

realtimepublishers.comtm

The Practical Guidetm To

Assuring Compliance



Rebecca Herold

Introduction

By Sean Daily, Series Editor

Welcome to *The Practical Guide to Assuring Compliance!*

The book you are about to read represents an entirely new modality of book publishing and a major first in the publishing industry. The founding concept behind Realtimepublishers.com is the idea of providing readers with high-quality books about today's most critical IT topics—at no cost to the reader. Although this may sound like a somewhat impossible feat to achieve, it is made possible through the vision and generosity of corporate sponsors such as NetIQ, who agree to bear the book's production expenses and host the book on its Web site for the benefit of its Web site visitors.

It should be pointed out that the free nature of these books does not in any way diminish their quality. Without reservation, I can tell you that this book is the equivalent of any similar printed book you might find at your local bookstore (with the notable exception that it won't cost you \$30 to \$80). In addition to the free nature of the books, this publishing model provides other significant benefits. For example, the electronic nature of this eBook makes events such as chapter updates and additions, or the release of a new edition of the book possible to achieve in a far shorter timeframe than is possible with printed books. Because we publish our titles in “real-time”—that is, as chapters are written or revised by the author—you benefit from receiving the information immediately rather than having to wait months or years to receive a complete product.

Finally, I'd like to note that although it is true that the sponsor's Web site is the exclusive online location of the book, this book is by no means a paid advertisement. Realtimepublishers is an independent publishing company and maintains, by written agreement with the sponsor, 100% editorial control over the content of our titles. However, by hosting this information, NetIQ has set itself apart from its competitors by providing real value to its customers and transforming its site into a true technical resource library—not just a place to learn about its company and products. It is my opinion that this system of content delivery is not only of immeasurable value to readers, but represents the future of book publishing.

As series editor, it is my *raison d'être* to locate and work only with the industry's leading authors and editors, and publish books that help IT personnel, IT managers, and users to do their everyday jobs. To that end, I encourage and welcome your feedback on this or any other book in the Realtimepublishers.com series. If you would like to submit a comment, question, or suggestion, please do so by sending an email to feedback@realtimepublishers.com, leaving feedback on our Web site at www.realtimepublishers.com, or calling us at (707) 539-5280.

Thanks for reading, and enjoy!

Sean Daily

Series Editor

Foreword

In the technology-centric environment in which we work today, the ability to manage information risks is yet another critical requirement for business success. Making an even more challenging environment, the government regulates almost every aspect of running a business. These two issues combine to create substantial responsibilities on the part of business executives.

From the Health Insurance Portability and Accountability Act (HIPAA) and the Sarbanes-Oxley Act in the United States to various international privacy and security laws, regulations have quite a grip on information technology—and that grip appears to be getting tighter. What used to be a concern only for corporate legal counsel and network administrators has grown to be the focal point of executive and boardroom discussions.

The government is mandating what would otherwise be general information technology best practices to force businesses to protect customer information and prevent corporate misdeeds. Businesses are often expected to have effective information security infrastructures in place—and the task of implementing such an infrastructure is not simple. These new government regulations have ushered in a new era for running a business.

Business executives are now faced with many questions about how to effectively manage information technology and stay out of legal trouble. General information security safeguards that are put in place and revisited once a year for the sake of compliance are not an effective way to manage these new regulatory challenges. Information security products in and of themselves are not the only solution either. What is required is a strong combination of policies, business processes, and technologies that are understood and supported not only by the executives but also by every employee. This recipe for success, combined with recent information security product innovations, has made the process of getting people and technology to work together to improve information security much easier.

Business executives that embrace a philosophy and culture of information security and lead by example can and will be successful during these challenging times of trying to balance compliance with information risks and business goals. Fortunately, positive side effects of solid information security leadership are enhanced information risk mitigation and ongoing government compliance.

One of the best ways for business executives to manage these issues and implement proper solutions is to educate themselves. However, with so many scattered resources available, it is difficult to sort through them to discover what really needs to be done. In this guide, Rebecca Herold has done an excellent job of presenting the essential information required. Her coverage of what IT and business executives really need to know and her practical solutions are worth their weight in gold.

Kevin Beaver, CISSP

Introduction.....	i
Foreword.....	ii
The Practical Guide to Assuring Compliance.....	1
Basing Security upon Service Management	1
Identifying Risks to Executives	2
Making Security a Business Responsibility.....	2
Determining the Effectiveness of In-House–Created Tools	3
Basing Security Effort upon Potential Impact	4
Establishing a Compliance-Management Framework	5
Establishing a Central Security Management Area	7
Creating a Security Charter.....	8
Designating a Distributed Security Implementation Group.....	9
Identifying Major Compliance Issues.....	10
Defining Information Assets.....	11
Defining Controls.....	11
Selecting Controls.....	13
General IT Controls	14
Application and Data Controls.....	14
Change Controls.....	15
Preventive and Detective Controls.....	16
Mitigating and Compensating Controls	17
Documenting the Compliance and Risk Management Process	18
Creating an Operationalized Compliance Framework.....	19
Identifying Legal and Regulatory Requirements.....	23
Determining What These Regulations and Standards Mean to Organizations.....	23
Finding Leverage Points for Standards and Regulations.....	24
Applying Policies and Practices Based Upon Business Environment, Drivers, and Goals.....	25
Determining Acceptable Risk and Choosing Appropriate Controls.....	25
Creating a Sustainable Policy Management Process	26
Certifying Security Controls.....	29
Verifying Controls Adequacy	29
Monitoring and Evaluating Policy and Control Effectiveness	29
Summary.....	30

Copyright Statement

© 2004 Realtimerepublishers.com, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtimerepublishers.com, Inc. (the "Materials") and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtimerepublishers.com, Inc or its web site sponsors. In no event shall Realtimerepublishers.com, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtimerepublishers.com and the Realtimerepublishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtimerepublishers.com, please contact us via e-mail at info@realtimerepublishers.com.

The Practical Guide to Assuring Compliance

In today's integrated, regulated, litigated environment, it is necessary to provide assurance to customers, business partners, regulators, and sometimes even the courts that you have done your due diligence in securing your IT infrastructure. New and updated United States laws are increasingly making corporate management responsible for ensuring compliance, as companies face substantial fines and penalties for not doing so. Existing and emerging global security and privacy laws and regulations make keeping up with multinational compliance requirements imperative.

Organizations must have a business-based security framework built upon leading practices that not only allow compliance with policy and regulations but also provide a way to proactively identify risks, document compliance gaps, and report the state of the current security environment. The security framework must provide a sustainable process that allows for ongoing management of risks and compliance and must be built upon leading practices, accepted standards, contractual requirements, and applicable laws.



Executives must implement information security programs and demonstrate due diligence for how their organizations' processes information.

Basing Security upon Service Management

Security should be part of the larger information management process and strategy and should be service management based. This epitome is accomplished through the creation and implementation of a shared security service implementation program and framework composed of

- Security architecture—The governance for security through which organization-wide policies are created and maintained
- Operational management—How and what the security and compliance areas do to offer security services throughout the organization to implement information security governance
- Certification and verification—A structured framework through which governance is implemented and ensured throughout the organization's business units



Automate your certification and verification processes as much as possible to ensure consistency and efficiency with these important tasks.

Identifying Risks to Executives

Executives have increasing exposure to information security risks as technology advances and new laws and regulations are implemented. Executives are susceptible to risks such as

- Not being aware of existing risks within the organization and not knowing which risks are most significant
- Failure to create, support, and communicate an adequate and effective security culture and control framework to meet business needs
- Failure to effectively delegate responsibilities for risk management throughout all levels of the organization
- Failure to detect where security weaknesses exist within the organizational business units
- Failure to successfully monitor risk management activities to ensure compliance with policy



Security is not a one-time effort. IT environments keep changing, new laws and regulations are being passed every day, and new security risks can occur or develop at any time.

Making Security a Business Responsibility

Information security must be viewed as a business responsibility and must be shared by all members of business management. It is most effective to incorporate security throughout the business units by creating a security management oversight council to ensure that there is clear security direction and apparent management support for security initiatives. Such a council should promote and enhance security within all business processes by applying appropriate commitment and adequate resources.


