



Information Security Governance Top Actions for Security Managers

Purpose of This Document

In today's globally networked business environment, the significance of information and corresponding information systems is truly massive to enterprises. Securing that information and incorporating it into an overall corporate or enterprise governance approach are critical. Too often, enterprise information security has been dealt with or relegated as a technology issue with little or no consideration given to the holistic enterprise priorities and requirements.

In 2001, ITGI published *Information Security Governance: Guidance for Boards of Directors and Executive Management*. It provides a background as to why information security is important and who, in addition to technology managers and security professionals, should be concerned. It focuses on what the board and senior management should do to help ensure information security fits within the governance framework.

This publication provides value and support to security managers and further expands understanding of information security governance. The list of questions on pages 16 to 24 of the *Information Security Governance: Guidance for Boards of Directors and Executive Management* publication was used to create a list of must-do actions for CISM, CISOs and information security managers.

Contents

Each of the following pages contains:

- A question for senior management
- Considerations for security managers
- Information sources
- Evaluation and performance criteria
- Security program initiatives

The next slide shows how this information is formatted on the page.



This box repeats a question for senior management from *Information Security Governance: Guidance for Boards of Directors and Executive Management*. The question is designed to uncover information security issues and determine how to successfully implement information security governance. The publication is available in the ISACA Bookstore and is posted at www.itgi.org, click on the hotlink *About ITGI* and then click on the hotlink to *Recent Publications*.

Considerations for Security Managers

This box elaborates the relevant issues in business terms that security managers should be concerned with regarding the question in the above box.

Information Sources

This box lists where information can be found within the enterprise and externally to assist the security manager in determining the enterprise's response to the question in the box at the top of the page.

Evaluation and Performance Criteria

This box lists the criteria that can be used by the security manager in determining how effectively the enterprise is addressing the security considerations listed in the box above.

Security Program Initiatives

This box details the steps that the enterprise should take to address the security considerations outlined in the boxes above. It lists what needs to be done/accomplished to meet the expectations that are raised in the question for the board. Following the steps for all 19 questions provides a strong foundation for information security governance in the enterprise.





Are information and information security critical to the entity? If so, does the board understand the criticality of information security?

Considerations for Security Managers

Business objectives and demands drive the requirements for information and the attendant needs for information security. For many organizations, adequately secured information is crucial to key business processes, business initiatives and programs, and long-term plans and activities. The information security program needs to be aligned with essential business processes and activities.

Unless board members understand the criticality of information security, there may be insufficient support for security programs intended to mitigate or manage the related risks.

Information Sources

- Annual reports
- Board and board committee reports
- Business strategy documents
- Industry analyst reports
- Business impact assessment
- Business risk analysis
- Audit reports
- Security incidents summaries
- Security strategy documentation
- Security architecture summary
- Discussions with business process owners

Evaluation and Performance Criteria

- Information security policies and mission statements can be easily and explicitly linked to business objectives and demands.
- Critical business initiatives and activities are identified, and requirements for the integrity and availability of processes, information and information resources in support of these initiatives and activities are defined.
- Sensitive and private information is identified and security program requirements for its protection are defined.
- Legal, regulatory and contractual requirements related to process integrity, information confidentiality and business process continuance are identified and security program requirements defined.
- Security performance requirements are defined, and compliance is measured and reported to executive management. Security activities and effectiveness are tied to business objectives and demands.
- Board members receive a minimum of one annual report on the status of security for discussion and endorsement at a board meeting.
- Board-level sponsorship for security exists. The sponsorship promotes security and aids understanding of other members of the board.

Security Program Initiatives

- At a high level, define the security program in terms of business initiatives, priorities and strategic goals. Integrate security planning into business planning activities.
- Regularly report to senior management and to the board of directors identifying areas of business risk and the status of security programs related to this risk.



Has management issued a policy statement on information security? If it has, is the policy statement subject to continual updating? If it is not, why not?

Considerations for Security Managers

All information systems users (e.g., management, staff, business partners) need to understand their roles and responsibilities to protect the confidentiality, availability and integrity of the organization’s information assets. This must be communicated to all users in the form of a written policy statement. The statement must set out management’s objectives and expectations for information security in clear, unambiguous terms, along with the implications of noncompliance. Its existence also demonstrates management’s commitment to information security.

