

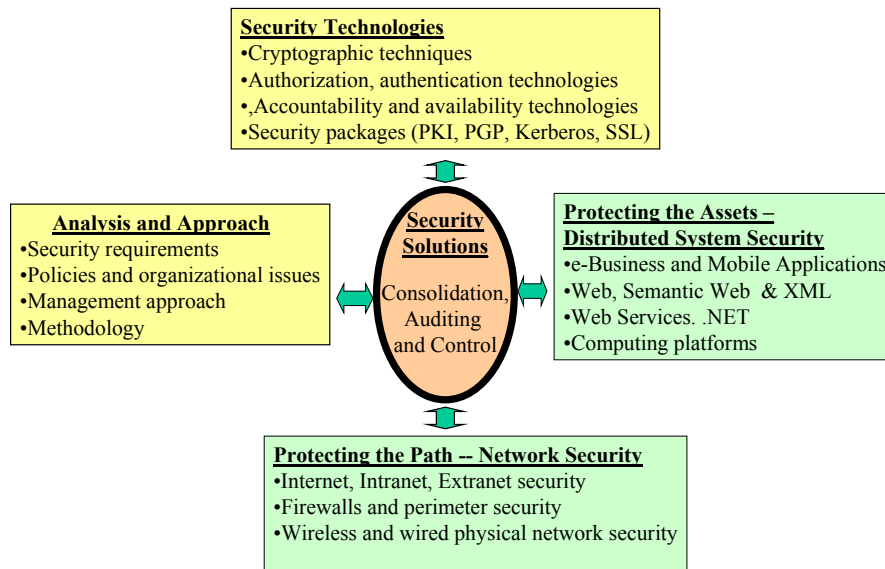
## **PART V:**

# **Putting the Pieces Together**

This part of the book concludes this book by putting all the pieces together into a solution (box with dark borders in the framework shown below).

Chapter 13: Audits and Controls for Security

Chapter 14: Building a Security Solution – The Wrapup



# 13 Audits and Controls for Security

13.1	INTRODUCTION .....	13-2
13.2	ESTABLISHING A CONTROL ENVIRONMENT .....	13-4
13.2.1	<i>Overview</i> .....	13-4
13.2.2	<i>Application Controls</i> .....	13-6
13.2.3	<i>IT Infrastructure Controls</i> .....	13-10
13.2.4	<i>Administrative and Process Controls</i> .....	13-11
13.2.5	<i>Costs and Benefits of Controls</i> .....	13-12
13.2.6	<i>Audits for Evaluating Controls</i> .....	13-14
13.3	SECURITY AUDITS – THE BIG PICTURE .....	13-15
13.3.1	<i>Introduction</i> .....	13-15
13.3.2	<i>Management Considerations in Security Audits</i> .....	13-16
13.3.3	<i>Security Policy as a Basis for Audits</i> .....	13-16
13.3.4	<i>Audit as an On-Going Process</i> .....	13-18
13.4	PREPARING AND PLANNING FOR A SECURITY AUDIT .....	13-18
13.4.1	<i>Setting Scope of the Audit</i> .....	13-18
13.4.2	<i>Gathering Information and Review of Documents</i> .....	13-19
13.4.3	<i>Develop an Audit Plan and Choose Tools</i> .....	13-20
13.5	EXECUTING A SECURITY AUDIT .....	13-21
13.5.1	<i>Getting Started</i> .....	13-21
13.5.2	<i>Interviews</i> .....	13-21
13.5.3	<i>Technical Investigations</i> .....	13-22
13.5.4	<i>The Tools</i> .....	13-22
13.6	CONCLUDING AN AUDIT – PREPARING THE AUDIT REPORT .....	13-24
13.6.1	<i>Consolidating and Analyzing the Results</i> .....	13-24
13.6.2	<i>The Audit Report</i> .....	13-24
13.7	CASE STUDY -- SECURITY AUDIT FOR THE FISH.COM NETWORK .....	13-26
13.7.1	<i>Executive Summary</i> .....	13-26
13.7.2	<i>Security Policies and Documentation</i> .....	13-27
13.7.3	<i>Network Security</i> .....	13-27
13.7.4	<i>Security Architecture and Design</i> .....	13-29
13.7.5	<i>Host Security</i> .....	13-29
13.7.6	<i>Physical Security</i> .....	13-30
13.8	SUGGESTED REVIEW QUESTIONS AND EXERCISE .....	13-31

## 13.1 Introduction

It is not enough to develop solutions once and then forget about them. Controls and audits are needed to assure *continued* secure operations. For example, suppose you

develop a highly secure solution in 2003 with the best policies, procedures, and technologies for an on-line purchasing system that supports mobile users. How do you know that the choices and decisions you have made will be followed in 2004, 2005, and 2006. In addition, how do you assure that the decisions made now are good enough and will last the technological as well as organizational changes in the next several years. Audits and controls are a good mechanism for smooth and effective operations for several years to come.

The word "audit" scares most people. The main idea of audit, in the business world, is that it is a formal evaluation of one or more components of an organization against some goals. There are different types of audits. A common example is the ever-feared income tax audit where the IRS conducts a detailed examination of your income and the taxes you have paid to assure that you have complied with the income tax laws. Another example is financial audits that are conducted to examine the financial records of a company based on traditional accounting practices to develop a clear picture of the company's financial situation.

IT audits are of particular interest to us because they determine the effectiveness of controls needed for efficient and secure operations. Proper controls, sometime needed for compliance with laws and regulations, can also be used as strategic tools to increase efficiency of processes, improve profitability of enterprises, and increase reliability of financial data<sup>1</sup>. Examples of these controls are the policies and procedures that control and restrict the access to sensitive applications, databases, and corporate network segments to minimize frauds and assaults. Section 13.2 introduces the main concepts of controls and the role of audits in evaluating controls. Although controls in IT have been around for several years, our goal is to highlight the newer issues of controls in the highly mobile technology intensive environments of the digital age.

While controls are needed to establish a secure and efficient enterprise, security audits are needed to assure that the controls are actually being used. Information security audits, introduced in Section 13.3, determine how the privacy, integrity, and availability of an organization's information is being achieved and what can be done if it is not. An information security audit is a formal assessment of how effectively the organization's security policies are being followed. There are numerous examples of companies that have well written security policies that no one follows; and then there are others with no security policies but a plethora of security technologies. The security audits formally examine and evaluate the management as well as the technical aspects of a company's security system. Due to its scope, this is not just a meeting, it involves planning, detailed investigations and interviews with key personnel, and an audit report that summarizes the findings (see sections 13.4, 13.5, and 13.6 ). A case study of a network audit concludes this chapter.

### Chapter Highlights

- Audits and controls for security are an essential aspect of security solutions.
- Controls are needed for an efficient and secure enterprise. Controls can be of

---

<sup>1</sup> Bell, T., et al, "Auditing Organizations Through a Strategic-Systems Lens", KPMG Publication, 1997

different type:

- Application controls are specific controls unique to each computerized application, such as payroll, accounts receivable, and order processing.
- IT infrastructure controls, traditionally known as “general controls”, span multiple technologies and are pervasive. They affect all applications supported by the organization's information technology infrastructure.
- Administrative and process controls are formalized standards, rules, procedures, and control disciplines to ensure that the organization's IT infrastructure and application controls are properly executed and enforced.
- New information technologies (increased use of XML, Web Services, wireless systems, and application servers) raise new control issues that have not been traditionally thought of in the past control procedures.
- Controls can increase efficiency and security of processes but controls can be expensive and frequently irritate people and lead to loss of productivity if used excessively. Some cost/benefit analysis are needed to determine which control mechanisms provide the most effective safeguards without sacrificing operational efficiency or cost.
- Organizations conduct IT audits to determine the effectiveness of controls. An IT audit identifies the controls that govern individual information systems and assesses their effectiveness.
- Security audit is special type of audit that concentrates on security. It involves an assessment of the procedures and practices of a site or an enterprise to determine the level of security risk created by these actions.
- Security audits can focus on specific applications, firewalls, hosts, networks, policies and procedures, physical support systems, and all of the above
- Security audits involve planning before the audit, execution of the audit where the necessary data is collected through interviews and experiments, and conclusion of the audit by developing an audit report.

