PRESCRIPTIVE GUIDE SERIES

Information Security and Multi-Compliance:

Avoiding Audit Fatigue with a Single IT Compliance Strategy

By Gene Kim
CTO, Tripwire, Inc.
&
Jennifer Bayuk
Cybersecurity Program Director,
Stevens Institute of Technology

tripwire™
Configuration Control for
Virtual and Physical IT Infrastructures

A TACTICAL GUIDE ENABLING YOU TO TAKE ACTION AND ACHIEVE OPERATIONAL EXCELLENCE.

TABLE OF CONTENTS

Tripwire software has been recommended, endorsed and/or certified by these agencies.

Common Criteria

SANS

CERT

CERTIFIED BY
the CENTER for
INTERNET SECURITY

Executive Summary

Experienced managers typically do not want to be held accountable for situations where they have little control or influence. However, this is not an unusual scenario for information security managers. It happens every time they are held responsible for failed results of a compliance audit, even though they had tried to close decisively security implementation gaps that would have led to a more successful outcome.

This situation typically occurs because business process owners and information technology (IT) management often view information security as a distraction from "real work." Furthermore, information security managers often discover too late that business and IT management were not as prepared for the audits as was represented, resulting in last-minute, but often inadequate, emergency preparation work. As a result, business stakeholders, IT, and information security management all must perform heroics to generate proof of controls that demonstrate compliance, necessitating the creation of new documents and presentations from scratch in response to auditor questions. Yet even heroics may not prevent the organization from failing the audit, which results in remediation work, audit retests, fines, and loss of auditor confidence in the security management process.

The compliance approach to meeting information security goals tends to follow the cycle of crisis-driven audit preparation, audit, audit findings, remediation, and retesting. This may also be followed by a highly political search of who is to blame for the unsuccessful audit. Often, the person held personally responsible will be the CIO, who may in turn blame the CISO or compliance officer. In either case, IT management has tremendous incentive to figure out a new, more effective approach to meeting these information security and compliance goals.

This Prescriptive Guide provides nine steps that information security managers can use to break the compliance blame cycle and build an information security program that more effectively mitigates security risk. By successfully executing these steps, the information security manager will no longer continually react to and manage the audit preparation crisis *du jour*. Instead, the information security manager will institute and rely upon regular, defined activities to complete the heavy lifting of preparing for a successful audit long before the audit occurs.

Completing the nine steps requires business stakeholders, IT management, and information security management to all mutually support the same goal. This guide describes how to gain this alignment and defines the various compliance roles so that information security and compliance activities become integrated into daily business operations.

Information Security Management's Dilemma

An ever increasing number of external forces mandate effective information security in the IT environment: the Sarbanes-Oxley (SOX) Act of 2002, the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act (HIPAA), Federal Trade Commission (FTC) stipulated judgments, emerging privacy laws, and the Payment Card Industry Data Security Standard (PCI DSS) are just a few examples of external legal and regulatory requirements with a mandatory security component.

These requirements have put unprecedented amounts of pressure on information security management, and specifically on the Chief Information Security Officers (CISOs), to demonstrate that effective controls exist to adequately secure IT systems and data. Many regulations require CISOs or others in an equivalent role to report on information security and compliance status to the highest levels of management and to the board of directors.

Unfortunately, simply launching an emergency project to comply with the letter of the law does not actually achieve compliance. Moreover, achieving and maintaining compliance through a project-driven approach has a number of significant operational challenges, some of which carry significant negative impact for the entire organization. For example:

- Information security is often organized and designed to minimally interfere with business and IT operations, but this setup often creates barriers to meeting compliance goals.
- Although information security is held accountable for the effectiveness of controls to meet compliance goals, the effectiveness of these controls relies upon other business and IT management to adequately prepare for and correctly interpret compliance audit requirements.
- Information security has the accountability, but not the organizational authority to prioritize and execute design and implement the required IT controls. Consequently, information security becomes merely an "IT audit liaison," primarily helping schedule meetings and track remediation tasks—and apologizing for failed tests.
- Information security often discovers too late that business and IT management were not as prepared for the audits as was represented, resulting in last-minute, emergency preparation work.
- Business, IT and information security management must perform heroics to generate proof of compliance, often creating new documents and presentations from scratch in response to auditor questions.
- The business may fail an audit test, requiring remediation work, audit retests, fines, loss of auditor confidence in the information security program, as well as loss of personal trust in the information security manager.
- An information security breach may occur, and the business must now explain how it occurred despite passing the audit.

There are also significant consequences when an organization achieves compliance through a project approach, as opposed to as an ongoing process:

- Scheduled, value-adding work and projects are delayed because of all the urgent and unplanned audit preparation work.
- The business continues to implement controls only as part of a one-time audit preparation project to achieve compliance, with little thought about how to maintain compliance over time. As a result, this level of effort must be repeated to prepare for the next audit, instead of integrating information security and compliance controls into daily business and IT operational processes.
- The business starts treating audit preparation as a legitimate value-adding project, even charging time against it. In reality, treating audit preparation as a project is the equivalent to classifying status report

writing as a valid project. Compliance must be a part of daily operations, not the result of a separate project.

