CHAPTER 4

Auditing Cybersecurity Programs

High-profile incursions against technology and defense firms, breaches of credit card information, thefts of personal data—all of these have increased the awareness of security issues among boards of directors, executives, and others charged with making their companies successful. Globally, regulations dealing with the protection of data and systems have proliferated, with Payment Card Industry (PCI) standards, the European Union General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), and other requirements forcing companies to improve their security posture or face penalties or fines. Defending firms against cyber attacks and ensuring compliance with security and privacy regulations require training, vigilance, and a number of technical and procedural controls that aren't second nature to most people in an organization. In response to these and other concerns, companies around the world have increased their investments in security.

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. This chapter provides an overview of considerations for auditing cybersecurity programs. Some of the topics covered here include

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

BACKGROUND

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. Cybersecurity programs take many different forms. 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. While the size of a company's security team is often directly proportional to the revenue or profitability of a company, other factors can also influence the size and scope of security programs.

Retail and financial organizations must comply with a

range of regulations related to the kinds of information and assets they process. Retailers usually handle credit cards, and must comply with PCI rules in order to offer that service to their customers. Banks and brokerages must comply with a range of governmental rules. In addition to compliance with the different laws and standards, these kinds of businesses must protect themselves from reputational damage, as they don't want their customers to go to competitors because of security flaws. Retailers and financial organizations often have security programs focused heavily on compliance, and their budgets can be quite high.

Technology companies, or those dealing with the design and production of sophisticated equipment, such as for defense or aerospace industries, may have a completely different set of security concerns. They may be most intent on protecting their intellectual property from theft by competitors, insiders, or external groups. Since they may not have to comply with specific regulations, their security programs are dictated more by their internal risk appetites. More risk-tolerant companies may have leaner security teams, while more risk-averse businesses may have larger teams.

Manufacturing firms may also have intellectual property to protect but might primarily be concerned with avoiding cybersecurity issues that would affect their production lines. Depending on how the company is structured, responsibility for the security of production floors might reside within the factory teams themselves,

or for larger companies, shared with a central security team. As with intellectual property firms, the scope of a security program is often related to the risk appetite of the business.

Credit agencies, nonprofits, governments, healthcare providers, and others might be targeted for the personal information they store and process. Some of the largest breaches to date have involved personal information. Personal data can be thought of like intellectual property but is often more regulated. Entities that deal heavily in personal data can incur fines and other costs when that data is stolen, so protecting it may be a high priority compared to other needs.

As in the previous chapter, there's no "one size fits all" approach. You must consider the overall organization and its risk posture in order to properly assess the program. Knowing the business needs and how they inform the company security program will help you evaluate the strength of a program and determine how to regard potential gaps. You may have to complete all of the steps discussed for contextual understanding before outlining strengths and improvement opportunities for each item.

STEPS FOR AUDITING CYBERSECURITY PROGRAMS

1. Assess the placement of the cybersecurity program within the overall organization and ensure appropriate oversight.

Most organizations ultimately identify someone to be responsible for information security for the company. This person is often designated as the chief information security officer (CISO), but could be identified as the director of information security, IT security manager, or might have a completely unrelated title, depending on the size and maturity of the team. In some companies, the chief information officer (CIO) is responsible for information security. Organizational reporting structures and lines of responsibility can vary greatly. This step helps set the stage for the rest of the audit by identifying the people responsible for information security and how they relate to the business at large.

How

Review organization charts to identify the information security team and management. The information security program is often part of the IT function, and the security manager may report to the CIO, but this is not always the case. In some larger organizations or those with higher cyber-related risk concerns, the CISO may report to the CEO or to another executive. Ensure that a clear reporting structure exists such that information security resources are guided through a single management chain or process. This provides the security group with clear objectives.

Interview the CISO or equivalent, or a delegate, to understand the level of oversight provided to the information security team under this structure. In many

cases this will be through executive committees or regular presentations to company boards of directors. In some cases this oversight may come from the CIO or another high-ranking person in the company. It is important that the activities of the information security team fall under the guidance of the company's overall management structure in some way to ensure alignment with business actions.

For example, you could be part of a firm with a CISO, who reports to the CIO, who reports to the executive steering committee, who reports to the board of directors. On a periodic basis, the executive steering committee may meet with the CIO and/or CISO to review the state of information security, and the board of directors may be kept informed.

Among companies with boards, it's common for the CIO or CISO to report at least annually to the board of directors on the state of the information security program.

Again, there's no single "correct" structure. The key objective of this step is to understand who is responsible for cybersecurity and what corporate oversight is in place to advise the program.

