GIVA'S IT AUDIT CHECKLIST: WHAT TO INCLUDE AND HOW TO CREATE AND USE IT

This checklist provides step-by-step guidance for preparing for and performing IT audits.

For more information, see our IT Audit Checklist blog post.

5 Common Types of IT Audits

Not all IT audits are created equally. They are designed to accomplish different objectives, like bolstering efficiency, improving security, or reviewing for compliance. Let's take a look at five unique types of IT audits:

1. *Application Audit*

An application audit focuses on figuring out if an organization's systems and applications are efficient and secure, being used appropriately, and compliant with any regulations. In most cases, application audits look directly at the systems that handle a company's data.

For example, healthcare providers must ensure that all their applications are HIPPA-compliant. Giva offers a range of products that meet the needs of healthcare institutions that require high security and compliance, like the Giva HIPAA-compliant cloud help desk software.

2. *Facility Audit*

Facility audits are all about assessing the physical security and environmental controls of an organization's IT facilities. Examples of IT facilities include an off-campus data center or an on-site server room. During a facility IT audit, an auditor will examine if the facility is adequately secure and well-maintained for sustainable business continuity.

3. *System Development Audit*

System development audits ensure that IT systems that are under development will meet the organization's standards. Similarly an audit of this type helps ensure that existing systems are also maintained and efficient.

4. *Management Audit*

A management audit examines the capacity of the IT management personnel to adequately support their organization. In particular, an IT management audit will verify if the IT department and personnel are aligned with the organization's strategies and business operations.

5. *Network Audit*

A network audit examines the network infrastructure, including intranets and extranets. An audit of these two types of networks checks for functionality, reliability, and security. An intranet is a private or in-house network that allows employees to share information, collaborate, and communicate. An extranet allows authorized users from outside the organization to gain access to an organization's internal resources.

5 Critical Items to Include in an IT Audit Checklist

Every IT audit checklist is different from the next. That's because each checklist should be customized to fit your needs. For example, they'll vary based on your industry, the IT department you're auditing, whether the auditor is in-house or third-party, and the overarching objective of the audit.

With that being said, we want to provide five checklist categories to help you better understand what can be (and probably should be) included on an IT audit checklist:

1. *System Security*

Antivirus Software

Antivirus software should be installed and active on all necessary devices. It should be updated regularly, especially after incidents occur.

Network Firewall

Firewalls should be installed, active, and updated on a routine basis. The firewalls should include intrusion detection and prevention systems.

Hardware

Devices should meet all minimum security requirements, like password-protected screen locks. All hardware should be properly inventoried, maintained, and tracked.

Passwords

Passwords must be encrypted and require alphabetic, numeric, and symbolic characters. Passwords must be changed every three months, and group passwords are not permitted. When invalid passwords are attempted, accounts should be locked.

Accounts

Outdated accounts need to be deactivated and removed. Any account information sharing should be encrypted. Necessary accounts need to have administration privileges.

Physical Security

IT facilities should have locked doors and windows. All company property is under video surveillance. Any and all mobile hardware is locked away in storage. When necessary, it should be checked in and out.

Alerts

A robust alert system should be in place and monitored at all times. The system should include alerts for unauthorized access, unplanned system modifications, and alerts for physical security intrusions.

2. Standards and Procedures

Employee Requirements

Background checks are required to access certain systems. All employees must acknowledge and sign security policy agreements. All employees must participate in security awareness training protocols.

Incident Recovery and Response

A comprehensive business emergency plan is documented, updated, and shared among all necessary stakeholders. Employees should undergo emergency response training on an annual basis. The overall chain of command for emergency response is well-defined.

Document Disposal

All sensitive documents should be shredded. Shredded documents should be stored correctly until the time of disposal and are disposed of by professionals. Similarly, all devices undergo a factory reset before changing users or before being thrown out or donated.

Backups

Necessary critical backups are performed on a daily basis. Backup systems are checked and validated regularly. And backed-up files should be stored in at least two different places.

3. *Documentation and Reporting*

Security Protocols

All security protocols should be formally documented. Similarly, they should be updated after any system modification or security event. Security protocols need to be shared with all employees, third-party vendors, and business partners.

IT Logs

Detailed logs of IT systems should be stored for at least six months. Storage of the IT logs needs to be secure. All logs should be reviewed on a weekly or monthly basis.

Incident Reports

A reliable incident reporting system should be in place at all times. Incident reports should record descriptions, times, and dates. Likewise, reports should include causes and solutions for the incidents, and procedures should be updated if necessary. When necessary, a business impact assessment should be carried out.