To ensure ongoing applicability and relevance, the policy statement needs to be reviewed and updated on an annual basis. Failure to update may demonstrate a lack of management commitment to information security, or the general lack of processes to manage organizational governance.

Information Sources

- The organization’s information security policy statement
- The organization’s internal governance program
- External sources for sample policy statements:
 - ISACA, www.isaca.org
 - Web searches
 - SANS Institute, www.sans.org

Evaluation and Performance Criteria

- A written policy statement exists. It may be in any form (e.g., hard copy, electronic, web site).
- The policy clearly states overall objectives and requirements for information security, scope (organization units, information assets), roles and responsibilities for each relevant party (e.g., asset owners, users, trustees), and any possible conditions for exceptions.
- The policy also clearly communicates the issuing authority and the implications of noncompliance.
- The information security policy framework serves to support more extensive statements of information security standards, practices and procedures.
- The issue/revision/review date is within the last year. If not, the policy statement still maintains relevance. Evidence exists (project documents, e-mails, memos to file) indicating that the policy statement has been reviewed.
- Overall strong security awareness on the part of all information system users exists. Understanding of security requirements and respect for implications of noncompliance are demonstrated.

Security Program Initiatives

- Define security requirements and create information security policy statements including an information security policy framework for supporting standards, procedures, guidelines and rules of use. Obtain support from executive management, and issue under its authority.
- Integrate the information security policy statement into the overall corporate governance program to ensure periodic review and update (or create a program if none exists).



What are the top three critical information assets of the enterprise? What confidence does management have regarding information availability, confidentiality and integrity over these critical information assets?

Considerations for Security Managers

Information assets include the entire collection of infrastructure (network and systems) hardware, programs and data needed to meet the organization’s information needs. They can represent a sizeable expenditure to acquire and maintain, and can be critical to the ongoing viability of the enterprise.

As an indication of the importance members of senior management give to information assets and their protection, they should be involved with, or endorse the results of, assessment processes identifying those information assets judged the *most* critical, in terms of their value to the organization.

For the top three, they should have confidence in their level of protection in the three key areas of information security:

- Availability—Information is available when required by the organization.
- Confidentiality—Information is obtained only by authorized users.
- Integrity—Information is not added, changed or deleted except by authorized users.

Information Sources

- Board of director minutes
- Executive committee minutes
- Information security committee minutes
- Information systems architecture
- Business risk assessments
- Business impact assessments
- Asset/classification register
- COBIT® *Security Baseline*

Evaluation and Performance Criteria

- Senior management is aware of critical information assets and demonstrates adequate concern regarding their protection.
- Evidence exists of a regularly meeting information security committee that includes senior management and addresses information security issues.
- An information security program is in place with demonstrated support from senior management (e.g., adequate funding, security policy issued by senior management).

Security Program Initiatives

- Establish an information security awareness and education program that includes senior management.
- Establish an information identification and classification scheme based on confidentiality, integrity and availability requirements.
- Create risk assessments related to critical information assets.
- Conduct ongoing security assessments.



Does management know where the enterprise is most vulnerable within the IT infrastructure?

Considerations for Security Managers

The information technology infrastructure consists of numerous physical devices (routers, servers, firewalls and business systems). These resources, and the information they process, can be vulnerable to the loss of confidentiality, integrity and availability, leaving management exposed to risk if such vulnerability is undetected.

It is therefore critical that the organization understand the nature and extent of threats to the IT infrastructure, the security mechanisms and procedures in place to mitigate those threats, and the vulnerabilities that remain. Steps must be taken to address the remaining vulnerabilities, starting with the most serious ones.

Information Sources

- Business risk assessments
- SAS 70 or Section 5900 reports
- IT architecture documents
- Internal audit reports
- External audit and evaluation reports
- External network assessments
- Network diagrams
- Network penetration results
- Security incident summaries
- Vendor-specific security bulletins (e.g., Microsoft Security Advisories)

Evaluation and Performance Criteria

- Business risk assessments are performed, clearly identifying critical IT infrastructure components and classifying and ranking them according to risk. Weaknesses are fully documented, along with recommended follow-up actions taken, especially for the areas of greatest vulnerability and risk.
- Adequate funding of security efforts exists in accordance with the degree of risk and business impact.
- Network diagrams are available, maintained on a regular basis and clearly describe the overall architecture. They identify key network perimeters and associated security protection mechanisms (e.g., firewall and IDS use and placement).
- Network vulnerability and penetration testing is performed on an annual basis. Results are delivered to senior management with clearly defined action plans to mitigate any identified risk.
- Critical infrastructure components are identified and continuously monitored.
- Senior IT management understands and agrees with security program activities and recommendations.