For some organizations, the oversight council may be part of an existing management body. In others, it will be most effective to create a new group of managers to oversee security. Typically, an information security oversight council

- Reviews, approves, and visibly supports information security policy and overall responsibilities
- Monitors significant changes in risks to information assets and emergence of major threats
- Reviews and monitors information security incidents and how they were resolved
- Approves major initiatives to enhance information security



The information security officer should head the information security management oversight council to ensure consistent security is implemented throughout the organization.

To be successful in today's information economy, enterprise business governance and IT governance can no longer be considered separate and distinct disciplines. Effective enterprise governance must focus individual and group expertise and experience where it will be most productive. Governance must monitor and measure performance and provide assurance to critical security issues. Information security must be regarded as an integral part of business strategy.

 An IT governance structure should link and integrate the IT security processes and resources with the business strategies and objectives.

A successful IT governance framework will integrate and optimize the way IT functions and associated business processes are planned, organized, acquired, implemented, delivered, supported, and monitored. IT governance, which includes security within every element, is integral to the success of enterprise-wide governance. IT governance should assure efficient, effective, and measurable improvements throughout all enterprise processes. Effective IT governance will enable the enterprise to use information in the most efficient and effective way possible, which will ultimately increase business benefits, put the organization in a position to take advantage of emerging opportunities, and enable the company to gain a competitive advantage.


Determining the Effectiveness of In-House–Created Tools

Many organizations develop software tools for network monitoring or to perform security activities internally in an effort to save money and avoid purchasing vendor products. Systems administrators often develop such tools for logging, auditing, and other similar types of non-compliance monitoring. Dependence upon such in-house–created tools and related procedures may seem cost effective for determining the effectiveness of security controls, but usually such tools tend to address security risks in a patchwork fashion, do not provide a big-picture view, leave compliance gaps, and do not consider all risks. IT environments are continually changing, and new security risks and threats can occur at any time. Security tools must be able to address such challenges. Consider the following questions to help determine whether the in-house security tools you use are effective:

- Can in-house tools address significant emerging risks?
- Have you performed a gap analysis to find areas that your in-house–created tools do not address?
- Have such tools been vetted by independent and objective personnel to determine thoroughness and effectiveness?
- Do the tools address all regulatory requirements for your organization?
- Are the tools compatible with all new systems?


-
- Will the tools still work when systems are upgraded or patched?
 - Can in-house personnel effectively support the tools?
 - Does clear and comprehensive documentation exist for the in-house tools?
 - Do you have more than one person who knows how to use the tools?
 - Are the tools, including the source code, stored securely so that only authorized personnel can access them?

If you answered no to any of these questions, your in-house tools may themselves be creating significant risks to your business and could create a false sense of security for your business managers.

 If you cannot make changes within your current tools to result in “yes” answers to all the previous questions, consider obtaining a comprehensive, vetted, and well-maintained security product. Doing so will save much time and effort for your internal staff in the long run compared with trying to support proprietary in-house code and tools.

Basing Security Effort upon Potential Impact

The amount of effort applied to implementing a safe and secure working environment should be based on how much of an impact security problems can have upon your business. However, implementing adequate and effective security does not necessarily mean investing large amounts of time or expense. For example, making the effort to raise awareness, identify security risks, and taking prudent precautions for IT practices and processes is achievable with significantly less effort when following a thoughtful compliance plan. Implementing the accompanying technical safeguards for the identified risks can be more complex and expensive. Thus, it is important for organizations to rely upon and implement proven products from reputable suppliers, and, when necessary, call experts for advice. It is important to remember that all these security efforts are not something that should be done once; they require constant and continuous attention.

 Managing security is not a one-time event. It must be done continuously and include a cycle of planning improvements to the security program components, implementing the changes, evaluating the effectiveness of the security program, then starting again with improvements.

Establishing a Compliance-Management Framework

An overall compliance-management framework must include needs assessment, design, metrics, evaluation, and ongoing sustainable value (see Figure 1). The implementation of a compliance-management framework must move from being a project to being a sustainable business process.

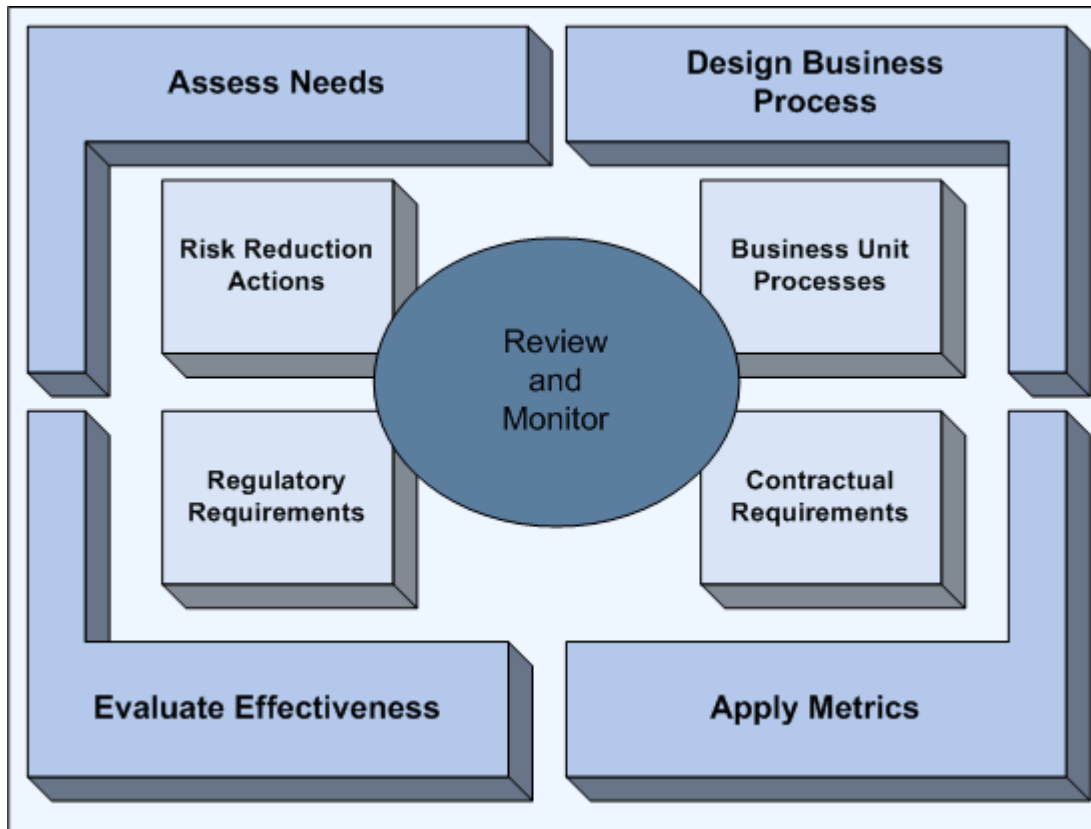


Figure 1: An overall compliance-management framework.

IT resources must be managed according to business and service-grouped processes to provide the information the organization needs to achieve business objectives. As technology, business, and regulatory issues have become more complex, it has become evident that there is a need for a security and control reference. A compliance-management framework should contain such a reference. Successful businesses need to appreciate and understand the risks and constraints of IT throughout all areas of the enterprise if they hope to achieve effective security direction and adequate business-based controls.

Management must determine a reasonable investment amount for security and controls within IT systems. They must learn how to balance risk and control investments in what is typically an unpredictable IT environment. They must learn how to implement controls in such an unpredictable IT environment to reduce risk to an acceptable level without interfering with business activities. Management must understand that although information systems security and controls help manage and reduce risks, such security and controls do not eliminate risks. The exact level of risk can never be known or measured; there is always uncertainty involved with trying to anticipate what security incidents can possibly occur.

