

Top 10 Security and Privacy Topics for IT Auditors

Sajay Rai, CISM, CPA, CISSP, is the chief executive officer and founder of Securely Yours LLC, Bloomfield Hills, Michigan, USA.

Philip Chukwuma, CISSP, is the chief technology officer at Securely Yours LLC.

During these tough economic times, every department in an organization is forced to show that it is providing value to the organization. IT internal audit departments are no different. IT auditors are reviewing their audit scope to ensure that the key risks facing the organization are being addressed. The following 10 topics should be on every IT auditor’s list for 2010-2011.

Every year, when the IT audit scope is reviewed and finalized, the auditors always wonder if they have taken into account all the potential IT risks facing their organization. Various methods and techniques are used to determine enterprise risks, and the IT scope is derived from those enterprise risks.

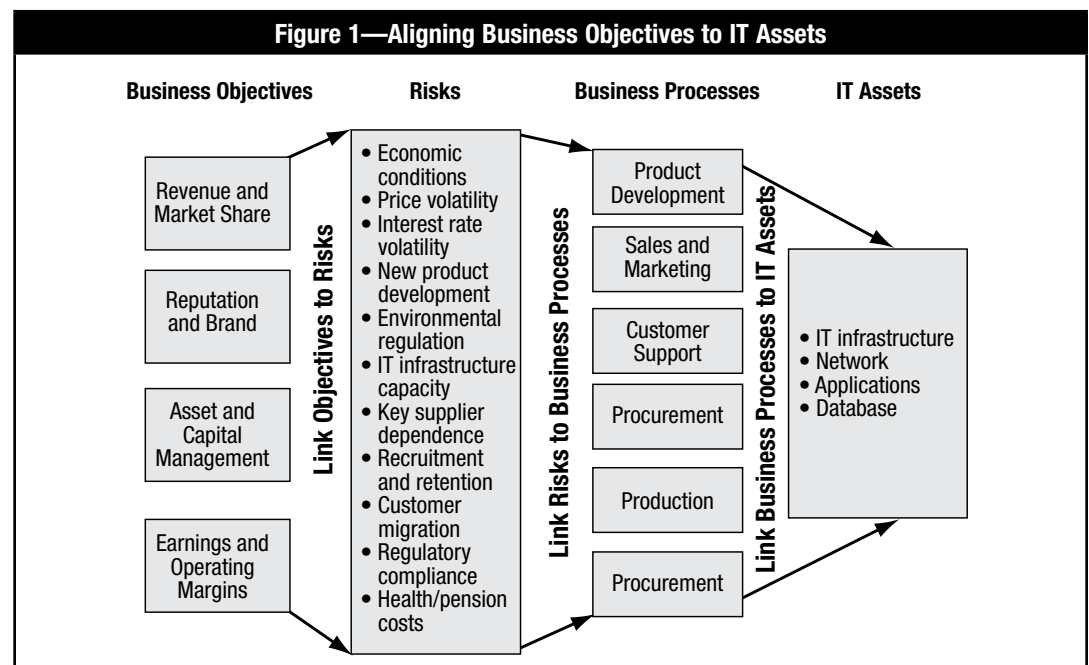
The following information security and privacy topics should be considered by all IT auditors before finalizing the IT audit scope. Within these topics, there are several angles an IT auditor could consider during the scope of the IT audit. There may not be a need to incorporate all these topics, but it is highly recommended that the topics—which are applicable across all businesses and industries—be considered before finalizing the annual IT audit plan.

TOPIC 1—KNOW WHERE YOUR ORGANIZATION’S “CROWN JEWELS” ARE

Most organizations will have a difficult time protecting their assets if they do not know where those assets are. Even though this statement sounds logical and simple, many organizations still do not have a good handle on their critical assets.

