
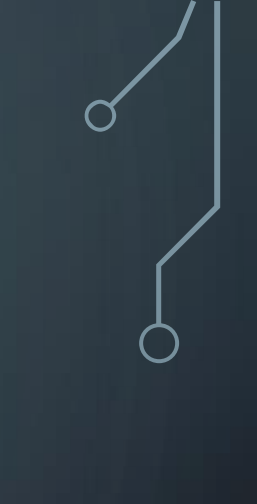
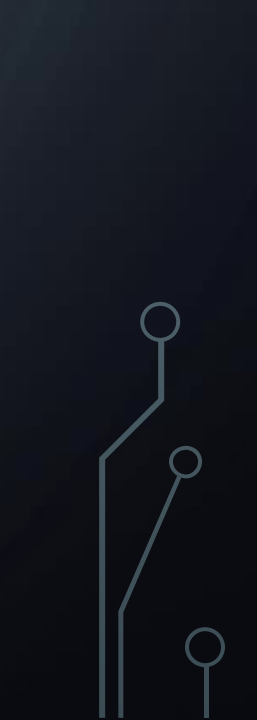


An abstract graphic on the left side of the slide, consisting of a network of thin, light-blue lines and small circles, resembling a circuit board or a data flow diagram. The lines are vertical and horizontal, with some diagonal connections, and the circles are small and white, acting as nodes or junctions.

THE IT AUDIT FUNCTION



OBJECTIVES

- Mission of the audit department
 - The role of the IT audit function
 - How to build and maintain an effective IT audit team
 - The importance of building relationships and the concept of independence
- 
- 
- 

IT AUDITORS

- Examines systems, processes, controls, policies, and people within an organization.
- Effective IT auditors need a strong technical and business background
- IT auditors can be internal or external to an organization

THE IT AUDIT MISSION

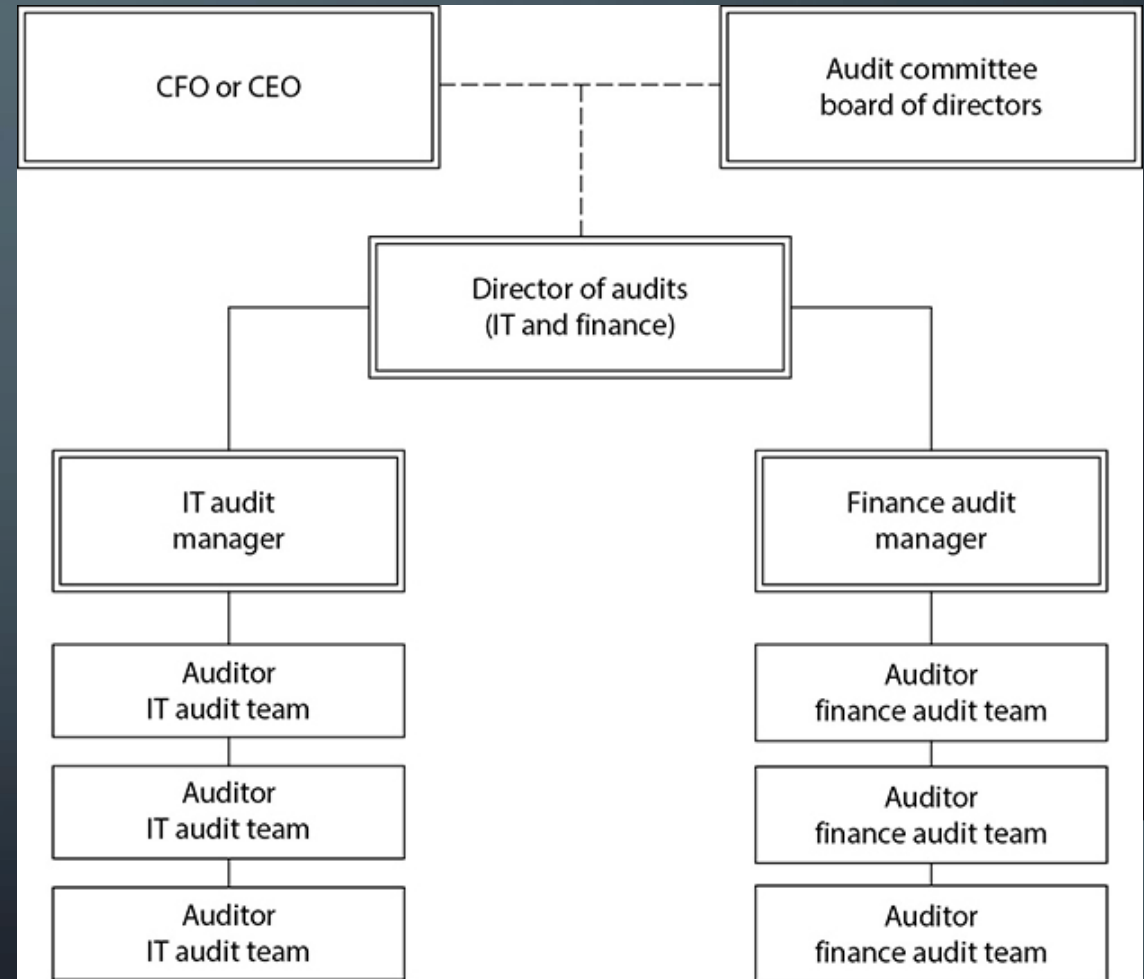
- What is the purpose of the audit department?
 - To report? To highlight issues? To make individuals look bad? To expose incompetence?
 - No... These are more adversarial mindsets that internal and even external audit departments can fall into...
 - The IT Audit function is meant to assist the mission of the business by helping to analyze and improve the state of internal technical, operational, and managerial controls within the business.
 - Auditees are not targets; they are partners.