Ultimately, management must decide on the level of risk it is willing to accept. Judging what level can be tolerated, particularly when weighed against the associated costs of the control compared with the cost of the asset being protected, can be a difficult management decision. To facilitate such decisions, management needs a framework of generally accepted IT security and control practices to benchmark the existing and planned IT environment.

New business complexities create a greater need for IT service users to be assured that adequate security and controls exist. Such assurance can be accomplished through certification and audit of IT services—either by internal or external reviewers—that ensure adequate, business-focused security and controls exists.

Implementing effective IT security and controls within information systems can cause confusion. Confusion results from the use of numerous and inconsistent evaluation methods. Before choosing one evaluation method, personnel within organizations who are responsible for implementing security and controls must first establish a general foundation of security and controls. The foundation for effective business security and controls will be comprised of actions that ensure business information is

- Effective
- Efficient
- Confidential
- Accurate
- Useful
- Timely
- Available
- Compliant
- Reliable

Adequate business resources must also be available throughout the business units to effectively incorporate security and controls. These resources include:

- People
- Applications
- Technology
- Facilities
- Data

Establishing a Central Security Management Area

A central security management area will ensure compliance projects and processes are operationalized throughout all business units. Suitable security management leadership must be established to approve the information security policy, assign security roles, and coordinate the implementation of security throughout all areas of the organization. This security management area should also serve as a source of specialized information security knowledge and advice for the organization. The central security management area should develop contacts with external security specialists (such as consultants, professional organizations, industry peers, and so on) to keep up with leading practices, industry trends, assessment methods, and new and emerging regulatory requirements as well as provide suitable liaison points when dealing with security incidents. Information security should be approached as multi-disciplinary.

☞ Involve and gain the cooperation of business unit managers, users, administrators, application designers, auditors, security staff, and specialists in areas such as insurance, physical security, and risk management. Collaborate with these contacts and maintain ongoing communications.

The central security management area will successfully incorporate security throughout the organization by ensuring that

- Security policies, goals, standards, and other security activities reflect business objectives
- An approach to security implementation is consistent with the organizational culture
- Visible support and commitment is obtained from executive management
- The organization has a clear understanding of security requirements, applicable laws and regulations, contractual requirements, risk assessment, and risk management
- Effective marketing of security to all levels of personnel are provided
- Widespread distribution of guidance information on security policies, standards, and guidelines is provided to all employees, contractors, and others who handle the organization's information
- Ongoing appropriate training and education is provided to all employees in addition to specialized education to target groups
- A comprehensive and balanced system of measurement is used to evaluate performance in information security management and a mechanism is in place for feedback and suggestions for improvement

Creating a Security Charter

A charter for the security function should be established by the central security management area and visibly endorsed and supported by senior management. The charter should outline the responsibility, authority, and accountability of the IT security function. The charter should be reviewed periodically to ensure that the independence, authority, and accountability of the IT security function are maintained. The charter should require the creation, implementation, and maintenance of a management framework to govern information security within the organization in a way that is best suited for business and supports business goals (see Figure 2).

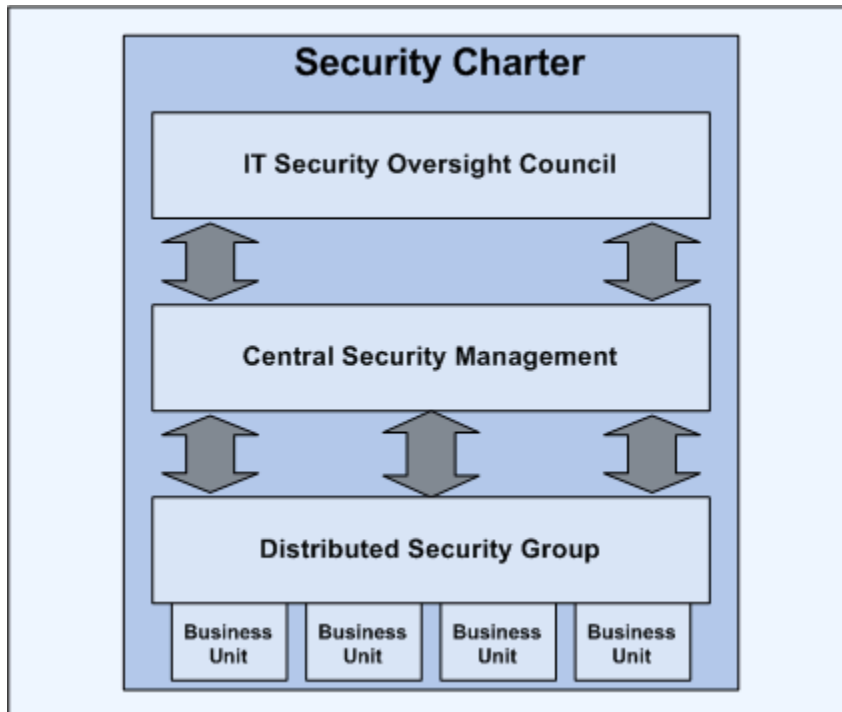



Figure 2: Develop a charter that demonstrates the organization's commitment to information security.

 Develop a written information security charter that demonstrates executive commitment to information security and customer privacy. Such a document helps organize support throughout the organization for reinforcing the importance of each employee's role in maintaining security.

Designating a Distributed Security Implementation Group

Identify key personnel within each of the business units and operational areas to be responsible for performing specific security activities that are crucial to your security program success. Train the personnel to efficiently and effectively perform the activities. Explain how the activities support the business and help to meet business goals. Specific security activities for the group should include:

- Identifying information assets
- Classifying and prioritizing assets
- Identifying risks
- Defining security and control requirements
- Testing security and control requirements
- Implementing security requirements
- Monitoring the effectiveness of security and controls
- Staying aware of new threats and risks
- Updating controls

This group should also act as a central advisory committee to provide recommendations to the security management area for the purchase, strategy development, and deployment of new security and controls equipment, software, and training based upon business needs and processes. The members of the group must be aware of the products currently available as well as the emerging technologies that may affect the viability of current products or purchases.



The members of the distributed security group should consist of a combination of visionaries, technical experts, and strategic business planners. Take care to ensure that the members of this group do not become unreasonably influenced by or restricted to one particular vendor or supplier.



Central procurement is a significant principle of security management. When an organization is spread out geographically, there is a tendency for each business unit or department to purchase IT resources independently. Organizations can easily lose control over standardized hardware and software systems and may end up with incompatible virtual private networks (VPNs), difficult maintenance and support, loss of savings that may have been available through bulk purchases, ineffective disaster recovery planning through the need to communicate with many vendors, and loss of inventory control. Computer equipment may become untraceable and subject to theft or misuse by personnel. The distributed security group should ensure that all procurement of IT equipment is centralized.



At a minimum, put security responsibilities into the job descriptions for the identified security positions. Ideally, put security responsibilities into all enterprise job descriptions to make it clear that security is everyone's responsibility. If the responsibilities are formally documented, and the personnel will have the security activities included in their appraisal process, it is more likely that the activities will be successfully accomplished.


Identifying Major Compliance Issues

Compliance involves following the requirements of the laws, regulations, and contractual arrangements to which the business process is subject. Management must ensure that appropriate procedures and systems are in place to determine whether personnel understand the implemented policies and procedures and that the policies and procedures are being followed. Compliance issues include:

- Contractual commitments
- External requirements
- Laws and regulations
- Generally accepted standards
- Organizational policies, procedures, and standards
- Legal and regulatory development monitoring
- Compliance monitoring
- Privacy
- Intellectual property

It is important to explore and identify the compliance issues for your organization. To do so, consider the following questions:


- Within which locations do you process, handle, or store information?
- With which information handling laws must you comply?
- With which privacy laws must you comply?
- Which business partners access or process your organization's information and/or processing systems?
- What information and privacy requirements exist within your customer contracts?
- What information and privacy requirements exist within your business partner contracts?
- For which copyright and licensing requirements is your organization obligated?

 Create a central compliance inventory to more easily document and track all compliance issues throughout the organization. Doing so will also help to ensure all compliance issues are addressed consistently throughout the organization.


