CHAPTER 3

Auditing Entity-Level Controls

In this chapter we will discuss how to audit entity-level controls, which are pervasive across an organization. We will be discussing the auditing of *information technology* (IT) areas such as

- Strategic planning and technology roadmaps
- Performance indicators and metrics
- Project approval and monitoring processes
- Policies, standards, and procedures
- Employee management
- Asset and capacity management
- System configuration change management

BACKGROUND

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. This chapter discusses areas that the auditor should expect to see centralized in an organization. If the topics covered in this chapter are not centralized, or at least centrally coordinated, at your company, questions as to

their overall effectiveness should arise. Most of these topics set the overall "tone at the top" for the IT organization and provide governance of the entire IT environment. If they are not centralized and/or standardized, the auditor should question the ability of the overall IT environment to be well controlled.

What is and is not considered an entity-level control is not always consistently defined and will vary by organization, depending on how the IT environment is defined. An area that is an entity-level process at one company will not necessarily be an entity-level process at another company. 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.

For example, Chapter 5 covers the topic of auditing data centers and areas such as physical security, environmental controls, system monitoring, and so on. Many companies have multiple decentralized data centers, meaning that these controls are not centralized for those companies. However, some companies have one data center and one set of processes for executing these areas, so physical security, environmental controls, and system monitoring would qualify as entity-level controls because they are centralized and pervasive. (However, such areas are not covered in this chapter, as they are covered in Chapter 5.) Auditors must use good judgment and knowledge of the company to determine what is and is not an entity-level control.

As mentioned earlier, the topics covered in this chapter should be centralized to a large degree because they provide for the core principles of IT governance. If these areas have no central coordination, the auditor should dig deep before signing off as to their effectiveness. Put another way, the areas covered in this chapter should be considered the minimum for an entity-level controls review. Other areas (such as data center operations) might be added based on the environment at your company.

NOTE 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. Conversely, weak entity-level controls increase the likelihood that controls will be weak throughout the organization, because upper management has not demonstrated and communicated to the organization that internal controls are valued. This often leads to inconsistency at the lower levels, because the personalities and values of lower-level managers will be the sole determining factors in how seriously internal controls are taken within the organization.

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.

TEST STEPS 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.

A poorly defined IT organization structure can lead to confusion regarding responsibilities, causing IT support functions to be performed inefficiently or ineffectively. For example, critical functions may be either neglected or performed redundantly.

Also, if lines of authority are not clearly established, it can lead to disagreement as to who has the ultimate ability to make a final decision. Finally, if IT duties are not segregated appropriately, it could lead to fraudulent activities and affect the integrity of the company's information and processes.

How

A "one size fits all" model for an IT organization doesn't exist, and you can't mechanically use a checklist to determine whether your company's IT organization is adequate. Instead, you must view the overall organization and apply judgment in determining whether it adequately addresses the most essential elements. With this in mind, the following discussion covers some key areas to consider during this review.

Review IT organization charts and ensure that they

clearly indicate reporting structures. The organization charts should provide an indication as to where in the company the various IT organizations meet. For example, in most companies, all IT organizations eventually report to the chief information officer (CIO) so that one ultimate authority is able to set rules for the overall IT environment. Ensure that your company has IT organization reporting structures that eventually report to a single source that is “close enough” to day-to-day IT operations to allow for effective governance and direction setting. If the IT organizations report to multiple CIOs or consolidate only to a high-level executive such as the chief executive officer (CEO), additional processes will likely be needed to develop an effective method for establishing overall policies, priorities, and governance for IT at the company. Otherwise, it is likely that “fiefdoms” will exist within IT, preventing the establishment of true entity-level IT controls.

Review IT organization charts and charters and ensure that they clearly delineate areas of responsibility. Determine whether it is clear how responsibilities are divided between organizations, or evaluate whether there is significant opportunity for confusion and overlap. In addition to reviewing documented organization charts and charters, consider interviewing a sample of IT employees and customers to determine whether there is a consistent understanding of the division of responsibility.

Evaluate the division of responsibilities within the IT organization to ensure that duties are segregated appropriately. You also should consider criticality in making judgments. It is more important that separation of duties be in place over critical financial systems than over systems providing support for minor convenience functions (such as the company's internal training system).