## 13.2 Establishing a Control Environment <sup>2</sup>

### 13.2.1 Overview

Simply stated, controls represent the combination of manual and automated measures that protect information systems and ensure that they perform according to corporate policies and procedures. These policies and procedures are needed to minimize IT errors, disaster, interruptions of service, computer crime, and breaches of security. Controls consist of all the policies, procedures, standards, and methods that ensure the safety of the organization's assets, the accuracy and reliability of its accounting records, and operational adherence to corporate standards.

<sup>2</sup> This discussion is an extension and update of Laudon and Laudon, "Management Information Systems", Prentice Hall, 8<sup>th</sup> Edition, 2003 (chapter 14).

Although controls have been used in IT for a number of years, there are some differences in the digital age:

- The focus of controls in the past was on internal systems and the employees who used these systems – management was considered a “trusted party”. However, the numerous frauds incurred by managers of large corporations such as Worldcom and Enron in the early 2000s have changed all that. At present, it should be assumed that some reports being audited may be prepared by managers who are dishonest. Thus it is more important to look at internal plus external threats.
- The control of information systems in the past was an afterthought that was addressed only towards the end of implementation. In the digital age, organizations are critically dependent on information systems, thus vulnerabilities and control issues must be identified and addressed as early as possible. The control and security of an information system must be an integral part of its design and must be attended to throughout the system's life cycle.
- New information technologies (increased use of XML, Web Services, wireless systems, and application servers) raise new control issues that have not been traditionally thought of in the control procedures. Specifically (we mentioned these in earlier chapters and will revisit them again in this chapter):
  - XML and its reliance on external DTDs requires new procedure for edit checking. Not only the XML document itself, but the DTD must also be controlled to make sure that the processing is not tampered with.
  - Web Services require new controls for the services that can be directly invoked over the Internet through WSDL that is published in a UDDI.
  - Wireless networks and mobile devices present many new challenges for controls. For example, in the past it was possible to install terminals in a physically secure area for restricted access. This is simply not possible with the highly mobile workforce of today that accesses corporate information over cellular networks.
  - Application servers such as IBM's Websphere and Microsoft's .NET support many applications. These new infrastructure components need to be properly controlled.

What type of controls are needed in modern information systems? In the past, most controls were defined in terms of application specific and general controls<sup>3</sup>. This thinking needs to be refined a bit. Let us use a variant of our framework shown in Figure 13-1 once again (I hope that you are not getting tired of it!). Controls for modern information systems need to separate the application specific, IT infrastructure, and management/process specific issues (see Figure 13-2 and Table 13-1). Specifically, a combination of controls are needed that span the entire stack (from networks to the applications):

- **Application controls** are specific controls unique to each computerized application, such as payroll, inventory, accounts receivable, and order processing. They consist of controls applied from the user functional area of a particular system and from programmed procedures.
- **IT infrastructure controls**, traditionally known as “general controls”, span multiple technologies and are pervasive. They affect all applications supported by the organization's information technology infrastructure. On the whole, these controls apply to all computerized applications and consist of a combination of hardware,

---

<sup>3</sup> Laudon and Laudon, "Management Information Systems", Prentice Hall, 8<sup>th</sup> Edition, 2003 (chapter 14).

systems software, and middleware services that create an overall control environment.

- **Administrative and process controls** are formalized standards, rules, procedures, and control disciplines to ensure that the organization's IT infrastructure and application controls are properly executed and enforced. The most important administrative controls are (1) segregation of functions, (2) written policies and procedures, and (3) supervision.

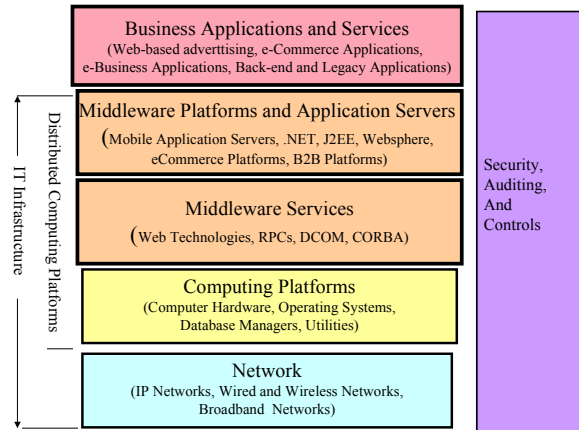


Figure 13-1: IT in the Digital Age

Table 13-1: Old Versus New View of Controls

Old Classification of Controls	New Classification of Controls
Application Controls: deal with application specific issues.	Application Controls: deal with application specific issues but with focus on increased use of XML and its variants in enterprise applications
General Controls: dealt with everything else, including administrative, IT infrastructure, and process controls.	General controls are subdivided into the following: - IT infrastructure controls - Administrative and process controls

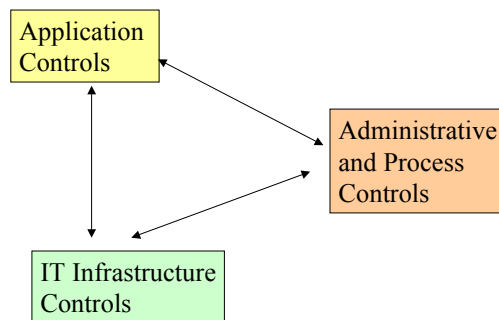


Figure 13-2: Interrelationships between Controls

### 13.2.2 Application Controls

Application controls apply to each business application, such as order processing and inventory control. The controls include automated and manual procedures that ensure

that only authorized data are completely and accurately processed by that application. For example, a control may be specified that no accountant be paid more than \$20,000 per month. This control may be enforced by programming the payroll program so that it flags any monthly paycheck higher than \$20,000 for an accountant.

The controls for each application should encompass the whole sequence of processing and are generally classified as (1) input controls, (2) processing controls, and (3) output controls. Naturally, some systems require more application controls than others, depending on the nature of the application. For example, a financial application that transfers large sums of money has many more controls than an application that prints address labels.

#### 13.2.2.1 Input Controls

These controls check data for accuracy and completeness when they are entered into the system. There are specific input controls such as the following:

- Edit checks control the input data for errors before they are processed. Input transactions that do not meet edit criteria are rejected. For example, data fields might be checked for correct format (age and zip code should not contain any alphabetic characters), valid range (age should not exceed 150 years), and required fields (credit card number must be entered for online purchasing). The edit checks can stop an online transaction from proceeding or produce lists of errors to be corrected later.
- Authorization controls to verify the authority of input providers as documents enter the computer systems. For example, control procedures can be set up to authorize only human resource department to enter payroll data.
- Data conversion controls to minimize conversion errors as data is transcribed from one form to another. For example, transcription errors in entering user addresses can be eliminated or reduced by directly reading addresses from a database instead of keyboard entries.
- Control totals can be established for input transactions. These totals may be a simple document count (e.g., counting that all 20 records for a 20 person department have been entered) or totals for some fields (e.g., total payroll should not exceed a specified limit).

#### 13.2.2.2 Processing Controls

Once data has been entered, processing controls establish that it is complete and accurate during processing. Many processing controls augment and compensate for the input control processing. Some of the processing controls are:

- Matching controls compare the input data with information held on system files. Although most matching occurs during input, more sophisticated checks and comparisons may be required during processing. For example, most online purchasing programs match the credit card information and the billing address entered by the user with the same formation in customer records before authorizing a purchase.
- Processing edits verify for reasonableness or consistency during processing. For example, consistency checks might be used by a utility company to compare a customer's water bill with previous bills. If the bill was 500 percent higher this month compared to last month, the bill would not be processed until the meter was rechecked.

- Control totals during processing reconcile the input control totals with the totals of items that have updated the file. For example, totals for monthly payroll should be compared with previous month payroll totals for sharp fluctuations if the staffing levels have not changed. Discrepancies are noted for investigation.

### 13.2.2.3 Output Controls

Output controls ensure that the results of automated processing are accurate and complete. Typical output controls include the following:

- Periodic synching and checking of outputs with actuals. For example, if a report says that the current inventory is reduced by 100 items, it is a good idea to verify that the inventory actually has been reduced by 100 and not by 500 items.
- Reviews of the computer processing logs to determine that all of the correct computer tasks executed properly and in the right sequence for processing
- Balancing output totals with input and processing totals.
- Authorization procedures to ensure that only the authorized entities (people, programs) receive the output reports, checks, or other critical documents.