Awareness of the critical assets within an organization begins with an enterprise risk management (ERM) process. This process aligns the risks identified by the business to the IT environment. Once it is understood which IT infrastructure and applications are identified as critical, the next step is to identify all the appropriate technologies associated with the infrastructure and applications (technologies like servers, databases, applications, source code, object code, etc.). Some of these technologies may reside overseas, including source code and data centers. **Figure 1** illustrates the process of aligning business objectives to IT assets.

Appropriate policies and standards guide an organization on how the critical assets should be protected. The data classification policy plays a key role in that process as well. A good



asset management process is also critical in ensuring that the critical assets are properly managed, backed up and archived.

Auditor's Role

The IT auditor audits the ERM process and verifies the completeness of the IT alignment. The IT auditor must also understand how the IT critical applications align to the overall enterprise risk.

Auditing the asset management process will verify that the critical assets are being managed in accordance with the IT policies.

TOPIC 2—REVIEW SECURITY AND PRIVACY POLICIES AND STANDARDS

Effective and adequate information security and privacy policies and standards are a must for every organization. These policies and standards provide guidance to everyone within the organization on how they should use the critical assets, what their role is to protect these assets, and how to ensure proper compliance with the laws and regulations. These policies and standards should take into account the global nature of most organizations and address the country-specific laws and regulations as well.

Auditor's Role

The IT auditor audits a selected subset of the information security and privacy policies and standards every year. The IT auditor begins with policies and standards related to access control, data classification and network security. During subsequent years, the IT auditor should focus on other policies and standards such as vendor management, vulnerability management and data leakage prevention.

One of the important roles of audit is to verify that the policies and standards are not just documented but are actually being implemented by users across the enterprise. This verification can be accomplished by performing an audit of the security training and awareness program (see topic 4).

TOPIC 3—ASSESS THE EFFECTIVENESS OF IDENTITY AND ACCESS MANAGEMENT PROCESS

The Identity and Access Management (IAM) process is the backbone process for ensuring that proper on-boarding, off-boarding and provisioning is performed within the organization. In the past, the activities within the IAM process

were manual and tedious to audit. But in the past few years, the development of IAM software has helped automate several of these functions and has provided seamless links among the on-boarding, off-boarding and provisioning processes. An automated IAM process alters the scope of the audit.

Auditor's Role

Instead of focusing on the actual access of each user, the IT auditor should focus on the IAM process and verify that the IAM process is working as designed. Auditing an automated IAM process ensures the integrity of the process. The audit should also focus on the workflow, which includes the approval hierarchy. A sample workflow of an IAM solution is shown in **figure 2**.

Several IAM vendors are starting to provide mechanisms to incorporate segregation of duties (SoD) checks within the workflow. If an organization has incorporated the SoD checks in the workflow, it is important to include this process within its audit scope.

