5 Testing Security Technology

There are many terms used to describe the technical review of security controls. Ethical hacking, penetration test, and security testing are often used interchangeably to describe a process that attempts to validate security configuration and vulnerabilities by exploiting them in a controlled manner to gain access to computer systems and networks. There are various ways that security testing can be conducted, and the choice of methods used ultimately comes down to the degree to which the test examines security as a system.

There are generally two distinct levels of security testing commonly performed today:

Vulnerability assessment:

- This technical assessment is intended to identify as many potential weaknesses in a host, application, or entire network as possible based on the scope of the engagement.
- Configurations, policies, and best practices are all used to identify potential weaknesses in the deployment or design of the entity being tested. These types of assessments are notorious for finding an enormous amount of potential problems that require a security expert to prioritize and validate real issues that need to be addressed.
- Running vulnerability scanning software can result in hundreds of pages of items being flagged as vulnerable when in reality they are not exploitable.

Read More https://veegent.com/application-security-audit/