

IT Handbook Presentation Information Security Booklet

Visual

Narrative

1.

IT Handbook Presentations

**Information Security
Booklet Overview:
Part 1**



Short Music Open

2.

What's changed?



The Information Security Booklet contains more than four times the information in the security section of the 1996 IS Handbook.

3.

Information Increase

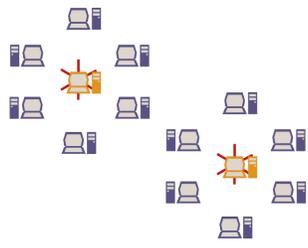


Why such a drastic increase in information?

Well, information security concerns have changed a lot in recent years. For example, most institutions once stored data on mainframes accessed by dumb terminals, which limited access to the institution's employees.

4.

Distributed Systems



But, the tremendous growth of networks and electronic banking has changed the nature of security threats—triggering a need for new and more robust security controls.

Visual

Narrative

5.



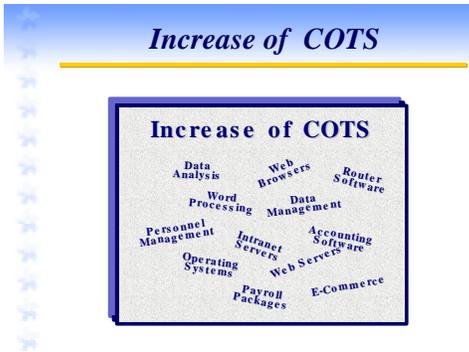
Now the world is wired, and there's been an explosion in the number of people outside of the institution who have potential access to enterprise data. There are now some one hundred and fifty million Internet users in the US alone, and that number is growing at a rate of some two million new users every month. External access opens a completely new class of threats to institutional data.

6.



Even the nature of the software used to process data in financial institutions has introduced new vulnerabilities. In the mainframe era, financial institutions primarily used custom-built software products—products produced solely for financial institutions. In that environment, an institution's precise security needs could be analyzed as part of system development and, customized security controls could be built directly into the software. Other software, such as an operating system, was likely selected with security in mind.

7.



Since 1996, financial institutions have dramatically increased their reliance on commercial-off-the-shelf, software, (COTS)—Generic software that wasn't necessarily designed to provide high-assurance security within a given operating environment and can add yet another layer of vulnerability.

8.



The same is true with networking protocols and other communication software, which are an integral part of the distributed information systems in today's financial institutions.

	Visual	Narrative
9.	<p><i>New InfoSec Risks</i></p> <ul style="list-style-type: none"> - Distributed systems - Increased connectivity - Reliance on off-the-shelf software 	<p>Distributed systems! Increased connectivity! Reliance on off-the-shelf software!</p> <p>The result? Institutions are now forced to rely more and more on...</p>
10.	<p><i>New InfoSec Risks</i></p> 	<p>software, systems, and protocols that introduce a diversity of security risks, risks that are growing rapidly. From identity theft to privacy regulations to institutional fraud, information security is by all measurements an important issue.</p> <p>This situation demands higher and higher sophistication in the risk management programs that protect enterprise data.</p>
11.	<p><i>Booklet Content</i></p> <ul style="list-style-type: none"> - Focuses on risk management 	<p>The Information Security Booklet describes an information security process with risk management components to address these new risks as well as traditional security risks.</p> <p>While specific security-related hardware, software, and controls will vary from institution to institution and change over time, it's sound risk management that will provide long-term security.</p>
12.	<p><i>Booklet Focus</i></p> 	<p>The Information Security Booklet focuses on these risk management issues rather than on providing information about product-specific security configurations.</p> <p>While such technical information is necessary in conducting effective IT examinations, it is not the primary purpose of the booklet, so the weight of the content is on process-related risk management issues.</p>

Visual

Narrative

13.

Focuses on risk management

Aimed at mid-level IT examiners



The Information Security Booklet assumes readers possess an intermediate level of technical knowledge as it relates to security software, hardware, protocols, and controls. The workprogram is designed to assist examiners in conducting risk-based examinations of moderately-complex to complex IT environments.

14.

Booklet Characteristics

Focuses on risk management

Aimed at mid-level IT examiners

Designed as a reference

Also, the booklet is designed as a reference for assessing the security program of a particular financial institution and not as a tool for conducting penetration tests or auditing specific security controls.

15.