> **NOTE** The specifics of which duties should be segregated from others will vary by company; however, the general idea is that the responsibilities for initiating, authorizing, inputting, processing, and checking data should be segregated so that one person does not have the ability to create a fraudulent transaction, authorize it, and hide the evidence. In other words, you're attempting to prevent one person from being able to subvert a critical process.

Following are some basic general guidelines that can be considered during the review. Again, this should not be used as a mechanical checklist, and the auditor should review for compensating controls when investigating potential exceptions.

- **IT personnel should not perform data entry.** Keep in mind that IT organizations differ in their composition across companies, so some data-entry personnel may be classified as IT in their companies. In this case, we're referring to IT personnel who are performing true systems support.

- **Programmers and those performing run/maintain support for systems should not directly be able to modify production code, production data, or the job-scheduling structure.** As with all these statements, when a segregation-of-duties issue seems apparent, the auditor should look for compensating controls before determining whether it is a true issue. Access to production data and code may not be a large risk if strict accountability and change-control procedures are in support of that access.
- **Programmers and those performing run/maintain support for systems should be separate from those performing IT operations support (such as support for networks, data centers, operating systems, and so on).**
- **An information security organization should be responsible for setting policies and monitoring for compliance with those policies.** This information security organization should have no operational responsibilities outside of those related to information security.

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.

To provide for long-term effectiveness, the IT organization must have some sort of strategy regarding where it plans to go, as opposed to being in reactive mode constantly, where day-to-day issues and crises are the only considerations. The IT organization must be aware of upcoming business needs and changes in the environment so that it can plan and react accordingly. It is important that IT priorities align with business priorities. Too many IT organizations lose sight of the fact that their only reason for existence is to support the company in meeting its business objectives. Instead, these IT organizations focus on becoming a "world-class IT shop," even when this goal doesn't directly support the overall company objectives. It is critical for IT organizations to stay grounded by tying their objectives to the company's objectives.

How

Look for evidence of a strategic planning process within IT, and understand how that planning is performed. Determine how company strategies and priorities were used in developing the IT strategies and priorities. Review documented short- and long-term IT priorities. Evaluate processes in place for periodically monitoring for progress against those priorities and for reevaluating and updating those priorities.

3. Determine whether technology and application strategies and roadmaps exist, and evaluate processes for long-range technical planning.

IT is a rapidly changing environment, and it is important that IT organizations understand and plan for change. Otherwise, the company's IT environment runs the risk of becoming obsolete and/or not fully leveraging technology to benefit the company.

How

Look for evidence that long-term technical planning is being performed. For purchased applications and technologies, determine whether IT understands the vendor's support roadmap for those products. The IT organization should understand when their versions of the products will cease to be supported and create plans for either upgrading or replacing the products. Determine whether processes are in place to monitor for changes in relevant technologies, consider how those changes will affect the company, and look for opportunities to use new technologies to help the company.

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.

The IT organization exists to support the business and its day-to-day operations. If minimum standards of performance are not established and measured, it is

difficult for the business to determine whether the IT organization's services are being performed at an acceptable level.

How

Obtain a copy of any metrics being captured for the IT organization's routine activities (such as system uptime and response time). Determine the goals for those metrics, and ensure that the appropriate stakeholders have approved those goals. If actual performance is significantly inferior to goals, determine whether root-cause analyses have been performed to understand the problem and whether plans are in place to solve the problem.

Review any SLAs (service level agreements) that have been established for supporting IT's key stakeholders. Ensure that processes are in place for measuring actual performance against the requirements of the SLA and for correcting any deviations.

Ensure that processes are in place for establishing budgets and for holding the IT organization accountable for meeting its budget. Obtain copies of the IT budget for the current and preceding years, as well as copies of any "budget versus actual" analyses. Determine how any significant variances were reported and resolved.

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.

Without a structured process for approving and prioritizing new IT projects, IT resources probably will not be deployed efficiently. Instead, they will be assigned on an ad hoc basis to whatever potential project comes up next. Also, IT projects may commence that do not meet the needs of the business and/or that are not as important as other potential projects to which those resources could be deployed. Without a structured process whereby management and key stakeholders periodically review the project's progress, it is more likely that the project will get off track and fail to meet key goals and milestones.