2. Assess the information-related risk management processes of the organization and evaluate how cybersecurity risks are identified and managed.

For most businesses, information security is much like insurance. Security rarely adds value to whatever the

company's business is; it often serves primarily to reduce risk. In order to reduce risk, you must first identify various risks and determine how your organization will respond to each. Managing risk in alignment with business goals is a primary function of the security organization. Without sound risk management processes, the information security organization will not be able to justify investment decisions related to security improvements.

How

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. In any case, you should be able to look for evidence that the information security team is considering cybersecurity risks facing the company and making appropriate decisions in response. Some artifacts or processes that may demonstrate this include

- 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
- Corporate-level risk planning processes

Some questions you may want to consider around this step include

- 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?

All organizations should have a clear understanding of their cybersecurity risks and a process by which to prioritize security investments.

3. Evaluate the scope of the cybersecurity program and its relationship to other IT functions within the organization.

As discussed earlier, 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. Regardless of organization, though, some common functions should be present in most information security teams, whether it's a one-person show or an entire security department.

How

Obtain organization charts or other artifacts describing the makeup and function of the security team. Interview functional leaders to gather more information.

A security program should be expected to cover a minimal set of practices in some form or fashion, including

- **Policy and compliance management** Defining security guidelines for the company
- **Awareness** Getting relevant security information into the hands of people who may need it
- **Vulnerability management** Helping the organization understand the risks and criticality of potential exploits and assisting with remediation
- **Security monitoring** Collecting log and alert data and detecting potential security events in the environment
- **Incident response** Dealing with viruses, breaches, or other malicious activities and helping to return the business to a normal state

In smaller organizations, the security team may also be responsible for managing operational aspects of security, such as firewall management, web or e-mail security, client or endpoint security, access control, remote access, authentication, and more. In larger

organizations, these may be handled by a separate operations team or by a team that dual-reports to the security director.

As organizations grow, they may add other security functions, such as security architecture or penetration testing.

It is also important to ascertain whether separation-of-duties risks exist due to the organizational structure or makeup. For example, when a system administrator is also a security administrator, there is a higher risk that security controls may be bypassed or reconfigured for expediency.

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.

IT security policy sets a baseline of expectations for employees of the company. If policies don't exist or provide adequate coverage, employees are forced to make up their own rules regarding security-related issues. The same concept extends to computer systems, which require a standard by which system security can be evaluated. If IT security policies are too lenient, they will not provide adequate protection of the company's information assets. If they are too strict, they either will be ignored or will place unnecessary overhead and costs on the business.

If the IT security policies aren't communicated to employees, they won't be followed. Additionally, if compliance with those policies is not monitored and enforced, employees will learn quickly that the policies can be ignored with no consequences, causing the policies to become "suggestions" rather than requirements.

How

Verify Adequate Policy Coverage Obtain a copy of your company's IT security policies. Ensure that they adequately cover your company's IT environment. At a minimum, the policies should include coverage of the following areas:

- Acceptable usage of the company's information assets by employees (for example, whether employees can use their computers, the Internet, and e-mail for personal reasons)
- Data classification, retention, and destruction
- Remote connectivity (for example, overall network security and security requirements for virtual private network [VPN] and other forms of connection to external parties)
- Passwords
- Server security (such as security requirements for Unix and Windows servers)
- Client security (such as security requirements for desktops and laptops)

- Logical access (such as requirements for obtaining and granting access to systems)

Review the policies for adequacy based on industry standards and the specific needs of your company. The audit steps in the other chapters of Part II can be used as guidelines.

Specifically review the company's password policy. It should provide adequate guidelines dictating requirements for the composition of company passwords (for example, minimum of eight characters, combination of letters and numbers, difficult to guess, and so on), for aging company passwords (such as requiring that they be changed every 90 days), for locking accounts after a certain number of unsuccessful logon attempts, for timing out login sessions after a period of inactivity, and for retaining a password history so that previous passwords cannot be reused for a certain period.

Specifically review the company's logical access policy. It should provide adequate guidelines dictating requirements for every user to have a unique ID, for accounts to be suspended upon employee termination or job change, and for users to be granted the minimum access necessary to perform their jobs.

Verify Stakeholder Buy-In Ensure that key stakeholders were included during policy creation. Obtain a list of employees involved in the creation and approval of the IT security policies, such as IT organizations that are expected to comply with the

policy. If IT security policies are created in a vacuum by the IT security organization without involving others, they are likely to be viewed as unrealistic and will be ignored. Involvement from those who provide the day-to-day support of the IT environment will bring an important perspective to the policies and also will ensure buy-in from those who need to enforce and comply with the policies. Ensure that the IT security policies were approved by an executive, such as the CIO or CEO. This will provide the IT organization with the authority and backing necessary to enforce the policies.