Gramm-Leach-Bliley Act

Section 501(b)

(b) FINANCIAL INSTITUTIONS SAFEGUARDS.—In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards—

(1) to insure the security and confidentiality of customer records and information;

(2) to protect against any anticipated threats or hazards to the security or integrity of such records; and

(3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

Another factor that played a significant role in the development of the Information Security Booklet is the Gramm-Leach-Bliley Act.

When the Act was signed in 1999, it resulted in the need for the five regulatory agencies to work closely in developing guidelines to meet requirements set forth in section 501(b) of the Act. During this time, the five agencies agreed that a more comprehensive security guidance was needed—one that went beyond a consumer focus of the Gramm-Leach-Bliley Act to also address financial institution and commercial customer records.

16.

Booklet Characteristics

Focuses on risk management

Aimed at mid-level IT examiners

Designed as a reference

Builds on 501(b) processes

The Security Booklet is designed to meet these needs and to build on the 501(b) guidelines by providing additional and more detailed explanations of sound security-process elements.

The booklet development team also saw the revision process as an opportunity to correct another problem...

Visual

Narrative

17.



that of inconsistent security among financial institutions and service providers.

Since the data and potential risks are the same, security should not be a function of where the data is held. The security process should be applied uniformly across organizational boundaries.

18.

Booklet Characteristics

- Focuses on risk management
- Aimed at mid-level IT examiners
- Designed as a reference
- Builds on 501(b) processes
- Supports consistent guidance

Therefore, agencies have developed information security guidance that can be consistently applied to both financial institutions and their technology service providers.

Now that we've looked at some of the general goals and characteristics of the Information Security Booklet, let's take a look at the content.

19.

Booklet Narrative

- Introduction
- Security Process
- Information Security Risk Assessment
- Information Security Strategy
- Security Controls Implementation
- Security Testing
- Monitoring and Updating

After a brief introduction, the narrative defines the security process and covers five issues related to examining the security of data in financial institutions:

- Information security risk assessment,
- Information security strategy,
- Security controls implementation,
- Security testing, and
- Monitoring and updating.

The introduction establishes the risk-management approach of the booklet and depicts "truly effective information security" as a continuous integration of processes, people, and technology to manage risk.

20.

InfoSec Objectives

- Availability
- Integrity
- Confidentiality
- Accountability
- Assurance

The objectives of effective information security are:

- Availability,
- Integrity,
- Confidentiality,
- Accountability, and
- Assurance.

	Visual	Narrative
21.	<p>Booklet Narrative</p> <ul style="list-style-type: none"> - Introduction - Security Process - Information Security Risk Assessment - Information Security Strategy - Security Controls Implementation - Security Testing - Monitoring and Updating 	<p>The second section defines “security process” as the method an organization uses to implement and achieve its security objectives.</p>
22.	<p>Security Process</p> <ul style="list-style-type: none"> - Information security risk assessment - Information security strategy - Security controls implementation - Security testing - Monitoring and updating 	<p>The process is outlined to include five areas:</p> <ul style="list-style-type: none"> ▪ Information security risk assessment, ▪ Information security strategy, ▪ Security controls implementation, ▪ Security testing, and ▪ Monitoring and updating.
23.	<p>Booklet Narrative</p> <ul style="list-style-type: none"> - Introduction - Security Process - Information Security Risk Assessment - Information Security Strategy - Security Controls Implementation - Security Testing - Monitoring and Updating 	<p>And, it is these five topics that provide the framework for the remainder of the booklet narrative. That is, there is one section on each of the issues listed here. Let’s take a brief look at the content in each of these sections.</p>
24.	<p>Booklet Narrative</p> <ul style="list-style-type: none"> - Introduction - Security Process - Information Security Risk Assessment - Information Security Strategy - Security Controls Implementation - Security Testing - Monitoring and Updating 	<p>Risk assessment is the process by which an institution identifies what needs to be done to achieve sufficient security. It involves identifying and analyzing threats, vulnerabilities, attacks, the probability of the attacks occurring, and probable outcomes.</p> <p>Risk assessment is the key driver in the information security process. This section of the booklet focuses first on the functional requirements for an effective security-risk-assessment program.</p>

