CHAPTER

13 Information Security Governance

THE CHAPTER DISCUSSES INFORMATION SECURITY GOVERNANCE. It also discusses information security policies. An organization's governance structure is an important part of its information security program. Governance focuses on the structure used to protect resources and data. This structure must provide security and support business needs. Strong governance helps create strong security programs.

Organizations use policies, standards, guidelines, and procedures to create their security program. These documents help guide employee conduct. They're tools that organizations use in many ways. They make sure that information technology resources are secured. They also help protect an organization from legal liability.

Chapter 13 Topics

This chapter covers the following topics and concepts:

- What information security governance is
- What information security governance documents are
- What recommended information security policies are
- What some case studies and examples are

Chapter 13 Goals

When you complete this chapter, you will be able to:

- Describe the key concepts and terms associated with information security governance
- Describe the goals of different information security governance documents
- Describe the different types of policies that can be used to govern information security

FYI

A zettabyte is 1 billion terabytes. To put things in perspective, the U.S. Library of Congress has collected almost 167 terabytes of data in its Web archive project. The Web archive project is collecting and preserving snapshots of the world's Web pages. These Web pages help show the world's cultural and intellectual heritage. You can learn about that project at *http://www.loc.gov/webarchiving*.

What Is Information Security Governance?

The University of California Global Information Industry Center tries to measure information use in the United States. It defines "information" as any flow of data delivered to people. It can be in any form. The center reported that Americans consumed 3.6 zettabytes of information in 2008.[1] Our use of information is growing. For businesses, data is a valuable asset.

An organization must find ways to protect its data. It also must make sure that data can be used for business reasons. This balance is key to an organization's success. Failing to strike the right balance can harm the organization's goals. Consider the following:

- An organization can't market its products without access to customer lists.
- Customers may complain about incorrect electronic data.
- If confidential data is disclosed, an organization faces embarrassment.

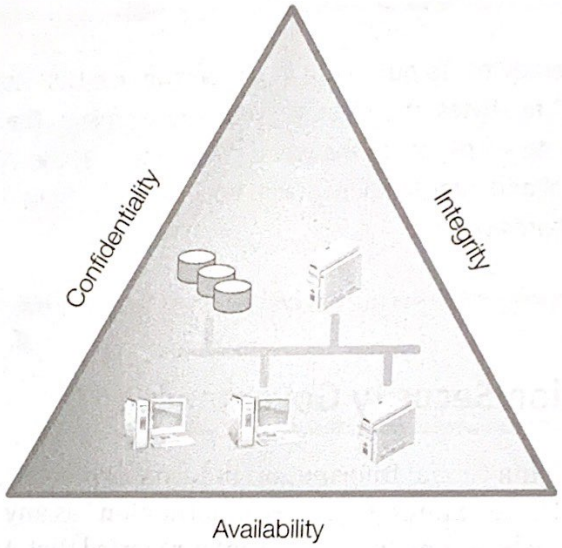
An organization's executive management team is responsible for governing the organization. This means it's also responsible for information security governance. **Information security governance (ISG)** is the executive management team's responsibility to protect an organization's information assets. ISG makes protecting information assets a business decision. To do this an organization must align its information security goals to its business needs. ISG moves information security beyond technical decisions. It makes security a strategic decision.

Organizations use ISG to enhance their business. ISG makes sure that information security goals are used to meet business goals. This means that the organization uses the security goals of confidentiality, integrity, and availability in a way that makes sense for the business. ISG also makes sure that there's proper accountability and oversight for meeting these goals. The C-I-A triad appears in Figure 13-1.

NOTE

The security goals of confidentiality, integrity, and availability are called the C-I-A triad or the A-I-C triad.

FIGURE 13-1
The C-I-A triad.



Information Security Governance Planning

Information security governance refers to executive management's responsibility to provide strategic direction, oversight, and accountability for the security of its data and information technology (IT) resources. Their main duty is to make sure that information security strategy supports business goals.

A common business goal is to make a profit. The organization must take into account many factors that affect this goal. Business drivers are forces that influence the organization's business goals. They can be internal or external. They include the people, processes, and trends.

An organization must balance business drivers to meet their goals. They do this during the business planning process. There are three types of business planning. They are:

- **Strategic planning**—This is long-term planning. **Strategic planning** focuses on preparing new approaches and planning for new technologies. It lays the groundwork for new business directions. ISG uses strategic planning to support business objectives.
- **Tactical planning**—This is short- to medium-term planning. **Tactical planning** allows an organization to be responsive to market conditions. It allows them to take advantage of short-term or unexpected opportunities. Tactical plans are usually six months or less in length.
- **Operational planning**—This is day-to-day planning. **Operational planning** focuses on the normal operations of an organization. It's responsive to daily issues.

Figure 13-2 illustrates the different types of business planning.

The organization's executive management team carries out strategic planning. This is when they determine the business's goals. Once it determines its business goals,

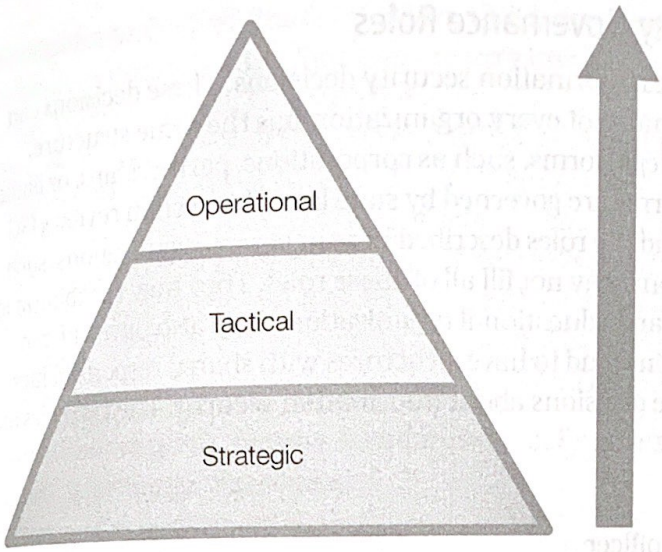


FIGURE 13-2 Business planning hierarchy.

