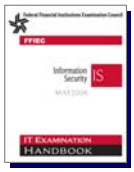
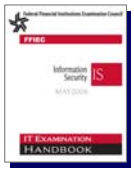
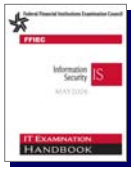
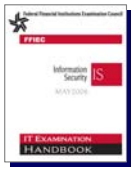
IT Handbook Presentation
Information Security Booklet

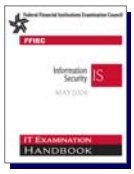
	Visual	Narrative
1.	*IT Handbook Presentations* ***Information Security Booklet*** *July 2006* 	This presentation provides a brief overview of the Information Security Booklet.
2.	*Booklet Focus* - **Risk assessment** - **Risk management processes** 	The booklet focuses on risk assessment and risk management processes. While specific security-related hardware, software, and controls may vary from institution to institution or change over time within a single institution,
3.	*Sound Practices* - **Identifying** - **Assessing** - **Managing** 	the booklet contains sound practices for identifying, assessing, and managing information security risks over the long-term. Consequently, the information provided in this booklet is related to the process of risk assessment and management, as applied to information security.

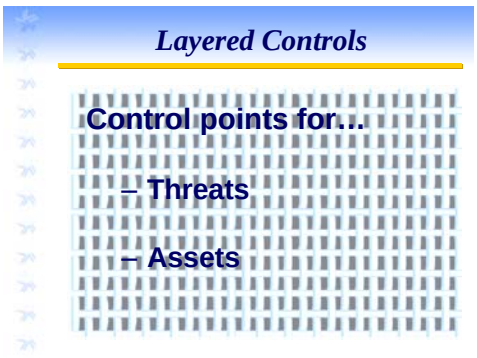
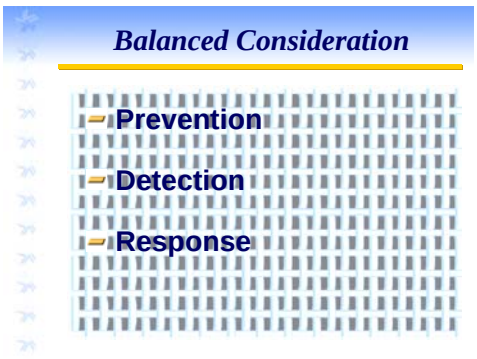
	Visual	Narrative
4.	**Assumptions** **Intermediate level of technical knowledge…** - **Software** - **Hardware** - **Protocols** - **Controls** 	The booklet assumes readers possess an intermediate level of technical knowledge as it relates to security software, hardware, protocols, and controls, and
5.	**Booklet Characteristics** - **Provides foundation for risk identification and assessment** - **Is designed as reference for assessing effectiveness of a security program** - **Builds on interagency guidelines** - **Supports guidelines for financial institutions and service providers**	▪ Provides a foundation for risk identification and risk assessment processes, ▪ Is designed as a reference for assessing the effectiveness of a security program in a particular financial institution or service provider, rather than as a tool for conducting penetration tests or auditing specific security controls, ▪ Builds on the Interagency Guidelines Establishing Information Security Standards that implemented section 501(b) of the Gramm-Leach-Bliley Act by providing additional and more detailed explanations of sound security-process elements, and ▪ Supports guidelines for both financial institutions and their service providers.
6.	**Booklet Structure** - **Introduction** - **Security Process** - **Information Security Risk Assessment** - **Information Security Strategy** - **Security Controls Implementation** - **Security Monitoring** - **Security Process Monitoring And Updating** 	The booklet's structure is composed of seven main sections.

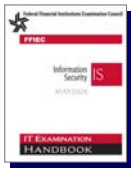
7.	**Introduction**
	- **Establishes risk management approach**
	- **Describes effective information security program as continuous integration of ...**
	  – **Processes**
	  – **People**
	  – **Technology**
		The introduction starts by establishing the risk management approach used in the booklet and describes an effective information security program as a continuous integration of processes, people, and technology to manage risk.

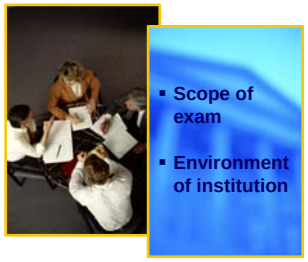
	Visual	Narrative
8.	**Booklet Structure** - Introduction - **Security Process** - Information Security Risk Assessment - Information Security Strategy - Security Controls Implementation - Security Monitoring - Security Process Monitoring And Updating 	The Security Process section defines "security process" as the method an organization uses to implement and achieve its security objectives, and establishes five primary issues related to examining the security of data in financial institutions.
9.	**Booklet Structure** - Introduction - Security Process - **Information Security Risk Assessment** - **Information Security Strategy** - **Security Controls Implementation** - **Security Monitoring** - **Security Process Monitoring And Updating** 	These five topics form the structure for the remainder of the narrative in the booklet. ▪ Information security risk assessment, ▪ Information security strategy, ▪ Security controls implementation, ▪ Security monitoring, and ▪ Security process monitoring and updating Let's take a brief look at what's covered in each topic.
10.	**Booklet Structure** - Introduction - Security Process - **Information Security Risk Assessment** - Information Security Strategy - Security Controls Implementation - Security Monitoring - Security Process Monitoring And Updating 	The risk assessment is the key driver and foundation of an effective information security program. In exploring this topic, the booklet focuses first on the functional requirements for an effective security risk assessment program.

