WIKIPEDIA

Information technology audit

An **information technology audit**, or **information systems audit**, is an examination of the management controls within an Information technology (IT) infrastructure. The evaluation of obtained evidence determines if the information systems are safeguarding assets, maintaining data integrity, and operating effectively to achieve the organization's goals or objectives. These reviews may be performed in conjunction with a financial statement audit, internal audit, or other form of attestation engagement.

IT audits are also known as "automated data processing (ADP) audits" and "computer audits". They were formerly called "electronic data processing (EDP) audits".

Contents

Purpose

An IT audit is different from a financial statement audit. While a financial audit's purpose is to evaluate whether the financial statements present fairly, in all material respects, an entity's financial position, results of operations, and cash flows in conformity to standard accounting practices, the purposes of an IT audit are to evaluate the system's internal control design and effectiveness. This includes, but is not limited to, efficiency and security protocols, development processes, and IT governance or oversight. Installing controls are necessary but not sufficient to provide adequate security. People responsible for security must consider if the controls are installed as intended, if they are effective, or if any breach in security has occurred and if so, what actions can be done to prevent future breaches. These inquiries must be answered by independent and unbiased observers. These observers are performing the task of information systems auditing. In an Information Systems (IS) environment, an audit is an examination of information systems, their inputs, outputs, and processing. [1]

The primary functions of an IT audit are to evaluate the systems that are in place to guard an organization's information. Specifically, information technology audits are used to evaluate the organization's ability to protect its information assets and to properly dispense information to authorized parties. The IT audit aims to evaluate the following:

Will the organization's computer systems be available for the business at all times when required? (known as availability) Will the information in the systems be disclosed only to authorized users? (known as security and confidentiality) Will the information provided by the system always be accurate, reliable, and timely? (measures the integrity) In this way, the audit hopes to assess the risk to the company's valuable asset (its information) and establish methods of minimizing those risks.

IT audits are also known as Information Systems Audit, ADP audits, EDP audits, or computer audits [2]

Types of IT audits

Various authorities have created differing taxonomies to distinguish the various types of IT audits. Goodman & Lawless state that there are three specific systematic approaches to carry out an IT audit:[3]

- **Technological innovation process audit**. This audit constructs a risk profile for existing and new projects. The audit will assess the length and depth of the company's experience in its chosen technologies, as well as its presence in relevant markets, the organization of each project, and the structure of the portion of the industry that deals with this project or product, organization and industry structure.
- **Innovative comparison audit**. This audit is an analysis of the innovative abilities of the company being audited, in comparison to its competitors. This requires examination of company's research and development facilities, as well as its track record in actually producing new products.
- **Technological position audit**: This audit reviews the technologies that the business currently has and that it needs to add. Technologies are characterized as being either "base", "key", "pacing" or "emerging".

Others describe the spectrum of IT audits with five categories of audits:

- **Systems and Applications**: An audit to verify that systems and applications are appropriate, are efficient, and are adequately controlled to ensure valid, reliable, timely, and secure input, processing, and output at all levels of a system's activity. System and process assurance audits form a subtype, focussing on business process-centric business IT systems. Such audits have the objective to assist financial auditors.[4]
- **Information Processing Facilities**: An audit to verify that the processing facility is controlled to ensure timely, accurate, and efficient processing of applications under normal and potentially disruptive conditions.
- **Systems Development**: An audit to verify that the systems under development meet the objectives of the organization, and to ensure that the systems are developed in accordance with generally accepted standards for systems development.
- **Management of IT and Enterprise Architecture**: An audit to verify that IT management has developed an organizational structure and procedures to ensure a controlled and efficient environment for information processing.
- **Client/Server, Telecommunications, Intranets, and Extranets**: An audit to verify that telecommunications controls are in place on the client (computer receiving services), server, and on the network connecting the clients and servers.

And some lump all IT audits as being one of only two type: "**general control review**" audits or "**application control review**" audits.