Verify Processes Around the Policies Review processes for periodically reviewing and updating the policies to ensure that they keep up with the ever-changing IT environment. Look for evidence that these processes have been executed.

Review processes for periodically evaluating changes in the environment that might necessitate the development of new policies. Look for evidence that these processes have been executed.

Ensure that provisions have been made for obtaining approved exemptions from the policy. There inevitably will be occasions when people do not think that they can comply with the policy. A defined process should be in place whereby those people can formally request an exemption from the policy. They should be required to state why they need an exemption and define the compensating controls that will be put in place. The IT

security organization should facilitate the exception process, including providing a recommendation and an opinion on the risk presented by the request, but they usually should avoid making the final decision as to whether or not to accept the risk. Instead, it should be a business decision. Review the escalation policy for the exemption process and ensure that business (as opposed to IT) management is involved at some point, at least for the acceptance of significant risks. Ensure that the final decisions are documented and retained.

> **NOTE** Look for evidence that the IT security policies are communicated adequately to all company employees. Potential vectors include referencing the policies during new-hire orientation and/or having all employees periodically sign a statement that they have read and agree to the policies.

Review processes implemented by IT security and other IT organizations for monitoring compliance with the policies. Ensure that enforcement and escalation processes are in place that result in the correction of noncompliant situations. Review a sample of recent applicable compliance-monitoring reports, and ensure that significant issues were tracked to resolution.

5. Review the awareness and communications functions of the security team, reviewing methods to train employees on security risks and concerns.

Employees starting a new job will usually receive

training about the expectations for the role and appropriate methods to do the job. When this training includes security information, employees can be better equipped to avoid security risks in their daily work, improving the overall security posture of the organization. An effective security awareness program educates employees on security concerns at a level and in a manner appropriate to their job functions. Most awareness programs will include several key elements; these should be assessed for their presence and effectiveness.

How

Discuss the scope of the security awareness program with the individual in charge of that function. You should expect the following primary elements in a complete program:

- General security training for new employees
- Periodic security training for current employees
- Ongoing general security awareness
- Role-specific security training for designated functions (for example, software developers)

Depending on the industry, size, and maturity of the organization, you may also find

- Education about nuisance or malicious e-mail, including unsolicited commercial e-mail (usually called “spam”) and social engineering messages

(usually termed “phishing”)

- Exercises to test employee ability to detect phishing e-mails
- Training about specific data types, such as intellectual property or personally identifiable information (PII)

Review the processes for providing general security training for new hires. Review the content to ensure that basics are covered, such as employee expectations around security, information on company security policies, key areas of concern or risk for the company, how to report security issues, and so on. Sample records from training systems or orientations to ensure that employees attended or reviewed security material.

Ensure that training is provided on a periodic basis. Depending on risk level and industry requirements, organizations may be required to provide security training very frequently, but many companies mandate annual or biennial security training for current employees. Discuss how training is assigned, and review processes for ensuring that training is completed. This may involve reminders to employees or escalations to supervisors. Sample training records to ensure employees have taken required security training.

Discuss the ongoing security awareness program. Awareness teams usually provide periodic updates to employees on various security topics. These could be very general, focusing on good security hygiene like

password protection, or very specific, focusing on a new type of phishing message, for example. Ongoing security awareness may be delivered in various ways. Organizations may use posters, mass e-mail, web content, social media, or in-person presentations to raise security awareness. Obtain samples of this content as evidence of ongoing awareness efforts.

Specific roles in the organization, or individuals dealing with certain kinds of data or systems, may require additional training beyond the general information provided to all employees. For example, IT personnel may have access to more data on employees because they support those systems; additional training for IT personnel should be considered for these cases. Software developers should receive training on how to recognize and avoid software vulnerabilities in the code they write. Employees who handle PII or other personal data should be trained on any specific requirements for those data types. Any employee who comes in contact with the company's sensitive intellectual property should be trained on how to recognize and handle company data. Review the timing and content of these training programs. As with other periodic training programs discussed earlier, annual or biennial training should be considered the minimum standard for role-specific or data-specific training.