4. *Performance Monitoring*

Outages

Frequencies of outages, both planned and unplanned, should be recorded. In addition, specific metrics related to outages should be recorded, such as mean time to resolve, mean time between outages, total downtime, and downtime by service.

Storage Utilization

How much storage is being utilized needs to be known at all times. This includes RAM storage, hard drive, and cloud storage utilization.

Network Performance

Certain network performance metrics should be reported. For example, upload speeds, download speeds, and network latency.

Finances

IT finances can be included in an audit. Financial data points include total IT expenses, IT expenses per employee, total cost per asset, and total cost per user group or user.

5. *Systems Development*

Design and new development

A robust review process should be implemented to determine which parts of the greater IT system need to be developed. When developments are made, they should be well documented and followed. In addition, developments should require approval when necessary. Lastly, documentation of developments should be comprehensive and accurate.

Testing

Testing of IT systems and controls should be rigorous and comprehensive. Likewise, testing of any and all programs needs to be implemented routinely and done correctly.

Implementation

Structured procedures for the implementation of new developments should be in place at all times. The implementation process needs to be documented and within compliance when necessary. Changes to the implementation plan should require approval. Likewise, specific security protocols should be followed during and after implementation. Afterward, documentation of the newly implemented control should be standard procedure.

The Process for How to Perform an IT Audit

How a business in the healthcare sector carries out its IT audits may vary drastically from how a law firm or large corporation facilitates its audits. That's because each institution's IT audit checklist will look a little different. Nonetheless, IT audits do have a generic progression from start to finish.

- *Schedule the Audit*

  Like a lot of things in life, sometimes the hardest step is the first one. But once you have an audit officially on the schedule, you can roll with the momentum. To mitigate operating too long without an audit, we recommend scheduling multiple audits so they become a normal routine in your business practice.

  To schedule your audit, you'll need to make a big decision: conduct an internal audit or hire an external auditor. Once you've decided that, you'll need to pick a date or a series of dates. Typically, it's best to schedule the audit during a "quiet" time on the business calendar, if possible.

- *Prepare for the Audit*

  Once you have the timeframe for an IT audit set in stone, it's time to start prepping.

  - Highlight the primary objectives of the audit
  - Define the scope of the audit, meaning what areas will be audited and the level of scrutiny they will be under
  - Create a more detailed audit schedule, such as which departments will be audited on which days and how much time is allotted for each one

- *Carry Out the Audit*

  If you perform an internal audit, it's time to execute the plan. If you've hired an external auditor, then it's time to let them work their magic. It's critical not to rush this step. That's because to benefit the most from the audit, you want to allow the process to unfold organically, as you outlined in your audit plan. Instead, focus on business as usual.

- *Report the Findings from the Audit*

  After the audit is completed according to your timeframe and plan, you will be left with a series of findings and suggestions. To make the most of these findings, you will want to incorporate them into an official audit report. If you performed multiple audits, a report should be created for each one. The report(s) should be cataloged for future reference.

  Typically, audit reports are two-fold: they highlight the business's strengths. Or what the business is already doing well. In addition, the report will also highlight the business's weaknesses. These are the areas that you'll focus on for improvement.

Next, you will want to devise an action plan for each weak point. For example, if your audit identified that some of your software is out of compliance with industry standards, you'll need to plan to update that.

- *Circle Back*

  After you have delivered your audit report and begun to carry out the different action plans to assess the weaknesses within your IT system, you'll want to eventually circle back to assess your progress.

  Put a date on the calendar in the near future to gauge if the proper corrections were implemented. If not, reassess your plan. If so, fantastic! It may be necessary to assign multiple dates to follow up. Before you know it, it will eventually become time for another IT audit, whereby you'll get a vivid picture of the improvements you've made in the past (and which weak points still require attention).

ABOUT GIVA

Founded in 1999, Giva was among the first to provide a suite of help desk and customer service/call center applications architected for the cloud.

Now, with hundreds of customer driven releases, the Giva Service Management™ Suite delivers an intuitive, easy-to-use design that can be deployed in just days and requires only one hour of training. Giva's robust, fast and painless reporting/analytics/KPIs quickly measure team productivity, responsiveness and customer satisfaction resulting in faster and higher quality decision-making. Customization and configuration are all point and click with no programming or consultants required to deliver a substantially lower total cost of ownership.

Giva is a private company headquartered in Sunnyvale, California serving delighted customers worldwide.