it must figure out how information security can support these goals. It will use the same types of planning strategies to think about information security. This is ISG planning. When planning for information security, the organization must think about:

- **Information needs**—The organization must ask how it uses data to meet its business goals. It must then think about how information security can support this. For instance, if an organization conducts most of its business on the Internet, it must think about availability and integrity. Its IT systems must hold accurate data and be ready to conduct business.
- **Regulatory requirements**—The organization must know its regulatory landscape. It must know the data protection laws that it must follow. Often these laws focus on protecting the confidentiality of certain types of data.
- **Risk management**—The organization must adopt a risk management approach. It must know the information security risks that it faces. It also must decide how it will respond to risk.
- **Security failures**—The organization must think about information security failures. It must consider the impact of a security breach, malware-infected IT resources, or unavailable data. There may be many negative impacts of an information security failure. These include lawsuits and breach notification costs. An organization will certainly lose customers after an information security incident. This affects its bottom line.

> **NOTE**
> A 2013 survey found that companies spend about $565,020 to notify customers if they experience a data breach.[2]

An organization answers these questions to determine ISG strategic direction. It makes sure that its information security goals support its business objectives. This is the role of ISG.

Common Information Security Governance Roles

It's important to know who makes information security decisions. These decisions can be strategic, tactical, or operational. Not every organization has the same structure. Organizations can have different legal forms, such as corporations, partnerships, or limited liability companies. These legal forms are governed by state law. This section reviews ISG roles. You will be more likely to find the roles described here in larger organizations, such as corporations. Smaller organizations may not fill all of these roles. They may combine many duties within one role. Nonprofit and educational organizations may also have different roles for people. These organizations tend to have structures with shared responsibilities.

Many different roles can make decisions about information security. The ISG roles are:

- Board of directors
- Chief information officer
- Chief information security officer
- Information security managers

The **board of directors (BOD)** runs an organization. It's an organization's top governance group. A board of directors is required by law to act with due care. It must make all of its decisions in the best interests of the organization. The BOD plans an organization's strategic direction. It also determines business goals. It makes sure that an organization uses its resources properly to meet these goals. Finally, it makes sure that an organization acts legally. If an organization does not have a board of directors, then its top-ranking executive group performs these duties.

The BOD determines how information security supports business goals. It does this through strategic planning. The BOD issues high-level information security policies. It delegates tactical and operational activities to other senior managers. The main duty of a BOD is governance.

> **NOTE**
>
> In March 2009, U.S. President Barack Obama appointed the first federal CIO. The federal CIO is responsible for government IT spending.

The **chief information officer (CIO)** is the organization's senior IT official. The CIO focuses on strategic IT issues. The CIO defines an organization's IT mission. It's the CIO's job to keep the BOD advised about IT issues. CIOs aren't usually involved in day-to-day IT operations. Their duties are strategic and tactical in nature. They often delegate responsibility for information security management (ISM) to a CISO.

A CIO isn't the same as a **chief technology officer (CTO)**. A CIO is responsible for a company's internal IT systems. CIOs focus on the systems used to run the organization's business. A CIO tends to be internally focused. A CTO develops a company's technology products. These are the products that the company delivers to its customers. A CTO tends to be externally focused.

The **chief information security officer (CISO)** is the organization's senior information security official. The role of the CISO is relatively new. It continues to evolve. Depending on an organization's structure, the CISO might report to the CIO. A CISO also could report

to the organization's chief financial officer. CISOs are responsible for an organization's information security strategy. They also are very involved in tactical planning. They aren't generally involved in daily IT operations.

The CISO makes sure that the CIO and BOD understand information security threats and how to respond to those threats. The CISO may make information security policy suggestions to the BOD. A CISO also helps determine information security safeguards. He or she delegates functional and operational tasks to other managers.

Information security managers are responsible for the functional management of an organization's information security program. They manage the operational activities. They implement the controls specified by the CISO. These managers might also:

- Create information security standards, guidelines, and procedure
- Participate in risk assessments
- Manage the security infrastructure

These roles work together. The higher-level roles make governance decisions. The lower-level roles are responsible for information security management and operational activities.

Information Security Governance and Management

Information security governance and **information security management** aren't the same thing. The terms are often used interchangeably. The distinction is subtle. You should keep in mind that sometimes the difference isn't clear. Many organizations use one or both terms to refer to all ISG and ISM activities. Many activities have both ISG and ISM elements.

ISG makes sure that security is used to support business goals. It's handled by the BOD, CIO, and CISO. It offers a process for oversight and accountability. It makes sure that there's a structure in place to direct information security activities.

ISM is the visible part of ISG activities. It makes sure that ISG policies are put into practice. It's the organization's day-to-day security operations. Table 13-1 compares ISG and ISM.

ISM maintains the organization's overall security posture. ISG states what that posture must be.

TABLE 13-1 Comparison of information security governance and information security management.

INFORMATION SECURITY GOVERNANCE	INFORMATION SECURITY MANAGEMENT
Strategic and tactical	Tactical and operational
Creates policies and strategy	Implements policies and strategy
Ultimate compliance authority and oversight	Day-to-day management and authority
BOD, CIO, CISO	Information security managers (with help from CIO and CISO)

Creating an Information Security Governance Program

There are many resources available to help organizations create an ISG program. The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) has created a comprehensive standard to help guide this process.[3] The standard uses the term ISM system to refer to both ISG and ISM activities.

The standard helps organizations create an ISM system. It uses a risk-based approach. It reviews how to operate, monitor, review, maintain, and improve the ISM system. It walks though each step. It discusses the processes that an organization must consider at each step.