More mature security programs may also include phishing training and phishing exercises or assessments. As phishing and other forms of social engineering have

grown, companies have responded by educating employees on how to recognize and avoid falling victim to phishing. If your organization has a phishing awareness program, discuss the parameters of the program with the team. This may include

- Content and timing of phishing awareness training for employees
- Phishing exercises (tests) to assess the effectiveness of awareness training
- Metrics or escalation processes associated with phishing exercises
- Phishing exercises tailored for high-risk groups such as finance, HR, or IT
- Methods for employees to report suspected phishing messages

Review the results of phishing exercises over time, if applicable. An effective program should see improved results as time goes by. Companies vary in how they handle the results of phishing exercises; discuss any escalation processes with the awareness team to understand how "failed" exercises are addressed. Ensure that any disciplinary action taken as a result of phishing exercises is handled in accordance with company policies.

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.

If an organization takes no action to maintain its security posture on an ongoing basis, its risk over time will increase. Thousands of vulnerabilities are discovered in common software every year; what was thought to be secure a month ago is often known to be less secure today due to the ongoing discovery of security vulnerabilities. Malicious actors are always looking for an edge, and companies must have active vulnerability programs so that they can be aware of new threats and potential exploits, as well as ways to reduce risk.

How

Review the organization's approach in finding and resolving vulnerabilities. An effective program should have a few key elements, discussed next.

Awareness of new threats and vulnerabilities Interview the individual or team in charge of vulnerability management. Assess how the team becomes aware of newly discovered vulnerabilities in products common to the environment, such as operating systems or web browsers. Most commonly, security teams will subscribe to one or more feeds from organizations that distribute vulnerability information. For example, the United States Computer Emergency Readiness Team (US-CERT) publishes vulnerability information as part of its National Cyber Awareness System. Some organizations may use automated feeds

from organizations like the National Institute of Standards and Technology (NIST). In addition, most major software companies provide methods for advising customers of security vulnerabilities in their products. The team should have a method of receiving and consuming new vulnerability data relevant to the products known to be in the environment.

Besides receiving information on known vulnerabilities, security teams should also receive information on emerging threats. These often come in the form of subscriptions to third-party threat intelligence services. This content can include information on how new vulnerabilities are being exploited, attack methods and other exploit tactics seen in the world, and general security news. Determine through interviews with the security team whether an external threat intelligence service is used and how the information is received and integrated with other processes. For example, some intelligence feeds can be integrated with monitoring systems to enhance detection capabilities. It's important for security teams to be aware of emerging threats in order to take proactive steps to protect company assets.

Vulnerability scanning and other methods to identify known vulnerabilities in the environment Vulnerability scanning can be a very effective control to ensure that patching procedures, firewall settings, and other security processes are providing the intended level of protection. Scanning can

also be used to identify vulnerabilities that have not yet been mitigated. Common vulnerability scanners, like those available from Qualys, Rapid7, or Tenable, can identify applications on a system, find services answering on open network ports, and more. The system state is correlated with a known list of vulnerabilities to produce a report of potential system risks. All organizations should use a scanning tool or a third-party scanning service. If your organization doesn't have one, you may want to explore a free trial of one of the commercial tools listed earlier or consider an open-source tool like OpenVAS.

NOTE Some types of vulnerability scanners can also scan software for errors that lead to security flaws. These tools are often used with web-based applications and will assess how code is written or how web content is constructed to identify application-level risks. A comprehensive vulnerability management program should include both system-level and application-level vulnerability scanning. This section primarily discusses system-level scanning.

Discuss the vulnerability scanning program with the security team. Scanning programs often have two primary objectives:

- Ensure that newly deployed systems are free of known vulnerabilities at the time of deployment
- Ensure the ongoing security of deployed systems by checking for vulnerabilities on a periodic basis

Your company should have a vulnerability scanning

policy that lists timing requirements for scans, as well as the criteria for remediating issues discovered in a scan. For example, your policy may require that Internet-facing systems be scanned on a monthly basis and any vulnerability rated as “Medium” or higher must be resolved within seven days of discovery. The timing and criticality criteria will vary by company and risk tolerance, but some level of periodic scanning and risk remediation should take place.

Review scan records for both new systems and existing systems to ensure that systems are being scanned in line with company policy. A system may be scanned multiple times in the process of identifying and resolving vulnerabilities; a final, “clean” scan is an indication that all relevant vulnerabilities were mitigated.

Evaluation of discovered vulnerabilities Vulnerabilities published by software makers or by groups like US-CERT, as well as vulnerabilities identified by scanners, are usually assigned a severity rating, such as Low, Medium, High, or Critical. Organizations may decide to accept the external rating and work accordingly or employ a process to evaluate the risk based on their own situations. As most companies deploy multiple layers of protection in a defense-in-depth strategy, some vulnerabilities rated as Critical may not be as important once the full scope of defenses is taken into account.