TOPIC 4—VERIFY THAT THE USERS UNDERSTAND THEIR ROLES AND RESPONSIBILITIES RELATED TO SECURITY AND PRIVACY

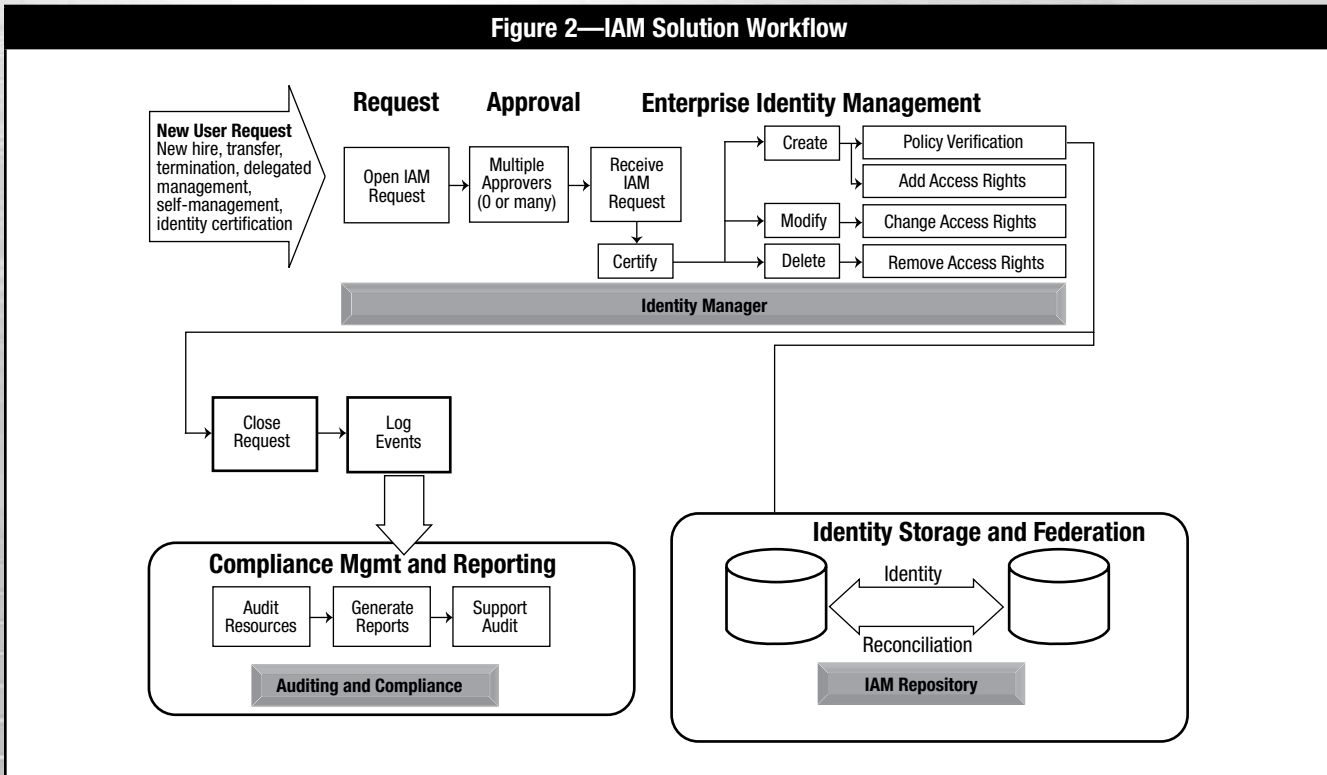
The education program has always been considered the “soft” side of the security program and traditionally has not received as much attention from IT auditors as it should. An effective information security awareness program goes a long way toward reducing the overall risk to the IT assets within an organization. In fact, this program is one way to ensure that the policies and standards are being implemented effectively across the enterprise.

For the past decade, experience has consistently shown that more than 65 percent of all security incidents occur within an organization,¹ although external incidents (such as those from hackers) get more media attention. The majority of internal incidents are caused by a lack of knowledge of information security and not fully understanding the individual's role and responsibility. Global employees create further complexities for organizations to communicate these policies effectively and efficiently.

Auditor's Role

During the audit of policies and standards, the IT auditor should understand how the policies and standards are being communicated across the enterprise. Every organization has

Figure 2—IAM Solution Workflow



a communication method (e-mail, posting on an intranet web page, periodic security seminars, monthly security awareness training, lunch-n-learns, etc.).

TOPIC 5—ASSESS THE EFFECTIVENESS OF THE MONITORING PROCESS

Monitoring has become very important to organizations as a result of compliance requirements from regulations, such as the US Sarbanes-Oxley Act, US Health Insurance Portability and Accountability Act (HIPAA), US Gramm-Leach-Bliley Act (GLBA), Payment Card Industry Data Security Standards (PCI DSS), Basel II, and other industry standards.

One aspect of monitoring that has not been adequately addressed by organizations is logging. Events from critical systems are not logged because some organizations argue that logging consumes too much disk space. In some organizations in which logging is enabled, logs are overwritten after a short time, making them ineffective.

