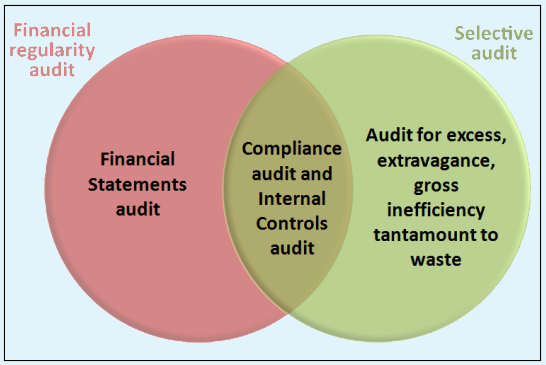
What is an IT Audit?

An Information Technology (IT) audit is an audit of an organisation's IT systems, management, operations and related processes.

An IT audit may be carried out in connection with a financial regularity audit or selective audit. As the records, services and operations of many organisations are often highly computerised, there is a need to evaluate the IT controls in the course of an audit of these organisations.

Types of Audits:

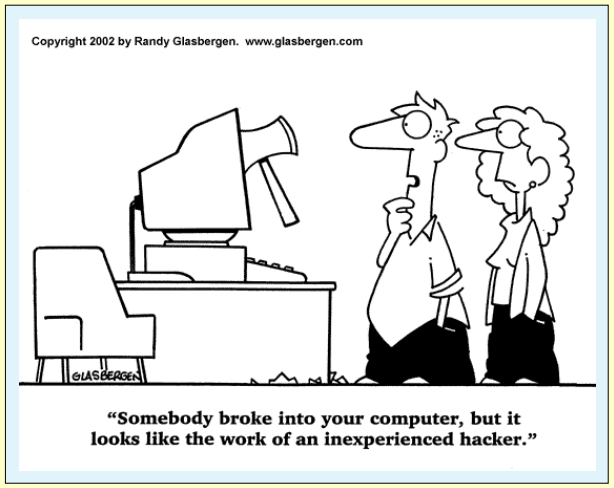


The objectives of IT audits include:

- Evaluating the reliability of data from IT systems which have an impact on the financial statements of the organisations.
- Ascertaining the level of compliance with the applicable laws, policies and standards in relation to IT.
- Checking if there are instances of excess, extravagance, gross inefficiency tantamount to waste in the use and management of IT systems.

Why is IT Audit important?

Many organisations are spending large amounts of money on IT because they recognise the tremendous benefits that IT can bring to their operations and services. However, they need to ensure that their IT systems are reliable, secure and not vulnerable to computer attacks.



IT audit is important because it gives assurance that the IT systems are adequately protected, provide reliable information to users and properly managed to achieve their intended benefits.

Many users rely on IT without knowing how the computers work. A computer error could be repeated indefinitely, causing more extensive damage than a human mistake.

IT audit could also help to reduce risks of data tampering, data loss or leakage, service disruption, and poor management of IT systems.

How is IT Audit carried out?

Generally, IT audit is carried out as follows:

1. Establish the IT audit objectives and scope.
2. Develop an audit plan to achieve the IT audit objectives.
3. Gather information on the relevant IT controls and evaluate them.
4. Perform audit tests, using Computer-Assisted Audit Techniques (CAATs) such as data extraction and analysis software or test data, where appropriate.
5. Report on the IT audit findings.

In performing its IT audits, the Auditor-General's Office (AGO) also checks for compliance with the Government policies, standards, laws and regulations on information and related technology.

Where appropriate, AGO uses the IT audit tools, technical guides and other resources recommended by ISACA (Information Systems Audit & Control Association), and encourages staff to be certified as CISA (Certified Information Systems Auditor).

Examples of AGO's IT Audit findings

• (2008) Test checks on IT access controls revealed lapses at 12 ministries and 4 organs of states. Access rights no longer required by 359 users were not promptly removed, in some cases for as long as 36 months.

• (2007) A software bought by an agency at a cost of $1.5 million was not cost effective. Due to certain problems, the software had not been used for 15 months.

• (2005) Information in a database for the public regarding certain registrations was not current. 18,161 of the registrations had expired for more than 11 months, including 13 cases which expired between 1992 and 2000.

• (2004) 36 officers no longer with an agency continued to have access rights to a system. 29 of them had left the agency for more than one year. 10 of the 29 officers were even given additional access rights after they left.

• (2001) A system file was found not secured properly, which could allow unauthorized programs to be run without being detected. The activities of the programmers who had access to the data and programs in the system were not reviewed by Management.

• (2000) An IT project to develop 17 application systems at a cost of $9.8 million was targeted for completion by December 1999. After 5 years, only 2 of the systems were implemented and $3.28 million had been spent on the project.

AUDITOR GENERAL'S REPORT

The things they did ... and did not do

Several ministries and stat boards taken to task, but AGO says not a reflection of state of governance

TODAY, July 24, 2008

REMOVAL OF COMPUTER ACCESS RIGHTS

Access rights to computer systems in ministries, state agencies and statutory boards should be given on a "need" basis to ensure confidentiality and integrity of systems and data, the AGO report said.

However, its checks revealed that lapses had occurred in some of these bodies.

For example, at 12 ministries and four organs of state, 359 users – who had either resigned, retired or been transferred or had their duties changed – did not have their existing access rights promptly removed.

The AGO suggested that these institutions look into effective ways of ensuring "prompt removal of access rights when no longer required".

Also working to plug loopholes is IE Singapore, the statutory board tasked with helping local firms venture abroad.

Last year, it wrote off 92 missing desktop computers, laptops and printers costing $277,681 "without carrying out a thorough investigation", according to the Auditor-General, who added that it was uncertain if sensitive information was still stored in the missing equipment acquired between 1986 and 2001.

IE Singapore said it had since "instituted measures to ensure that both the fixed assets and disposals will be independently accounted for."

Weekend TODAY, July 15-16, 2006

Security lapses found in some Govt systems

THE Auditor General's report has found that weak controls on computer systems is a common thread in government ministries here.

For example, at the Ministry of Communication, Information and the Arts, two users were given duplicate access with powerful rights that were not required. There were similar issues at departments like Singapore Customs, the Inland Revenue Authority of Singapore and the Health Sciences Authority. The report also pointed out irregularities

TODAY, July 14, 2006

www.ago.gov.sg

IT Audit

AGO

Auditor-General's Office
Singapore

Auditing for the Nation