Defining Information Assets

Organizations must know what information assets they own or manage. Assets must be identified in order to establish controls to secure them. After all, if you don't know what you are protecting, how can you possibly protect it? Creating an inventory of information assets will help ensure that effective asset protection takes place. Establishing an inventory may also be required for other business purposes, such as health and safety, insurance, or financial asset management reasons.

Creating an information asset inventory process is an important aspect of risk management. An organization must identify assets and the relative value and importance of these assets. Based on this information, an organization can provide levels of protection commensurate with the value and importance of the assets. Create and maintain an inventory of the assets associated with each information system. Clearly identify each asset along with the corresponding owners, security classification—such as confidential, secret, internal use only, public, or whatever classification labels you are using—and current location (important for resumption and recovery from loss or damage). Classification will enable the proper identification of security requirements that drive the selection of appropriate controls to protect the information.


 Ideally, the information asset inventory should be automatically generated or at least automatically maintained. If not, it will be out of date very quickly and will not aid in the risk management process.

Once the inventory is created, prioritize the assets and applications that support critical business functions. Determining the criticality of information assets might seem overwhelming at first and can be quite an arduous task. However, it is important to identify at least the business mission-critical assets. As with creating the inventory, it will be most efficient to use an automated tool to assist with this task.

 Work with the business continuity group to determine what has already been identified as critical. If your organization doesn't have a business continuity group, focus on assets that must be available for your business to function and generate revenue or service customers. Remember to include the core processing systems requirements, such as minimum storage requirements, minimum memory requirements, bandwidth requirements, and so on.

Defining Controls

Security controls are implemented to protect the confidentiality, integrity, and availability of information resources. Confidentiality controls help prevent unauthorized disclosure of information. Integrity controls help prevent unauthorized modification of information and systems. Availability controls help to ensure that uninterrupted access to information and IT resources is provided.

 Within various standards and regulations throughout the world, the terms *controls*, *safeguards*, and *countermeasures* are often used synonymously.

Information security is achieved by implementing a set of controls appropriate for the business and processing environment. There are three main types of controls—administrative, technical, and physical—to address and help to insure confidentiality, integrity, and availability. Such controls must be in place to ensure that the business and security objectives of the organization are met. Examples of administrative controls include:

- Policies
- Standards
- Procedures
- Guidelines
- Awareness activities
- Training
- Personnel screening

Examples of technical controls include:

- Logical access controls
- Security devices
- Identification
- Authentication
- Encryption

Examples of physical controls include:

- Facility protections
- Security guards
- Closed-circuit television and other monitoring devices
- Locks
- Physical intrusion detection
- Environmental controls

It is a current reality that many IT systems were not designed to be secure. The security that can be achieved through technical means is limited and should be supported by appropriate management and procedures by using administrative and physical controls. Identifying which controls should be in place requires careful planning and attention to detail. Information security management needs participation by all areas throughout the organization to successfully implement controls. Information security management also needs active participation and cooperation from business partners, vendors, suppliers, customers, and shareholders. Specialist advice from outside the organization may also be needed.

Selecting Controls


After identifying information assets, risks, and security requirements, select and implement controls to reduce risks to an acceptable level. Some controls are not applicable to every information system or environment and might not be practicable for all organizations. Controls should be selected based on the cost of implementation in relation to the risks being reduced and the potential losses if a security breach occurs. Also take into consideration non-monetary factors such as loss of reputation and applicable laws.

General controls considered to be essential to an organization from a legislative and regulatory perspective include:


- Protecting data and privacy of personal information
- Safeguarding organizational records
- Protecting intellectual property and maintaining intellectual property rights

General controls considered to be common best practice for information security include:

- Publishing and communicating information security policies
- Allocating information security responsibilities
- Implementing ongoing information security education, awareness, and training
- Implementing procedures and processes to report security incidents
- Incorporating technical security controls into the systems and process-development life cycle
- Establishing business continuity management

 Ensure that the costs and benefits of security and controls are carefully examined in monetary and non-monetary terms. The costs of controls must not exceed their benefits or the potential impact of risks.


Applicable business management must formally accept the chosen controls to ensure the most effective implementation; facilitating acceptance and implementation throughout the organization. All security requirements should be identified during the requirements phase of a project and justified, agreed upon, and documented as part of the overall business case for an information system or business process.

 Don't forget to define the security requirements for business continuity management during the requirements phase of a project. Doing so will ensure that the planned activation, fallback, and resumption processes for the business are supported by the proposed solution.

General IT Controls


Organizations have many types of information resources to protect from unauthorized access. The security management framework must include controls to ensure that only the intended people and processes can access information for necessary business purposes. In addition, the framework must establish a way to allow only the level of access necessary to accomplish business tasks. IT controls are necessary to prevent compromise or theft of information and information processing facilities. Controls must protect information and information processing facilities from disclosure to, modification by, or theft by unauthorized persons. Controls must be implemented to minimize to the fullest extent feasible and appropriate loss or damage to IT resources.

More controls are needed beyond simply requiring user identifiers and passwords—there is much more involved with implementing effective IT controls. There are many different methods, techniques, technologies, and models to consider and choose from to best serve your business purposes and systems.

 The most effective controls are incorporated in a layered approach to ensure that all gaps have been addressed and vulnerabilities are not overlooked. A layered approach also helps protect the organization if one control fails or is compromised—the other controls will continue to provide protection to the organization. For example, using antivirus software on the mail gateway and users' desktops as well as a packet-filtering router and a firewall.

Application and Data Controls

Application and data controls are used for transactions and data that relate to each computer-based application or system and are tailored to address the business risks for the particular corresponding application or system. The objectives of application and data controls are to ensure the completeness and accuracy of the records and the validity of the data input to the application or system from both manual and automated or programmed processing.

 Examples of application and data controls include using checksums, encrypting data while in transit or in storage, employing data input validation, performing batch total reconciliation, and so on.

Change Controls

Changes within software and systems development and maintenance are inevitable and must be carefully controlled to ensure that security and controls are established and preserved during updates. A process must be in place to deal with changes or the project will not meet milestones and important controls may be lost in the shuffle. It is also important for such a process to be followed to ensure that the changes do not result in controls (or lack of controls) that negate the established security policies and risk reduction requirements. The following list highlights typical change control process steps:

1. Outline business reasons for the changes
2. Formally submit the change request
3. Review and analyze the request
4. Develop the change implementation strategy
5. Determine the costs of the implementation
6. Identify the security and control considerations
7. Document the change request
8. Submit the change request for approval
9. Change the application or system
10. Document backup procedures
11. Link the changes in the code or system to the formal change control request
12. Test the changes and ensure that they have gained quality control approval
13. Repeat steps 8 through 12 until the changes have been approved
14. Make version changes and move to production
15. Report changes to business management and other affected users

Preventive and Detective Controls

Preventive and detective controls are operational controls that are vital to ensuring that a business process is adequately secured; these controls are often overlooked or omitted.

Preventive controls are used to help keep undesirable incidents from occurring. They are the first line of defense for a business process. There are administrative, technical, and physical types of preventive controls. Examples of administrative preventive controls include:

- Policies and procedures
- Background checks
- Hiring practices
- Documented termination processes
- Data classification and labeling
- Security awareness and training
- Separation of duties

Examples of physical preventive controls include:

- Guards
- Fences
- Locks
- Visible alarms
- Badges
- Swipe cards

Examples of technical preventive controls include:

- Passwords
- Biometrics
- Smart cards
- Encryption
- Malware protection
- Firewalls
- Router access control lists (ACL)
- Intrusion prevention systems

Detective controls identify problems and errors in access controls and can be used to help determine the effectiveness of the preventive controls that are in place. Detective controls typically produce information that can be reviewed after an event occurs to help understand what caused the event and that can identify suspicious activity to point to an event. There are administrative, technical, and physical types of detective controls. Examples of administrative detective controls include:

- Sharing responsibilities
- Job rotation
- Inspections
- Evaluations
- Investigations

Examples of technical detective controls include:


- Intrusion detection systems
- Audit log reviews
- Incident report reviews
- Violation report reviews

Examples of physical detective controls include:


- Guards viewing cameras and monitors
- Motion detectors
- Video camera feeds

Mitigating and Compensating Controls

There will be situations in which it might not be possible to completely implement control objectives as required, resulting in increased risk to business operations. Additionally, in some situations, a desired control may be missing or cannot be implemented. In such events, management must evaluate the costs and benefits of implementing additional controls to compensate for the lack of required controls and adequately reduce risk. Compensating controls may include other technologies, procedures, or manual activities to further reduce risk to an acceptable level.

