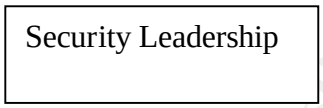
Global Information Assurance Certification Paper

Lynn Gaw
Security Essentials (GSEC) v1.4b

Designing the Security Program for Your Organization: A Top Down Approach

Introduction

A layered approach of the security program should address both technical and non-technical approaches[1]. This paper will outline a series of considerations that address a number of control objectives "governance" that need to be included in the design of an effective security program. In many cases the establishment of an Information Security focus is as a result of a major security incident, an upcoming audit, and/or poor audit results. This can result in a reactionary focus that fixes the immediate issues but does not build a long term strategy and may not apply the fixes consistently across the infrastructure. Without the ongoing strategy and the supporting program the measures taken will be short lived. The implementation of security begins with the board and/or the executive in the organization and steps through a number of process areas that define the ongoing strategy for information security, the roles throughout the organization, the policies, procedures, standards and guidelines framework, the user and security program management, monitoring, the technology controls, and other supporting mechanisms that need to be in place in order to be successful on an ongoing basis. A number of resources from the Internet, books, magazines, your organization, and other organizations will help in defining how to make this Security program flow work for your organization.



In order to be effective information security requires an executive/board level focus. The program needs to be driven by business needs and be aligned with the corporate strategies so that it is seen as an enabler of controls rather than a hindrance to the business processes. The goal of information security should be to enable the business meet in achieving it's objectives while reducing the risks to the organization.

The COBIT framework, which provides control objectives for IT includes a section, DS5 "Ensure Systems Security", that covers many of the areas outlined in this paper. Other sections of the COBIT framework also apply equally to Information Security as they do to Information Technology, Application Development and other areas of the Information Systems organization. The planning & organization P04 Objective to Define the Information Technology Organization and Relationships indicates that the following items should be taken into consideration:

[1] Information Security Governance: Guidance for Boards of Directors and Executive Management, www.itgi.org/infosecurity.pdf, IT Governance Institute, (Sep 10, 2002)

- Board level responsibility for IT
- Management's direction and supervision of IT
- IT's alignment with the business
- IT's involvement in key decision processes
- Organizational flexibility
- Clear roles and responsibilities
- Balance between supervision and empowerment
- Job descriptions
- Staffing levels and key personnel
- Organizational positioning of security, quality and internal control functions
- Segregation of duties[2]

Further process steps in the methodology will be linked to alignment with the business, risk assessment, and to involvement in key decision processes, continuous improvement, the ongoing assessment of the security needs and the ability of the current program to address them.

The security organization may fall under IT or may be independent of IT and report directly to senior executives in either case executive support is necessary to ensure that Information Security is applied consistently across the organization. If Information Security reports to IT a process will need to be defined for dealing directly with the executive under certain circumstances. Information Security needs to have a the business as their number one priority and needs to ensure the security of assets based on requirements set by the business, they are the conscience of IT and this may occasionally be in conflict with the plans or actions of the IT department, it is important that there is a mechanism for promoting awareness of these issues and their associated risk to IT management and ultimately to the executive.

Management input is required in order to define what is important to the organization and to define the amount of residual risk the organization is willing to accept. This will drive the creation of the security policy. Management support is also needed in order to define and gain support for the roles throughout the organization that will be needed to support Information Security, such as business owners, stewards, trainers, auditors, Human Resources personnel, Legal and users. Management will also provide an important link for the dissemination of the awareness program.

In a look at the best practices of 8 organizations establishing a central management focal point was highlighted as one of the key practices. These organizations designated a central group to be responsible for Information Security, they provided the group with ready and independent access to senior executives, they designated staff and funding to Information Security and they ensured that staff had, and continued to enhance, professional and technical skills[3].

[2] COBIT 3rd Edition Control Objectives, http://www.isaca.org/control.pdf; IT Governance Institute, (Sep 10, 2002)
[3] Information Security Management Learning from Leading Organizations, www.gao.gov/special.pubs/pdf_sing.pdf, United States General Accounting Office, (Sep 23, 2002)

In defining this central focus you will need to determine if a centralized, decentralized or federated model works best for your organization. The organizational culture may fit one model more appropriately than another. Each model has its strengths and weaknesses, awareness of how each model works will help define the best fit for your organization and will also help you build processes that can reduce the risks of the weaknesses in that approach.

Centralized: Centralized organizations have a strong corporate culture, top-down management, and a single IT service provider.[4] The centralized group is responsible for policy, program, implementation, and monitoring. This approach can ensure that your program is established across the organization but may result in a single point of view that can cause issues in design and implementation of security measures.

Decentralized : Decentralized organizations have power spread out to individual divisions or units, which act independently.[5] Each department / division / business unit designs, implements and monitors their own security program. This approach means that each area gets the focus that it needs and has staff with the detailed skills necessary for the assets under their control but may result in inconsistent application of security programs across the organization.

Federated: Federated organizations are a hybrid of decentralized and centralized organizations.[6] A centralized group creates the policy and defines the strategy, individual departments/divisions/business units implement the strategies, and provide a feedback loop to the centralized group. Each area gets the focus and expertise it needs, the centralized group ensures consistency and can also review issues for indications of systemic problems. This approach will rely heavily on relationships and processes established between the various business areas.

Once the best fit from the above organizational breakdowns has been determined and the executive sponsorship has been established you can begin to build the roles and responsibilities. The role of the executive will be defined as part of the Leadership process, other roles and responsibilities across the organization will need to be defined as part of the Security Program. Each of these roles will result in processes and procedures that will need to be defined in the policy, procedure, standards and guidelines framework.

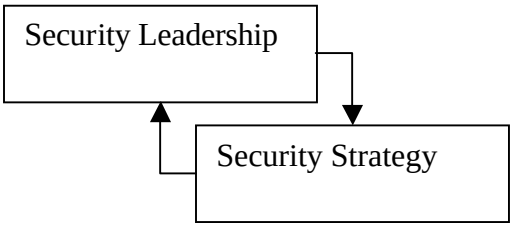
The role of the executive may be as follows:

> Approve strategy / program / overall policy making sure that it is aligned with business initiatives
>
> Give direction as to the risk tolerance of the organization.

