MODULE 3B: AUDITING CYBERSECURITY PROGRAMS

OBJECTIVES

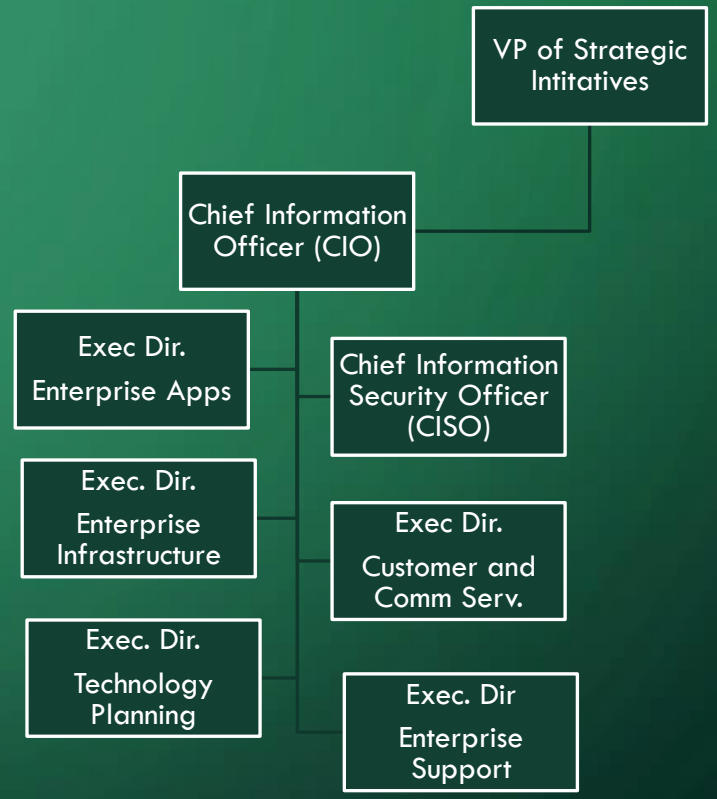
- Auditing Cybersecurity Programs
  - Scope and structure of cybersecurity programs
  - Organizational oversight and governance
  - Common functions and services of security programs
  - Specific technical and procedural items to review

AUDITING CYBERSECURITY PROGRAMS

- As an auditor, some of the first things you'll need to understand are the size, scope, and purpose of the firm's cybersecurity program.
- In small companies, the entire security team might reside in one person, whose day job is to help with IT issues when not answering the phones. Very large organizations might have hundreds of security personnel spread across many functions, and some may have as many external security service providers as they have employees.

WHO'S IN CHARGE?

- Assess the placement of the cybersecurity program within the overall organization and ensure appropriate oversight.
- A CISO? Who does the CISO report to? How is the cybersecurity department structured within the larger organization?
  - Use inside information and org charts.



RISK MANAGEMENT PROCESS

- Many very large and complex risk management processes exist, and many organizations follow them to the letter. If this is the case, you may only need to review the outputs of these processes to see that the firm is assessing and identifying risks adequately. More often though, risk processes are less formal.

- Periodic, formal threat and risk assessments for critical systems
- Third-party testing of security controls and correction of any identified deficiencies
- Compliance programs and monitoring of internal controls
- Strategic planning processes that prioritize initiatives based on risk or value
- How are risks identified, and how does the team align on how to address them?
- What role do business leaders and other stakeholders play in the decision process?
- Are cybersecurity threats considered in the overall organization risk discussions?

WHAT IS THE SCOPE OF THE CYBERSECURITY PROGRAM?

- Cybersecurity programs can differ greatly in size and scope. As an auditor, you'll need to determine how the security needs of the organization—defined in part by its risk posture—are met by the structure of the information security program.
- Cyber programs should cover functions like Policy and Compliance management, awareness training, vulnerability management, security monitoring, incident response, regardless of their size.

SECURITY POLICIES

- Review the security policy and compliance functions of the organization, ensuring that IT security policies exist and provide adequate requirements for the security of the environment. Determine how those policies are communicated and how compliance is monitored and enforced.
- Are they in place? Are they too strict? Are they too lenient?
- Most important, are security policies being followed?
  - Look at organizational practices to find out.

REFLECTIONS

- Auditing and understanding the cybersecurity program is going to give you a lot of insight into the business as a whole. Again, we're starting with the big rocks, and moving to the smaller on.

Checklist for Auditing Cybersecurity Programs	
❑	1. Assess the placement of the cybersecurity program within the overall organization and ensure appropriate oversight.
❑	2. Assess the information-related risk management processes of the organization and evaluate how cybersecurity risks are identified and managed.
❑	3. Evaluate the scope of the cybersecurity program and its relationship to other IT functions within the organization.
❑	4. Review the security policy and compliance functions of the organization, ensuring that IT security policies exist and provide adequate requirements for the security of the environment. Determine how those policies are communicated and how compliance is monitored and enforced.
❑	5. Review the awareness and communications functions of the security team, reviewing methods to train employees on security risks and concerns.
❑	6. Review the vulnerability management function of the organization, ensuring that the team is aware of emerging threats and vulnerabilities and has processes to identify at-risk systems in the environment.
❑	7. Assess the security monitoring function of the security team, reviewing log collection and alert processing and detection capabilities.
❑	8. Assess the incident response function of the security team, ensuring that the organization is able to respond effectively to various kinds of security events.
❑	9. Assess other functions of the security team as appropriate.
❑	10. Review and evaluate policies and processes for assigning ownership of company data, classifying the data, protecting the data in accordance with their classification, and defining the data's life cycle.
❑	11. Determine how security policies and security risk are handled in organizational IT processes.
❑	12. Review and evaluate processes for ensuring that security personnel have the skills and knowledge necessary for performing their jobs.
❑	13. Assess that metrics are collected commensurate with the goals of the security program and that metrics are reported to appropriate management personnel.
❑	14. Review processes around the use of managed security service providers (MSSPs) within the security team.
❑	15. Determine how the organization ensures that its security controls are effective.