A number of IT Audit professionals from the Information Assurance realm consider there to be three fundamental types of controls regardless of the type of audit to be performed, especially in the IT realm. Many frameworks and standards try to break controls into different disciplines or arenas, terming them “Security Controls“, ”Access Controls“, “IA Controls” in an effort to define the types of controls involved. At a more fundamental level, these controls can be shown to consist of three types of fundamental controls: Protective/Preventative Controls, Detective Controls and Reactive/Corrective Controls.

In an IS, there are two types of auditors and audits: internal and external. IS auditing is usually a part of accounting internal auditing, and is frequently performed by corporate internal auditors. An external auditor reviews the findings of the internal audit as well as the inputs, processing and outputs of information systems. The external audit of information systems is frequently a part of the overall external auditing performed by a Certified Public Accountant (CPA) firm.[1]

IS auditing considers all the potential hazards and controls in information systems. It focuses on issues like operations, data, integrity, software applications, security, privacy, budgets and expenditures, cost control, and productivity. Guidelines are available to assist auditors in their jobs, such as those from Information Systems Audit and Control Association.[1]

IT Audit process

The following are basic steps in performing the Information Technology Audit Process:[5]

1. Planning IN
2. Studying and Evaluating Controls
3. Testing and Evaluating Controls
4. Reporting
5. Follow-up
6. Reports

Security

Auditing information security is a vital part of any IT audit and is often understood to be the primary purpose of an IT Audit. The broad scope of auditing information security includes such topics as data centers (the physical security of data centers and the logical security of databases, servers and network infrastructure components),[6] networks and application security. Like most technical realms, these topics are always evolving; IT auditors must constantly continue to expand their knowledge and understanding of the systems and environment& pursuit in system company.

History of IT Auditing

The concept of IT auditing was formed in the mid-1960s. Since that time, IT auditing has gone through numerous changes, largely due to advances in technology and the incorporation of technology into business.

Currently, there are many IT dependent companies that rely on the Information Technology in order to operate their business e.g. Telecommunication or Banking company. For the other types of business, IT plays the big part of company including the applying of workflow instead of using the paper request form, using the application control instead of manual control which is more reliable or implementing the ERP application to facilitate the organization by using only 1 application. According to these, the importance of IT Audit is constantly increased. One of the most important role of the IT Audit is to audit over the critical system in order to support the Financial audit or to support the specific regulations announced e.g. SOX.