How

Review any available documentation regarding the project proposal and approval process. Evaluate the process for potential holes that might allow a project to commence without approval. Look for evidence that proposed projects have been prioritized prior to approval and that some discipline and commonality exist within this approval process. Consider selecting a sample of active IT projects and obtaining evidence that those projects went through an appropriate process of proposal, prioritization, and approval. Review evidence that management and key stakeholders are periodically

reviewing the status, schedule, and budget for active IT projects. Ensure that the project approval process calls for a thorough cost analysis before project commencement so that management can make an informed decision regarding expected return on investment (ROI) for the project. These cost analyses should consider not only the project start-up costs but also ongoing costs, such as software maintenance, hardware maintenance, support (labor) costs, power and cooling requirements for system hardware, and so on. This element is often omitted erroneously, leading to misinformed decisions. Start-up costs are only a fraction of the total ongoing costs for implementing a new system. A multiyear (five years is often a good target) total cost model should be developed as part of the initial project analysis.

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.

If standards are not in place and enforced in the IT environment, projects probably will be executed in an undisciplined fashion, quality issues will exist in developed or purchased products, and the IT environment will be unnecessarily diverse (leading to increased support costs and potential interface issues).

How

Determine whether documented standards govern areas such as the following. If so, review those standards and ensure that they are adequate.

- **Project management** See Chapter 17 for guidelines regarding key elements that should exist within project management standards.
- **Software development** Standards should exist governing the development of code, including standards for naming, revision history, comments, and calls to other programs. Without such standards, the time and effort required for one person to support and troubleshoot another person's code increase significantly. Note that depending on the size of the IT organization, it may be acceptable for programming standards to be decentralized to a degree. However, each significant development organization should have a set of standards. See Chapter 17 for guidelines regarding key elements that should exist within these standards.
- **System configuration** This would include standard configuration for laptops, desktops, servers, and common user software packages. Common configuration will help ensure that the systems are supportable and that they have the appropriate security settings.
- **Hardware and software** Standards should exist governing the hardware and software that are

approved and supported for use in the company. This should include the specific versions that are supported. Otherwise, the IT environment likely will consist of a multitude of products performing similar functions, driving up IT support costs and leading to problems with the ability of the various products to interface with each other.

- **Quality assurance standards** Standards should exist that ensure that the development process includes the evaluation of security risks and internal control requirements.

Look for evidence that these standards are communicated to all relevant IT employees, and determine how these standards are enforced.

NOTE Consider reviewing a sample of recent and active IT projects for evidence that the standards were followed. Consider reviewing a sample of systems for deviations from configuration, hardware, and software standards.

7. Review and evaluate risk-assessment processes in place for the IT organization.

Without these processes, the IT organization will be unaware of risks to the achievement of its objectives and therefore will not have the ability to make conscious decisions regarding whether to accept or mitigate those risks.

How

Some overlap exists between this step and some of the other steps mentioned in this chapter, many of which are designed to determine how the IT organization is evaluating its own risks. You might consider this step to be adequately covered without explicitly performing it. However, you should look for evidence that the IT organization is periodically considering the risks to the IT environment and making conscious decisions as to whether to accept, mitigate, or avoid those risks. Risk-assessment mechanisms could include the following:

- Monitoring internal controls in the IT environment, including internal audits and self-assessments
- Performing formal threat and risk assessments of critical data centers and systems
- Performing periodic reviews of the strategic IT plans and technical roadmaps and assessing risks to the achievement of those plans
- Monitoring compliance with information security policies and other relevant IT policies

8. Review and evaluate processes for ensuring that IT employees at the company have the skills and knowledge necessary to perform their jobs.

If employees in the IT organization are not qualified to perform their jobs, the quality of IT services will be poor. If mechanisms are not in place for maintaining and enhancing the knowledge and skills of IT employees,

their knowledge can become outdated and obsolete.

How

Review human resources (HR) policies and processes as they relate to IT employees. 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 IT 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 IT organization'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 IT employees have individual training plans and/or evidence that they have taken training over the past year.
- Review performance-review processes. Look for evidence that IT 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.

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.

If your company is found to be in violation of applicable laws and regulations (such as Health Insurance Portability and Accountability Act [HIPAA] and Sarbanes-Oxley), it could face stiff penalties and fines, a damaged reputation, lawsuits, and possibly cessation of the company. If a robust process is not in place for monitoring the regulatory environment, the company may be unaware of new laws and regulations, resulting in noncompliance.

