Policy Issues and Fundamentals

Solutions in this chapter:

- The Role in Relation to Policy Creation and Compliance

Introduction

In this chapter we look at the auditor's role in relation to policy and incident handling.

It is important to remember that security is not just about technology. Security is about people. It is the people within your organization that will determine the success or failure of any information security program. As such it is crucial that they understand the need for security and that security is there as an aide and not a roadblock. Remember, security is about the people within your organization just as much as the information they seek to protect.

The auditor's role in this process is to validate the policy and processes. Policy is the tool we use to guide people. The auditor needs to work with management and the information owners to ensure that an effective system is implemented.

The Auditor's Role in Relation to Policy Creation and Compliance

The auditor's role is to measure and report on risk. Consequently, audit is a tool of management. It is not the auditor's role to decide on what needs to occur. This is where most security professionals err. In taking security issues and vulnerabilities personally they redirect focus from the issues. That said, auditors need to be involved in the creation of policy and procedures. This also involves the incident handling process from the creation of a policy to the follow-up after an incident occurs.

In order to report on risk, the auditor needs to be a researcher. It is not expected that any auditor will know everything, but in moving through the organization they will need to gain an understanding of both the business processes and new regulations or other compliance issues that apply. In order to create a policy that effectively matches the risk profile of the organization, the auditor needs to understand both the stance taken by management as regards to risk and how policy relates to it.

The key aspect here is measure and report. The auditor can provide invaluable input into the creation of effective controls associated with the policy and give feedback to management as to the potential cost of implementing a policy against the consequences of taking another course of action.

Secondly, is the auditor who will need to measure conformity and compliance with the policy and processes within the organization. In previous chapters it was noted that policy should be developed on the SMART principle. In particular, the M in this principle represents measurable. The auditors experience and background can provide invaluable information satiated with the creation of metrics. No policy or process can be deemed to be effective it cannot be measured.

SMART

Specific
Measurable
Attainable
Realistic
Timely

Specific

A specific goal has a likelihood of being success than a general goal. The questions used to create a specific goal require that you answer the six "W" questions:

- Who — Who is involved?
- What — What do you want to accomplish?
- Where — Identify a location.
- When — Establish the time frame.
- Which — Identify requirements and constraints.
- Why — Specific reasons, purpose or benefits of accomplishing the goal.

Measurable

Establish concrete criteria and metrics to measures progress toward the attainment of the goal. Measuring progress helps ensure that you stay on target, reach your defined dates, and achieve the goal.

To determine if a goal is measurable, ask

- How much?
- How many?
- How will I know when the goal has been successfully accomplished?

Attainable

When you recognize the goals that are most important, you begin to make them come true. You develop the attitudes, abilities, skills, and financial capacity to reach them. You start considering previously overlooked opportunities to ensure the achievement of your goals.

It is possible to attain nearly all any goals that are set when you plan each step and establish a time frame that allows the completion of those steps. Goals that seem far away and out of reach eventually end up closer and turn out to be attainable. This is not because the goal has shrunk, but due to growth.

Realistic

To be realistic, a goal must represent an objective toward which you are capable of achieving. A goal may be both lofty and realistic. Every goal must represent progress. A lofty goal is frequently easier to achieve than a low one as a low goals apply low motivational force. Some of the most difficult tasks to accomplish seem easy due to passion - they become a labor of love.

A goal is almost certainly realistic if you truly believe that it can be accomplished. Further means to knowing if a goal is realistic is to determine if you have accomplished a similar task previously. Alternately, ask what conditions would have to exist to achieve this goal.

Timely

A goal needs to be able to be completed in a set time frame. Without a time frame, no sense of urgency can be created.

T can also mean Tangible. A goal is tangible when it can be experienced with at least one of the senses. These can be, taste, touch, smell, sight or hearing. A tangible goal results in a greater prospect of making it specific and measurable and thus achievable.

Policy Responsibilities

When considering policy, the auditor needs to postulate the impact of the organization from a number of standpoints. It is necessary to consider both a top-down and bottom-up approach in order to make policy truly effective. This means creating ways to both engage employees and involve management. In this manner, the auditor can be seen as not just the organizational policeman but as a business enabler.