Effective monitoring requires planning to identify those events that are of consequence to the organization. These events should be logged, classified and prioritized. Where a threshold is required, it should be set so that a log/monitor

event is generated. Log reviews should be assigned to specific individuals for monitoring. Where continuous monitoring is required, the critical events should be forwarded to an event management system, such as a security information and event management (SIEM) system. A SIEM system will actively monitor events and raise alerts. It can also be used to generate compliance and attestation reports on all the monitored systems on set intervals (e.g., daily, monthly, quarterly). The logging process should readily identify access to critical events, unauthorized access attempts, usage, modification and copying of critical data.

Auditor’s Role

The responsible IT auditor should determine if logging is enabled in critical systems. Where logs are enabled, the IT auditor should verify that there is a process for monitoring. The IT auditor should also verify that the process has been assigned to a person and that this person is executing this process. The focus here is on data leakage prevention (DLP). Besides verifying that the proper access is granted to each individual, the IT auditor must focus on how the approved users are using the “crown jewels.” Are data being encrypted

properly before they are sent outside of the organization? Depending on an organization's DLP policy, the SIEM system can potentially help the IT auditor determine if the data are being copied on USB drives and leaving the organization.

TOPIC 6—REVIEW THE GRC PROCESSES FOR THE ORGANIZATION

IT risks have become a greater concern for management. Management is spending millions to identify IT risks and establish a governance process to address and manage those risks. Management interest can be attributed to regulations and industry standards, such as Sarbanes-Oxley, HIPAA, GLBA, PCI DSS and Basel II, and the liabilities for noncompliance. One way to address governance, risk and compliance (GRC) is to create an executive level position such as chief information security officer (CISO) and/or chief compliance officer (CCO). The CISO and/or CCO become responsible for creating the processes for GRC and executing periodic compliance reviews. Working with the information security committee, internal auditors and external auditors, these executives identify, catalog and remediate IT risks within their organization.

Auditor's Role

In today's business environment, GRC processes are critical to the IT auditor. The IT auditor should examine corporate governance processes and verify that an infrastructure has been created to identify and manage risks. The governance structure should be active and ongoing, which means that the executives should conduct periodic meetings to address risks. The auditor should also identify all relevant regulations and industry standards and perform periodic compliance reviews based on identified and relevant risks. Noncompliance should be tracked and managed by executive management.

TOPIC 7—AUDIT THE EXTENDED ENTERPRISE

Security is only as strong as the weakest link. Does the organization do business in a federated manner and as such grant access to business partners? Does the organization outsource its IT to a third-party vendor? Does the organization's service contract with any of its vendors include giving a vendor network access to its systems? Can users create their own IT environment, such as a wireless network, without proper authorization? Most organizations are connected to the Internet, meaning that their IT infrastructure is not an isolated island. As such, organizations' security should always be addressed beyond their internal boundaries.

Auditor's Role

This is an area in which many IT audits have fallen short. The internal auditor should identify how the organization is connected to the outside, and who on the outside is connected to the organization. There is a total reliance by some organizations on Statement on Auditing Standards No. 70 (SAS 70) Type II reports for review of external vendors. While SAS 70 is good, it is not final. The IT auditor should first verify that there is a policy in place to address third-party connections. In addition to the SAS 70 report, the organization should periodically perform its own audit of the vendor to certify that its policies and security needs are being adequately addressed (the organization may have to ensure that the vendor contracts allow for this audit). Changes performed by the third-party vendor on systems affecting the organization should follow the organization's normal change management process.

Also, the IT auditor should follow the entire process within the extended enterprise where the "crown jewels" reside. For example, an enterprise may do an exceptional job of protecting "crown jewels" within the enterprise, but an unencrypted backup tape can fall off a vendor's truck and expose critical information and put the enterprise at risk. An audit of the entire process will definitely reduce the risks associated with the extended enterprise. This extended enterprise may exist globally and could add more complexity to the IT audit plans.

