Information security audit

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. Auditing information security covers topics from auditing the physical security of data centers to auditing the logical security of databases, and highlights key components to look for and different methods for auditing these areas.

When centered on the Information technology (IT) aspects of information security, it can be seen as a part of an information technology audit. It is often then referred to as an information technology security audit or a computer security audit. However, information security encompasses much more than IT.

Contents

The audit process
- Audit planning & preparation
- Establishing audit objectives
- Performing the review
- Issuing the review report

Who performs audits

The audited systems
- Network vulnerabilities
- Controls
- Encryption and IT audit
- Logical security audit
- Specific tools used in network security
- Behavioural audit

Auditing application security
- Application security
- Segregation of duties
- Summary

Information Security Officer (ISO)

See also

References

Bibliography

External links

The audit process

Audit planning & preparation

An auditor should be adequately educated about the company and its critical business activities before conducting a data center review. The objective of the data center is to align data center activities with the goals of the business while maintaining the security and integrity of critical information and processes. To adequately determine whether the client's goal is being achieved, the auditor should perform the following before conducting the review:

- Meet with IT management to determine possible areas of concern
- Review the current IT organization chart
- Review job descriptions of data center employees
- Research all operating systems, software applications, and data center equipment operating within the data center
- Review the company's IT policies and procedures
- Evaluate the company's IT budget and systems planning documentation
- Review the data center's disaster recovery plan

Establishing audit objectives

The next step in conducting a review of a corporate data center takes place when the auditor outlines the data center audit objectives. Auditors consider multiple factors that relate to data center procedures and activities that potentially identify audit risks in the operating environment and assess the controls in place that mitigate those risks. After thorough testing and analysis, the auditor is able to adequately determine if the data center maintains proper controls and is operating efficiently and effectively.

Following is a list of objectives the auditor should review:

- Personnel procedures and responsibilities, including systems and cross-functional training
- Change management processes are in place and followed by IT and management personnel
- Appropriate back up procedures are in place to minimize downtime and prevent loss of important data
- The data center has adequate physical security controls to prevent unauthorized access to the data center
- Adequate environmental controls are in place to ensure equipment is protected from fire and flooding

Performing the review

The next step is collecting evidence to satisfy data center audit objectives. This involves travelling to the data center location and observing processes and within the data center. The following review procedures should be conducted to satisfy the pre-determined audit objectives:

- Data centre personnel – All data center personnel should be authorized to access the data center (key cards, login ID's, secure passwords, etc.). Datacenter employees are adequately educated about data center equipment and properly perform their jobs. Vendor service personnel are supervised when doing work on data center equipment. The auditor should observe and interview data center employees to satisfy their objectives.
- Equipment – The auditor should verify that all data center equipment is working properly and effectively. Equipment utilization reports, equipment inspection for damage and functionality,

system downtime records and equipment performance measurements all help the auditor determine the state of data center equipment. Additionally, the auditor should interview employees to determine if preventative maintenance policies are in place and performed.
- Policies and Procedures – All data center policies and procedures should be documented and located at the data center. Important documented procedures include data center personnel job responsibilities, back up policies, security policies, employee termination policies, system operating procedures and an overview of operating systems.
- Physical security / environmental controls – The auditor should assess the security of the client's data center. Physical security includes bodyguards, locked cages, man traps, single entrances, bolted-down equipment, and computer monitoring systems. Additionally, environmental controls should be in place to ensure the security of data center equipment. These include Air conditioning units, raised floors, humidifiers and uninterruptible power supply.
- Backup procedures – The auditor should verify that the client has backup procedures in place in the case of system failure. Clients may maintain a backup data center at a separate location that allows them to instantaneously continue operations in the instance of system failure.

Issuing the review report

The data center review report should summarize the auditor's findings and be similar in format to a standard review report. The review report should be dated as of the completion of the auditor's inquiry and procedures. It should state what the review entailed and explain that a review provides only "limited assurance" to third parties.

Who performs audits

Generally, computer security audits are performed by:

1. Federal or State Regulators - Certified accountants, CISA. Federal OTS, OCC, DOJ, etc.
2. Corporate Internal Auditors - Certificated accountants, CISA, Certified Internet Audit Professional (CIAP).[1]
3. External Auditors - Specialized in areas related to technology auditing.
4. Consultants - Outsourcing the technology auditing where the organization lacks the specialized skill set.