Security Program Initiatives

- Establish a risk management program that ensures critical IT assets are identified, threats and vulnerabilities are evaluated, and appropriate action is taken to deal with the associated risk. Include ongoing assessment of vulnerabilities through monitoring for system weaknesses, intrusion and vulnerability testing, and testing of contingency plans. Assessment should also include vulnerability management and security patch management frameworks.
- Create complete network infrastructure diagrams.
- Establish a security bulletin/vulnerability monitoring process.



Can the entity continue to operate if the critical information is unavailable, compromised or lost? What would be the consequences of a security incident in terms of lost revenues, lost customers and damaged investor confidence? What would be the consequences if the infrastructure became inoperable?

Considerations for Security Managers

Most business processes depend on the information systems used to support them. The loss of availability of information system or network infrastructure components has an impact on the ability to perform the business process, ranging from *minimal* (the process can carry on unimpeded or be delayed without any consequence to the organization) to *extreme* (the process cannot carry on, with serious implications to the organization). It is essential to identify all important information assets, and analyze the *business impact* if any asset is unavailable, compromised or lost. The impact on the business can include factors such as public embarrassment, delayed payments to suppliers and employees, legal and regulatory issues, and administrative problems, but special focus is typically on lost revenues, customers and investor confidence (especially for publicly traded companies). Consideration must be given not only to individual business systems (e.g., sales and accounts receivable) but also to the infrastructure used to support those systems (e.g., network hardware, firewalls, and connections to business partners and the Internet).

Information Sources

- Business impact analysis
- Business risk assessments
- Business continuity plans prepared in response
- Guidance for conducting analysis and creating recovery plans:
 - CIAC, www.ciac.org
 - CERT, www.cert.org
 - NIST, www.nist.gov
 - ISACA, www.isaca.org

Evaluation and Performance Criteria

- The security policy on risk assessment defines risk limits and risk tolerance with regard to information availability and standards for business impact analysis.
- A formal, written business impact analysis (BIA) exists that identifies critical information and the implications of loss. It includes evidence that business owners are involved in assessing risks and impact.
- A formal, written business continuity plan (BCP) exists, describing steps to be taken in the event of critical information becoming unavailable. It includes evaluation criteria used to declare a disaster, detailed recovery procedures and contact lists. It should be available in hard copy and electronic form, and stored offsite.
- Evidence is available that the BIA and BCP are reviewed and updated on a regular basis and that staff are fully trained.
- Evidence exists of BCP testing, including minutes from project meetings, detailed test plans and postmortem examinations. Scope of tests must cover all aspects of the plan (usually done with multiple tests over a period of time). Evidence exists that findings from tests resulted in plan updates.
- No actual incidents have occurred that caused loss or public embarrassment.

Security Program Initiatives

- Establish a risk management program to ensure critical IT assets are identified, threats and vulnerabilities are evaluated, and appropriate action is taken.
- Perform business impact analysis for all key information systems and supporting infrastructure. Ensure staff members are properly trained in BCP techniques.
- Create business continuity plans that enable recovery of information systems or initiate alternate business procedures within an agreed time frame.
- Perform regular testing of business continuity plans to identify weaknesses and improve response.



What information assets are subject to laws and regulations? What has management instituted to assure compliance with them?

Considerations for Security Managers

Organizations are subject to many laws and regulations based on their jurisdiction, industry, contractual arrangements and legal form (e.g., publicly traded corporation). Many impose strict requirements over the management of information assets, especially the protection of private information such as customer and employee data. A failure to meet these requirements can result in significant penalties, liability and damage to the organization's reputation.

Compliance with the multitude of laws and regulations calls for the application of legal expertise within a formal, ongoing program that identifies all relevant requirements, including privacy limitations, intellectual and property rights, and other legal, regulatory, contractual and insurance requirements. The program must then determine the information security measures needed for compliance and ensure those measures are in effect.