Any organization can use this standard. It's designed to be flexible to meet an organization's needs. It can be especially helpful to organizations that have never managed information security on a strategic level. It's also designed to work with the ISO/IEC security controls standard called ISO/IEC 27002:2013, Information Technology—Security Techniques—Code of Practice for Information Security Controls.

Organizations must review their ISM systems. They need to know if their ISM controls are improving security. To do this, they must measure their effectiveness. The ISO/IEC has guidance on this as well. That document is titled "ISO/IEC 27004:2009 Information Technology—Security Techniques—Information Security Management—Measurement."

This standard helps organizations review their ISM system. It helps organizations create control measurements. It also helps them analyze the measurements. The process helps organizations decide if their policies or controls need to be changed.

Information Security Governance in the Federal Government

Congress created the Federal Information Security Management Act (FISMA) to protect federal data and IT resources.[4] U.S. federal agencies must comply with it. Federal agencies fall under the executive branch of the U.S. government. They report to the President of the United States.

FISMA requires each federal agency to develop an information security program. Each agency must name a CISO to lead the program. The program must assess the agency's information security risk. It must include plans to reduce that risk. It also must provide security awareness and training activities to employees.

Agencies must report on their FISMA compliance progress each year. They send these reports to the Government Accountability Office (GAO).

NOTE

You can view the GAO high-risk Web site at *http://www.gao.gov/highrisk/.*

Information security is a high priority for the federal government. Since 1997, the GAO has included "protecting the federal government's information systems and nation's cyber critical infrastructures" on its "high risk list." Issues are high-risk if they're vulnerable to fraud, waste, abuse, or mismanagement. The GAO publishes the list every two years.[5]

Information Security Governance Documents

An organization's ISG documents form the basis of its information security program. They document the organization's commitment to information security. They're used to address:

- The organization's information security goals
- How the organization protects its own data
- How the organization protects the data of others
- Compliance with legal and regulatory requirements
- Employee information security responsibilities
- Consequences for failing to meet responsibilities

Organizations use policies, standards, guidelines, and procedures to create their security program. These documents work together to support information security goals. A formal policy is the highest-level governance document. Standards are the next level. Then procedures. Guidelines provide security advice. The documents move from the general (policies) to the more specific (procedure). Figure 13-3 shows how these documents work together.

For purposes of this discussion, these documents are collectively referred to as "ISG documents" or "policies." You should keep in mind that the term *policies* is often used in a very generic way. It's used to describe the entire suite of ISG documents. It will be clear from the text when the term is used in the generic way.

NOTE
ISG documents are administrative safeguards.

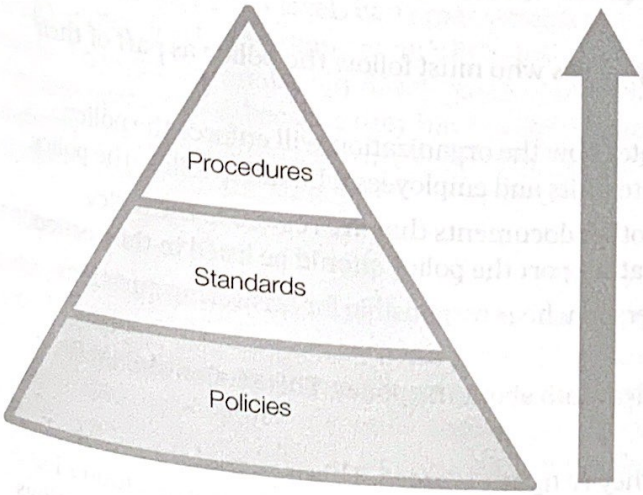


FIGURE 13-3
Information security governance documents.

A formal **policy** is executive management's high-level statement of information security direction and goals. They're the top level of governance documents. They help minimize risk by laying out the organization's information security strategy. High-level policies are approved by an organization's BOD.

The BOD uses policies to set forth its information security goals. They also state compliance expectations. Not all organizations will have the same types of high-level policies. They're unique to each organization. Each organization develops policies by reviewing its regulatory landscape. They also must take into account the size and complexity of the organization and its IT systems. They also think about how information security can be used to meet business goals.

Policies must be drafted with care. Policy elements vary among organizations. However, there are some common elements to all policies. They include:

- **Policy statement**—States the expected behavior, actions, or outcomes. It's a clear statement of permitted or forbidden actions.
- **Policy exclusions**—Lists situations or people who aren't covered by the policy. For the most part, there shouldn't be many exclusions in a high-level policy.
- **Policy rationale**—States the reason why the policy exists. This includes the legal or regulatory reasons for the policy. A policy might be drafted in response to information security threats.
- **Policy definitions**—Defines terms that have special meaning. Terms with common definitions don't need to be defined.
- **Who is affected by the policy**—States the people, units, or departments affected by the policy. In a high-level policy, this usually is all of the organization's employees.
- **Who must follow the policy**—Lists who must follow the policy as part of their job responsibilities.
- **Compliance language**—States how the organization will enforce the policy. It also states what happens to units and employees who fail to follow the policy.
- **Related documents**—Lists other documents that are related to the policy. Standards or procedures that support the policy should be listed in this section.
- **Policy contact**—Lists the person who is responsible for answering questions about the policy.
- **Policy history**—Lists historical data about the policy. This section should list revision and review dates.

High-level policies are concise. They're tightly worded. This is so that they're easy to understand. A high-level information security policy states the organization's information security expectations. These high-level documents don't include explanations about how to meet those expectations. Supporting documents provide that detail. Supporting documents are standards, guidelines, and procedures.

FYI

The SANS Institute has a policy Web page. It gives drafting advice. It also has sample policies. You can view this resource at *http://www.sans.org/security-resources/policies/*.

Policy documents tend to go through a lengthy development and review process. The process can be very time consuming. This is because policies are high-level governance documents from executive management. They have a broad scope and address the whole organization.