	Visual	Narrative
25.	<div style="border: 1px solid blue; padding: 5px;"> <p style="text-align: center;"><i>Risk Assessment Functions</i></p> <ul style="list-style-type: none"> – Gathering information – Analyzing information – Prioritizing responses </div>	<p>There are many acceptable risk assessment methodologies that a financial institution can use, as long as the methodology covers the key functions of:</p> <ul style="list-style-type: none"> ▪ Gathering Information, ▪ Analyzing Information, and ▪ Prioritizing Responses.
26.	<div style="border: 1px solid blue; padding: 5px;"> <p style="text-align: center;"><i>Key Aspects of Assessment</i></p> <ul style="list-style-type: none"> – Multidisciplinary and knowledge-based – Systematic and central controlled – Integrated Process – Accountable activities – Documented – Knowledge-enhancing – Regularly updated </div>	<p>The Information Security Risk Assessment section then discusses key aspects that examiners should consider when looking at a particular program. These aspects are:</p> <ul style="list-style-type: none"> ▪ Multidisciplinary and knowledge-based (requiring a consensus evaluation by a broad range of users with a variety of expertise and business knowledge); ▪ Systematic and centrally controlled (ensuring standardization, consistency, and completeness of risk assessment policies and procedures); ▪ Integrated with other parts of the security process (linking the selection and implementation of security controls with the timing and nature of testing); ▪ Accountability activities (placing operational responsibility on appropriate members of the management team, and holding senior management and the board accountable for the overall adequacy of the security program. ▪ Sufficiently documented (including assessment process and procedures, risks identified and accepted, and risk mitigation decisions made); and ▪ Knowledge-enhancing (increasing management's knowledge to enable rapid response to future changes in technologies, new types of threats, and new regulatory requirements)? <p>Finally, effective risk assessment should be...</p> <ul style="list-style-type: none"> ▪ Regularly updated (evolving as new information effecting information security risks is identified) <p>Senior management should review their entire risk assessment process at least once a year and ensure that new relevant information has been appropriately considered.</p>

Visual

Narrative

27.

Booklet Narrative

- Introduction
- Security Process
- **Information Security Risk Assessment**
- Information Security Strategy
- Security Controls Implementation
- Security Testing
- Monitoring and Updating

Once management of a financial institution has completed a sound risk assessment by gathering and analyzing information and prioritizing responses, it needs to develop a strategy to address the identified risks.

28.

Booklet Narrative

- Introduction
- Security Process
- Information Security Risk Assessment
- **Information Security Strategy**
- Security Controls Implementation
- Security Testing
- Monitoring and Updating

The next section in the booklet addresses this issue. A financial institution's information security strategy is a plan to manage the risks identified in the risk assessment.

29.

Plan Components

- **Technology**
- **Policies**
- **Procedures**
- **Training**

That plan should integrate technology, policies, procedures and training and include:

30.

Plan Strategies



- Cost Comparisons



- Layered Controls



- Implementation Policies

- Cost comparisons among approaches that might be appropriate to the institution's particular environment and complexity,
- Layered controls that establish multiple control points, and
- Policies that guide the control implementation process.

Visual

Narrative

31.

Booklet Narrative

- Introduction
- Security Process
- Information Security Risk Assessment
- Information Security Strategy
- **Security Controls Implementation**
- Security Testing
- Monitoring and Updating

Discussion of Security Controls Implementation is by far the major portion of the Information Security Handbook. We will take a look at that information in part two. This part of the security process is where all of the analysis and planning actually goes into play, where an institution:

32.

IT Handbook Presentations

Information Security Booklet Overview: Part 2



Short Music Open

The security-controls-implementation part of the security process is where all of the analysis and planning actually goes into play, where an institution:

33.

Security Controls Implementation

- **Technology**
- **People**
- **Process**

- Acquires and installs the technology,
 - Assigns duties and responsibilities and trains staff, and
 - Puts its security program into practice.
- Let's take a look at the topics this section covers.

Visual

Narrative

34.

Security Controls Implementation

- Logical and Administrative Access Control
- Physical Security
- Encryption
- Malicious Code
- Systems Development, Acquisition, and Maintenance
- Software Development and Acquisition
- Host and User Equipment Acquisition and Maintenance

Security Controls Implementation

- Personnel Security
- Electronic and Paper-based Media Handling
- Logging and Data Collection
- Service Provider Oversight
- Intrusion Detection and Response
- Business Continuity Considerations
- Insurance

As compared to the nineteen-ninety six IS Examination Handbook; the fourteen topics in this section reflect a significant increase in both the variety and the volume of technologies discussed.

As shown here, most of the content is new, reflecting technology, process, and implementation changes since publication of the earlier handbook.

