FITSI Candidate Handbook

Candidate Handbook
Outlining the FITSI
Exam Process for the
FITSP Certification

Version 1.2

Published 11/13/2013

This page is left intentionally blank

TABLE OF CONTENTS

1. Overview

Welcome to the Federal IT Security Institute (FITSI) certification program. The FITSI Candidate Handbook provides important logistical and procedural information for those wishing to pursue a FITSI certification. This guide is updated as needed and provides an overview of the processes and procedures that candidates must follow to apply for and attempt this exam.

Provided by the Federal IT Security Institute (FITSI), candidates can obtain this FITSI Candidate Handbook free of charge at the following website: http://www.fitsi.org/documents.

This document may be forwarded to professional colleagues but must be kept in its original form.

2. Statement of Purpose

The purpose of the FITSI certification program is to validate the skills of IT security professionals against NIST standards and documentation. The certification allows the individual to demonstrate their knowledge of IT standards as set by NIST publications and thus making a minimum level of competency easily identifiable to those in the industry. The FITSP program is broken into four certifications based on roles: Manager, Designer, Operator and Auditor. Application for one of the FITSP certifications is open to all information security persons.

FITSI does not restrict candidacy based on membership to any society, undue financial conditions or on other conditions not germane to the scope of this certification. FITSI is a non-discriminatory certification body and is compliant with Federal and state ADA regulations.

3. Overview of the FITSP Certification

A. FITSP-Manager

The FITSP-Manager certification is intended for federal workforce personnel, both federal employees and contractors, ***whose role is primarily focused on the management and oversight of systems owned by, or operated on behalf of, the federal government of the United States***. The following list highlights, but may not comprehensively capture, the commonly articulated roles characterized within federal statutory, regulatory, standards, and/or guidance documents that relate to the FITSP-Manager certification.

1) Authorizing Official
2) Chief Information Officer
3) Senior Agency Information Security Officer
4) Chief Information Security Officer
5) Chief Technology Officer
6) Freedom of Information Act Official
7) Information Resource Manager
8) Information Assurance Manager
9) Information Security Manager
10) Information Security Program Manager
11) Information Systems Security Officers
12) IT Security Compliance Officer
13) Privacy Act Official (Privacy Officers)
14) Program and Functional Managers
15) Procurement Officers
16) Risk Executive
17) Senior/Executive Agency Leader
18) System Owner

B. FITSP-Designer

The FITSP-Designer certification is intended for federal workforce personnel, both federal employees and contractors, ***whose role is primarily focused on the design and development of systems owned by, or operated on behalf of, the federal government of the United States***. The following list highlights, but may not comprehensively capture, the commonly articulated roles characterized within federal statutory, regulatory, standards, and/or guidance documents that relate to the FITSP-Designer certification:

1) IT Security Engineer
2) Programmer
3) Security Engineer
4) System Designer
5) System Developer

C. FITSP-Operator

The FITSP-Operator certification is intended for federal workforce personnel, both federal employees and contractors, ***whose role is primarily focused on the***

implementation and operations of systems owned by, or operated on behalf of, the federal government of the United States. The following list highlights, but may not comprehensively capture, the commonly articulated roles characterized within federal statutory, regulatory, standards, and/or guidance documents that relate to the FITSP-Operator certification.

1) Data Center Manager
2) Database Administrator
3) IT Security Operations
4) Maintenance Professional
5) Network Administrator
6) Network Security Specialists
7) Security Administrator
8) System Administrators
9) System Operations Personnel
10) Technical Support Professionals
11) Telecommunications Personnel

D. FITSP-Auditor

The FITSP-Auditor certification is designed to demonstrate that federal workforce personnel, both federal employees and contractors, ***who possess the knowledge of federal IT security requirements necessary to successfully audit and review the management, operational, and technical IT security controls for systems owned by, or operated on behalf of, the federal government***.

1) Assessor
2) External IT auditor
3) Evaluator
4) Internal IT auditor
5) Reviewer
6) Risk/Vulnerability Analyst

4. Scope of the FITSP Certification

A. Overview

Candidates of all four certification roles (Manager, Designer, Operator and Auditor) are tested on a comprehensive Federal Body of Knowledge (FBK), which consists of a library of federal statutes, regulations, standards, and guidelines. The FBK is broken down into six domains and 21 IT security topic areas.

Domains

1. Domain 1 – NIST Special Publications
2. Domain 2 – NIST Federal Information Processing Standards (FIPS)
3. Domain 3 – NIST Control Families
4. Domain 4 – Governmental Laws and Regulations
5. Domain 5 – NIST Risk Management Framework
6. Domain 6 – NIST Interagency Reports

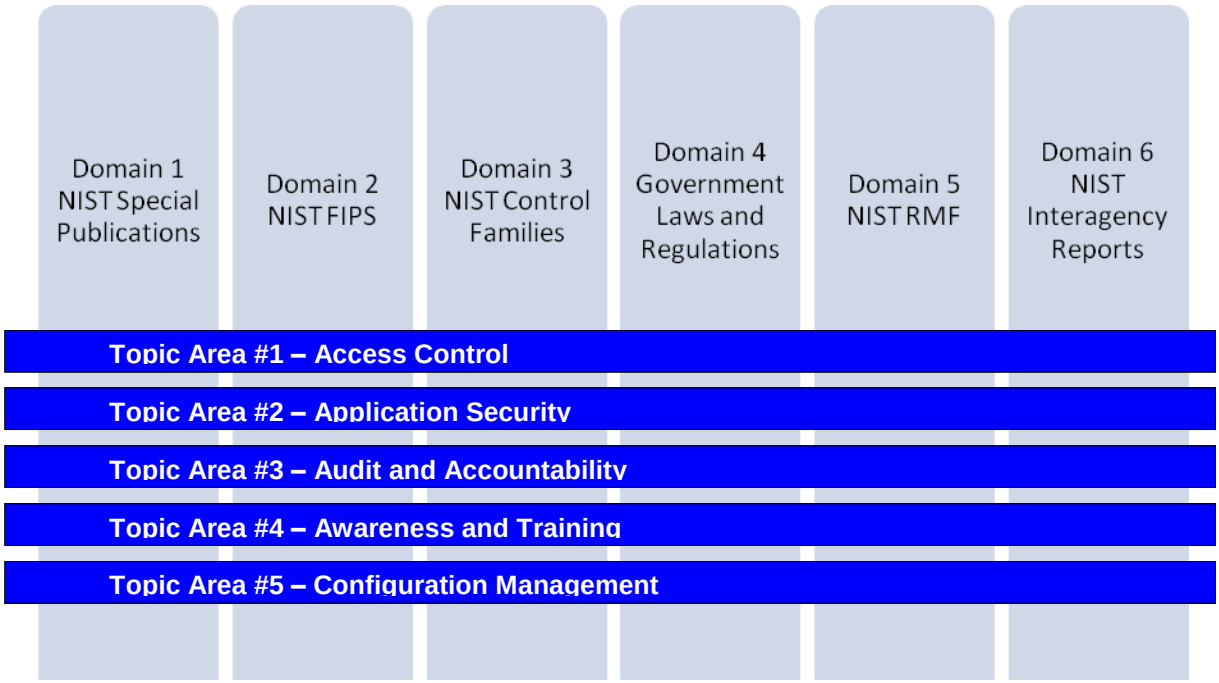
IT Security Topic Areas

1. Access Control
2. Application Security
3. Audit and Accountability
4. Awareness and Training
5. Configuration Management
6. Contingency Planning
7. Data Security
8. Identification and Authentication
9. Incident Response
10. Maintenance
11. Media Protection
12. Personnel Security
13. Physical and Environmental Protection
14. Planning
15. Program Management
16. Regulatory and Standards Compliance
17. Risk Assessment
18. Security Assessment and Authorization
    a. (Formerly Certification, Accreditation, and Security Assessments)
19. System and Communications Protection
20. System and Information Integrity
21. System and Services Acquisition

Domains are the boundaries of knowledge that are applicable within the federal government. The IT security topic areas include themes and skills that IT security professionals are expected to understand. ***The FITSP certification exams include questions that cover the intersection between the six domains and the 21 IT security topic areas (see illustration below).***

Seventeen of the 21 IT Security topic areas are derived directly from the minimum control requirements defined in Federal Information Processing Standard 200 (FIPS 200), one is defined in NIST SP 800-53 (Program Management) and three come from the Department of Homeland Security (DHS) Essential Body of Knowledge (EBK) IT Security competencies.

The interwoven nature of the domains and topic areas is represented below. Only five out of the 21 topic areas are listed for illustration purposes.



The following are the approximate areas of focus on which the four certification roles candidate are tested:

Role	NIST Special Pubs	NIST FIPS	NIST Control Families	Laws and Regulations	NIST RMF	NIST IR
Manager	18%-22%	8%-12%	8%-12%	18%-22%	27%-33%	8%-10%
Designer	27%-33%	8%-12%	18%-22%	8%-12%	23%-27%	3%-7%
Operator	27%-33%	8%-12%	26%-30%	10%-14%	8%-12%	8%-12%
Auditor	35%-39%	8%-12%	13%-17%	13%-17%	13%-17%	6%-10%

B. Domains

The FITSP program is represented by the FITSP Federal Body of Knowledge (FBK). The FBK is broken down into six domains. A domain is considered an area of knowledge.

1. NIST Special Publications - This domain focuses on the full range of NIST 800 series special publications.

2. NIST Federal Information Processing Standards - This domain focuses on roughly 13 Federal Information Processing Standards depending upon the role based certification pursued (i.e., FIPS 140-2, FIPS 180-3, FIPS 197, etc.).

3. NIST Control Families - This domain focuses on the 18 control families as defined in NIST SP 800-53. Candidates are expected to be familiar with the 18 control families and corresponding controls from each family.

4. Government Laws and Regulations - This domain focuses on the memorandums, circulars, executive orders, and laws that are required by OMB, Congress and Presidential Directives. Examples would include the FDCC as detailed in OMB M07-11, FISMA, OMB A-130 Appendix III, HSPD-12, etc.

5. NIST Risk Management Framework - This domain focuses on the NIST RMF in support of system authorization. Documents such as NIST SP 800-37 Rev 1 and supporting documents are tested.

6. NIST Interagency Reports - This domain focuses on several key NIST Interagency Reports that have been published to date.

Reference material in the form of the FITSI Candidate Handbook can be electronically downloaded at http://www.fitsi.org/documents.

C. Exam Objectives

The exam objectives for each of the four roles are listed below. The following are representative task and knowledge statements, as well as the objectives in each of the 21 IT security topic areas that a FITSP is expected to understand and to be able to apply.