Information Sources

- Privacy acts
- Incorporating acts
- Tax acts
- Telecommunication acts
- Securities regulations
- Significant contracts
- Service level agreements
- Insurance contracts
- Other special-purpose legislation (e.g., relating to health, safety, employment)
- Risk assessment reports
- Security procedures

Evaluation and Performance Criteria

- Appropriate legal expertise exists, either internally or via an outside firm that is contracted for the purpose.
- Appropriate expertise exists for specialized regulations (e.g., workers compensation, employment regulations and industry-specific requirements).
- A compliance officer position exists within the organization, or an individual is accountable for compliance activities.
- Organization policy requires that all significant contracts are subject to legal review.
- Documented evidence exists of research into the laws relating to the business. Examples include meeting agendas and minutes with legal counsel, and detailed reports or opinions describing legal obligations.
- A formal information security process exists that records requirements identified by the previously mentioned processes, and ensures appropriate response via existing information security programs.

Security Program Initiatives

- Establish a legal and regulatory compliance committee consisting of representatives from information security, legal counsel, human resources, corporate compliance, and related legal and regulatory experts.
- Identify and join local special interest groups or forums that address legal and regulatory compliance issues.
- Establish a requirement for legal representation in risk assessments, and ensure that legal and regulatory needs are addressed in security procedures.



Does the information security policy address the concerns of the board and management on information security (tone at the top), cover identified risks, establish an appropriate infrastructure to manage and control the risks, and establish appropriate monitoring and feedback procedures?

Considerations for Security Managers

The information security policy is the focal point for establishing and conveying the organization’s security requirements. It sets the tone for the information security practices within an organization, defining appropriate behavior and setting the stage for the security program.

It must clearly originate from and be approved by senior management, and communicate the importance of information security to the entire organization. A good policy document includes the overall importance of security within the organization, identifies what is being protected, identifies key risks and mechanisms for dealing with those risks and provides for ongoing and regular monitoring and feedback to ensure the policies are enacted and enforced. Regular updates are needed to reflect changing business needs and practices.

Information Sources

- Information security policy
- Security policy statements
- Security standards
- Computer and network hardening documents
- Examples of information security policies from:
 - ISACA
 - NIST
 - ISO
 - SANS
 - CERT
 - BS 7799
 - RFC 2196

Evaluation and Performance Criteria

- A consistently applied policy development framework exists that guides formulation, rollout, understanding and compliance.
- A formal, written information security policy is dated and approved by senior management.
- Policy enforcement is considered and decided upon at the time of policy development.
- An information security policy framework exists that includes standards, procedures, guidelines and rules of use.
- A high percentage of IT-related plans and policies are developed and documented covering IT security mission, vision, goals, values and code of conduct.
- No, or a limited number of, new implementations are delayed by security concerns.
- Clear evidence exists of monitoring and feedback such as security log and incident reports, including defined metrics.

Security Program Initiatives

- Establish ownership for security and continuity with enterprise managers.
- Establish a security function that assists management in the development of policies and assists the enterprise in carrying them out.
- Establish an information security policy and compliance framework.
- Establish security baselines and rigorously monitor compliance. This should include supporting standards, procedures and guidelines.



Has the organization ever had its network security checked by a third party?

Considerations for Security Managers

Computer networks are comprised of numerous infrastructure components (routers, switches, firewalls and servers) connected by shared media for the purpose of exchanging data. Access to the network, including the physical devices and the data sent among them, must be protected through the appropriate protective measures. These include a wide and complex variety of safeguards that are used to form layers of security around the network.

Due to the complexity of the mechanisms involved, it is critical that network defenses be tested regularly, both to ensure they continue to operate and to help detect any potential gaps or weaknesses. To enhance testing effectiveness, add objectivity and expertise, and simulate attacks from outsiders, periodic use of third-party expertise is recommended. (Note that some or all aspects of network services may be outsourced to a third-party provider. While independent external testing is still important, it must be done within the limits of the related service level agreement.)