### 13.2.2.4 Controlling XML-based Applications

XML is one of the most popular Web technologies at present with applications in e-commerce, finance, manufacturing, engineering, and many other areas. As discussed in Chapter 10, XML has introduced several control and security concerns. In particular, XML and its reliance on an external DTD require new procedure for edit checking. For example, a DTD can specify that a certain field is optional and thus bypass the processing of the field. Thus, not only the XML document itself, but the DTD must also be controlled to make sure that the processing is not tampered with. Consider, for example, the following DTD for the customer record we discussed in Chapter 10:

```
<!ELEMENT customer (name, address?, phone?)>
<!ATTLIST customer id CDATA #REQUIRED>
<!ELEMENT name (first, middle?, last)>
<!ELEMENT address (street+, city, state, zip)>
<!ELEMENT phone (#PCDATA)>
<!ELEMENT first (#PCDATA)>
<!ELEMENT middle (#PCDATA)>
<!ELEMENT last (#PCDATA)>
<!ELEMENT street (#PCDATA)>
<!ELEMENT city (#PCDATA)>
<!ELEMENT state (#PCDATA)>
<!ELEMENT zip (#PCDATA)>
```

In a DTD, optional fields are suffixed by a “?”. For example “address?” and “phone?” indicate that address and phone number are optional, but the name is not. A DTD parser will make sure that all XML documents that describe the customer have a name entry but will bypass the address or phone entry. But if someone changes the DTD to change a sensitive field to optional, then the DTD parser will completely ignore the field.

The concern is that intrusion of DTDs or Schema can have a very serious impact on controls. A straightforward way of controlling and securing an XML document and DTD is to encrypt it and then use some type of message digests for integrity before transmitting over the network. This can be, and is done, on a regular basis by using SSL or TLS. However, different parts of the same XML document need different levels of security and thus may need XML Encryption and XML Signatures as discussed in Chapter 10.



### 13.2.2.5 Application and Shared Data Security Controls

Application data files contain application specific information. For example, payroll files contain information used by the payroll program. In addition to application specific data, "shared corporate data" exists in corporations. This data is accessed by multiple applications and users throughout an organization. Customer and inventory files are common examples of shared corporate data. Data security controls ensure that valuable business data files, application specific or shared, are not subject to unauthorized access, change, or destruction. Such controls are required for data files when they are in use and when they are being held for storage. When data can be input on-line through a remote device, entry of unauthorized input must be prevented. For example, a credit note could be altered to match a sales invoice on file. In such situations, security can be developed on several levels:

- The use of ID/passwords can be required before anyone can log on to the system. .
- Additional sets of passwords and security restrictions can be developed for specific systems and applications. For example, database management security software can limit access to specific files, such as the files for the payroll system. It can also restrict the type of access (read versus update) so that some users will be allowed to read while others to update the file.
- Remote devices can be physically restricted so that they are available only to authorized individuals. This is, however, difficult for handheld devices. In such cases, each handheld device should have its own ID/password system with which a user cannot use the device. For example, 3G wireless devices provide strong authorization and authentication at the handset for additional security.

Security profiles can be created to allow different people different access. For example:

- Different security profiles are needed for online purchasing. A merchant needs to know a buyer's name, the items bought and shipping address but does not need the credit card information. However, the bank needs to know the credit card information but has no interest in the goods bought. Thus two different profiles should be created.
- Different security profiles are needed for medical records. A doctor or nurse may need medical details but not all personal materials such as health insurer, but a hospital administrator may need to see admission and insurer information but should be prevented from viewing medical history.
- Different security profiles can also be assigned for users of an on-line personnel database with sensitive information such as employees' salaries, benefits, and medical histories. One set of users can perform clerical functions such as inputting employee data into the system. These individuals can be allowed to update the system but can neither read nor update sensitive fields such as salary, medical history, or earnings data. However, senior managers may be allowed to read all employee data fields for their areas, including medical history and salary but not update anything.

These profiles would be established and maintained by a data security system. If XML was used in these cases, then XML encryption could be used to encrypt different parts of a document (see Chapter 10).

### 13.2.2.6 Controls on Mobile and Externally Invoked Applications

Mobile applications raise security and control concerns as discussed in Chapter 12. In particular, online transactions from handsets can result in fraud and theft and mobile users increase the chance of eavesdropping. It is especially important to pay attention to the business aware code written for mobile applications.

The mobile application controls can be discussed in terms of mobile client, Web tier, and the back-end transaction control issues. In particular, most unique issues are concerned with the mobile clients. In particular, the mobile client software needs to be controlled and protected. We discussed most of these issues in Chapter 12.

Another control issue is with applications that can be invoked externally. Web Services, discussed in Chapter 11, is an example. These services allow applications to be advertised and invoked from the Internet users directly by using UDDI and WSDL (see Chapter 11). The main control issue is that UDDI as well as WSDL could inadvertently expose some services that the company would rather not publicize. Once a service is defined as WSDL and then further advertised through UDDI, then almost anyone can invoke it. Public UDDI Registries have suffered because many services they contain are not provided or adequately supported by the service providers. Thus controls are needed before advertising a service. Approaches discussed in Chapter 11 could be used to exercise some controls.

### 13.2.3 IT Infrastructure Controls

These controls are overall controls governing the organization's information technology infrastructure. They apply to all application areas. These controls include the following:

**System Software Controls.** These controls are essential for the various categories of system software such as operating systems, utilities, compilers, database management systems, transaction management systems, and IDEs (Integrated Development Environments). System software controls monitor the use of system software and prevent unauthorized access to this sensitive asset. Proper controls of system software are important because this software is used to generate, monitor and control application programs, databases, and user accounts. Consider the following examples:

- Access to operating system libraries, such as Windows and Unix admin files, must be controlled because they show who can run in privileged mode and who cannot.
- Database management system resources, such as Oracle and SQL Server dictionaries, must be protected because they show the database schemas and authorization lists.
- IDEs, such as IBM's Websphere Studio and Microsoft's .NET Visual Studio, are used to develop software and thus must be protected from potential attacks (software generated by a suspect IDE is highly suspect).

**Middleware Controls.** These controls are essential because many mission critical applications rely on layers of middleware to operate properly. As stated in Chapter 11, an intruder can completely destroy the integrity of an application by modifying the middleware being used by the application. An intruder can potentially modify the remote messaging middleware to redirect the notifications to a suspicious site. In this case, the application code itself is not modified, only the middleware used by the application is,

but the application cannot be trusted. Middleware itself should be placed in protected areas with proper authentication and authorization controls.

**Middleware Platforms and Application Server Controls.** These controls are needed to protect the middleware components that have been packaged together by vendors for special purposes. Examples of these platforms, also known as application servers, are the e-commerce platforms such as WebSphere ([www.ibm.com](http://www.ibm.com)), Broadvision ([www.broadvision.com](http://www.broadvision.com)), and OpenMarket ([www.openmarket.com](http://www.openmarket.com)) that combine Web, mobile access, cataloging, payment, order processing and other services together for E-commerce. Thus integrity of these platforms is important for proper operation of the applications they rely on. For example, an application developed by using IBM Websphere will not work properly if Webshere itself has been compromised.

**Computer Hardware Controls.** These controls ensure that computer hardware is physically secure and can be accessed only by authorized individuals. Critical computing devices should be protected against fires and extremes of temperature and humidity. It is also important to back up processing and disk storage devices to maintain constant service. Most computer hardware at present checks for equipment malfunction and attempts to recover from errors.

**Mobile Hardware and Network Controls.** These controls need special attention because mobile devices are getting smaller and can be misplaced, stolen or lost. Such device must have a logon procedure and their loss should be reported immediately for proper actions. In general, wireless networks and mobile devices present many new challenges for control. Many of these issues are difficult to deal with. For example, in the past it was possible to install terminals in a physically secure area for restricted access. Only people walking into that room could use the terminals. This is simply not possible with the highly mobile workforce of today that accesses corporate information over cellular networks. Some controls can be used by employing, for example, infrared technology to use line of sight LANs in buildings for added controls (this is done in several military applications). For external wireless network access, the approaches discussed in Chapter 9 can be used. This, however, is an open area of research and investigation.