---

[4] Improve Software Management, http://www.window.state.tx.us/tpr/tpr5/3cg/cg07.html, Carole Keeton Rylander Windows on State Government, (Sep 23, 2002)
[5] Improve Software Management, http://www.window.state.tx.us/tpr/tpr5/3cg/cg07.html, Carole Keeton Rylander Windows on State Government, (Sep 23, 2002)
[6] Improve Software Management, http://www.window.state.tx.us/tpr/tpr5/3cg/cg07.html, Carole Keeton Rylander Windows on State Government, (Sep 23, 2002)

Determine what an acceptable residual risk level is should an initiative not comply with the governing policy, procedures, standards and guidelines.



The security strategy is the overall vision and initiatives to affect improvement and change within the enterprise security architecture.

The security strategy for an organization should be aligned with the IT and business mission, vision, and strategies. The security strategy should outline a 3 to 5 year plan and review should be performed on an annual basis to determine if the strategy still supports the IT and business initiatives required that support the organization. Planning is an important part of management for any business area and is equally important for Information Security.

In the initial setup of the department and program the strategy will be easier to create if it falls later in the steps. First the governing security policy will need to be defined, the processes required in order to support the policy and the organization will need to be determined, an understanding of the value of the assets to the organization will be required, and definition of a risk assessment process for reviewing the assets of greatest value will need to be created. Once this information is gathered you can determine the issues and the priorities for the initial strategy. A good starting point in the information gathering process can be to complete a survey of management throughout the organization.

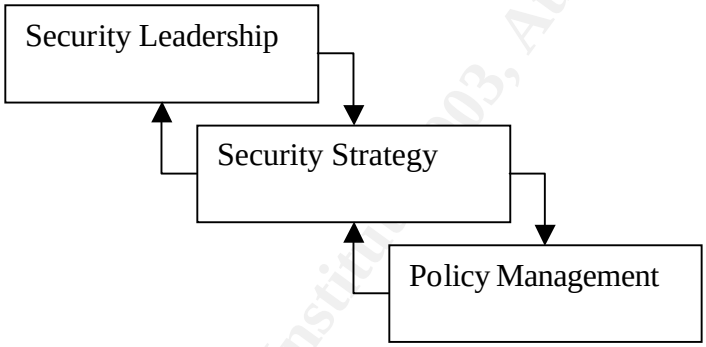
The following questions can provide valuable information in establishing the first strategy and may also be useful on an ongoing basis to ensure that the strategy is still linked to business requirements.

What is your organizational culture?
What are the most important business processes and how are they supported by Information Technology resources?
What changes are expected in the coming year(s) in business processes and the support of Information Technology resources?
For the major business processes, how is the information classified (Confidentiality, Integrity, Availability) – importance & order?
What control objectives need to be supported by the security program (segregation of duties, etc.)?
How should security be governed/managed for the organization?
What is the role of the sponsor for Information Security?
What are the expected achievements of the strategy for the organization?
What do they see as their role and responsibilities in regards to Information Security?

What should the governing security policy be for the organization?
Is the governing security policy still valid for the organization?
What should the security policies achieve?
What awareness, training, level of understanding do personnel need, of their roles and responsibilities, in regard to Information Security?
What are the issues or areas for improvement in Information Security?
What expectations do they have in regards to Information Security?

Ongoing risk assessments, monitoring and reporting processes and the building of information security into existing processes, will provide the feedback for maintaining the strategy year on year.

Each of the remaining sections of the methodology will link back to the strategy. Technology solutions (IDS, Firewalls, Virus protection, etc), user management (access controls, authentication methods, etc), monitoring (audit tools, reporting tools, etc) as well as other areas will drive the need for projects/solutions that will become part of the strategy based on the business need and the priorities. Having this continuous link between the business needs, the implementations, the risk assessment process and the strategy will provide the information necessary to gain support for the projects and the budget associated with them.



The cornerstone of an effective information security program is a well written policy statement. A policy is a high-level statement of enterprise beliefs, goals, and objectives and the general means for their attainment for a specified subject area[7]. The policy should be built on a security objective and a framework of core principles. The overall policy will drive the creation of issue or system specific policies that will then result in the creation of procedures, standards and guidelines.

The creation of an effective security policy is highlighted in a number of resources as critical to the success of the security program. The overall policy may be supported by a number of issue or system specific policies that will differ dependant on the organization.

Some common policies include:

[7] Thomas R. Peltier; Information Security Policies, Procedures, and Standards, Auerbach Publications, p21

Appropriate use of computer resources
Use of Internet
Use of E-mail
Phone usage

The policies will drive the creation of procedures, standards and guidelines. Policy should not change very often (3-5 year) and should be approved by the executive.

A policy should include, as a minimum, a topic portion that defines the goals of the policy, identification of the major responsibilities of management, employees and the administrator of the policy, the scope defines how narrow or broad the application of the policy is, and responsibility for ensuring compliance as well as the actions taken as a result of non-compliance. The study of best practices highlights the need to link the policies to business risks, and to support the policies through a central security group. [8]

Procedures define the step by step instructions of how a policy will be implemented. Procedures will change more often than policy. Procedures may contain any of the following items:
Title – brief but descriptive
Intent – what is the procedure trying to accomplish
Scope – what exactly is the scope of the procedure
Responsibilities – identify, by job function, who will carry out the steps
Sequence of events – information on timing or conditions for performing the tasks
Approvals – identify the who must approve the procedure before it can be placed into production
Prerequisites – what conditions must be in place prior to executing the procedure
Definitions – dependant on the audience you may need to provide definitions of any acronyms used in the procedure
Equipment required – list any equipment, tools, supplies, documentation, media, forms, special ID's or passwords that will be needed in order to complete the procedure
Warnings – identify any tasks that if executed out of sequence or not completed successfully will result in damage to the system or other resources in the infrastructure
Precautions – will identify steps to be taken to avoid problems, such as unplug prior to beginning work or disconnect from network prior to installation, etc.
Procedure – the actual steps to be taken
Version information – current version number, author, date, supercedes information
Document number – tracking number for the document

The procedure may include flowcharts, screen captures, photographs or other supporting information that make them easier to follow.