 For example, it is an accepted best practice to prevent application developers from accessing the production environment to limit the risk of having improperly tested or unauthorized program code changes. However, if the application developer is also part of the application support team, a compensating control could be used to *allow* the developer *restricted* (monitored and/or limited) access to the production system, under certain conditions when it is necessary for business continuity. The compensating controls could be a combination of requiring the developer to use a special user ID in such circumstances, along with logging all activity under the ID, and having management review the ID activity regularly.

There will be situations in which there may not be effective controls available to reduce the amount of risk to acceptable levels. In these situations, mitigating controls should be implemented. Mitigating controls are additional measures that help lower the risk to more acceptable levels. During the mitigation process, identify alternative or additional control methods to further reduce risk.

 For example, much sensitive information is now being stored and processed on portable computing devices, such as PDAs. A user ID and password that provide access to the sensitive information stored on such devices does not provide sufficient security controls. Additional mitigating controls that can be used to further reduce risk include such measures as implementing data encryption on the device as well as installing a physical security mechanism to the device to make it less likely that the device will be stolen or lost.

Documenting the Compliance and Risk Management Process

A critical component of creating the security management framework and supporting processes is identifying business and security requirements. To accomplish this, assess risks to the organization and identify compliance requirements. The risk assessment will identify threats to assess and evaluate as well as enable an organization to estimate vulnerability to and likelihood of threat occurrence and potential impact to the organization. Identify the legal, statutory, regulatory, and contractual requirements that the organization has with trading partners, contractors, and service providers. Identify all principles, objectives, and requirements for information processing within the organization that exist to support operations. With this information, and the previously performed tasks, document the compliance and risk management process. The process will generally include the following steps:

1. Identify risks
2. Establish policies and procedures linked to business risks
3. Communicate policies, standards, and guidelines
4. Establish supporting procedures
5. Train and certify users
6. Control access
7. Test controls
8. Monitor systems and access
9. Retain audit logs
10. Ensure acceptable usage
11. Enforce segregation of duties
12. Ensure business continuity and availability
13. Educate personnel about security programs
14. Enhance personnel security skills and knowledge with ongoing awareness activities
15. Evaluate effectiveness

Creating an Operationalized Compliance Framework

An organization must know partner and customer contracts and related security issues. To ensure internal compliance, the organization must communicate security charter and security program components continuously through a sustainable ongoing framework. And, very important but often overlooked, an organization must monitor and evaluate policy and control effectiveness (see Figure 3). To enable these measures, an organization must:

- Establish a full security policy life cycle
- Manage policies using a consistent, sustainable, and automated life cycle
- Ensure that policies evolve to counteract the continually adjusting landscape of regulations and threats to the enterprise
- Establish communication paths within the business units to ensure that all issues are covered by the policies and that the requirements support business functions appropriately
- Monitor and evaluate policy and control effectiveness

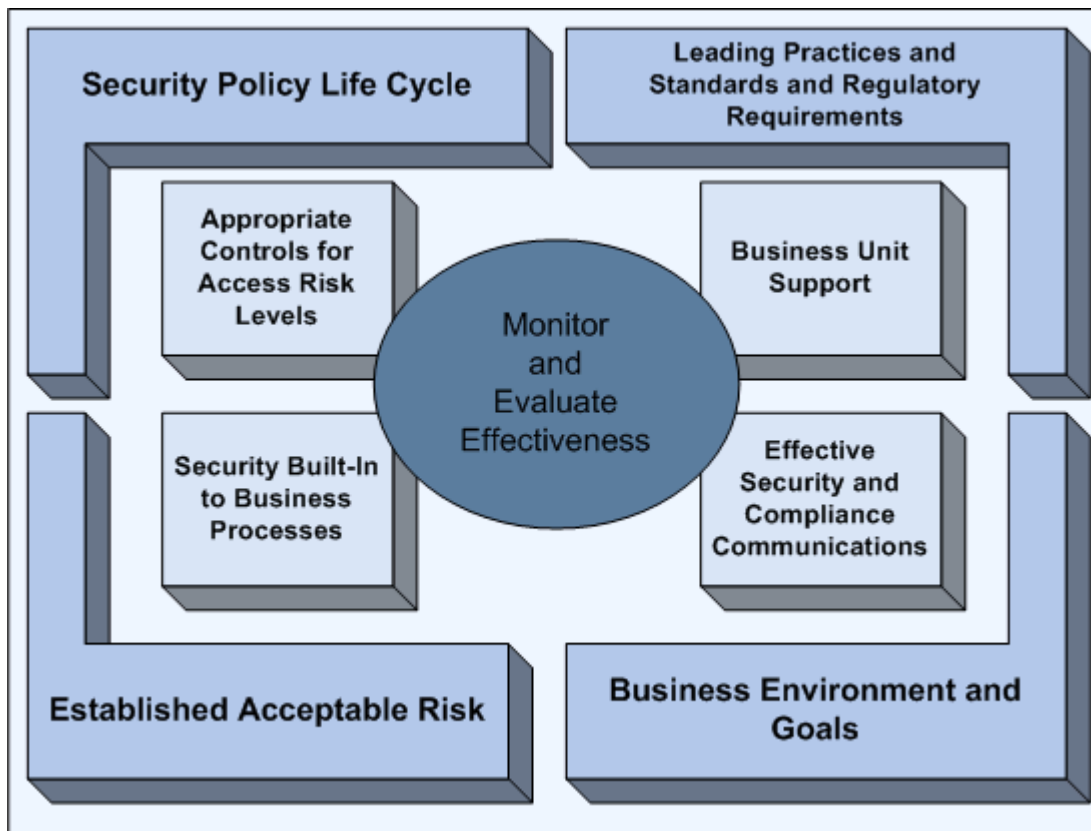


Figure 3: Develop an operationalized compliance framework.

In an attempt to attain a consistently high level of computer security, several organizations—especially those that are government-sponsored—have established information and computer security standards. The standards are used to determine the security classification that a hardware or software product is assigned and to identify controls based upon risks. The standards identify the security criteria that a product or service must meet in order adequately provide security. Popular standards include:

- Control Objectives for Information and related Technology (COBIT)
- Generally Accepted Systems Security Principles (GASSP)
- ISO 17799—Code of practice for Information Security Management
- Organization for Economic Co-operation and Development (OECD) international control recommendations
- Common Criteria—Formal methods of test; the successor of the Trusted Computer Security Evaluation Criteria (known as the Orange Book)

The challenge organizations face when using such standards is that, with the exception of the more general OECD principles, they are so massive and stringent that few organizations make it all the way through the requirements—let alone dedicate the time and resources necessary to become completely compliant with any one of them. However, organizations can use the most applicable objectives that are common across the standards as a basis for information governance controls. There are many overlapping concepts between two of the most commonly used standards, ISO 17799 and COBIT.

ISO 17799

British Standard (BS) 7799 is a standard that sets the requirements for an information security management system and is recognized and used worldwide. The requirements “help identify, manage and minimize the range of threats to which information is regularly subjected.” The BS 7799 information security standard is published in two parts:

- ISO/IEC 17799—Code of practice for Information Security Management (commonly referenced as ISO 17799)
- BS 7799-2:2002—Specification for Information Security Management

This process-driven and technology-independent standard was developed by a consortium of companies throughout the world and describes best practices for information security in the following operational areas:

- Security policy
- Organizational security
- Asset classification and control
- Personnel security
- Physical and environmental security
- Communications and operations management
- Access control
- Systems development and maintenance
- Business continuity management
- Compliance



The ISO 17799 standard gained widespread recognition following publication by the International Standards Organization (ISO) in December of 2000. Formal certification and accreditation were introduced around the same time.

