FITSP-Auditor Exam Objectives Guide

An Overview of the Competencies Measured on the FITSP-A Certification

2010 Edition

This page is left intentionally blank

TABLE OF CONTENTS

1. Executive Overview

The FITSP-Auditor Exam Objectives Guide (EOG) provides a summary of the skills and competencies based on the topic areas from the Federal Body of Knowledge (FBK) that will appear on the FITSP-Auditor exam. These skills and competencies are outlined in the 21 topic areas of the FBK and come from three sources: 17 are derived from the minimum security requirements found in NIST Federal Information Processing Standard 200, one comes from NIST SP800-53 Rev3 Appendix G (Program Management), and three come from the Department of Homeland Security Essential Body of Knowledge (EBK).

Provided by the Federal IT Security Institute (FITSI), candidates can obtain this EOG free of charge at the Institute's website: http://www.fitsi.org. This document may be forwarded to professional colleagues but must be kept in its original form.

2. Relationship of the FITSI Exam Guides

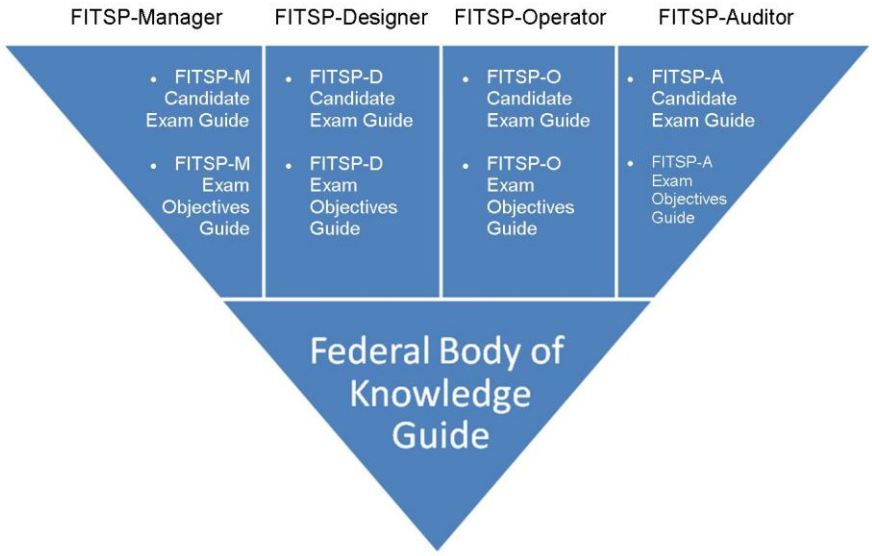
This guide is one of several documents published by FITSI to provide candidates with an understanding of the FITSP exam components. The three types of documents and their purposes are:

1. Candidate Exam Guide
   - Provides candidates with an overall understanding of the details of an exam for a particular FITSP certification role (Manager, Designer, Operator or Auditor).

2. Exam Objectives Guide
   - Provides the skills being measured and the exam objectives for a particular FITSP certification role (Manager, Designer, Operator or Auditor)

3. Federal Body of Knowledge Guide
   - Provides a detailed walkthrough of the set of domains, topics, publications and terminology that make up the FBK. This is an overarching document that provides the foundation for all the FITSP certification roles.

Below is a visual representation of how all these documents are interrelated:



3. FITSP-Auditor Exam Objectives

The FITSP-Auditor is focused on the FBK issues related to the high-level knowledge an IT auditor must possess to successfully audit and review cost-effective, risk-based IT security of systems operated by or on behalf of the federal government. 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-Auditor is expected to understand and be able to apply.

Access Control

- 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
- 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

- 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

- 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 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

- 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

- Audit baseline configurations to ensure maintenance throughout the respective system development life cycles (SDLC)
- Review inventories of 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

- 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

- 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 information and information systems

Identification and Authentication

- 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

- 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, documenting, and reporting of incidents to appropriate organizational officials and/or authorities

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

- 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

- Audit processes and controls that are compatible and consistent with an organization's information security program

Physical and Environmental Protection

- 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

- 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 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

- Audit controls that ensure individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy
- Review security mechanisms that 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

- 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

(Formerly Certification, Accreditation, and Security Assessments)

- 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
- 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

- 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

- 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
- 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

- 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

- Audit strategies for compliance with the organization's information security program
- Identify and stay current on all 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