Information Protection

Rebecca Herold
Information Privacy, Security and Compliance Consultant, Rebecca Herold and Associates LLC, Van Meter, Iowa, U.S.A.

Abstract
Successful information protection and security requires the participation, compliance, and support of all personnel within an organization, regardless of their positions, locations, or relationships with the company. This includes any person who has been granted access to the organization’s extended enterprise information, and any employee, contractor, vendor, or business associate of the company who uses information systems resources as part of the job. A brief overview of the information protection and security responsibilities for various groups within an organization follows.

ALL PERSONNEL WITHIN THE ORGANIZATION
All personnel have an obligation to use the information according to the specific protection requirements established by an organization’s information owner or information security delegate. A few of the basic obligations include, but are not limited to, the following:

- Maintaining confidentiality of log-on passwords
- Ensuring the security of information entrusted to their care
- Using the organization’s business assets and information resources for approved purposes only
- Adhering to all information security policies, procedures, standards, and guidelines
- Promptly reporting security incidents to the appropriate management area

Information Security Oversight Committee
An information protection and/or security oversight committee comprising representatives from various areas of an organization should exist or be created if not already in existence. The members should include high-level representatives from each of the revenue business units, as well as a representative from the organization’s legal, corporate auditing, human resources, physical and facilities management, and finance and accounting areas. The oversight committee should be responsible for ensuring and supporting the establishment, implementation, and maintenance of information protection awareness and training programs to assist management in the security of corporate information assets. Additionally, the committee should be kept informed of all information security-related issues, new technologies, and provide input for information security, protection costs, and budget approvals.

Corporate Auditing
The corporate auditing department should be responsible for ensuring compliance with information protection and security policies, standards, procedures, and guidelines. They should ensure that the organizational business units are operating in a manner consistent with policies and standards, and ensure any audit plan includes a compliance review of applicable information protection policies and standards that are related to the audit topic. Additionally, a high-level management member of the corporate auditing department should play an active role in the organization’s information security oversight committee.

Human Resources
The human resources department of an organization should be responsible for providing timely information to the centrally managed information protection department, as well as the enterprise and division systems managers and application administrators, about corporate personnel terminations or transfers. They should also enforce the stated consequences of non-compliance with the corporate policies, and a high-level member of the human resources department should play an active role in the organization’s information security oversight committee.

Law
The law department should assign to someone the responsibility for reviewing the enterprise security policies and standards for legal and regulatory compliance and enforceability. The law department should also be advised of and responsible for addressing legal issues arising from security incidents. Additionally, a high-
level member of the law department should play an active role in the organization’s information security oversight committee. This person should be savvy with computer and information technology (IT) and related issues; otherwise, the person will not make a positive contribution to the oversight committee, and could, in fact, create unnecessary roadblocks or stop necessary progress owing to lack of knowledge of the issues.

Managers

The organization’s line management should retain primary responsibility for identifying and protecting information and computer assets within their assigned areas of management control. When talking about a manager, one is referring to any person who has been specifically given responsibility for directing the actions of others and overseeing their work—basically, the immediate manager or supervisor of an employee. Managers have ultimate responsibility for all user identity documents (IDs) and information owned by company employees in the areas of their control. In the case of nonemployee individuals, such as contractors, consultants, and so on, managers are responsible for the activity and the company assets used by these individuals. These managers are the ones usually responsible for hiring the outside party. Managers have additional information protection and security responsibilities including, but not limited to, the following:

- Continually monitor the practices of employees and consultants under their control and take necessary corrective actions to ensure compliance with the organization’s policies and standards.
- Inform the appropriate security administration department of the termination of any employee so that the user ID owned by that individual can be revoked, suspended, or made inaccessible in a timely manner.
- Inform the appropriate security administration department of the transfer of any employee if the transfer involves the change of access rights or privileges.
- Report any security incident or suspected incident to the centralized information protection department.
- Ensure the currency of user ID information (e.g., employee identification number and account information of the user ID owner).
- Educate the employees in their area of the organization’s security policies, procedures, and standards for which they are accountable.

IT Administrators (Information Delegates)

A person, organization, or process that implements or administers security controls for the information owners is referred to as an information delegate. Such information delegates typically (but not always) are part of the IT departments with primary responsibilities for dealing with backup and recovery of the business information, applying and updating information access controls, installing and maintaining information security technology, and systems and so on.

An information delegate is also any company employee who owns a user ID that has been assigned attributes or privileges associated with access control systems, such as Top Secret, RACF, ACF2 and so on. This user ID allows them to set system-wide security controls or administrator user IDs and information resource access rights. These security and systems administrators may report to either a business division or the central information protection department.