Information Sources

- Network diagrams
- Host computer security standards
- Network security standards (especially for firewalls)
- Results of internal testing exercises
- Vulnerability reports from third parties

Evaluation and Performance Criteria

- Written results from internal testing exist. Scope of testing covers all critical network resources. Weaknesses are highlighted, and follow-up action is completed.
- Project documentation exists to identify potential third-party testers, and evaluate testing capabilities, expertise and price. Selection process results in an appropriate engagement letter for testing assignment, including defined scope, reporting process and price.
- Written results from third-party testing exist. Weaknesses are fully documented, along with recommended follow-up action.
- Evidence exists of follow-up action taken on a timely basis. Samples of follow-up actions indicate their satisfactory completion.
- Evidence exists of periodic third-party evaluation of security over network architectures, network security standards and procedures.

Security Program Initiatives

- Establish a program of regular internal network security testing, with appropriate follow-up on all recommendations.
- Establish a program of regular third-party network security testing, with appropriate follow-up on all recommendations.
- Define requirements for third-party reports for outsourced network services.



Does the organization provide information security awareness training to all and is security part of staff and management’s appraisals? Does the training appear adequate considering the assessed risks?

Considerations for Security Managers

For information security measures to be effective, all information system users must be aware of their roles and responsibilities. A security awareness program consists of ongoing efforts to ensure all staff members recognize their role, understand the elements of good security and actively participate in protecting the organization’s information resources.

The program should be part of new employee orientation, be included in annual employee reviews and form part of the organization’s culture.

In high-risk environments, the failure to follow required security practices can be particularly damaging. As a result, ensuring adequate security awareness among all parties is particularly important.

Information Sources

- Job descriptions
- Performance appraisal forms
- Information security intranet web site
- Code of conduct for new employees and contractors relating to use of information resources
- HR employee handbook
- Contracts of employment

Evaluation and Performance Criteria

- Evidence exists of a repetitive and assertive awareness program that reaches every employee. It should include regular items in the company newsletter, e-mails, posters, web-based awareness campaigns and regular meetings.
- There are clearly outlined statements of accountability for information security in job descriptions.
- Forms used during annual performance reviews include reference and ratings covering information security tasks.
- There is a measured improvement in employee awareness of system security principles and performance of duties in a secure manner. Examples include decreases in failed access attempts, password failures and help desk password resets.
- A high percentage of IT security plans and policies are communicated to all stakeholders, especially IT staff.

Security Program Initiatives

- Establish an ongoing security awareness program consisting of a repetitive and assertive communications plan that reaches every employee.
- Create a project with human resources to update all job descriptions with security objectives and apply appropriate awards and disciplinary measures.
- Create a project with human resources to include a rating of employee security activities in their annual appraisal process.
- Develop a code of conduct/rules of use/confidentiality agreements for information system use.



Is management confident that security is being adequately addressed in the company?

Considerations for Security Managers

Management's confidence is directly related to its understanding of the issues and the risks. One method for assessing confidence might come from third-party risk assessments and corresponding action plans. Identifying and clearing up a minimum number of gaps in a timely manner are good indicators of a solid security program.

This necessitates having the appropriate security staff with management and technical expertise, along with programs for delivering security principles to senior management and line staff. A security department that reports directly to senior management is a good indicator of senior management's concern. The degree of funding assigned to security and shown within the financial statements that is commensurate with the level of risk to the organization also shows that security is being addressed adequately.

Information Sources

- Third-party risk assessments
- Departmental budgets
- Security awareness programs
- Organizational charts
- Internal audit assessments/reports

Evaluation and Performance Criteria

- Evidence exists that management and staff have a common understanding of security importance, requirements, vulnerabilities and threats, and understand and accept their own security responsibilities. Examples include meeting minutes, security awareness sessions and the budget assigned to security.
- A security department exists within the organization, or for small organizations, an identifiable individual is responsible for security.
- Evidence exists that annual risk assessments are produced and action plan items are accomplished.
- A formal information security program exists that records annual project plans, action lists and regular assessments. Results are published to senior management with clearly defined goals and action plans to mitigate any identified risk.
- A process/liaison exists with internal audit to follow up and resolve reported security weaknesses and issues.

Security Program Initiatives

- Establish a well-defined security department with clearly delineated goals and documented plans to achieve those objectives, reporting directly to senior management.
- Ensure regular meetings with senior management to report progress.





How is the board kept informed of information security issues? When was the last briefing made to the board on security risks and status of security improvements?