	Manager	Designer	Operator	Auditor
Access Control	• Manage system components that enable the limitation of information system access to authorized users • Oversee security elements in a system so that they limit access to processes	• Design system components that enable the limitation of information system access to authorized users • Develop security elements in a system so that they limit access to processes	• Implement system components that enable the limitation of information system access to authorized users • Configure security elements in a system so that they limit access to processes acting	• Audit system components that enable the limitation of information system access to authorized users • Review security elements in a system so that they limit access to processes

	acting on behalf of authorized users • Govern controls on a system that facilitate the limitation of information system access to devices (including other information systems) • Direct system controls that govern the types of transactions and functions that authorized users are permitted to exercise	acting on behalf of authorized users • Construct controls on a system that facilitate the limitation of information system access to devices (including other information systems) • Create system controls that govern the types of transactions and functions that authorized users are permitted to exercise	on behalf of authorized users • Enable controls on a system that facilitate the limitation of information system access to devices (including other information systems) • Deploy system controls that govern the types of transactions and functions that authorized users are permitted to exercise	acting on behalf of authorized users • Assess controls on a system that facilitate the limitation of information system access to devices (including other information systems) • Inspect system controls that govern the types of transactions and functions that authorized users are permitted to exercise
Application Security	• Manage security requirements during software development activities on a system • Oversee processes that translate security requirements into application design elements • Direct mechanisms that govern the development of secure code and exploit mitigation	• Design security requirements during software development activities on a system • Construct processes that translate security requirements into application design elements • Build mechanisms that govern the development of secure code and exploit mitigation	• Facilitate security requirements discovery during software development activities on a system • Assist processes that translate security requirements into application design elements • Implement mechanisms that govern the development of secure code and exploit mitigation	• Evaluate security requirements during software development activities on a system • Review processes that translate security requirements into application design elements • Audit mechanisms that govern the development of secure code and exploit mitigation
Awareness and Training	• Manage training elements so that managers and users of organizational information systems are made aware of the security risks associated with their activities • Oversee training elements that promote managers and users awareness of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures	• Design training elements so that managers and users of organizational information systems are made aware of the security risks associated with their activities • Develop training elements that promote managers and users awareness of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the	• Configure training elements so that managers and users of organizational information systems are made aware of the security risks associated with their activities • Implement training elements that promote managers and users awareness of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information	• Review training elements so that managers and users of organizational information systems are made aware of the security risks associated with their activities • Assess training elements that promote managers and users awareness of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the

	related to the security of organizational information systems • Govern training elements that validate organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities	security of organizational information systems • Construct training elements that validate organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities	systems • Enable training elements that validate organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities	security of organizational information systems • Inspect training elements that validate organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities
Audit and Accountability	• Manage controls in a system that facilitate the creation, protection, and retention of information system audit records to the extent needed to enable the monitoring, analysis, and investigation of the system • Direct security elements in a system to enable the reporting of unlawful, unauthorized, or inappropriate information system activity • Oversee controls in a system to facilitate that the actions of individual information system users can be uniquely traced to those users so that they can be held accountable for their actions	• Design controls in a system that facilitate the creation, protection, and retention of information system audit records to the extent needed to enable the monitoring, analysis, and investigation of the system • Develop security elements in a system to enable the reporting of unlawful, unauthorized, or inappropriate information system activity • Construct controls in a system to facilitate that the actions of individual information system users can be uniquely traced to those users so that they can be held accountable for their actions	• Deploy controls in a system that facilitate the creation, protection, and retention of information system audit records to the extent needed to enable the monitoring, analysis, and investigation of the system • Operate security elements in a system to enable the reporting of unlawful, unauthorized, or inappropriate information system activity • Enable controls in a system to facilitate that the actions of individual information system users can be uniquely traced to those users so that they can be held accountable for their actions	• Review controls in a system that facilitate the creation, protection, and retention of information system audit records to the extent needed to enable the monitoring, analysis, and investigation of the system • Inspect security elements in a system to enable the reporting of unlawful, unauthorized, or inappropriate information system activity • Audit controls in a system to facilitate that the actions of individual information system users can be uniquely traced to those users so that they can be held accountable for their actions
Configuration Management	• Manage baseline configurations throughout the respective system development life cycles (SDLC) • Oversee inventories of organizational information systems (including	• Design and maintain baseline configurations throughout the respective system development life cycles (SDLC) • Develop inventories of organizational information systems (including	• Implement and maintain baseline configurations throughout the respective system development life cycles (SDLC) • Maintain inventories of organizational information systems (including hardware,	• Audit baseline configurations to ensure maintenance throughout the respective system development life cycles (SDLC) • Review inventories of organizational information systems

	hardware, software, firmware, and documentation) throughout the respective system development life cycles • Direct a plan that establishes and enforces the security configuration settings for information technology products employed in organizational information systems	hardware, software, firmware, and documentation) throughout the respective system development life cycles • Design a plan that establishes and enforces the security configuration settings for information technology products employed in organizational information systems	software, firmware, and documentation) throughout the respective system development life cycles • Deploy a plan that establishes and enforces the security configuration settings for information technology products employed in organizational information systems	(including hardware, software, firmware, and documentation) throughout the respective system development life cycles • Evaluate plans that establishes and enforces the security configuration settings for information technology products employed in organizational information systems
Contingency Planning	• Manage a plan that establishes and maintains effective implementation plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations	• Design a plan that establishes and maintains effective implementation plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations	• Operate a plan that establishes and maintains effective implementation plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations	• Audit plans that establish and maintain effective implementation plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations
Data Security	• Supervise controls that facilitate the necessary levels of confidentiality of information found within the organization's information system • Manage safeguards in the system that facilitate the necessary levels of integrity of information found within information systems • Govern controls that facilitate the	• Design controls that facilitate the necessary levels of confidentiality of information found within the organization's information system • Develop safeguards in the system that facilitate the necessary levels of integrity of information found within information systems • Create controls that facilitate the necessary levels of availability of	• Configure controls that facilitate the necessary levels of confidentiality of information found within the organization's information system • Operate safeguards in the system that facilitate the necessary levels of integrity of information found within information systems • Enable controls that facilitate the necessary levels of availability of information and	• Review controls that facilitate the necessary levels of confidentiality of information found within the organization's information system • Evaluate safeguards in the system that facilitate the necessary levels of integrity of information found within information systems • Audit controls that facilitate the necessary levels of availability of

	necessary levels of availability of information and information systems	information and information systems	information systems	information and information systems
Identification and Authentication	• Oversee identification mechanisms for users of information systems and authenticate (or verify) the identities of those users as a prerequisite to allowing access to organizational information systems • Direct the identification of processes in information systems acting on behalf of users, and authenticate (or verify) the identities of those processes as a prerequisite to allowing access to organizational information systems • Manage identification mechanisms for devices and authenticate (or verify) the identities of those devices as a prerequisite to allowing access to organizational information systems	• Design identification mechanisms for users of information systems and authenticate (or verify) the identities of those users as a prerequisite to allowing access to organizational information systems • Design the identification of processes in information systems acting on behalf of users, and authenticate (or verify) the identities of those processes as a prerequisite to allowing access to organizational information systems • Construct identification mechanisms for devices and authenticate (or verify) the identities of those devices as a prerequisite to allowing access to organizational information systems	• Implement identification mechanisms for users of information systems and authenticate (or verify) the identities of those users as a prerequisite to allowing access to organizational information systems • Enable the identification of processes in information systems acting on behalf of users, and authenticate (or verify) the identities of those processes as a prerequisite to allowing access to organizational information systems • Deploy identification mechanisms for devices and authenticate (or verify) the identities of those devices as a prerequisite to allowing access to organizational information systems	• Inspect identification mechanisms for users of information systems and authenticate (or verify) the identities of those users as a prerequisite to allowing access to organizational information systems • Review the identification of processes in information systems acting on behalf of users, and authenticate (or verify) the identities of those processes as a prerequisite to allowing access to organizational information systems • Audit identification mechanisms for devices and authenticate (or verify) the identities of those devices as a prerequisite to allowing access to organizational information systems
Incident Response	• Supervise the establishment of an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities • Oversee the	• Develop the establishment of an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities • Design the tracking,	• Maintain an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities • Implement the tracking, documenting, and reporting of incidents to appropriate	• Inspect the establishment of an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities • Audit the tracking,

	tracking, documenting, and reporting of incidents to appropriate organizational officials and/or authorities	documenting, and reporting of incidents to appropriate organizational officials and/or authorities	organizational officials and/or authorities	documenting, and reporting of incidents to appropriate organizational officials and/or authorities
Maintenance	• Manage processes that performs periodic and timely maintenance on organizational information systems • Supervise processes that provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance	• Build processes that performs periodic and timely maintenance on organizational information systems • Develop processes that provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance	• Configure processes that performs periodic and timely maintenance on organizational information systems • Operate processes that provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance	• Review processes that performs periodic and timely maintenance on organizational information systems • Evaluate processes that provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance
Media Protection	• Direct mechanisms that facilitate the protection of paper information system media • Oversee system controls that facilitate the protection of digital information system media • Administer system safeguards that enable the limitation of access to information on information system media to authorized users • Manage systems mechanisms that enable the sanitization or destruction of information system media before disposal or release for reuse	• Develop mechanisms that facilitate the protection of paper information system media • Design system controls that facilitate the protection of digital information system media • Create system safeguards that enable the limitation of access to information on information system media to authorized users • Construct systems mechanisms that enable the sanitization or destruction of information system media before disposal or release for reuse	• Implement mechanisms that facilitate the protection of paper information system media • Configure system controls that facilitate the protection of digital information system media • Maintain system safeguards that enable the limitation of access to information on information system media to authorized users • Execute systems mechanisms that enable the sanitization or destruction of information system media before disposal or release for reuse	• Audit mechanisms that facilitate the protection of paper information system media • Review system controls that facilitate the protection of digital information system media • Assess system safeguards that enable the limitation of access to information on information system media to authorized users • Evaluate systems mechanisms that enable the sanitization or destruction of information system media before disposal or release for reuse
Program Management	• Direct processes and controls that are compatible and consistent with an	• Design processes and controls that are compatible and consistent with an	• Facilitate processes and controls that are compatible and consistent with an	• Audit processes and controls that are compatible and consistent with an

	organization's information security program	organization's information security program	organization's information security program	organization's information security program
Physical and Environmental Protection	• Manage security mechanisms that limit the physical access to information systems, equipment, and the respective operating environments to authorized individuals • Govern protection mechanisms that protect the physical plant and support infrastructure for information systems • Direct plans for the provision of supporting utilities for information systems • Supervise controls that protect information systems against environmental hazards • Oversee the appropriate environmental controls in facilities containing information systems	• Create security mechanisms that limit the physical access to information systems, equipment, and the respective operating environments to authorized individuals • Design protection mechanisms that protect the physical plant and support infrastructure for information systems • Develop plans for the provision of supporting utilities for information systems • Create controls that protect information systems against environmental hazards • Construct the appropriate environmental controls in facilities containing information systems	• Enable security mechanisms that limit the physical access to information systems, equipment, and the respective operating environments to authorized individuals • Operate protection mechanisms that protect the physical plant and support infrastructure for information systems • Execute plans for the provision of supporting utilities for information systems • Configure controls that protect information systems against environmental hazards • Facilitate the appropriate environmental controls in facilities containing information systems	• Review security mechanisms that limit the physical access to information systems, equipment, and the respective operating environments to authorized individuals • Assess protection mechanisms that protect the physical plant and support infrastructure for information systems • Audit plans for the provision of supporting utilities for information systems • Evaluate controls that protect information systems against environmental hazards • Inspect the appropriate environmental controls in facilities containing information systems
Planning	• Direct security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems • Administer documentation of the security plans for organizational information	• Develop security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems • Construct documentation of the security plans for organizational information systems that	• Deploy security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems • Implement documentation of the security plans for organizational information systems that describe the security controls	• Audit security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems • Review documentation of the security plans for organizational information systems that

	systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems • Manage processes to facilitate the periodic update of security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems • Supervise processes to handle the implementation of security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems	describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems • Design processes to facilitate the periodic update of security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems • Develop processes to handle the implementation of security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems	in place or planned for the information systems and the rules of behavior for individuals accessing the information systems • Execute processes to facilitate the periodic update of security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems	describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems • Inspect processes to facilitate the periodic update of security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems • Assess processes to handle the implementation of security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems
Personnel Security	• Oversee controls that ensure individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy • Supervise security	• Design controls that ensure individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy • Construct security	• Enable controls that ensure individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy • Configure security mechanisms that	• Audit controls that ensure individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy • Review security mechanisms that

	mechanisms that ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers • Manage formal sanctions for personnel failing to comply with organizational security policies and procedures	mechanisms that ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers • Design formal sanctions for personnel failing to comply with organizational security policies and procedures	ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers • Execute formal sanctions for personnel failing to comply with organizational security policies and procedures	ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers • Assess formal sanctions for personnel failing to comply with organizational security policies and procedures
Risk Assessment	• Oversee the necessary mechanisms to ensure periodic assessment of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.	• Design the necessary mechanisms to ensure periodic assessment of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.	• Deploy the necessary mechanisms to ensure periodic assessment of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.	• Audit the necessary mechanisms to ensure periodic assessment of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.
Security Assessments and Authorization	• Direct processes that facilitate the periodic assessment of the security controls in organizational information systems to determine if the controls are effective in their application • Administer and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational	• Design processes that facilitate the periodic assessment of the security controls in organizational information systems to determine if the controls are effective in their application • Design and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information	• Enable processes that facilitate the periodic assessment of the security controls in organizational information systems to determine if the controls are effective in their application • Implement and maintain plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems	• Review processes that facilitate the periodic assessment of the security controls in organizational information systems to determine if the controls are effective in their application • Assess and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational

	information systems • Manage mechanisms that authorize the operation of organizational information systems and any associated information system connections • Supervise processes that facilitate the monitoring of information system security controls on an ongoing basis to ensure the continued effectiveness of the controls	systems • Design mechanisms that authorize the operation of organizational information systems and any associated information system connections • Develop processes that facilitate the monitoring of information system security controls on an ongoing basis to ensure the continued effectiveness of the controls	• Deploy mechanisms that authorize the operation of organizational information systems and any associated information system connections • Execute processes that facilitate the monitoring of information system security controls on an ongoing basis to ensure the continued effectiveness of the controls	information systems • Inspect mechanisms that authorize the operation of organizational information systems and any associated information system connections • Evaluate processes that facilitate the monitoring of information system security controls on an ongoing basis to ensure the continued effectiveness of the controls
System and Services Acquisition	• Govern strategies for the allocation of sufficient resources to adequately protect organizational information systems • Oversee mechanisms that ensure the use of system development life cycle processes that incorporate information security considerations • Administer software usage and installation restrictions on information systems • Direct processes that ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization	• Develop strategies for the allocation of sufficient resources to adequately protect organizational information systems • Develop mechanisms that ensure the use of system development life cycle processes that incorporate information security considerations • Design software usage and installation restrictions on information systems • Construct processes that ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization	• Execute strategies for the allocation of sufficient resources to adequately protect organizational information systems • Enable mechanisms that ensure the use of system development life cycle processes that incorporate information security considerations • Configure software usage and installation restrictions on information systems • Implement processes that ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization	• Audit strategies for the allocation of sufficient resources to adequately protect organizational information systems • Review mechanisms that ensure the use of system development life cycle processes that incorporate information security considerations • Assess software usage and installation restrictions on information systems • Evaluate processes that ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization
System and Communication Protection	• Oversee processes that monitor, control, and protect	• Design processes that monitor, control, and protect	• Implement processes that monitor, control, and protect	• Audit processes that monitor, control, and protect

	organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems • Administer techniques that employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems	organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems • Design techniques that employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems	organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems • Execute techniques that employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems	organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems • Review techniques that employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems
System and Information Integrity	• Manage the identification, reporting, and correcting of system flaws which should be done in a timely manner • Supervise processes that provide protection from malicious code at appropriate locations within organizational information systems • Direct mechanisms that monitor information system security alerts and advisories that take appropriate actions in response	• Develop the identification, reporting, and correcting of system flaws which should be done in a timely manner • Design processes that provide protection from malicious code at appropriate locations within organizational information systems • Build mechanisms that monitor information system security alerts and advisories that take appropriate actions in response	• Implement the identification, reporting, and correcting of system flaws which should be done in a timely manner • Enable processes that provide protection from malicious code at appropriate locations within organizational information systems • Configure mechanisms that monitor information system security alerts and advisories that take appropriate actions in response	• Audit the identification, reporting, and correcting of system flaws which should be done in a timely manner • Assess processes that provide protection from malicious code at appropriate locations within organizational information systems • Review mechanisms that monitor information system security alerts and advisories that take appropriate actions in response
Regulatory and Standards Compliance	• Manage strategies for compliance with the organization's information security program	• Design strategies for compliance with the organization's information security program • Identify and stay current on all	• Implement strategies for compliance with the organization's information security program • Identify and stay current on all	• Audit strategies for compliance with the organization's information security program • Identify and stay current on all

	• Identify and stay current on all laws, regulations, standards, and best practices applicable to the organization • Oversee relationships with all regulatory information security organizations and appropriate industry groups, forums, and stakeholders • Keep informed on pending information security changes, trends, and best practices by participating in collaborative settings • Supervise information security compliance performance measurement components	laws, regulations, standards, and best practices applicable to the organization • Establish relationships with all regulatory information security organizations and appropriate industry groups, forums, and stakeholders • Keep informed on pending information security changes, trends, and best practices by participating in collaborative settings • Design information security compliance performance measurement components	laws, regulations, standards, and best practices applicable to the organization • Establish relationships with all regulatory information security organizations and appropriate industry groups, forums, and stakeholders • Keep informed on pending information security changes, trends, and best practices by participating in collaborative settings • Operate information security compliance performance measurement components	laws, regulations, standards, and best practices applicable to the organization • Establish relationships with all regulatory information security organizations and appropriate industry groups, forums, and stakeholders • Keep informed on pending information security changes, trends, and best practices by participating in collaborative settings • Review information security compliance performance measurement components

5. Application Process

Candidates shall complete the following steps to apply for FITSI certification:

1. Submit an online registration form at http://www.fitsi.org at least 5 calendar days prior to the desired exam date. During registration, the candidate will be asked for name, postal address, email address, telephone contact number, certification applying for, exam location, exam date and payment information. Electronic submission of credit card information is preferred. Those not wishing to submit electronic payment information must contact our billing office within 5 business of exam date. (See Corporate Contact Information at the end of this document).
2. Within 1 business of your electronic registration, your electronic payment fee will be processed. Once payment is verified, you will receive an email verifying your exam date, time and location. Candidates must bring a copy of the verification email to the exam.
3. Arrive at the exam with 2 forms of identification (1 must be a photo ID; both must have copies of your signature) and a copy of your verification exam date, time and location email.
4. After taking your confirmed exam, you will immediately be given your pass/fail results.
5. Candidates who successfully pass the certification exam will have 180 calendar days (6 months) to submit a *FITSI Certification Application.* The FITSI *Certification Application* will be emailed to candidates who have passed the Certification exam. Candidates must have 5 years of relevant experience in the information security field to qualify for certification. (See Certification Eligibility Requirements below). Completed *FITSI Certification Application* should be emailed to contactus@fitsi.org.
6. As part of the FITSI Certification Application, candidates must submit **two** endorsement forms for a professional colleague that can verify stated work experience. The professional endorsement forms are included in the FITSI Certification Application which will be emailed to candidates who have passed the certification exam.
7. Candidates who successfully pass the certification exam, submit the *FITSI Certification Application,* and meet all eligibility requirements *shall* receive a Certification Packet. The Certification Packet shall contain one each of the following:
    - FITSI certification certificate
    - FITSI Identification card
    - FITSI Certification Holder Handbook
    - FITSP challenge coin.

The certification packet will be sent via US mail at the address provided at registration.

Each of these steps is explained in greater detail in the remainder of this Candidate Handbook.

A. Completed Application for Certification Exam

A completed application will require the following:

- Completed electronic application at http://www.FITSI.org
- Validated payment
- Acknowledgement of accepting terms outlined in the Candidate Handbook Agreement

B. Certification Eligibility Requirements

A FITSP candidate for any of the four roles needs to have five years of information security experience to qualify for certification. This experience can be in the form of a practitioner, a manager, an instructor, an implementer, an auditor, etc. Upon successfully passing the certification exam, a candidate must submit a *FITSI Certification Application* demonstrating the five years of relevant work experience. *FITSI Certification Applications* should be emailed to contactus@fitsi.org.

As part of the FITSI Certification Application, candidates must submit two *Professional Letter of Endorsement Forms* from a current or immediate past supervisors validating the stated work experience. The form can be emailed to contactus@fitsi.org or faxed to FITSI Corporate Offices.

Candidates, who successfully pass the certification exam but do not hold 5 years of information security experience or cannot have the experience validated, will not be granted certification. No refund of examination fee will occur in this case.

FITSP candidates are able to waive portions of the experience requirements if the candidate possesses other complimentary security certifications and/or education experience. Candidates cannot waive more than 3 years experience in total with any combination of education or certifications. Candidates can waive one year of experience for a bachelor degree and can waive a second year with a master's degree in an information technology or information assurance focus. Degrees must be issued by a fully accredited institution.

Candidates can also waive 1 year experience by possessing one or more of the following IT security certifications:

- CISM - Certified Information Security Manager
- CISSP - Certified Information Systems Security Professional
- CISA - Certified Information Systems Auditor
- GIAC - Global Information Assurance Certified
- CEH - Certified Ethical Hacker Security+
- SSCP - System Security Certified Practitioner
- SCNA - Security Certified Network Architect
- SCNS - Security Certified Network Specialist
- CAP – Certified Authorization Professional

Candidates will be fairly judged by the certification committee as to their eligibility for certification. Eligibility will be determined solely based on the criteria established above and shall not be influenced by behavior outside of the scope of the requirements and of the certification exam. The eligibility requirement decision shall be made by the Certification committee who shall not participate in the training or on-site evaluation of the candidate.