Information delegates are also responsible for implementing and administering security controls for corporate extended enterprise information as instructed by the information owner or delegate. Some of the responsibilities of information delegates include, but are not limited to, the following:

- Perform backups according to the backup requirements established by the information owner.
- Document backup schedule, backup intervals, storage locations, and number of backup generation copies.
- Regularly test backups to ensure they can be used successfully to restore data.
- When necessary, restore lost or corrupted information from backup media to return the application to production status.
- Perform related tape and direct access storage device management functions as required to ensure availability of the information to the business.
- Ensure record retention requirements are met based on the information owner’s analysis.
- Implement and administer security controls for corporate extended enterprise information as instructed by the information owner or delegate.
- Electronically store information in locations based on classification.
- Specifically identify the privileges associated with each system, and categorize the staff allocated to these privileges.
- Produce security log reports that will report applications and system violations and incidents to the central information protection department.
- Understand the different data environments and the impact of granting access to them.
- Ensure access requests are consistent with the information directions and security guidelines.
- Administer access rights according to criteria established by the information owners.
- Create and remove user IDs as directed by the appropriate managers.
• Administer the system within the scope of the job
description and functional responsibilities.
• Distribute and follow up on security violation reports.
• Report suspected security breaches to your central
information protection department.
• Give passwords of newly created user IDs to the user
ID owner only.
• Maintain responsibility for day-to-day security of
information.

Information Asset and Systems Owners

The information asset owner for a specific data item is a
management position within the business area facing the
greatest negative impact from disclosure or loss of that
information. The information asset owner is ultimately
responsible for ensuring that appropriate protection
requirements for the information assets are defined and
implemented. The information owner responsibilities
include, but are not limited to, the following:

• Assign initial information classification and periodi-
cally review the classification to ensure it still meets
the business needs.
• Ensure security controls are in place and commensu-
rate with the information classification.
• Review and ensure currency of the access rights asso-
ciated with information assets they own.
• Determine security requirements, access criteria, and
backup requirements for the information assets
they own.
• Report suspected security breaches to corporate
security.
• Perform, or delegate if desired, the following:
  ○ Approval authority for access requests from other
  business units or assign a delegate in the same
  business unit as the executive or manager owner.
  ○ Backup and recovery duties or assign to the
  information custodian.
  ○ Approval of the disclosure of information.
  ○ Act on notifications received concerning security
  violations against their information assets.
  ○ Determine information availability requirements.
  ○ Assess information risks.

Systems owners must consider three fundamental
security areas: management controls, operational con-
trols, and technical controls. They must follow the
direction and requests of the information owners when
establishing access controls in these three areas.

Information Protection

An area should exist that is responsible for determining
your organization’s information protection and security
directions (strategies, procedures, guidelines), as
approved or suggested by the information protection
oversight committee, to ensure information is controlled
and secured based on its value, risk of loss or compro-
mise, and ease of recoverability. As a very high
overview, some of the responsibilities of an information
protection department include, but are not limited to, the
following:

• Provide information security guidelines to the infor-
  mation management process.
• Develop a basic understanding of your organization’s
  information to ensure proper controls are
  implemented.
• Provide information security design input, consulting,
  and review.
• Ensure appropriate security controls are built into
  new applications.
• Provide information security expertise and support
  for electronic interchange.
• Create information protection audit standards and
  baselines.
• Help reduce the organization’s liability by demonstr-
  ating a standard of due care or diligence by fol-
  lowing general standards or practices of
  professional care.
• Help ensure awareness of information protection and
  security issues throughout the entire organization and
  act as internal information security consultants to
  project members.
• Promote and evaluate information and computer
  security in IT products and services.
• Advise others within the organization of information
  security needs and requirements.

The remainder of this entry includes a full discussion
of the roles and related issues of the information protec-
tion department.

WHAT IS THE ROLE OF INFORMATION
PROTECTION?

Secure information and network systems are essential to
providing high-quality services to customers, avoiding
fraud and disclosure of sensitive information, promoting
efficient business operations, and complying with laws
and regulations. The organization must make informa-
tion protection a visible, integral component of all
business operations. The best way to accomplish this is
to establish a department dedicated to ensuring the pro-
tection of all the information assets of the organization
throughout every department and process. Information
protection, or information security, is a very broad
discipline.
The information protection department should fulfill five basic roles:

1. Support information risk management processes.
2. Create corporate information protection policies and procedures.
3. Ensure information protection awareness and training.
4. Ensure the integration of information protection into all management practices.
5. Support the organization’s business objectives.