Audit personnel

Professional certifications

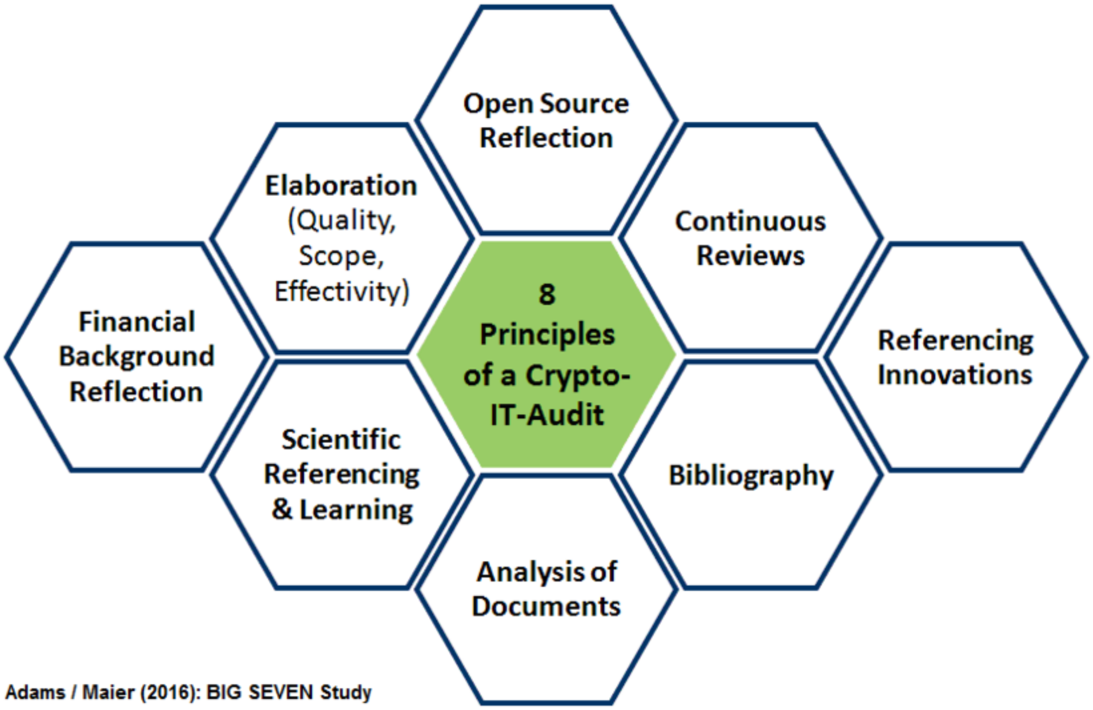
- Certified Information Systems Auditor (CISA)
- Practitioner Certificate in Information Security Auditing (PCISA) [7]
- Certified Internal Auditor (CIA)
- Certified in Risk and Information Systems Control (CRISC)
- Certification and Accreditation Professional (CAP)
- Certified Computer Professional (CCP)
- Certified Information Privacy Professional (CIPP)
- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- Certified Public Accountant (CPA)
- Certified Internal Controls Auditor (CICA)
- Forensics Certified Public Accountant (FCPA)
- Certified Fraud Examiner (CFE)
- Certified Forensic Accountant (CrFA)
- Certified Commercial Professional Accountant (CCPA)
- Certified Accounts Executive (CEA)
- Certified Professional Internal Auditor (CPIA)
- Certified Professional Management Auditor (CPMA)
- Chartered Accountant (CA)
- Chartered Certified Accountant (ACCA/FCCA)
- GIAC Certified System & Network Auditor (GSNA)[8]
- Certified Information Technology Professional (CITP); to certify, auditors should have 3 years experience
- Certified e-Forensic Accounting Professional] (CFAP)[9]
- Certified ERP Audit Professional (CEAP)[10])

Principles of an IT Audit

The following principles of an audit should find a reflection:[11]

- **Timeliness:** Only when the processes and programming is continuous inspected in regard to their potential susceptibility to faults and weaknesses, but as well with regard to the continuation of the analysis of the found strengths, or by comparative functional analysis with similar applications an updated frame can be continued.
- **Source openness:** It requires an explicit reference in the audit of encrypted programs, how the handling of open source has to be understood. E.g. programs, offering an open source application, but not considering the IM server as open source, have to be regarded as critical. An auditor should take an own position to the paradigm of the need of the open source nature within cryptologic applications.
- **Elaborateness:** Audit processes should be oriented to certain minimum standard. The recent audit processes of encrypting software often vary greatly in quality, in the scope and effectiveness and also experience in the media reception often differing perceptions. Because of the need of special knowledge on the one hand and to be able to read programming code and then on the other hand to also have knowledge of encryption procedures, many users even trust the shortest statements of formal confirmation. Individual commitment as an auditor, e.g. for quality, scale and effectiveness, is thus to be assessed reflexively for yourself and to be documented within the audit.

- **The financial context:** Further transparency is needed to clarify whether the software has been developed commercially and whether the audit was funded commercially (paid Audit). It makes a difference whether it is a private hobby / community project or whether a commercial company is behind it.


Open Source Reflection
Elaboration (Quality, Scope, Effectivity)
Continuous Reviews
Financial Background Reflection
8 Principles of a Crypto-IT-Audit
Referencing Innovations
Scientific Referencing & Learning
Bibliography
Analysis of Documents
Adams / Maier (2016): BIG SEVEN Study

- **Scientific referencing of learning perspectives:** Each audit should describe the findings in detail within the context and also highlight progress and development needs constructively. An auditor is not the parent of the program, but at least he or she is in a role of a mentor, if the auditor is regarded as part of a PDCA learning circle (PDCA = Plan-Do-Check-Act). There should be next to the description of the detected vulnerabilities also a description of the innovative opportunities and the development of the potentials.
- **Literature-inclusion:** A reader should not rely solely on the results of one review, but also judge according to a loop of a management system (e.g. PDCA, see above), to ensure, that the development team or the reviewer was and is prepared to carry out further analysis, and also in the development and review process is open to learnings and to consider notes of others. A list of references should be accompanied in each case of an audit.
- **Inclusion of user manuals & documentation:** Further a check should be done, whether there are manuals and technical documentations, and, if these are expanded.
- **Identify references to innovations:** Applications that allow both, messaging to offline and online contacts, so considering chat and e-mail in one application - as it is also the case with GoldBug - should be tested with high priority (criterion of presence chats in addition to the e-mail function). The auditor should also highlight the references to innovations and underpin further research and development needs.