Standards define the mandatory activities, actions, settings, rules or regulations (what) that give the policies the specific direction needed in order for them to be applicable, meaningful and effective. Standards will change frequently, possibly with every new patch to software or with every new version of hardware. In order to remain effective

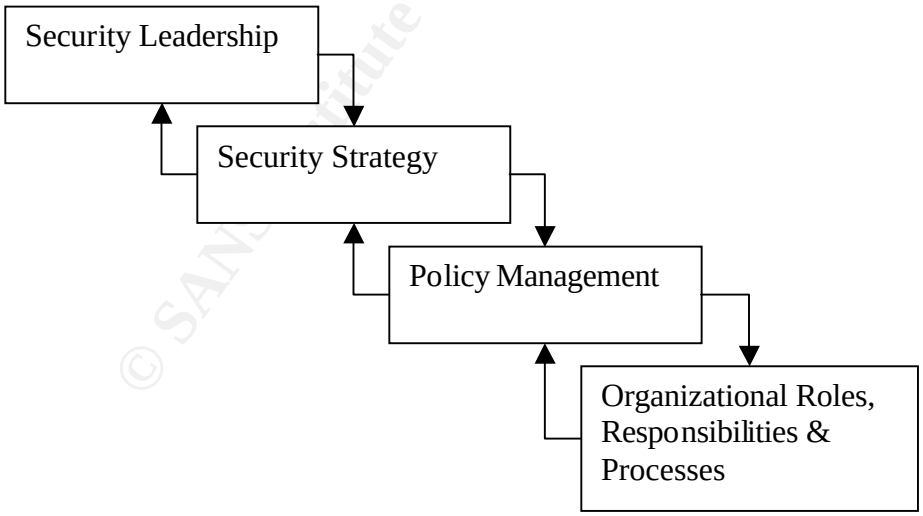
[8] Information Security Management Learning from Leading Organizations, www.gao.gov/special.pubs/pdf_sing.pdf, United States General Accounting Office, (Sep 23, 2002)

they must be practical, understandable, applicable, current and reviewed on a regular basis.

Guidelines are recommendations and therefore are not mandatory. They provide additional information, a framework, possibly above the requirements outlined in the standards, for securing specific IT components.

In order to be successful you will want to align your security policies, procedures, standards and guidelines with others that already exist in your organization. Examine processes (incident management, change management, application development, project management, etc.) and documentation (support desk knowledge base, software installation instructions, etc.) to determine how to fit the security requirements into existing documentation. A procedure for installation of a new W2K server can be expanded to include the steps required to secure the server (the standard can be expanded to include any specific settings that should be applied), it may also link to a checklist that is used during the installation and can provide information for update/maintenance of the disaster recovery plan. It is also good practice to ensure the update of standards and procedures as part of the change management process. If it is built into existing procedures it is more likely to be used, followed, maintained and consistent.

An effective policy, procedure, standards and guidelines framework will also link to the User Management, Security Administration and Asset Management levels of the framework to be detailed later in this paper. Linking policies to business risks also helps to make the need for them better understood and the need for compliance with them easier to communicate.



Information security is the responsibility of everyone who can affect the security of an IT system. Each division / department may have specific roles and responsibilities in the establishment and ongoing success of the security program. The organizational roles, responsibilities and processes throughout the organization in relation to security, not just of those within the security group, need to be defined. This also includes the areas required to ensure the effective implementation of security directives. Once the roles

and responsibilities have been defined processes and procedures will need to be created to provide support.

The key players of security within the organization are:

Executive committee / Senior management

- Comprised of executive-level management who are the approval authority for all security relating to the protection of enterprise processes, systems and electronic information assets.
- The project sponsor for the information security architecture, however, ultimate responsibility lays with the most senior executive i.e. the CEO.
- Approve and champion all security awareness programs.
- Ensure business processes can be appropriately recovered (Technology protection & Continuity: Business Continuity Plan)
- Set a good example by following all applicable Information security practices.

Security Committee

- Depending on the organizational culture and the centralized / decentralized / federated approach it may be necessary to establish a security committee. The purpose of this committee should be to identify and monitor the risks the organization is facing in regards to information.
- This committee should include physical security, audit, and IT security-related risks as they impact the information and processes. Depending on the industry this may also include Privacy, Legal, Product safety, project management office, etc. The committee should include all the necessary representation without becoming too large and hindering decision making processes.

Legal

- Ensure compliance with regulatory and good business practices.

Procurement

- Prior to purchasing any software or equipment, there should be a completed approval stating that the goods and services meet security expectations. This office should be knowledgeable about security policies and procedures and should bring them to the attention of those submitting procurement requests.

CFO

- Ensuring the flow of financial information across the organization has integrity to enable accurate financial reporting.

Personnel

- The personnel or human resources office is normally the first point of contact in helping managers determine if a security background investigation is necessary for a particular position. The personnel and security offices normally work closely on issues involving background

investigations. The personnel office may also be responsible for providing security-related exit procedures when employees leave an organization.[9]

Physical Security

- The physical security office is usually responsible for developing and enforcing appropriate physical security safeguards, in consultation with IT security management, program and functional managers, and others, as appropriate. Physical security should address not only central IT installations, but also backup facilities and office environments.[10]

Physical Plant

- This office is responsible for ensuring the provision of such services as electrical power and environmental safeguards, that are necessary for the safe and secure operation of an organization's IT systems. Often they are augmented by separate medical, fire, hazardous waste, or life safety personnel.[11]

Training Office

- An organization has to decide whether the primary responsibility for training users, operators, and managers in IT security rests with the training office or the IT security program office. In either case, the two organizations should work together to develop an effective training program.[12]

Audit

- Auditors are responsible for examining IT systems to see whether the system is meeting stated IT security requirements, including system and organization policies, and whether IT security safeguards are appropriate. Informal audits can be performed by those operating the IT system under review or, if impartiality is important, by outside auditors.[13]

Director of IS / CIO

- Ensuring that the IT strategy is aligned with the business objectives and strategy.
- Responsible for ensuring that technology deployed adequately meets the security guidelines and standards defined by the organization.

