Chapter 1

Introduction

This chapter includes:

Audit Essentials and Principles

- What are an Audit, Assessment, and Reviews?

The Various Auditing Standards and Certifications

- ISACA and CISA
- GSNA
- CIA and the IIA
- FISCAM
- COBIT

Introduction

This book provides comprehensive methodology, enabling the staff charged with an IT security audit to create a sound framework, allowing them to meet the challenges of compliance in a way that aligns with both business and technical needs. This "roadmap" provides a way of interpreting complex, often confusing, compliance requirements within the larger scope of an organization's overall needs

Data held on IT systems is valuable and critical to the continued success of any organization. We all rely on information systems to store and process information, so it is essential that we maintain Information Security. The goal of this book is to define an economical and yet secure manner of meeting an organizations compliance needs for IT. To do this we need to understand the terminology that we have based this on and hence the focus of this chapter. We first need to define what security itself is.

The purpose of information security is to preserve:

Confidentiality - Data is only accessed by those with the right to view the data.

Integrity - Data can be relied upon to be accurate and processed correctly.

Availability -Data can be accessed when needed.

Consequently, the securing of information and thus the role of the Security professional requires the following tasks to be completed in a competent manner:

1. The definition and maintenance of security policies/strategies.
2. Implementing and ensuring compliance to Policies and Procedures within the organization:
    a. The IT security organization needs a clear statement of mission and strategy. Definition of security roles & processes.
    b. Users, administrators and managers should have clearly defined roles/responsibilities and aware of them.
    c. User / support staff may require training to be able to assume the responsibilities assigned to them.
3. Effective use of mechanisms and controls to enforce security
4. Well defined Technical Guidelines and controls for the systems used within the organization
5. Assurance (audits and regular risk assessments).

IT security is not about making a perfect system, it is about making a system that is resilient and that can survive the rigors it is exposed to. Compliance comes down to due diligence. If you can show that your system is resilient to attack and that it has a baseline of acceptable controls, you will be compliant with nearly any standard or regulation. @TechEdQuery due diligence is half the equation – need to include due care. Due diligence is the IT security persons role. Due care is the managements role in approving and allowing IT to implement solutions. Actually, the terms due care and due diligence mean the same thing – so in a way the comment is correct in what is being attempted to be stated but is also wrong.

Does Security belong within IT?

The simple answer is yes. The more developed answer is that information security affects all aspects of an organization, not just IT. Security needs to be the concern of all within an organization from the simple use to senior management.

Management Support

If management does not succeed in the establishment of a sound security infrastructure (including policy, communication, processes standards and even culture) within the organization, then there is little likelihood of an organization being able to remain secure. Standards, Guidelines and Procedures are developed using the Security Policy. Without these, security cannot be maintained. Without management support there cannot be enforcement, liability or co-ordination of incidents. Management support for Information Security controls is fundamental to the continuing security of any organization.

Management can facilitate education and awareness strategies with the organization. Good awareness processes and management support will help in the overall security of an organization as;

1. An organization's personnel cannot be held responsible for their actions unless it can be demonstrated that they were aware of the policy prior to any enforcement attempts,

2. Education helps mitigate corporate and personal liability, avoidance concerning breaches of criminal and civil law, statutory, regulatory or contractual obligations, and any security requirement,

3. Awareness training raises the effectiveness of security protection and controls; it helps reduce fraud and abuse of the computing infrastructure and increases the return on investment of the organization's investments in both security as well as in computing infrastructure in general.

Job Roles and responsibilities

Dependant on the size of an organization, responsibility may be divided into the following defined roles. It is important that responsibility is apparent and is supported by management. To achieve this, the accountable persons must actually assume their accountabilities (i.e. they have powers necessary to take corresponding decisions and the experience/knowledge to take the right decisions). Management and Human resources should ensure that the necessary roles are correctly implemented.

Board and Executives: The Board of Directors and the managing director or CEO (or equivalent e.g. President) are ultimately responsible for security strategy and must make the necessary resources available to combat business threats. This group is ultimately responsible for disseminating strategy and establishing security-aware customs within the organization. They have the mandate to protect and insure for continuity of the corporation and to protect and insure for profitability of the corporation. Information Security plays a crucial role in both of these aspects of senior management's roles.

Business process / data / operation owner: is directly responsible for a particular process or business unit's data and reports directly to top management. He/she analyses the impact of security failures and specifies classification and guidelines/processes to ensure the security of the data for which he/she is responsible. There should not be any influence on auditing. **Process Owner**: is responsible for the process design, not for the performance of the process itself. The process owner is additionally responsible for the metrics linked to the process feedback systems, the documentation of the process, and the education of the process performers in its structure and performance. The process owner is accountable for sustaining the development of the process and for identifying opportunities to improve the process. The process owner is the individual ultimately accountable for improving a process.

IT Security manager/director: is responsible for the overall security within the organization. The IT security manager(s) defines IT security guidelines together with the process owner. He/she is also responsible for security awareness and advising management correctly on security issues. He/she may also carry out risk analyses. It is important that this person be up-to-date on the latest security problems/risks/solutions. Co-ordination with partner companies, security organizations and industry groups is also important.

