SECURITY

Network Security Auditing

The complete guide to auditing network security, measuring risk, and promoting compliance

ciscopress.com

Chris Jackson, CCIE® No. 6256

Network Security Auditing

Chris Jackson, CCIE No. 6256Cisco Press

Cisco Press

800 East 96th Street

Indianapolis, IN 46240

This page intentionally left blank

Chapter 5

Auditing Cisco Security Solutions

Cisco offers an extensive security technology portfolio that encompasses every aspect of network communications. Auditing this wide range of devices requires an approach that analyzes the network as a system of controls and not just as individual devices. This chapter's purpose is to define security services that are enabled through logical groupings of Cisco products. These security services deliver business solutions through security controls that cover people, process, and technology. The introduction of these auditing domains provides a roadmap for how the remainder of this book is organized and also puts into context how each domain is used to address the security needs of a business. The process of defining auditable items for each domain using control frameworks and recommendations for building auditing checklists through the use of good security practices are also discussed.

Auditors and Technology

As information technology and its usages increase, companies have become more reliant on computers to automate business processes. The depth of IT audits and the skills required of auditors has increased dramatically as a result. In the early days of assessing security, auditors typically focused on identifying the presence or location of specific technologies, such as firewalls and routers, and less on how well these technical controls were integrated into the business processes or their effectiveness. The mere presence of a security device did not indicate that it was adequately protecting the digital assets of the organization or mitigating risk, but it was a required control and that was good enough. Much of this disconnect over the effectiveness of security controls had to do with the fact that auditors in general were not technologically inclined, having most often come from the financial world. This lack of understanding technology would lend itself to interesting and often heated conversations during which system administrators had to defend their use of a particular technology because it was not on the auditor's checklist, and the auditor simply did not understand how it worked.

Luckily, information security auditors are now much more knowledgeable about the role of technology and how security controls operate. The sheer number of technologies implemented in business today, such as video, voice, instant messaging, and web applications, has and continues to challenge an auditor's technical skills. There is also an ever-changing list of new threats that face the organization as these new technologies and protocols are introduced. Security used to be focused on the perimeter of the network as a means to determine what was considered trusted or not trusted. Now, the border of the network no longer stops at the firewall, and it's not uncommon to have the edge of your network be at a coffee shop or a hotel halfway across the world through an SSL VPN connection. Factor in the business side of security, with the need to manage the growing risks, regulatory compliance, and the desire to use technology to enable new and more profitable business ventures, and it becomes plain to see what a challenging task it is to audit today's IT systems. Auditors must understand the technology to spot risk, and without that knowledge, the quality and effectiveness of their assessments are greatly diminished.

Security as a System

Effective auditors think of security as a system, where the alignment of people, process, and technology to the goals of the business determine the success or failure of a security program. Security is a system of moving parts in much the same way that a car is. It's a good idea to have your mechanic inspect your car before going on a long trip. You would hope that he would do more than simply check that the doors lock or that the engine runs. To properly inspect a vehicle, there are numerous checks that must be performed to evaluate many individual components that make up independent, yet cooperative systems within the vehicle, such as the engine, drive train, instrument cluster, steering, braking, and safety features. Spot checking does not tell you if you can anticipate any problems on your trip; a more thorough operations test is required. Of course, a mechanic won't inspect every single wire, knob, or button in the car, but he should check the areas that have the highest risk of leaving you stranded on the side of the road. Inspecting the security controls of a business is a similar process; as the auditor, you inspect the organization's security controls based on identified risk, compliance to policy, and the law.

The auditor's inspection is key to the health of an organization's security program. The auditor's primary deliverable back to the organization is a risk assessment report, which details the impact those risks could potentially pose to the confidentiality, integrity, and availability of the business assets. The auditor is also responsible for identifying weaknesses in controls, which are determined through the review of records, logs, and actually testing the functionality of those controls. Additionally, an auditor must also identify weaknesses in process, which can be one of the biggest areas of risk an organization faces. If a backup tape storing hundreds of thousands of credit card numbers turns up missing, this clearly is not a technology problem, but one of process in the handling and protection of sensitive media.

Another important aspect of the auditor's job is to recommend new or updated controls to address deficiencies found during the audit process. These recommendations address

the risks found and might even include specific technologies or solutions that can better protect assets found to be vulnerable. Recommendations that are focused on best practices and industry standards also help to address process areas in need of improvement or that can be better preformed through technology. Most audit reports have a prioritized list of deficiencies found and usually include recommendations on what can be done to address those deficiencies.

