IT Audits

An Information Technology (IT) audit is a review and evaluation of an organization's IT infrastructure, information system processes and operations. In some cases, an IT audit is used to validate or attest to what your organization has stated in paper review evaluations. Many partners are now requiring audits of their third party suppliers (often small businesses) to verify that sharing sensitive information with the partner is safe. IT audits should be performed every 1-2 years to ensure that the appropriate IT controls are in place and are functioning properly to minimize business risk.

FACT 1: IT AUDITORS

IT audits are performed by certified and specially trained personnel, also known as auditors. An IT auditor's role is to review and identify any weaknesses within an information system's network. Once the weaknesses have been identified, IT auditors present their findings and recommendations to management. It is management's responsibility to prioritize and ameliorate the audit findings.

A good IT auditor will look at the people, processes and technology to support your business -- and compare your organization's approach against an industry standard, such as ISO 27001. You should ask your auditor which standard that will be used to perform the assessment.

FACT 2: HOW AN IT AUDIT IS PERFORMED

An IT audit consists of the following:

- Audit testing:

  Tests are performed on the information system's internal controls to ensure that the appropriate processes and procedures are in place to appropriately safeguard the IT infrastructure. While performing these tests, the IT auditor inspects and evaluates the organization's compliance with government regulations (if applicable) and/or information security frameworks.

Did you know?

√ Financial auditors are now asking for the results of an IT audit as part of their review of the company

√ Vendors and/or partners are asking for the results of an IT audit prior to signing a partnership agreement

√ Decide what IT security framework your company will use

√ Check out the NCSS guide on IT security frameworks

√ Use the NCSS CARES tool to assess your company's security readiness

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service, **web@thencss.org** or visit us at the link below.

JOIN THE NCSS

Become a member of **The National Cybersecurity Society** today and learn more about how to protect your business from a cyber attack.

- Documentation:

  Information collected during the course of the audit is documented within "audit work papers." The work papers contain the procedures performed during the audit, the evidence obtained, and any opinions reached by the IT auditor.

- Identifying IT Audit Findings:

  "Findings" are generally known as deficiencies that require corrective actions. Once all findings have been identified, they will be discussed with the appropriate officials and the IT auditor will provide recommendations for remediation.

- Completing the IT Audit Report:

  At the conclusion of the IT audit, the auditor will prepare a report summarizing the results of the audit, the IT auditors' testing approach, and any suggested recommendations for remediating any findings identified throughout the course of the assessment.

FACT 3: PREPARING FOR AN IT AUDIT

Best practices for preparing for an IT audit include the following:

1. Stay up-to-date with IT security and compliance frameworks (know which compliance framework your company used to establish your IT security program);
2. Plan ahead - perform a self-review;
3. Be available;
4. Communicate to your employees who will work with the auditors;
5. Ask the auditors what you can do to prepare prior to their arrival on site.

FACT 4: IT AUDIT RESULTS

After an IT audit, the auditor will recommend an action plan related to external and internal IT processes and systems that were assessed. Take steps to prioritize the recommendations and complete an action plan. Correcting the deficiencies as recommended by the auditor, will improve your organizations' security, efficiency, and operations. With the right security controls in place, an organization will have the necessary mechanisms to ensure that the critical assets of the company are secured and protected.

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.

JOIN THE NCSS

Become a member of **The National Cybersecurity Society** today and learn more about how to protect your business from a cyber attack.

WWW.**NATIONALCYBERSECURITYSOCIETY**.ORG

THE NATIONAL **CYBERSECURITY** SOCIETY

FACT 5: BENEFITS OF AN IT AUDIT

Although an IT auditing can sound daunting, it will help ensure the confidentiality and integrity of the company's data. IT governance constitutes leadership, frameworks, and practices to ensure the company's critical assets are protected. An IT audit will help further the IT governance of the company.

ADDITIONAL RESOURCES:

Advantages of an IT Audit
http://bkmsh.com/advantages-of-an-it-audit/

How to Prepare for an Audit
http://www.audit.gatech.edu/resources/how-prepare-audit

How to Perform an Information Technology Audit by Roland DuBeau
https://www.scarlettculture.com/blog/how-perform-information-technology-audit

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.

JOIN THE NCSS

Become a member of **The National Cybersecurity Society** today and learn more about how to protect your business from a cyber attack.

WWW.**NATIONALCYBERSECURITYSOCIETY**.ORG