### 13.2.4 Administrative and Process Controls

Administrative and process controls are formalized standards, rules, procedures, and control disciplines to ensure that the organization's IT infrastructure and application controls are properly executed and enforced. Some of these controls are administrative while others are concerned with processes such as software development and computer operations.

#### 13.2.4.1 Administrative Controls

Administrative controls are internal controls that involve the following:

- **Separation of Duties.** This disperses responsibilities to multiple people to minimize the risk of errors or fraudulent manipulation of the organization's assets. For example, the individuals responsible for database management software should not be the same ones who can initiate transactions that change the values in user databases. A typical practice is to have the organization's information systems

department responsible for data and program files and end users responsible for initiating transactions such as payments or checks.

- **Proper Authorization.** This is naturally important to avoid misuse. This also includes physical controls over assets and records.
- **Written Documents, Records, Policies and Procedures.** These establish formal standards for controlling information system operations. Procedures must be formalized in writing and authorized by the appropriate level of management. Accountabilities and responsibilities must be clearly specified and recorded.
- **Supervision of Personnel.** This ensures that the controls for an information system are performed as intended. Without adequate supervision, the best-designed set of controls may be bypassed, short circuited, or neglected.
- **Other Measures.** Several other controls can be instituted for improved administrations. These include independent checks on performance, reassignments and forced leaves.

#### 13.2.4.2 Process Controls

A wide range of processes exist in modern organizations. Here is a short discussion of two that need to be controlled:

- **Systems Development Controls.** The systems development process needs to be reviewed at various points to ensure that the process is properly controlled and managed. Different system development methodologies are used by different organizations. Independent of the methodology, the systems development audit looks for the presence of formal review points at various stages of development that allow users and management to approve or disapprove the implementation. The audit should look for the use of controls and quality assurance techniques for program development; conversion; and testing and for complete and thorough system, user, and operations documentation. The systems development audit should also examine the level of user involvement at each stage of implementation and check for the use of a formal cost-benefit methodology in establishing system feasibility.
- **Computer Operations Controls.** Computer operations controls apply to the work of the computer operations department and help ensure that automated and manual procedures are consistently and correctly applied to the storage and processing of data. They include controls over the setup of processing jobs and backup and recovery of jobs that end abnormally. Specific instructions for backup and recovery can be developed so that, in the event of a hardware or software failure, the recovery process for production programs, system software, and data files does not create erroneous changes in the system. These operation procedures are difficult to design and enforce in today's highly mobile environments where sensitive data from a mainframe database can be stored on a handheld device and then sent to multiple servers at multiple sites for processing .

#### 13.2.5 Costs and Benefits of Controls

Controls can increase efficiency of processes, improve profitability of enterprises, and increase reliability of financial data. In addition, controls are necessary in many cases for compliance with laws and regulations. However, controls can be expensive and frequently irritate people and lead to loss of productivity if used excessively. If all the

control mechanisms previously discussed were implemented, they could make the system economically or operationally unfeasible. Some cost/benefit analysis are needed to determine which control mechanisms provide the most effective safeguards without sacrificing operational efficiency or cost. The following criteria could be used for understanding the tradeoffs:

- **Importance of Data.** How much control is built into a system depends on the importance of its data. Sensitive and important information such as health records and payroll data should have higher standards of control than an address list for yearly Christmas cards.
- **Efficiency Considerations.** Efficiency, complexity, and expense of each control technique must be considered before implementation of a control. For example, checking of each field may be time consuming and operationally impossible for hundreds of thousands of telephone bills. But it is quite feasible to verify only critical data such as dollar amounts and account numbers, while ignoring names and addresses.
- **Risk Mitigation.** The level of risk if a specific activity or process is not properly controlled is an important factor. For example, if an event is likely to occur no more than once a year, with a maximum of \$10,000 loss to the organization, it would not be advisable to spend \$100,000 on the design and maintenance of a control to protect against that event.

Table 13-2 illustrates sample results of a risk assessment for an on-line order processing system that processes thousands of orders per day. The various risks (physical as well as bad conduct) are listed as risks with percentages, averages and expected losses. Once the risks have been assessed, system builders can work on the control points with the greatest vulnerability and potential loss. In this case, controls should focus on ways to minimize the risk of power failures and fires. Risks and their likely impact can be qualitative (L, M, H) in cases where organizations may not know the precise probability of threats and the impact of such events.

**Table 13-2; Risk Analysis of Online Order Processing system**

Exposure	Probability of Occurrence (%)	Loss range / Average	Expected Annual Loss
Power Failure	20%	\$10,000-\$200,000 (\$105,000)	\$20,000 (approximately)
Fire	5%	\$100,000-\$1,000,000 (\$550,000)	\$21,000 (approximately)
Fraud	5%	\$1,000-\$100,000 (\$50,500)	\$2,000 (approximately)
User error	90%	\$100-20,000 (\$10,500)	\$9,000 (approximately)

To decide which controls to use, information system builders must examine tradeoffs between control techniques and their inter-relationships. A control weakness at one point may compensate for a strong control at another. It may not be cost effective to build strong and expensive controls at every point in the processing cycle if the areas of greatest risk are secure or if compensating controls exist elsewhere. It is the combination

of all of the controls developed for a particular application that determines its overall effectiveness. In some sense, it is quite similar to security design – weaknesses at lower layers (network transport) can be compensated at higher layers (middleware and applications).

### **13.2.6 Audits for Evaluating Controls**

Organizations conduct IT audits, also called MIS or EDP audits, to determine the effectiveness of controls. An IT audit identifies the controls that govern individual information systems and assesses their effectiveness. To conduct such an audit, the auditor must acquire a thorough understanding of the applications, the IT infrastructure and the administrative procedures of the organization.

During the audit, the auditor(s) usually go through numerous documents and interview key individuals who use and operate a specific information system concerning their activities and procedures. Different types of controls, ranging from application controls to administrative controls, are examined. The auditor typically traces the flow of sample transactions through the system and performs numerous tests, using automated audit software.

The IT audit produces an audit report that lists and ranks all control weaknesses and estimates the probability of their occurrence. It then assesses the financial and organizational impact of each threat. The detailed audit findings are typically organized on one-page worksheets for each discovered weakness with the following information:

- The weakness, its implications, and suggested courses of action.
- Checklists for the management to document corrective steps
- A comment block to dispute the finding if appropriate

In some case, one worksheet is prepared for related weaknesses for one area. For example, an auditor may list all control weaknesses in a loan system on a single worksheet. This type of finding can be basis for discussing weaknesses with management for corrective actions. Management is expected to devise a plan for countering significant weaknesses in controls.

It is important here to point out the weaknesses of audits based primarily on review of internal reports. An auditor should not rely solely on examining internal control reports because they could be created by people who may have different agendas. Unfortunately, many controls are created by managers who may be dishonest. Even if the audits were done correctly, the receiving management may want to hide the results. To reduce the influence of current management on audits with possibility of fraud, an external committee is usually formed to oversee the audit. The auditors report to and work directly with the audit committee during the audit.

## 13.3 Security Audits – The Big Picture

### 13.3.1 Introduction

Simply stated, a security audit is a policy based assessment of security risks. It involves an assessment of the procedures and practices of a site or an enterprise to determine the level of risk created by these actions. Although a security audit comprises a number of stages, summarized in Table 13-3, it is (should be) a dynamic and on-going examination of site methodologies and practices. An important element of security audits is ongoing communication with the key participants of an audit. The audit participants may change depending on what is being audited:

- Specific applications
- Firewalls
- Hosts
- Networks
- Policies and procedures
- Physical support systems such as fire alarms, exits, electrical power systems, and emergency systems
- All of the above

**Table 13-3: Stages of a Security Audit**

Stage of Audit	Percentage Of Total Time
Preparing for an Audit - Setting the scope - Establishing a timeline - Identifying key players	10-15%
Conducting the Audit - Reviewing Policy/Docs - Talking/Interviewing - Technical Investigation - Reviewing Data	50-55%
Concluding an Audit - Writing the Report - Report Presentation - Post Audit Actions	35-40%

The audit involves reviewing of policy documents (if any exist), interviewing, technical investigations/experiments and reviewing of data collected in logs and audit trails. On completion, the auditor(s) should have a clear idea of the risk exposure and security level of the systems that have been examined. In addition, the auditors gain insights on the compliance level of the users and systems being audited. The results of an audit are captured in a report that highlights the key findings (good news, bad news) and suggestions for improvement. The report should also pinpoint the potential damage in

case of an attack and propose a strategy to ensure minimal damage. We will review the various audit activities in the next sections.