The audited systems

Network vulnerabilities

- Interception: Data that is being transmitted over the network is vulnerable to being intercepted by an unintended third party who could put the data to harmful use.
- Availability: Networks have become wide-spanning, crossing hundreds or thousands of miles which many rely on to access company information, and lost connectivity could cause business interruption.
- Access/entry point: Networks are vulnerable to unwanted access. A weak point in the network can make that information available to intruders. It can also provide an entry point for viruses and Trojan horses.[2]

Controls

- Interception controls: Interception can be partially deterred by physical access controls at data centers and offices, including where communication links terminate and where the network wiring and distributions are located. Encryption also helps to secure wireless networks.
- Availability controls: The best control for this is to have excellent network architecture and monitoring. The network should have redundant paths between every resource and an access point and automatic routing to switch the traffic to the available path without loss of data or time.
- Access/entry point controls: Most network controls are put at the point where the network connects with an external network. These controls limit the traffic that passes through the network. These can include firewalls, intrusion detection systems, and antivirus software.

The auditor should ask certain questions to better understand the network and its vulnerabilities. The auditor should first assess the extent of the network is and how it is structured. A network diagram can assist the auditor in this process. The next question an auditor should ask is what critical information this network must protect. Things such as enterprise systems, mail servers, web servers, and host applications accessed by customers are typically areas of focus. It is also important to know who has access and to what parts. Do customers and vendors have access to systems on the network? Can employees access information from home? Lastly, the auditor should assess how the network is connected to external networks and how it is protected. Most networks are at least connected to the internet, which could be a point of vulnerability. These are critical questions in protecting networks.

Encryption and IT audit

In assessing the need for a client to implement encryption policies for their organization, the Auditor should conduct an analysis of the client's risk and data value. Companies with multiple external users, e-commerce applications, and sensitive customer/employee information should maintain rigid encryption policies aimed at encrypting the correct data at the appropriate stage in the data collection process.

Auditors should continually evaluate their client's encryption policies and procedures. Companies that are heavily reliant on e-commerce systems and wireless networks are extremely vulnerable to theft and loss of critical information in transmission. Policies and procedures should be documented and carried out to ensure that all transmitted data is protected.

The auditor should verify that management has controls in place over the data encryption management process. Access to keys should require dual control, keys should be composed of two separate components and should be maintained on a computer that is not accessible to programmers or outside users. Furthermore, management should attest that encryption policies ensure data protection at the desired level and verify that the cost of encrypting the data does not exceed the value of the information itself. All data that is required to be maintained for an extensive amount of time should be encrypted and transported to a remote location. Procedures should be in place to guarantee that all encrypted sensitive information arrives at its location and is stored properly. Finally, the auditor should attain verification from management that the encryption system is strong, not attackable, and compliant with all local and international laws and regulations.

Logical security audit

The first step in an audit of any system is to seek to understand its components and its structure. When auditing logical security the auditor should investigate what security controls are in place, and how they work. In particular, the following areas are key points in auditing logical security:

- Passwords: Every company should have written policies regarding passwords, and employees' use of them. Passwords should not be shared and employees should have mandatory scheduled changes. Employees should have user rights that are in line with their job functions. They should also be aware of proper log on/ log off procedures. Also helpful are security tokens, small devices that authorized users of computer programs or networks carry to assist in identity confirmation. They can also store cryptographic keys and biometric data. The most popular type of security token (RSA's SecurID) displays a number that changes every minute. Users are authenticated by entering a personal identification number and the number on the token.
- Termination Procedures: Proper termination procedures so that, old employees can no longer access the network. This can be done by changing passwords and codes. Also, all id cards and badges that are in circulation should be documented and accounted for.
- Special User Accounts: Special User Accounts and other privileged accounts should be monitored and have proper controls in place.
- Remote Access: Remote access is often a point where intruders can enter a system. The logical security tools used for remote access should be very strict. Remote access should be logged.

Specific tools used in network security

Network security is achieved by various tools including firewalls and proxy servers, encryption, logical security and access controls, anti-virus software, and auditing systems such as log management.

Firewalls are a very basic part of network security. They are often placed between the private local network and the internet. Firewalls provide a flow-through for traffic in which it can be authenticated, monitored, logged, and reported. Some different types of firewalls include network layer firewalls, screened subnet firewalls, packet filter firewalls, dynamic packet filtering firewalls, hybrid firewalls, transparent firewalls, and application-level firewalls.