System supplier: Installs and maintains systems. A service level agreement should exist defining the customer/supplier roles and responsibilities. The supplier may be, for example, an external contracting company or the internal datacenter or System/Security administrator. This person is responsible for the correct use of security mechanisms.

System designer: The persons who develop a system have a key role in ensuring that a system can be used securely. New development projects must consider security requirements at an early stage.

Project Leaders: ensure that Security guidelines are adhered to in projects.

Line Managers: ensure that their personnel are fully aware of security policies and does not provide objectives that conflict with policy. He/she enforces policy and checks actual progress.

Users: Users, or "*information processors/operators*" are responsible for their actions. They are aware of company security policy, understand what the consequences of their actions are and act accordingly. They have effective mechanisms at their disposal so that they can operate with the desired level of security. Should users receive confidential information that is not classified, they are responsible for classifying and distribution of this information.

Auditor: is an independent person, within or outside the company, who checks the status of IT security, much in the same way as a Financial Auditor verifies the validity of accounting records. It is important that the Auditor be independent, not being involved in security administration. Often external consultants fulfill this role, since they can offer a more objective view of policies, processes, organizations and mechanisms.

What is an Audit, Assessment, and Review?

The initial thing we need to do is develop a common terminology that we will use. This chapter is designed to introduce the “key terms of art” used within the audit and security profession and to thus allow the IT professional, management and business to all speak the same language. Terms of art are those terms used in the profession.

Audit

The American Institute of Certified Public Accountants (AICPA) defines two definitive classes of Audit, internal and external. An audit consists of the evaluation of an organization’s systems processes and controls and is performed against a set standard or documented process. Audits are designed to provide an independent assessment through testing and evaluation of a series of representations about the system or process. An audit may also provide a gap analysis of the operating effectiveness of the internal controls.

External audits are commonly conducted (or at least should be) by independent parties with no rights or capability to alter or update the system they are auditing (AICPA). In many cases, the external auditor is precluded from even advising their client. They are limited to reporting any control gaps and leading the client to a source of accepted principles. Due to these restrictions, an indication of the maturity or a system against an external standard (such as COBIT) is often engaged.

Internal audits involve a feedback process where the auditor may not only audit the system but also potentially provide advice in a limited fashion. They differ from the external audit in allowing the auditor to discuss mitigation strategies with the owner of the system that is being audited.

Neither an internal or external auditor can validly become involved in the implementation or design process. They may assess the level to which a design or implementation meets its desired outcomes, but must be careful not to offer advice on how to design or implement a system. Most crucially, an auditor should never be involved with the audit of a system they have designed and/or implemented.

There is a large variety of audit types. Some examples include SAS 70 (part 1 or 2) audits, audits of ISO 9001,17799:2/27001 controls, and audits of HIPPA controls. There are many different types of audits and many standards that an audit may be applied to. We go into these in detail later in the book, so do not worry of you are unsure of what they are now. Each of these audit types are documented in the appendixes as well.

An audit must follow a rigorous program. A vulnerability assessment as it is commonly run is more correctly termed as a controls assessment. A controls assessment may also be known as a security controls review.

Inspection and Reviews

An audit differs from an inspection in that an audit makes representations about past results and/or performance. An inspection evaluates results at the current point in time. For an audit to be valid, it must be conducted according to accepted principles. In this, the audit team and individual auditors must be certified and qualified for the engagement. Numerous "audits" are provided without certification, these however are in consequence qualified reviews.

Penetration tests and Red Teaming

A Penetration test is an attempt to bypass controls and gain access to a single system. The goal of the Penetration test is to prove that the system may be compromised. A Penetration test does not assess the relative control strength nor the system or processes deployed, rather, it is a "red teaming" (see below for details) styled exercise designed to determine if illicit access can be obtained, but with a restricted scope. The issue is that it is infeasible to prove a negative. As such, there is no scientifically valid manner to determine if all vulnerabilities have been found and this point needs to be remembered when deciding on whether to use a Penetration test process.

Cohen (1998-2) notes in respect to red-teaming organizations “one of the teams I work with routinely asks whether they are allowed to kidnap anyone to get the job done. They usually get turned down, and they are rarely allowed to torture anyone they kidnap”. Red teaming is based on nearly anything goes.

The greatest strength of the Penetration test lies in its being able to market the need to improve internal controls to internal management. This may seem contradictory, but it is based on perception. Being that the Internet is seen as the greatest threat to an organization’s security, management are often focused on the firewall and Internet gateway to the exclusion of the applicable security concerns and risks. As such, Penetration tests do help in selling the need for an increased focus on information security, but often at the expense of an unfocused application of these efforts.

A Penetration test is of limited value in the greater scheme of a systems information security audit program due to the restricted nature of the test and the lack of inclusion of many key controls. Contrary to popular opinion, penetration testing does not simulate the process used by an attacker. The attacker is not limited in the level of time or funds in the manner that restricts the Penetration tester. Whereas a successful Penetration test may note vulnerabilities, an unsuccessful Penetration test does not prove the security of a system (Dijkstra, 1976).

"**Red Teaming**" differs from penetration testing in that it is designed to compromise or penetrate a site at all costs. It is not limited to any particular attack vector (such as a VPN or Internet) but rather is an attempt to access the systems in any feasible manner (including physical access). A typical red teaming goals would include objectives such as "steal 100,000 for Big Bank without being caught and deliver the report of how to do this to the executive of Big Bank" or "Copy file X which is marked as secret".