Policies are rarely changed. This is because they contain language that sets forth general expectations. The broad goals stated in a policy shouldn't need to be changed often. Standards and procedures are used to provide flexibility. They're easier to change. An organization can easily update these documents in response to changing technology conditions.

Standards

Standards support high-level policies. They're just below policies in the ISG documents hierarchy. They state the activities and actions needed to meet policy goals. Standards are more specific than policies. Standards may require employees to take (or refrain from) certain actions. Standards often state a minimum level of behavior or actions that must be met to comply with a policy. This is called a **baseline**.

Standards are technology neutral. They don't refer to specific technologies or products. Instead, they refer to the safeguards and controls an organization should use to protect data and IT resources.

A number of different ISG levels can create standards. They're usually created at the CIO or CISO level. An organization's BOD isn't usually involved in creating standards. An organization usually develops standards with input from information security managers. This is because they have overall organizational responsibility for implementing information security. They're the subject matter experts in what it will take to implement the standard.

Procedures

Procedures are the lowest level of ISG documents. They're step-by-step checklists. They explain "how" to meet security goals or conduct security-related activities. Organizations often tailor their procedures to a certain type of technology. They also can be limited to the activities of specific departments or end users.

Procedures usually only address single tasks. They're designed to be flexible. They change as technology changes.

Information security managers usually create procedures. Sometimes a CIO or CISO may review procedures. For the most part, however, they're department- or technology-specific documents.

Governance Documents Work Together

Policies, standards, and procedures work together to protect information security. Policies set forth the general expectation. Standards further define those expectations. Procedures tell end users how to comply with the expectations. An example might work as follows:

Policy Statement: All employee passwords to the organization's IT resources must be strong passwords.

Standard Statement: All strong passwords must have at least eight characters and have at least one number and one letter.

Procedural Statement: To change a user account password in the Microsoft Windows 8 operating system, you must do the following:

1. Swipe to open Settings.
2. Tap on Change PC Settings.
3. Tap on Accounts.
4. Tap on Sign-in Options.
5. Tap on Change Your Password.
6. Follow the onscreen instructions for changing your password.

In this example, an employee knows what the expectation is ("a strong password"), how the expectation is defined ("a strong password is eight characters and has at least one number and one letter"), and how to meet the expectation ("checklist for changing a Windows 8 account password").

Guidelines

Guidelines are the most flexible type of ISG document. Organizations can issue guidelines for a number of reasons. They issue guidelines to:

- Encourage employees to adopt good information security practices
- Educate employees about security threats and how to respond to them
- Encourage employees to take action in areas that the organization can't

An organization can use guidelines to give information security advice. They can recommend actions that an employee can apply on their own. The guidelines help employees adopt behaviors that improve information security. Sometimes they address specific kinds of employee behavior. They also might address a specific security issue. For example, an organization might create a guideline to help employees learn how to avoid social engineering attacks.

Organizations might issue guidelines to address issues that they can't control through technical measures. This is where the organization needs its employees to help it protect IT resources. They hope that they can encourage employees to read the guidelines and take individual action.

For example, an organization may allow its employees to access its IT systems from home. It allows this because it increases productivity. It allows employees to work from home on days when they otherwise would not be working. (For example, if a parent stays home to care for a sick child.) However, the organization must safeguard its IT resources from security threats introduced by this activity. One security threat is malware that might be on an employee's home computer that could be transmitted to the organization's IT resources.

The organization has no real way to make employees use good security practices at home. It has no real authority to require employees to protect their home computers. To encourage employees to secure their home computers, the organization can issue a guideline. The guideline outlines security safeguards that employees can use at home. Following the guideline benefits employees. This is because it helps them secure their own personal data. It also helps protect the organization's IT resources if the employee follows the recommended practices. Both the employee's computer and the organization's IT resources are protected. It's a winning situation for everyone.

Creating Information Security Policies

Each type of ISG document has a different role and focus. They might be directed at different audiences. They might address similar issues from different standpoints. However, they do share some similarities. These similarities include:

- They must be easy to understand.
- They must have a well-defined scope.
- They must be regularly reviewed.
- They must be communicated to all employees.

First, the documents must be easy to read. All employees must be able to understand them. Even if the subject matter deals with legal issues, the document itself should be free from legalese. The documents shouldn't use technical jargon. The only time it's OK to use complex language is when it's needed to help employees know their responsibilities. Otherwise, these documents must be understandable. This makes sure that employees can follow them.

Second, ISG documents must have a clear scope. They must clearly address a specific aspect of the organization's security program. Employees shouldn't have to consult many high-level documents to determine the organization's stance on a single issue.

Third, the organization must regularly review its ISG documents. Information security doesn't exist in a vacuum. Risks change. Laws change. Technology changes. An organization must respond to these changes in their security program. To do this, they must review their ISG documents on a regular basis to make sure that they're current.

Legalese Versus Plain Language

Legalese is an unflattering term used to describe legal writing. Legalese is language that uses too many legal phrases. It uses many Latin terms. It usually has long sentences with many commas. It's dense and hard to read. Lawyers are needed to translate documents written in legalese.

There's a growing trend in the legal profession to write documents in *plain language*. This means that documents are written in the language that people use when they speak. This helps make documents more understandable. People can understand these documents faster. They also are less likely to misunderstand them.

The trend is to use plain language to write formal documents. However, legalese appears in high-level policies on a regular basis. This is because these documents are formal governance documents. An organization's legal counsel often writes them.

Legalese can make it hard to understand some very simple concepts. This is frustrating for people who need to follow the policies. Some examples of legalese and plain language follow. Are there other ways that you can make these policy statements easier to read?

Example 1—Consent

Legalese: All users of the organization's information technology resources, as a condition to the use of such resources, specifically consent to the general rights of the organization as specified herein.

Plain Language: All users of the organization's IT resources agree to the terms of this policy.

Example 2—Least Privilege

Legalese: Any access permitted hereunder shall be the minimum access required in order to protect the organization's interests.