The process of encryption involves converting plain text into a series of unreadable characters known as the ciphertext. If the encrypted text is stolen or attained while in transit, the content is unreadable to the viewer. This guarantees secure transmission and is extremely useful to companies sending/receiving critical information. Once encrypted information arrives at its intended recipient, the decryption process is deployed to restore the ciphertext back to plaintext.

Proxy servers hide the true address of the client workstation and can also act as a firewall. Proxy server firewalls have special software to enforce authentication. Proxy server firewalls act as a middle man for user requests.

Antivirus software programs such as McAfee and Symantec software locate and dispose of malicious content. These virus protection programs run live updates to ensure they have the latest information about known computer viruses.

Logical security includes software safeguards for an organization's systems, including user ID and password access, authentication, access rights and authority levels. These measures are to ensure that only authorized users are able to perform actions or access information in a network or a workstation.

Auditing systems, track and record what happens over an organization's network. Log Management solutions are often used to centrally collect audit trails from heterogeneous systems for analysis and forensics. Log management is excellent for tracking and identifying unauthorized users that might be trying to access the network, and what authorized users have been accessing in the network and changes to user authorities. Software that record and index user activities within window sessions such as ObserveIT provide a comprehensive audit trail of user activities when connected remotely through terminal services, Citrix and other remote access software.[3]

According to a 2006 survey of 3243 Nmap users by Insecure.Org,[4] Nessus, Wireshark, and Snort were some top-rated network security tools. According to the same survey, the BackTrack Live CD is the top-rated information security auditing and penetration testing distribution. Nessus is a remote security scanner that performs over 1200 security checks for Linux, BSD, and Solaris. Wireshark analyzes network protocol for Unix and Windows, and Snort is an intrusion detection system that also supports Microsoft Windows. Nessus, Wireshark, and Snort are free. Some other popular products for network security include OmniGuard, Guardian, and LANGuard. Omniguard is a firewall, as is Guardian which also provides virus protection. LANGuard provides network auditing, intrusion detection, and network management. For log management, solutions from vendors such as SenSage and others are the choice for government agencies and highly regulated industries.

Behavioural audit

Vulnerabilities are often not related to a technical weakness in an organization's IT systems, but rather related to individual behaviour within the organization. A simple example of this is users leaving their computers unlocked or being vulnerable to phishing attacks. As a result, a thorough InfoSec audit will frequently include a penetration test in which auditors attempt to gain access to as much of the system as possible, from both the perspective of a typical employee as well as an outsider.[5]

System and process assurance audits combine elements from IT infrastructure and application/information security audits and use diverse controls in categories such as Completeness, Accuracy, Validity (V) and Restricted access (CAVR).[6]

Auditing application security

Application security

Application Security centers on three main functions:

- Programming
- Processing
- Access

When it comes to programming it is important to ensure proper physical and password protection exists around servers and mainframes for the development and update of key systems. Having physical access security at one's data center or office such as electronic badges and badge readers, security guards, choke points, and security cameras is vitally important to ensuring the security of applications and data. Then one needs to have security around changes to the system. Those usually have to do with proper security access to make the changes and having proper authorization procedures in place for pulling programming changes from development through test and finally into production.

With processing, it is important that procedures and monitoring of a few different aspects such as the input of falsified or erroneous data, incomplete processing, duplicate transactions and untimely processing are in place. Making sure that input is randomly reviewed or that all processing has proper approval is a way to ensure this. It is important to be able to identify incomplete processing and ensure that proper procedures are in place for either completing it or deleting it from the system if it was in error. There should also be procedures to identify and correct duplicate entries. Finally, when it comes to processing that is not being done on a timely basis one should back-track the associated data to see where the delay is coming from and identify whether or not this delay creates any control concerns.

Finally, access, it is important to realize that maintaining network security against unauthorized access is one of the major focuses for companies as threats can come from a few sources. First, one have internal unauthorized access. It is very important to have system access passwords that must be changed regularly and that there is a way to track access and changes so one is able to identify who made what changes. All activity should be logged. The second arena to be concerned with is remote access, people accessing one's system from the outside through the internet. Setting up firewalls and password protection to on-line data changes are key to protecting against unauthorized remote access. One way to identify weaknesses in access controls is to bring in a hacker to try and crack one's system by either gaining entry to the building and using an internal terminal or hacking in from the outside through remote access.