Both government and business have used red teaming for many decades in a variety of areas including physical and logical based testing. At its simplest, it is a peer review concept. Another way to look at it is a method of assessing vulnerabilities. In cases where red teaming refers to the provision of adversarial perspectives, and the design of the red team is not hampered in the matter is that ethical attacks are. There is a little correlation between a red team exercise and an ethical attack.

The formation of red teams (or cells) is a situation unlikely to occur in any ethical attack. Further, internal intelligence is unlikely to be gathered as part of an ethical attack. In this instance is more likely that the ethical attack will consist of an attack against the Internet gateway. An engagement to red team is wider in scope, areas including internal subversion and associated control checks cannot be ignored in this type of test.

Penetration testing, if done correctly, can provide some value in its free-form approach if the limitations to scope inherent in this type of test are understood. When correctly implemented, a Penetration test adds a level of uncertainty to the testing. The benefit of this uncertainty is that it might uncover potential flaws in the system or controls that had not been taken into account when designing the control system. To be of value, a Penetration test needs to do more than a simple tool based scan of a system.

Red Teams: Fred Cohen states that "in simplest terms, these services provide information on and demonstrations of vulnerabilities… Many people believe that the most important impacts of Red Teaming are in the effects of the results on management decision-making. In many cases, the sole purpose of this effort is usually to provide management with a graphic demonstration of the vulnerabilities faced by the organization. The information security specialists know that there is a big problem, but they are having difficulting making management understand. So they decide to do a sample penetration to make the impact of vulnerabilities clearer."

Penetration Testing needs to do something novel and unexpected.

There is little similarity between a penetration test, vulnerability assessment, risk assessment or audit. The lack of understanding of these differences often impedes the implementation of effective security controls. We will explain each of these terms in detail throughout the book. An explanation is also provided in the glossary.

Ethical Attacks

Ethical Attacks are a subset of penetration testing. They are designed to externally validate a set of controls in a manner that is thought to simulate an attack against the system. It should be noted that ethical attackers are not actually testing system security in the manner of an attacker due to a variety of restraints. It has been demonstrated (Cohen, 1997) that ethical attacks do far less to categorically qualify security risks than many other forms of testing. They do not for instance take note of internal controls. Many of the potential vulnerabilities cannot be discovered in a penetration test by the nature of the testing method. Next, it needs to

be remembered that there is an economic cost associated with ethical attack styled penetration testing. The Ethical attacker is constrained by a budget of time and thus money, the real attacker is not.

.

Blind testing by its very nature will take longer to complete than auditing a site with access and knowledge of all the systems (Dijstra, 1976) if any level of assurance is required. The review undertaken by the ethical attacker is thus hobbled from the start. It is infeasible to state that the contractor will have more knowledge at the end of a review if it is done as an ethical attack with limited knowledge over a systems review with full information.

Being a black box test format (see the definition below), the lack of foreknowledge as to the qualification of value associated with any particular asset negates the possible assessment of a vulnerability status by an ethical attack process (Dodson, 2005). Rather, the process is designed to determine a subset of all possible control failures, which may lead to a system breach or compromise. This subset can never equal the entire control set of possible hazards and vulnerabilities.

This said ethical attacks do have value. In particular, they are useful for process testing. If the systems and security team go through the internal processes, they can use the ethical attack process as a means of determining an estimate of the levels of protection using time based security. This is achieved by measuring the detection time and the response time. These times may then be compared at different periods (such as weekends and nights) to determine the level of protection over the system.

Unfortunately, most ethical attacks are not used as an exercise to quantify the level of protection or risk to a system. Rather they are used as a simple de facto vulnerability assessment.

Vulnerability Assessment

A vulnerability assessment is an assessment and gap analysis of a site's or a system's control strengths. A vulnerability assessment is a risk-based process. The process involves the identification and classification of the primary vulnerabilities that may result in a system impact. Often, methodologies such as fault tree analysis or CCA (cause consequence analysis) are employed in this process.

GAP Analysis: A Gap analysis is a useful tool in to deciding upon strategies and tactics. The process consists of baselining the present state and comparing this to a desired or `target' state. The difference is the gap between them. The process is used for the purpose of determining how to get from one state to a new state. It consists of answering the questions: “Where are we?” and “Where do we want to be?”

A vulnerability assessment is a critical component of any threat risk assessment. Following the vulnerability assessment, an impact analysis is conducted to be used in conjunction with a threat report to provide for an estimation of the organization’s risk to selected attack vectors. There are various processes and procedures used to provide vulnerability assessments and threat/risk determinations. Some standards such as AS/NZS 4360:2006 are commonly mandated by government organizations (such as the New South Walses (NSW) State government in Australia. Canada, the UK and USA all have their own requirements).

Vulnerability assessments are part of a complete risk analysis program (Moore, 2001). Vulnerability assessments involve the cataloguing of assets and capabilities. The lack of internal knowledge provided in the

typical ethical attack process precludes this phase. A vulnerability assessment helps to quantify and discern the level of risk to a system (Linde, 1975).