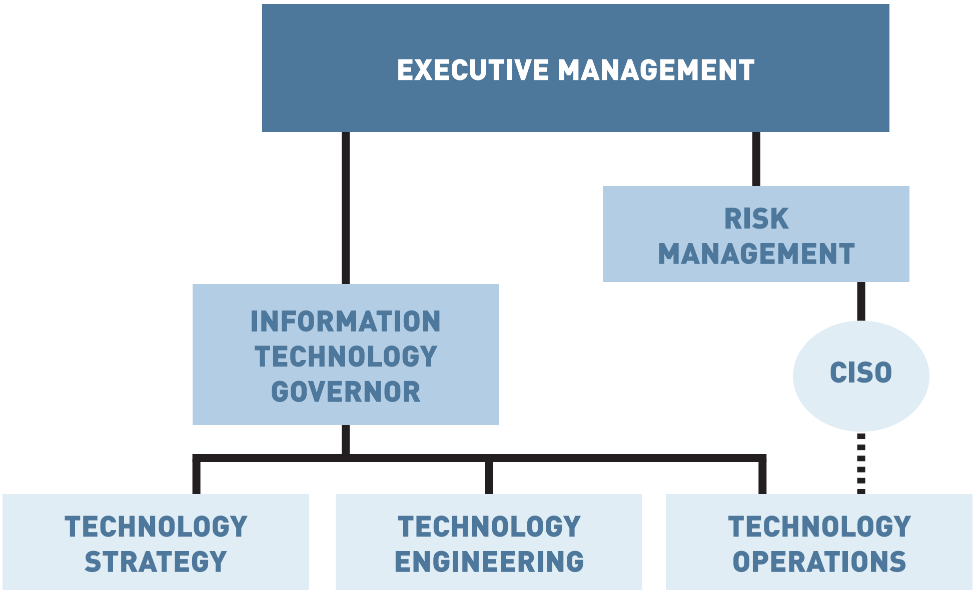
- Multiple regulatory and contractual requirements result in IT controls being tested numerous times by numerous parties, often resulting in management having to perform work multiple times unnecessarily to support different audits.

Nine Steps to Building An Information Security Compliance Program that Works

This paper provides nine steps information security managers can implement to build an information security compliance program that mitigates the negative issues described above. After successfully executing these steps, the information security manager no longer manages a crisis-driven audit preparation project using resources controlled by others. Instead, the information security manager institutes and relies on regular patterns of defined activities to complete the heavy lifting of preparing for a successful audit long before the audit occurs.

Successful completion of these steps also ensures the regular generation of evidence of the effectiveness of controls. This evidence is not only required by auditors to demonstrate proof of controls, but also provides upper management proof that information security and compliance needs have been fully addressed.

By the nature of the job, the successful execution of an information security compliance project is dependent on active collaboration among all areas of the organization that process information. However, as a result of how the information security profession has evolved, the information security manager is often held accountable for meeting information security compliance objectives, but does not have full control over the systems for which he or she is responsible. Information security rarely has the ability to impact business processes outside of IT.



The value network of typical information security managers. Solid lines show business line management. The dotted line shows a common relationship between information security and the technologists who secure the systems.

The objective of the nine steps is to ensure that management activity conforms to the expectations of industry standard auditors. It starts with identifying organizational goals, and includes identifying risks, implementing required controls (entity level controls, as well as preventive and detective), and being able to test the controls in an automated manner. And because compliance measurement reports are being generated well in advance of the audit, there is a far higher likelihood that there will be time to complete any needed remediation tasks.

To make this transformation, the information security manager must:

STEP	DESCRIPTION
Step 1: Align with tone at the top	Ensure that compliance activity is clearly managed from the top down.
Step 2: Create a set of merged information security and compliance/business goals	Document IT governance goals and risks to achieving those goals, and confirm that information security and compliance helps achieve those goals.
Step 3: Define ideal information security goal indicators	Develop theoretical ideal indicators that demonstrate that information security goals are being met.
Step 4: Gain an end-to-end understanding of information flow	Do an end-to-end business process walk-through to understand and document: • Where sensitive information enters, transits, is stored, and exits the organization. • Specific risks to organizational goals and information flow. • Where reliance is placed on technology to prevent and detect control failures.
Step 5: Agree upon control ownership, roles and responsibilities	Clearly define roles and responsibilities for audit compliance activities at the process owner level.
Step 6: Define the control tests so business process control owners will agree with the results	Make sure that evidence that demonstrates compliance goals have been met can be generated in an automated manner, upon demand.
Step 7: Schedule and conduct regular control tests	Conduct tests of controls effectiveness frequently enough be able to rely on their effectiveness regardless of variances in audit scope and timing.
Step 8: Organize metrics and remediation reports	Track the completion of required remediation work, ideally to be completed well in advance of the audit.
Step 9: Detect and respond to significant changes to the control environment	Have the situational awareness to know when the information flow or control environment has significantly changed, requiring these steps to be redone (for example, when an application is changed to allow consumer data to be downloaded to desktops instead of being viewed through pre-defined application reports).

Executing these steps may require considerable work, especially when defining management control objectives and designing corresponding control activities. However, these proactive efforts are far preferable to micromanaging individual administration processes and procedures, preparing for an audit in a crisis mode, and remediating the findings of an audit.