TOPIC 8—REVIEW THE PLANS FOR BUSINESS CONTINUITY

Business continuity planning (BCP) is a way to provide for the continued existence and operation of the organization. BCP and the related disaster recovery (DR) provide processes that can assure continued operation. BCP requires the identification and classification of all business processes and the identification and classification of associated business risks. A business continuity plan should be created that defines how the business will operate during interruptions and should include chain of command, employee safety, vendor management, supply chain, etc. The size of an organization also affects its BCP/DR plan. This plan should be tested and modified periodically. If business processes change, those changes should be reflected in the plan. BCP/DR testing is not a single department exercise, but rather should involve the whole organization. If a partial test is being performed, then all the departments and groups affected should be involved

in the testing. Changes to the plan should also go through the normal change management process and be documented appropriately. BCP/DR should be owned by a member of executive management and managed by individuals responsible for maintaining the plan. The plan should also define how to communicate with the general public and the employees respectively. With BCP, the question is always: What can go wrong?

Auditor's Role

The IT auditor should verify that a business continuity plan exists and is maintained and tested periodically. The IT auditor should also make sure that the plan covers all the risks associated with the business and that it is enough to keep the business in operation in times of disruption. The IT auditor should understand the difference between business continuity and disaster recovery and make sure that each is adequately addressed and periodically tested.

TOPIC 9—VERIFY THAT THE BUSINESS LEADERS ARE AWARE OF AND UNDERSTAND IT INITIATIVES

In the past, IT and IT initiatives had been thought of as an expense in many organizations. While this may still be true for many organizations, IT is now interwoven into core business processes. Management investment in IT continues to grow; however, management does not have a complete understanding of all IT initiatives. Part of this is that management is not informed of some IT initiatives and in some cases in which management is informed, executive management may not have an understanding of or interest in IT initiatives. Management of IT initiatives is part of IT governance. Management should know about and be an active participant in IT initiatives. The status of IT initiatives should be reported to management because this will not only help executive management better understand current IT initiatives, it will also help management understand business risks inherent in IT operations. Executive understanding of IT initiatives will also assist management in planning for future IT initiatives and help to properly align the initiatives with existing business requirements. When management understands IT initiatives, it is easier to obtain management approval for IT projects and gain a management sponsor. The goal for IT should be to make sure that IT initiatives are aligned with business objectives and to report often to management about the status of IT initiatives.

Auditor's Role

The IT auditor identifies a catalog of IT initiatives, reviews the business reasons for the project and identifies the executive sponsor for the project. The IT auditor obtains and reviews the management reports from IT to executive management and verifies that sufficient information is provided to management. The IT auditor verifies that IT initiatives are adequately aligned with business objectives.

TOPIC 10—VERIFY THAT THE ORGANIZATION'S RISKS ARE COVERED BY AN ADEQUATE INSURANCE POLICY

A business operating without insurance is like jumping off an airplane at 20,000 feet without a parachute. Organizations should identify their business risks and adequately insure against the risks. If an incident occurs, carrying an adequate business insurance policy can help ensure that the organization will not be out of business the next day.

Auditor's Role

The IT auditor should ensure that business risks have been fully identified and carry adequate insurance coverage. The IT auditor should also audit the process used by organizations to determine the level of insurance required.

CONCLUSION

During the best of times or the worst of times, these topics have stood out to be the backbone of a good information security and privacy program. These topics should get appropriate considerations during the scoping of the yearly IT audits. IT auditors will feel more comfortable once they have reviewed these topics and verified the prioritization of the IT audit topics scheduled for the year. While not every one of these topics may make the IT audit plan for the year, the IT auditor will feel confident that at least the appropriate topics were reviewed prior to finalizing the IT audit plan.

ENDNOTE

¹ PGP Corp. and Vontu Inc., "2006 Annual Study: Cost of a Data Breach," 2006, table 1, p. 6