Considerations for Security Managers

The board should be kept apprised of information security issues through regular meetings of the appropriate committee members (e.g., audit committee or IT steering committee where these exist). Regular reports from risk assessments and the action plans to mitigate any risks discovered by those assessments should be distilled into a brief summary, highlighting key issues and risks and the plans to address them. Such briefings should occur at least annually or semiannually.

Regular, more frequent reports produced by the head of security are provided to the audit committee (or perhaps an IT or IS steering committee/group), documenting risks and progress in mitigating those risks.

Information Sources

- Board meeting minutes
- Audit committee reports
- Security assessments
- Meeting schedules

Evaluation and Performance Criteria

- Evidence exists of board agendas showing audit committee attendance (where one exists).
- Written board minutes exist indicating the outcome of meetings attended by the audit committee.
- Board minutes' issue/revision dates are within the last year. Evidence exists (agenda items, discussion and comments) indicating that security has been reviewed.
- Reports exist from the head of security to the audit committee with risks assessed and progress outlined for mitigating those risks.

Security Program Initiatives

- Require that the head of security report progress and issues to the audit committee (or, in its absence, to a security steering group composed of senior management).
- Require that the audit committee report security issues to the board on at least an annual basis or that the board receives a report annually on security progress.



When was the last risk assessment made on the criticality of information security assets? When is the next risk assessment scheduled?

Considerations for Security Managers

Risk assessments are an integral part of business practices and should be performed on a regular basis, such as annually. Identifying how often these assessments are needed requires knowledge of the business and the overall risks associated with that business.

Evidence of corporate change (such as mergers or acquisitions) should trigger new assessments. In their absence, assessments should be conducted within predetermined time frames.

Information Sources

- Meeting minutes and agendas
- IT security group planning documents
- Institute of Risk Management
- Octave, www.cert.com/octave
- NIST, <http://csrc.nist.gov/publications/nistpubs>

Evaluation and Performance Criteria

- Evidence exists of a documented risk assessment program undertaken within the current year.
- Risk assessments follow a formal structure using processes such as Octave or NIST 800-30.
- Scheduling exists for the next assessment and is included in management meetings or meeting agendas.
- A risk management standard exists that clearly outlines responsibilities, objectives, level of support and degree of documentation.
- Clearly defined roles and responsibilities exist for risk management ownership and management accountability.

Security Program Initiatives

- Create and schedule a comprehensive risk assessment program.
- Perform risk assessments for new information systems/new infrastructure components.



Is IT security risk assessment a regular agenda item at IT management meetings and does management follow through with improvement initiatives?

Considerations for Security Managers

Regular IT risk assessments help ensure the overall security posture of an organization. IT management involvement ensures that the assessments have a high profile and get accomplished on a regular schedule with clear action plans for correcting any deficiencies.

IT management is then seen to be proactive in supporting the completion of action plans, thus ensuring steadily improving results over time.

Information Sources

- IT management meeting agendas
- Meeting minutes
- Risk assessments
- Detailed action plans
- Security assessments
- Department budgets

Evaluation and Performance Criteria

- Clearly defined roles and responsibilities exist for risk management ownership and management accountability.
- Clearly defined responsibilities and procedures exist for defining, agreeing on and funding risk management improvements.
- Evidence exists of IT management meetings discussing security risk assessment results and initiatives for improvement.
- Evidence exists of action plans with clearly defined timelines and current results.
- Security department budgets exist that clearly show ability to procure software, hardware or other items needed to implement action items.
- The risk assessment process is included in system development life cycle (SDLC) projects.
- The risk assessment process is included in the change management process.

Security Program Initiatives

- Add a risk assessment program as an agenda item in regular IT management meetings.
- Ensure scheduled IT meetings include the head of security.





What are other people doing, and how is the enterprise placed in relation to them? What is industry best practice and how does the enterprise compare?

Considerations for Security Managers

Understanding the organization’s particular industry and its needs is critical to maintaining a level of security and control that is reasonable. Adhering to best practices shows that the security team and management have learned from the mistakes of others. Best practices are often arrived at by hard experience, helping the organization avoid those same mistakes.

Following the best practices does not immunize the organization from problems, but does help insulate and reduce the risks. Security assessments based on best practices are a useful tool to help ensure the appropriate degree of control exists and offers a way to judge the organization’s place within a similar community.

