CERT'S PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

Internal Audit's Role in Information Security: An Introduction

Key Message: Internal Audit can serve a key role in putting an effective information security program in place, and keeping it there.

Executive Summary

The internal audit function in any organization plays a critical role in ensuring board-level and management expectations are met. Internal audit serves as one of the key checks and balances for successful governance, risk management, compliance, and ethics programs. In addition, internal audit evaluates and represents the organization's state of information security and privacy. This role is escalating in importance given the growing dependence on information in digital form and the constantly changing legal and regulatory landscape.

In this podcast, Dan Swanson, president and CEO of Dan Swanson and Associates, and former director of professional practices at the Institute of Internal Auditors, discusses how internal audit can help build and sustain an effective information security program.

PART 1: INTERNAL AUDIT AS ASSURANCE PROVIDER

What Is the Role of Internal Audit (IA)?

Internal audit responsibilities vary based on market sector and the size of the organization.

In general, IA's key roles include:

- providing assurance to senior management and board directors that leaders and organizational units are performing as reported
- assessing and evaluating the operating practices of organizational units or functions
- conducting annual and selected project-level audits as determined by risk assessment results
- identifying where the highest priority improvements are needed based on risk

How Does IA Stay Objective and Independent?

IA objectivity, independence, and separation of duties from operational responsibilities are critical. These are accomplished via

- the audit mandate, charter, and terms of reference
- IA independent reporting lines to the board and the board audit committee
- direct CEO sponsorship

While IA may consult with senior leaders, IA does not perform management activities.

At senior management request and with board audit committee approval, IA will often work more directly with security, privacy, risk management, and business continuity functions on their program improvements.

How Does IA Get Involved with Information Security?

All internal audit findings, recommendations, and actions are risk-based. Security is pervasive so tends to be on most internal audit function's top ten lists.

Security is often incorporated as an audit objective when evaluating other functions and projects, such as finance (ensuring the security of finance information).

In addition, audits are often conducted for the organization's security program or function as well as for specific technologies.

All of these in combination provide a comprehensive evaluation of the organization's security efforts.

PART 2: INTERNAL AUDIT AS COLLABORATOR

How Can IA Assist in Putting an Effective Information Security Program in Place?

Collaboration is key.

Security's objective is to reduce risk and protect information. IA's role is to help determine the best bang for the buck (given you can't secure everything).

IA typically performs an independent gap analysis of the security program every two to three years. In addition, Audit assesses security risk on critical initiatives as determined by the organization's strategic plan.

Building an Effective Internal Audit/Security Relationship

IA often meets with security managers on a quarterly or other agreed-to basis to address audit findings, challenges, and successes.

Information security professionals and managers should consider reaching out and making internal audit their new best friend as IA is often able to get messages delivered in places and to roles that are difficult for security managers to accomplish.

What Types of Issues Might IA Raise to the Board?

First and foremost, IA must have good communication with managers at all levels to constructively work through audit issues, findings, and management action plans.

IA is expected to periodically report audit results to the board in accordance with the annual audit plan. IA needs to discern what findings and issues require board-level attention and action.

A key aspect of IA reports to the board is that there are **NO SURPRISES** for managers whose audit results are being presented.

Specific security issues that may be discussed at the board level include:

- Accountability for security (roles, responsibilities)
- Security practice and technology implementation in support of process improvement

What Actions Can Business Leaders Take to Engage IA in Information Security?

Invite IA to help with management self-assessment.

Seek IA opinions on strengths and areas needing improvement.

Ask IA to conduct a formal audit, recognizing that significant findings will be reported. This is, in effect, asking for a public report card and thus raises the bar for improvement.

Resources

The Institute of Internal Auditors

Information Systems Audit and Control Association

Center for Internet Security

Ask the Auditor: Who Is Responsible for Information Security?

Dan Swanson's Compliance Week column

EDPACS: The EDP Audit, Control, and Security Newsletter.

IT Audit Checklist: Privacy and Data Protection