Risk Management

Risk management is a necessary element of a comprehensive information protection and security program. What is risk management? The General Accounting Office (GAO) has a good, high-level definition: risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk. There are four basic principles of effective risk management.

Assess risk and determine needs

The organization must recognize that information is an essential asset that must be protected. When high-level executives understand and demonstrate that managing risks is important and necessary, it will help to ensure that security is taken seriously at lower levels in the organization and that security programs have adequate resources.

The organization must develop practical risk assessment procedures that clearly link security to business needs. However, spend too much time must not be spent trying to quantify the risks precisely—the difficulty in identifying such data makes the task inefficient and overly time consuming.

The organization must hold program and business managers accountable for ensuring compliance with information protection policies, procedures, and standards. The accountability factor will help ensure that managers understand the importance of information protection and not dismiss it, considering it a hindrance.

The risks must be managed on a continuing basis. As new technologies evolve, one must stay abreast of the associated risks to information assets. And, as new information protection tools become available, one must know how such tools can help mitigate risks within the organization.

Establish a central information protection and risk management focus

The information protection department will focus on central information protection and risk management.

Key information protection risk management activities must be carried out. The information protection department will serve as a catalyst for ensuring that information security risks are considered in planned and ongoing operations. There is a need to provide advice and expertise to all organizational levels and keep managers informed about security issues. Information protection should research potential threats, vulnerabilities, and control techniques, and test controls, assess risks, and identify needed policies.

The information protection department must have ready and independent access to senior executives. Security concerns can often be at odds with the desires of business managers and system developers when they are developing new computer applications—they want to do so quickly and want to avoid controls that they view as impeding efficiency and convenience. By elevating security concerns to higher management levels, it helps ensure that the risks are understood by those with the most to lose from information security incidents and that information security is taken into account when decisions are made.

The information protection department must have dedicated funding and staff. Information protection budgets need to cover central staff salaries, training and awareness costs, and security software and hardware.

The central information protection department must strive to enhance the professionalism and technical skills of the staff. It is important in fulfilling one’s role as a trusted information security advisor to be informed on new information security vulnerabilities as well as new information security tools and practices.

Information and systems security must be cost-effective

The costs and benefits of security must be carefully examined in both monetary and nonmonetary terms to ensure that the cost of controls does not exceed expected benefits. Security benefits have direct and indirect costs. Direct costs include purchasing, installing, and administering security measures, such as access control software or fire-suppression systems. Indirect costs include system performance, employee morale, and retraining requirements.

Information and systems security must be periodically reassessed

Security is never perfect when a system is implemented. Systems users and operators discover new vulnerabilities or ways to intentionally or accidentally circumvent security. Changes in the system or the environment can also create new vulnerabilities. Procedures become outdated over time. All these issues make it necessary to
periodically reassess the effectiveness of the organization’s security.

**Information Protection Policies, Procedures, Standards, and Guidelines**

The information protection department must create corporate information protection policies with business unit input and support. Additionally, they must provide guidance and training to help the individual business units create their own procedures, standards, and guidelines that support the corporate information protection policies.

Information protection department must create and implement appropriate policies and related controls

There is a need to link the information protection policies created to the business risks of the organization. The information protection policies must be adjusted on a continuing basis to respond to newly identified risks. Paying particular attention to addressing user behavior within the information protection policies must be ensured.

Distinguish between information protection policies and guidelines or standards. Policies generally outline fundamental requirements that managers consider mandatory. Guidelines and standards contain more detailed rules on how to implement the policies.

It is vital to the success of the information protection policies for the oversight group and executive management to visibly support the organization’s information protection policies.

**Information and systems security is often constrained by societal factors**

The ability of the information protection department to support the mission of the organization may be limited by various social factors depending upon the country in which its offices are located, or the laws and regulations that exist within certain locations where the organization does business. The information protection department must know the operating environments and ensure the organization’s policies are in sync with these environments.

**Awareness and Training**

The information protection department must make the organization aware of information protection policies, related issues, and news on an ongoing basis. Additionally, adequate training must be provided—not only to help ensure personnel know how to address information security risks and threats, but also to keep the information protection department personnel up-to-date on the most appropriate methods of ensuring information security.

An information protection department must promote awareness of information protection issues and concerns throughout your entire organization

The information protection department must continually educate users and others on risks and related policies. Merely sending out a memo to the management once every year or two is not sufficient. Use attention-getting and user-friendly techniques to promote awareness of information protection issues. Awareness techniques do not need to be dry or boring—they should not be, or the personnel will not take notice of the message one is trying to send.