Information Sources

- Third-party security professionals
- Third-party assessments
- Internal security assessments
- Industry resources, trade groups
- Vendor best practices

Evaluation and Performance Criteria

- Evidence exists that security staff understand the industry and implement improvements related to those specific needs. This includes best practices obtained from independent sources.
- A reality check of the security strategy is conducted by a third party to increase objectivity and is repeated at appropriate times.
- Evidence exists that security staff belong to and attend events by organized security groups and associations, such as ISACA, ISSA and vendor events/sessions.
- Security assessments take account of industry best practices.
- Security staff have membership and participation in industry-specific security groups and also attend regular meetings with peers in their specific industry area.
- Consultation is held with external/internal audit regarding current best practices.

Security Program Initiatives

- Establish a program to analyze industry best practices and implement security according to those practices.
- Perform risk assessments based on acceptable industry best practices and compare results. Create action plans to close any gaps and monitor for completion.
- Establish requirements for security qualifications (e.g., CISM, CISSP) and continuing professional education requirements.





When was the last performance review of the person responsible for information security (i.e., the information security officer)? Is the process to keep management informed on security issues by the information security officer adequate?

Considerations for Security Managers

As for any employee, it is important for the information security officer to have a clear understanding of the expectations for his/her performance and to receive timely (at least annual) evaluations of that performance and feedback on ways to improve.

It is also important that open lines of communication exist so that the information security officer can keep senior management informed on a timely basis for ongoing and emerging security issues.

Information Sources

- IS officer job descriptions
- IS officer job performance appraisals
- Related memos, e-mails and meeting minutes
- Audit reports of the security function

Evaluation and Performance Criteria

- A formal, written job description for the information security officer function clearly describes responsibilities, duties and performance criteria.
- A written performance appraisal for the information security officer was completed within the last year. It includes ranking based on evaluation criteria from the job description, as well as specific goals and recommendations for future performance.
- Evidence exists of regular briefings by the information security officer to senior management (e-mails, memos, minutes from meetings) along with demonstrated follow-up where necessary. For urgent security issues (e.g., large-scale vulnerability discovered, successful system penetration), notification and initial follow-up action is taken within 48 hours.

Security Program Initiatives

- In cooperation with human resources (HR), initiate a complete job description and job performance appraisal mechanism for the information security officer position (or incorporate it into existing HR programs).
- Institute a regular communications mechanism from the information security officer to senior management (including head of internal audit) for ongoing security issues.
- Institute an emergency communications mechanism for urgent security issues.



What safeguards have been established over systems connected to the Internet to protect the entity from virus and other attacks? Are the systems being actively monitored and is management kept informed of the results?

Considerations for Security Managers

Information systems connected to the Internet have the ability to exchange data with millions of similarly connected computers throughout the world. This ability invites attempts from malicious Internet users to harm the organization’s information systems with viruses or other programs. Internet connectivity also facilitates attacks where malicious users attempt to identify and exploit security weaknesses that may exist within the organization’s information systems.

To prevent harm to the systems, Internet-connected systems require strict safeguards that are kept up to date to protect against the latest viruses and other types of attacks. In addition, the systems must be monitored to ensure that attacks are not successful, as well as to alert the organization of new or increased attack levels.

Information Sources

- Network documentation
- Internal security reviews
- Internal security testing
- Logging and monitoring reports
- Intrusion detection system (IDS)/ intrusion prevention system (IPS) reports
- CERT
- Vendor security updates (e.g., Microsoft, Sun, Cisco)

Evaluation and Performance Criteria

- Documentation exists showing that all Internet-connected infrastructure components are identified and have appropriate security architecture and design such as IDS and hardened servers.
- Security assessments have been conducted for each, with weaknesses identified and formally reported. Remedial action has been taken, with documented test results showing that weaknesses are eliminated.
- A change management process is in place to find newly identified security weaknesses for all infrastructure components. It includes security alerts issued by vendors and third parties. The change process includes appropriate testing and rollout procedures.
- An antivirus management process is in place to update antivirus software and virus signatures.
- A regular program of vulnerability and penetration testing exists, evidenced by documented test results.
- Evidence exists of log results collected, analyzed and acted on from all Internet-connected infrastructure components.
- Intrusion detection and intrusion prevention tools are deployed and actively monitored, with evidence of alerts being recorded and actions being taken. A spam/e-mail/spyware management process in place.

