FITSI FITSP-Auditor Certification Competence Breakdown

A Breakdown of the
Tasks, Knowledge,
and Skill Statements
on the
FITSP-Auditor
Certification

Version 3.0

Published 04/30/23

This page is left intentionally blank

Table of Contents

1. Overview

The FITSP-Auditor certification aims to recognize a candidate's competence to perform an "audit and assess role" for the management, operational, and technical IT security controls for systems owned by or operated on behalf of the United States Federal Government.

This document has been developed to detail how the competence is broken down into tasks, knowledge and skill statements, in the FITSP-Auditor certification role offered by the Federal IT Security Institute (FITSI). It can be used by FITSI stakeholders to understand what is being validated with FITSP Certification Candidate when they take the FITSP-Auditor certification exam.

2. Background

This section provides information regarding the sources used in developing this document.

A. Vocabulary Definitions

This document uses three terms that are defined in this section. The definitions of these terms are sourced from *ISO/IEC TS 17027:2014 - Conformity assessment — Vocabulary related to competence of persons used for certification of persons*. The three terms defined here are competence, knowledge, and skill.

- Competence - ability to apply knowledge and skills to achieve intended results.

- Knowledge - facts, information, truths, principles or understanding acquired through experience or education.

- Skill – ability to perform a task or activity with a specific intended outcome acquired through education, training, experience, or other means.

B. How FITSI Determines the Tasks, Knowledge, and Skills

The United States Congress mandates federal IT security requirements through laws. In 2002, Congress passed the Federal Information Security Management Act (FISMA). In section **§ 11331. Responsibilities for Federal information systems standards** of FISMA, the National Institute of Standards and Technology (NIST) is instructed to prescribe standards and guidelines pertaining to Federal information systems. NIST is required to provide minimum information security requirements and standards that apply to all Federal information systems. These standards are compulsory and binding to the extent determined necessary by the Secretary of Commerce to improve the efficiency of operation or security of Federal information systems.

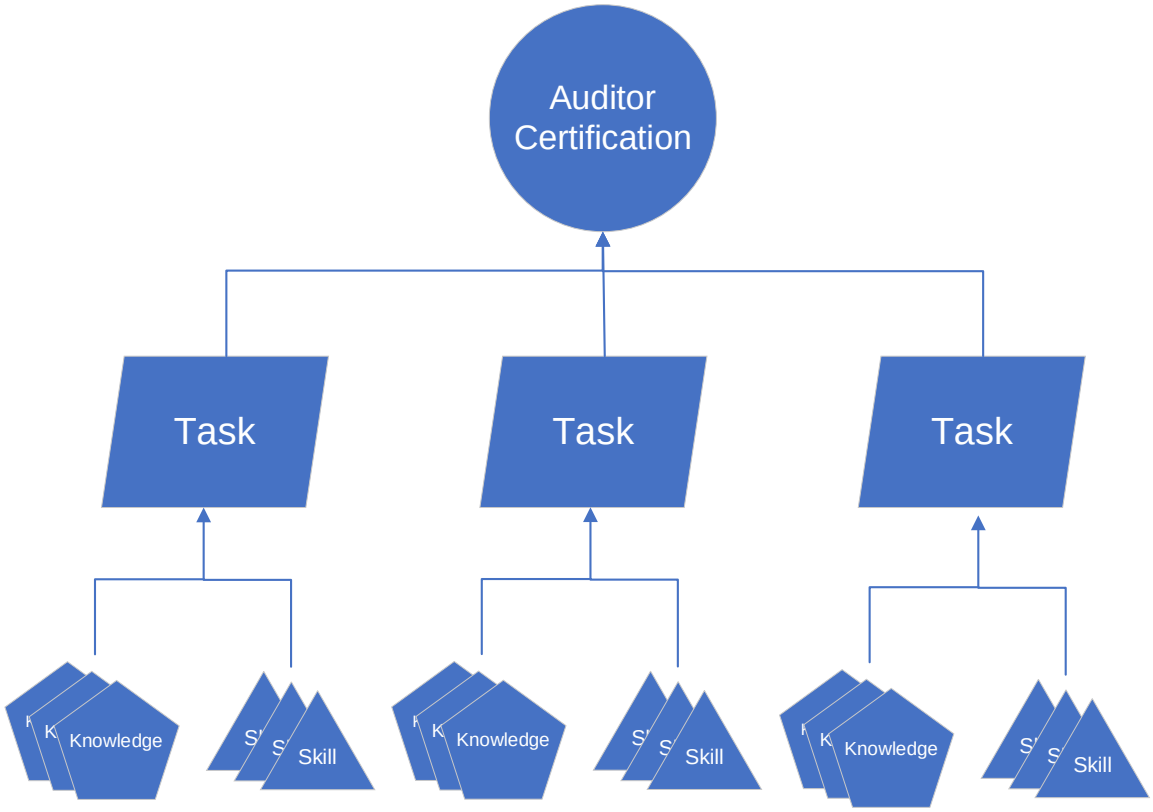
In March of 2006, NIST published Federal Information Processing Standard 200 (FIPS 200) entitled "Minimum Security Requirements for Federal Information and Information Systems." Federal agencies are required to be in compliance with this standard no later than one year from its effective date. FIPS 200 outlines all the tasks Federal information security practitioners must follow to protect and defend Federal information systems. **Noncompliance with these tasks in this standard is a violation of federal law.**