Individually, each of the nine steps constitutes a best practice in information security management. Collectively, these steps enable control over the end-to-end information flow in any given IT infrastructure. However, it is unrealistic to think that any given information security manager has the time or resources to manually perform each step. The key to quickly and easily preparing for an audit is to determine which control activities are routinely used in compliance and information security audits, and to automate the management of tasks that make up those activities. In this paper, we also discuss which of these tasks can be automated and the types of solutions you can use to provide that automation.

Terminology Used in This Document

Throughout this paper, we will use the terms IT governor, end-to-end business process, information flow, and controls reliance. Following is an explanation of these terms.

IT governor refers to the highest ranking IT professional in the organization. This individual bears ultimate responsibility for the smooth operation of information technology, which typically includes IT project delivery and providing reliable IT service. The company's board of directors, or equivalent, holds this individual accountable for all issues related to IT. A subset of the IT governor's responsibility is compliance with the organization's information security goals.

End-to-end business process view typically refers to documenting and understanding all the steps required to achieve the desired organizational result, from when work enters to when it leaves the organization. Examples of business processes include sales order entry, materials management, and mortgage application processing. Examples of typical artifacts of gaining an end-to-end understanding of a business process include flowcharts, documentation of controls and procedures such as approvals and exceptions).

Information flow is almost synonymous with "end-to-end business process," but focuses on automated business processes that have information that must be protected. For example, if a business process requires a salesperson to manually negotiate the terms of every deal, there may be little or no automated information flow in the pricing process. In contrast, a sales process for an online stock trading site may obtain prices from an application that processes automated data feeds, so likely has 100 percent reliance on an information flow.

Controls reliance[1] is placed on an IT control when the control provides critical functionality that must operate as designed in order to detect or prevent errors. Critical functionality is the logic in a system that enables it to attain its objectives. For financial reporting, controls reliance is placed on the calculations and controls required to ensure the integrity of account balances and values. For IT operations, controls reliance is often placed on all the functionality provided by the IT service required to fulfill the business objectives, of which any impairment will negatively impact the business.

Here are 3 examples of when there is reliance on an IT control:

1. For SOX-404 financial reporting for the accounts payable process, suppose that reliance is placed on an automated three-way match control in the enterprise resource planning (ERP) system that ensures that only invoices with valid purchase orders and packing slips are paid. As long as the three-way match setting is enabled and does not change, we can trust the results of the accounts payable process that is enabled by the ERP system.

   Consequently, IT management must prove that no unauthorized changes were made to the match-setting software and the configuration parameter that enables the three-way match check. Why? Because an unauthorized change could disable the IT functionality that we rely upon, which could result in an undetected financial statement error. In other words, we rely on the correct configuration of the three-way match setting, which then relies on effective change controls.
2. For daily operations of the web auction ordering business process, reliance is placed on all the IT services and systems that deliver critical functionality that must be available to process customer orders. This critical functionality includes the web site that delivers the user presentation, the Java code that creates the web presentation, the databases, operating systems, and networking devices, as well as the interfaces to the business systems where customer transactions are uploaded.

[1] Definition from the *Visible Ops Security Handbook: Achieving Common Security and IT Operations Objectives in 4 Practical Steps (Cite authors: Gene Kim, Paul Love, George Spafford, 2008)*

To safeguard the objective of high availability and ability to process revenue, change management controls are necessary. These management controls ensure that all changes to the various components are properly reviewed and authorized, and that no untested or unauthorized changes are implemented. Why? Because an uncontrolled change could disrupt company operations. In other words, management relies on the fact that all order entry systems function according to a business plan, and plan execution relies on the proper functioning of all order entry IT services for operations, which in turn relies on effective change controls.

3. For compliance with emissions laws and regulations in a petroleum company, reliance may be placed on sensors in the smokestacks of refining plants. These sensors are used to support the assertion that the refinery's emissions are in compliance with laws and regulations. These sensors are monitored by IT services, and reliance is placed on the correct functioning of the sensors, as well as on the supporting IT services.

   To safeguard the objective of complying with emissions laws, management must monitor not just the emissions themselves, but also control changes to the sensors and the IT services that support them because changes could impair critical functionality. Uncontrolled change could result in management's inability to validate actual emission outputs and potentially result in fines and lawsuits.

Presented next are the nine steps that we must implement as information security managers to build an information security framework that works.

Step 1: Align with the tone at the top

The current approach to meeting information security goals tends to follow the cycle of audit preparation in crisis mode, audit, audit findings, remediation, and retesting. Typically, this cycle is followed by blame for an unsuccessful audit. As IT governors find that their organizations hold them personally accountable for meeting information security and compliance goals, they have a tremendous incentive to figure out a new, more effective approach to meeting these information security and compliance goals.

In this step, our goal is to propose to the IT governor a way to break the failing compliance cycle by placing more effective controls on the audit environment. Our challenge is to define and communicate what needs to be done in a way that is palatable for their IT governor to champion within the organization. After all, as information security management, we cannot succeed without recognition and required support from IT management.

The first step in changing the audit control environment is helping IT governors understand that they share accountability for information security outcomes with their information security manager. The next step is to gain firm agreement about the changes to the audit control environment that must be made.

Step 2: Create a set of merged information security and compliance/business goals

Our goal in this step is to jointly define with the IT governor where the achievement of IT governance and business goals requires the achievement of information security and compliance goals. We start first with the IT governance and business goals, list the risks that could prevent their achievement, and then identify where information security controls can mitigate those risks.