An information protection department must monitor and evaluate policy and control effectiveness of the policies

The information protection department needs to monitor factors that affect risk and indicate security effectiveness. One key to success is to keep summary records of actual security incidents within the organization to measure the types of violations and the damage suffered from the incidents. These records will be valuable input for risk assessments and budget decisions. The results of monitoring and record keeping can help to determine subsequent information protection efforts and hold managers accountable for the activities and incidents that occur. Staying aware of new information protection and security monitoring tools and techniques is must to address the issues found during monitoring.

An information protection department must extend security responsibilities to those outside the organization

The organization and the systems owners have security responsibilities outside the organization. They have a responsibility to share appropriate knowledge about the existence and extent of security measures with the external users (e.g., customers, business partners and so on) for them to be confident that the systems are adequately secured and can help to address any risks that is communicated to them.

An information protection department must make security responsibilities explicit

Information and systems security responsibilities and accountability must be clearly and explicitly documented and communicated. The information security...
responsibilities of all groups and audiences within the organization must be communicated to them, using effective methods and on an ongoing basis.

Management Practices

Information and systems security must be an integral element of sound management practices. Ultimately, managers of the areas owning the information must decide what level of risk they are willing to accept, taking into account the cost of security controls as well as the potential financial impact of not having the security controls. The information protection department must help the management understand the risks and associated costs. Information and systems security requires a comprehensive approach that is integrated within the organization’s management practices. The information protection department also needs to work with traditional security disciplines, such as physical and personnel security. To help integrate information protection within the management practices, use the following:

- Establish a process to coordinate implementation of information security measures. The process should coordinate specific information security roles and responsibilities organization-wide, and it should aid agreement about specific information security methods and processes, such as risk assessment and a security classification system. Additionally, the process should facilitate coordination of organization-wide security initiatives and promote integration of security into the organizational information planning process. The process should call for implementation of specific security measures for new systems or services and include guidelines for reviewing information security incidents. Also, the process should promote visible business support for information security throughout the organization.
- Establish a management approval process to centrally authorize new IT facilities from both a business and technical standpoint.
- Make managers responsible for maintaining the local information system security environment and supporting the corporate information protection policies when they approve new facilities, systems, and applications.
- Establish procedures to check hardware and software to ensure compatibility with other system components before implementing them into the corporate systems environment.
- Create a centralized process for authorizing the use of personal information processing systems and facilities for use in processing business information. Include processes to ensure necessary controls are implemented. In conjunction with this, ensure the vulnerabilities inherent in using personal information processing systems and facilities for business purposes have been assessed.
- Ensure management uses the information protection department for specialized information security advice and guidance.
- Create a liaison between the information protection department and external information security organizations, including industry and government security specialists, law enforcement authorities, IT service providers, and telecommunications authorities, to stay abreast with new information security threats and technologies and to learn from the experiences of others.
- Establish management procedures to ensure that the exchange of security information with outside entities is restricted so that confidential organizational information is not divulged to unauthorized persons.
- Ensure information protection policies and practices throughout the organization are independently reviewed to ensure feasibility, effectiveness, and compliance with written policies.

Business Objectives

Information protection must support the business needs, objectives, and mission statement of the organization. Information and systems security practices must support the mission of the organization. Through the selection and application of appropriate safeguards, the information protection department will help the organization’s mission by protecting its physical and electronic information and financial resources, reputation, legal position, employees, and other tangible and intangible assets. Well-chosen information security policies and procedures do not exist for their own sake—they are put in place to protect the organization’s assets and support the organizational mission. Information security is a means to an end, and not an end in itself. In a private-sector business, having good security is usually secondary to the need to make a profit. With this in mind, security ought to be seen as a way to increase the firm’s ability to make a profit. In a public sector agency, security is usually secondary to the agency’s provision of services to citizens. Security, in this case then, ought to be considered as a way to help improve the service provided to the public.

So, what is a good mission statement for the information protection department? It really depends upon the business, environment, company size, industry, and several other factors. To determine the information protection department’s mission statement, ask yourself these questions:
Information Protection

- What do the personnel, systems users, and customers expect with regard to information and systems security controls and procedures?
- Will the organization lose valued staff or customers if information and systems security is not taken seriously enough, or if it is implemented in such a manner that functionality is noticeably impaired?
- Has any downtime or monetary loss occurred within the organization as a result of security incidents?
- Is the organization concerned about insider threats? Does it trust its users? Are most of the systems users local or remote?
- Does the organization keep non-public information online? What is the loss to the organization if this information is compromised or stolen?
- What would be the impact of negative publicity if the organization suffered an information security incident?
- Are there security guidelines, regulations, or laws the organization is required to meet?
- How important are confidentiality, integrity, and availability to the overall operation of the organization?
- Have the information and network security decisions that have been made been consistent with the business needs and economic stance of the organization?
- Does the information protection department is located within the organization.