C. Fees for Certification

The Certification Fees are listed in the document *FITSI Fee Schedule* and can be found at http://www.fitsi.org/documents. Any adjustment in Certification fees shall be posted on the FITSI web site at the site referenced above.

D. Other Associated Fees

Other associated Certification fees such as annual maintenance fees or replacement fees are listed in the document *FITSI Fee Schedule* and can be found at http://www.fitsi.org/documents.

E. Exam Sites

FITST certification exams are administered at various locations. For a current listing of the exam locations and times, please see the most current list of upcoming exams at http://www.fitsi.org.

Companies or groups wishing to hold an on-site certification exam should contact the FITSI headquarters. There is a 10 person minimum requirement for scheduling an on-site exam. FITSI contact information can be found at the end of this Candidate Handbook.

6. Special Circumstances and Related Fees

A. Incomplete Applications/Registrations

Applicants will be notified if their application is incomplete. Failure to complete the application one week prior to the exam, may result in canceling the examination request and a refund of fees. A processing fee shall be deducted from any refunded fees. Processing fees can be found in the document *FITSI Fee Schedule* at http://www.fitsi.org/documents.

B. Cancellation / Fee Refund

Fully processed examination fees are non-refundable. Failure to attend the exam will result in a forfeit of exam fees. For an additional fee, a candidate can re-schedule the exam date to within a 6 month period from the originally scheduled exam date. A re-schedule request must be made prior to the originally scheduled exam date. All re-schedule requests must by faxed or emailed to FITSI Corporate Offices 24 hours prior to the originally scheduled exam date. See *FITSI Corporate Information* at the end of this Candidate Handbook for fax and emailing information. The re-scheduling fee can be found in the document *FITSI Fee Schedule* at http://www.fitsi.org/documents.

C. Extreme Circumstances

If a candidate has missed the exam due to an emergency or hardship, including, but not limited to: serious illness, death in immediate family, traffic accident, court appearance, jury duty or military duty, the candidate may be permitted to reschedule to the exam at no additional charge. To avoid penalty, the candidate must submit written verification and supporting documentation of the situation to FITSI within 30 calendar days of the original exam date. All written correspondence should be faxed or emailed to FITSI Corporate Headquarters, listed in the back of the Candidate Handbook. The Certification Manager will notify the candidate of FITSI's decision within 30 calendar days of the receipt of the requested documentation.

If such a request is not made, the candidate will forfeit the full examination fee. To apply for a future exam date, the candidate must start the application process from the beginning, including paying another full exam fee.

7. The Examination

FITSI certification exams are computer based exams where the questions are in the form of multiple choice. The test may include trial items which will not be identified as such or scored.

Exams will be taken at a FITSI designated location. Candidates will have three (3) hours from the announced start time of the test to complete the exam. Exams are offered in English only. A FITSI proctor and/or Exam Administrator will be on hand to set up the exam, distribute and collect any necessary paperwork. The Proctor or the Exam Administrator may not answer any questions pertaining to the exam content before, during or after the exam.

A. Special Requests

Arrangements may be made to provide exam candidates, with a documented disability (as defined by Title III of the Americans with Disabilities act), special accommodations for the exam. Candidates in need of special accommodations must submit the *Exam Candidate Special Accommodations* form with their application. This form can be found be downloaded at the following website location: http://www.fitsi.org/documents.

FITSI shall make every attempt to accommodate such special accommodation requests. Because FITSI utilizes third party locations for testing, a candidate's request may not be feasible at the test location requested. The candidate may be asked to choose a more appropriate testing location. The Certification Manager will notify the candidate of FITSI's decision within 30 calendar days of receipt of the written request.

8. Preparing for the Examination

FITSP certification candidates can expect a computer-based exam that is 3 hours in length. The exam contains multiple choice questions covering all aspects of the Federal Body of Knowledge (FBK). The FBK domains are listed below:

1. **NIST Special Publications (SP)**

2. **NIST Federal Information Processing Standards (FIPS)**

3. **NIST Control Families (CF)**

4. **Government Laws and Regulations**

5. **NIST Risk Management Framework (RMF)**

6. **NIST Interagency Reports (IR)**

To successfully pass the FITSP exam, candidates must obtain the reported cut score.

A. Authoritative Reference List

The Authoritative Reference List provides a concise yet detailed guide to information relative to the FITSP certification exam. This list is intended for use as a study aid only. FITSI does not intend the list to imply endorsement of the specific references, nor are the test questions necessarily taken from these sources.

1. Documents listed in the Federal Body of Knowledge - FITSI publishes a Federal Body of Knowledge that is used at the criteria in the exam. Candidates can review the documents listed in Appendix A of this document for a full listing of all regulations, guidance and standards. The FBK is updated as necessary.

2. FITSI Authorized Courseware – in the second quarter of 2012, FITSI is releasing courseware (textbook and practice test questions) for the FITSP-Manager certification role. This guide will be available from FITSI Authorized Training Centers (FATC) or directly from FITSI at http://www.fitsi.org.

9. On the Day of the Exam

A. Exam Check In

Candidates must report to the designated exam test location at least 30 minutes before posted start time of the exam. Candidates arriving after the exam start time must re-schedule the exam. Re-scheduling fees shall apply. Candidates must present the following at check in:

- Copy of Exam Confirmation Email
- 2 forms of identifications (1 photo ID; both need to contain a valid signature)

Candidates will be asked to sign an *Exam Regulations Form* where exam center rules and regulations are outlined. Candidates should read and understand all the stated rules and regulations. This form is provided at the end of this Candidate Handbook for reference. Also, Candidates will be given a *Candidate Comment Form*, also found at the end of this Handbook. Any questions or comments related to the exam or exam center may be documented here. This form shall be collected at the end of the exam whether or not the exam candidate has listed any comments or questions.

Candidates who arrive later than the posted exam time or do not have a copy of the exam confirmation email or 2 forms of ID may NOT be permitted to enter the exam room. Candidates arriving after the posted exam start time or lacking the exam confirmation email or appropriate ID must pay a re-scheduling fee if they wish to take the exam at another time. Otherwise, the candidate will forfeit the full exam fee amount.

Candidates are reminded that the exam will last 3 hours and there are no scheduled breaks.

B. Taking the Exam

Seating in the exam room is not assigned. Candidates are to be seated and have all outside materials put away at start time. Such materials include but are not limited to: backpacks, briefcases, papers, computers, cell phones, calculators, drinks and food. Candidates may have one pen or pencil for use with the *Candidate Comment Form* only. This form must be returned at the end of the exam whether the candidate has comments or not. No other notes may be taken. The exam protector will instruct the candidates on the test format and will initiate the exam. The proctor may not answer any test content related questions before, during or after the test. All test related questions should be marked on the *Candidate Comment Form*. Any comments you have after leaving the test center should be emailed directly to FITSI headquarters. See *FITSI Corporate Information* at the end of this Candidate Handbook for fax number and email address.

Candidates will have 3 hours from the start of the exam to complete the exam. No additional time will be allotted. There will not be any scheduled breaks. Escorted bathroom breaks will be permitted on an as needed basis. Exam time will not be extended to accommodate bathroom breaks. If a candidate chooses to end his or her exam early, he may not re-enter the exam room.

C. Exam Center Rules

The following are rules enforced at all test centers:

- All candidates must have 2 IDs (1 photo ID;both must contain candidate signature) and Exam Confirmation Email to be admitted to the test room.
- Candidates must arrive 30 minutes prior to their assigned time.
- Candidates arriving after posted exam start time will not be permitted in the exam room and will have to contact FITSI to reschedule the exam. A re-scheduling fee will apply.
- No guests are permitted in the exam room.
- No reference material, books, papers or personal items are allowed in the exam room. Briefcases and backpacks must securely be stored in the designated area.
- No electronic devices are permitted in the exam room. Such items include but are not limited to: cell phones, recording devices, cameras, computers, calculators, music devices, pagers or PDA's.
- No weapons or instruments that may be reasonably used as weapons may be brought into the exam room.
- No test material, documents etc are to be taken from the exam room. Candidates must leave their *Candidate Comment Form* with the proctor. Failure to do so shall result in an automatic "failure" of the exam.
- Candidates may not communicate with another exam candidate during the exam. Proctors are authorized to maintain a secure and proper testing environment and are permitted to ask candidates to move to achieve such.
- No questions concerning the exam content may be asked before, during or after the exam time. The proctor will not - at any time - respond to questions regarding exam content. All comments are to be documented on the Candidate Comment Form or emailed to FITSI post-exam.
- Neither food nor drink is permitted in the exam room. Tobacco or gum is not permitted in the exam room.
- There are no scheduled breaks during the exam. Candidates are permitted breaks on an individual basis, but no additional time will be allotted for the breaks. Candidates who request a break must be escorted at all times.
- Candidates are not permitted to talk or communicate in any manner during an individual break. Those who do talk or communicate will not be permitted back into the exam room and will forfeit any associated exam fees. Their exams will not be scored.
- Candidates may not copy in writing or otherwise record for transmit to others any exam question and/or answers or other aspects of the exam (Candidate is however, allowed to comment on exam items on the Exam Comments form).
- Candidates may not offer or assist or solicit assistance from other candidates, the proctor or those responsible for administration of the exam.
- Candidates may not engage in any other conduct or inappropriate behavior which is injurious to the integrity of the exam or the candidates.

Failure to abide by these Exam Rules will result in dismissal from the exam. Such candidates may be barred from future exams. Exam proctors are authorized to take

immediate and appropriate measures against candidates caught violating Exam Rules. The candidate is entitled to appeal the dismissal with the appeals committee in accordance with FITSI's appeals policy.