In this step, we start to capture in writing a set of merged, mutual goals that IT governor can support. And in order for them to hold someone accountable, each of these goals must be stated in a way that is achievable, measurable and verifiable.

For a goal to be achievable, we must describe what an audit scenario looks like when the goal has been accomplished. We cannot simply state these goals as "achieve compliance with regulation XYZ." Instead, we state the risk and then state the information security goals required to mitigate the risk.

The following example shows how information security and business goals can be merged and stated as an achievable, measurable and verifiable goal that provides specific direction for supporting business information security goals.

> *A manufacturing company must comply with a regulatory requirement that certain chemical toxins are never released into the atmosphere in amounts over 10 particles per second. The manufacturing control system has been designed to ensure that this toxin is released at a rate of only 1 particle per second.*

We start creating the merged goals by answering the following questions:

> ***What is the business objective?***
>
> *Ensure smooth operation of the manufacturing in accordance to the business plan and all associated laws and regulations.*
>
> ***What are the information security and compliance risks?***
>
> *The manufacturing control system could fail and release more than the allowed amount of the chemical toxin into the atmosphere or the measurement system would not detect this release. Also, the manufacturing control measurement data could be altered or lost, which would prevent management from validating emissions output compliance.*
>
> ***What is my information security goal to address this risk?***
>
> *We must maintain integrity over the particle release measurement process and the measurement data.*
>
> ***What control will we implement to meet this goal?***
>
> *An access and measurement testing control process will protect the toxin release measurement software against tampering. The control will alert operations when changes to access are detected and when abnormal variations in the toxin measurements occur. The alert response will include automated and manual procedures that verify that the algorithm installed in the production system is the same as the one that underwent rigorous pre-production system testing.*
>
> ***What does plant management (the business process owner) need to do to support this goal?***
>
> *The control process would require the business process owner to configure the production system to minimize the access any given individual needs to change the algorithm and the corresponding data. The control process would also require the business process owner to minimize the job functions that require access to the algorithms and the measurement data.*

Note that the last part of the example has been phrased as a business technology requirement rather than an information security requirement. The amount of information security control and business process owner control over technology that it takes to achieve the business goal is clearly stated and understandable. This clear statement allows the business process owner and the IT governor to more easily agree upon the corresponding information security goal.

Upon completion of this step, we have documented the business goals, the risks that could prevent the achievement of those goals, and outlined the information security and compliance goals that would mitigate those risks. We have also started to frame what controls are required to achieve those goals.

By creating this merged set of goals , the IT governor will ideally support the next steps and will also recognize how information security can closely support business compliance goals, help with the efficiency and effectiveness of operations, and assist in creating well-defined technology management objectives.

Step 3: Define ideal information security goal indicators

There are many different approaches to achieving the desired outcomes of any given business process control. However, some approaches require considerably more audit work than others to verify their effectiveness. In general, the more subjective judgment required by management, the more testing and sampling audit must do. Consequently, our goal is to design controls to allow as much objective measurement as possible.

In this step, we explain how change and access controls can be designed to ensure audit preparation and testing are as efficient as possible.

Efficiently Using Change and Configuration Controls to Meet Business Process Goals

Ideally, we would agree that the business process goal for information security has been achieved when management can demonstrate that they are using the approved standard system configuration and that the configuration has not changed. We will record the approved standard configuration that controls the information flow, including the timestamp, file type, file size, and cryptographic checksum of files. These attributes become the yardstick by which we measure whether the business process information security goal has been met. At any given point in time, there is only one authorized, or "correct" set of values for those attributes.

In this approach, the business process owner agrees in advance that the method by which the correctness of the file contents should be determined is through a series of automated tests that compare the authorized set of values for the attributes against the current set of values. Any discrepancies, or exceptions, let us know when unauthorized changes have been made to the files. The decisions about what constitutes a correct configuration is made in terms that the IT governor easily understands and can agree on.

Presumably this approach would have few exceptions, and the amount of time required by both IT staff and auditors would be minimal. Note also that if the business process owner routinely enforces the information security goal, the business process owner, rather than the information security professional, would need to explain any exceptions.

Contrast this to a process where management has to manually review all changes, perhaps after each software release, and then manually compares observed changes to the approved release. This requires considerably more management judgment and vigilance. Comparing the efficiency of the two change control approaches is discussed in Addendum A.

Efficiently Using Access Controls to Meet Business Process Goals

Another common information security objective is to control user access. Ideally, the business process goal for information security has been met when the standard system configuration ensures that all user access provisioned is required by a business purpose. The measurable attribute is the list of roles corresponding to job descriptions, which becomes the yardstick for measuring whether the information security objective has been met.

In this approach, the business process owner agrees in advance to execute a given business process that relies on certain job activities corresponding to defined job functions. This approach demonstrates that the control goal is met by showing that each individual who has access belongs to a specific job function, and that any exceptions can be correlated with an access request that has an approved business purpose. The decisions about who should have access to what are evident in the agreed upon system configuration. Decisions about minimizing access are made at the macro level in terms that are easily understood and agreed upon by the IT governor.