There are three tiers supporting the function of the auditor. These are:

1. Top-down approach where information is gathered from and reported back to management. In this tier the auditor gains an understanding of the organization's vision and mission and an insight into the risk level accepted by management.

2. The bottom-up approach enables the auditor to gain an insight into the workings of the organization through dealings with the employees. This tier is one of the most overlooked. It should be remembered that no understanding of the organization can be achieved without understanding the employees of the organization.

3. The final tier is research. One of the key roles of an auditor is to tie together the strategic values of the management tier with the operational implementations from the employee tier and to understand where the organization is going.

The auditor is in the unique position with any organization to see where the organization currently is and to also see whether it is on track to where management is attempting to steer the organization to be. In measuring and reporting on compliance, the auditor has the unique view of the organization that provides both a wide spectrum vision and a close-up view.

Employees

Each employee is responsible for complying with the policies and procedures that relate to them and for cooperating with IT and audit staff to protect the resources of the organization. HR needs to work with management to ensure that the correct procedures and processes are being followed. Human Resources must ensure that each employee becomes familiar and complies with the organizations Policy.

It is the auditor's role to ensure that the policy considerations can be met. In the event that a policy is unenforceable or otherwise does not meet the needs of the organization the auditor needs to work with HR and management to bring policy into line with the requirements of the organization.

The auditor is in a unique position to:

- Facilitate change,
- Measure the effectiveness of existing processes,
- Gain an insight into the inner workings of the organization and its culture,
- Gain an insight into early signs of discontent or other problems in the workplace,
- Research compliance requirements and changes to legislation,
- Gain access to multiple departments across the organization, and
- Speak directly to senior management.

Management

Both audit and human resources need to work with senior management to ensure compliance when:

- Enforcing the policies, standards, procedures, and guidelines for the protection of IT resources and information.
- The appointment of IT support representatives, and in the provision of apt funding, training, and resources to those people for information security and compliance related responsibilities.
- Applying sanctions consistent with Human Resources policies to individuals and department heads that break provisions of this policy, either willfully, accidentally, or through ignorance.
- Designating Data Stewards for each significant collection of business information, who in turn are responsible for determining the value of their information and implementing appropriate security measures as specified in the Data Access Policy
- Sponsoring internal awareness and training programs to familiarize employees with the security policy, procedures and recommended practices.

The auditor has a unique position within any organization. The role entails dealing with employees from all levels of an organization. Though many auditors shy at the idea of spending time in the factory floor or

production centers (or for that matter whatever the roots of the organization may be), this is one of the primary sources of information available to the auditor.

Policy Creation

The creation or review of any policy should be focused on a predetermined objective. Whenever any policy is being created the following questions should be asked:

- What is the purpose of the policy and why does it exist in the first place?
- Is the policy still valid or does it need to be updated/removed?
- How does the policy relate to the vision and mission of the organization? Of the Department?
- Does the policy meet the needs of the organization?
- Does the policy enable the organization to comply with the regulations and standards that it must meet?
- Is there a process associated with the policy in order to measure its success?

It is the role of the auditor to work with management in order to answer these questions. Those individuals in management who have initiated the policy and associated processes are the most likely to understand the reasons why. It is the auditor's role to provide information to these individuals as to the best method that may be used to achieve the scope of the policy and to integrate a means of measuring and reporting the effects of the policy (both good and bad).

Policy Conformance

It is the auditor's role to work with others within the organization (such as human resources) to determine whether the policy has been implemented correctly and if it is otherwise being complied with. This process involves asking the questions:

- How effective is the policy?
    - How could the policy be improved?
- Is the policy being followed or complied with?
    - Can the policy be complied with?
    - Are there discrepancies with the policy that make it difficult to comply to?
    - Is the policy still valid?
    - Do employees understand the policy?

This process involves customizing the above questions and relating them to the individual task at hand. For instance, if the organization has implemented a new antivirus system it would be possible to ask how

effective the product is a protecting the organization. This could be a comparison against any previous system with the new one or it could be an overall measurement of the effectiveness of the device overall.