How

Look for a single point of contact that is responsible for monitoring the regulatory environment and its impact on IT. This person or organization should be responsible for identifying laws and regulations that apply to the company's IT environment, ensuring that the responsibility for complying with those rules has been explicitly assigned to the appropriate organization(s), and monitoring the regulatory environment for additions and changes that will affect the company. If no single person or organization is responsible for this (or a small

subset of people, each with a specific regulatory domain to cover), it likely will be done on an ad hoc basis, providing no assurance of full coverage. Review the processes used to monitor the regulatory environment, and evaluate their effectiveness. Obtain a list of IT-applicable regulations that have been identified, and look for evidence that responsibility for compliance with those regulations has been assigned and is being monitored. See Chapter 20 for more information on laws and regulations that may be applicable to your company.

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.

Because the IT environment exists to support the company's employees in performing their jobs, it is critical that processes exist whereby those employees can provide input into the quality of service they are receiving. Otherwise, the IT organization may be misaligned with its users and not be aware of it.

How

Ensure that a helpdesk function provides end users with the ability to report problems. Review and evaluate processes for capturing problems and ensuring that they are tracked to resolution. Obtain a list of recent tickets and select a sample, ensuring that all tickets were resolved and that no tickets were closed without the

consent of the user who entered the ticket.

Ensure that a process exists for obtaining end-user feedback after tickets are closed. Look for evidence that user-satisfaction metrics are kept and that management follows up on end-user feedback.

To ensure that the helpdesk does not seek customer satisfaction at the expense of security, review policies and processes for obtaining proper approvals prior to responding to user requests for having passwords reset and for obtaining system access. Review a sample of these sorts of tickets, and ensure that proper processes were followed and approvals obtained.

Look for the existence of customer steering teams to provide input and prioritization of IT projects and enhancements. For significant areas of the business, key stakeholders should be identified to provide guidance to the IT organization regarding projects and decisions that affect them. Otherwise, the IT organization will be making decisions in a vacuum and likely will work on projects or enhancements that do not provide the greatest value for the business.

Review any SLAs that have been established for supporting IT's key stakeholders. Ensure that processes are in place for measuring actual performance against the requirements of the SLA and for correcting any deviations.

11. Review and evaluate processes for managing third-party services, ensuring that their roles and

responsibilities are clearly defined and monitoring their performance.

Many companies outsource some or all of their IT support processes, including areas such as PC support, web server hosting, system support, programming, and so on. If these vendors are not managed appropriately, it can lead to poor service and unacceptable quality in the IT environment. Depending on what portion of the IT environment has been outsourced, these problems could significantly affect the company's operations.

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 SLAs. 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. 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.

See Chapter 16 for more details on auditing outsourced operations.

12. Review and evaluate processes for controlling nonemployee logical access.

Most companies employ some level of outsourcing and contract labor to supplement their internal workforce. Also, some companies allow third-party vendors a degree of logical access to purchased systems for troubleshooting and support purposes. Because these personnel are not employees of the company, they are less likely to have a personal investment in the company's success or an awareness of the company's policies and culture. If their access to company information assets is not governed, and if expectations regarding their use of that access are not communicated,

it is more likely that company information assets will be exposed unnecessarily or misused.

How

Ensure that policies require approval and sponsorship from an employee prior to a nonemployee obtaining logical access to company systems. If feasible, obtain a sample of nonemployee accounts and validate that they have appropriate approval and sponsorship.

Review and evaluate processes for communicating company policies (including IT security policies) to nonemployees prior to granting them system access. Look for evidence that this communication has taken place. For example, if all nonemployees are required to sign a statement that they have read and agree to the policies, pull a sample of nonemployees and obtain copies of these agreements.

Review and evaluate processes for removing logical access from nonemployees when they have ceased to work with your company or otherwise no longer need access. Consider obtaining a sample of current nonemployee accounts and validating that those nonemployees are still working with your company and still have a need for their current level of access.

Ensure that nondisclosure agreements (NDAs) are signed by nonemployees to legally protect your company from inappropriate use of company data. Pull a sample of nonemployee accounts and obtain a copy of the NDAs for them.

Ensure that consideration has been given to identifying data that should not be accessed by nonemployees and activities that should not be performed by nonemployees. For example, your company may decide that access to certain levels of financial data should never be granted to nonemployees. Or it may decide that nonemployees should never be granted system administration duties. The answer will depend on your company's industry and philosophies; however, an evaluation process should take place, and the results of that evaluation should be documented in company policy and enforced. This evaluation should be part of the data classification effort described in Chapter 4 and should drive the restrictions on nonemployee logical access.