System, Network and Application Administrators

- Responsible for the development, administration and maintenance of networks.
- Participate in the development of system security standards and guidelines, as appropriate.
- Ensure systems comply with standards and guidelines

Communications / Telecommunications Staff

[9] http://www.cse-cst.gc.ca/en/documents/knowledge_centre/publications/manuals/mg9e.pdf
[10] http://www.cse-cst.gc.ca/en/documents/knowledge_centre/publications/manuals/mg9e.pdf
[11] http://www.cse-cst.gc.ca/en/documents/knowledge_centre/publications/manuals/mg9e.pdf
[12] http://www.cse-cst.gc.ca/en/documents/knowledge_centre/publications/manuals/mg9e.pdf
[13] http://www.cse-cst.gc.ca/en/documents/knowledge_centre/publications/manuals/mg9e.pdf

- This office is normally responsible for providing communications services, including voice, data, video and facsimile service. Their responsibilities for communication systems are similar to those of the network management.[14]

Help Desk

- The help desk may or may not be tasked with incident handling (this will depend on skills requirements and the confidentiality needs of the organization). The help desk, whether responsible or not, needs to be able to recognize security incidents and refer the caller to the appropriate person or department/division/organization for a response.[15]

Information Security Management

- Overall responsibility for information security matters, including co-ordination of issues/initiatives at the executive level.
- Ensuring that there are adequate resources and appropriate skill-sets to support the security program to achieve the security strategy across the organization
- Responsible for developing the security strategy and policies as well as ensuring they are enabled across the organization.
- Ensure systems can be appropriately recovered in the event of a disaster

Security Team

- Centralized team of personnel responsible for setting the guidelines and standards and supporting the implementation of security across the organization.
- Responsible for performing security awareness initiatives.
- Responsible for emergency response initiatives.

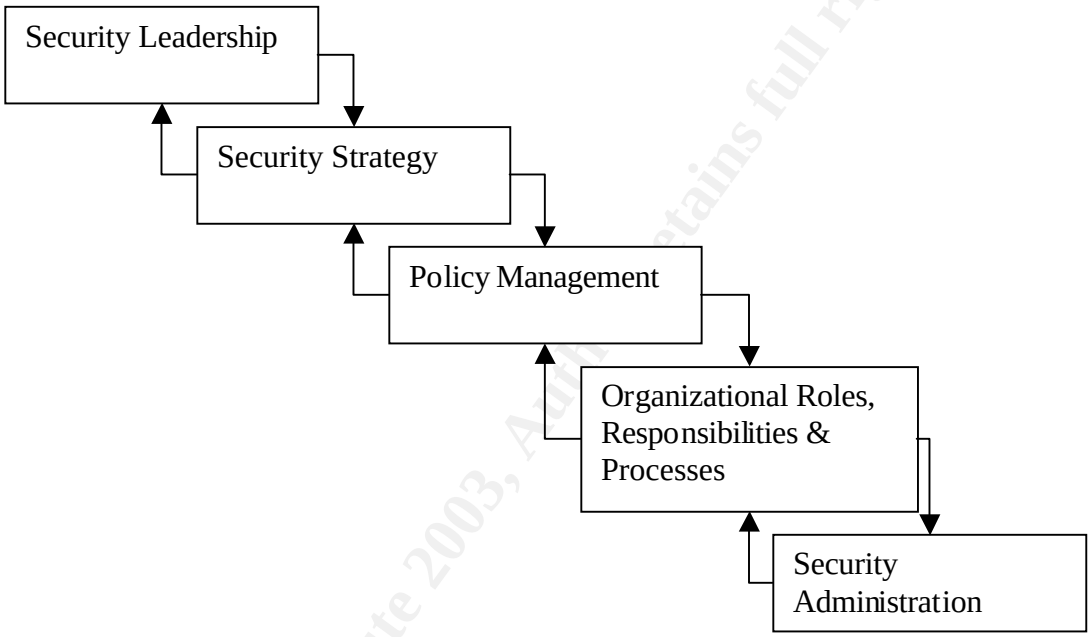
Application Owners/Stewards

- Each application / IT asset should be assigned an application/asset owner. The application/asset owner may decide to appoint a steward to carry out their role.
- Responsible for assigning data classification to the application/asset
- Reviews access lists and approves new access
- Approves changes to the application/asset (change management process)
- Represents the business perspective in risk management analysis

Establishing application/asset owners/stewards addresses COBIT DS5.8 – Data Classification that requires that management should implement procedures to ensure that all data are classified in terms of sensitivity by a formal and explicit decision by the data owner according to the data classification scheme.[16] The classification of data also drives the needs in the security of IT Assets.

[14] http://www.cse-cst.gc.ca/en/documents/knowledge_centre/publications/manuals/mg9e.pdf
[15] http://www.cse-cst.gc.ca/en/documents/knowledge_centre/publications/manuals/mg9e.pdf
[16] COBIT 3rd Edition Control Objectives, http://www.isaca.org/control.pdf; IT Governance Institute, (Sep 10, 2002)

Processes and procedures will need to be identified, created or updated, and monitored for the organizational roles and responsibilities. For example, an approval process would need to be created in order to supply the necessary security approvals to procurement before the purchase of systems. There may be multiple processes required to support the relationship with Personnel, for example, a process for requesting background checks for those positions where it is deemed necessary, or a notification procedure for new hires / changes or terminations of employees. The requirements for processes and procedures will vary dependant of the roles and responsibilities identified in the organization but the ongoing success of the security program will be dependant on their existence (whether formal or informal).



Security Administration addresses the processes, procedures and responsibilities for management and administration of the security architecture.

Security Administration can be broken down into the following three areas:

Risk Management is the ongoing process of evaluating risks to the IT resources of the organization. The assessment process includes the analysis, mitigation of risks to an acceptable level and ongoing maintenance/monitoring of the risks to IT resources. This would include research activities and ongoing monitoring/subscription to various resources for information on changes in risk. It should be well understood that the balance between acceptable and unacceptable risk is a management decision. The risk assessment process may or may not reside with Information Security in your organization, if it is not a function of Information Security it is important that Information Security be an integral part of the process.

There are many sources of information on risk assessment:

http://www.cse-cst.gc.ca/en/documents/knowledge_centre/publications/manuals/mg9e.pdf

http://www.cert.org/archive/pdf/01tr016.pdf

http://www.cse-cst.gc.ca/en/documents/knowledge_centre/publications/manuals/mg3e.pdf

http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

http://www.gao.gov/special.pubs/ai00033.pdf

Review the various methods available and pick the method that best fits your organization and the level of detail it may require. Risk assessment can be seen as a detailed and difficult process for the business but it is extremely important that they are involved in the process. Risk analysis should be performed from both a business and a technology perspective. Approval of the action plans and the residual risk for both business and technology must be owned by the business, ultimately by the most senior executives. Research the training opportunities available as you design and implement the risk assessment process for the organization.