D. Exam Irregularities

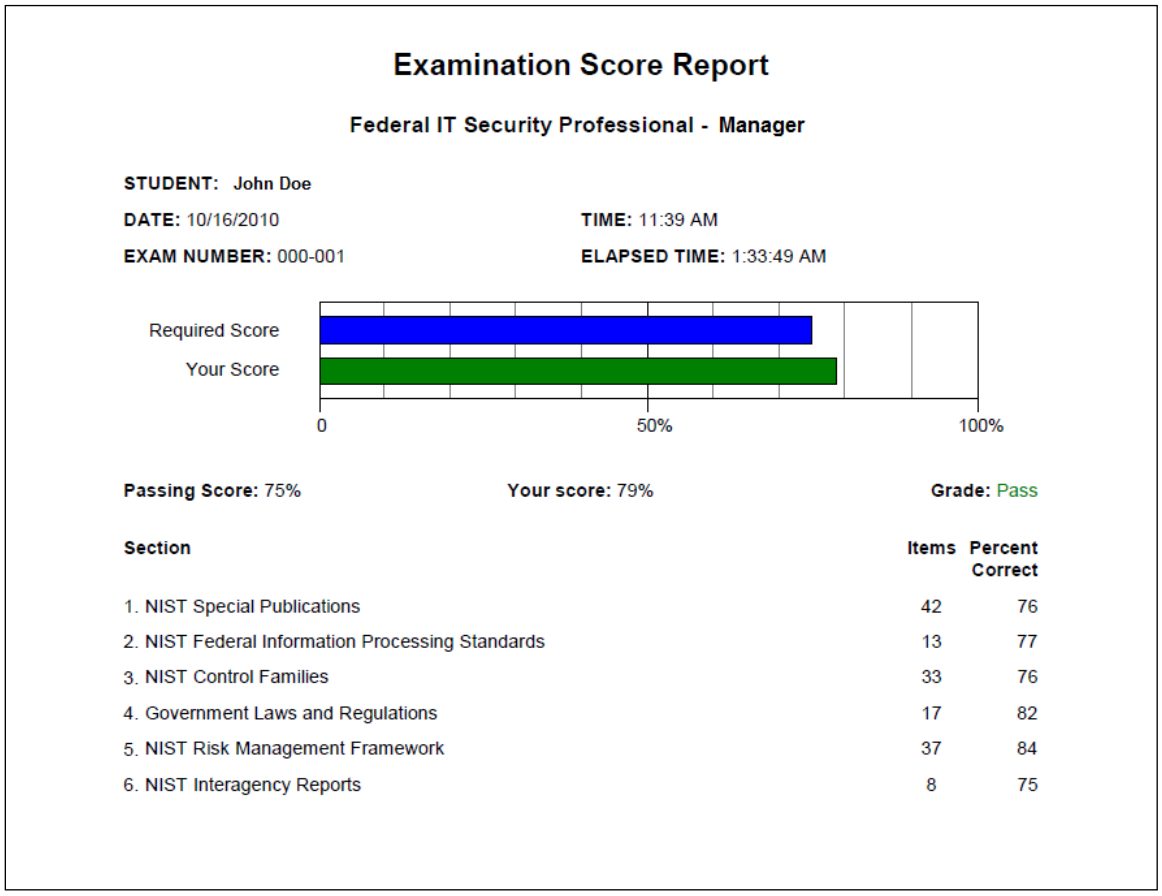
Should the testing be interrupted for an unforeseen reason (power outage, act of God or other), the Exam Administrator shall use his best judgment on how to proceed. The Exam Administrator has the option to cancel the exam, restart the exam or continue the exam.

- **Canceling an exam due to weather or any other unforeseeable event**
  The Certification Manager has the authority to cancel an exam due to weather, issues at the testing location or any other unforeseen event that would prohibit testing. In the event an exam is canceled, it will be re-scheduled at the earliest time possible. The Certification Manager will make every attempt to notify exam candidates in a timely manner of such cancelation. Candidates will not have to pay a re-scheduling fee in this instance. While the Certification Manager will make every attempt to re-schedule the exam for the same location, they cannot guarantee this.
- **Canceling an exam that was interrupted**
  The Exam Administrator has the authority to cancel an exam in progress if necessary (in the event of power outage, act of God or other). Each candidate shall be eligible to sign up for another exam for no additional fees. In this case, the candidate's answers and current score shall be erased.
- **Restarting an exam that was interrupted**
  If time allows, the Exam Administrator has the authority to re-start an exam that was interrupted for reasons stated above. Candidates will be allotted a total of 3 hours to complete the exam. If a candidate chooses not to restart the exam at that time, he shall be able to register for another scheduled exam at no additional charge. In this case, the candidate's answers and current score shall be erased.
- **Continuing an exam that was interrupted**
  If the Exam Administrator deems to continue an exam that was interrupted for reasons stated above, he has the authority to continue the exam if conditions allow. The time of the interruption shall not be counted towards exam time. Any individual who does not wish to continue the exam he shall be able to register for another scheduled exam at no additional charge. In this case, the candidate's answers and current score shall be erased.
- **Lost or unreadable exams**
  FITSI will take all available precautions to ensure the appropriate and secure handling of completed exams. In the rare and extreme case in which the completed exams become lost or unreadable, candidates will be required to undergo re-testing. No additional exam fees will be charged in this case.

10. Notification of Results

Candidates that abide to all exam day rules and regulations and have turned in their Exam Comment Form (even if blank), will receive exam results upon completion of the exam. Each candidate will be given paper copy of a Score Report similar to the example shown here.

3



Examination Score Report

Federal IT Security Professional - Manager

STUDENT: John Doe

DATE: 10/16/2010 **TIME:** 11:39 AM

EXAM NUMBER: 000-001 **ELAPSED TIME:** 1:33:49 AM

Passing Score: 75% **Your score:** 79% **Grade:** Pass

Section	Items	Percent Correct
1. NIST Special Publications	42	76
2. NIST Federal Information Processing Standards	13	77
3. NIST Control Families	33	76
4. Government Laws and Regulations	17	82
5. NIST Risk Management Framework	37	84
6. NIST Interagency Reports	8	75

Figure 1: Example of Certification Exam Score Report

A. Results – Passing

A candidate, who successfully completes the examination, submits a Certification Application outlining 5 years of information security experience and endorsement forms within 180 calendar days of their exam date shall be granted certification. These candidates will receive a Certification Packet within 30 calendar days of submitting all required documentation.

A Certification Packet contains the following:

- Welcome letter
- FITSP Certification

- FITSI ID/Certification Card
- FITSP Challenge Coin
- Certification Holder Handbook
- CPE Document

Each certified candidate will be assigned a unique FITSI ID number and a unique Certification Number.

Below is an example of a FITSP-Manager Certification, the FITSI ID/Certification Card and the FITSP Challenge Coin. Material is similar for Designer, Operator and Auditor.

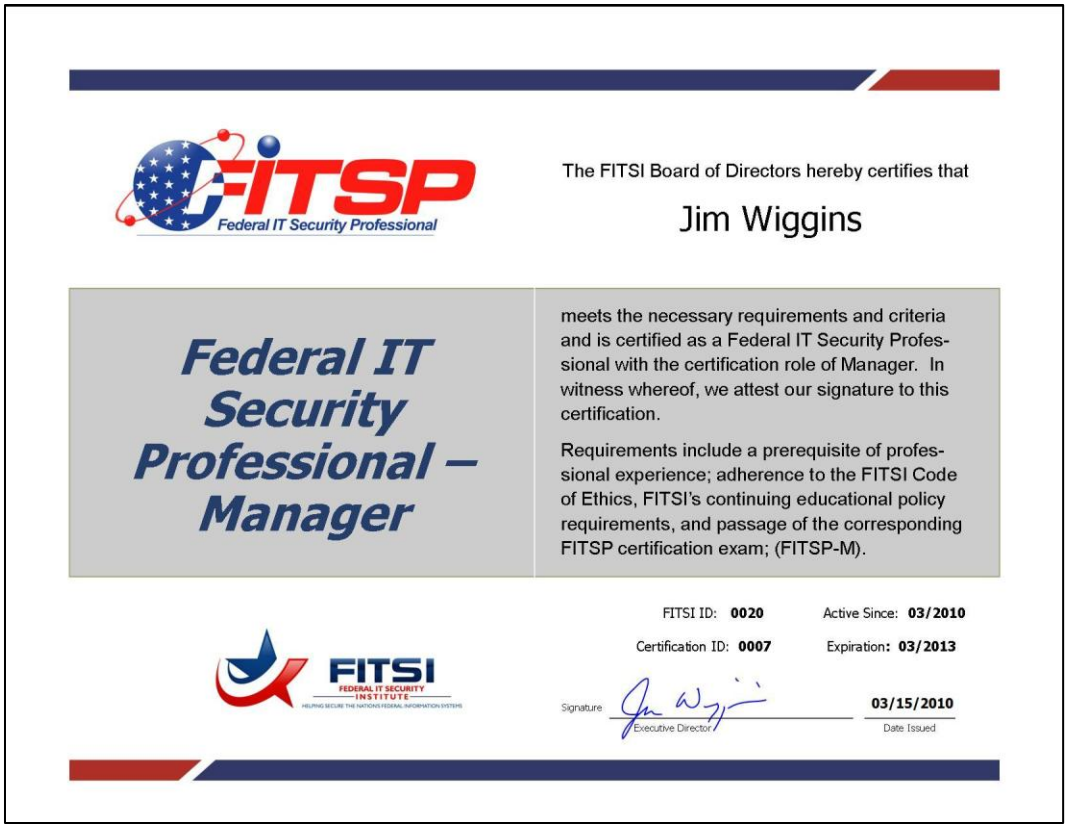


Figure 2: Example of a FITSP-Manager Certification

Figure 3: Example of a FITSI ID/Certification Card

Figure 4: Example of a FITSP Challenge Coin

All contents of the Certification Packet remain the property of FITSI. FITSI may withdraw, cancel, revoke or otherwise annul the certification for just cause as outlined in the Certification Holder Handbook.

Candidates who successfully pass the Certification exam, but cannot provide documentation outlining 5 years information technologies experience and two professional Endorsement Forms, shall not be granted certification. A denial of certification can be appealed by the candidate.

B. Results – Failing

Candidates who fail to meet the exam criteria to pass the exam will be notified at the completion of the exam via the Exam Score Report. No other documentation will be sent.

C. Retesting

Candidates who fail to achieve to a passing score will be eligible to take the test again, for a re-testing fee, after a waiting period of 21 calendar days. Candidates who fail to re-take the exam in a one year period will be charged at the initial exam rate. Candidates who wish to re-take the exam must notify FITSI via email at contactus@FITSI.org.

D. Appeals Policy

Any decision rendered by one of FITSI committees, staff or consultant that impacts a FITSI member or candidate can be appealed through the FITSI Appeals Committee. All appeals must be made within 30 calendar days of the receipt of the decision being appealed.

Appeals can be submitted to FITSI regarding one of the following areas:

- Certification Denial
- Certification Revocation
- Refund Refusal
- Other decisions and/or issues

An appeal can be filed by submitting the appeals forms found at the following website: http://www.fitsi.org/documents. This form should be filled out and emailed to FITSI at contactus@fitsi.org.

Once an appeals form is received FITSI will carry out the following steps:

1. Initial Appeal Acknowledgement
   Receipt of an appeal shall be acknowledged within 30 calendar days of receipt. The acknowledgement will include:
   - Email acknowledging the appeal
   - The appeals process for issue at hand
   - An Appeals Committee member point of contact
   - A timeline for response and action by the Appeals Committee

2. Appeals Review
   Appeals received shall be reviewed by the Appeals Committee within 30 calendar days of receipt. A response will be sent to the appellant within 30 calendar days. All responses shall be sent electronically.

3. Appeals Decision/Response
   The response from the Appeals Committee will be one of the following:
   - Appeal denied
   - Appeal accepted
   - Request for more information

   All responses will include a detailed explanation of the response.