Presumably this approach would have few exceptions, and the amount of time required by both IT staff and auditors would be minimal. Note also that if the business process owner routinely enforces the information security goal, the business process owner, rather than the IT or information security professional, would have to explain any exceptions. The actual cost savings associated with this method compared to alternate methods depends on the number of users in the audit test sample.

Contrast this to a process where requests for user access are made via an online form, and the responsible manager must then decide whether to authorize the access request. In this case, we rely on individual decision-making on a case-by-case basis, which requires the auditor to validate whether access is still minimized. This process requires considerably more management judgment and audit work to validate. Comparing the efficiency of the two change control approaches is discussed further in Addendum A.

Step 4: Gain an end-to-end understanding of information flow

In the previous step, we created ideal information security goal indicators, where we favored reliance on the measurement of information attributes (for example, configuration attributes, user roles and job descriptions) instead of relying on administrative activity and supervisory controls. By doing this, we elevate protection requirements beyond a simple set of procedures and processes to demonstrating control over the end-to-end information flow. By specifying the required attributes, we gain an end-to-end view of information flow through the IT infrastructure and we can enforce accountability of managers to specific outcomes rather than to a set of procedures and processes. This focus also produces a more complete set of audit and control requirements than a traditional business application focus because information flow extends far beyond the boundaries of an IT application.

Consider the following scenario:

> *A merchant has a business process that supports a customer loyalty program. The program includes issuing branded credit cards. The consumer credit information flow starts with a customer filling out an online application form, which is sent to the credit calculation application, is then sent to a sales application, and ends up in an application that runs on the desktop of every customer service representative.*
>
> ***What is the business goal?***
>
> *To ensure that customers approved for the credit card services are capable of meeting their obligations, so that any credit extended to the customer is likely to be repaid.*
>
> ***What are the business, information security and compliance risks?***
>
> *That information collected from the customer will be inaccurate or the information will be inadvertently disclosed, violating regulatory requirements on the protection of consumer information.*
>
> ***Through what applications does the information flow?***
>
> *The online application form is delivered through a third-party vendor, the credit calculation is done on cloud computing resources, the sales application is run internally by IT operations, and the customer service application is run by a combination of internally developed server software and desktop software on the customer service desktops.*

By constructing the end-to-end information flow through a business process, we often reveal business use of information on desktops and cloud computing environments. When we view information control requirements in the context of information flow, merely distinguishing between authorized and unauthorized access requests within a single application is clearly insufficient. Experienced auditors will quickly recognize when an IT organization does not demonstrate end-to-end understanding of information flow.

Applications provide micro-level access control. Today's enterprise requires the ability to distinguish authorized from unauthorized information flow through the infrastructure at a macro level. When the IT governor agrees that a macro approach is preferable, he or she will also likely agree that the best contribution of information security is at the drawing board when a project is initiated, using the information security requirements process. In other words, exposing the control requirements of each step in the information flow can introduce opportunities for improvements, such as reorganizing, rearchitecting and reconsidering sourcing decisions.

Our next step is to ensure that all IT assets in the IT infrastructure that support the information flow are demonstrably protected by business process controls.

Step 5: Agree upon control ownership, roles and responsibilities

At this point, we have defined what needs to be controlled through the entire information flow, specifically around user access and configuration changes. Furthermore, we have defined what the ideal demonstration of business process owner control over IT would look like at each point in the information flow; for example, when management is approving greater access to the information that the defined job function requires. We also have an understanding of what IT entities the information flows through; for example, through third party vendors, cloud computing resources, and internal IT operations.

Now we must agree upon or assign the business process owner for each of these controls. These owners are responsible for implementing and regularly auditing, in an automated manner, each of the controls within their area of responsibility. The goal is for them to regularly review these automated audit reports and remediate issues as part of daily operations as opposed to scrambling to generate the reports before the auditors show up.

We identify organizational owners by inventorying the hardware and software components that deliver the IT service at each point in the information flow. Each of these components presents a potential data leak, availability issue and integrity threat. Consequently, all of these components are in scope for an audit concerned with that business process.

For instance, consider the previous example of the business process that evaluates the likelihood of customers repaying credit extended via the branded credit card. When we look at assigning ownership of the various components of the sales application, it may look like:

APPLICATION LAYER	TECHNOLOGY	MANAGEMENT OWNER
Sales Application	Java J2EE app	VP App Dev
Database	Oracle	Director, Database
Operating System	Solaris	Director, Midrange Systems
Network	Cisco, Juniper	Director, Network Ops
Virtualization	VMware ESX	Manger, Virtualization

If we find that any IT assets in the information flow have no IT owner accountable for them, we will have the IT governor directly address this issue. As information security managers, we must leverage accountability assignments made by the IT governor to ensure that the responsible IT technology owners integrate information security responsibilities into their job functions.

Once we identify each business process control owner, typically an IT manager, these owners must define a standard information security configuration for each of the IT assets he or she is responsible for in the information flow. This standard configuration includes detailed descriptions and technical specifications of the software relied upon to safeguard information and detect potential intrusions. The standard configuration also includes file object attributes, configuration settings, encryption key configurations and other parameters used by management.

Each standard configuration must be automatically monitored for deviations. The business process control owner should only accept detected changes made to the agreed upon standard configuration if the changes are deemed valid within the context of a change validation process and if they do not threaten the security of the information.