Discuss with the vulnerability team whether published severity levels are evaluated independently of the external rating. Review the criteria for those decisions, and examine evidence of this activity. Common criteria include whether an exploit can occur remotely, whether there is evidence of active exploits in the world against a published vulnerability, whether a patch or other remediation is available, and the type of negative action that occurs as a result of the exploit.

Many organizations track metrics comparing the published severity level to the "judged" level. This can be particularly important for prioritization of remediation activity. A vulnerability judged to be Critical in nature might drive urgent action across the company, but if judged lower, might fall under routine maintenance or patching.

Processes to communicate and track results and actions Discuss how the vulnerabilities are resolved. In some organizations, the vulnerability management team may be in charge of mitigating discovered vulnerabilities. Other organizations may use an outsourced service. Some will turn over mitigation to the application teams responsible for each server. Whatever the case, there should be a clear process in place to scan systems and provide results to the appropriate teams.

Discuss how vulnerabilities are tracked to closure. Most organizations will track vulnerability status over time in order to ensure that teams take action as

directed. Obtain relevant metrics as evidence. Review what happens when a team is not able to resolve a vulnerability within the specified time frame.

7. Assess the security monitoring function of the security team, reviewing log collection and alert processing and detection capabilities.

Organizations frequently task a dedicated individual or team with monitoring the environment for adverse security events. Whatever the organizational structure, the company should have people, processes, and technology in place to review system data and identify security issues. The auditor should ensure that the monitoring group has the appropriate systems available and is taking necessary action to monitor the environment and protect the company.

How

Review the processes and technologies to collect and correlate system log data and alerts. Discuss the monitoring system with members of the security operations center (SOC) team. You should be able to identify the key systems and interfaces used by the team.

A key technical component of most SOCs is a security information and event manager (SIEM), which collects and correlates log data from many sources to find events of interest. A SIEM usually stores log data from different sources in the environment, such as firewalls, proxies, antivirus systems, authentication servers, and more. This data is transmitted from remote systems and stored

centrally. Review the SIEM policies to assess the amount of data stored, the sources used, and the retention time. While log sources can vary widely, a common data set will include the types of systems mentioned earlier. Retention time is dependent on the amount of storage available, but six to twelve months is a good reference point. SIEMs can be used to monitor for unusual input in near real time or can be used for forensic investigation, such as incident reconstruction.

Discuss with the SOC team how log data is protected from unauthorized access or manipulation. Access to read log data from the SIEM should be restricted to need-to-know individuals only; no one should have access or the ability to modify log data once stored in the SIEM. Ask the SOC to provide information on access controls for the log repository.

SIEMs and other tools in the SOC can be used to correlate data for the purposes of identifying unusual activity. Review the process for developing alerts from correlated data. Security events often happen right along with “normal” events, so it’s important for a SOC to develop alerts at a proper level. The team should have an ongoing process to improve the fidelity of alert systems and should be able to provide evidence based on previous events that justifies why a threshold or alert level was set in a particular way. In addition, if the team subscribes to a threat intelligence service, determine how that information is integrated with the SIEM or other detection systems to improve monitoring.

You should also discuss how actions or alerts are tracked to resolution. Some companies use an incident tracking system to manage alerts and security incidents. Others may track issues manually in spreadsheets. Request a sample of incidents from the system in use; you should be able to see an alert being tracked to closure. If a rule in the SIEM or other system is generating alerts and no one is taking action, you should question why that alert is being generated or why nothing is being done in response.

Outside of SIEMs and other tools in use by the SOC to detect events, employees may also notice suspicious activity. Ensure that a mechanism exists for employees to report security incidents or concerns and that those reports are tracked to resolution. Review a sample of recently reported incidents, and determine whether they were resolved adequately.

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.

Almost every alert, virus detection, or phishing report generates some kind of response. In many companies, the severity of the incident dictates the type of response. When a significant security event occurs, the team may invoke a formal incident response (IR) process. This ensures that the right steps are followed and the right people within the company are notified of the situation. As an auditor, you should review the IR function to

ensure that a documented process exists and will be followed should a security event occur.

How

Request a copy of the IR process. If the team does not have a documented IR process, you should try to assess how the organization would handle a larger-scale security event. Most organizations are well prepared to respond to a nuisance-level virus, for example, but if a ransomware incident affected half of the organization's systems and shut down business applications, how would the security team respond?

An effective IR plan should include the following components:

- Criteria for invoking different levels of response.
- Identification of key roles and responsibilities in the event of an incident. For example, an incident manager should be identified who would be "in charge" of the response process.
- Decision points for contacting other levels of the organization, including security management, IT management, business teams, legal advisors, communications teams, and others.
- Guidelines for the preferred course of action when dealing with certain event types. For example, incidents involving retail systems may drive a different response than incidents involving facilities systems. It's preferable to document

these scenarios in advance where possible rather than make decisions during the stress of an actual incident.