4. Appeals Escalation

All decisions made by the Appeals Committee are considered final.

11. Code of Ethics

All candidates who pursue a FITSI certification must agree to abide by the FITSI Code of Ethics. Below are the tenets that all certification holders must agree to follow:

- Endeavor to protect the Nation's citizens, information systems, information, processes and facilities.
- Maintain a high level of personal integrity in any and all transactions with customers, stakeholders, colleagues and acquaintances.
- Maintain the confidentiality of all sensitive information (i.e.: Personally Identifiable Information) such that it does not create unnecessary risk for people and organizations.
- Refuse to engage in intentional activities that affect the availability of any and all IT systems and processes; both personally and professionally.
- Promote research and sharing of ideas and information that are worthy of such action. Give back to the community by adding value when possible.
- Refuse to foster FUD (Fear, Uncertainty and Doubt) in any and all interactions with both personal and professional relationships.
- Avoid conflicts of interest and recues oneself when appropriate.

Violations of any of this Code of Ethics can be grounds for revocation of a certification holder's certification(s) and/or membership (where applicable) in FITSI.

12. Maintenance Requirements

All FITSP certifications are valid for three years but can be revoked by FITSI for violations of the Code of Ethics or other egregious acts that undermine the good character that must be demonstrated by a holder of a FITSP certification. FITSP certification holders must earn Continuing Professional Education (CPE) units. A minimum of 20 CPEs is to be earned each year. Once a candidate is certified, they will be provided a private account at the FITSI website to login and record annual CPE activities.

In additional to earning 20 CPEs per year for the three year period, FITSP certification holders must pay a $45 annual certification maintenance fee to FITSI. If a FITSP candidate earns more than one FITSI certification they must earn 20 CPEs per year for each certification role.

FITSI has published a whitepaper titled "Earning CPEs for FITSI certification." This paper is available on the FITSI private portal at http://www.fitsi.org and provides detailed guidance on how a certification holder should log CPEs. This document is also provided to new certification holders when they receive their FITSI certification in the mail.

13. Recertification Requirements

Once a candidate becomes certified, the certification is good for three years. Candidates must maintain their certification by paying a $45 annual maintenance fee and earn a minimum of 20 CPEs per year. Each three year period will be automatically renewed as long as the member maintains their CPEs and membership fee requirements current.

14. Forms

The most current version of the forms referenced in this handbook can be downloaded from the following website:

http://www.fitsi.org/documents

FITSI Contact Information

Certification Exam Registration web address:
http://www.fitsi.org

FITSI Corporate Contact Information:

Federal IT Security Institute (FITSI)
3213 Duke St.
Suite 190
Alexandria, VA 22314

Phone: 703-828-1196
Fax: 703-754-8215
Web site: http://www.fitsi.org
General Email: contactus@fitsi.org

Resumes submission: contactus@fitsi.org
Exam rescheduling request: contactus@fitsi.org – please indicate "reschedule" in the subject line
Exam Hardship rescheduling request: contactus@fitsi.org – please indicate "hardship" in the subject line.
Exam Comments: contactus@fitsi.org – please indicate "comments" in the subject line
Change of address: contactus@fitsi.org – please indicate "change of address" in the subject line.

15. Appendixes

Appendix A – Federal Body of Knowledge Breakdown

The purpose of this section is to provide the reader with a broad overview of the domains and topic areas. Because the exam focuses on federal statutes, regulations, standards, and guidelines, this guide provides a breakdown for each FITSP domain and topic area.

The reader advised that this document serves simply as a reference on what constitutes the boundary of the Federal Body of Knowledge (FBK).

Domains

Domain 1 – NIST Special Publications

NIST Special Publications are written to provide guidance and best practices to federal agencies on how to protect the agency's missions, business functions, and environment of operation. These publications can be downloaded for free at the following website: http://csrc.nist.gov.

1. 800-12 -An Introduction to Computer Security: The NIST Handbook
2. 800-13 - Telecommunications Security Guidelines for Telecommunications Management Network
3. 800-14- Generally Accepted Principles and Practices for Securing Information Technology Systems
4. 800-16 - Information Technology Security Training Requirements: A Role- and Performance-Based Model
5. 800-18 Rev 1 - Guide for Developing Security Plans for Federal Information Systems
6. 800-21 2nd Ed - Guideline for Implementing Cryptography in the Federal Government
7. 800-23 - Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products
8. 800-24 - PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does
9. 800-25 - Federal Agency Use of Public Key Technology for Digital Signatures and Authentication
10. 800-27 Rev A - Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
11. 800-28 Version 2 - Guidelines on Active Content and Mobile Code
12. 800- 30 - Risk Management Guide for Information Technology Systems
13. 800-32 - Introduction to Public Key Technology and the Federal PKI Infrastructure
14. 800-33 - Underlying Technical Models for Information Technology Security
15. 800-35 - Guide to Information Technology Security Services
16. 800-36 - Guide to Selecting Information Technology Security Products
17. 800-37 Rev 1 - Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
18. 800-40 Version 2 - Creating a Patch and Vulnerability Management Program
19. 800-41Rev 1 - Guidelines on Firewalls and Firewall Policy
20. 800-44 Version 2 - Guidelines on Securing Public Web Servers
21. 800-45 Version 2 - Guidelines on Electronic Mail Security
22. 800-46 Rev 1 - Guide to Enterprise Telework and Remote Access Security
23. 800-47 - Security Guide for Interconnecting Information Technology Systems
24. 800-48 Rev 1 - Guide to Securing Legacy IEEE 802.11 Wireless Networks
25. 800-49 - Federal S/MIME V3 Client Profile
26. 800-50 - Building an Information Technology Security Awareness and Training Program
27. 800-51 - Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme
28. 800-52 - Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations

29. 800-53 Rev4 - Security and Privacy Controls for Federal Information Systems and Organizations
30. 800-53A - Guide for Assessing the Security Controls in Federal Information Systems
31. 800-55 Rev 1 - Performance Measurement Guide for Information Security
32. 800-56 A - Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography
33. 800-57 - Recommendation for Key Management
34. 800-60 Rev 1 - Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes) - Volume 1: Guide Volume 2: Appendices
35. 800-61 Rev 1 - Computer Security Incident Handling Guide
36. 800-63 Version 1.0.2 - Electronic Authentication Guideline
37. 800-64 Rev 2 – Security Considerations in the System Development Life Cycle
38. 800-65 - Integrating IT Security into the Capital Planning and Investment Control Process
39. 800-66 Rev 1 - An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
40. 800-70 Rev 1 - Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developer
41. 800-77 - Guide to IPSec VPNs
42. 800-78-2 - Cryptographic Algorithms and Key Sizes for Personal Identity Verification
43. 800-79-1 - Guidelines for the Accreditation of Personal Identity Verification (PIV) Card Issuers (PCI's)
44. 800-81 - Secure Domain Name System (DNS) Deployment Guide
45. 800-83 - Guide to Malware Incident Prevention and Handling
46. 800-84 - Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities
47. 800-86 - Guide to Integrating Forensic Techniques into Incident Response
48. 800-87 Rev 1 - Codes for Identification of Federal and Federally-Assisted Organizations
49. 800-88 - Guidelines for Media Sanitization
50. 800-89 - Recommendation for Obtaining Assurances for Digital Signature Applications
51. 800-92 - Guide to Computer Security Log Management
52. 800-94 - Guide to Intrusion Detection and Prevention Systems (IDPS)
53. 800-95 - Guide to Secure Web Services
54. 800-96 - PIV Card to Reader Interoperability Guidelines
55. 800-97 - Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i
56. 800-98 - Guidelines for Securing Radio Frequency Identification (RFID) Systems
57. 800-100 - Information Security Handbook: A Guide for Managers
58. 800-107 - Recommendation for Applications Using Approved Hash Algorithms
59. 800-111 - Guide to Storage Encryption Technologies for End User Devices
60. 800-113 - Guide to SSL VPNs
61. 800-114 - User's Guide to Securing External Devices for Telework and Remote Access
62. 800-115 - Technical Guide to Information Security Testing and Assessment
63. 800-121 - Guide to Bluetooth Security
64. 800-122 - Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
65. 800-123 - Guide to General Server Security
66. 800-124 - Guidelines on Cell Phone and PDA Security
67. 800-128 - Guide for Security-Focused Configuration Management of Information Systems
68. 800-137 - Information Security Continuous Monitoring for Federal Information Systems and Organizations

Domain 2 - NIST Federal Information Processing Standards

Below is the list of all NIST Federal Information Processing Standards (FIPS) that are included in the FBK. These standards can be downloaded at the following website: http://csrc.nist.gov.

1. FIPS 201-1 - Personal Identity Verification (PIV) of Federal Employees and Contractors
2. FIPS 200 - Minimum Security Requirements for Federal Information and Information Systems
3. FIPS 199 - Standards for Security Categorization of Federal Information and Information Systems
4. FIPS 198-1 - The Keyed-Hash Message Authentication Code
5. FIPS 197 - Advanced Encryption Standard
6. FIPS 196 - Entity Authentication Using Public Key Cryptography
7. FIPS 191 - Guideline for the Analysis of Local Area Network Security
8. FIPS 190 - Guideline for the Use of Advanced Authentication Technology Alternatives
9. FIPS 188 - Standard Security Label for Information Transfer
10. FIPS 186-3 - Digital Signature Standard (DSS)
11. FIPS 185 - Escrowed Encryption Standard
12. FIPS 181 - Automated Password Generator
13. FIPS 180-3 - Secure Hash Standard (SHS)
14. FIPS 140-2 - Security Requirements for Cryptographic Modules
15. FIPS 113 - Computer Data Authentication (no electronic version available)

Domain 3 - NIST Control Families

NIST SP 800-53 Rev3 identifies 18 control families that must be incorporated into the design of federal systems. These control families are broken into three categories of controls (management, technical and operational).

1. Access Control
2. Awareness and Training
3. Audit and Accountability
4. Security Assessment and Authorization
5. Configuration Management
6. Contingency Planning
7. Identification and Authentication
8. Incident Response
9. Maintenance
10. Media Protection
11. Physical and Environmental Protection
12. Planning
13. Personnel Security
14. Risk Assessment
15. System and Services Acquisition
16. System and Communication Protection
17. System and Information Integrity
18. Program Management (organization level)

Domain 4 - Government Laws and Regulations

Listed below are the Acts of Congress, OMB memos, executive orders and presidential directives that impact federal IT systems. Acts of Congress, executive orders and presidential directive are available at a number of Internet locations. OMB memos and bulletins can be obtained from http://www.whitehouse.gov/omb.