THE IT AUDIT MISSION

- The internal audit department's goal should be to promote internal controls and help the company develop cost-effective solutions for addressing issues.
 - The internal auditor shouldn't just "report" on issues, but help the organization improve and resolve issues!
 - Just like any other department, the internal audit department provides value to the company through it's knowledge of how to evaluate internal controls.

INDEPENDENCE: THE GREAT MYTH

- Independence is one of the cornerstone principles of an audit department. It is also one of the biggest excuses used by audit departments to avoid adding value. Almost all audit departments point to their independence as one of the keys to their success and the reason that the audit committee can rely on them.
- As an auditor, you work for the company and report to its management; therefore, you are not independent.
- Objectivity should be valued over independence



BUSINESS ADVISORY AUDITS

- The cost of correcting issues and adding controls post-implementation is significantly higher than the cost of doing it right the first time. In terms of independence, there is no difference between providing an assessment of a system or solution prior to implementation and providing an assessment after implementation. There is a difference, however, in how much value the auditor is adding to the company.
- Keeping with good cybersecurity principles, proactive security measures and a proactive mindset are superior to a reactive mindset. Auditors can be extremely valuable for providing insights on developing internal security controls that are built into the system upfront.
- Good auditors help security professionals and IT teams with designing and implementing effective controls on our information systems. We need to move past the auditing days of “you’ve done this, this, and this, wrong... now fix it”.

BUSINESS ADVISORY AUDITS

- Now that we've established that it's okay to speak to your fellow employees about internal controls even when you're not auditing them, let's talk about some of the best ways to do this.
- These methods as a whole are often referred to as business advisory audits. We will discuss four methods for promoting internal controls at the company outside of your formal audits:
 - Early involvement
 - Informal audits
 - Knowledge sharing
 - Self-assessments

BUSINESS ADVISORY AUDITS

- Early involvement – Provide internal security control advice early throughout projects before implementation. This pays off dividends. This doesn't need to be a full audit, but rather the auditor providing input on IT projects.
- Informal audits – Review and analyses risks, and help employees to understand the state of internal controls on an ongoing basis. You don't necessarily need to conduct a formal audit.
- Knowledge sharing – Find ways to efficiently and effectively share your findings and knowledge with the rest of the company
- Self-assessments – Have a resource where the rest of the company can perform their own assessments. Work smart!