To help get started with creating an information protection department mission statement, here is an example to use in conjunction with considering the previous questions:

The mission of the information protection department is to ensure the confidentiality, integrity, and availability of the organization’s information; provide information protection guidance to the organization’s personnel; and help ensure compliance with information security laws and regulations while promoting the organization’s mission statement, business initiatives, and objectives.

Information Protection Budgeting

What should be the organization’s budget for information protection? One will not like the answer; however, there is no benchmark for what information protection and security could or should cost within organizations. The variables from organization to organization are too great for such a number. Plus, it really depends upon how information protection and security costs are spread throughout the organization and where the information protection department is located within the organization.

Most information and network security spending recommendations are in extremes. The Gartner Group research in 2000 showed that government agencies spent 3.3% of their IT budgets on security—a significantly higher average percentage than all organizations as a whole spent on security (2.6%). Both numbers represent a very low amount to spend to protect an organization’s information assets. Then there is the opinion of a former chief security officer (CSO) at an online trading firm who believes the information security budget should be 4–10% of total company revenues and not part of the IT budget at all. An October 2001, Computerworld/P.J. Morgan security poll had showed that companies with annual revenues of more than $500 million were expected to spend the most on security in 2002, when security-related investments would have accounted for 11.2% of total IT budgets on average, compared with an average of 10.3% for all the users that responded to the poll. However, there are other polls, such as a 2001 survey from Metricnet, that showed that only 33% of companies polled after September 11, 2001, had spent more than 5% of their IT budgets on security. What is probably the most realistic target for information security spending is the one given by eSecurityOnline.com, which indicates information protection should be 3–5% of the company’s total revenue.

Unfortunately, it has been documented in more than one news report that some CIOs do not consider information security a normal or prudent business expense. Some CFOs and CEOs have been quoted as saying information security expenses were “nuisance protection.” Some decision makers need hard evidence of a security threat to their companies before they will respond. But doing nothing is not a viable option. It only takes one significant security incident to bring down a company.

When budgeting for information protection, keep in mind the facts and experiences of others. As the San Francisco-based Computer Security Institute found in its 2001 annual Computer Crime and Security Survey, 85% of the respondents admitted they had detected computer security breaches during the year. Although only 35% of the respondents admitted to being able to quantify the losses, the total financial impact from these incidents was a staggering $378 million in losses.

The CIO of the Department of Energy’s Lawrence Livermore National Laboratory in Livermore, California, indicated in 2001 that security incidents had risen steadily by about 20% a year. Security of information is not a declining issue; it is an increasingly significant issue to address. Basically, security is a matter of existence or nonexistence for data.

So, to help establish the information protection budget:

- Establish need before cost. If the organization knows money is going to be a stumbling block, then it must not lead with a budget request. Instead, a break down of the company’s functions by business process will illustrate how these processes are tied to the
Executive management must clearly and unequivocally support information protection and security initiatives. It must provide a role model for the rest of the organization that adhering to information protection policies and practices is the right thing to do. It must ensure information protection is built into the management framework. The management framework should be established to initiate and control the implementation of information security within the organization. Ideally, the structure of a security program should result from the implementation of a planned and integrated management philosophy. Managing computer security at multiple levels brings many benefits. The higher levels (such as the headquarters or unit levels) must understand the organization as a whole, exercise more authority, set policy, and enforce compliance with applicable policies and procedures. On the other hand, the systems levels (such as the computer facility and applications levels) know the technical and procedural requirements and problems. The information protection department addresses the overall management of security within the organization as well as corporate activities such as policy development and oversight. The system-level security program can then focus on the management of security for a particular information processing system. A central information protection department can disseminate security-related information throughout the organization in an efficient and cost-effective manner. A central information protection department has an increased ability to influence external and internal policy decisions. A central information protection department can help ensure spending its scarce security dollars more efficiently. Another advantage of a centralized program is its ability to negotiate discounts based on volume purchasing of security hardware and software.

Where Does the Information Security Role Best Fit within the Organization?

Information security should be separated from operations. When the security program is embedded in IT operations, the security program often lacks independence, exercises minimal authority, receives little management attention, and lacks resources. In fact, the GAO identified this type of organizational mode (information security as part of IT operations) as a principal basic weakness in federal agency IT security programs.