13. Review and evaluate processes for ensuring that the company is in compliance with applicable software licenses.

Using software illegally can lead to penalties, fines, and lawsuits. It is increasingly easy for company employees to download software from the Internet. If companies do not develop processes for preventing or tracking such activity (as well as tracking the use of company licenses for purchased software), they can find themselves subject to software vendor audits without the ability to account properly for the company's use of the vendor's software.

How

Look for evidence that the company maintains a list of

enterprise software licenses (such as for Microsoft Office, ERP application accounts, and so on) and has developed a process for monitoring use of those licenses and complying with the terms of agreement. Determine how decentralized (nonenterprise) licenses are monitored and tracked. This would include software purchased by employees and placed on their company computers, as well as software downloaded from the Internet. Truly comprehensive software asset management requires a centralized database that contains information on exactly what software the company has the right to use (licenses purchased) and on exactly what software is being used in the environment (licenses used) and can compare the two. Test the effectiveness of the method used at your company either by performing your own scans on a sample of computers or by reviewing evidence from the company's processes.

14. Review and evaluate controls over remote access into the company's network (such as VPN and dedicated external connections).

Allowing remote access to a network basically results in that network being extended beyond its normal confines, bypassing normal perimeter controls such as firewalls. A lack of strong controls regarding this access can result in inappropriate access to the network and a compromised network.

How

Ensure that strong authentication (e.g., multifactor

authentication) is required for remote access and that these credentials are transmitted over secure (such as encrypted) communication channels. Question any remote authentication schemes that require only an ID and password. IDs and passwords can and will be compromised, so they alone are not enough for verifying the identify of a user. Multifactor authentication requires at least two factors, such as a password plus a physical or virtual token, in order to authenticate, reducing the risk posed by a compromised password.

Determine whether approval processes are in place for granting remote access, especially for nonemployees. Pull a sample of users with remote access and look for evidence of approval. Also evaluate processes for removing remote access accounts when employees leave the company. Pull a sample of users with remote access and ensure that they are still active employees.

Evaluate controls for ensuring that dedicated external connections to business partners are removed when no longer needed. Work with the appropriate IT organization (for example, the network team) to pull a sample of current connections and, by means of interviews and documentation review, determine whether they are still legitimately necessary.

Evaluate controls for ensuring that unauthorized connections cannot be made to the network and/or for detecting them if they are. Evaluate controls for ensuring that unauthorized connection points cannot be placed on the network and/or for detecting them if they are.

Ensure that policies provide minimum security requirements that should be met by all machines accessing the network remotely. This should include requirements for operating system patch level and antimalware protection. Look for preventive or detective controls that enforce these requirements.

Ensure that machines that are remotely accessing the network are not permitted to be dual-homed, which would bridge networks. This should be enforced technically where possible and by explicit agreement otherwise.

15. Ensure that hiring and termination procedures are clear and comprehensive.

Hiring procedures ensure that employees are submitted to drug screens and background checks, where local laws permit, prior to beginning work within an organization. Termination procedures ensure that access to company systems and facilities is revoked before a disgruntled employee can cause damage and that company property is returned. Inadequate hiring or termination procedures would expose the company to sabotage or abuse of privileges that could result in an information security compromise.

How

Review HR policies and procedures for the hiring and termination of employees. Ensure that hiring procedures include background checks, drug screens, and confidentiality agreements. Ensure that termination

procedures include physical and logical access revocation, return of company-owned equipment, and, where appropriate, supervision while the former employee collects his or her belongings.

16. Review and evaluate policies and procedures for controlling the procurement and movement of hardware.

Asset management is the controlling, tracking, and reporting of organizational assets to facilitate accounting for the assets. Without effective asset management, the company will be subject to the increased expense of duplicate equipment in situations where equipment is available but unaccounted for. The company will also be subject to unnecessary lease expenses if leased equipment is not adequately tracked and returned on time. Similarly, without adequate asset management, end-of-life equipment conditions may not be noted, resulting in increased risk of hardware failure. Additionally, theft of equipment that is not tracked likely would go unnoticed. In the context of this step, the assets being referred to are computer hardware, such as desktops, laptops, servers, and so on.