Plain Language: Access to IT resources is limited to the minimum amount needed.

Example 3—Warranties

Legalese: The organization makes no warranties of any kind with respect to the organization's information technology resources it provides. The organization will not be responsible for damages resulting from the use of organization's information technology resources, including, but not limited to, loss of data resulting from delays, non-deliveries, missed deliveries, or service interruptions caused by the negligence of an organization employee, or by any user's error or omissions. The organization specifically denies any responsibility for the accuracy or quality of information obtained through organization's information technology resources.

Plain Language: The organization provides IT resources "as is." The organization makes no promises about service level or data accuracy. The organization isn't responsible for errors. Use of IT resources is at a user's own risk.

Finally, an organization must communicate the ISG documents to its employees. Employees can't follow policies that they don't know about. Good communication makes sure that employees view ISG documents as business enablers. Organizations can communicate ISG documents to employees in a number of ways. They can use newsletters, in-person and online training, or company-wide e-mail messages.

Policy Development Process

Organizations should create a structured ISG document development process. A formal process gives many areas the opportunity to comment on a policy. This is very important for high-level policies that apply to the whole organization. A formal process also makes sure that final policies are communicated to employees. It also provides organizations with a way to make sure that policies are reviewed regularly.

In general, a policy development process should include the following steps:

1. Development
2. Stakeholder review
3. Management approval
4. Communication to employees
5. Documentation of compliance or exceptions
6. Continued awareness activities
7. Maintenance and review

The need for a new ISG document is determined in the development phase. The BOD, CIO, or CISO might decide that there's a need for a high-level policy. An information security department might suggest that there's a need for a new high-level document. The idea for a new ISG document really can come from anywhere in an organization. This section focuses on how high-level policies are created. However, the same development process is recommended for other ISG documents as well.

Once a policy need is identified, the BOD must determine the goals of the policy. To do this, it reviews a number of areas. It looks at its use of IT resources. It reviews the data that it's legally required to protect. It considers its business objectives. An organization's CIO or CISO will give advice about information security issues. The BOD also might consider how other companies in the same industry approach a certain type of issue. After this review, the BOD establishes the policy goals.

An organization must take care when it drafts high-level policies. It must make sure that a new high-level policy doesn't conflict with any previously issued policy. Stakeholders must review the draft when it's finished.

FYI

In drafting an ISG document, it's important to be consistent. A writer should use consistent grammar, punctuation, and format. This makes the document more readable. It also makes it easier for employees to understand the document.

At the next step, stakeholders review the ISG draft documents. **Stakeholders** are interested parties. They're employees and departments that will be affected by the new policy. They also may be subject matter experts in the underlying policy subject matter. IT resource managers also will review the document at this point. They do this to make sure that they can implement technical controls to meet the policy.

This also is the step where legal counsel, risk management, and audit will review the document. These groups make sure that the document meets the organization's regulatory needs. Risk management and audit departments will want to make sure that they can measure policy compliance. Legal counsel makes sure that the document helps protect the organization from legal liability. The organization may revise the policy many times during this step.

The policy must be signed when it's in final form. The BOD must always review and sign high-level information security policies. Their support is crucial for a successful information security program. They don't always sign lower-level documents. The executive with authority over certain tasks may sign lower-level documents. For example, a CIO or CISO might sign standards or guidelines. Departmental managers and supervisors may sign procedures for their specific areas.

The next step is the communication step. It's one of the most critical steps in the development process. Communication is necessary to make sure that all employees know about the new policy. It helps employees know where to find resources to follow the policy. Organizations can communicate new policies in a number of different ways. Internal newsletters, memos, and company-wide e-mails can all be used to inform employees about a new policy.

As part of the process, an organization must measure policy compliance. It must know how departments act to meet policy requirements. It also must note any exceptions to compliance. An organization can show compliance by documenting the following:

- When the ISG document was approved
- How and when it was communicated to employees
- Actions departments took to meet the responsibilities stated in the ISG document
- Deviations from the requirements in the ISG document

> **NOTE**
> Compliance is an ongoing process. Organizations must continuously monitor compliance.

Sometimes departments might request an exception to a policy. They can request an exception for a number of reasons. For example, a policy might state a technical control that an IT system can't meet for a very legitimate reason.

Organizations must have a formal way to review policy exception requests. The BOD must review, approve, and document each high-level policy exception request. A BOD might assign this role to an upper management official such as a CIO or CISO. Exception requests from standards and procedures might be handled by the CIO or CISO as well.

An organization must carefully consider exception requests. This is because every policy exception weakens the organization's security posture. There are two main reasons to grant a policy exception request. The first is when following the policy negatively affects

the organization's business objectives. This might happen when a policy control interferes with a critical business process.

The second reason to approve an exception request is when the cost to comply with the policy is more than the cost of noncompliance. For example, an organization may grant an exception request if a particular IT resource is incapable of technically meeting a policy requirement. It might do this if buying new equipment is too expensive. In those cases, the organization still must implement controls to protect the IT resource. The policy exception request must document how an area will use compensating controls to meet the spirit of the policy.

The development process must continually educate employees about policy compliance. Ongoing security training and awareness is required to keep employees aware of their responsibilities. An organization must build regular policy awareness activities into its day-to-day routine. They can be included in other training programs, such as workplace safety programs.

Finally, an organization must review its ISG documents on a regular schedule. They must make sure the documents continue to reflect business and information security goals. Sometimes internal or external factors change so much that an organization must change its policies. At this point, it can either update its policy or withdraw it and create a new one. A BOD demonstrates due diligence and reasonable care when it regularly reviews its policies. Figure 13-4 shows the policy development process.