### **13.3.2 Management Considerations in Security Audits**

Management needs to decide when and why to do a security audit, who should do the audit, what should be the frequency of audits, and who should be involved in the audits.

Security audits should be ideally part of a scheduled maintenance process with frequency of 12-24 months, 12 months, or 6 months. However, many security audits are conducted due to an emergency or after a disastrous event. For example, after 9/11, many companies embarked on a variety of security and disaster recovery audits. In addition, security audits are frequently conducted before major business events such as acquisitions and mergers. The business drivers for security audits may include, in addition to measuring policy compliance and assessing risk, estimation of potential damage and response to security and privacy laws and regulations.

Security audits can be conducted internally or by an external contractor. In either case, the auditors should have the relevant technical expertise and the interpersonal skills to deal with a very wide range of people. The ability to communicate the findings in clear and concise terms and an understanding of the organization under review are also essential. The auditor must have the required permissions to access the systems being examined, especially when the target systems are regulated and require security clearance from the government.

Although the company management typically initiates a security audit and hires the auditors, the auditors must be independent enough to suspect the very management that hired them! It is especially important for the security auditors to look beyond the IT systems and consider the users, the managers, the system administrators, the physical site, and the developers of IT. Even when the IT systems are technically secure, the people around them may be involved in shady practices. In general, the risk of attacks from internal staff increases as the value of the assets being protected increases (naturally!).

### **13.3.3 Security Policy as a Basis for Audits**

As stated previously, a security audit is essentially an examination of how effectively the organization's security policy is being implemented. When performing an audit, the auditors typically start with a security policy that the organization has as a basis for assessment. The auditors determine whether the policy document covers all the basic components of security elements – so the document should be comprehensive. Good policies that are complete and also written in plain English are very rare. A security policy is useless unless people read and understand the document. A good security policy is a complete, comprehensive and understandable document that clearly specifies:

- Who can use what resources
- Proper versus improper use of the resources
- Granting access and use with indication of when an access should expire (a consultant I know used a system three years ago and still has access to it although he did not need it after a two week consulting assignment at that time).
- System administrator privileges



- User rights and responsibilities
- What to do with sensitive information
- Desired security configurations of systems

While it is good to have a complete, comprehensive and understandable policy document, it is even better to have one. Unfortunately, it is possible to find a number of organizations where a written security policy simply does not exist. If there is no defined security policy then the auditors should start defining one or recommend that one is created after the audit is complete. The “Site Security Handbook, RFC 2196” is a good starting point to develop a security policy. Published in 1997, RFC 2196 is an update of the earlier “Site Security Handbook - RFC 1244” that was developed in 1991. This Handbook can be used as a guide by the auditor if no security policy document exists and can also serve as an example of security policy handbook to be developed by the company after completion of an audit. Another well known standard for security policies is the British Standard 7799 (see the sidebar “British Standard 7799 for Policies”). Many other documents can be found at the website ([www.auditnet.org](http://www.auditnet.org)).

Once developed, security policies should be used as a means of standardizing security practices by having them read and signed off by all employees. Security practices that are based on unwritten or informal assertions cannot be generally understood and practiced by all employees in the organization. Furthermore, compliance of the policy cannot be enforced until all employees have read and signed off on them. Written security policies are not intended to question the integrity and competency of employees; instead, they ensure that everyone at every level understands how to protect corporate assets and agrees to fulfill their obligations in order to do so.

It is easier to write policies than to follow them. Employees often choose convenience over security. For example, we all know that we should choose difficult-to-guess passwords, but then we have to remember them also. Many employees still either use simple passwords that they can remember or use contorted ones but then write them on sticky notes for quick reference. Thus good auditors check for sticky notes on the monitor and look under the keyboard for passwords. In addition, software development managers may know that local administrator accounts should be password protected; yet, they may just bypass that step in the haste to build a system. These types of weaknesses are known to the intruders and should be checked by good auditors.

It is not enough to measure security policy compliance -- the policy itself should be scrutinized. Does it accurately reflect how the organization actually protects IT assets, do the employees know about it, is it too difficult to follow or is it trivial and concentrates on irrelevant issues? It is also important to assure that the policy reflect industry standards for the type of IT resources being protected.

It is crucial to understand the risks if the policies are not specified or if they are not followed. Risk analysis, as discussed in a previous chapter, is the process of identifying and assessing the risk of something happening. Before embarking on a security audit, the security auditors should familiarize themselves with risk management and analysis concepts and tools.

### **British Standard 7799 for Policies**

This standard is internationally known for policy specifications. The standard, known as BS7799, is a set of recommendations organized in 10 major sections. These sections cover policies for areas such as business continuity planning, system access control, system development, physical and environmental security, personal security, security organization, computer and network security, and asset classification and control. For additional information, see [www.securityauditor.net](http://www.securityauditor.net).

### **13.3.4 Audit as an On-Going Process**

Companies go through audits on an on-going basis. Each audit should build on previous audits and help refine the policy and correct deficiencies that were discovered through the earlier audits. If the same deficiencies appear year after year, something is wrong with this picture. In addition to recurring threats, new threats are introduced as organizations evolve and their security structures change with the evolutions. Thus, security audit is not a one-time task, but a continual effort to improve information protection. While tools are an important part of the audit process, the audit process is more about knowing the organizational structure and finding new approaches to determine risks in the evolving digital enterprises.

## **13.4 Preparing and Planning for a Security Audit**

Security audits, especially of large scale systems, are long and arduous undertakings. Before embarking on a security auditor, a fair amount of homework and preparation is needed. Auditors need to set the scope of the audit, review the documents, prepare questions to be asked, and review tools and techniques to be used. For example, the auditors need to review the results of any previous audits that may have been conducted and also need to know the tools they will use or refer to during this audit.

### **13.4.1 Setting Scope of the Audit**

Auditors need to first work with the client to determine the scope of the audit. Good auditors clearly define scope of the audit and have it understood and agreed to by the clients before start. Factors to consider for establishing scope include:

- The business driver for audit, i.e., any specific reasons or vulnerabilities that the company is concerned about.
- The type of data being protected and the value/importance of that data to the client organization. This helps in risk analysis.
- The depth as well as breadth of the audit. Modern IT systems, as we have seen so far, consist of a large number of components, including hosts, middleware platforms, servers of different types, firewalls and the wired/wireless networks. The

auditors must decide on the number of components to be included in the audit and how deeply each component will be examined. This will help in determining the duration of the audit because some systems, by their very nature, require a greater level of scrutiny to determine the vulnerabilities.

- Record of previous security violations to determine the past problems and gauge future effort.
- The time available to complete the audit, the availability of key personnel at the site to be audited, and the talent/expertise of the auditors.

### 13.4.2 Gathering Information and Review of Documents

As part of audit preparation, the auditors review several documents. **Site survey** is one of the first documents to be reviewed. This is a technical description of the site hosts, what do they house (applications, data) and how they are interconnected. This document also includes management and user demographics. Even if out of date, this document can still provide a general framework for preparation. Another important document to be reviewed is answers to **previous security questionnaires**. The respondents to the questionnaires are typically asked to rate the controls used for access to various IT assets. These controls may include: management controls, authentication/access controls, system administration controls and procedures, connections to external networks, remote access, physical security, outsider access to systems, incident response, and contingency/disaster planning. These questionnaires are subjective measurements but are useful because they provide a general understanding of agreed-upon security practices.

Site surveys and security questionnaires are very useful to auditors for preparation plus concluding an audit. These two documents can be part of the audit report that is produced at the end of an audit. Given an opportunity, the auditor should write these documents clearly with quantifiable responses of specific requirements. They should also include special considerations such as electronic commerce, healthcare and financial record processing if appropriate. For instance, healthcare companies have special audit requirements and credit card companies have compliance templates listing specific security considerations for their products. These considerations specify network, operating system, and application security as well as physical security considerations.