11.	***Effective Risk Assessment***
	- **Identifying and valuing assets**
	- **Analyzing**
	  – **Threats**
	  – **Vulnerabilities**
	  – **Potential attacks**
	  – **Probability of attacks**
	  – **Probable outcomes**
		The information security risk assessment process involves identifying and valuing the institution's assets and analyzing the threats, vulnerabilities, and potential attacks against those assets, the probability of the attacks occurring, and probable outcomes if those attacks take place.

	Visual	Narrative
12.	**Acceptable Methodologies** 	There are many acceptable risk assessment methodologies institutions can use for assessing their information security vulnerabilities.
13.	**Acceptable Methodologies** - Gathering necessary information - Identifying information and information systems - Analyzing the information - Assigning risk ratings	Any of these methods can be effective, as long as they incorporate the four key elements, which include: ▪ Gathering necessary information, ▪ Identifying information and information systems, ▪ Analyzing the information, and ▪ Assigning risk ratings.
14.	**Risk Assessment** - Multidisciplinary and knowledge-based approach - Systematic and central control - Integrated process - Accountable activities - Documentation - Enhanced knowledge - Regular updates	Also included in this section are the key practices examiners should consider when looking at the risk assessment process within a particular institution: ▪ Multidisciplinary and knowledge-based Approach, ▪ Systematic and central control, ▪ Integrated process, ▪ Accountable activities, ▪ Documentation, ▪ Enhanced knowledge, and ▪ Regular updates.
15.	**Booklet Structure** - Introduction - Security Process - Information Security Risk Assessment - Information Security Strategy - Security Controls Implementation - Security Monitoring - Security Process Monitoring And Updating 	Once a financial institution's management team has completed a sound risk assessment, gathered and analyzed information and prioritized required responses, it should develop strategies for addressing the potential security risks that have been identified.

	Visual	Narrative
16.		An information security strategy is a plan to mitigate risks while complying with legal, statutory, regulatory, contractual, and internally developed requirements.
17.		An institution's overall information security strategy should include: ▪ Specific policies, standards, and procedures that guide the board of directors, officers and employees, ▪ Technology designs, ▪ Resource dedication, and ▪ Adequate training and testing.
18.		These elements should then be woven together as a set of layered controls that establish multiple control points, or points of protection, between potential threats and the organization's assets.
19.		They should also demonstrate an appropriate and balanced consideration of the elements of prevention, detection, and response mechanisms.

	Visual	Narrative
20.	**Booklet Structure** - Introduction - Security Process - Information Security Risk Assessment - Information Security Strategy - **Security Controls Implementation** - Security Monitoring - Security Process Monitoring And Updating 	The security controls implementation phase of the security process is where an institution:
21.	**Controls Implementation** - **Acquires and installs technology** - **Assigns duties and responsibilities** - **Trains staff** - **Puts program into practice**	▪ Acquires and installs the technology, ▪ Assigns duties and responsibilities and trains staff, and ▪ Puts its security program into practice.
22.	**Controls Implementation** **Multiple and complex...** - **Processes** - **Staff responsibilities** - **Techniques** - **Technologies**	As this implementation can involve multiple and complex processes, staff responsibilities, techniques, and technologies, the topic comprises the majority of content in the Information Security Handbook.
23.	**Security Controls Implementation** - **Access Control** - **Physical and Environmental Protection** - **Encryption** - **Malicious Code Prevention** - **Systems Development, Acquisition, and Maintenance** - **Personnel Security** - **Data Security** - **Service Provider Oversight** - **Business Continuity Considerations** - **Insurance**	This section of the booklet covers multiple aspects related to implementation, including the topics on: ▪ Access control, ▪ Physical and environmental protection, ▪ Encryption, ▪ Malicious code prevention, ▪ Systems development, acquisition, and maintenance, ▪ Personnel security, ▪ Data security, ▪ Service provider oversight, ▪ Business continuity considerations, and ▪ Insurance.