Vulnerabilities and potential threats to the resources being tested are determined in this process. There are a variety of areas being tested; both internal and external testing is required. Once these areas are taken into account the test will be expanded to test the physical threats and other tests outside the reach of the ethical attack or basic penetration test."

Black and White Box Testing

Both vulnerability assessments and penetration tests may be conducted as a white box or black box analysis. A black box analysis is instigated with little or no knowledge of the system being tested. A white box analysis is conducted with all details of the system provided to the tester in advance of the testing process (Dijstra, 1976).

Tools Based Scanning

The common perception that running an automated scanner such as Nessus or one of its commercial counterparts is in itself a vulnerability or penetration test is false. The belief that these services act as an audit is even further from the truth.

Most of the so-called penetration tests that are provided are no more than a system scan using tools. A penetration test, if correctly designed and implemented will attempt the use of various methodologies to bypass controls. In some instances, this may involve the creation of new or novel scripts/programs and even social engineering.

The issue is not that many people commonly use the words interchangeably but that so-called professionals fail to differentiate the terms. Of particular concern is the use of the term audit and the designation auditor. This is as these terms are often restricted in legislation as most jurisdictions have statutory requirements surrounding their use and application.

Agreed Procedures Review

Information security systems provide many of the functions that construct a control system. Of particular concern are controls that limit access to accounting and financial records. This includes records held by systems that provide an e-commerce transaction path. In many jurisdictions, it is an offence to sign off an audit report when you are not a certified auditor. Traditionally the path around this has been not to call the process of testing the system an audit, but rather to call it an agreed procedures review. An agreed procedures review or simply a review is an analysis of controls performed against an agreed process.

Acceptance testing

Acceptance testing is one of the final occasions to recognize any risk or exposure in a system (Myagmar, 2005). The development and implementation of an approved, inclusive and prescribed plan will support the successful execution of a solution, with the least interruption to critical systems. The process of acceptance testing is to gain an acceptance of the changes or introduction of a system.

Acceptance testing is more correctly an audit or qualified review of a set of implementation objectives to ensure that the system meets the required levels of performance or security.

Data conversion

Testing a Data Conversion is a two-stage process (AICPA). Initially the planning process associated with the data conversion is reviewed to determine the sufficiency of any proposed controls. The subsequent stage occurs after the conversion process. The aims of this process are to present an independent evaluation as to the completeness and accuracy of the data after the conversion.

Any conversion of data into another form or to another system bears an elevated risk of error, omission or other deviations to the completeness and accuracy of that data. Standard input and process controls are frequently not maintained in the data conversion process. To be successful, any project, which includes a data conversion process, requires that the accuracy and completeness of the conversion process be preserved.

The Taxonomy

Class	Definition	Categories	Sub-Categories
Audit	An audit, consisting of an evaluation of an organization's systems processes and controls, is performed against a set standard or documented process. Audits are designed to provide an assessment through a qualified appraisal of the representations, which have been made concerning the system or process.	Internal	• Financial • Controls • Audit against Policy and Procedures
		External	• Audit against a Standard or legislative Requirement • Contract • Service Delivery • Application • System
Assessment	Numerous "*audits*" are provided without certification, these however are qualified reviews.	Vulnerability Assessment	• Tools Based System Scan • Vulnerability

			Analysis
		Qualified Review	• Ethical Attack • penetration test
		• Gap Analysis • Controls Assessment • Threat / Risk Assessment	
Inspection	An inspection captures the state of security at a point in time. An inspection is generally used as a part of the audit process to test controls.		
Penetration testing	A penetration test is an attempt to bypass controls and gain access to a single system. The goal of the penetration test is to determine vectors over which a system may be compromised.	• Ethical Attack • Grey Hat Verification • penetration test The nature of the testing is such that a failure to uncover any vulnerabilities does not imply that the system is secure	

Vulnerability

A vulnerability is any weakness to a system that can be triggered (either by accident or intent) to exploit a weakness in a system (NIST, 800-42).

Although it is commonly called a vulnerability, an unpatched system or "hole" does not in itself create a vulnerability. What is being noted is a potential vulnerability. Other information needs to be associated with this potential vulnerability before it may be classified as a vulnerability. There is great difference between a potential vulnerability and a vulnerability. Before this determination can be made, it is necessary to understand the system being tested.

The limited knowledge provided in blind testing or other black box test processes are seldom adequate to provide this information. Although the ethical attacker or even penetration tester may stumble across a potential vulnerability with possibly serious consequences, it is rarely likely that they will be able to determine this without additional internal information.

Threat-Source

A Threat-Source is either (NIST, 800-30):

1. Intent and method targeted at the intentional exploitation of a vulnerability, or
2. A situation and method that may accidentally trigger an exposure to a system vulnerability.

Threat

A threat is the potential for a threat-source to exercise or exploit a specific vulnerability. A threat may be either accidental or intentional in nature.

Risk

Risk is “a function of the likelihood of a given threat-source’s exercising a particular potential vulnerability and the resulting impact of that adverse event on the organization”. A risk is a probabilistic event that may be modeled quantifiably using survival and hazard functions.

Risk Management

This is the process of identifying, assessing and controlling risk. Risk management is the process where the level of risk is maintained within accepted bounds. It is not possible to mitigate all risk and cost constraints due to the economic law of diminishing returns always leave some risk.