1. Acts of Congress

a) Privacy Act of 1974
    a. as amended 5 U.S.C. § 552a.
b) Paperwork Reduction Act of 1980
    a. 44 USC § 3501, et. seq.
c) Computer Security Act of 1987
    a. Replaced by FISMA and is no longer in effect
d) Chief Financial Officers Act of 1990
e) Government Performance and Results Act of 1993
f) Paperwork and Elimination Act of 1998
g) Government Information Security Reform Act
    a. Replace by FISMA and is no longer in effect
h) Federal Information Security Management Act of 2002
    a. 44 U.S.C. 3541, et. Seq.
i) Health Insurance Portability and Accountability Act
j) Clinger-Cohen Act of 1996

2. OMB Memorandums

a) M-09-32 – Update on the Trusted Internet Connections Initiative
b) M-09-29 - FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management
c) M-09-02 - Information Technology Management Structure and Governance Framework
d) M-08-27 - Guidance for Trusted Internet Connection (TIC) Compliance
e) M-08-23 - Securing the Federal Government's Domain Name System Infrastructure
f) M-08-22 - Guidance on the Federal Desktop Core Configuration (FDCC)
g) M-08-21 – FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management
h) M-08-16 – Guidance for Trusted Internet Connection Statement of Capability Form (SOC)
i) M-08-09 – New FISMA Privacy Reporting Requirements for FY 2008
j) M-08-05 - Implementation of Trusted Internet Connections (TIC)
k) M-08-01 - HSPD-12 Implementation Status
l) M-07-19 – FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management
m) M-07-18 - Ensuring New Acquisitions Include Common Security Configurations
n) M-07-16 - Safeguarding Against and Responding to the Breach of Personally Identifiable Information
o) M-07-11 - Implementation of Commonly Accepted Security Configurations for Windows Operating Systems
p) M-07-06 - Validating and Monitoring Agency Issuance of Personal Identity Verification Credentials
q) Recommendations for Identity Theft Related Data Breach Notification
r) M-06-20 - FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management
s) M-06-19 - Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments
t) M-06-18 - Acquisition of Products and Services for Implementation of HSPD-12
u) M-06-16 - Protection of Sensitive Agency Information
v) M-06-15 - Safeguarding Personally Identifiable Information
w) M-06-06 - Sample Privacy Documents for Agency Implementation of Homeland Security Presidential Directive (HSPD) 12
x) M-05-24 - Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors

y) M05-16 - Regulation on Maintaining Telecommunication Services During a Crisis or Emergency in Federally-owned Buildings
z) M05-15 - FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management
a) M-05-08 - Designation of Senior Agency Officials for Privacy
b) M-05-05 - Electronic Signatures: How to Mitigate the Risk of Commercial Managed Services
c) M-05-04 - Policies for Federal Agency Public Websites
d) M-04-26 - Personal Use Policies and "File Sharing" Technology
e) M-04-25 – FY 2004 Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting
f) M-04-16 - Software Acquisition
g) M-04-15 - Development of Homeland Security Presidential Directive (HSPD) - 7 Critical Infrastructure Protection Plans to Protect Federal Critical Infrastructures and Key Resources
h) M-04-04 - E-Authentication Guidance for Federal Agencies
i) M-03-22 - OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
j) M-03-19 - FY 2003 Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting
k) M-03-18 - Implementation Guidance for the E-Government Act of 2002
l) M-02-09 - Reporting Instructions for the Government Information Security Reform Act and Updated Guidance on Security Plans of Action and Milestones
a) M-02-01 - Guidance for Preparing and Submitting Security Plans of Action and Milestones
b) M-01-24 - Reporting Instructions for the Government Information Security Reform Act
c) M-01-08 - Guidance on Implementing the Government Information Security Reform Act
d) M-01-05 - Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy
e) M-00-13 - Privacy Policies and Data Collection on Federal Web Sites
a) M-00-10 - OMB Procedures and Guidance on Implementing the Government Paperwork Elimination Act
b) M-00-07 - Incorporating and Funding Security in Information Systems Investments
c) M-00-01 - Day One Planning and Request for Updated Business Continuity and Contingency Plans
d) M-99-20 - Security of Federal Automated Information Resources
e) M-99-18 - Privacy Policies on Federal Web Sites
f) M-99-16 - Business Continuity and Contingency Planning for the Year 2000

3. OMB Circular

a) Office of Management and Budget Circular A-11, Preparation, Submission and Execution of the Budget, June 2008
b) Office of Management and Budget Circular A-123, Management Responsibility for Internal Control, December 2004
c) Office of Management and Budget Circular A-127-Revised, Financial Management Systems, January 2009
d) Office of Management and Budget Circular A-130, Appendix III, Security of Federal Information Resources
e) Executive Office of the President, Office of Management and Budget, Office of Federal Procurement Policy, Emergency Acquisitions, May 2007

4. Homeland Security President Directives

a) HSPD-3 – Homeland Security Advisory System
b) HSPD-5 – Management of Domestic Incidents
c) HSPD-7 – Critical Infrastructure Identification, Prioritization, and Protection
d) HSPD-8 – National Preparedness

e) HSPD-12 – Policy for a Common Identification Standard for Federal Employees and Contractors
f) HSPD-20/NSPD-51 – National Continuity Policy
g) HSPD-24 – Biometrics for Identification and Screening to Enhance National Security

5. Executive Orders

a) EO 12958 – Classified National Security Information
b) 36 Code of Federal Regulation Part 1236, *Management of Vital Records*, revised as of July 1, 2000
c) 41 Code of Federal Regulations 101.20.103-4, *Occupant Emergency Program*, revised as of July 1, 2000
d) EO 12472 – Assignment of National Security and Emergency Preparedness Telecommunications Functions
e) EO 12656 – Assignment of Emergency Preparedness Responsibilities
f) EO 13231 – Critical Infrastructure Protection in the Information Age
g) FCD 1 – Federal Executive Branch National Continuity Program and Requirements, Feb 2008
h) FCD 2 – Federal Executive Branch Mission Essential function and Primary Mission Essential Function Identification and Submission Process, Feb 2008

6. Federal Audit Standards

a) Government Audit Standards (Yellow Book)
b) GAO / PCIE Financial Audit Manual (FAM)
c) GAO Federal Information Systems Control Audit Manual (FISCAM)

Domain 5 - NIST Risk Management Framework (formerly C&A)

The Risk Management Framework deals with system authorization and is identified in NIST Special Publication 800-37 Rev1 and supporting documents. These special publications and standards can be downloaded at the following website: http://csrc.nist.gov.

1. 800-18 Rev1 - Guide for Developing Security Plans for Federal Information Systems
2. 800-34 - Contingency Planning Guide for Information Technology Systems
3. 800-47 - Security Guide for Interconnecting Information Technology Systems
4. 800-53 Rev3 - Recommended Security Controls for Federal Information Systems
5. 800-53A - Guide for Assessing the Security Controls in Federal Information Systems
6. 800-37 Rev1 - Guide for the Security Certification and Accreditation of Federal Information Systems
7. 800-59 - Guideline for Identifying an Information System as a National Security System
8. 800-60 Rev1- Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes)
9. 800-66 - An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
10. 800-115 - Technical Guide to Information Security Testing and Assessment
11. FIPS 200 - Minimum Security Requirements for Federal Information and Information Systems
12. FIPS 199 - Standards for Security Categorization of Federal Information and Information Systems

Domain 6 - NIST Interagency Reports

NIST Interagency or Internal Reports (NISTIRs) describe research of a technical nature of interest to a specialized audience. These NISTIRs can be downloaded at the following website: http://csrc.nist.gov.

1. IR 7581 - System and Network Security Acronyms and Abbreviations
2. IR 7564 - Directions in Security Metrics Research
3. IR 7536 - 2008 Computer Security Division Annual Report
4. IR 7459 - Information Security Guide for Government Executives
5. IR 7358 - Program Review for Information Security Management Assistance (PRISMA)
6. IR 7316 - Assessment of Access Control Systems
7. IR 7298 - Glossary of Key Information Security Terms
8. IR 7206 - Smart Cards and Mobile Device Authentication: An Overview and Implementation

IT Security Topic Areas

The purpose of this listing is to provide a basic understanding of key terms and concepts rather than offer an exhaustive list. Knowledge of these terms and concepts is the foundation for effective performance of job functions associated with each of the management, operational and technical topic areas.

Seventeen of the 21 IT Security topic areas are derived from the requirements defined in the Federal Information Processing Standard 200 (FIPS 200). One of the topic areas, Program Management, is new and comes from NIST SP 800-53 Rev3 (Appendix G). Three of the topic areas (Application Security, Data Security and Regulatory and Standards Compliance) are derived from the DHS EBK.

Topic Area 1 – Access Control

This topic area refers to the knowledge and understanding that organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

• Access	• Least Privilege
• Access Authority	• Mandatory Access Control (MAC)
• Access Control	• Permitted Actions
• Access Control List	• Previous Login Notification
• Account Management	• Role Based Access Control (RBAC)
• Access Enforcement	• Security Attributes
• Authorization	• Separation of Duties
• Brute Force	• Session Lock
• Concurrent Session Control	• Session Termination
• Discretionary Access Control (DAC)	• System Use Notification
• Information Flow Enforcement	• Unsuccessful Login Attempt

Topic Area 2 – Application Security

This topic area refers to the knowledge and understanding that organizations need to address security requirements in software development, handle the translation of security requirements into application design elements, and deal with the development of secure code and exploit mitigation.

• Application Controls	• Secure System Design
• Baseline Security	• Security Change Management
• Certification	• Security Requirements Analysis
• Configuration Management	• Security Specifications
• Patch Management	• Security Testing and Evaluation
• Process Maturity	• Security Vulnerability Analysis

• Risk Assessment • Risk Mitigation • Secure Coding • Secure Coding Principles • Secure Coding Tools	• Software Assurance • System Development Life Cycle (SDLC) • System Engineering • Technical Security Controls • Virtualization Technology

Topic Area 3 – Audit and Accountability

This topic area refers to the knowledge and understanding that organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

• Accountability • Auditable Event • Audit • Audit Analysis • Audit Data • Audit Generation • Audit Policy • Audit Record Retention • Audit Reduction Tool • Audit Report • Audit Reduction	• Audit Review • Audit Trail • Audit Storage Capacity • Audit Failure Response • Contents of Audit Record • Monitoring for Information Disclosure • Non-repudiation • Protection of Audit Information • Session Audit • Time Stamps

Topic Area 4 – Awareness and Training

This topic area refers to the knowledge and understanding that organizations must: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

• Awareness (Information Security) • Behavioral Outcome • Certification • Computer Based Training (CBT) • Curriculum • Education (Information Security) • End User Security Training • Information Sharing • Instructional Systems Design (ISD)	• IT Security Education • IT Security Training Program • Learning Management System (LMS) • Learning Objectives • Needs Assessment (IT Security) • Role-Based Training • Testing • Training (Information Security) • Training Assessment

• Instructor Led Training (ILT) • IT Security Awareness • IT Security Awareness and Training Program	• Training Effectiveness • Training Effectiveness Evaluation • Web Based Training (WBT)

Topic Area 5 – Configuration Management

This topic area refers to the knowledge and understanding that organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.