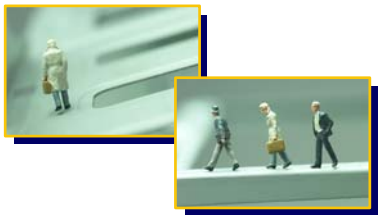
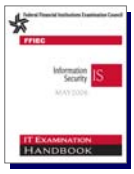
	Visual	Narrative
24.	*Issue Oriented* 	Readers should keep in mind that the discussion in this section is not intended to provide specific technical information. Instead, you will find an explanation of the issues that are important for an institution to consider when making technical decisions.
25.	*Issue Oriented* 	For example, the institution's password policy is discussed rather than the technology used to implement a specific password protection program.
26.	*Critical Questions* - How was the policy developed? - How is it enforced? - Is it appropriate for technologies in place at institution?	The critical questions concerning this issue, from an examination standpoint, are: how was the policy developed; how is it enforced; and is it appropriate for the technologies in place at the institution? These considerations are fundamental, irrespective of technology.
27.	*Implementation Section*  ▪ Scope of exam ▪ Environment of institution	The implementation section of the booklet, in particular, is intended as a resource. In examining a specific institution, the significance of each of the topics covered in this section will vary, depending on the scope of the exam and the environment of the institution under review.

	Visual	Narrative
28.	**Security Controls Implementation** - Access Control - Physical and Environmental Protection - Encryption - Malicious Code Prevention - Systems Development, Acquisition, and Maintenance - Personnel Security - Data Security - Service Provider Oversight - Business Continuity Considerations - Insurance	In final analysis, each of the topics in this section, along with multiple subtopics, will provide examiners with a broad range of resources for conducting exams in various types of institutions.
29.	**Booklet Structure** - Introduction - Security Process - Information Security Risk Assessment - Information Security Strategy - Security Controls Implementation - Security Monitoring - Security Process Monitoring And Updating 	Once an institution's security controls are in place, the institution should implement processes to monitor the platforms, applications, network, and security systems.
30.	**Security Monitoring** - Platforms - Applications - Network - Security	Institutions should continually monitor network activity, which is typically an operational procedure performed over a period of time, that provides continual assurance of the effectiveness of the security controls that are in place.

31.	**Security Monitoring**
	- Activity monitoring
	  – Firewalls
	  – Network intrusion detection systems
	  – Honeypots
	  – Host intrusion detection systems
	  – Log transmission, normalization, storage, and protection
		Activity monitoring should include:
		▪ Firewalls,
		▪ Network intrusion detection systems,
		▪ Honeypots,
		▪ Host intrusion detection systems, and
		▪ Log transmission, normalization, storage, and protection.

	Visual	Narrative

32.	**Security Monitoring**
	- **Activity monitoring**
	- **Condition monitoring**
	  – **Self assessments**
	  – **Metrics**
	  – **Independent tests**
		In addition to activity monitoring, institutions should also conduct condition monitoring through periodic testing. This type of monitoring will require activities such as:
		▪ Self assessments,
		▪ Metrics, and
		▪ Independent tests.

33.	**Security Monitoring** 	How an institution analyzes and responds to the results gathered in its activity and condition monitoring depends on the size and complexity of the organization.
34.	**Security Monitoring** 	Smaller, less complex institutions may assign operational personnel to the analysis and response function, while larger, more complex institutions may maintain a security response center that monitors and analyzes information as activities occur.
35.	**Booklet Structure** - Introduction - Security Process - Information Security Risk Assessment - Information Security Strategy - Security Controls Implementation - Security Monitoring - **Security Process Monitoring And Updating** 	As critical as monitoring security controls is to the security of an institution's information, equally important is the ongoing monitoring of the institution's overall security processes. A static security program can provide a false sense of security and will inevitably become ineffective over time.

	Visual	Narrative

36.	**Monitoring and Updating**
	- **Monitor**
	  – New threats and vulnerabilities
	  – Actual attacks
	  – Existing security controls
	- **Update**
	  – Risk assessments
	  – Strategies
	  – Controls
		Financial institutions should continuously gather and analyze information regarding new threats and vulnerabilities, actual attacks on the institution or others, and the effectiveness of the existing security controls. Management should then use that information to update their current risk assessment, strategies, and controls to address the changing environment.

37.	**Outsourcing** - **Analysis** - **Response** 	Institutions of all sizes may outsource various functions, including analysis and response. However, outsourcing does not relieve the institution of its responsibility for safeguarding critical information.
38.	**Outsourcing** - **Control failures identified before security incidents occurs** - **Intrusions detected in time for effective response** - **Sufficient information to support post-event forensics activities**	The institution should ensure that control failures are identified before a security incident occurs. An intrusion or other security incident should be detected in sufficient time to enable an effective and timely response. Sufficient information should be preserved to support post-event forensics activities.
39.	**Appendices** - **Examination Procedures** - **Glossary** - **Laws, Regulations, and Guidance**	Finally, the booklet concludes with a set of useful appendices: ▪ Appendix A, the examination procedures, ▪ Appendix B, a comprehensive glossary of information security terms, and ▪ Appendix C, references to laws, regulations, and guidance relating to the topic.