Security Program Initiatives

- Identify and harden all Internet-connected infrastructure components, including follow-up testing.
- Establish a coordinated logging, monitoring and follow-up program for Internet-connected systems.
- Establish a program to monitor security alerts from sources such as software vendors and CERT, disseminate them within the organization and ensure follow-up.
- Install and monitor intrusion detection and intrusion prevention systems.



What safeguards have been established for the physical security over computer assets and do they appear adequate?

Considerations for Security Managers

Information system hardware and software typically represent significant expenditures by the organization. The data stored within these systems are similarly valuable. Both must be protected against theft, damage, destruction and other types of unauthorized access that may impair the value of these assets.

Physical security consists of traditional measures such as perimeter fences, locks, guards, alarms and surveillance systems designed to prevent or detect unauthorized access. It also includes facilities such as fire suppressant systems and backup generators that help reduce the damage that can occur. The physical security measures taken must be appropriate, adequate and relative to the value of the assets being protected.

Information Sources

- Security assessments conducted internally or by third parties
- Security incident and follow-up reporting by the organization's private security force

Evaluation and Performance Criteria

- Physical security and environment control assessments have been conducted for all key information assets, with weaknesses identified and formally reported. Remedial action has been taken, with documented review or test results showing that weaknesses are eliminated.
- A tour of all main information processing facilities shows that physical security measures are in place and not being bypassed (e.g., doors left open, more than one person at a time passing through a secured door, or alarms disabled or bypassed).
- A private security force (or equivalent) exists. Patrols cover all key information assets. Suspicious activity is reported and follow-up occurs. There is formal reporting of security breaches, including liaison with law enforcement officials.
- There is a demonstrated decrease in information-system-related losses or incidents, or at least containment at acceptable levels.

Security Program Initiatives

- Establish an ongoing program of physical security reviews.
- Establish the organization's private security force.





When was the last time an information security audit was performed? Does management track its own progress on recommendations?

Considerations for Security Managers

The complete program of information security policy, mechanisms and procedures must be tested to ensure their ongoing effectiveness. In addition to ongoing security assessments carried out by information security staff, there should be a program of regular security audits performed by appropriately knowledgeable audit staff, covering all information assets and security issues.

Once the audit is complete, project management techniques should be employed to track the findings and recommendations, and ensure timely follow-up action.

Information Sources

- Formal reports from security audit
- Project management documentation covering follow-up on audit findings and recommendations

Evaluation and Performance Criteria

- Formal, written reports exist on security audits. Reports should include detailed information on audit scope, findings and recommendations. Collectively, scopes of audits must cover all critical information security program components.
- There is formal response to audit findings documenting the disposition of each finding and recommendation. Where a finding is accepted, reference is made to projects struck to address the security weakness. Where the finding is disputed, there is evidence of comprehensive research and testing to ensure no weakness exists.
- Project management documentation covers follow-up activities that address identified security weaknesses.
- There is full compliance, or agreed-upon and recorded deviations from minimum security requirements.

Security Program Initiatives

- Ensure that a program of regular security audits exists, conducted by adequately trained audit staff, and the combined scope of audits covers all critical security areas at least every 12 months.
- Establish projects to ensure timely follow-up of all audit findings.
- Ensure that an audit is conducted periodically covering the security program itself and the way in which it is managed.



Is there a security program in place that covers all of the previous questions? Is there clear accountability about who carries it out?

Considerations for Security Managers

A formal, well-planned and completely executed information security program is required to ensure the organization’s information assets are adequately protected. Without such a program, important security practices may be overlooked, resulting in unacceptable risks to the organization.

Responsibility for all aspects of the information security program must be clearly defined and communicated to all staff.

Information Sources

- Information security policies, standards and procedures
- Job descriptions
- Organization charts

Evaluation and Performance Criteria

- Formal plans cover all major security projects for the security program including resource requirements and timescales for implementation.
- Formal, written security policies, standards and procedures cover all aspects of the information security program.
- Clearly outlined statements of accountability exist for information security in job descriptions.
- The organization chart shows that the corporate security function reports to senior management and is responsible for executing the security program. The group charter and reporting relationship ensures proper authority, executive support and mitigation of any potential conflicts of interest.

Security Program Initiatives

- Institute an information security program that covers the contents of this publication.

