Mainframe audit

A **mainframe audit** is a comprehensive inspection of computer processes, security, and procedures,with recommendations for improvement.

Contents

Definition of mainframe

A mainframe computer is not easy to define. Most people associate a mainframe with a large computer, but mainframes are getting smaller all the time. The terms *mainframe* and *enterprise server* are converging. Supercomputers are generally used for their speed and complexity, while mainframes are used for storing large volumes of sensitive data. Mainframes are typically the most secure, efficient, and cost-effective computing option for organizations dealing with transactions on a large, enterprise-level scale.

Considerations

Organizations in different industries have different auditing and security requirements. Some factors affecting the organizations' requirements are: regulatory requirements and other external factors; management, objectives, and business practices; and the organizations' performance compared to the industry. This information can be obtained by conducting outside research, interviewing employees, touring the data center and observing activities, consultations with technical experts, and looking at company manuals and business plans.

Another consideration is the level of mainframe access employees have and if password policies are in place and followed. Evidence of implementation can be obtained by requesting employee manuals, evaluating the software and user histories, and by physical observation of the environment. (Gallegos, 2004).

Physical access is also an area of interest. Are cables adequately protected from damage and sniffing between the Network and the Data Center? This can be achieved by proper routing of the cables, encryption, and a good network topology. Physical observation of where the cables are routed and

confirmation of the security procedures should be obtained. Tests of controls should be conducted to determine any additional weaknesses.

Does the mainframe have access to an adequate uninterruptible power supply? Are physical controls such as power badges for access, fire suppression devices, and locks in place to protect the data center (and the mainframe inside) from theft, manipulation or damage? Physical observation is necessary to ensure these requirements.

The Operating System

- What controls are in place to make sure the system is continually updated?
- Is the software configured to do updates, or is it done by the system technicians?
- Controls should be in place to deter unauthorized manipulation or theft of data.
- Proper separation of duties also needs to be verified. The company's internal controls need to be tested to determine if they are effective.
- Samples of entries into the system should be examined to verify that the controls are effective, while unauthorized and suspicious voided transactions need to be investigated. (Gallegos, 2004)
- Are there any processes on the system that could needlessly compromise other components?
- Procedures and measures need to be in place to minimize the risk of unauthorized access through Backdoors in the system, such as the Program Properties Table (PPT).
- There should be an accurate audit trail that can be followed. (The Henderson Group, October, 2001)

Security server

- Are proper separation of duties implemented and enforced, and are technology and procedures in place to make sure there is a continuous and accurate audit trail?
- Controls need to be put in place to minimize the risk of unnecessary and unauthorized entry into the system, and the protection of passwords.
- Computer-assisted audit techniques should be used to scan the system (continuous monitoring is ideal), with human observations conducted to verify procedures, such as to verify that protocols like separation of duties are being followed.
- Security software such as RACF, ACF2, and Top Secret need to be constantly evaluated to verify that they are providing the necessary security and if additional protection such as new firewalls is needed. (The Henderson Group, August, 2002). These products are the mainframe's main access control mechanism and as such, special care should be applied when analyzing. Verify proper user types are in use and that the sharing of credentials is never accepted.

Application system

- Is concerned with the performance and the controls of the system.
- Is it able to limit unauthorized access and data manipulation?

Evaluate whether sufficient evidence was obtained

After performing the necessary tests and procedures, determine whether the evidence obtained is sufficient to come to a conclusion and recommendation.

How is the security of the mainframe maintained?

Mainframes, despite their reliability, possess so much data that precautions need to be taken to protect the information they hold and the integrity of the system. Security is maintained with the following techniques:

- Physical controls over the mainframe and its components.
- Encryption techniques.
- Putting procedures in place that prevent unnecessary and unauthorized entries into a system and that input, output, or processing is recorded and accessible to the auditor. This is particularly important for people with elevated privilege.
- Security Software such as RACF, ACF2, and Top Secret.
- Constant testing of the security system to determine any potential weaknesses.
- Properly protecting backdoor accesses.
- Continual examination of the techniques to determine effectiveness.

To gauge the effectiveness of these internal controls an auditor should do outside research, physically observe controls as needed, test the controls, perform substantive tests, and employ computer assisted audit techniques when prudent.

References

- Gallegos, F., Senft, S., Manson, D., Gonzales, C. (2004). Information Technology Control and Audit. (2nd ed.) Boca Raton, Florida: Auerbach Publications.
- Messier jr., W., F. (2003) Auditing & Assurance Services: A Systematic Approach. (3rd ed.) New York: McGraw-Hill/Irwin.
- Licker, M., D. (2003). Dictionary of Computing & Communications. New York: McGraw-Hill
- Philip, G. (2000). The University of Chicago Press: Science and Technology Encyclopedia. Chicago, IL: The University of Chicago Press.
- O'Brien, J., A., (2002). Management Information Systems: Managing Information Technology in the E-Business Enterprise. 5th ed. New York: McGraw-Hill/Irwin.

External links

- The History of Computing Project (https://web.archive.org/web/20050624075909/http://www.thocp.net/hardware/mainframe.htm) (updated January 15, 2006). Mainframe. Retrieved January 27, 2006.
- Mainframes.com (http://www.mainframes.com/) (No Date). Retrieved January 27, 2006.
- The Henderson Group (October, 2001) Mainframe Audit News: Issue no.1 (http://www.stuhenderson.com/MANEWS01.pdf). Also issues 2 (http://www.stuhenderson.com/MANEWS02.pdf), 3 (http://www.stuhenderson.com/MANEWS03.pdf) and 4 (http://www.stuhenderson.com/MANEWS04.pdf) from the same source. Retrieved January 27, 2006.