Segregation of duties

When you have a function that deals with money either incoming or outgoing it is very important to make sure that duties are segregated to minimize and hopefully prevent fraud. One of the key ways to ensure proper segregation of duties (SoD) from a systems perspective is to review individuals' access authorizations. Certain systems such as SAP claim to come with the capability to perform SoD tests, but the functionality provided is elementary, requiring very time-consuming queries to be built and is limited to the transaction level only with little or no use of the object or field values assigned to the user through the transaction, which often produces misleading results. For complex systems such as SAP, it is often preferred to use tools developed specifically to assess and analyze SoD conflicts and other types of system activity. For other systems or for multiple system formats you should monitor which users may have superuser access to the system giving them unlimited access to all aspects of the system. Also, developing a matrix for all functions highlighting the points where proper segregation of duties has been breached will help identify potential material weaknesses by cross-checking each employee's available accesses. This is as important if not more so in the development function as it is in production. Ensuring that people who develop the programs are not the ones who are authorized to pull it into production is key to preventing unauthorized programs into the production environment where they can be used to perpetrate fraud.

Summary

By and large, the two concepts of application security and segregation of duties are both in many ways connected and they both have the same goal, to protect the integrity of the companies' data and to prevent fraud. For application security, it has to do with preventing unauthorized access to hardware and software through having proper security measures both physical and electronic in place. With segregation of duties, it is primarily a physical review of individuals' access to the systems and processing and ensuring that there are no overlaps that could lead to fraud.

Information Security Officer (ISO)

Information Security Officer (ISO) is a relatively new position, which has emerged in organizations to deal in the aftermath of chaotic growth in information technology and network communication. The role of the ISO has been very nebulous since the problem that they were created to address was not defined clearly. The role of an ISO has become one of following the dynamics of the security environment and keeping the risk posture balanced for the organization.[7]

See also

- Computer security
- Defensive computing
- Directive 95/46/EC on the protection of personal data (European Union)
- Ethical hack
- Information security
- Penetration test
- Security breach

References

1. Certified Internet Audit Professional (CIAP), International Computer Auditing Education Association (ICAEA), http://www.iacae.org/English/Certification/CIAP.php
2. "Cyber Security Guide" (https://www.blueclone.com/). Wednesday, 2 December 2020
3. "Record and replay secure remote access of outsource providers and remote employees" (https://web.archive.org/web/20090709064514/http://www.observeit-sys.com/record_secure_remote_access.asp). ObserveIT. Archived from the original (http://www.observeit-sys.com/record_secure_remote_access.asp) on 2009-07-09. Retrieved 2008-11-23.
4. Lyon, Gordon (2006). "Top 100 Network Security Tools" (http://sectools.org/). *SecTools.org*. Retrieved 2006-08-24.
5. "10 Pieces of Advice That Will Help You Protect Your Data" (http://www.360ict.co.uk/data-protection-and-security-tips). 360ict. Retrieved 24 June 2016.
6. K. Julisch et al., Compliance by design - Bridging the chasm between auditors and IT architects (http://soadecisions.org/download/ComplianceByDesign-AAM.pdf) Computers & Security 30(6-7): 410-426 (2011)
7. Security Audit for Compliance with Policies (https://www.albany.edu/cyber/graduate/dfstudent/auditprocess%20copy.pdf?__cf_chl_captcha_tk__=pmd_Bnabi43NSu1An8wDfe4iIPIAfNIMfVBQuFw6yU8v2Og-1630791630-0-gqNtZGzNAyWjcnBszQil). albany.edu

Bibliography

- Gallegos, Frederick; Senft, Sandra; Manson, Daniel P.; Gonzales, Carol (2004). *Technology Control and Audit (2nd ed.)*. Auerbach Publications. ISBN 0-8493-2032-1.

External links

- Examining Data Centers (http://www.auditnet.org/docs/datacent.txt)
- Network Auditing (http://www.windowsecurity.com/software/Network-Auditing/)
- The OpenXDAS project (http://openxdas.sourceforge.net)

- Information Systems and Audit Control Association (ISACA) (http://www.isaca.org/Template.cfm?Section=IT_Audit_Basics&Template=/ContentManagement/ContentDisplay.cfm&ContentID=11234)
- The Institute of Internal Auditors (https://web.archive.org/web/20050326062253/http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=5444)