Users will find:

- More detail on topics such as encryption and passwords
- New topics such as malicious codes, and an
- Increased emphasis on issues such as logical access.

What users will not find in this section are details on how to evaluate specific virus software or how a particular server should be secured. To the contrary, the section emphasizes what issues are important for an institution to consider when making these types of technical decisions.

For example, the institution's password policy, how it was developed, how it is enforced, and is it appropriate for the technologies in place in that institution. These issues are important considerations for any technology that relies on passwords. Keep in mind that the booklet, and in particular this section, is intended as a resource. The significance of each of the topics to an examination will vary, depending on the scope of the exam and the environment of the institution under review.

35.

Physical Security

Action Summary:
 Financial institutions should define physical security zones and implement appropriate preventative and detective controls in each zone to protect against the risks of:

- Physical penetration by malicious or unauthorized people,
- Damage from environmental contaminants, and
- Electronic penetration through active or passive electronic emissions.

Action Summaries within the fourteen topics provide a high level overview of the content in each topic and subtopic. For example the Physical Security Action Summary states that "Financial institutions should define physical security zones and implement appropriate preventative and detective controls in each zone to protect against the risks of:

- Physical penetration by malicious or unauthorized people,
- Damage from environmental contaminants, and
- Electronic penetration through active or passive electronic emissions."

Visual

Narrative

36.

Booklet Narrative

- Introduction
- Security Process
- Information Security Risk Assessment
- Information Security Strategy
- **Security Controls Implementation**
- Security Testing
- Monitoring and Updating

In final analysis, each of the topics in this section, along with the multiple subtopics, provide you with a broad range of resources for conducting exams in various types of institutions.

37.

Booklet Narrative

- Introduction
- Security Process
- Information Security Risk Assessment
- Information Security Strategy
- Security Controls Implementation
- **Security Testing**
- **Monitoring and Updating**

Security Testing and Monitoring and Updating! Now, let's take a brief look at these two sections before moving on to the workprogram.

38.

Security Testing



Institutions need strong testing programs to assure that potential security risks have been accurately assessed and sufficiently mitigated. That is, ...

39.

Security Testing

- **Appropriate**
- **Comprehensive**
- **Performing as intended**
- **Tested as appropriate**

TEST RESULTS

are the controls implemented:

- Appropriate for the institution,
- Sufficiently comprehensive
- Performing as intended, and
- Tested at an appropriate frequency?

The greater the risk, the greater the need for the assurance provided by a sound testing program. Appropriateness, comprehensiveness, and frequency needed in a specific institution are all related to the risks that the institution faces. The testing plan should be driven by the institution's risk assessment.

Visual

Narrative

40.

Range of Tests



There are many types of security tests, from password crackers to scanners to social engineering, and a range of tests may be necessary to gain a complete picture of control effectiveness. Management is responsible for selecting and designing these tests so that the results, in total, support conclusions that the institution's security-control objectives are being met.

41.

Variety of Testers



Many individuals within the institution, such as systems administrators and security staff, conduct testing. But, to assure the credibility of test results, testing by individuals not associated with the design or maintenance of the system is also necessary. Three types of independent tests exist:

42.

Independent Test Types

- **Audits**
- **Assessments**
- **Penetration tests**



- Audits, which compare the state of the system against a set of standards
- Assessments, which locate security vulnerabilities and identify corrective actions, and
- Penetration tests, which subject systems to real-world attacks conducted by testing personnel.

43.

Key Aspects of Testing

- **Based on the risks posed**
- **Mitigate the risks posed to systems**
- **Used to evaluate objectives**

Key aspects to keep in mind when evaluating the effectiveness of security testing programs include:

- Is the testing plan, test selection, and test frequency based on the risks that controls are not functioning properly;
- Do controls mitigate the risks posed to the systems by the testing; and
- Does the institution use test results to evaluate whether security objectives have been met?

Visual

Narrative

44. **Dynamic Problem**



In the end, information security is a dynamic problem that requires continuous monitoring and frequent updating.
Financial institutions should continuously monitor and analyze information on:

45. **Monitoring and Updating**

- New threats and vulnerabilities
- Attacks suffered by similar institutions
- Effectiveness of its existing security controls



- New threats and vulnerabilities,
- Attacks suffered by similar institutions, and
- The effectiveness of its existing security controls to mitigate these emerging threats.

46. **Update**

- Risk assessment
- Strategies
- Controls

This information is used to update the institution's risk assessment, strategies, and controls.