As commerce is about risk, being that all profit is determined through the taking of risk above the base bond rate, risk will continue to exist in all aspects of business and other business aspects, including information security.

The Decision Test of the process

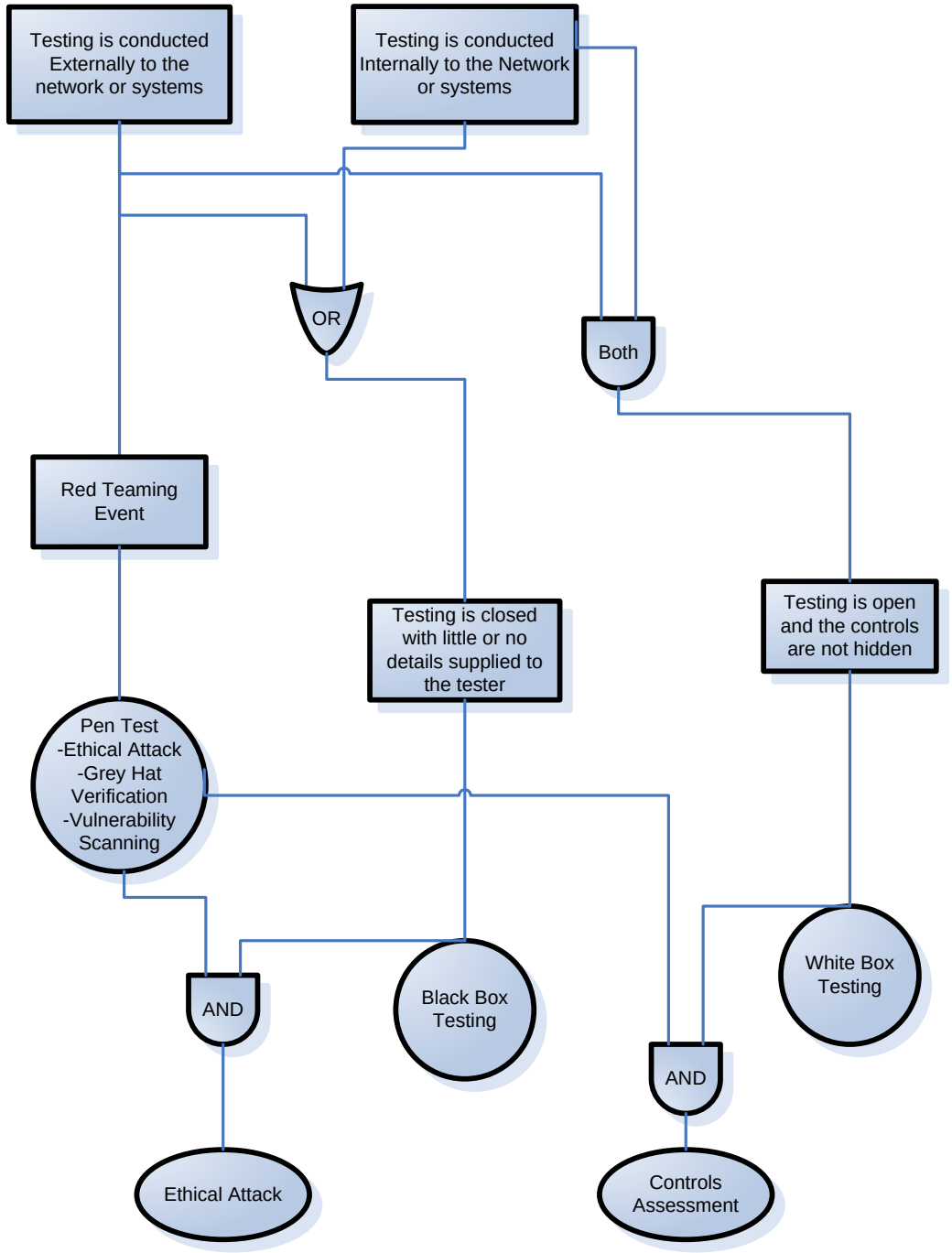

Figure 1.1 The process of deciding what you have tested and how

Controls

To have an effect on an assessment of any system, it is essential that the auditor have a good understanding of controls as applied to information systems (COSO). Controls as used within the field of information systems incorporate the policies, procedures, practices and organizational structures, which the undertaking has

implemented in order to provide for a reasonable level of assurance that their objectives will be accomplished. The controls implemented within a computer system are intended to provide an efficacy and effectiveness of operations, consistency and compliance with the laws, rules and regulations with which the undertaking needs to adhere.

There are two principal control types that the Information Systems auditor needs to be aware of and understand. These are general controls and application controls, each of which will be covered in further detail below. Controls range from the "soft" controls such as the integrity and ethical values of staff, the philosophy and operating style of management, the competence and professionalism of employees and the effectiveness of communication through to “hard” controls such as segregation of duties, network choke points and authorization processes. Soft controls are a more difficult area to assess, as there are no generally agreed and defined approaches to the conduct of an appraisal of these controls. For this reason, many auditors fail to assess them adequately.