Another area is to look at the cost of compliance. In conforming to the policy what cost is the organization experiencing against the cost of non-conformance.

Incident Handling

Incident Handling (IH) and auditing are related. Both of these processes serve as policy and process/procedure assessment tools and aid in measuring risk. The distinction is that audit generally occurs prior to an incident. The auditors should work with teams from IT to create processes before an incident occurs.

The aim is to proactively construct incident handling procedures before an event occurs. This is a process of understanding the risk associated with the systems deployed within an organization and its people. Auditors and other staff within the organization should work together to assess the level of threat and the type of threat faced by the organization; record the vulnerabilities that may affect systems.

Working together the organization will develop an understanding of how it may be affected by a compromise to its systems or other incident. This process will then allow for the creation of layered defenses, designed to (where possible) mitigate the damage or at the least minimize the damage to the organization.

The other role of the auditor in the incident handling process is to assess the effectiveness of the procedures. There are two aspects to this:

1. Running drills and other tests to validate the processes before an incident occurs, and
2. Reporting on the effectiveness as well as any possible improvements to the process based on the consequences of an incident and the effectiveness of the incident handling process during the incident.

SCORE

SCORE (http://www.sans.org/score/) is a repository of effective policies, processes and tools. Its mission is detailed below.

The SCORE project states that it *"is a cooperative effort between SANS/GIAC and the Center for Internet Security (CIS). SCORE is a community of security professionals from a wide range of organizations and backgrounds working to develop consensus regarding minimum standards and best practice information, essentially acting as the research engine for CIS. After consensus is reached and best practice recommendations are validated, they may be formalized by CIS as best practice and minimum standards benchmarks for general use by industry at large.*

SCORE Objectives:

- *Promote, develop and publish security checklists.*
- *Build these checklists via consensus, and through open discussion through SCORE mailing lists.*

- *Use existing references, recruit GIAC-certified professionals, and enlist subject matter experts, where and when possible.*"

There are multiple "Sample Incident Handling Forms" freely available at the site (http://www.sans.org/score/incidentforms/) that will aid in the creation of an effective incident handling program.

Security Incident Forms

1. Incident Contact List
2. Incident Identification
3. Incident Survey
4. Incident Containment
5. Incident Eradication
6. Incident Communication Log

Intellectual Property Incident Handling Forms

1. Incident Form Checklist
2. Incident Contacts
3. Incident Identification
4. Incident Containment
5. Incident Eradication
6. Incident Communication Log

Standards and Compliance

All organizations have both standards and regulations that they will need to apply in order to be successful. The auditor is management's tool in reporting how effectively the organization is complying with its requirements. A number of the areas that an organization will need to comply with have been detailed below.

The audit committee and audit department should have an audit charter. This is the scope of the audit department. It is in effect the vision and mission statements for the audit department defining their goals, limits and reporting structure. The audit charter will aid in focusing the auditor in respect of complying with the organizations needs.

Compliance with legal requirements

To avoid breaches of any statutory, criminal or civil obligations and of any security requirements, the design, operation and use of IT systems may be subject to statutory and contractual security requirements. Legal compliance is a detailed topic and is specific to both locality and industry. It has become a major driver for information technology investments. “Compliance” in the true sense of the word entails a legal requirement or a standard for context.

It is important that the organizations security administrator is familiar with the pertinent legal standards and requirements for their location and industry. Compliance issues, demand that organizations must look beyond the hype of current laws and regulations to address topics such as corporate governance, privacy, encryption laws, signature laws, and critical infrastructure requirements simultaneously.

International organizations must understand the legal requirements of various jurisdictions, including the similarities and conflicts among them.

A failure to understand the broader context of applicable legal requirements could result in multiple secluded solutions. Conflicts among them may become apparent from a lack of understanding regarding the differences in various jurisdictions. This is likely to result in compliance failures or in over compliance. Either under or over compliance is likely to cost an organization in the end.

Policy Compliance

A review of compliance against policy is usually achieved through the use of both internal audit and through external organizations working in conjunction with the human resources department. This style of review is designed as a method to both qualify and sometimes quantify that employees and other parties who are affected by the organizations security policy (including contractors and business partners) both comply with the policy and understand it.