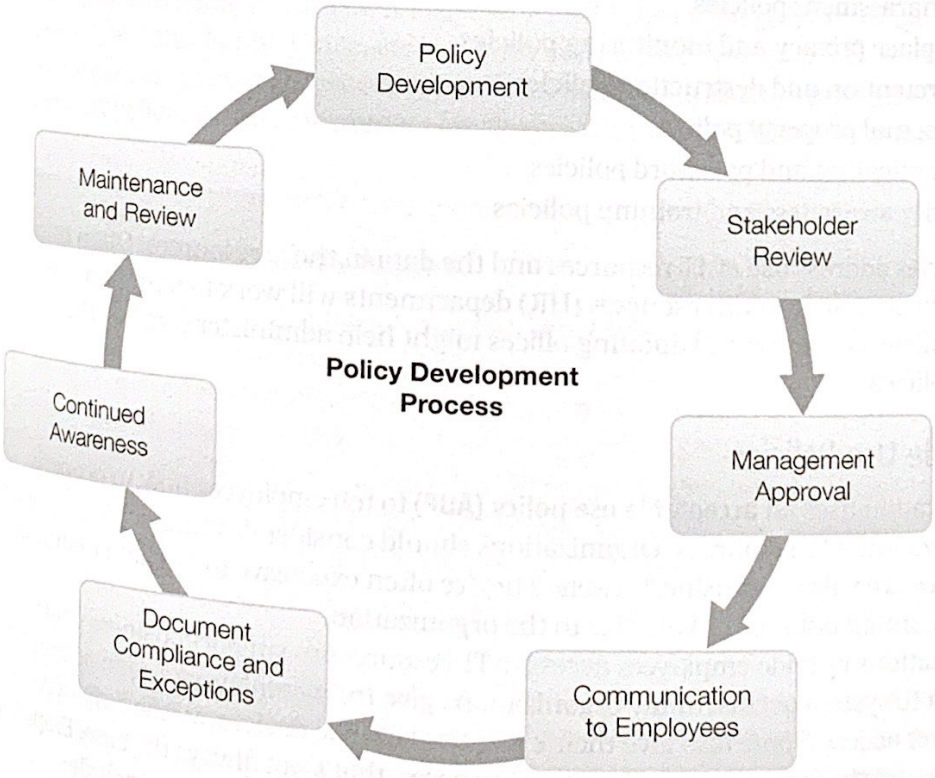


FIGURE 13-4 Policy development process.

An organization can adjust the development process if necessary. For example, it might need to create a new policy to respond to a new law. It can step that policy through the development process quickly. It can then go back and review the document once the urgent regulatory need has passed.

The process can be shortened for some ISG documents. Standards and procedures that apply to one department only may go through a shortened process. This is because there may not be as many people who need to comment on them.

An organization uses ISG documents to support its business objectives and information security goals. These policies form the basis of an information security program. They also set the tone for a culture of information security awareness.

Recommended Information Security Policies

Information security policies will vary across organizations. This is because all organizations are different. They have different business goals. Their security needs aren't the same. Their cultures are different.

The list of information security issues to address in a policy is endless. However, all organizations face some basic security issues. They should create policies to address these issues. The basic policies that organizations should consider include:

- Acceptable use policies
- Anti-harassment policies
- Workplace privacy and monitoring policies
- Data retention and destruction policies
- Intellectual property policies
- Authentication and password policies
- Security awareness and training policies

These policies address use of IT resources and the data in those resources. Often information security and human resources (HR) departments will work together on some of these policies. Business and auditing offices might help administer some of these types of policies.

Acceptable Use Policies

An organization uses an **acceptable use policy (AUP)** to tell employees how to properly use organizational IT resources. Organizations should consider drafting an AUP because IT resources are valuable business assets. They're often expensive to buy and maintain. They also contain data that's valuable to the organization.

Organizations provide employees access to IT resources to support business goals. In addition to system access, many organizations give their employees e-mail accounts and Internet access. Some also give their executives mobile devices. While employees are supposed to use these resources for business purposes, that's not always the case. Employees can use these resources in many non-business ways. Some of these uses include:

- Sending and receiving personal e-mails at a work e-mail address
- Chain mail and hoax e-mail messages sent around the office
- Non-business Internet use
- Online shopping
- Accessing social networking sites during work hours
- Downloading free software (or pirated software) for non-business use
- File sharing throughout a workplace or over the Internet

Improper use of an organization's IT resources can be costly. It can result in information security compromises. It can introduce malware onto IT systems. An organization might be legally responsible for an employee's misuse of IT resources in some instances. Non-business use of IT resources can distract employees. It can lead to lost productivity.

An AUP can help prevent some of these issues. An AUP states a code of conduct. It states permitted uses of IT resources. It also lists prohibited actions. Finally, it states the consequences for violating the acceptable use rules. An AUP is one of the most important information security policy documents. It can help prevent a wide range of activities that could harm the organization's IT resources.

An AUP can address a number of concerns. They include personnel, legal, and information security issues. HR departments like AUPs because they help promote workplace productivity. They also want to make sure that employees aren't accessing or sharing objectionable electronic materials. Such behavior can cause severe disruptions in the workplace. In some instances, it also can subject the organization to liability for its employees' actions. For instance, an employer can be held responsible in some cases where an employee is using IT resources to harass other individuals. AUPs give HR departments a policy reason to terminate employees who use IT resources inappropriately.

Would an AUP Help in This Situation?

The "I Love You" or "Love Bug" worm was discovered in May 2000. At the time, it was thought to be one of the largest and most destructive computer worms ever. It spread via e-mail messages with "ILOVEYOU" in the subject line. The messages included an attachment disguised as a love letter. Once a user opened the attachment (and who wouldn't open a love letter?), the worm infected the user's computer. It sent itself to everyone in the user's e-mail address book. It destroyed computer files. It also searched for sensitive information and sent it back to its creator.

At one point, industry experts estimated that the worm affected computers at more than 80 percent of U.S. businesses. Could an information security policy have helped stop the spread of the worm? What if an AUP stated that employees could not open e-mail attachments that they were not expecting? What if the consequence for opening that type of attachment included job termination? Would that have helped in this case?