COBIT

COBIT serves as a framework of generally applicable security and control practices for IT control and is recognized and used worldwide. The report can be ordered from the Information Systems Audit and Control Association (ISACA) by phone or mail. The COBIT framework strives to help management benchmark the security and control practices of IT environments, allows users of IT services to be assured that adequate security and control exists, and allows auditors to substantiate their opinions about internal control and to advise on IT security and control matters. The primary motivation for ISACA to provide the framework was to enable the development of clear policy and good practices for IT control throughout the industry worldwide. It consists of four primary operational domains, each with multiple identified control processes.



COBIT was first published in 1996 and is now in its third edition. COBIT is one of the most popular and internationally accepted sets of guidance materials for IT governance.

There are many commonalities between the assorted security standards. For example, at a high level, ISO 17799 and COBIT both recommend 20 common controls, as Figure 4 illustrates.

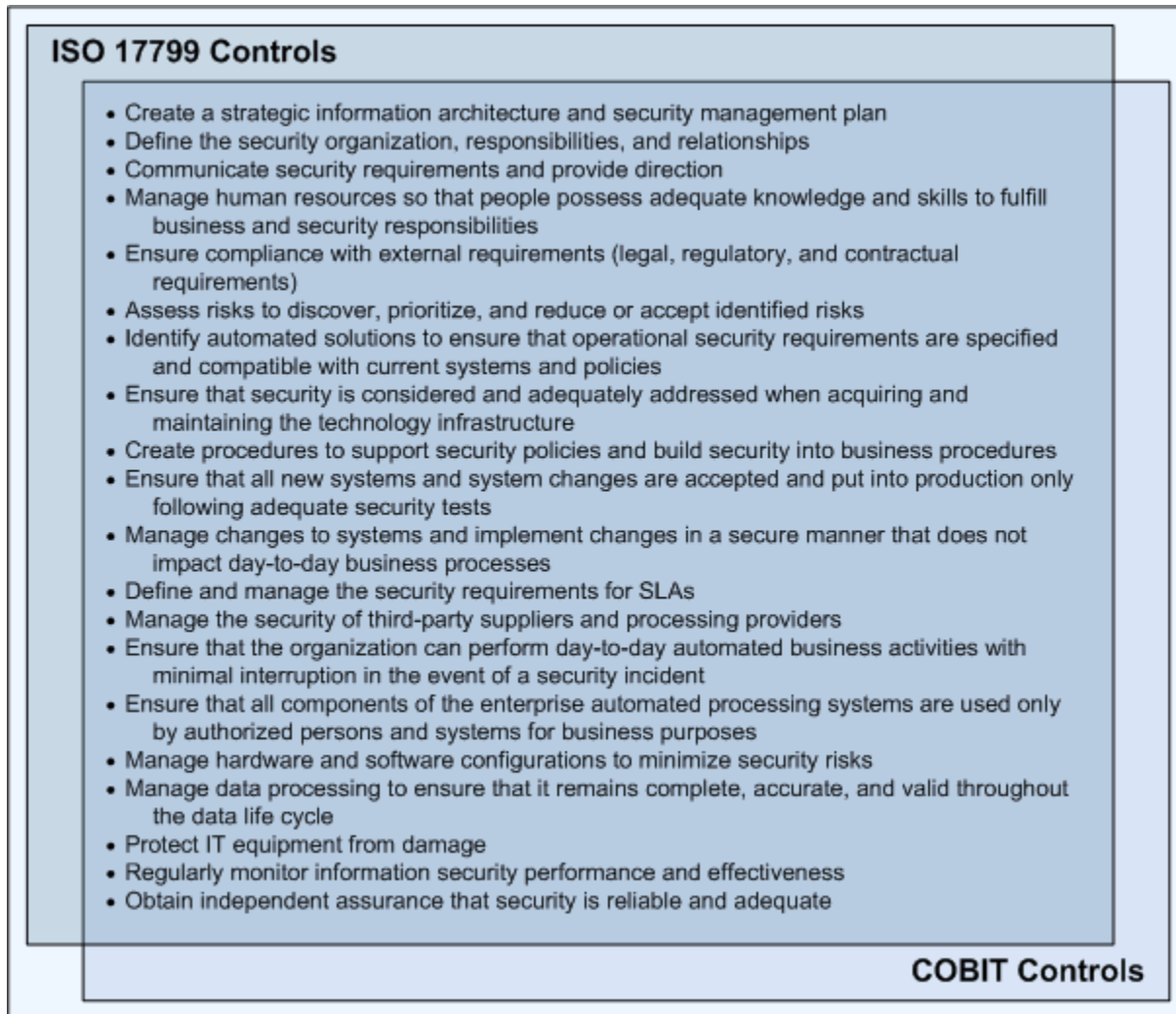


Figure 4: Common controls between ISO 17799 and COBIT.


For more information about ISO 17799 and COBIT, see <http://www.iso.ch> and <http://www.isaca.org/cobit.htm>, respectively.

Identifying Legal and Regulatory Requirements

There are a growing number of laws and regulations that include requirements for organizations to provide security controls and demonstrate compliance assurance. Regulations—such as the United States’ Health Insurance Portability and Accountability Act (HIPAA), the United States’ Gramm-Leach-Bliley Act, the United State’s Sarbanes-Oxley Act, California regulation SB1386, the European Union’s Data Protection Directive, Canada’s Personal Information Protection and Electronic Documents Act (PIPEDA), South Africa’s Prevention of Organized Crime Act of 1998, and South Africa’s Financial Intelligence Centre Act 2001—are examples of just a few of the laws that require organizations doing business under the regulation’s jurisdictions to implement very specific security and privacy controls. Most regulations advise using generally accepted standards to implement the controls.

Determining What These Regulations and Standards Mean to Organizations

Regulatory requirements and standards impact all areas of an organization. There must be an effective framework in place to ensure that all organizational areas understand and comply with the requirements as they are applicable to each business unit. The centralized security management area, in partnership with the organization’s legal team, must keep up to date with all laws and regulations that apply to the organization, and use them as input to the business case justification for security and controls compliance (as well as input to the business impact analysis and other planning processes). A process should be in place to communicate new and updated regulations and standards effectively, efficiently, and expeditiously throughout operational management. This process will more easily and effectively be accomplished by using the information security oversight council and the distributed information security group.

 Establish an automated system to quickly communicate new and updated regulatory requirements through the operational management areas, to the information security oversight council, and to the distributed information security group. Choose a system that will confirm all recipients have received and read the notifications.

Regulations can not only have a profound impact on organizations through noncompliance fines, penalties, and resulting bad publicity and damaged reputation but also provide the leverage to help sell security throughout the organization. Because regulations often reference the use of best practices and standards, they can be used to promote standards based upon widely accepted practices such as ISO 17799 and COBIT for IT governance and controls. In fact, the United States Federal Trade Commission (FTC) had reportedly stated that it considers the Gramm-Leach-Bliley Act Safeguards Rule a standard of due care that would apply to even non-financial companies.

By implementing controls based upon regulatory requirements and international standards, organizations will realize positive business operational benefits. Implement controls based upon regulatory requirements and international standards that

- Demonstrate due diligence
- Are proven non-proprietary and best practice worldwide standards
- Contribute to compliance with many regulations and laws, many of which were built around such standards
- Demonstrate that a standard of care exists
- Help to ensure business objectives are met with regard to regulatory compliance
- Generally help to reduce risks to the entire organization

Finding Leverage Points for Standards and Regulations

Identify the common controls among all your regulatory requirements and chosen controls standards. You will get leverage in your security management and compliance efforts by demonstrating the controls you have chosen are not only promoted by just one standard or regulation but also are common leading security practices and principles throughout many cross-sections of industries.