CONTROL GUIDELINES

- As you prepare for audits, one of the most frequent questions you'll hear is, "What do you people look for?" Wouldn't it be nice if you could just tell them to go to your website for the answer?
- Why not let people know what you look for when auditing Unix, for example? Why not let them know the basic sorts of controls you look for when auditing an application? This will not only help people prepare for your audits but will also provide excellent information for anyone else at the company who may be interested but whom you have no plans to audit.
- Posting control guidelines on your website empowers groups expecting an audit. Some groups actually will spend time up-front finding weaknesses and implementing appropriate controls. This effort benefits the company and the group being audited.

RELATIONSHIP BUILDING: PARTNERING VS. POLICING

- An effective internal audit department considers the audit to be a partnership with fellow employees and not a policing function.
- An effective audit department is involved year-round with key functions and does not just swoop in and out when performing audits. The audit should be an occasional event in an ongoing relationship.
- At the end of an audit, the people you've been auditing should look back and realize that it was a helpful experience and was not unpleasant.

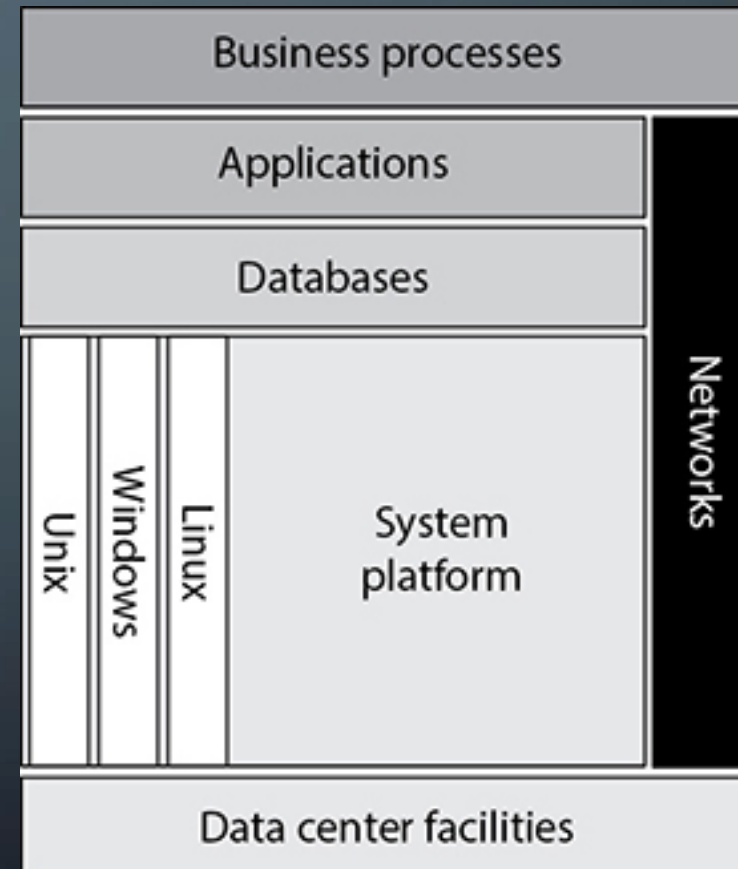


LEARNING TO BUILD PARTNERSHIPS

- To arrive at these results, the relationship between the IT auditors and the IT organization must be a cooperative, collaborative one.
- Be intentional about regular updates and meetings with IT management.
- Establish formal audit liaisons with different IT organizations.
- Participate in company governance activities.
- Cultivate an attitude of collaboration and cooperation.
- Implement job swaps with the IT organization.
- Involve the IT organization in IT audit hiring decisions.