In 2014, Congress passed the Federal Information Security Moderation Act (FISMA 2014), reaffirming NIST's role in section **§ 11331** (above). Federal agencies are required to ensure timely agency adoption of and compliance with and compliance with standards promulgated under section 11331 of title 40.

FIPS 200 has 40 tasks that all practitioners must implement to support the requirements of federal agencies. The Tasks, Knowledge, and Skills defined in Section 3 of this document come directly from the FIPS 200 standard.

C. Visual Representation of the Certification Role, Tasks, Knowledge, and Skills

Below is a visual of how these items are used in the FITSP Certification Program.



3. Competence Breakdown

This section provides the breakdown of the Tasks and corresponding Knowledge Statements and Skill Statements of the Auditor certification role.

Topic #1 - Access Control

- Task #1 – Audit the limitation of 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.
    - Knowledge Statements
        - Knowledge of auditing and assessing security controls.
        - Knowledge of information systems.
        - Knowledge of information system access.
        - Knowledge of limiting access.
        - Knowledge of authorized users, process acting on behalf of authorized users, devices.
        - Knowledge of permitted transactions and functions.
    - Skills Statements
        - Ability to audit the limitation of information system access.

Topic #2 - Audit and Accountability

- Task #2 – Inspect the creation, protection, and retention of information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.
    - Knowledge Statements
        - Knowledge of auditing and assessing security controls.
        - Knowledge of information systems.
        - Knowledge of information system audit records.
        - Knowledge of unlawful, unauthorized, or inappropriate information system activity.
    - Skill Statements
        - Ability to audit the creation, protection, and retention of records.
        - Ability to audit the analysis, investigation, and reporting of information system activity.
- Task #3 – Evaluate elements to 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.
    - Knowledge Statements
        - Knowledge of auditing and assessing security controls.
        - Knowledge of actions of information system users.

        - Knowledge of holding users accountable for their actions.
    - Skill Statements
        - Ability to audit elements that trace users to their actions.

Topic #3 - Awareness and Training

- Task #4 – Review elements to 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.
    - Knowledge Statements
        - Knowledge of auditing and assessing security controls.
        - Knowledge of security risks of managers and users on organizational information systems.
        - Knowledge of applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures.
    - Skill Statements
        - Ability to audit elements ensuring managers and users are aware of the security risks associated with their activities.

- Task #5 – Assess elements to ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.
    - Knowledge Statements
        - Knowledge of auditing and assessing security controls.
        - Knowledge of training organizational personnel.
        - Knowledge of information system-related duties and responsibilities.
    - Skill Statements
        - Ability to audit the training of organizational personnel.

Topic #4 - Configuration Management

- Task #6 – Audit the establishment and maintenance of baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.
    - Knowledge Statements
        - Knowledge of auditing and assessing security controls.
        - Knowledge of baseline configurations and inventories.
        - Knowledge of information systems.
        - Knowledge of system development life cycles.

        - Knowledge of hardware, software, firmware, and documentation.
    - Skill Statements
        - Ability to audit configurations and inventories.
- Task #7 – Review the establishment and enforcement of security configuration settings for information technology products employed in organizational information systems.
    - Knowledge Statements
        - Knowledge of auditing and assessing security controls.
        - Knowledge of security configuration settings.
        - Knowledge of information technology products.
        - Knowledge of information systems.
    - Skill Statements
        - Ability to audit elements that establish and enforce settings.

Topic #5 - Contingency Planning

- Task #8 – Assess the establishment, maintenance, and effectiveness of 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.
    - Knowledge Statements
        - Knowledge of auditing and assessing security controls.
        - Knowledge of emergency response plans.
        - Knowledge of backup operations.
        - Knowledge of post-disaster recovery for an information system.
        - Knowledge of continuity of operations.
    - Skill Statements
        - Ability to audit contingency plans.
        - Ability to audit the availability of critical information resources.