There are several controls that are considered guiding principles. They provide a good starting point for implementing information security controls, and are based on essential legislative requirements or considered to be common best practices for information security based upon international standards. Controls considered to be essential to an organization from a legislative and international law point of view include:

- Protecting data and privacy of personal information
- Safeguarding organizational records
- Protecting intellectual property and adhering to intellectual property rights

Controls considered as common best practices throughout all industries for information security include:

- Establishing an information security policy document
- Allocating information security responsibilities
- Providing information security awareness and training
- Reporting security incidents through established and documented procedures
- Establishing business continuity management procedures and systems

These controls apply to most organizations and environments. Implement these controls according to the specific risks within the organization, and use them as a starting point and basis to build upon, along with your risks assessment results and regulatory and contractual requirements.

Applying Policies and Practices Based Upon Business Environment, Drivers, and Goals

The policies and practices chosen must be applied as appropriate to the business environment. Business unit leaders must understand how policies and practices apply to business goals and activities and actively work to incorporate security and controls within daily business activities. Security and controls must support the business drivers, or the business unit leaders will not support them (see Figure 5).

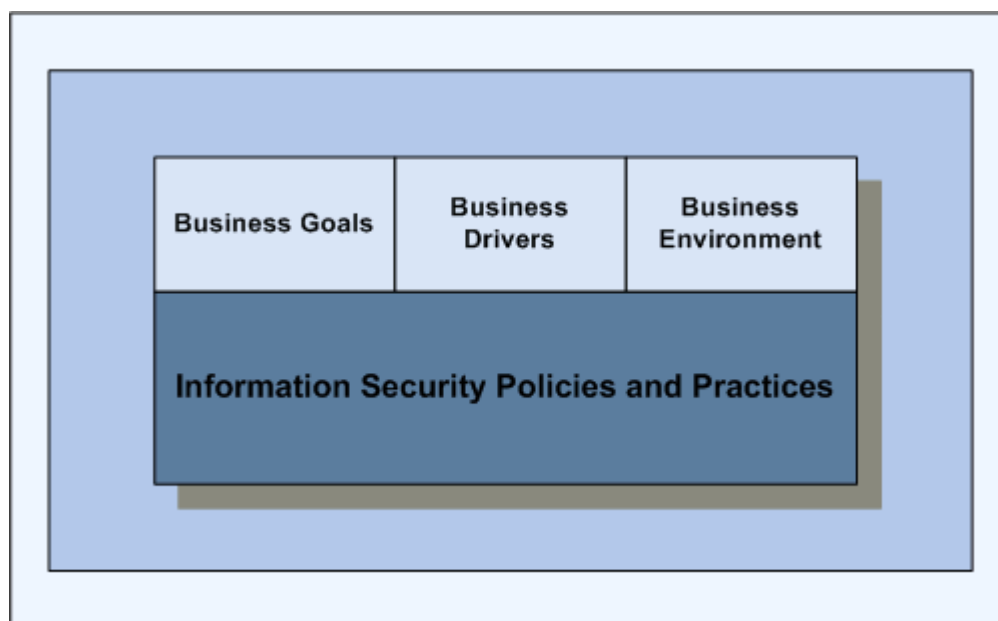


Figure 5: Information security policies and practices must support the business goals, drivers, and environment.

Determining Acceptable Risk and Choosing Appropriate Controls

Determine which information and IT assets are at risk and prioritize them for remediation. Address the vulnerabilities on the most critical assets with the highest impact vulnerabilities that are most at risk because of the likelihood the vulnerability may be exploited is high. You must prioritize the order of addressing risks by risk level. After prioritizing the risks, along with the systems or applications that need to be fixed, begin the remediation process.

☞ A common way to think of risk is as a mathematical formula:

$$\text{Risk (likelihood)} = \text{Asset (value)} \times \text{Vulnerability (severity)} \times \text{Threat (exploit probability)}$$

Assess risks to satisfy the business requirement of supporting management decisions by reaching IT goals. Respond to threats by reducing complexity, increasing objectivity, and identifying important decision factors. IT risk identification involves the entire organization and takes into consideration:

- Risk management ownership and accountability
- Different types of IT risks (technology, security, continuity, regulatory, contractual and so on)
- Defined and communicated risk tolerance profiles
- Cause analyses and risk brainstorming sessions
- Quantitative and qualitative risk measurement
- Risk assessment methodology
- Risk reduction action plan
- Evaluations for certifications
- Reassessments for verifications

Creating a Sustainable Policy Management Process

Security and control policies are living documents and must be managed as such. Many organizations make the mistake of issuing policies, then never, or not often enough, reviewing them to determine the new regulatory requirements, contractual requirements, business process changes, or others issues that necessitate policy modifications. Determining the effectiveness of policies, and when policies must be updated, requires the cooperation and involvement of all business unit leaders in addition to the information security oversight council and distributed information security group. Never forget that security policies and controls are ultimately implemented to support business goals and requirements and reduce risks appropriately.

A security policy passes through a life cycle (see Figure 6):

- Research
- Risk assessment for the topic
- Policy creation
- Management buy-in and support
- Policy approval
- Policy communication throughout the entire organization

- Awareness and training for personnel and applicable target groups
- Policy enforcement
- Policy success evaluation and related metrics
- Policy review and updates to keep it valid and feasible as regulations, technology, and contractual requirements change
- Policy retirement when it is no longer valid

If an organization does not recognize the activities involved with policy development and management, the policies produced will likely be poorly written, incomplete, inadequately address related issues, redundant, disregarded by management, irrelevant, and/or unfeasible.

Using the security policy life cycle approach will help ensure that the policy management process is comprehensive and addresses all functions necessary to create an effective policy. Effective policy management will lead to a greater understanding of the policy development process through the definition of discrete roles and responsibilities, through enhanced visibility of the steps necessary in developing effective policies, and through the integration of disparate tasks into a cohesive process that aims to generate, implement, and maintain policies.

👉 Create a timeline for each of your policies showing target dates to complete each step of the policy life cycle.

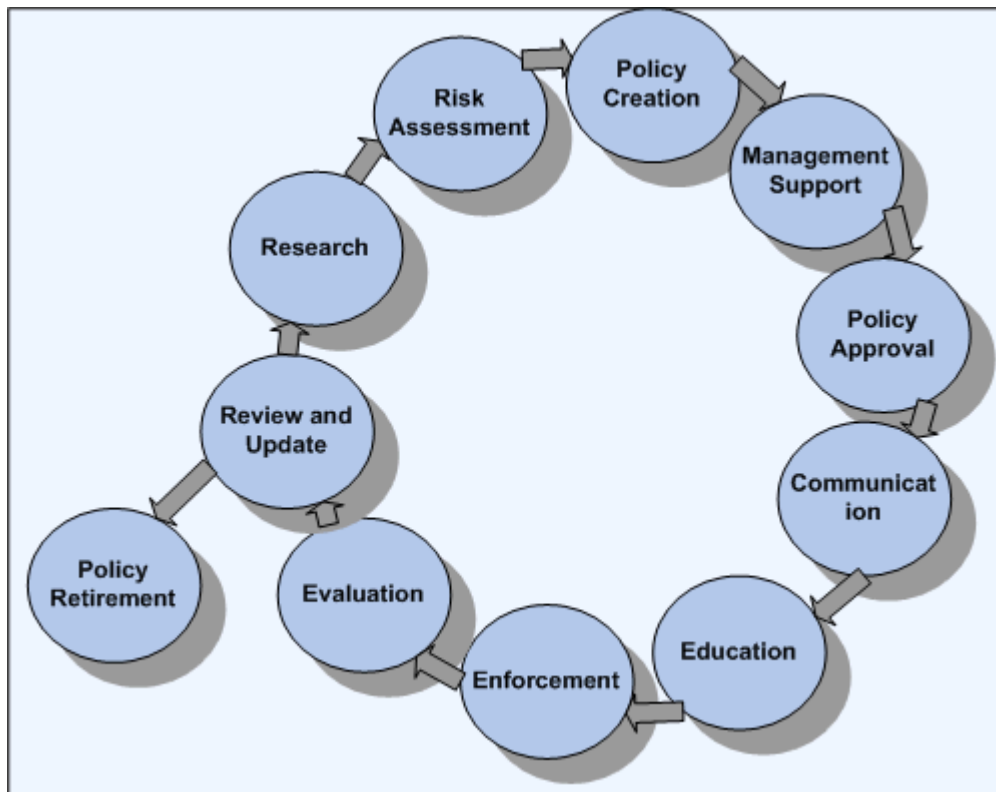


Figure 6: Information security policy life cycle.