Ongoing monitoring of risks would also include tracking of bugs, hot fixes and patches for the systems in the organization. The monitoring based on risk would identify when a patch should be applied, it should then fall into change management processes established in the organization and become part of the ongoing security operations that need to be in place. The change management and project management processes also need to be linked to the risk assessment process. Before a change to the infrastructure is implemented it should be determined if there are impacts on the security of the assets in the infrastructure.

COBIT DS5.1 Manage Security Measures includes many objectives:

- Translating risk assessment information to the IT security plans
- Implementing the IT security plans
- Updating the IT security plan to reflect changes in the IT configuration
- Assessing the impact of change requests on IT security
- Monitoring the implementation of the IT security plan
- Aligning IT security procedures to other policies and procedures[17]

Ongoing monitoring or risk also addresses BOBIT DS5.12 – Reaccreditation where management should ensure that reaccreditation of security is periodically performed to keep up-to-date the formally approved security level and the acceptance of the residual risk.[18]

The risk management process is also effective tool in supporting your awareness programs.

Security Metrics and Operations would include the ongoing metrics needed to support the security organization. The metrics will vary based on the needs of the organization by may include # of reported incidents, # of viruses detected, # of incidents detected by

[17] COBIT 3rd Edition Control Objectives, http://www.isaca.org/control.pdf; IT Governance Institute, (Sep 10, 2002)
[18] COBIT 3rd Edition Control Objectives, http://www.isaca.org/control.pdf; IT Governance Institute, (Sep 10, 2002)

the IDS, etc. Included in this area would be the ongoing tasks associated with maintaining the effectiveness of the security program. This could include the regular review of documentation, review of the change management processes in place, assessments/audits of IT resources including reporting of results, determining responses and monitoring the progress in mitigating audit points. Operations would also include the patch testing and implementation for the resources in place.

Operations would also include the processes that need to be established in order to support COBIT DS5.9 – Central Identification and Access Rights Management where controls are in place to ensure that the identification and access rights of users as well as the identify of system and data ownership are established and managed in a unique and central manner to obtain consistency and efficiency of global access control.[19] This links to the policy management section in the setting of user authentication policy, procedure and standards, as well as to the organization and the role of owners/stewards. As part of the operations process regular reports will be run listing user access, managing the review process and taking the individual owner reports and review for systemic (too much access across too many systems). Audit of the process would also be part of the operations of the security program.

Security Monitoring is the processes surrounding the monitoring and incident response efforts to ensure continuous compliance to security requirements. This would include audit log monitoring, firewall monitoring, IDS report review and monitoring, incident response procedures and reporting requirements, as well as other monitoring requirements as determined by the security program requirements. Incident response will require the establishment of both an incident response team (may include physical security, audit, human resources, etc.) and the procedures that need to be in place in the event of an incident. It is critical that procedures are followed in order to gather the necessary information (chain of control) while working to get the organization back up and running as quickly as possible with the minimal amount of damage to the infrastructure.

Some resources that are useful in designing the incident response team and procedures are:

http://www.sei.cmu.edu/pub/documents/98.reports/pdf/98hb001.pdf

http://www.cio.com/research/security/incident_response.pdf

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/windows/windows2000/staysecure/secopsj4.asp

http://www.macromedia.com/v1/DocumentCenter/Partners/ASZ_ASWPS_Incident_Response.pdf

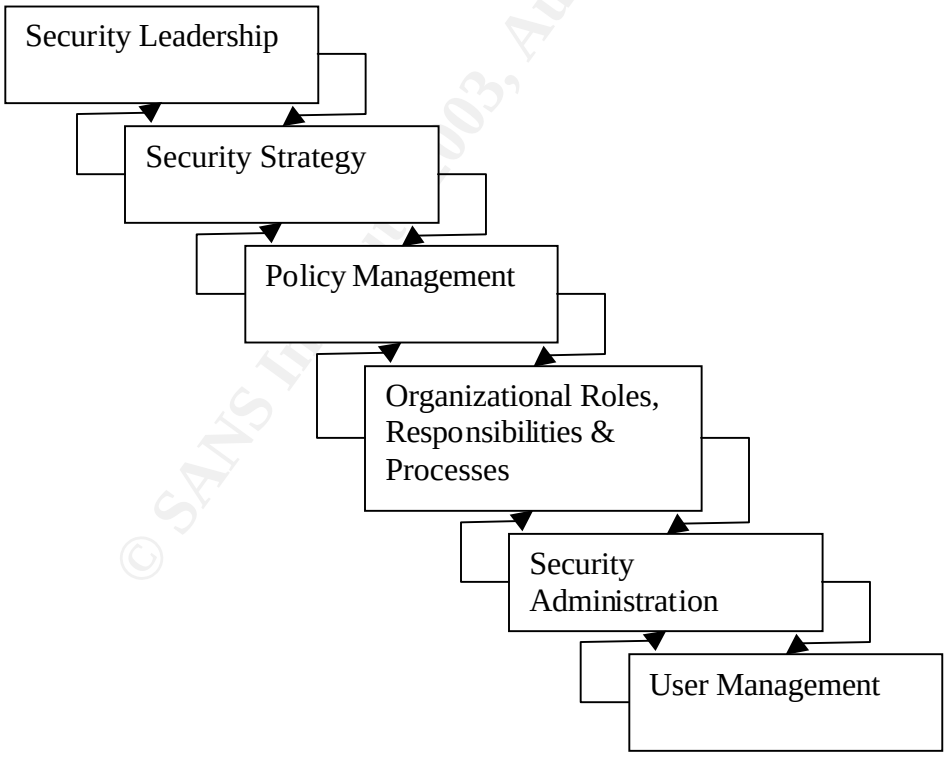
A well defined and easily used monitoring program addresses the COBIT DS5.7 security surveillance objective that IT security administration should ensure that security activity is logged and any indication of imminent security violation is reported immediately to all who may be concerned, internally and externally, and is acted upon in a timely manner.[20] In order to be successful in meeting this objective it will be

[19] COBIT 3rd Edition Control Objectives, http://www.isaca.org/control.pdf; IT Governance Institute, (Sep 10, 2002)
[20] COBIT 3rd Edition Control Objectives, http://www.isaca.org/control.pdf; IT Governance Institute, (Sep 10, 2002)

necessary to look at tools for gathering information from the many audit and event logs in the infrastructure. Capturing log data is only as good as your ability to review it regularly and to conduct trend analysis on the data.