FYI

Lost productivity isn't a new issue for organizations. Coffee breaks and water-cooler chats have always been productivity concerns. The Internet and ease of access to non-work-related information and entertainment is a relatively new nuisance.

Legal departments use AUPs to help an organization meet regulatory responsibilities. They also use them to help limit an organization's legal liability. For instance, an AUP can state that employees may not use unlicensed software on their computers. This helps protect the organization from copyright infringement claims. An organization protects itself in these cases by pointing to its AUP and showing that the employee violated it. If the AUP forbids the action, the legal department has evidence that the employee acted in violation of company rules. This helps create a legal defense.

Information security departments also are interested in making sure that an organization has a well-written AUP. Improper use of IT resources can have information security consequences. Employees surfing the Internet, exchanging personal e-mails, or visiting social networking sites are consuming network bandwidth. They may be using valuable network storage space for non-business content.

Their activities also could introduce malware onto the organizations IT systems. Malware could compromise data and have wide-ranging consequences. At a minimum, productivity is hampered while IT departments work to remove the malware. At its worst, the malware could transmit sensitive organizational information to external attackers. It also could expose personal indentifying information. That could trigger state breach notification laws.

AUPs also address internal employee threats. Employees can potentially use their access to IT resources to snoop or spy on the organization. They also could spy on other employees. Disgruntled employees could use their access to sabotage IT resources and data. An AUP specifically prohibits these actions. An organization can fire an employee for violating an AUP.

AUP Terms

An organization protects against these concerns by having a written AUP. Some general terms that you see in AUPs include:

- IT resources are provided for business use only.
- Employees must use IT resources and data on them for business purposes only.
- Employees must not tamper with IT resources or data on those resources.
- Employees should not access any data they don't have a business reason to see.
- No personal use of organizational IT resources is allowed.
- Don't use IT resources to circumvent security measures.
- IT resources may be monitored to ensure employee compliance.
- Use of IT resources is evidence of the employee's consent to the terms of the AUP.

AUPs may have terms about a particular type of IT resource, such as e-mail or Internet use. Some organizations include these terms in one broad AUP. Other organizations may create a separate AUP for each type of technology. Common e-mail and Internet AUP terms include:

- Don't send e-mail with sensitive organization information to external recipients.
- Don't send e-mail with sensitive organization information to internal recipients unless they have a business need to have that information.
- Don't send e-mail with offensive text, pictures, or links to offensive Web sites. Content is offensive if it's demeaning based on race, gender, national origin, disability, religion, or politics.
- Don't open e-mail attachments from unknown senders. Don't open e-mail messages with unexpected attachments.
- Don't click on embedded links in an e-mail from unknown senders.
- Don't download files from the Internet without permission from a business supervisor and the information security department.
- Don't use file-sharing applications or services without permission from a business supervisor and the information security department.
- Don't use IT resources to access the Internet to view offensive material.
- Don't use IT resources to access the Internet to visit social networking sites.
- Don't use IT resources for online shopping.
- Don't use IT resources to engage in activity that violates the law.

Mobile devices pose special information security threats. They're small, pocket-sized computing devices. They include cell phones, smartphones, and personal digital assistants (PDAs). Use of mobile phones is rising. A January 2014 Pew Internet & American Life Project report found that 90 percent of U.S. adults have cell phones or smartphones. Sixty-three percent of those users access the Internet from their cell phone.[6]

Many people buy their own mobile devices and use them for work purposes. Organizations sometimes give their employees mobile devices. These devices pose security threats because they can hold an organization's sensitive information. Employee's can use these devices to browse the Internet, send and receive e-mail, and view documents. The computing capacity of these devices continues to grow. They can store large amounts of data. Many of the same types of malware that infect larger IT resources also can harm these devices.

Mobile devices also are a vulnerability because of their portable nature. People can easily lose or misplace their mobile devices. They're easy to steal. A lost or stolen mobile device can put an organization's data at risk.

An AUP places controls on the use of mobile devices for business purposes. In addition to terms about e-mail and Internet use, an AUP might have specific terms about mobile devices:

- Mobile devices that are used to access organizational resources or data must be password protected.
- Mobile devices (whether provided by the organization or purchased by an employee and used for business purposes) must not store sensitive organizational information.
- Employees must immediately report the loss of a mobile device used to access organizational resources.

Organizations typically make employees aware of their AUPs when the employee begins employment. They may print it in an employee handbook. Organizations may ask employees to read the AUP. They also might ask employees to sign an acknowledgment form. It states that the employee understands and agrees to follow the rules in the AUP. The acknowledgment also might state that an employee understands the consequences for failing to follow an AUP.

Organizations should require employees to review the AUP yearly. They also must require that employees review the AUP any time it's revised. They may ask employees to sign a new acknowledgment form at that time. This helps the organization make sure that employees are aware of their responsibilities.

Enforcement

The 2007 Electronic Monitoring and Surveillance Survey found that 28 percent of employers have fired employees for e-mail abuse. The same survey said that of those employees fired for e-mail abuse, 64 percent were fired for violating company policy.[7]

An AUP must specify the consequences for violating it. Consequences for violating an AUP can include:

- Suspension of access to IT resources
- Limited access to IT resources
- Employee reprimand
- Employment suspension
- Employment termination
- Referral to law enforcement

Modest AUP violations may result in suspending an employee's access to IT resources for a period of time. An organization could fire an employee for a particularly harmful AUP violation. AUP violations that amount to criminal conduct should be reported to law enforcement. For example, an organization should notify the police if an employee uses its IT resources to launch a malware attack.

It can sometimes be hard for organizations to enforce their AUPs. This is especially true if they have no technical methods to monitor compliance. Most organizations depend on employees to police their own behavior. They may have a procedure for employees to report AUP violations.