Developing a Knowledge-Driven Compliance Framework

The security controls and compliance framework must have built-in security, controls, and contractual and regulatory knowledge to be effective (see Figure 7). This framework can be developed by mapping the standards, regulations, and contractual requirements to the framework model. Doing so will enable more successful and sustainable compliance and help the organization keep up with new and changing regulations, laws, technology, and contracts.

The framework must also provide and sustain knowledge of the organization's current security environment and activities being done to address risks. The organization must respond rapidly to protect the enterprise business environment and IT architecture and ensure compliance. There must be a capability to quickly and easily document and report the current risk environment, responsibilities for addressing risks, compliance timeframes, and associated controls.

The organization must know partner and customer contracts and related security issues. To ensure internal compliance, organizations must communicate the security charter, personnel, requirements, and program components continuously through a sustainable ongoing framework. And, very important but often overlooked, an organization must monitor and evaluate policy and control effectiveness.

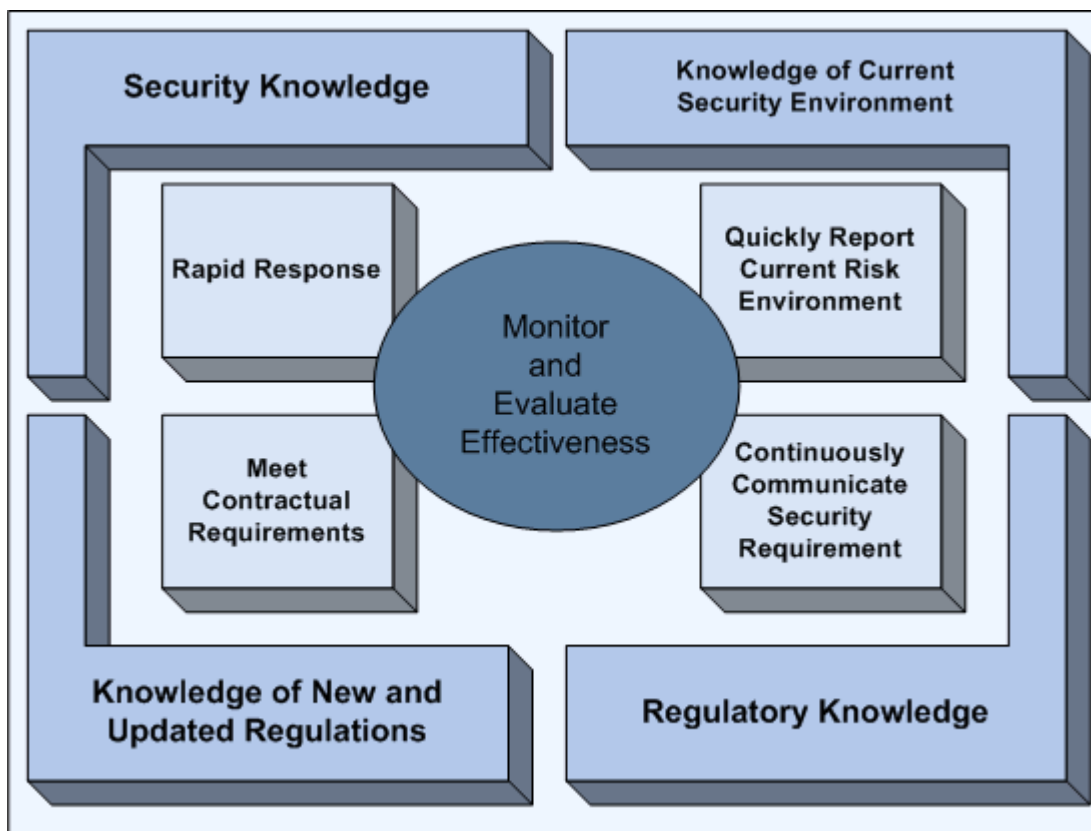



Figure 7: Knowledge-driven security framework.

Certifying Security Controls

Certification is generally the review of a process or system from a user perspective. The users review the new or updated process or system and ensure that the process or system will meet the original business requirements outlined at the start of the project and be compatible with existing security policy, procedures, and business objectives. The security management area must also be involved to review the process or system to ensure that it is adequately addressing security threats and risks. They will need to consider the sensitivity of the data within the system or process, the reliance of the business process on the system (availability), regulatory requirements (such as data protection or archival time), documentation, and user training. They must determine that the process or system protects information and IT resources adequately.

 The users involved in testing should include applicable distributed security group members whenever possible.

Verifying Controls Adequacy

Following certification, and at regularly scheduled times following implementation, the process or system should undergo a review to verify the controls are still processing appropriately and that the documentation for the tests and controls during the certification process are sound. Review management should ensure the test and controls are appropriate and complete. This review is the final approval by management to permit the new or updated process or system to move into production. Management must review the changes to the process or system in the context of its operational setting. They must evaluate the certification reports and recommendations from security regarding whether the system is adequately secured and meets user requirements and the proposed implementation timetable. This process may include accepting the residual risks that could not be addressed. Following verification of the controls and security, the process or system can be moved to a production status.

Monitoring and Evaluating Policy and Control Effectiveness

Businesses use income statements to determine profits and losses; measurements that all management use to determine how well a business is doing and to make adjustments in processes and activities to improve. Likewise, when managing information security, it is important to measure how well the in-place security measures are meeting requirements and securing information. To do so, organizations must identify and implement security metrics throughout every area of the organization. The security metrics will help identify whether security is adequately reducing security risks and complying with all contractual and regulatory requirements. Once the metrics are applied, organizations can use the results to identify gaps with policies, requirements, and regulations and to justify funding additional security activities and projects. The chosen security monitoring and evaluation should

- Determine whether IT processes and systems are in compliance with security policies
- Determine whether the implemented policies, standards, and corrective actions taken are effectively working to improve overall security
- Notify the central security management area of issues and business areas that are not compliant with policies and standards

Summary

The security compliance assurance roadmap organizations follow should incorporate all the elements discussed so far. All levels throughout an organization must view security and accompanying controls as a shared service implementation program. One area cannot ensure effective and efficient security and controls throughout an organization:

- The security architecture provides IT security and controls governance. Central authority for the organization security management function resides here and it is where policies and standards are created and maintained. The security architecture should be designed for the long term, independent of technology. This architecture must be communicated throughout all operational areas of business management within the organization.
- Operational management is the implementation actions and processes that occur to ensure IT security and controls governance are implemented throughout the organization. Organizational management must ensure that all controls are implemented throughout every business unit.
- New and updated operations and systems must be certified and verified to ensure that adequate and effective controls and security are implemented prior to moving into production. The certification and verification areas use monitoring and a review process to ensure IT security and controls governance has been effectively implemented throughout all organizational business units.
- Monitoring and review processes must be established to ensure that security and controls are still effective and adequate.
- Security metrics must be used to evaluate level of success with security efforts and to identify gaps with contractual and regulatory requirements.

There must be a full understanding of IT governance and security and control issues at all levels of the organization, and awareness and formal training is vital to ensuring this understanding. IT processes must be aligned with the business and with the IT strategy and there must be a clear understanding of business goals and processes supported by defined controls. Responsibilities must be monitored, certified, and verified through both administrative methods—such as service level agreements (SLAs)—and automated means.

Improvement in IT processes and controls should be based upon an understanding obtained through monitoring, certification, and verification. Such measurements and evaluations must be determined from defined procedures and process metrics. Management must define the amount of risk tolerance under which processes will operate. Action must be taken to improve processes that appear not to be working effectively or are no longer valid. With these factors in place, an organization can be assured of compliance.