Definition of Internal Control

The Committee of Sponsoring Organizations of the Treadway Commission [COSO] defines an Internal Control as follows:

- Internal control is a process, affected by an entity’s board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:
  - Effectiveness and efficiency of operations
  - Reliability of financial reporting
  - Compliance with applicable laws and regulations

Key Concepts

- Internal control is a process. It is a means to an end, not an end in itself.
- Internal controls are influenced by people. It is not merely policy manuals and forms, but people at every level of an organization.
- Internal control can be expected to provide only reasonable assurance, not absolute assurance, to an entity’s management and board.
- Internal controls are geared to the achievement of objectives in one or more separate but overlapping categories (COSO, Key Concepts).

When applied to Information Systems in totality as used within an undertaking, controls encompass not only the domain associated with financial reporting as used by COSO, but rather all aspects of the undertakings operations. The Key Concepts expressed within COSO surmise the wider objectives associated with Information Systems in an efficient means.

Controls (both general and application) are processes designed to deliver an objective. The auditor is chiefly concerned with the controls that provide for confidentiality, integrity and availability of information systems. From a wider view than information security, information systems controls can cover such diverse goals as systems efficiency, speed and cost effectiveness or economy. The important note to remember is that a control is a process to achieve an objective. The aim in assessing a control is to test if the undertaking can achieve its desired objective effectively.

Both general and application IT controls are designated as either "key" or "operational".

Key Controls

Key controls are those upon which the undertaking holds reliance. They warrant that objectives such as access rights, the integrity of operations and data and reporting are both valid and consistent. Key controls are at times confused with good practice. They are however not the same. A common example is the use of modular, structured and well-documented program code in application development. This is an excellent practice but is not a key control. Key controls generally require accuracy and reliability of processing. They do not for instance consider operational efficiency.

Operational Controls

Operational Controls are focused on the day-to-day operation of the undertaking to make certain that all of the undertakings objectives are achieved in the most efficient method. It is common for operational controls to slowly become an impediment to business over time and one of the key areas that needs to be monitored in both maintaining and reviewing operational controls is whether they still provide for the objectives they were intended to meet.

Systems efficiency and effectiveness are examples of the areas addressed within the scope of operational control.

General controls

General controls include the processes that are applied generically across the undertaking or in sections of the undertaking's Information Systems. Common general controls within an undertaking include both the organizational and administrative structure of the undertaking and its information systems processing areas.

Policies, operational procedures, systems standards, the availability of staff, their skill and training and the "tone from the top" given by management are just a few of the many aspects that encompass an undertakings general control framework.

The auditor needs to gain an overall impression of the controls present in the Information Systems environment. General controls form the foundation on which all other controls within the organization are built upon. If the Information Systems General controls are not sound, it is highly unlikely that the organization will be able to maintain an effective control structure or to achieve any level of system security.

In reviewing general controls, the auditors should include any infrastructure and environmental controls in the review. The adequacy of air conditioning (both for temperature and for humidity), smoke detectors or preferably fire suppression systems, well maintained power supply systems (uninterruptible power supplies,

generators, and surge arrestors) and an uncontaminated grime and particulate free situation are all controls. Even something as (seemingly) simple as orderly and identifiable electrical and network cabling all add to the continuing operation of an undertaking is Information Systems.

It is important to consider not only the logical access to a system, but also physical access controls. It is often the case that logical access to computer systems is tightly monitored and regulated, but physical access is left wide open. Considering there are many commands and settings that can be executed only from the physical console on many systems, physical controls are often of key importance.

In reviewing physical controls, it is necessary to conserve not only the individual systems but also the overall access control measures. One example of this would include the use of facility controls such as having security guards at entry gates, displayed identification badges, the logging of visitor access to a site and enclosing all servers in a secure location will aid in increasing the level of assurance one can take over an undertaking's control framework.

Application Controls

Application controls are interconnected transversely within both the transactions and data, which may be either manual or programmed. The objective of an application control is to affirm the completeness and accuracy of the records and the validity of the entries created or processed in the system.

Application controls incorporate data input validation, agreement of batch totals, hashing and control checks as well as encryption of the transmitted data for both privacy and integrity.

Application controls are not all "hard" controls. Controls for buying & developing software, policy development, management, communication, education, and change management can all come under the category of an application control.

An application control is one that it is built into and acts as an element of the business process. Thus, application controls act to ensure completeness, accuracy, business authorization and validity of processed transactions. It is important to remember that where controls are implemented in an interconnected environment, the business controls on the processes must also cover the entire range of the operation (being defined as the entire collection of business systems and processes used by this action within the application being assessed).

In assessing application controls, business process definitions need to be analyzed to ensure that they are compliant with the business controls. Often these processes are expressed within a notational format (Kramer, 2003). Some example formats include:

- BPEL - Business Process Execution Language
- BPMN - Business Process Modeling Notation
- ebXML Meta-Models
- ERM – Entity relationship models (Inc. CODD Diagrams)
- FDL – Flow Definition Language

- UML – Unified Modeling Language

IT Governance

There are various definitions of IT governance. Weill and Ross focus on "Specifying the decision rights and accountability framework to encourage desirable behavior in the use of IT." (Weill, P. & Ross, J. W., 2004)

We can compare this with the perspective of the IT Governance Institute, which develops the classifications within the keystone system where "the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives." (IT Governance Institute 2003)

Alternatively, the Australian Standard for Corporate Governance of ICT [AS8015] characterizes Corporate Governance of ICT through "The system by which the current and future use of Information and Communication Technologies (ICT) is directed and controlled. It involves evaluating and directing the plans for the use of ICT to support the organization and monitoring this use to achieve plans. It includes the strategy and policies for using ICT within an organization."