THE ROLE OF THE IT AUDIT TEAM

- Business Processes
- Applications
- Data Centers
- Databases
- Operating Systems
- Networks
- Data Management



CAREER IT AUDITORS VS. IT PROFESSIONALS

Career IT Auditors

- These are the people whose entire background basically consists of performing IT audit work at various companies. They generally will have CISA or CISSP certifications and lots of experience at performing general controls reviews and Sarbanes-Oxley compliance reviews.
- It is essential that some career IT auditors are on your team, because they are well versed in audit theory and in internal controls at a conceptual level. They understand how the audit process works and the important concepts of testing and substantiation.
 - Sometimes lack hard skills or technical experience in the IT Field
 - Challenging to see the audit from the IT (or auditee) point of view

IT Professionals

- IT professionals are subject matter experts on technology but have no experience with auditing. These auditors can bring incredible maturity of understanding to your team in their specific field of expertise, allowing you to enhance your audit approach and audit tools for reviewing those technologies.
- However, it can be tough to find the right personality fit. If you use IT professionals on your team, you need to be aware of some common pitfalls.
 - Weak documentation skills (sometimes)
 - Nostalgia

KEY TRAITS OF A SUCCESSFUL IT AUDITOR

- As you begin your search to build out your audit team, consider the following key traits of a successful IT auditor:
- Ability to dig into technical details without getting lost in the details.
- Analytical and critical thinking skills. It is important for the auditor not only to understand technologies but also be able to use that knowledge to uncover risk to the business and apply judgment regarding degrees of risk. You need people who can think through a process or technology and frame up the risk to the company. This requires the auditor to take a “big picture” perspective when evaluating risk and determining the significance of potential issues.
- Communication skills (both written and oral). An auditor must be able to help all levels (from the most detailed technical person to the highest level of management) understand exactly why something is of concern. This means that the auditor must be able to lay it out logically in layperson’s terms for management but also explain all the technical details of a concern to the people who work in the area.
- Ability to learn the key concepts of new technologies quickly and identify key risk points within those technologies.
- Willingness not to be touching a specific technology daily. It’s important for auditors to understand that although performing audit analyses requires a lot of hands-on work, they won’t be acting as the administrator of a production Unix box, managing routers, and so on.
- Relationship-building skills. Auditors must be able to build solid, trust-based relationships with their customers. This includes the ability to feel empathy for their customers and consider the world from their side of the table.
- Business acumen. As discussed earlier, the mission of the audit department is to add value to the company. Auditors will be better able to do that if they understand the company’s business and are able to tie their risk assessments and audit recommendations to how they support the business’s objectives.
- Data mining and analytics skills. While not every auditor will be a data extraction and analysis specialist (as described earlier in this chapter), every auditor needs to know how to analyze data and arrive at data-driven conclusions.

MAINTAINING EXPERTISE

- Training is essential for IT auditors because technologies and techniques change constantly. Your auditors won't be supporting the technologies day to day (which necessitates keeping up with changes), so if you're not intentional about maintaining your expertise, your team's knowledge will quickly become outdated. It's never fun when you take your department's expert to a meeting and you find out that he or she has become a "dinosaur" who lacks knowledge of the latest developments.

RELATIONSHIP WITH EXTERNAL AUDITORS AND INTERNAL ASSURANCE FUNCTIONS

- A healthy relationship must be maintained between internal and external auditors
- No one likes having his or her work reviewed and questioned, even though the external auditors are just giving the internal auditors a taste of their own medicine. We must accept the fact, however, that the external auditors are a legitimate need. A healthy working relationship between the internal and external auditors, where information is shared freely, is the best environment to create and provides the most value to your company.

SUMMARY

- The real mission of the internal audit department is to add value by helping improve the state of internal controls at the company.
- Internal auditors are not truly independent, but they should be objective.
- It is important to find ways to accomplish the department's mission outside of formal audits. Early involvement, informal audits, knowledge sharing, self-assessments, and continuous auditing are five important tools in this regard.
- Building and maintaining good relationships with the IT organization are critical elements of the IT audit team's success.
- Successful IT audit teams generally will consist of a combination of career auditors and IT professionals.
- It is critical to develop methods for maintaining the technical expertise of the IT audit team.
- A healthy relationship should be developed with external IT auditors and internal assurance functions.