The plan should have been reviewed by security and IT management as well as other stakeholders, such as legal teams or risk officers.

9. Assess other functions of the security team as appropriate.

Larger or more mature organizations or those in specific industries may have other elements in their security programs. If those elements are not being executed with appropriate controls, they might not meet the objectives for which they were created.

How

Some example functions are listed next; you can use basic auditing principles, including interviews and gathering documentation, to determine if the function meets its stated objectives for the company. Security architecture teams often serve as consultants for other areas of IT or for the other security teams. Frequently having deep technical expertise in one or more areas, security architects have a broad understanding of security principles and can apply this knowledge to many problems. Most commonly, security architects will participate in or drive major security-related initiatives for the company or will engage with other IT teams to ensure security concerns are properly addressed in

project work.

Security infrastructure teams manage the devices and software responsible for providing much of the technical security for the company. These might include firewalls, web gateways, remote access systems, multifactor authentication platforms, authentication systems, identity and access management software, and more. Auditing many of these technologies is covered elsewhere in this book.

Security teams also have projects of their own and as a result may have project management activities within their scope. Sound project management practices are as important to the security effort as they are elsewhere in IT organizations. The elements in Chapter 17 on auditing company projects also apply to project teams within the security department.

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.

Although IT is responsible for providing the technology and mechanisms for protecting company data, a framework must be in place for making decisions as to what level of protection is necessary for any given data element (based on the criticality of the data). Without such a framework, there will be inconsistency in how data is protected, likely resulting in some data being underprotected (thereby placing critical information

assets at risk) or overprotected (leading to unnecessary costs). If the life cycle of data is not defined, it will lead to data being retained longer than necessary (resulting in additional storage costs and possible legal liabilities) or being destroyed prematurely (leading to potential operational, legal, or tax issues).

How

Review the company's data classification policy. It should have provisions for identifying owners for all critical company data. It also should provide a framework for classifying that data based on its criticality (for example, confidential, internal data, public data). This framework should provide specific definitions of each classification level, along with specific requirements for how data at each level should be protected (for example, encryption).

Review evidence that the data classification policy has been implemented. Look for a list of data owners and documentation indicating that those owners have classified their data. For a sample of this data, review evidence that protection has been implemented in alignment with the classification.

Determine whether life cycle information has been created for company data. For a sample of major data elements, review documentation of the data's life cycle requirements, including retention, archive, and destruction requirements. Ideally, requirements will be identified for how long the data should be active (online,

easily accessible, modifiable if appropriate, and backed up periodically), when and for how long they should be archived (possibly offline, not necessarily easy to access, no longer modifiable, and no longer backed up periodically), and when they should be destroyed.

Review evidence that life cycle requirements have been implemented.

11. Determine how security policies and security risk are handled in organizational IT processes.

A firm can have the best security team with the best policies and a great awareness and vulnerability program, but if the organization-at-large doesn't account for security concerns in broader processes, security problems may arise that could have been avoided. As an auditor, you should ensure that various functions of the business, particularly in the IT space, understand security requirements and involve the security team when questions arise.

How

Discuss IT processes with members of your IT department's operations or development teams. Ask how security issues are addressed during project planning, and determine whether the security team is involved in aspects of IT project work. If there is a formal project approval process, determine if the information security team participates in the approvals.

Vulnerability management and software patching go hand in hand, and teams that are responsible for system

administration or software development should be able to demonstrate via patch schedules that software vulnerabilities are being mitigated. Software development teams should also use security scanning tools to identify potential vulnerabilities during software creation.

If your company has a security architecture function, determine how it engages with the broader portfolio of IT efforts. Security architects can help address potential security concerns early in a project and ensure that strategic security concerns are taken into account.

In general, each area of the organization should have an understanding of security policies and should be able to articulate how those policies are being addressed in their processes.

As you review Chapter 17 on auditing company projects, consider how cybersecurity concerns are addressed as part of project management.

12. Review and evaluate processes for ensuring that security personnel have the skills and knowledge necessary for performing their jobs.

As discussed in the previous chapter, if employees are not qualified to perform their jobs, the quality of the work they do will be poor. This is no different for the information security team. If mechanisms are not in place for maintaining and enhancing the knowledge and skills of security personnel, their knowledge can become outdated and obsolete.

