

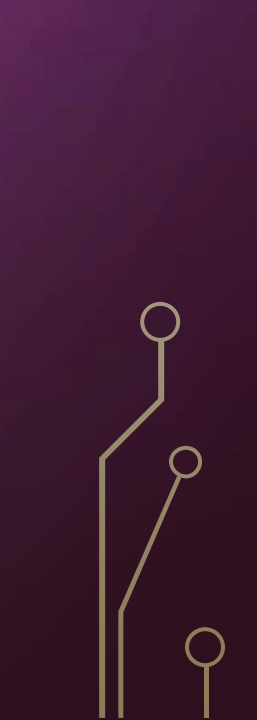


A decorative graphic on the left side of the slide, consisting of a network of white lines and small circles on a purple gradient background, resembling a circuit board or a stylized tree structure.

MODULE 3A: AUDITING ENTITY- LEVEL CONTROLS



OBJECTIVES

- Auditing Entity-Level Controls
 - What are Entity-Level Controls
 - Why are they important?
 - Where does the auditor come in?
 - How to audit-entity level controls?
- 
- 
- 

ENTITY-LEVEL CONTROLS

- When you think of entity-level controls, think of business-wide, large, administrative controls, and centralization.
- Because entity-level controls are pervasive across an organization, you can audit them once and feel confident that you have covered the topic for the whole company.
 - The definition of an entity-level control may vary by company or by the auditor
- However, there's really no mystery to it—it all comes down to what is centralized and pervasive at your company. If a critical IT process is centralized, it is a good candidate for an entity-level controls review.

ENTITY-LEVEL CONTROLS

- Strong IT entity-level controls form a foundation for the IT control environment within a company. They demonstrate that IT management is serious about internal controls, risk management, and governance.
- A strong overall control environment and attitude that originates from the top tends to trickle down throughout the organization and leads to strong controls over decentralized processes and functions.


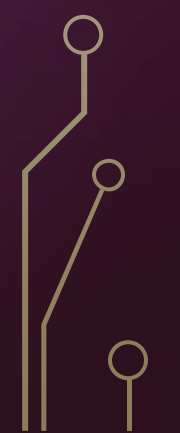


AUDITING CYBERSECURITY PROGRAMS

- While larger or more mature businesses have had security programs for many years, over the last decade almost every company of any appreciable size has either created a security program or increased its attention to existing programs. As with any large investment, companies want to know that their efforts are meeting the needs of the organization.
- This is where the auditor comes in.



ENTITY-LEVEL CONTROLS

- It is critical for upper management to communicate and set the tone that internal controls, risk management, and governance are valued and will be rewarded. Without this message, departments are more likely to focus on cutting costs, managing their budgets, and meeting their schedules, with no consideration given to internal controls.
- 
- 

AUDITING ENTITY-LEVEL CONTROLS

Checklist for Auditing Entity-Level Controls

- ☐ 1. Review the overall IT organization structure to ensure that it provides for clear assignment of authority and responsibility over IT operations and that it provides for adequate segregation of duties.
- ☐ 2. Review the IT strategic planning process and ensure that it aligns with business strategies. Evaluate the IT organization's processes for monitoring progress against the strategic plan.
- ☐ 3. Determine whether technology and application strategies and roadmaps exist, and evaluate processes for long-range technical planning.
- ☐ 4. Review performance indicators and measurements for IT. Ensure that processes and metrics are in place (and approved by key stakeholders) for measuring performance of day-to-day activities and for tracking performance against service level agreements, budgets, and other operational requirements.

AUDITING ENTITY-LEVEL CONTROLS

- ☐ 5. Review the IT organization's process for approving and prioritizing new projects. Determine whether this process is adequate for ensuring that system acquisition and development projects cannot commence without approval. Ensure that management and key stakeholders review project status, schedule, and budget periodically throughout the life of significant projects.
- ☐ 6. Evaluate standards for governing the execution of IT projects and for ensuring the quality of products developed or acquired by the IT organization. Determine how these standards are communicated and enforced.
- ☐ 7. Review and evaluate risk-assessment processes in place for the IT organization.
- ☐ 8. Review and evaluate processes for ensuring that IT employees at the company have the skills and knowledge necessary to perform their jobs.
- ☐ 9. Ensure that effective processes exist for complying with applicable laws and regulations that affect IT and for maintaining awareness of changes in the regulatory environment.
- ☐ 10. Review and evaluate processes for ensuring that end users of the IT environment can report problems, are appropriately involved in IT decisions, and are satisfied with the services provided by IT.
- ☐ 11. Review and evaluate processes for managing third-party services, ensuring that their roles and responsibilities are clearly defined and monitoring their performance.
- ☐ 12. Review and evaluate processes for controlling nonemployee logical access.

AUDITING ENTITY-LEVEL CONTROLS

- ☐ 13. Review and evaluate processes for ensuring that the company is in compliance with applicable software licenses.
- ☐ 14. Review and evaluate controls over remote access into the company's network (such as VPN and dedicated external connections).
- ☐ 15. Ensure that hiring and termination procedures are clear and comprehensive.
- ☐ 16. Review and evaluate policies and procedures for controlling the procurement and movement of hardware.
- ☐ 17. Ensure that system configurations are controlled with change management to avoid unnecessary system outages.
- ☐ 18. Ensure that media transportation, storage, reuse, and disposal are addressed adequately by company-wide policies and procedures.
- ☐ 19. Verify that capacity monitoring and planning are addressed adequately by company policies and procedures.
- ☐ 20. Review and evaluate the company's identity and access management processes.
- ☐ 21. Review and evaluate the elements of the company's cybersecurity program.
- ☐ 22. Based on the structure of your company's IT organization and processes, identify and audit other entity-level IT processes.

REFLECTIONS

- An IT Audit is a big task. Start with the large entity-level controls to gain an understanding of the organization and its practices, then start tackling the constituent components, which is what we're going to be covering for the remainder of the course.