A well designed monitoring program also address COBIT DS5.10 – Violation and Security Activity Reports that require that IT security administration should ensure that violation and security activity is logged, reported, reviewed and appropriately escalated on a regular basis to identify and resolve incidents involving unauthorized activity.[21] This links to the security incident process that will need to be established as part of the overall program design that addresses COBIT DS5.11 – Incident Handling where management should establish a computer security incident handling capability to address security incidents by providing a centralized platform with sufficient expertise and equipped with rapid and security communications facilities.[22]

Monitoring would also include the link to internal and external audit as an independent source of assessment of the current state of the information security program. Audit can be focused on a particular area of asset management (i.e. Firewall, Account Management, etc.) or on processes (Policy & Procedure audit, Risk Management Process audit, etc.) Regular audit also provides valuable feedback to the security strategy.



User Management covers two areas:

[21] COBIT 3rd Edition Control Objectives, http://www.isaca.org/control.pdf; IT Governance Institute, (Sep 10, 2002)
[22] COBIT 3rd Edition Control Objectives, http://www.isaca.org/control.pdf; IT Governance Institute, (Sep 10, 2002)

User Management identifies the core business processes, which users participate in to support the security of data. User management surrounds the processes of identifying ownership / stewardship for the IT resources, developing procedures for the creation, review, change and deletion of user accounts for those IT resources. User management also should address the fact that access should be granted on "need to know" and "least privilege" principles.

Proper setup of the User Management process addresses COBIT control objective DS5.3 – In an online IT environment, IT management should implement procedures in line with the security policy that provides access security control based on the individual's demonstrated need to view, add, change or delete data.[23]

Proper establishment of owners/stewards and the creation of procedures for creating, reviewing, deleting user accounts addresses the COBIT DS5.4 User Account Management objective that management should establish procedures to ensure timely action relating to requesting, establishing, issuing, suspending and closing of user accounts. A formal approval procedure outlining the data or system owner granting the access privileges should be included.[24] As well as COBIT DS5.5 Management review of user accounts objective that management should have a control process in place to review and confirm access rights periodically.[25] This need should drive the creation of 2 important procedures. First the procedure with HR and/or payroll to notify IT of personnel changes, this may drive additional IT procedures such as Return of Company Assets, Removal of User Access, Reassignment of ownership of data files, etc. Second would be the ongoing procedure for reporting, reviewing, updating, and storage of the records of review for proof of compliance of user account access.

User Awareness is a critical component of the security program and the level of awareness and education, that end-users should have regarding their responsibilities and assurance. Users are often the weak link in the security program. If security measures are seen as a hindrance users will find a way to bypass them. If there is not monitoring process to check for compliance to policies, procedures and standards users will go back to old habits. Often one of the weakest links in the asset management is the selection of weak passwords by the user. Well defined and established user awareness programs should touch on the importance of the user in the overall security program. The user awareness program may include general awareness information that can be done in seminars, emails, postings, and/or newsletters. The program should also include user specific awareness training dependant on job function, owner/steward roles, administrative roles, management responsibilities and system developer roles. The user specific training can be completed in one on one training sessions, group training sessions and through the distribution of policies, procedures and standards to the required personnel.

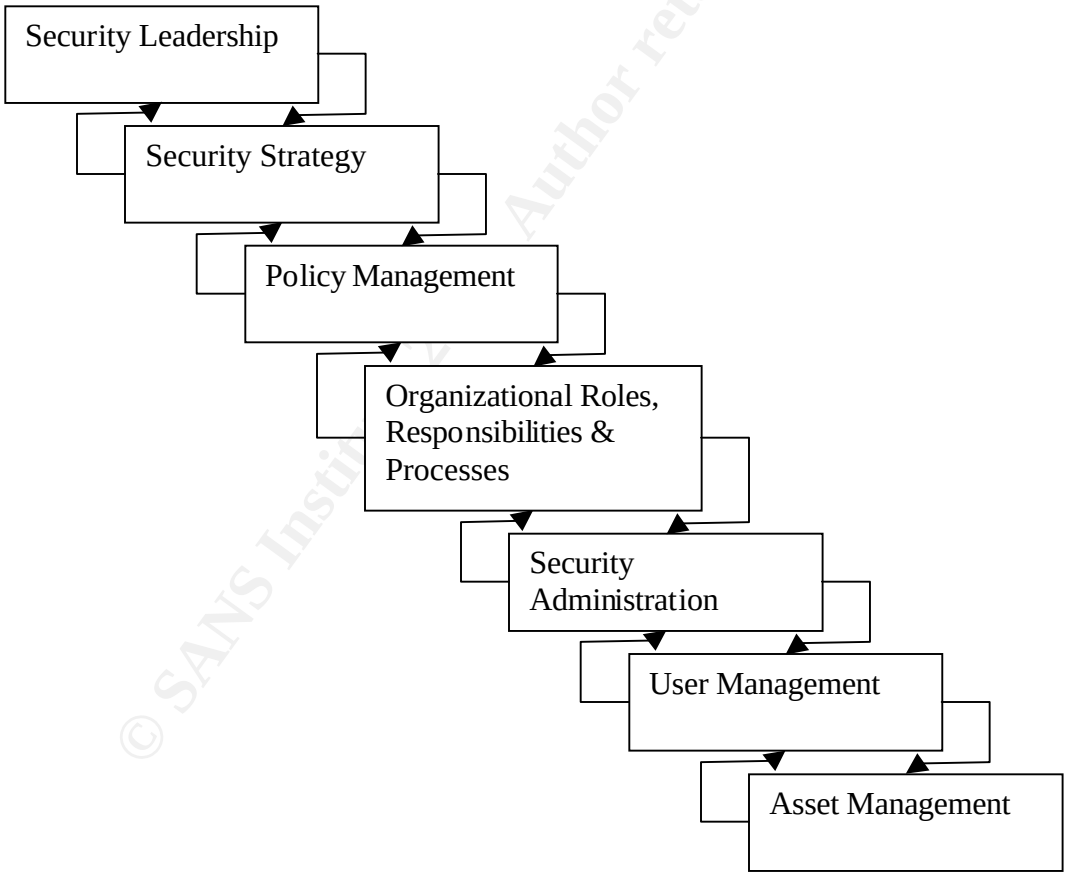
Another consideration is the skill set required by certain job functions in order to support their role in the security program. Although it may not be the responsibility of Information Security to arrange or deliver administrator training, for example, there

[23] COBIT 3rd Edition Control Objectives, http://www.isaca.org/control.pdf; IT Governance Institute, (Sep 10, 2002)
[24] COBIT 3rd Edition Control Objectives, http://www.isaca.org/control.pdf; IT Governance Institute, (Sep 10, 2002)
[25] COBIT 3rd Edition Control Objectives, http://www.isaca.org/control.pdf; IT Governance Institute, (Sep 10, 2002)

should be a process available for auditing the skill sets and recommending appropriate training.