How

Review and evaluate the company's asset management policies and procedures, and ensure that they encompass the following:

- **Asset procurement process** Ensure that this

process requires appropriate approvals prior to the purchase of hardware.

- **Asset tracking** Ensure that the company is using asset tags and has an asset management database.
- **Current inventory of all equipment** Ensure that an inventory contains the asset number and location of all hardware, along with information about the equipment's warranty status, lease expiration, and overall life cycle (that is, when it is no longer eligible for vendor support). Ensure that an effective mechanism is in place for keeping this inventory up to date. A sample of asset tags also should be inspected visibly and tied back to the inventory.
- **Asset move and disposal procedures** Ensure that unused equipment is stored in a secure manner. Also ensure that data is erased properly from equipment prior to its disposal.

17. Ensure that system configurations are controlled with change management to avoid unnecessary system outages.

Configuration change management ensures that system changes are controlled and tracked to reduce the risk of system outages. It includes planning, scheduling, applying, and tracking changes to systems for the purpose of reducing the risk of those changes to the environment.

How

Change activities can affect two areas: hardware and software (including operating system–level changes). Ensure that the configuration management procedures include processes for the following:

- Requesting changes (including processes for end users to request changes)
- Determining the specifics of what should change
- Prioritizing and approving proposed changes
- Scheduling approved changes
- Testing and approving changes prior to implementation
- Communicating planned changes prior to implementation
- Implementing changes
- Rolling back (removing) changes that don't work as expected after implementation

Also review change-control documentation to verify that changes are fully documented, approved, and tracked. Approvals should incorporate a risk assessment and typically are granted by a committee made up of stakeholders. You should be able to obtain a sample of change-control requests, as well as other configuration management documentation, from IT management.

18. Ensure that media transportation, storage, reuse, and disposal are addressed adequately by

company-wide policies and procedures.

Media controls ensure that information on data-storage media remains confidential and is protected from premature deterioration or destruction. Inadequate media transportation, storage, reuse, and disposal policies and procedures expose organizations to possible unauthorized disclosure or destruction of critical information. One increasingly common type of security incident is the loss of backup media in transit by third-party carriers. A number of high-profile companies have fallen victim to this threat in recent years and have incurred losses due to legal actions, reputation damage, and incident response costs.

How

Computer media, including but not limited to backup tapes, CDs and DVDs, hard disks, and USB drives, must be strictly controlled to ensure data privacy. Since backup operators, computer technicians, system administrators, third-party carriers, and even end users handle storage media, media policies and procedures should address these disparate roles. When auditing media control policies and procedures, look for the following:

- Requirements for sensitive information to be encrypted prior to transporting it through a third-party carrier
- Requirements for magnetic media to be digitally shredded or degaussed prior to reuse or disposal

- Requirements for optical and paper media to be physically shredded prior to disposal
- Requirements for users to be trained adequately on how to store and dispose of computer media, including removable media such as USB drives
- Requirements for computer media to be stored in a physically secure, temperature-controlled, and dry location to prevent damage to the media

You can obtain this information through the review of IT policies, procedures, and security awareness training documents, as well as user interviews.

19. Verify that capacity monitoring and planning are addressed adequately by company policies and procedures.

Anticipating and monitoring the capacity of data center facilities, computer systems, and applications are critical parts of ensuring system availability. When companies neglect these controls, they often experience system outages and data loss.

How

Review for the following:

- Selected architecture documents to ensure that systems and facilities are designed to anticipated capacity requirements
- System monitoring procedures, paying particular attention to capacity thresholds

- System monitoring logs to determine the percentage of systems that are approaching or exceeding capacity thresholds
- System availability reports to ensure that system capacity issues are not causing undue downtime

Since capacity management is addressed most often by the groups responsible for data centers, applications, or system management, specific procedures should be addressed within these areas.

20. Review and evaluate the company's identity and access management processes.

In practically every chapter of this book, you will find audit steps on this topic. As you evaluate each individual system and technology, it is important to understand how access to it is controlled. However, while it is possible that every system in your environment will have its own individual accounts and account management processes, hopefully there will be some level of centralization. Otherwise, you will be relying on each individual system to implement appropriate controls covering typical account tasks such as account creation, password management, and account deletion. Also, without centralized account management, users may be forced to track multiple IDs and passwords, making it more likely that they will write their passwords down and store them in an easy-to-find location. While just about every technology has its own native accounts and passwords, most also provide for some sort of ability to

reference or sync with a centralized directory and authentication mechanism. This is often referred to as "federating" identities—where one system trusts the authentication coming from another system.