47. **Booklet Narrative**

- Introduction
- Security Process
- Information Security Risk Assessment
- Information Security Strategy
- Security Controls Implementation
- Security Testing
- Monitoring and Updating

Now that you have seen the type of information in the narrative sections of the booklet, let's see how that information translates into the associated workprogram.

The goal of your information security examinations should be...

	Visual	Narrative
48.	<div style="border: 1px solid blue; padding: 5px; margin-bottom: 10px;"> <p style="text-align: center;"><i>Workprogram Goals</i></p> <hr style="border: 1px solid yellow;"/> <ul style="list-style-type: none"> – Draw conclusions about: <ul style="list-style-type: none"> – Quantity of risk – Quality of risk management <p style="text-align: center; font-size: 2em; color: red; font-weight: bold;">GOAL</p> </div>	<p>to draw conclusions about the quantity of risks and the quality of risk management in a manner that is consistent with a risk-based examination approach.</p> <p>This goal is consistent with the view that information security is an ongoing process. That is, the quality of security is a function of the quality of the processes that the institution has in place.</p> <p>While actual controls may change overtime, sound processes are the basis for ongoing effectiveness in a security program. The condition of security controls at a given time, however, may be one indicator of the effectiveness of the institution's overall security process.</p> <p>In support of these exam goals, the workprogram is divided into two tiers.</p>
49.	<div style="border: 1px solid blue; padding: 5px; margin-bottom: 10px;"> <p style="text-align: center;"><i>Workprogram Tiers</i></p> <hr style="border: 1px solid yellow;"/> <ul style="list-style-type: none"> – Tier 1 - overview of risk and risk management processes </div>	<p>In the Tier One part of the workprogram, the objectives and procedures will assist you to assess the effectiveness of how an institution is identifying and managing risks within its particular environment.</p>
50.	<div style="border: 1px solid blue; padding: 5px; margin-bottom: 10px;"> <p style="text-align: center;"><i>Workprogram Tiers</i></p> <hr style="border: 1px solid yellow;"/> <ul style="list-style-type: none"> – Tier 1 - overview of risk and risk management processes – Risk-management quality: <ul style="list-style-type: none"> – Risk assessment – Strategy – Control policies – Testing – Security administration </div>	<p>Part of that assessment includes evaluating the quality of risk management, including:</p> <ul style="list-style-type: none"> ▪ Risk assessment, ▪ Strategy, ▪ Control policies, ▪ Testing, and ▪ Security administration.
51.	<div style="border: 1px solid blue; padding: 5px;"> <p style="text-align: center;"><i>Workprogram Tiers</i></p> <hr style="border: 1px solid yellow;"/> <ul style="list-style-type: none"> – Tier 1 - overview of risk and risk management processes – Tier 2 - verification procedures </div>	<p>Tier Two focuses more on actual control implementation within the institution. The objectives and procedures provide for additional validation, as warranted, to verify the effectiveness of the institution's implementation of controls.</p>

Visual

Narrative

52.

Tier 2 Considerations

- Authentication and access controls
- Network security
- Host security
- User equipment security
- Physical security
- Personnel security
- Application security
- Software development and acquisition
- Business continuity security
- Intrusion detection and response
- Service provider oversight security
- Encryption
- Data security

Acknowledging that all devices are subject to a common set of concerns, the Tier Two Workprogram provides a set of broad considerations that you can apply to a variety of technologies within a given institution. For example, authentication and authorization are common issues for multiple types of devices.

This move away from device-specific procedures supports a risk-management approach in examinations and allows for consistent security standards to be applied among different types of institutions that may have differing needs and technical configurations.

53.

Important Issues

- Effective controls?
- Tested and updated?



In the end, the important issue is, "does management have appropriate and effective controls in place, and are those controls tested and updated as necessary?"

54.

Need For Customization



While comprehensive, the workprogram does not provide for every conceivable situation or environment. Rather, it's designed as a toolkit, providing the examiner with a variety of tools that can be tailored to fit specific devices or controls encountered in any examination.

55.

Need For Customization



The selection and modification of the workprogram should reflect the needs of your specific examination.

Visual

Narrative

56.

Information Security Handbook



Always keep in mind that the examination workprogram is not designed to require you to duplicate tests that institutions should be running on their own. It is the institution's responsibility to find and correct vulnerabilities.

57.

Information Security Handbook



The workprogram provides examiners with a comprehensive tool to make sure that management is, in fact, securing its data.