In addition to the site survey and questionnaires, the auditors should review the following documents:

- Hardware/software inventory of the site and network topology showing how the sites are interconnected. This information may not be completely specified in site survey and may be available in corporate planning charts.
- Key personnel with roles and responsibilities and emergency phone numbers of key personnel. This information should be validated for recency (key personnel may have disappeared, changed jobs, moved, or left the world).
- Incident logs indicating past occurrences. Auditors, especially internal auditors, should review these logs to gain an idea of historical weak points in the organization's security profile. Auditors should also examine current conditions to ensure that repeat incidents cannot occur.
- Intrusion Detection System (IDS) and Firewall log trends. These are especially important for systems that allow Internet connections. Auditors should review these logs to determine any attempts to exploit weaknesses. This analysis may lead to

underlying reasons (such as an insecure wireless access point and faulty firewall rules).

### 13.4.3 Develop an Audit Plan and Choose Tools

An audit plan covers how will audit be executed, with which personnel, and using what tools. The plan should state the objective of the audit and contain some logistical details, such as the time of the audit, which site staff may be involved and how the audit will affect daily operations. During the audit, the auditors may need to restrict access to some of the systems under test. The plan should state that such tests will be performed out of business hours to minimize impact on day-to-day operations. The plan is discussed with the requesting agency and approved before an audit commences.

Besides the plan, it is also important to determine audit tools and environment (this information may be part of the plan). Auditors must verify that all tools used for the audit have not been tampered with. This is called the golden rule of security auditing because if the results of the auditing tools cannot be trusted, the audit is useless. To trust a tool, the easiest solution is to create a check-sum (message digest) of the file, which can be used to verify the tool later. It is also possible to create a digital signature of the tool by using PGP or PKI.

Finally, auditors should prepare key questions that security audits should attempt to answer. These questions may be answered during the discussions with staff members or other activities of the audit process. These questions should be part of the planning process and should summarize the results of the audit. Here is a sample, based on [Kapp 2000]<sup>4</sup> – we have transformed it into our PIA4 analysis framework:

Privacy and Integrity questions:

- Are there adequate cryptographic tools in place to govern data encryption, and have these tools been properly configured?
- Have custom-built applications been written with security in mind?
- How have these custom applications been tested for security flaws?
- Are the security settings for operating systems in accordance with accepted industry security practices?
- Have all unnecessary applications and computer services been eliminated for each system?
- Are these operating systems and commercial applications patched to current levels?

Authorization and authentication questions:

- Are passwords difficult to crack?
- Are there access control lists (ACLs) in place on network devices to control who has access to shared data?
- How are configuration and code changes documented at every level? How are these records reviewed and who conducts the review?

Accountability questions:

- Are there audit logs to record who accesses data?
- Are the audit logs reviewed?

---

<sup>4</sup> Kapp, J., "Security Audit", PC Network Advisor, July 2000

- How are configuration and code changes documented at every level? How are these records reviewed and who conducts the review?

Availability and continuity planning questions:

- How is backup media stored? Who has access to it? Is it up-to-date?
- Is there a disaster recovery plan? Have the participants and stakeholders ever rehearsed the disaster recovery plan?

## 13.5 Executing a Security Audit

### 13.5.1 Getting Started

The security audits typically start with an initiation meeting between the key players in the audit. In this meeting, the auditors clarify the scope of the audit, if needed, what they are going to do, and how exactly they are planning to do it. This is effectively a quick walkthrough the audit plan to answer any last minute questions, handle special requests, and make any changes before getting started. After this, the security auditors go through a series of personal interviews, examination of system settings, analyses of network access procedures, and historical files.

The main focus of all these activities is to determine how security policies - the foundation of security strategy - are actually used. During the audit, the auditors collect a great deal of data about various aspects of security through interviews, vulnerability tests of various IT components, access controls assessment, and other evaluations. Throughout this process, the auditors should follow their planned checklist, but also keep eyes open for unexpected problems and look beyond any preconceived notions or expectations. In addition, the auditors should be thorough, fair, and consistent throughout the audit.

### 13.5.2 Interviews

Interviews are a vital part of security audits. Informal discussions with staff members in addition to formal interviews can be quite revealing. To determine if the users have seen the security policy, the auditors can examine usage patterns of policy documents (electronic versions if available) and see if the users have seen and read the security policy. However, a simple question such as "do you know what is the policy for password expiration?" can yield surprising insights.

Who should be interviewed? It is clearly impossible to interview thousands of people in large corporations. But sample members from different groups who have access to the site and as a result the IT assets systems should be included. Thus some members of technical staff, "normal" system users, management, and customer groups should be on the interview list. Some of the questions to be asked in an interview are:

- What systems do you use and how frequently?
- Have you seen/read the security policy?
- What can you do that you should not be able to do?
- What you cannot do that you should be able to do?

- Could yo get root/system privileges?
- What are systems used for?
- What are the critical systems?

### 13.5.3 Technical Investigations

Auditors need to review many system logs and other data files to look for usage patterns and possible suspicious use. Many audit tools such as ISS, CyberCop or SATAN can be used to help in this task and can be pre-programmed to look for special events. In addition, the auditors should check systems against known vulnerability advisories from groups such as CERT, bugtraq, NTBugtraq and L0pht. Many of these advisories are run by the so called “white hat” hacker groups; these groups investigate common systems to look for vulnerabilities and publish this information on the Internet.

It is also important to look at the startup processes of the systems being audited to detect the processes that are not supposed to be there. Furthermore, the auditors should search the systems for applications and programs that run in a privileged state and examine them carefully. The network services should be checked for unnecessary programs. Some tools scan the source code of programs and determine the code that is not used as part of the program normal execution. This code may be suspect and should be removed from the system. In many cases, such code is un-intentionally left by the developers in the haste of completing a project, but it can be malicious code that could be invoked by an event such as time and date.

Home-grown applications should be reviewed to locate any possible developer errors that could result in a security issue. The errors to look for are those that could result in buffer overflows and backdoors. Auditors should also look for the programs that attempt to elevate themselves during execution, i.e., such as changing from running as a normal user to running as a privileged user. Many tools to study the dynamic behavior of programs are available on Unix as well as Windows platforms. These tools should be used to see how the suspect programs behave while executing.

Network audits produce massive amounts of data. In large networks, simply too many paths and options exist to defy detailed analysis. It may be necessary to reduce the size of the audit by choosing key areas and perform random spot checks. Basically, network audits require more time, thus it is important to take a more strategic position. Audits of wireless networks is virtually an uncovered ground at present.

### 13.5.4 The Tools

A large number of tools are commercially available at present to aid the system administrator. Some tools detect changes in system configurations, some test for known security issues and some monitor systems in real time, such as network sniffers. Most of these tools are available on Windows, Unix, and Linux environments. Examples of some of the tools are:

- COPS/Tiger
- Crack
- SATAN/ISS
- lsof /pff
- tcpdump

- `ipscend`

The auditors may also want to cause some problems to see how the system would behave under attack. Several commercially available tools such as ISS, NESSUS and CyberCop can launch “Denial of Service” (DoS) attacks. If no machines fail as a result of these tests, then it is a good sign. Additional tests that break into systems can also be used. However, some of the tests can potentially cause actual damage, thus they should be used carefully and sparingly.

A large amount of data is collected by these tools. This data plus the other information collected during the audit should be preserved for future reference. This data should be stored in an encrypted form because it may have some sensitive information. The information may be stored on a CD that can be distributed to authorized users.

### **Web Sites for Security Audit Information**

[www.auditnet.org](http://www.auditnet.org) - an extensive website with a large repository of audit tools, including security audit tools.

<http://packetstorm.security.com> -- a very good source of the latest security issues.

[www.rootshell.com](http://www.rootshell.com) -- source of security issue information (not kept up to date, but still useful).

[www.securityfocus.com](http://www.securityfocus.com) -- a mailing list for the discussion and announcement of computer security vulnerabilities.

[www.ntbugtraq.com](http://www.ntbugtraq.com) -- Windows platform version of the Bugtraq mailing list.

[www.cs.purdue.edu/coast/coast.html](http://www.cs.purdue.edu/coast/coast.html) -- COAST (Computer Operations, Audit and Security Technology) is a computer security research project at the Computer Sciences Department at Purdue University.

[www.ciac.org/ciac/](http://www.ciac.org/ciac/) -- CIAC (Computer Incident Advisory Capability) provides tools and advisory information.

[www.cert.org](http://www.cert.org) -- CERT (Computer Emergency Response Team) provides information regarding many security issues, including advisory information.