How

Review human resources (HR) policies and processes as they relate to the security team. These may be the same as processes covered for IT in the previous chapter. Look for mechanisms that ensure that qualified people are hired and that provide for continuous enhancements of employee skills and knowledge. Review evidence that these policies and processes are followed. Here are some examples:

- Ensure that job descriptions exist for all positions and that the job descriptions specifically state the knowledge and skills required for each job. Review evidence that these job descriptions are referenced during the hiring process. Review processes for keeping the job descriptions up to date.
- Review the security team's training policies and ensure that they provide the opportunity for employees to attend training classes and seminars for enhancing and updating their skills and knowledge. Look for evidence that employees have taken training over the past year.
- Review performance-review processes. Look for evidence that employees are receiving regular feedback on their performance. Ensure that processes exist for identifying poor performers, coaching them, and moving them out of the organization if performance does not improve. Conversely, ensure that processes exist for

identifying top performers, rewarding them, and providing them with incentives to remain at the company.

13. Assess that metrics are collected commensurate with the goals of the security program and that metrics are reported to appropriate management personnel.

Performance-based organizations are fond of saying "you get what you measure." Metrics help an organization track various aspects of its performance, which can help drive decisions about investments in people, processes, or technologies. Metrics can take a number of different forms, from simple instrumentation (for example, how many e-mails are blocked as spam in a week) to maturity or capability (for example, mean time to remediate known vulnerabilities). Security teams should track metrics to improve their own operations but should also consider metrics to share with stakeholders. These may not always be the same items. As an auditor, you should identify the metrics that are collected, with whom they are shared, and what the organization does with them.

How

Obtain metrics from the owners of the various security services the organization provides. As you review the metrics, you should consider whether the organization takes action based on the metrics, or if the item is for instrumentation purposes only. While there is much debate in security circles about the effectiveness of

different metrics, some you might commonly find include

- Number of security incidents
- Mean time to detect/mean time to resolve incidents
- Alerts from various security systems, such as antivirus software, data loss prevention systems, network firewalls, web application firewalls, and others
- Number of exceptions to security policies
- Percentage of systems patched/unpatched
- Number of vulnerabilities found/resolved/unresolved
- Expenses of the security program

If no or few metrics are collected, you will want to understand whether there is a technical limitation, or whether the team views those metrics as not helpful or interesting.

Metrics can also take the form of maturity measurements against external assessments or external standards. For example, if an organization employs an implementation standard such as NIST 800-53, metrics could show a percentage of compliance to that standard. Similar metrics could be created against the Center for Internet Security's Critical Security Controls, standards like ISO 27001, the NIST Cybersecurity Framework, and others. Metrics of this type can help identify gaps in a

program and prioritize investment areas.

For any metric, it's important to understand who is consuming the data. If a measurement is not being reviewed or acted upon, it has very little value to the organization. Metrics that are of interest to system administrators will be different from those of interest to senior executives, but the organization should be able to provide metrics suitable for different audiences. If metrics are not being presented to management, an auditor should ask how the value of the program is understood by those managers.

14. Review processes around the use of managed security service providers (MSSPs) within the security team.

As discussed in Chapter 3, many companies outsource various IT support processes, and this can include parts of the security program. If these vendors are not selected and managed appropriately, the service may not meet the needs of the organization. Depending on what portions of the security function have been outsourced, these problems could reduce the effectiveness of the security team and increase company risk.

MSSPs commonly provide monitoring services for specific elements of a program. For example, an MSSP might receive all employee reports of spam or phishing and may perform a triage function to identify those that need additional attention. Some organizations may outsource their entire security operations center to an MSSP. Smaller organizations may leverage MSSPs to

gain specific expertise, while larger organizations may use them to offload some functions and allow internal resources to focus on other efforts.

The audit steps for this item are also covered in Chapter 3 but are listed here for completeness.

How

Review the process for selecting vendors. Ensure that the process requires soliciting multiple competitive bids, the comparison of each vendor against predefined criteria, involvement of knowledgeable procurement personnel to help negotiate the contract, evaluation of the vendor's technical support capabilities and experience providing support for companies of similar size and industries as yours, performance of a thorough cost analysis, and investigation of each vendor's qualifications and financial health. For a sample of recent vendor selections, review evidence that the process was followed.

Ensure that contracts with third-party service providers specifically define the roles and responsibilities of the vendor and include defined service level agreements (SLAs). For security services, this may include delivery of metrics or reports related to the service. Review a sample of contracts for evidence that expectations have been specifically defined.

Ensure that contracts include nondisclosure clauses, preventing the vendor from disclosing company information. While this may be critical in many areas of

the company, a disclosure of security-related information can be damaging, as sensitive vulnerability data or investigation-related information could be used maliciously by outsiders. Also ensure that contracts include right-to-audit clauses that allow you to audit vendor activities that are critical to your company. Review a sample of contracts for evidence that these clauses are in place where applicable.