This is mostly either an internal Audit or Human resources function. It is common for organizations to test compliance with the policy, but understanding is generally overlooked. It is not enough for an employee to blindly follow a policy and process. Without understanding errors will eventually occur and an incident will result.

Third Party and Government Reviews

Many organizations (e.g. the Health or Finance Industries) have external legal requirements, which not only need to be met, but which may be audited externally. These organizations not only have to satisfy the basic security needs that apply to all organizations (as a consequence of avoiding contributory negligence and contractual breaches for instance), but also need to meet selected set of standards.

Organizations have been known to lose their license to operate if an audit is failed. At the least fines or other penalties may apply. In some instances, criminal sanctions apply to organizations that do not meet the regulatory requirements.

It is important that the network and system administrators always check and understand all relevant legislation, which may concern their organization. It is the role of the audit department to ensure that management knows the level of comprehension within the organization. If for instance network administrators

do not understand the need for maintaining router logs, it is the responsibility of the auditor to report this to management.

System audit considerations

To minimize interference because of the system audit process, there must be controls to safeguard operational systems and audit tools during system audits.

To assist with an audit using this methodology, the auditor should develop a questionnaire that contains questions pertinent to the controls implemented by the organization. There are examples of both standards documents and checklists included with the appendix to this book. Obviously in cases where you are only evaluating the security of a certain area within your organization, not all controls are relevant. It is important to use your judgment based on individual requirements to decide which controls should be used.

In the individual system chapters of this book, a number of tools that may be used in the creation of the checklist have been included.

Internal and External Standards

Standards both internal and external to an organization may be useful in creating and updating security policy and procedure. External standards are often useful as a benchmark or starting point. The auditor needs to communicate the standards and their potential effect on the organization to management.

Internal Standards

Many industries have certain baseline policies (e.g. Health or Finance). As noted previously, failure to strictly adhere to these standards may result in severe penalties.

All organizations should develop standards to be used and implemented within itself. Often external standards can be used as a guideline and have been found to be a good initial guideline to kick-start the process of developing standards. These have been covered in more detail in other sections of this book.

External Standards

Some of the more commonly known and used standards are detailed below. These are often used as a foundation in setting up a security program, policies and procedures and also as a baseline to review the depth of any existing standards within an organization.

Human Resource (HR) Issues

Human resources departments have a crucial role to play in regards to the security of an organization. The human resources department needs to be involved with the organizations security to reduce risks of:

- human error, theft, fraud or misuse of facilities;
- to ensure that users are aware of information security threats and concerns, and are equipped to support the corporate security policy in the course of their normal work;

- to minimize the damage from security incidents and malfunctions and learn from such incidents.

Some of the key areas needed within an organization which should be fulfilled by HR are;

- Ensuring that “Terms and Conditions of Employment - Employment Letters / Contracts” have been issued and cover the security requirements of an organization;
- Ensure that Employee Confidential Information Undertaking documents have been completed;
- Create and issue policies on Intellectual Property Rights and ensure that an Employee Undertaking has been signed;
- Create and enforce policies on privacy issues such as Sharing Employee Information;
- Creating and Conducting Induction Training;
- Suggested Disciplinary Process for management;
- Ensuring that a Grievance Procedure exists;
- Conducting Exit Interviews for staff leaving the organization;
- Checking Information Security Clearance Levels where needed.

Draft a policy

Based on the results of a policy review or risk assessment, the auditor can create and present examples of draft policy to management (such as security policies for the IT infrastructure and processes). Human Resources need to be involved, both in initially developing (and then maintaining) an employee manual that identifies the policy and security training needs and schedules. These policies and schedules should be communicated to all stakeholders at all branches, with automatic alerts for the scheduled steps. Human Resources are often the best means to accomplish this task.

It may be the case that management does not decide to implement a policy that the audit team has recommended. When this occurs, the auditor should not be disappointed. It is important to remember that the auditor’s role is to measure and report on risk. Reporting a policy discrepancy and offering an example does not mean that management will implement it.

Summary