Making users aware of the risks involved with their user accounts addresses the COBIT DS5.6 User control of user accounts control objective where users should systematically control the activity of their proper account(s). Also information mechanisms should be in place to allow them to oversee normal activity as well as to be alerted to unusual activity in a timely manner.[26]

Ongoing risk assessment also helps to promote the awareness program. As the business becomes more involved in determining the level of acceptable risk to the organization, assessing changes to IT assets from a risk perspective, approving the measures taken to reduce risk and approving the residual risk it will become more aware of the appropriate application of Information Security and the issues resulting from non-compliance. Participation in the assessment and approval of the measures to be taken also helps to promote buy-in for the ongoing use of those measures.



Asset management covers the securing of the IT resources. This will start with physical and environmental controls of the data centre, wiring closets, telecommunications rooms, etc. and will then move into system configuration, virus detection, firewall

[26] COBIT 3rd Edition Control Objectives, http://www.isaca.org/control.pdf; IT Governance Institute, (Sep 10, 2002)

implementation, zoning of the network in order to protect the critical resources appropriately, implementation of network and host based intrusion detection tools, and others dependant on the IT resources in place, the needs of the business, and the risk tolerance of the organization.

Asset management also includes the establishment of the identification, authentication and access controls for the IT resources. Determining the critical system for the business and completing a risk assessment on those systems will identify the level of control that will be needed in the authentication process. This may be limited to user ID and password policy or may expand to include biometrics, SecureID, or smart cards. Properly established user authentication addresses the COBIT DS5.3 Identification, authentication and access control objective that states that the logical access to and use of IT computing resources should be restricted by the implementation of adequate identification, authentication and authorization mechanisms, linking users and resources with access rules. Such mechanisms should prevent unauthorized personnel, dial-up connections and other system (network) entry ports from accessing computer resources and minimize the need for authorized users to use multiple sign-ons. Procedures should also be in place to keep authentication and access mechanisms effective (e.g., regular password changes).[27] This also links to the regular review of access rights in the user management process.

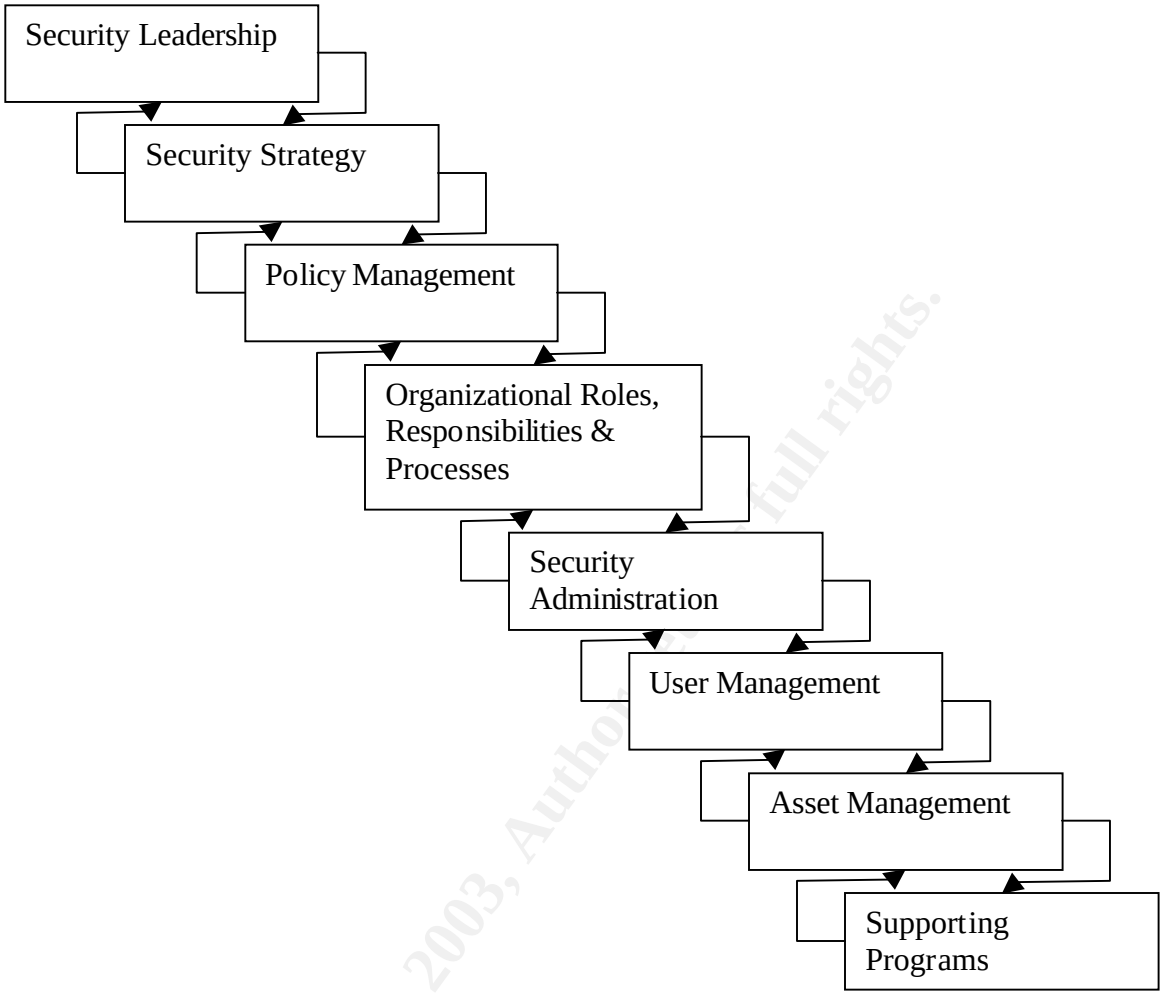
The remaining COBIT DS5 control objectives would be addressed by the design and implementation of asset controls