The location of the information protection department needs to be based on the organization’s goals, structure, and culture. To be effective, a central information protection department must be an established part of organization management.

Should information protection be a separate business unit reporting to the CEO?

This is the ideal situation. Korn/Ferry’s Jim Bock, a recruiter who specializes in IT and information security placements, has noticed that more CSOs are starting to report directly to the CEO, on a peer level to the CIO. This provides information protection with a direct line to executive management and demonstrates the importance of information security to the rest of the organization.
Should information protection be a separate business unit reporting to the CIO?

This is becoming more commonplace. This could be an effective area for the information protection group. However, there exists conflict of interest in this position. Additionally, security budgets may get cut to increase spending in the other IT areas for which the CIO has responsibility. Based upon latter-day history and published reports, CIOs tend to focus more on technology and security; they may not understand the diverse information protection needs that extend beyond the IT arena.

Should information protection be a separate business unit reporting to the CFO?

This could possibly work if the CFO also understands the information security finance issues. However, it is not likely because it is difficult (if not impossible) to show a return on investment for information security costs; so this may not be a good location for the information protection department.

Should information protection exist as a department within IT reporting to the IT VP?

This is generally not a good idea. Not only does this create a true conflict of interest, but it also demonstrates to the rest of the organization an attitude of decreased importance of information security within the organization. It creates a competition of security dollars with other IT dollars. Additionally, it sends the message that information protection is only a technical matter and does not extend to all areas of business processes (such as hard-copy protection, voice, fax, mail, etc.).

Should information protection exist as a group within corporate auditing reporting to the corporate auditor?

This has been attempted within several large organizations, and none have had success with this arrangement. Not only does this create a huge conflict of interest—auditors cannot objectively audit and evaluate the same security practices the people within their same area created—but it also sends the message to the rest of the organization that information security professionals fill the same role as auditors.

Should information protection exist as a group within human resources reporting to the HR VP?

This could work. One advantage of this arrangement is that the area creating the information protection policies would be within the same area as the people who enforce the policies from a disciplinary aspect. However, this could also create a conflict of interest. Also, by placing information protection within the HR area, you could send the message to the rest of the organization that information protection is a type of police unit; and it could also place it too far from executive management.

Should information protection exist within facilities management reporting to the risk management director?

This does place all types of risk functions together, making it easier to link physical and personnel security with information security. However, this could be too far removed from executive management to be effective.

Should information protection exist as a group within IT reporting to middle management?

This is probably the worst place to put the information protection group. Not only is this too far removed from executive management, but this also creates a conflict of interest with the IT processes to which information security practices apply. It also sends a message to the rest of the organization that information protection is not of significant importance to the entire organization and that it only applies to the organization’s computer systems.

What Security Positions Should Exist, and What are the Roles, Requirements, and Job Descriptions for Each?

Responsibilities for accomplishing information security requirements must be clearly defined. The information security policy should provide general guidance on the allocation of security roles and responsibilities within the organization. General information security roles and responsibilities must be supplemented with a more detailed local interpretation for specific sites, systems, and services. The security of an information system must be made the responsibility of the owner of that system. To avoid any misunderstanding about individual responsibilities, assets and security processes associated with each individual must be clearly defined. To avoid misunderstanding individual responsibilities, the manager responsible for each asset or security process must be assigned and documented and also authorization levels must be defined and documented. Multiple levels of dedicated information security positions must exist to ensure full and successful integration of information protection into all aspects of the organization’s business processes. So what positions are going to accomplish all these tasks? A few example job descriptions can be found in Table 1. The following are some suggestions of
Table 1  Example job descriptions
The following job descriptions should provide a reference to help create unique job descriptions for information security-related positions based upon the organization’s needs.

**Compliance officer**

**Job description**

A regulatory/compliance attorney to monitor, interpret, and communicate laws and legislation impacting regulation. Such laws and legislation include Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulations. The compliance officer will be responsible for compliance and quality control covering all areas within the IT and operations areas. Responsibilities include:

- Quality assurance
- Approval and release of all personal health information
- HIPAA compliance oversight and implementation
- Ensuring all records and activities are maintained acceptably in accordance with health and regulatory authorities

**Qualifications**

- J. D. with outstanding academics and a minimum of 10 years of experience
- Three to five years' existing experience with healthcare compliance and regulatory issues
- In-depth familiarity with federal and state regulatory matters (Medicare, Medicaid, fraud, privacy, abuse, etc.)