Other Terms

Objectivity

Objectivity is an independent mental attitude that you should maintain in performing any engagement – whether an audit, review or inspection. Objectivity requires you to perform in such a manner that you have an honest belief in your work and that no significant quality compromises are made.

Ethics

When auditing you have an obligation to exercise honesty, objectivity and diligence in the performance of your duties and responsibilities. An auditor must:

- Exhibit loyalty in all matters pertaining to the affairs of the client or to whomever you may be rendering a service. However, you will not knowingly be a part of any illegal or improper activity.
- Refrain from entering into any activity which may be in conflict with the interest of the client or your firm, or which would prejudice your ability to carry out objectively your duties and responsibilities. Remember, other departments are internal clients.
- Not accept a fee or gift from an employee, a client, a customer or a business associate of the client without the knowledge and consent of your firm's senior management and only when openly announced.
- Be prudent in the use of information acquired in the course of your duties. You shall not use confidential information for any personal gain or in a manner that would be detrimental to the welfare of your firm or their customers.

- When expressing an opinion, use all reasonable care to obtain sufficient factual evidence to warrant such expression. In your reporting, you shall reveal such material facts known to you, which, if not revealed, could either distort the report of the results of operations under review or conceal unlawful practice.

Act professionally at all times.

Ethics, "The Ten Commandments of Computer Ethics"

The following is a code of ethics suggested by the Computer Ethics Institute, Washington, D.C, USA. It is recommended that the IT Auditor learn this and use it as a guide in his/her duties.

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.
7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that insure consideration and respect for your fellow human being.

Planning

Adequate planning should include consideration of:

- Communication with all who need to know about the audit.
- Any personnel to be used on the assignment
- Background information on the customer.
- Work to be done and the general approach.
- The format and general content of the report to be issued.

Planning is important to ensure that results will reflect the objectives of the audit. The planning should be documented and should include:

- Establishing audit objectives and scope of work.
- Obtaining background information about what is to be reviewed.
- Determining the resources necessary to perform the audit.
- Communication with all who need to know about the review.
- Performing, as appropriate, an on-site survey to become familiar with activities and services to be reviewed, to identify areas for emphasis, and to invite client/management comments and suggestions.
- Determine how, when, and to whom results will be communicated.
- Obtaining approval of the work plan from all concerned parties.

Examining and Evaluating Information

You should collect, analyze, interpret, and document information to support your findings. The process of examining and evaluating information is as follows:

- Information should be collected on all matters related to the objective and scope of work.
- Information should be sufficient, competent, relevant, and useful to provide a sound basis for findings and recommendations.
- Sufficient information is factual, adequate, and convincing so that a prudent, informed person would reach the same conclusions as the final report author.
- Information should be reliable and accurate. Ensure that all information is correct through verification. An SRS (Simple Random Sample) or a stratified sample of the information should be verified to source to ensure accuracy.
- The auditor should ensure that all the information supplied is relevant to the particular project and is consistent with the objectives.
- When designing audit procedures and any testing techniques which are to be employed, the procedures should be selected in advance (where practicable), and subsequently expanded or altered where circumstances warrant.

A Preliminary Survey

Sufficient background information must be obtained about the client's activities before an effective program can be prepared. This is usually done through a preliminary survey in which as much information as is practicable and useful is gathered. Most of this information is obtained orally from responsible officials within the organization. It focuses on the size and scope of activities, operating practices, and internal controls. Some concurrent tests may be made during the survey phase, usually to evaluate assertions regarding operating practices.

The preliminary survey usually identifies matters warranting in-depth attention. These may include areas in which there may be weaknesses in internal controls, inefficient operations, or lack of compliance with internal policies, and legislative requirements. In some cases the policy or process itself may be ineffective and in need of updating or improvement.

After preparation the next stage is to write a 'program' that will focus on matters that are potentially hazardous to the client (either internal or external), plus any others of special interest. These specific objectives represent the framework around which a fabric of procedures is woven.

The Program, Criteria for defining Procedures

A 'program' should conform to certain criteria if it is to satisfy the overall objectives of the review/audit. When creating the review or audit program, each work step should be documented and justified. The objective of the operation and the controls to be tested must be taken into consideration when designing any test. Further, all stages and processes to be employed in the audit process should include positive instructions with a justification and reasoning for their inclusion. It is not good practice to state these processes in the form of questions without an explanation.

- The audit program should be flexible and permit the auditor to be able to use his/her judgment in order to deviate from the prescribed procedures. Further, there are instances where it may be necessary to extend the work done in this process. Any time where a major deviation from the original scope is proposed, management must be informed and the change should be documented in the Program.
- The audit program should not be cluttered with information or material from sources that are readily available. Where textual or online sources are available, it is preferable to include a reference to the external authority. An example would be a stage of a program that calls for the use of Microsoft's Baseline Analysis tool (MBSA). Rather than adding a 10-page appendix on how to run the MBSA Scanner, include a link to Microsoft's help site.
- Any unnecessary information should be avoided. Include only what is needed to perform the audit work. Do not include documents just because they are there!