DS5.13	Counterparty Trust
DS5.14	Transaction Authorization
DS5.15	Non-repudiation
DS5.16	Trusted path
DS5.17	Protection of Security Functions
DS5.18	Cryptographic Key Management
DS5.19	Malicious Software Prevention, Detection and Correction
DS5.20	Firewall Architectures and Connections with Public Networks
DS5.21	Protection of Electronic Value[28]

These control objectives are addressed by virus protection, cryptography, intrusion detection, firewall configuration, and physical controls. The extent of the control will differ with the organization, the data protection needs based on the classifications and the baseline measures that are put in place across all IT Assets.

The protection of the IT assets will evolve over time and is an important component that feeds back to the security strategy process.

[27] COBIT 3rd Edition Control Objectives, http://www.isaca.org/control.pdf; IT Governance Institute, (Sep 10, 2002)
[28] COBIT 3rd Edition Control Objectives, http://www.isaca.org/control.pdf; IT Governance Institute, (Sep 10, 2002)



Supporting programs may or may not fall under the Information Security umbrella at your organization. These would include the creation, testing and maintenance of disaster recovery and business continuity plans. If responsibility for these supporting programs is not included in the responsibilities of Information Security they still need to be an integral part of the process. First ensuring that disaster recovery and business continuity plans are in place mitigates risk in the event of disaster. Second, Information Security needs to make sure that, in the event of a disaster, implementation of the disaster recovery and/or business continuity plans does not cause unacceptable levels of risk for the organization.

Summary

Security and audit issues found at the asset management layer in the process are symptoms of weak strategy, policy, and processes at the higher levels. Addressing only asset management with technology solutions will be ineffective unless people and process are also considered. Without the leadership, organizational responsibilities, administration and user management security will be implemented inconsistently and process will not be in place to review it regularly, to link it to the strategic planning, project management, change management, and incident management processes, these

factors will contribute to the reduction of security levels over time. You may need to implement asset management solutions to quickly address major issues in the infrastructure, but make sure you step back, look at the big picture, plan appropriately and apply your resources, people and $'s, effectively.

List of References

Thomas R. Peltier. Information Security Policies. Procedures and Standards. Auerbach Publications

Ing. Jacques A. Cazemier, Dr. Ir. Paul L. Overbeek, Drs. Louk M.C. Peters. Best Practice for Security Management. Office of Government Commerce. 1999

David J. McKerrow. Canadian Handbook on Information Technology Security. March 1998. http://www.cse-cst.gc.ca/en/documents/knowledge_centre/publications/manuals/mg9e.pdf. Government of Canada, Communications Security Establishment. (Oct 7, 2002)

Christopher J. Alberts, Audrey J. Dorofee. Octave Criteria Version 2.0. December 2001. http://www.cert.org/archive/pdf/01tr016.pdf Carnegie Mellon Software Engineering Institute(Oct 7, 2002)

A Guide to Risk Assessment and Safeguard Selection for Information Technology Systems. January 1996. http://www.cse-cst.gc.ca/en/documents/knowledge_centre/publications/manuals/mg3e.pdf Government of Canada, Communications Security Establishment. (October 7, 2002).

Gary Stoneburner, Alice Goguen, Alexis Feringa. Risk Management Guide for Information Technology Systems. 2001. http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf National Institute of Standards and Technology. (Sept 23, 2002)

Information Security Risk Assessment Practices of Leading Organizations. November 1999. http://www.gao.gov/special.pubs/ai00033.pdf United States General Accounting Office (Sept 23, 2002)

An Introduction to Computer Security: The NIST Handbook. http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf National Institute of Standards and Technology (Sept 23, 2002)

Creating, Implementing and Managing the Information Security Lifecycle. http://downloads.securityfocus.com/library/securityCycle.pdf Internet Security Systems (Oct 7, 2002)

Defense in Depth. http://nsa1.www.conxion.com/support/guides/sd-1.pdf National Security Agency. (October 7, 2002)

Gary Stoneburner. Underlying Technical Models for Information Technology Security. December 2001. http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf National Institute of Standards and Technology (Sept 23, 2002)

IT Governance Executive Summary. http://itgovernance.org/itgovexecsummary.pdf IT Governance Institute. (Oct 7, 2002)

Marianne Swanson, Barbara Guttman. Generally Accepted Principles and Practices for Securing Information Technology Systems. September 1996.

http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf National Institute of Standards and Technology (Sept 23, 2002)
Information Security Governance: Guidance for Boards of Directors and Executive Management. http://www.itgi.org/infosecurity.pdf IT Governance Institute (Oct 7, 2002)

Information Security Management Learning from Leading Organizations. May 1998. http://www.gao.gov/special.pubs/pdf_sing.pdf United States General Accounting Office. (Sept 23, 2002)

Board Briefing on IT Governance. http://www.itgi.org/boardbriefing.pdf IT Governance Institute (Oct 7, 2002)

Generally Accepted System Security Principles (GASSP). June 1999. http://web.mit.edu/security/www/GASSP/GASSP.DOC International Information Security Foundation (I^2SF). (Sept 23, 2002)

Moira J. West-Brown, Don Stikvoort, Klaus-Peter Kossakowski. Handbook for Computer Security Incident Response Teams (CSIRTs).December 1998. http://www.sei.cmu.edu/pub/documents/98.reports/pdf/98hb001.pdf Carnegie Mellon Software Engineering Institute, (Sept 18, 2002)

CIO Cyberthreat Response & Reporting Guidelines. http://www.cio.com/research/security/incident_response.pdf CIO Magazine. (Oct 14, 2002)

Job Aid 4 - Incident Response Quick Reference Card

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/windows/windows2000/staysecure/secopsj4.asp Microsoft Corporation (Oct 14, 2002)

Incident Response. January 8, 2001. http://www.macromedia.com/v1/DocumentCenter/Partners/ASZ_ASWPS_Incident_Response.pdf Allaire Security.(Oct 7, 2002)