With full support of the IT governor to enforce business goals, we should be able to work with each IT owner to devise a standard configuration report that can be used to authoritatively determine whether information flow is protected. Moreover, this reporting process itself must be subject to the same level of automated audit control tests. Otherwise, technology used for security metrics reporting may report no changes when there have been changes due to simple technical failures such as a failed database update. Note that in both cases, such automated reporting must rely upon a previously compiled repository of technical configurations known to provide assurance that the information within the flow was handled according to procedures agreed to and supported by IT staff.

As information security managers, we must ensure that compliance and exception reports are not generated just before the auditors arrive. Instead, these management control tools should be run periodically to detect and track exceptions. The same business process control owner responsible for the smooth operation of the IT asset is also expected to maintain these reports.

Step 6: Define the control tests so business process control owners will agree with the results

The effectiveness of a business process control goal may be measured by comparing the expected, standard configuration to the configuration returned by the automated control test. In reality the business may be audited, or for other reasons may need metrics for measuring compliance with information security goals before the business process control owners have applied the standard configurations to production systems. In fact, secure configurations may be designed long before they are applied to the relevant production systems. But it's still important to determine and take deviation measurements when configurations deviate from a known standard configuration. These deviation measurements can be used to build a remediation task list that both the IT owner and information security manager know about, and any known deviations should be shared with auditors.

So why would we share this evidence with an auditor? It's true that disclosing this need for remediation can be used as evidence for audit findings. However, the audit report will likely note that remediation is in progress and that the percent of inventory that is out of compliance is being reduced by these remediation efforts. By disclosing this evidence, the audit will conclude with much less time and effort by IT staff than if the auditors had to devise information security tests to detect these deviations.

To generate this evidence, the monitoring business process control owners performed would need to use the same reports an auditor would request. In the case of the previous examples, the control owners would need reports that list the set of authorized users and the set of authorized system changes. These reports should be designed to serve two purposes: to ensure that any exceptions the auditor will find have already been reviewed by IT management, and to ensure risk-based decisions have been appropriately made with respect to the exceptions.

Information security management adds value by anticipating the need for and providing an IT governor-sponsored information security program with remediation processes that address any evidence of unauthorized usage or change indicated by the reports. By coordinating information security management and IT governance processes, IT does not need to spend any extra staff time to gather information for auditors to pass an audit.

Step 7: Schedule and conduct regular control tests

Once information security management and business process control owners have agreed that a given standard configuration provides adequate information security and that auditing of the configuration can be automated, these decisions must be validated with respect to actual practice. An audit report that is used only by the information security management team and not given complete credence by the IT owner will be of little value to compliance efforts.

The attribute measurements of the controls must be tested frequently enough to capture any changes to the standard configuration that would present risk to the information flow. In an environment that processes millions of transactions per minute, the time threshold within which vulnerabilities should be detected will be very short. In an environment that infrequently processes transactions of value, detection of an inadequate information security configuration may be performed less frequently. Where user access and/or configuration standards are critical for meeting business process control goals, exceptions to expected configurations should generate alerts.

Where the information security goals for each information flow have been agreed upon between information security management and IT governance, the responsibility for the smooth function of each IT asset in the information flow includes the smooth functioning of the information security features that the business process control owner has agreed will be supported by that IT asset. It also includes configuration of alarms that alert IT staff when an IT asset is malfunctioning. Inadequate information security configuration is just one issue a responsible IT manager (the business process control owner) should be on the alert for, so the percentage of information security alerts should be a small fraction of the alerts the IT manager attends to on a day-to-day basis.

The role of the information security manager is to collaborate with the business process control owner on the implementation of the control enough to ensure the implementation meets the business goals for information security and conforms to the framework of the overall information security program. The information security manager should not confuse this role with taking ownership or reporting responsibility for a given portion of the business process control owner's job function. Accountability is maintained only when the process by which information security is managed and measured is not separate and distinct from the rest of the business process control owner's job.

Step 8: Organize metrics and remediation reports

For information security management to take many of the steps discussed in this paper, we must first be able to maintain control of the information flow. To have that control, we must create an information inventory by completely identifying all information flows of value to the business and of interest to an auditor. However, for this inventorying process to take place, the IT governor and information security manager must agree upon the necessity of the information inventory.

Each organization may take a different approach to taking an information inventory. However, the information inventory is only complete if it includes the set of information inventory definitions that cover any area of the business that contains any type of information flow. Some organizations use their corporate business unit structure as the basis for the classification scheme of their information inventory. Other organizations may share so many IT services that it is more convenient to classify information inventory at the IT service level—for example, the organization may classify information flow for the customer tracking data service. Even if one of the top-level classifications ends up being"miscellaneous items that have few audit and compliance requirements,"the information classification effort should exclude no information flow.

Each information inventory item may contain multiple information flows. For example, a single information inventory item may include alternative Internet-accessible options for data delivery, internal information flows for business processes and other internal information flows for administrative use. Each of these should be defined in terms of the existing IT infrastructure as well as the roadmap that supports them. The existing IT infrastructure is the set of IT assets whose current configurations are directly in scope for business process control objectives and corresponding audit, and the roadmap defines the evidence that changes to the IT assets are authorized.