Cisco Security Auditing Domains

One of the first questions new auditors typically ask is, "Where do you start when assessing security?" It can be intimidating when you think about it, looking at all the different aspects of the business to determine whether or not those processes, procedures, and technologies protect the assets they are intended to protect. If you had armies of people that you could send throughout the organization, it would be easy to conduct a comprehensive audit, but unfortunately, the reality of budget constraints and the need to do more with less forces businesses to be a bit more judicious in the allocation of resources. The next best and more realistic way to audit security is to divide security into manageable domains that are focused on business requirements and take into account the operational aspect of security. This approach is also used to manage the audit process by creating logical divisions that represent how companies actually use security products.

Defining the scope of an audit is one of the most critical parts to get right from the beginning in an auditing engagement. Audits can be conducted from the top down at the organizational level or from the bottom up at the technology or process level. Tailoring the audit to the organization's requirements ensures that the auditor meets expectations and can properly manage the audit process. The scope of an audit can be differentiated by what level of the business is being analyzed. In general, there are four high-level business-focused audit categories:

- **Auditing an organization:** This level of auditing is typically focused on the governance aspect of security and touches all aspects of the business. Organizational auditing is often done in conjunction with certification or accreditation (such as ISO 27001) and can be involved from a resource and time standpoint.
- **Auditing a domain:** Domains are IT services offered to the business and at this level, the auditor groups interconnected processes, technologies, and business functions to assess them as one unit. These domains encompass all of the people, processes, and technologies associated with security service areas such as remote access, perimeter intrusion prevention, and access control. This level is primarily focused on service delivery, architecture, and meeting the security requirements of the business.
- **Auditing a function:** At this level, the auditor assesses a functional aspect of the business that includes multiple processes and technologies used to secure the business service. Business functions represent business services such as HR, finance, and manufacturing. An auditor reviews the function-specific security controls, technologies, and processes used by the business function.

- **Auditing a process:** The lowest level of auditing and most specific is to assess a security process. A *process* is defined as the steps performed to accomplish a specific task, for example, to create new user access to the network. The auditor reviews and observes all of the steps from process initiation to completion for policy compliance and good security practices.

Auditors might be asked to audit at any of these four levels, but auditing at the domain level most represents assessing security as a system. With Cisco products, security features and capabilities are integrated into every device, so the concept of multiple functions, processes, and controls being in the same device must be considered. A router can be a firewall, IPS, and phone system all at the same time, which means that the auditor must logically separate out the services offered by the device when testing. Each domain identifies multiple layers of defense in depth and the policies and procedures that are applicable. Individual security devices and technologies can reside in multiple domains, which highlights their multifunctional role.

The seven auditing domains, as described briefly, are the foundation for the organization of the rest of this book and build upon each other for auditing network security. We focus on each of these domains in more detail in subsequent chapters of this book. It's important to note that the domains covered are focused on Cisco network security and are not indicative of all aspects of security; for example, physical security and disaster recovery are not included in this list. Although these domains are important for organizations to address, they are outside of the scope of this book. The following list shows the seven auditing domains:

- Policy, compliance, and management
- Infrastructure security
- Perimeter intrusion prevention
- Access control
- Secure remote access
- Endpoint protection
- Unified Communication

Policy, Compliance, and Management

Policy, compliance, and management are the foundations of all security programs, so it is fitting that the first domain focuses on these aspects from which security controls are born. This domain is where policy is reviewed to identify whether or not the appropriate policies are in place to guide the organization and address regulatory compliance. Management and monitoring of policy and compliance can be automated through Cisco management technologies and are assessed in this domain, too.

- Processes and functions assessed:
  - Key policies are instituted.

- Controls and countermeasures are defined.
- Standards are identified.
- Assets are identified and assessed.
- Risks are identified.
- Vulnerabilities are determined.
- Security governance programs are created.
- Auditing is conducted.
- Law and industry compliance requirements are identified.

- Cisco technologies assessed:
  - Cisco Security Manager
  - Monitoring Analysis and Response System (MARS)
  - Network Compliance Manager

Infrastructure Security

The infrastructure security domain concerns itself with auditing routers, switches, and wireless for best practice to properly secure critical services. Regardless of the vector of entry into the network, be it wired or wireless, care should be taken to ensure the confidentiality, integrity, and availability of services being offered. Infrastructure security should be considered a minimum for properly securing an organization's access to computing resources. Much of this domain utilizes best practices, Cisco SAFE, and Cisco Validated Designs as the foundations for configuring the many security features that exist on routers and switches.

- Processes and functions assessed:
  - Configuration of best practices
  - Change control
  - Router baseline security
  - Switch baseline security
  - Wireless baseline security
- Cisco technologies assessed:
  - Router
  - Switches
  - Wireless