**Chief security officer**

**Job description:**

The role of the information security department is primarily to safeguard the confidential information, assets, and intellectual property that belongs to or is processed by the organization. The scope of this position primarily involves computer security but also covers physical security as it relates to the safeguarding of information and assets. The CSO is responsible for enforcing the information security policy, creating new procedures, and reviewing existing procedures to ensure that information is handled in an appropriate manner and meets all legislative requirements, such as those set by the HIPAA security and privacy standards. The security officer must also be very familiar with antivirus software, internet protocol firewalls, virtual private network (VPN) devices, cryptographic ciphers, and other aspects of computer security

**Requirement:**

- Experience with systems and networking security
- Experience with implementing and auditing security measures in a multiprocessor environment
- Experience with data center security
- Experience with business resumption planning
- Experience with firewalls, VPNs, and other security devices
- Good communication skills, both verbal and written
- Good understanding of security- and privacy-related legislation as it applies to the Maintenance Management Information System (MMIS)
- Basic knowledge of cryptography as it relates to computer security
- CISSP certification

**Duties and responsibilities:**

The information security department has the following responsibilities:

- Create and implement information security policies and procedures
- Ensure that procedures adhere to the security policies
- Ensure that network security devices exist and are functioning correctly where they are required (such as firewalls and software tools such as antivirus software, intrusion detection software, log analysis software, etc.)
- Keep up-to-date on known computer security issues and ensure that all security devices and software are continuously updated as problems are found
- Assist the operations team in establishing procedures and documentation pertaining to network security
- Assist the engineering team to ensure that infrastructure design does not contain security weaknesses
- Assist the facilities department to ensure that physical security is adequate to protect critical information and assets
- Assist the customer systems administration and the professional services groups in advising clients on network security issues

(Continued)
• Provide basic security training programs for all employees, and—when they access information—partners, business associates, and customers
• In the event of a security incident, work with the appropriate authorities as directed by the executive
• Work with external auditors to ensure that information security is adequate and evaluate external auditors to ensure that external auditors meet proper qualifications

The CSO has the following responsibilities:
• Ensure that the information security department is able to fulfill the above mandate
• Hire personnel for the information security department
• Hold regular meetings and set goals for information security personnel
• Perform employee evaluations of information security personnel as directed by human resources
• Ensure that information security staff receives proper training and certification where required
• Participate in setting information security policies and procedures
• Review all company procedures that involve information security
• Manage the corporate information security policies and make recommendations for modifications as the needs arise

Information security administrator

Job specifications

The information security administrator will:
• Work with security analysts and application developers to code and develop information security rules, roles, policies, standards and so on.
• Analyze existing security rules to ensure no problems will occur as new rules are defined, objects added and so on.
• Work with other administrative areas in information security activities
• Troubleshoot problems when they occur in the test and production environments
• Define and implement access control requirements and processes to ensure appropriate information access authorization across the organizations
• Plan and develop user administration and security awareness measures to safeguard information against accidental or unauthorized modification, destruction, or disclosure
• Manage the overall functions of user account administration and the company-wide information security awareness training program according to corporate policies and federal regulations
• Define relevant data security objectives, goals, and procedures
• Evaluate data security user administration, resource protection, and security awareness training effectiveness
• Evaluate and select security software products to support the assigned functions
• Coordinate security software installation
• Meet with senior management regarding data security issues
• Participate in designing and implementing an overall data security program
• Work with internal and external auditors as required
• Ensure that user administration and information security awareness training programs adhere to HIPAA and other regulations

Qualifications
• Human relations and communication skills to effectively interact with personnel from technical areas, internal auditors, and end users, promoting information security as an enabler and not as an inhibitor
• Decision-making ability to define data security policies, goals, and tactics, and to accurately measure these practices as well as risk assessments and selection of security devices including software tools
• Ability to organize and prioritize work to balance cost and risk factors and bring adequate data security measures to the IT environments
• Ability to jointly establish measurable goals and objectives with staff, monitor progress on attainment of them, and adjust as required
• Ability to work collaboratively with IT and business unit management
• Ability to relate business requirements and risks to technology implementation for security-related issues
• Knowledge of role-based authorization methodologies and authentication technologies
• Knowledge of generally accepted security practices such as ISO 17799 standards
• Security administration experience
• Good communication skills
• Two to four years of security administration experience
• SSCP or CISSP certification a plus, but not required
positions for to consider establishing within an organization:

- **Chief Security Officer.** The CSO must raise security issues and help to develop solutions. This position must communicate directly with executive management and effectively communicate information security concerns and needs. The CSO will ensure security management is integrated into the management of all corporate systems and processes to assure that system managers and data owners consider security in the planning and operation of the system. This position establishes liaisons with external groups to take advantage of external information sources and to improve the dissemination of this information throughout the organization.