The Program

Much of the information generated at this point will also serve as the introduction to the final report to the customer and should generally include the following information:

Introduction and background

The introduction should include information about the audit client. This would relate to either the external firm or even the internal department being reviewed. Any relevant information to the audit concerning the client should be included in this section of the document. This includes:

- activities,
- function,

- history and objectives
- principal locations or sites

This is included such that the personnel conducting the engagement have ready access to all information needed to understand and carry out the program.

Purpose and scope of the report

The purpose and scope of the report should be included early in the process. In particular, the scope should specify the types of services and tests that are in included and in particular, it needs to include any services or systems that are specifically excluded.

Objectives of the project

The special goals or objectives of the review should be clearly stated. In this, it is important to document the reasons why the review is being conducted and any explicit outcomes that have been determined to rely on this process.

Definition of terms

Any unique terms or abbreviations used within the report or the audited entity should be defined or explained. This is particularly important in cases where others will make use of the report (such as a report issued by the Internal Auditors, which is expected to be issued to the external audit team). It should also be remembered that reports are often supplied to parties to whom the report was not initially designed to be distributed. In some cases, company boards may take interest in these reports and it cannot be expected that all the technical jargon and terminology will be known to these recipients.

Procedures

For most audits and reviews, it is necessary to stipulate the procedures that will be followed prior to the start of the engagement. This should be done in a manner that does not restrict your professional judgment. Procedure lists should never be used as a blind checklist in a way that lessens initiative and thoroughness. It is essential to remember that the auditor adds value; otherwise, it would be just like running an automated script.

The well-tailored program should not be delayed. The tester should run develop the audit/review program immediately after he/she has completed a preliminary site or system survey.

Time management is important. Audit programs prepared too late and hence too close to a deadline are frequently flawed by gaps and inadequacies with the result that they could fail to either determine or give priority to significant issues.

There are a wide number of certifications and certifying bodies. In the course of the book we will cover many of them and the related standards. Some of the primary ones are listed below.

ISACA

ISACA (www.isaca.org) is the foremost IT audit, compliance and governance professional society. They provide frameworks, professional accreditation and guidance on audit, security, risk and governance.

CISA

CISA, or the Certified Information Systems Auditor certification is the baseline for information systems audit professionals. CISA is recognized worldwide as the leading designation for IS audit, control and security professionals. The certification is not highly technical, but ensures that the holder understands the basics of audit and compliance.

COBIT

Control Objectives for Information and related Technology (COBIT) is a framework for control over IT that fits with and supports the Committee of Sponsoring Organisations of the Treadway Commission's (COSO's) Internal Control—Integrated Framework. This is a widely accepted control framework for enterprise governance and risk management, and similar compliant frameworks. ISACA states that:

COBIT is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. COBIT enables clear policy development and good practice for IT control throughout organizations. COBIT emphasizes regulatory compliance, helps organizations to increase the value attained from IT, enables alignment and simplifies implementation of the COBIT framework.

GSNA (SANS / GIAC)

SANS (www.sans.org) have the premier technical accreditation for IT auditors. The GSNA (GIAC Systems and Network Auditor) is the most comprehensive certification for technical staff responsible for securing and auditing information systems. Auditors who wish to demonstrate technical knowledge of the systems they are responsible for auditing should consider this certification. GIAC Systems and Network Auditors (GSNAs) have been tested to show that they have knowledge, skills and abilities to apply basic risk analysis techniques and to conduct a technical audit of essential information systems.

GIAC Security Audit Essentials (GSAE) is also available for professionals entering the information security industry who are tasked with auditing organization policy, procedure, risk, or policy conformance. SANS also have a number of specialist certifications in the audit and compliance sphere such as the GIAC Certified ISO-17799 Specialist (G7799) for ISO 2700x work.

The highest level compliance accreditation is the GIAC Security Expert, Compliance (GSE-Compliance)http://www.giac.org/certifications/gse-compliance.php. Like all GIAC Platinum level certifications (GSE), this is limited to the few. The GSE-Compliance like all GSE certifications require multiple days of hands on testing covering a variety of platforms.

IIA (The Institute of Internal Auditors)

The IIA (www.theiia.org) is the professional association for internal auditors and risk advisers. They cover the gamut of risk and audit fields from financial audit to IT.

CIA

The Certified Internal Auditor is a designation for those wishing to work as internal auditors either inside a firm or in a professional services organization.

FISCAM

FISCAM, or the Federal Information System Controls Audit Manual is the standard against which FISMA (Federal Information Security Management Act) is measured. The Act requires all US Federal government agencies to handle personal information with concern for security, as specified by NIST. They must also submit an annual report to the Office of Management and Budget (OMB) describing their IT security status.

The typical reports required as part of the IT Audit process include:

- Password Aging
- User Privileges
- System Privileges
- Remote Access
- Consolidated Change Logs
- NTFS Permissions
- Role Permissions & Membership
- User Access
- Auditing Enabled

Overview

Many other standards and compliance requirements abound. We will cover these in more detail throughout the book. The key matter that this material seeks to address is that making a secure system will not only allow you to create a system that is compliant with a single standard or act, but that will demonstrate due diligence and thus show compliance with nearly any standard.

The key to security is survivability. We hope to show you how to achieve it.