An enterprise identity and access management process will increase security (by allowing for centralized controls) and will also increase efficiency (by eliminating duplicate efforts).

How

Review for the existence of "enterprise" accounts. These are accounts (identities) that can be used across multiple systems and environments. Review the enterprise account processes for the following controls:

- Procedures for creating accounts and ensuring that each account is associated with and can be traced to a specific individual.
- Processes for ensuring accounts are removed or disabled in a timely fashion in the event of employee termination. Terminating an account in the central directory should result in a cascade effect, where that account is removed or disabled in all systems that subscribe to the central directory.
- Processes for suspending access to individual systems in the event of a job change within the company (or otherwise requiring revalidation of that access).

Determine what company systems are tied into the enterprise identity and access management process. Evaluate processes for identifying and prioritizing systems to be included in the enterprise identity and access management process.

If the identity and access management process includes a centralized authentication mechanism, verify that appropriate password and authentication controls are in place. Review password settings (such as password composition requirements and password aging rules) for appropriateness and for compliance with your company's policies. Review the need for and existence of stronger forms of authentication (e.g., two-factor authentication).

Again, each individual chapter in this section addresses this topic in terms of the specific technology or topic under review. The purpose of this step is to understand and evaluate to what extent these processes are centrally managed and controlled.

21. Review and evaluate the elements of the company's cybersecurity program.

Cybersecurity has become a critical concern for all companies and their ability to maintain the confidentiality, integrity, and availability of their information and processes.

How

This entity-level control is important enough that it has been separated into its own chapter. See Chapter 4 for details.

22. Based on the structure of your company's IT organization and processes, identify and audit other entity-level IT processes.

By identifying those baseline IT controls, you should be able to reduce testing during other audits and avoid repetition. For example, if your company has only one production data center, you can test the physical security and environmental controls of that data center once. Then, as you perform audits of individual systems that are housed in that data center, instead of auditing the physical security and environmental controls for each of those systems (which would be very repetitive because they're all in the same place), you can just reference your entity-level audit of those topics and move on. Also, by performing audits of centralized processes, you will have an understanding of potential compensating controls in the overall IT environment that may mitigate concerns you have with lower-level controls.

> **NOTE** If a critical IT process at your company is centralized, it is a good candidate for being reviewed during an entity-level controls audit. By auditing it once at the company level, you will be able to rely on the results of that audit when performing audits of other IT systems and processes.

How

Review the topics covered in the other chapters in Part II of this book, and consider whether any of those areas are centralized at your company. Those topics are candidates for an entity-level controls review. Here are some likely

candidates:

- Data center physical security and environmental controls (see Chapter 5)
- System monitoring (such as performance and availability) and incident reporting (see Chapter 5)
- Disaster recovery planning (see Chapter 5)
- Backup processes (see Chapter 5)
- Network security and management (see Chapter 6)
- Windows system administration processes (such as account management and security monitoring) (see Chapter 7)
- Security of baselines used for deployment of new Windows systems (see Chapter 7)
- Malware protection (such as antivirus, patching, and compliance checking) (see Chapters 7 and 14)
- Unix/Linux system administration processes (such as account management, security monitoring, and security patching) (see Chapter 8)
- Security of baselines used for deployment of new Unix and Linux systems (see Chapter 8)
- Software change controls for internally developed code (see Chapter 15)

KNOWLEDGE BASE

As mentioned throughout this chapter, the specifics of entity-level controls will vary from company to company. However, the best general sources of information on IT-

specific entity-level controls can be found on the Information Systems Audit and Control Association (ISACA) website (www.isaca.org), where details on the control objectives for information and related technology (COBIT) framework and guidelines for Sarbanes-Oxley IT compliance testing are available. In addition, general guidelines on entity-level controls (not specific to IT) and links to resources related to the popular Committee of Sponsoring Organizations (COSO) model of internal controls can be found on the website for the Institute of Internal Auditors (IIA) at www.theiia.org. Finally, your external auditors likely will have some published guidelines to share with you on this topic.

MASTER CHECKLIST

The following table summarizes the steps listed herein for auditing entity-level 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.

- ❑ 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.
- ❑ 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.