CYBER SECURITY AUDIT

THE OBJECTIVE OF A CYBER SECURITY AUDIT IS TO PROVIDE MANAGEMENT WITH AN ASSESSMENT OF AN ORGANIZATION'S CYBER SECURITY POLICIES AND PROCEDURES AND THEIR OPERATING EFFECTIVENESS. ADDITIONALLY, CYBER SECURITY AUDITS IDENTIFY INTERNAL CONTROL AND REGULATORY DEFICIENCIES THAT COULD PUT THE ORGANIZATION AT RISK.

A cyber security audit focuses on cyber security standards, guidelines and procedures, as well as the implementation of these controls. The cyber security audit relies on other operational audits as well.[1]

Primary security and control issues for cyber security audits are:

- Protection of sensitive data and intellectual property
- Protection of networks to which multiple information resource are connected
- Responsibility and accountability for the device and information contained in it

The scope of a cyber security audit includes:

- Data security policies relating to the network, database and applications in place
- Data loss prevention measures deployed
- Effective network access controls implemented
- Detection/prevention systems deployed
- Security controls established (physical and logical)
- Incident response program implemented

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) GUIDELINES

There are many approaches available for specifying cyber security control environments, such as NIST Special Publication (SP) 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations.[2] SP 800-53 provides guidelines for selecting and specifying security controls for information systems supporting executive agencies of the federal government. It is prescriptive in nature, contains detailed definitions, and may help organizations develop their own overarching cyber security process(es).

KEY ELEMENTS OF CYBER SECURITY AUDITING: CONTROLS AND THREATS

Part of auditing is ensuring that organizations have implemented controls. This means that preventative tools such as firewalls and antivirus software have been put in place. It also means that awareness efforts have been made, and that user education about password construction and backups has been provided. Regular updates—to both preventative tools and awareness efforts—are a necessity. That's why regular audits are so important; your organization must ensure that these processes are well-designed, executed properly and as up-to-date as possible. Cyber security audits should be done annually based on business needs. They should include planned activities with specific start and end dates, including exact expectations and clear communications.[3]

Threats, both internal and external, have the potential to impact confidentiality, integrity and availability if controls are not in place. And the definition of 'threat' is broad, encompassing a variety of elements that can impact an enterprise. New laws and regulations or growth in data may pose a threat to the organization. Human threats can include everything from carelessness to espionage. And, of course, there are an array of technical threats, including, but in no way limited to, malicious code, unauthorized access, malware, or hardware/software failures.

The amount or significance of threat can vary, dependent upon whether the enterprise is working in cloud, mobile, Internet of Things (IoT), big data or security analytics. As information shifts location (moving from mobile, to IoT, to cloud, for example), there will be a need for new classes of controls to address the new locations of information, and those new classes of controls will require updating as well—and auditing.

AN AUDIT IN THREE PARTS

The cyber security audit and review process contribute to cyber security audit success. Internal auditors and risk management professionals have key roles to play, as does enterprise management.

Management — Management ultimately owns the risk decisions made for the organization. Therefore, it has a vested interest in ensuring that cyber security controls exist and are operating effectively. Decisions are typically made based on guidance received during the risk management processes, on the appropriate direction to take.

Risk Management — Risk assessments are typically made based on guidance by the security officer at an organization and enterprise management make decisions, employing risk management processes. The objective in any risk assessment is twofold. First, it is critical to communicate the state of the risk so that it is easy to understand and be clear on the level of risk involved. Secondly—and just as significantly—the ways in which to address that risk must be identified as well. This provides both problem and solution, and mitigates the negative impact of that risk to an enterprise.

The risk landscape is ever-changing. It is important to have defined processes, trained and competent cyber security resources, and a governance framework to ensure that appropriate actions are carried out by enterprise leadership and managed effectively to address current and emerging threats.

Internal Audit — Auditing is a security measure—not an inconvenience. It is critical to protecting an enterprise in today's global digital economy. The internal audit department plays a vital role in cyber security auditing in many organizations, and often has a dotted-line reporting relationship to the audit committee to ensure an independent view is being communicated at the board level of the enterprise.

Audit helps enterprises with the challenges of managing cyber threats, by providing an objective evaluation of the controls and making recommendations to improve them as well as assisting the senior management and the board of directors understand and respond to cyber risks.

Organizations, especially within the public sector, also contract for the services of external auditors to provide independent assurance of the financial and operational controls primarily to ensure the controls design is effective and the needs of the organization are being met.

---

1 ISACA IS Audit / Assurance Program Cybersecurity: Based on the NIST Cybersecurity Framework

2 National Institute of Standards and Technology (NIST), NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, USA, 2015, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

3 ISACA Auditing Cyber Security: Evaluating Risk and Auditing Controls, http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Auditing-Cyber-Security.aspx

ISACA®

Contact:

Tara Wisniewski
twisniewski@isaca.org
847.660.5673

Jen Gremmels
jgremmels@isaca.org
847.385.7207