- **Information Protection Director.** This position oversees the information protection department and staff. This position communicates significant issues to the CSO, sets goals, and creates plans for the information protection department, including budget development. This position establishes liaisons that should be established with internal groups, including the information resources management office and traditional security offices.

- **Information Protection Awareness and Training Manager.** This position oversees all awareness and training activities within the organization. This position communicates with all areas of the organization about information protection issues and policies on an ongoing basis. This position ensures that all personnel and parties involved with outsourcing and customer communications are aware of their security responsibilities.

- **Information Protection Technical/Network Manager.** This position works directly with the IT areas to analyze and assess risks within the IT systems and functions. This position stays abreast of new information security risks as well as new and effective information security tools. This position also analyzes third-party connection risks and establishes requirements for the identified risks.

- **Information Protection Administration Manager.** This position oversees user account and access control practices. This person should have a wide experience range over many different security areas.

- **Privacy Officer.** This position ensures the organization addresses new and emerging privacy regulations and concerns.

- **Internal Auditor.** This position performs audits within the corporate auditing area in such a way as to ensure compliance with corporate information protection policies, procedures, and standards.

- **Security Administrator.** The systems security administrator should participate in the selection and implementation of appropriate technical controls and security procedures, understand system vulnerabilities, and be able to respond quickly to system security problems. The security administrator is responsible for the daily administration of user IDs and system controls, and works primarily with the user community.

- **Information Security Oversight Committee.** This is a management information security forum established to provide direction and promote information protection visibility. The committee is responsible for reviewing and approving information security policy and overall responsibilities. Additionally, this committee is responsible for monitoring exposure to major threats to information assets, for reviewing and monitoring security incidents, and for approving major initiatives to enhance information security.

### How Do You Effectively Maintain Separation of Duties?

When considering quality assurance for computer program code development, the principles of separation of duty are well established. For example, the person who designs or codes a program must not be the only one to test the design or the code. There is a need for similar separation of duties for information protection responsibilities to reduce the likelihood of accidental compromise or fraud. A good example is the 1996 Omega case where the network administrator, Tim Lloyd, was an employee who was responsible for anything to do with manufacturing the manufacturing of computers. As a result, when Lloyd was terminated, he was able to add a line of program code to a major manufacturing program that ultimately deleted and purged all the programs in the system. Lloyd also had erased all the backup tapes, for which he also had complete control. Ultimately, the company suffered $12 million in damages, lost its competitive footing in the high-tech instrument and measurement market, and 80 employees lost their jobs as a result. If separation of duties had been in place, this could have been avoided.

Management must be active in hiring practices (ensuring background checks) bonding individuals (which should be routine for individuals in all critical areas) and auditing and monitoring, which should be routine practices. Users should be recertified to resources, and resources to users, at least annually to ensure proper access controls are in place. Because the system administration group is probably placed within the confines of the computer room, an audit of physical and logical controls also needs to be performed by a third party.

Certain information protection duties must not be performed by the same person or within one area. For example, there should be separation of roles of systems operators, systems administrators, and security...
administrators, and separation of security-relevant functions from others. Admittedly, ideal separation can be costly in time and money, and often possible only within large staffs. There is a need to make information security responsibilities dependent upon the business, organization size, and associated risks. One must perform risk assessment to determine what information protection tasks should be centralized and what should be distributed. When considering separation of duties for information security roles, it is helpful to use a tool similar to the one in Table 2.

**How Large Should the Information Protection/Security Department Be?**

If only there was one easy answer to the question of how large an information protection department should be. This is one of the most commonly asked questions raised at information security conferences over the previous several years, and asked regularly within all the major information security companies. There is no “best practice” magic number or ratio. The size of an information protection department depends on many factors. These include, but are not limited to, the following:

- Industry
- Organization size
- Network diversification and size
- Number of network users
- Geographical locations

- Outsourced functions

Whatever size one determines is best for the organization, there is a need to ensure the staff chosen has a security background or, at least, has some basic security training.

**SUMMARY**

This entry reviewed a wide range of issues involved in creating an information protection program and department. Specifically:

- Organizational information protection responsibilities
- Roles of an information protection department
- Information protection budgeting
- Executive management support of information protection
- Where to place the information protection department within an organization
- Separation of information security duties
- Descriptions of information protection responsibilities

Accompanying this entry is a tool to help determine separation of information security duties (Table 2) and some examples of information protection job descriptions to help in getting one written (Table 1).
BIBLIOGRAPHY

3. NIST, Generally Accepted System Security Principles (GSSPs).