[www.l0pht.com](http://www.l0pht.com) -- L0pht performs testing of commonly used tools for security.

Source: Kapp, J., “Security Audit”, PC Network Advisor, July 2000

## **13.6 Concluding an Audit – Preparing the Audit Report**

### **13.6.1 Consolidating and Analyzing the Results**

The auditors conduct an outgoing briefing after the audit is complete. The purpose of this meeting is to inform management of any problems that need immediate correction and to answer any general questions from the management. The auditors are usually not in a position to provide definitive answers at this point because they need to analyze the audit data in detail. As a principle, the auditors should refrain from giving too much information in this meeting.

The auditors start the task of analyzing interview and vulnerability test results after getting back to the office. There may be a need for a quick meeting between the auditors to help focus and resolve any differences of opinion between the auditors. During this meeting, the auditors develop a schedule for report preparation, assign responsibilities, and identify problem areas and possible solutions. The output of this meeting may be the detailed format of the audit report and who will write what sections. Independent of the format, the audit report should be simple and direct, containing objective findings and effective ways to correct the discovered deficiencies. The audit staff should also prepare the report as quickly as possible so that the auditing company can promptly correct the problems discovered during the audit. It is usually best to develop the executive summary first so that the management can be briefed as soon as possible.

After the audit report has been written and presented, all responsible personnel should meet to discuss any action items that may arise. Each action item should be assigned a person responsible with a due date. Urgent action items should be naturally addressed quickly before the company falls prey to the security problems identified.

### **13.6.2 The Audit Report**

The large amount of information accumulated during the audit is consolidated and presented in a report which explains the key findings clearly to the intended audience. The audience may consist of board members, MIS/IT managers and IT staff of the target company. Due to the mixed audience, the audit report should be written in a simple and direct manner with clear discussion of findings and the ways to correct the deficiencies. It is important to capture the strengths as well as deficiencies of the audited company in the executive summary for an overall balanced view. It is a good idea to develop the executive summary first and share it with the management soon after return. However, this should not be done too hastily to avoid false alarms and rejoicing.

The audit report, approximately 20-100 pages in length, can follow different formats (most auditing firms have their own report templates) but generally start with executive summary, followed by detailed findings and supporting data. The report should be structured so that the level of technical detail increases as the report proceeds. Thus everything the managers need to know should be in the first few sections of the report (typically a quarter of the report). Since most managers do not need to know the technical details, these sections should be presented in clear and non-technical manner. A possible format of the report may be as follows:

- Executive summary



- Scope of the audit and main recommendations
- Main body of the report with detailed information
- Final conclusions and detailed recommendations
- Appendices

The executive summary should be limited to one or two pages, and should highlight the strengths as well as deficiencies of the audited company. The focus of executive summary should be on the *results* and implications of the results. Any process issues such as how the audit was conducted should be ideally postponed to a later section, unless needed. The purpose is to capture the key findings and help the management to take appropriate actions.

After the executive summary, the scope of the audit should be explained and main recommendations should be listed in a prioritized manner. The purpose is to clearly state the scope and reasons for doing the audit and give a brief overview of the systems audited. If applicable, it should also highlight changes in security since the last audit if any, and should mention the compliance status of the organization to published policies. It is also relevant to briefly discuss the tools and methods that were used in the audit and what was discovered as a result. In some case, especially in small audits, this section can be included in the executive summary.

After the first two management sections, the auditors provide detailed report based on audit checklists. This is the main body of the report and should be complete and educate the reader. It should explain and defend, with technical details where necessary, all the recommendations and claims with the evidence gathered during the audit. Here are some hints and suggestions:

- The audit findings should be organized on one-page worksheets for each discovered problem. The worksheet should describe the problem, its implications, and suggested courses of action. The worksheet should be as complete as possible and should discuss the specific tools and methods that were used. This is quite helpful to the audited company because one or more sheets can be assigned to managers for action. It is a good idea to provide specific checklists on the worksheet for the site to document corrective steps and a comment block to dispute the finding if appropriate. The worksheets can be clustered by the type of audit, i.e., worksheets from host audit, worksheets from network audit, etc.
- If there have been previous audits, then compare/contrast this audit with the previous audits. It is important to explain if the problems identified in the previous audit were fixed and whether the policy was changed to reflect the problems. If previous problems were not fixed, why not and what needs to be done.
- The problems should be broken into smaller pieces with details of what was looked at and why it was reviewed. Were any new problems found, what were they, and how they were found (new tools, interviews, accidental discoveries). When breaking problems into smaller pieces, it is a good idea to decompose them in terms of audit categories such as host-level and network-level security.

The final conclusions and detailed recommendations section integrates the executive summary and the main body into a clear and coherent message. The total system level of security should be graded and detailed recommendations should be prioritized and summarized. The audited company should be given an opportunity to further investigate and question the results of the findings. Thus details of the collected audit data (where it

is stored and how it can be accessed) should be given and the main contact names for further discussion should be provided.

The appendices should include details that could not fit into the main report. They may include details about tools used during the audit, relevant technical details of the systems or networks examined, significant outputs from audit tools, lists of important security patches used in the audits, and other relevant details. A bibliography of suggested reading of books, articles, and Websites should also be included.

## **13.7 Case Study – Security Audit for the Fish.com Network**

**Note:** This is an abbreviated version of the security audit of the fish.com computer network conducted by Dan Farmer and Wietse Venema in April, 1996 (it was discussed in a one day security audit seminar in 1996). The discussion in this section abbreviates and follows the structure of the 34 page security audit report. Full version of this case study and two other case studies, along with other course materials are posted at the Website (<http://www.porcupine.org/auditing/>). Although fish.com has disappeared as a company and the network being audited is somewhat old, this is a good example of security audit reports.

### **13.7.1 Executive Summary**

The fish.com network in 1996 was a small network (between 4-6 hosts) connected to the Internet by a wireless router. Its primary mission was to provide a stable security research platform, a Web server and development platform, and a place for about 35 accounts to connect and interact with the Internet. Fish.com was often subject to probes or attacks and had been broken into several times, but never had an official security audit before April, 1996. The general security philosophy was to try and keep intruders off of the fish.com hosts; if they would succeed in penetrating the defenses, it was assumed that root access was going to be obtained.

The audit examined all significant facets of the fish.com network that would affect its security including host and network security, physical security, documentation (including the security policy), any special or unusual network daemons, home-grown programs, or network services running, and finally the overall security architecture of the network.

The major problems found in several different areas of the fish.com network were:

- A poor security policy and a general lack of security guidelines and written documentation
- Weak host security, file permissions, limited security patches, etc.

A serious but relatively easy to fix problem was found in a CGI script that was accessible via the Web - it allowed an arbitrary user to execute an arbitrary program (as user nobody) on flying.fish.com, the main fish.com machine. Additional problems were found but are not listed here.

The fish.com network had inconsistent security and fell below its own modest policy standards. Intruders could gain access to the hosts on the network by exploiting holes and

problems that were fairly trivial to exploit, mostly left there by careless or sloppy system administration work, which, in turn, was aggravated by a lack of procedural guidelines, security policies, or documentation.

### 13.7.2 Security Policies and Documentation

**Summary.** The fish.com network had a very simple security policy that needed revising. On the positive side, the policy did inform users of their very basic responsibilities (including no sharing of accounts or passwords, admonishing them not to abuse or look at private files of other users, etc.) and how to contact the system staff in case of emergency. The following table summarizes the evaluation of security policies in terms of how well they clarify who can use the resources, what is the proper use, etc.