Note that thinking about information flow in terms of a framework for an information security program does not necessarily mean that staff need to be re-organized around responsibilities associated with managing information flow. Thinking in these terms simply allows us to clearly define the scope of the business process control goals based on the actual information of the business. The responsibility for a secure configuration for each component may remain as is; however, if no overall coordinator is responsible for ensuring secure interactions between components of an infrastructure that support a specific information flow, then a security architect may be needed.

Step 9: Detect and respond to significant changes to the control environment.

Even in an organization where the accountability of IT owners for information security goals is well defined and managed with metrics, the requirement for business process owner control over information flow continues to require scrutiny from an information security perspective. This continued scrutiny is critical because any change to the configuration of any device within the information flow may put business goals at risk.

The following example illustrates just how configuration changes within a given information flow can put business goals at risk:

> *A business has an information flow that allows business users to interact with data one record at a time through a web application on the internal network. The web developers decide to add a feature so that users can download reports about this data to their desktops. This new feature will change the information flow by now allowing it to go to user desktops. Every organization that is part of the current information flow must be aware that changes to the information flow may impact management control in a way that is beyond their control.*

Changes that impact information flow should pass through a higher level of review and may result in changes to the scope of the information flow. In this example, if the developers were allowed to make the change, then desktop configuration and user data transfer capabilities would become part of the information flow and would be within the scope of the information security management planning. Desktop configuration and user data transfer capabilities would also be within the scope of audits concerned with the category of information in the information flow.

An IT environment in which control over end-to-end information flow can be set at the organization level and automatically audited upon demand allows automated monitoring of both access and configuration by business process control owners, as described in Step 3. In our current example, the monitoring process would detect any and all changes developers made to software. These would include web code changes as well as database query changes. Each of these changes would appear individually on a change detection console, and an information security process would compare the detected change with records of authorized changes to the information flow roadmap. Where the roadmap did not specify the changes that appeared from monitoring, an unauthorized change would be declared, and would presumably prompt an investigation into its impact on the information flow.

The Role of Tripwire Enterprise in the Nine Steps

In order to prove the effectiveness of the change and configuration controls and user access controls instituted as a result of the nine steps, we must rely on objective evidence. As the recognized leader in configuration control with powerful configuration assessment and change auditing capabilities, Tripwire® Enterprise enables organizations to provide that evidence by:

- Proving that configurations match the authorized secure state
- Proving that all system changes were authorized
- Proving that all user access changes were authorized
- Enforcing the organization's configuration policies, whether internal or external

With the complex nature of today's data center that increasingly includes virtualized infrastructure, having a single point of control for gaining visibility into changes to configurations and user access, as well as ensuring consistency of IT system configurations is a must. This single point of control ensures that in the face of dynamic environments that include application upgrades, automatically installed patches, user-made system setting changes, virtual machine managers, and virtual machines, we can still deliver high availability and performance and comply with operational and security standards.

Moving from Crisis Management to Routine Preparation

As information security managers, if we execute Steps 1 through 9 and verify the effectiveness of our controls with a configuration control solution like Tripwire Enterprise, audit preparation should be easy because all the heavy lifting has been done long before an audit. Audit goals are by definition stated clearly in terms of information security requirements for management control with respect to some type of information or business process. The controls are designed to help us determine whether management has considered risks related to the business process and whether they've adequately addressed those risks with business process controls that are measured and monitored. Through this well-planned, proactive approach, we transform audit preparation from a crisis management exercise to the routine preparation of a status report.

Addendum To Step 3: Contrasting Approaches To Controlling Change And Access

Examples and explanations of how to meet management objectives for change controls and access controls described in Step 3.

Meeting Management Objectives for Change Controls

Consider the 3rd example of reliance on IT management controls for monitoring emissions on page 9. Two possible alternatives for change controls are:

1. A process that certifies that the file system that contains the measurement software contains only the minimum number of executable programs and data sets necessary to accomplish the measurement function. Every time new measurement software code is released, the list of files in the file system gets updated. Any additional files must be certified as necessary to be included in the updated software configuration. Any time an individual logs in to any system to which this file system is available, an alert is sent to an operations team. The team verifies that an authorized individual did the login. The team also issues a command to list the files on the system. The team compares this list to the list of files authorized in the last release to provide assurance that the recent access did not result in a file system change.
2. In this alternative, the operations team similarly certifies that the file system contains only the minimum number of files required. In addition, the team creates a standard system configuration by recording and securely storing the timestamp, file type, file size, and cryptographic checksum of file contents at the time the release was certified. Periodically, an automated process lists all the files in the system and records the current timestamp, file type, file size, and cryptographic checksum of file contents. These values are compared to those recorded and stored at the time of the authorized release and any variations are accounted for. Operations monitors the results of this process to assure that the process is always running and that the monitoring process itself has not been subject to tampering.

There are important differences that make the second approach the preferred approach: the first approach relies on an expectation that changes are made only by individual actions taken by users when they login via expected processes. The second specifies what the management control objective looks like in terms of the desired result: a standard system configuration that does not change. The timestamp, file type, file size, and cryptographic checksum of files that control the information flow are measurable attributes of the information itself, and become the yardstick used to measure whether the management information security objective is met. At any given point of time, there is only one authorized set of values for those measurements.