This **list of audit principles for crypto applications** describes - beyond the methods of technical analysis - particularly core values, that should be taken into account

Emerging Issues

There are also new audits being imposed by various standard boards which are required to be performed, depending upon the audited organization, which will affect IT and ensure that IT departments are performing certain functions and controls appropriately to be considered compliant. Examples of such audits are SSAE 16, ISAE 3402, and ISO27001:2013.

Web Presence Audits

The extension of the corporate IT presence beyond the corporate firewall (e.g. the adoption of social media by the enterprise along with the proliferation of cloud-based tools like social media management systems) has elevated the importance of incorporating web presence audits into the IT/IS audit. The purposes of these audits include ensuring the company is taking the necessary steps to:

- rein in use of unauthorized tools (e.g. "shadow IT")
- minimize damage to reputation
- maintain regulatory compliance

- prevent information leakage
- mitigate third-party risk
- minimize governance risk[12][13]

Enterprise Communications Audits

The rise of VOIP networks and issues like BYOD and the increasing capabilities of modern enterprise telephony systems causes increased risk of critical telephony infrastructure being mis-configured, leaving the enterprise open to the possibility of communications fraud or reduced system stability. Banks, Financial institutions, and contact centers typically set up policies to be enforced across their communications systems. The task of auditing that the communications systems are in compliance with the policy falls on specialized telecom auditors. These audits ensure that the company's communication systems:

- adhere to stated policy
- follow policies designed to minimize the risk of hacking or phreaking
- maintain regulatory compliance
- prevent or minimize toll fraud
- mitigate third-party risk
- minimize governance risk[14][15]

Enterprise Communications Audits are also called voice audits,[16] but the term is increasingly deprecated as communications infrastructure increasingly becomes data-oriented and data-dependent. The term "telephony audit"[17] is also deprecated because modern communications infrastructure, especially when dealing with customers, is omni-channel, where interaction takes place across multiple channels, not just over the telephone.[18] One of the key issues that plagues enterprise communication audits is the lack of industry-defined or government-approved standards. IT audits are built on the basis of adherence to standards and policies published by organizations such as NIST and PCI, but the absence of such standards for enterprise communications audits means that these audits have to be based an organization's internal standards and policies, rather than industry standards. As a result, enterprise communications audits are still manually done, with random sampling checks. Policy Audit Automation tools for enterprise communications have only recently become available.[19]

See also

Computer Forensics

- Computer forensics
- Data analysis

Operations

- Helpdesk and incident reporting auditing
- Change management auditing
- Disaster recovery and business continuity auditing
- SAS 70

Miscellaneous

- XBRL assurance

Irregularities and Illegal Acts

- AICPA Standard: SAS 99 Consideration of Fraud in a Financial Statement Audit
- Computer fraud case studies