Table 13-4: SECURITY POLICIES EVALUATION

Evaluation Parameters	Evaluation (5 being best, 0 worst)
Who can use resources	4
Proper use	2
Granting access and use	3
System Administrative privileges	1
User rights & responsibilities.	2
Sensitive information	2

**Recommendations.** While the entire policy could be reworked, the following items would be an acceptable start towards a good security policy. In order of importance:

- Inventory and codify what the various systems do and give each of them a brief security configuration, stating (at least) what is absolutely necessary or what is absolutely not allowed
- List the security tools used to monitor the system, give a schedule of how often they are to be run, and describe who is responsible for resolving their output
- Give sharper definition as to what the system administrators can and cannot do
- Keep the policy updated, as well as inform users of changes to the policy, so they'll be informed as to the current policy
- List all the users on the host and state the reason why they have an account and what hosts they're allowed to log in from
- Document and map out the network

### 13.7.3 Network Security

**Summary.** Figure 13-3 shows the Fish.com network configuration as it existed in 1996. The LAN communicated with the Internet via an encrypted wireless router and utilized Ethernet for local communication. There were four hosts, a CISCO router, and three small hubs making up the basic network. Flying.fish.com and bi.fish.com were Sun SPARCstation UNIX machines and were the general user machine and nameserver, respectively. Tuna.fish.com was a PC running Windows 95. Angel.fish.com was another

SPARCstation that was not directly connected to the Internet. Network packets were delivered unfiltered to all systems attached to the local network. Human visitors could bring along their own machines (typically portable PC's or UNIX boxes) and plug them directly into the fish.com network.

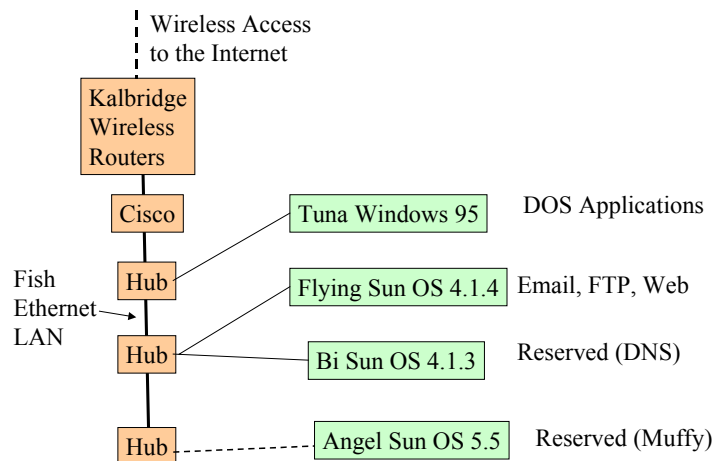


Figure 13-3: Fish.com Network

In general, network services were fairly secure. The most dangerous services (NFS, the r-cmds, etc.) had been disabled, and most unused services were not activated. Network logins were allowed only from selected sites (this was accomplished with the TCP wrappers) and one-time passwords were required for logins from non-local hosts.

Problems did exist, however. The most serious was that flying.fish.com, the Web server, had a CGI script that passed uncensored data to /usr/ucb/mail, hence allowing external users to execute arbitrary commands (as user nobody) on the system. In addition, packet screening and IP spoofing countermeasures were not taken, even though existing hardware (the routers and the Sun machines) could easily perform this task.

The following table summarizes the evaluation of network security in terms of email, name services, etc.

Table 13-5: NETWORK SECURITY EVALUATION

Evaluation Parameters	Evaluation (5 being best, 0 worst)
Anonymous Services	1
General Network Services	4
Mail	4
Name Services	3
Network Access Control	2
Security Patches	4
Trust	5
Windowing Systems	4

**Recommendations.** Network security would be improved if the fish.com network could:

- Fix the flawed httpd CGI script dforder.pl
- Install packet screening and anti IP spoofing measures

In addition, the network security of fish.com would be greatly improved if the nameservice problems were taken care of and the ability for users to ftp from anywhere on the network was removed.

#### 13.7.4 Security Architecture and Design

**Summary.** Fish.com's security architecture was relatively simple. The network, and how it interacted with the individual hosts dictated the protection scheme used. Almost no trust was allowed -- remote commands were disabled -- there were no live modems or other network connections attached to any machine. One-time passwords were required to log in from the Internet. Angel.fish.com was a potential problem, however, since it was mostly treated internally as a machine off of the Internet. Bi.fish.com was mostly a relic and could be decommissioned or stripped bare. The following table summarizes the evaluation of security architecture in terms of basic design, trust and connectivity.

Table 13-6: SECURITY ARCHITECTURE & DESIGN EVALUATION

Evaluation Parameters	Evaluation (5 being best, 0 worst)
Basic Design	3
Trust	5
External Connectivity	5

**Recommendations.** The fish.com network should:

- Install a packet filter between the LAN and Internet
- Treat angel.fish.com as a machine on the Internet
- Move DNS to flying.fish.com

#### 13.7.5 Host Security

**Summary.** The fish.com UNIX hosts (the PC was not tested) had inconsistent and fairly poor host security. There were many important files that had poor file permission modes and several security patches could be installed. On the positive side, the user level authentication methods were excellent, and the individual users' account security were very good. The following table summarizes the evaluation of host security in terms of authentication, security patches, user security, and others.

Table 13-7: HOST SECURITY EVALUATION

Evaluation Parameters	Evaluation (5 being best, 0 worst)
Auditing and Logs	1
Authentication	4
Filesystem	4
Security Patches	3
User Security	2

**Recommendations.** A number of repairs must be done to the fish.com systems to make it more secure. In addition, flying.fish.com could be made more secure through security patches. Details of this patches are not given here.

### 13.7.6 Physical Security

**Summary:** Fish.com resided on the second floor of a building in a fairly typical San Franciscan condominium. A large number of people (visiting friends and acquaintances), both regular users and not, could get physical access to the machines, as could a house cleaning person who came every other week. It would be fairly simple to gain access to the machines by approaching via the backyard (up the fire escape), the roof (the building had two adjacent buildings that gave roof access), or from one of the neighboring condominiums; the back sliding glass doors were often left unlocked. The machine rooms (i.e. bedrooms and living room) all had heat activated water sprinklers, and a dry chemical ABC fire extinguisher was easily accessible from any room. Simple surge protectors were on all the computers, but there was no UPS. Backups were done sporadically, not organized very well, and were kept on shelves scattered about the house. The following table summarizes the evaluation of physical security in terms of physical access, disaster, backup, and others.

Table 13-8: PHYSICAL SECURITY EVALUATION

Evaluation Parameters	Evaluation (5 being best, 0 worst)
Physical Access	2
Disaster	2
Resistance & Recovery	0
Physical Authentication	4
Backups	1

**Recommendations:** Several steps that might be normally suggested to improve physical security could not be practically suggested because the company was located in a home. However, there were several fairly simple measures that could be taken that would increase the physical security situation without changing the location:

- All the computers should run a screen locking program

- Keep the backdoors locked
- Put backups in a locked fireproof box
- Save old backups off-site
- Keep the cats from sleeping on the monitors

### Sources of Additional Information

Books and articles:

- Bell, T., et al, "Auditing Organizations Through a Strategic-Systems Lens", KPMG Publication, 1997
- Andress, M., "Surviving Security", SAMS Books, 2002 (Chapter 16).
- Kapp, J., "Security Audit", PC Network Advisor, July 2000
- Venema, W. and Farmer, D., "Security Auditing and Risk Analysis", One Day Seminar, April 30th, 1996, <http://www.porcupine.org/auditing/>
- Bill Hayes, "Conducting a Security Audit: An Introductory Overview", May 26, 2003, <http://www.bitwise.net/iawww/it.htm>

Some good sites for security auditing information:

- [www.auditnet.org](http://www.auditnet.org)
- [www.security-audit.com](http://www.security-audit.com)
- [www.itaudit.com](http://www.itaudit.com)
- <http://www.bitwise.net/iawww/it.htm>

The following two documents from ([www.securityfocus.com](http://www.securityfocus.com)) may be also of value:

- "Introduction to Security Policies (Four-Part series)", Charl Van der Walt, Security Focus.
- "Assessing Internet Security Risk (five-part series)", Charl Van der Walt, Security Focus

## 13.8 Suggested Review Questions and Exercise

- 1) What are different types of audits and how is security audit different from the others?
- 2) What are the main control issues that are different in modern digital enterprises? What type of approaches can be used?
- 3) What are the main considerations in application controls? Which ones are new and different in the digital age?
- 4) What are the main considerations in IT infrastructure controls? Which ones are new and different in the digital age?
- 5) What are the main considerations in administrative and process controls? Which ones are new and different in the digital age?

- 6)** What are the main steps in a security audit? Draw a flowchart that shows the input/output of each.
- 7)** Why is audit preparation important? What are the goals of this effort?
- 8)** What are the most important steps in security audits and why?
- 9)** What are the main considerations in preparing an audit report?
- 10)** Find a security audit report that deals with some of the more recent control issues.