Anti-Harassment Policies

Workplace harassment is a serious issue. *Harassment* is unwanted verbal or physical conduct. It's conduct that demeans or threatens a person. Some examples include:

- Telling lewd, sexist, or racist jokes
- Making racially derogatory comments
- Making remarks about body shape, looks, or clothing
- Starting at people in a suggestive manner
- Making negative comments about a person's religious beliefs
- Threatening a person or his or her family with harm

Workplace harassment can violate federal law. This happens when the unwanted conduct is based on certain characteristics. The main law in this area is Title VII of the 1964 Civil Rights Act.[8] It forbids workplace discrimination based on race, sex, religion, disability, and ethnicity. These are called immutable characteristics. A person can't change them.

Title VII applies to most public and private employers. Employers with 15 or more employees must follow it. The law states that employers have a duty to prevent workplace discrimination. They also have a duty to stop it if they know about it. Workplace discrimination and harassment claims are often tied together.

Workplace harassment has always been a major issue for employers. The rise in Internet and e-mail communications in the work environment adds extra complications. They introduce a new way for harassers to communicate with victims. E-mails shared among employees that have offensive, explicit, or violent content could lead to harassment claims. So could viewing offensive material from a work computer screen in a public area. Employee-downloaded screensavers on an organization's computers can be a problem if they're offensive.

These activities raise legal liability when other employees are offended or feel harassed. Employees also could make tort claims against an employer for intentional infliction of emotional distress.

Employers use anti-harassment policies to help limit liability for workplace harassment. Many organizations develop no-tolerance policies. They often use their AUPs to forbid offensive use of IT resources as well. Many organizations do this. However, the issue is serious enough that organizations should have a separate anti-harassment policy. In addition to forbidding in-person harassment, the policy should state that an organization's IT resources can't be used to harass others.

Anti-harassment policies should contain the following elements:

- **Definition of harassment**—It should define inappropriate conduct. This includes in-person and electronic interactions that are threatening, intimidating, or offensive in nature. Conduct is offensive if it's demeaning based on race, gender, national original, disability, religion, or politics.
- **Reporting**—The organization must give employees a way to report harassment. The reporting method must include alternatives if the alleged harasser is a victim's direct supervisor.

- **Investigation**—An organization must investigate harassment complaints. They must stop harassment when they have reasonable evidence that it's occurring.
- **No Retaliation**—The organization must make sure that it doesn't retaliate against employees who file harassment complaints. *Retaliation* is an adverse employment action made for a non-job-related reason. An organization may not take an adverse employment action against an employee who files a harassment complaint just because that employee filed a complaint.
- **Sanctions**—The policy should state the consequences for violating the policy.

> **NOTE**
>
> In 2000, Dow Chemical Co. fired 74 employees for sending e-mails with pornography and violent images. It also disciplined more than 400 additional employees for similar actions. Dow had policies that prohibited employees from sending such e-mails.

Information security personnel may participate in a harassment investigation. They may investigate whether the organization's IT resources hold evidence related to the claim.

The law allows victims to recover damages from their harassers. They also might be able to recover damages from the harassers' employers if they failed to respond to harassment complaints. The law allows victims to receive compensatory damages. They also can receive punitive damages in some cases. The damages can be substantial.

Workplace Privacy and Monitoring Policies

Workplace privacy addresses an employee's privacy rights at work. It's a controversial issue. Employees don't like to have their activities monitored. It can create feelings of distrust in a workplace.

Workplace privacy and monitoring is an area of law that continues to develop. For the most part, however, U.S. employees have very few privacy rights in their use of an organization's IT resources. An organization may monitor an employee's work e-mail and Internet use in many instances. Monitoring is usually allowed if there's a legitimate business reason for it. Legitimate reasons to monitor e-mail and Internet access include:

- Assessing employee productivity
- Monitoring operational use of IT resources
- Monitoring policy compliance
- Monitoring the use of the organization's intellectual property
- Investigating allegations of wrongdoing
- Managing risk and protecting against legal liability

The information security department is often involved in workplace monitoring activities. This department has the knowledge and ability to carry out an organization's desire to monitor IT resource use.

Does Cyber Monday Pose a Productivity Problem?

Black Friday is the day after the U.S. Thanksgiving holiday. It's the traditional start of the winter holiday shopping season. Stores and retailers often have sales on this day to encourage shoppers to spend money.

Cyber Monday is the first Monday after the holiday. It's the cyber-equivalent to Black Friday. Many retailers noticed an increase in online sales on this day. They suggested that this was because employees used their employer's computers and high-speed connections to shop online when they returned to work after the holiday. The National Retail Federation (NRF) created the term in 2005 to describe this activity.[9]

A 2013 NRF survey said that more than 131.5 million Americans reported that they planned to shop on Cyber Monday. Almost 16 million of these shoppers planned to use their work computers.[10]

How should an organization deal with Cyber Monday? What are the problems that it poses for productivity? What are the problems that it poses for information security?

Employers usually win employee legal challenges against monitoring of business e-mail and Internet use. To win these challenges, organizations must show that they had a legitimate business reason for monitoring IT resources. They also must show that they conducted the monitoring in a proper way.

Workplace privacy and monitoring policies are often combined together. They inform employees that:

- Their use of IT resources isn't private.
- Their use of IT resources is monitored.

Well-written policies give employees clear notice that they have no expectation of privacy in an organization's IT resources. They give an employee notice that their use of IT resources will be monitored. They also might state why an organization monitors its IT resources. Finally, they should state that an organization doesn't waive its right to monitor IT resources even if it chooses not to do so all the time.

Data Retention and Destruction Policies

Data retention and destruction is a hot topic for many organizations. **Data retention policies** state how data is controlled throughout its life cycle. Laws and organizational policies help determine retention periods.

Data destruction policies state how data must be destroyed when it reaches the end of its life cycle. Organizations must destroy paper and electronic data when it's no longer needed. For electronic data, this means destroying it in primary and backup storage systems.