References

1. Rainer, R. Kelly, and Casey G. Cegielski. Introduction to information systems. 3rd ed. Hoboken, N.J.: Wiley ;, 2011. Print.
2. http://jobsearchtech.about.com/od/historyoftechindustry/g/IT_Audit.htm
3. Richard A. Goodman; Michael W. Lawless (1994). *Technology and strategy: conceptual models and diagnostics* (https://books.google.com/books?id=GIRdX9hIL1EC). Oxford University Press US. ISBN 978-0-19-507949-4. Retrieved May 9, 2010.
4. K. Julisch et al., Compliance by Design – Bridging the Chasm between Auditors and IT Architects (http://soadecisions.org/download/ComplianceByDesign-AAM.pdf). Computers & Security, Elsevier. Volume 30, Issue 6-7, Sep.-Oct. 2011.
5. Davis, Robert E. (2005). *IT Auditing: An Adaptive Process* (http://www.theiia.org/bookstore/product/it-auditing-an-adaptive-process-1263.cfm). Mission Viejo: Pleier Corporation. ISBN 978-0974302997.
6. "Advanced System, Network and Perimeter Auditing" (http://www.sans.org/security-training/auditing-networks-perimeters-and-systems-6-mid).
7. "IISP accredited certification" (http://www.ultimariskmanagement.com/URM/pdf/training/PCISA.pdf) (PDF).
8. "GIAC GSNA Information" (http://www.giac.org/certifications/audit/gsna.php).
9. http://www.iacae.org/English/Certification/CFAP.php
10. ICAEA, "Certification Program", http://www.iacae.org/English/Certification/CEAP.php
11. References to further core audit principles, in: Adams, David / Maier, Ann-Kathrin (2016): BIG SEVEN Study, open source crypto-messengers to be compared - or: Comprehensive Confidentiality Review & Audit of GoldBug, Encrypting E-Mail-Client & Secure Instant Messenger, Descriptions, tests and analysis reviews of 20 functions of the application GoldBug based on the essential fields and methods of evaluation of the 8 major international audit manuals for IT security investigations including 38 figures and 87 tables., URL: https://sf.net/projects/goldbug/files/bigseven-crypto-audit.pdf - English / German Language, Version 1.1, 305 pages, June 2016 (ISBN: DNB 110368003X - 2016B14779)
12. Juergens, Michael. "Social Media Risks Create an Expanded Role for Internal Audit" (http://deloitte.wsj.com/riskandcompliance/2013/08/06/social-media-risks-create-an-expanded-role-for-internal-audit/). *Wall Street Journal*. Retrieved 10 August 2015.
13. "Social Media Audit/Assurance Program" (http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Social-Media-Audit-Assurance-Program.aspx). *ISACA*. ISACA. Retrieved 10 August 2015.
14. Lingo, Steve. "A Communications Audit: The First Step on the Way to Unified Communications" (http://blog.xo.com/communications/unified-communications/a-communications-audit-the-first-step-on-the-way-to-unified-communications/). *The XO Blog*. Retrieved 17 Jan 2016.
15. "Telephone System Audit Service" (http://www.1st-comms.com/1st_communications_telephone_system_audit_service.htm). *1st Communications Services*. 1st Communications Services.
16. "Voice Audit" (http://www.securelogix.com/voice-audit.html). *www.securelogix.com*. Retrieved 2016-01-20.
17. "IP Telephony Design and Audit Guidelines" (http://www.eurotelecom.ro/files/IP_Telephony_Design_and_Audit_Guidelines_June_2003.pdf) (PDF). *www.eurotelecom.ro*.
18. "What is omnichannel? - Definition from WhatIs.com" (http://searchcio.techtarget.com/definition/omnichannel). *SearchCIO*. Retrieved 2016-01-20.
19. "Assertion" (http://www.smarterhi.com/assertion/). *SmarterHi Communications*. Retrieved 2016-01-21.

External links

- A career as Information Systems Auditor (http://www.networkmagazineindia.com/200312/securedview01.shtml), by Avinash Kadam (Network Magazine)
- IT Audit Careers guide (http://www.isrisk.net/information-technology-it-audit-computer-audit-careers-guide/)
- Federal Financial Institutions Examination Council (http://www.ffiec.gov/ffiecinfobase/booklets/audit/audit.pdf) (FFIEC)
- The need for CAAT Technology (https://web.archive.org/web/20130610150803/http://www.auditware.co.uk/content/76/The-need-for-CAATs)
- Open Security Architecture- Controls and patterns to secure IT systems (http://www.opensecurityarchitecture.org)
- American Institute of Certified Public Accountants (http://www.aicpa.org/) (AICPA)
- IT Services Library (http://www.itil-officialsite.com/home/home.asp) (ITIL)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Information_technology_audit&oldid=837616211"

This page was last edited on 21 April 2018, at 23:07.