Review processes for monitoring the performance and providing oversight of existing third-party service providers. For a sample of existing vendors, look for evidence that they are being monitored for compliance with SLAs and that they are performing the responsibilities defined in the contract.

15. Determine how the organization ensures that its security controls are effective.

When protecting its information assets, a business may consider hundreds of different security controls. Even the most secure organizations in the world don't implement every possible defense or control; whether due to cost, complexity, or a trade-off on usability or employee acceptance of a control, a certain set of controls is implemented. From the steps discussed earlier, you should be able to determine both how the organization sees risk and how it prioritizes mitigations. But how does a group know that what it has implemented will be effective in meeting its security needs?

Independent assessments, including attestations or certifications, external audits, incident response exercises, and penetration testing, can examine the effectiveness of controls and provide visibility to gaps.

Independent attestations or certifications may involve visits by external audit teams and may relate to widely known evaluations such as Statement on Standards for Attestation Engagements (SSAE) or the International Organization for Standardization (ISO). Within these families are many areas for control evaluation, but the most relevant for these purposes are the ISO 27000 series, dealing with information security management systems, and the System and Organization Controls (SOC) attestations of SSAE. In either case, a review of the security function and the various controls in place is performed by an external team. In the case of SSAE/SOC, some types of reports include evaluating the operational effectiveness of security controls.

External audits will include many of the same elements defined in this book. Depending on the scope and purpose of such an audit, the assessment could include detailed control evaluations. In an ideal case, an internal auditor and an external auditor would find the same sets of controls and potential gaps. Having an external audit provides an additional layer of independence to assure management that the audit is free from undue influence and represents an accurate picture of the control landscape.

Incident response exercises are intended to test the

ability of the incident response team to handle various types of events by evaluating processes used by that team. An incident response exercise should involve various members of the response team as well as individuals or teams that might be affected by a major security event, such as legal teams, HR or privacy, operational teams, communications, and others as appropriate. This type of exercise can ensure that teams communicate adequately and that response processes are properly documented and followed.

Penetration testing is probably the best way to evaluate the security controls of an organization. Penetration tests, or "pen" tests, provide assurance that a control can withstand an effort by a determined individual or team to defeat that control. A pen test might involve social engineering, physical probing, vulnerability scanning, use of known or unknown exploits, and more. These tests are usually performed by skilled individuals under specific rules of engagement determined by the parties involved. Pen tests may be conducted against a specific target or for a certain goal (evaluating a particular high-value application), or may be more general in nature (assessing perimeter defenses).

An auditor should evaluate the presence, scope, and frequency of independent assessments, as well as the processes used to handle the results of those evaluations.

How

Determine through interviews of the CISO or delegates which types of independent assessments, if any, are used by the organization to evaluate its security program. Examine the artifacts produced by these efforts to ensure they include actual testing of controls.

Review how the results are processed and resolved. The results of any external evaluation should include recommendations on how the organization can improve. While these are only recommendations, the organization should have some process to consider the information and determine how to proceed. One common practice is to review the results with appropriate management teams and align on which recommendations will be addressed. Actions resulting from these discussions should be tracked to closure.

KNOWLEDGE BASE

As mentioned throughout this chapter, the composition and scope of information security programs will vary from company to company. However, many reference sources are available on security policy models, management structures, and more. Information on security program best practices is available at sources including SANS (www.sans.org), the Information Systems Audit and Control Association (ISACA, www.isaca.org), and the Institute of Internal Auditors (IIA, www.theiia.org). The ISO publishes standards (available for a fee), including ISO 27001, that describe information security management systems. Finally, your

external auditors likely will have some information to share with you on this topic.

The following table lists various resources where you can find more information about the topics in this chapter.

Resource	Website
Information Systems Audit and Control Association	www.isaca.org
Institute of Internal Auditors	www.theiia.org
National Vulnerability Database	https://nvd.nist.gov
United States Computer Emergency Readiness Team (US-CERT)	www.us-cert.gov
SANS	www.sans.org
Common Vulnerabilities and Exposures (CVE)	cve.mitre.org
National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)	www.nist.gov/cyberframework
International Organization for Standardization (ISO) 27001	www.iso.org/isoiec-27001-information-security.html
The Center for Internet Security	www.cisecurity.org
Computer Security Resource Center	https://csrc.nist.gov

MASTER CHECKLIST

The following table summarizes the steps listed herein for auditing cybersecurity programs.

Auditing Cybersecurity Programs

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.