• Access Restriction for Change • Baseline Configuration • Configuration Change • Configuration Management Plan • Configuration Management Policy	• Configuration Setting • Federal Desktop Core Configuration • Least Functionality • Security Checklists • Security Impact Analysis

Topic Area 6 – Contingency Planning

This topic area refers to the knowledge and understanding that organizations must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

• Alternate Processing / Storage Site • Backup Strategy • Business Continuity Plan • Business Impact Analysis • Business Recovery Plan • Call Tree • Cold Site • Contingency Plan • Contingency Plan Policy • Contingency Plan Training • Contingency Plan Testing • Continuity of Operations Plan • Continuity of Support Plan • Crisis Communication • Cyber Incident Response • Delegation of Authority • Disaster Recovery Plan	• Disruption • Essential Functions • Hot Site • Information Technology • Interoperable Communications • Mission Assurance • Occupant Emergency Plan • Order of Succession • Preparedness/Readiness • Reconstitution • Recovery • Risk Mitigation • Standard Operating Procedures • Telecommunications Services • Threat Environment • Vital Records and Databases • Warm Site

Topic Area 7 – Data Security

This topic area refers to the knowledge and understanding that organizations must protect information and information systems at the appropriate level of confidentiality, integrity and availability.

• Access Control • Adequate Security • Aggregation • Antivirus Software • Assurance • Authentication • Authorization • Availability • Chain of Custody • Confidentiality • Data Classification • Decryption • Digital Signatures • Discretionary Access Control • Electronic Commerce • Encryption • Firewall Configuration • Identity Data and Access Management • Identity Management • Information Classification Scheme	• Integrity • Least Privilege • Mandatory Access Control • Need-to-Know • Non-repudiation • Personally Identifiable Information • Privacy • Privilege Levels • Public Key Infrastructure • Role-Based Access Control • Rule-Based Access Control • Secure Data Handling • Security Clearance • Sensitive Information • Sensitivity Determination • Sensitivity of Data • Steganography • System of Record • User Privileges • User Provisioning

Topic Area 8 – Identification and Authentication

This topic area refers to the knowledge and understanding that organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

• Authenticate • Authentication • Authentication Mechanism • Authentication Mode • Authentication Protocol • Authentication Token • Authenticator Feedback • Authenticator Management • Authenticity • Biometric • Biometric System • Biometric Information • Device Authentication	• Device Identification • Digital Certificate • Certificate Policy • Certificate Revocation List (CRL) • Certification Authority • Claimant • Credential • Cryptographic Module Authentication • Electronic Authentication • Identification • Identifier Management • Mutual Authentication

Topic Area 9 – Incident Response

This topic area refers to the knowledge and understanding that organizations must: (i) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.

• Attack Signature	• Incident Response Testing
• Computer Forensics	• Incident Response Training
• Computer Security Incident	• Intrusion
• Computer Security Incident Response Team	• Intrusion Prevention System
• Computer Security	• Intrusion Detection System
• Escalation Procedures	• Measures
• Honey Pot	• Personally Identifiable Information (PII)
• Incident Handling	• Reconstitution of System
• Incident Monitoring	• Security Alerts
• Incident Records	• Security Incident
• Incident Reporting	• System Compromise
• Incident Response Assistance	• Threat Motivation
• Incident Response Plan	• Unauthorized Access
• Incident Response Policy	• Vulnerability

Topic Area 10 – Maintenance

This topic area refers to the knowledge and understanding that organizations must: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

• Antivirus Software	• Security Data Analysis
• Backup	• Security Measures
• Baseline	• Security Reporting
• Configuration Management	• System Hardening
• Controlled Maintenance	• System Logs
• Insider Threat	• System Maintenance Policy
• Maintenance Tools	• System Monitoring
• Maintenance Personnel	• Threat Analysis
• Non-Local Maintenance	• Threat Monitoring
• Patch Management	• Timely Maintenance
• Penetration Testing	• Vulnerability Analysis

Topic Area 11 – Media Protection

This topic area refers to the knowledge and understanding that organizations must: (i) protect information system media, both paper and digital; (ii) limit access to information

on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.

• Degaussing • Media Access • Media Destruction • Media Marking	• Media Protection Policy • Media Storage • Media Transport • Sanitization

Topic Area 12 – Personnel Security

This topic area refers to the knowledge and understanding that organizations must: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

• Access Agreement • Background Checks • Background Investigation • Confidentiality • Digital Identity • Human Resources • Insider Threat • Job Rotation • Nondisclosure Agreement • Position Categorization • Position Sensitivity • Personnel Sanctions	• Personnel Security Policy • Personnel Screening • Personnel Termination • Personnel Transfer • Security Breach • Security Clearance • Separation of Duties • Social Engineering • Special Background Investigation (SBI) • Suitability Determination • Third-Party Personnel Security

Topic Area 13 – Physical and Environmental Protection

This topic area refers to the knowledge and understanding that organizations must: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

• Access Cards • Access Control • Access Control for Output Devices • Access Control for Transmission Medium • Access Records • Alarm	• Inventory • Location of Information System Components • Manmade Threat • Monitoring Physical Access • Natural Threat • Perimeter Defense

• Alternate Work Site • Asset Disposal • Biometrics • Defense-in-Depth • Delivery and Removal • Emergency Lighting • Emergency Power • Environmental Threat • Fire Protection • Information Leakage	• Physical and Environmental Policy • Physical Access Authorization • Physical Access Control • Power Equipment and Power Cabling • Risk Management • Temperature and Humidity Control • Threat and Vulnerability Assessment • Video Surveillance • Visitor Control • Water Damage Protection

Topic Area 14 – Planning

This topic area refers to the knowledge and understanding that organizations must develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

• Privacy Impact Assessment • Rules of Behavior • Security Planning Policy	• Security Planning Procedures • Security Related Activity Planning • System Security Plan

Topic Area 15 – Program Management

This topic area refers to the knowledge and understanding that organizations are required to implement security program management controls to provide a foundation for the organization's information security program.

• Critical Infrastructure Plan • Enterprise Architecture • Information Security Measures of Performance • Information Security Program Plan • Information Security Resources	• Information System Inventory • Mission/Business Process Definition • Security Authorization Process • Senior Information Security Officer • Plan of Action and Milestones Process • Risk Management Strategy

Topic Area 16 – Regulatory and Standards Compliance

This topic area refers to the application of principles, policies, and procedures that enable an organization to meet applicable information security laws, regulations, standards, and policies to satisfy statutory requirements, perform industry-wide best practices, and achieve information security program goals.

• Accountability • Assessment • Auditing • Certification • Compliance • Ethics • Evaluation • Governance • Laws	• Policy • Privacy Principles • Procedure • Regulations • Security Program • Standards • Validation • Verification

Topic Area 17 – Risk Assessment

This topic area refers to the knowledge and understanding that organizations must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

• Acceptable Risk • Assessment • Asset Valuation • Business Impact Analysis • Controls • Impact • Inside Threat • Likelihood Determination • National Vulnerability Database • Qualitative • Quantitative • Risk • Risk Assessment • Risk Assessment Policy • Risk Avoidance • Risk Level	• Risk Limitation • Risk Management • Risk Matrix • Risk Mitigation • Risk Research • Risk Scale • Risk Transference • Security Categorization • Security Controls • Security Measures • Threat • Threat and Vulnerability • Threat Modeling • Types of Risk • Vulnerability • Vulnerability Scanning

Topic Area 18 – Security Assessments and Authorization

(Formerly Certification, Accreditation, and Security Assessments)

This topic area refers to knowledge and understanding that organizations must: (i) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

• Assessment Method • Assessment Procedure • Authorization (to operate) • Authorization Boundary • Authorize Process • Authorizing Official • Designated Representative • Dynamic Subsystem • Common Control Provider • Common Control • Compensating Control • Complex Information System • Continuous Monitoring • Cost Effective • Critical Control • External Subsystems	• Hybrid Security Control • Information Owner/Steward • Information System Boundary • Information System Owner • Information System Security Engineer • Information Type • Interconnection Agreement • Net-centric Architecture • Plan of Action and Milestones (POAM) • Reciprocity • Risk Executive • Security Control Assessor • Senior Information Security Officer • Tailored Security Control Baseline • Volatile Control

Topic Area 19 – System and Communication Protection

This topic area refers to the knowledge and understanding that organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

• Application Partitioning • Boundary Protection • Collaborative Computing Devices • Communications Security • Configuration • Covert Channel Analysis • Cryptographic Key Establishment • Cryptographic Key Management • Defense-in-Depth	• Penetration Testing • Port • Protection of Information at Rest • Public Access Protections • Public Key Infrastructure Certificates • Resource Priority • Router • Secure Name Resolution • Security Function Isolation

• Denial of Service Protection • Emission Security • Encryption Technologies • Fail in Known State • Firewall • Heterogeneity • Honeypots • Hub • Information in Shared Resources • Information System Partitioning • Intrusion Detection System • Intrusion Prevention Systems • Load Balancers • Mobile Code • Network Architecture • Network Disconnect • Networking Models and Protocols • Network Segmentation • Non-Modifiable Executable Programs	• Security Trust • Session Authenticity • Switch • System and Communications Protection Policy • Telecommunications Technology • Thin Nodes • Transmission Confidentiality • Transmission of Security Attributes • Transmission Integrity • Transmission Preparation Integrity • Trusted Path • Use of Cryptography • Virtual Private Network (VPN) • VOIP • Virtualization Techniques • Vulnerability • Web Services Security • Wired and Wireless Networks

Topic Area 20 – System and Information Integrity

This topic area refers to the knowledge and understanding organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

• Agent • Antivirus Software • Application • Application Content Filtering • Blended Attack • Boot Sector Virus • Buffer Overflow • Computer Virus • Error Handling • Flaw Remediation • Information Input Restrictions	• Information Input Validation • Information Output Handling and Retention • Information System Monitoring • Macro Virus • Malicious Code Protection • Predictable Failure Prevention • Security Alerts, Advisories, and Directives • Security Functionality Verification • Spam Protection • Software and Information Integrity • System and Information Integrity Policy

Topic Area 21 – System and Services Acquisition

This topic area refers to the knowledge and understanding that organizations must: (i) allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure

that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

• Acquisitions • Allocation of Resources • Business Impact Analysis • Contract • Cost-Benefit Analysis • Critical Information System Components • Developer Configuration Management • Developer Security Testing • Disposal • External Information System Services • Information System Documentation • Life Cycle Support • Prequalification • Regulatory Compliance • Request for Information • Request for Proposal (RFP)	• Risk Analysis • Risk-Based Decision • Risk Mitigation • Security Engineering Principles • Security Requirements • Service Level Agreement (SLA) • System and Services Acquisition Policy • Software usage Restrictions • Solicitation • Supply Chain Protection • Statement of Objectives (SOO) • Statement of Work (SOW) • Total Cost of Ownership (TCO) • Trustworthiness • User Installed Software