In the first case, audit of the management control objective would require a demonstration that each authorized release of system software has been certified and approved, and some explanation of why any authorized users would need to access the file system without making any changes. Yet it gives the auditor no way to assess whether or not a file that is authorized to exist on the system has not been changed outside of the change control process. The auditor would have to perform detailed analysis of file contents to achieve the management control objective of restricting unauthorized changes. This would require close teamwork with the development team as well as operating system administrators.

In the second case, management has agreed in advance that the method by which the correctness of the file contents should be determined is through a series of automated tests. It demonstrates that the control objective is met by showing each file on the system has a set of attributes, and that the combination of these measurements can be used to provide assurance that the information flow has integrity. In other words, we can prove that we know when unauthorized changes have been made to the files. The decisions about what constitutes a correct configuration is made in terms that the IT governor easily understands and can agree on.

Presumably the second case would have few exceptions and the amount of time required by both IT staff and auditors in the second case would be exponentially less than in the first. Note that if operations routinely enforces the information security goal, they, rather than the information security professional, would need to explain any exceptions.

Meeting Management Objectives for Access Controls

Now consider a more routine example of reliance on information security generally to control access to business applications. Two possible alternatives for access controls are:

1. Users make access requests using an online form that prompts the user to enter a business purpose. The access requests are routed to the plant manager, who is charged with reviewing the job function of the requestor and the business purpose of the requested access. Based on this information, the plant manager makes a decision on whether business process justifies access.
2. Employees and contract staff are assigned roles that correspond to job descriptions. Plant information is segregated and flows into distinct business processes, and these processes are labeled with roles corresponding to the job functions that support the processes. Each role is associated with a set of access permissions to various segments of information flow specified by the plant manager.

   IT devises a standard system configuration so that these permissions are automatically provisioned for the user based on job descriptions. When a user requires more access than automatically provisioned, the user is required to state a business purpose. The plant manager must approve the business purpose. The access is provisioned to meet the requirements of the business purpose, and the new access permissions become part of the standard system configuration.

There are important differences that make the second approach the preferred approach. The first approach relies on individual decision-making to accomplish the management control objective. The second approach specifies what the management control objective looks like in terms of the desired result: a standard system configuration that ensures that all access provisioned is required by a business purpose. The labels on the information flow become a measurable attribute of the information itself, and the list of roles corresponding to job descriptions becomes the yardstick for measuring whether the information security objective has been met.

In the first case, audit of the management control objective would require a demonstration that each individual with access has a corresponding, approved request for that access. This approach requires the plant manager to explain each business purpose and makes the auditor determine whether or not the process has achieved the management control objective of minimizing access by job function.

In the second case, management has agreed in advance that the plant manager executes a given business process by relying on certain activities that correspond to defined job functions. This approach demonstrates that the control objective is met by showing that each individual who has access belongs to a role, and that any exceptions can be correlated with an access request that has an approved business purpose. The decisions about who should have what access are evident in the agreed upon system configuration. Decisions about minimizing access are made at the macro level in terms that are easily understood and agreed upon by the IT governor.

Presumably the second case would have few exceptions, and the amount of time required by both IT staff and auditors in the second case would be exponentially less than in the first. Note that if the plant manager routinely enforces the information security goal, the plant manager, rather than the IT or information security professional, would have to explain any exceptions. The actual cost savings of choosing alternative one over alternative two would depend on the number of users in the audit test sample.

About the Authors

Jennifer Bayuk

Jennifer Bayuk is an independent consultant on topics of information confidentiality, integrity, and availability. She is engaged in a wide variety of industries with projects ranging from oversight policy and metrics to technical architecture and requirements. Jennifer has a wide variety of experience in virtually every aspect of the Information Security. She was a Chief Information Security Officer, a Security Architect, a Manager of Information Systems Internal Audit, a Big 4 Security Principal Consultant and Auditor, and a Security Software Engineer.

Jennifer frequently publishes on information security and audit topics. Jennifer has lectured for organizations that include ISACA, NIST, and CSI. She is certified in Information Systems Audit (CISA), Information Security Management (CISM), Information Systems Security (CISSP), and IT Governance (CGEIT). She is an industry professor at the Stevens Institute of Technology and has Masters Degrees in Computer Science and Philosophy.

Gene Kim

Gene Kim is the CTO and co-founder of Tripwire, Inc. In 1992, he co-authored Tripwire while at Purdue University with Dr. Gene Spafford. Since 1999, he has been studying high performing IT operations and security organizations. In 2004, he co-wrote the Visible Ops Handbook, codifying how to successfully transform IT organizations from "good to great." In 2008, he co-authored Security Visible Ops Handbook, a handbook describing how to link IT security and operational objectives in four practical steps by integrating security controls into IT operational, software development and project management processes.

Gene is a certified IS auditor, and is part of the Institute of Internal Auditors GAIT task force that developed and published the GAIT Principles and Methodology in January 2007, designed to help management appropriately scope the IT portions of SOX-404. In 2007, ComputerWorld added Gene to the "40 Innovative IT People Under The Age Of 40" list, and was given the Outstanding Alumnus Award by the Department of Computer Sciences at Purdue University for achievement and leadership in the profession.

tripwire™
www.tripwire.com
US TOLL FREE: 1.800.TRIPWIRE **MAIN:** 503.276.7500 **FAX:** 503.223.0182
101 SW Main St., Ste. 1500 Portland, OR 97204