Topic #6 - Identification and Authentication

- Task #9 – Review elements to ensure the identification of 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.
    - Knowledge Statements
        - Knowledge of auditing and assessing security controls.
        - Knowledge of identification and authentication.
        - Knowledge of users, processes, and devices.
    - Skill Statements

        - Ability to audit identification and authentication elements on organizational information systems.

Topic #7 - Incident Response

- Task #10 – Assess the establishment of an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.
    - Knowledge Statements
        - Knowledge of auditing and assessing security controls.
        - Knowledge of incident handling capabilities (preparation, detection, analysis, containment, recovery, and user response activities).
    - Skill Statements
        - Ability to audit incident handling capabilities.
- Task #11 – Inspect the tracking, documentation, and reporting of incidents to appropriate organizational officials or authorities.
    - Knowledge Statements
        - Knowledge of auditing and assessing security controls.
        - Knowledge of incidents.
        - Knowledge of organizational officials and authorities.
    - Skill Statements
        - Ability to audit the tracking, documenting, and reporting of incidents.

Topic #8 - Maintenance

- Task #12 – Audit the performability of periodic and timely maintenance on organizational information systems.
    - Knowledge Statements
        - Knowledge of auditing and assessing security controls.
        - Knowledge of maintenance of information systems.
    - Skill Statements
        - Ability to audit elements that perform maintenance activities.
- Task #13 – Review the provision of effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.
    - Knowledge Statements
        - Knowledge of auditing and assessing security controls.
        - Knowledge of security controls.
        - Knowledge of maintenance tools, techniques, and people.
    - Skill Statements
        - Ability to audit the provisioning of controls.

        - Ability to audit elements that perform information system maintenance.

Topic #9 - Media Protection

- Task #14 – Evaluate the protection of information system media, both paper and digital.
    - Knowledge Statements
        - Knowledge of auditing and assessing security controls.
        - Knowledge of media types (paper and digital).
        - Knowledge of media protections.
    - Skill Statements
        - Ability to audit the protection of media.
- Task #15 – Audit the limitation of access to information or information system media to authorized users.
    - Knowledge Statements
        - Knowledge of auditing and assessing security controls.
        - Knowledge of media types.
        - Knowledge of authorized users.
        - Knowledge of information types.
        - Knowledge of information systems.
    - Skill Statements
        - Ability to audit access control limitations.
- Task #16 – Review the sanitization or destruction of information system media before disposal or release for reuse.
    - Knowledge Statements
        - Knowledge of auditing and assessing security controls.
        - Knowledge of sanitation and distribution methods.
        - Knowledge of media types.
        - Knowledge of information systems.
    - Skill Statements
        - Ability to audit the sanitization or destruction of media.

Topic #10 - Personnel Security

- Task #17 – Evaluate elements to ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions.
    - Knowledge Statements
        - Knowledge of auditing and assessing security controls.
        - Knowledge of positions of responsibility.
        - Knowledge of third-party service providers.
        - Knowledge of security criteria for positions.
    - Skill Statements
        - Ability to audit trusted positions.

- Task #18 – Audit elements to ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers.
    - Knowledge Statements
        - Knowledge of auditing and assessing security controls.
        - Knowledge of information.
        - Knowledge of information systems.
        - Knowledge of protection methods.
        - Knowledge of terminations and transfers.
    - Skill Statements
        - Ability to audit protection methods.
- Task #19 – Review the employment of formal sanctions for personnel failing to comply with organizational security policies and procedures.
    - Knowledge Statements
        - Knowledge of auditing and assessing security controls.
        - Knowledge of formal sanctions for personnel.
        - Knowledge of security policies and procedures.
    - Skill Statements
        - Ability to audit formal sanctions for personnel.

Topic #11 - Physical and Environmental Protection

- Task #20 – Inspect the limitation of physical access to information systems, equipment, and the respective operating environments to authorized individuals.
    - Knowledge Statements
        - Knowledge of auditing and assessing security controls.
        - Knowledge of physical access.
        - Knowledge of information systems, equipment, and operating environments.
    - Skill Statements
        - Ability to audit the limitation of physical access to authorized individuals.
- Task #21 – Evaluate the protection of the physical plant and supporting infrastructure for information systems.
    - Knowledge Statements
        - Knowledge of auditing and assessing security controls.
        - Knowledge of physical plants.
        - Knowledge of supporting infrastructure.
        - Knowledge of information systems.
    - Skill Statements
        - Ability to audit the implementation of protections.
- Task #22 – Audit the provision of supporting utilities for information systems.
    - Knowledge Statements

        - Knowledge of auditing and assessing security controls.
        - Knowledge of supporting utilities.
        - Knowledge of information systems.
    - Skill Statements
        - Ability to audit the configuration of utilities.
- Task #23 – Review the protection of information systems against environmental hazards.
    - Knowledge Statements
        - Knowledge of auditing and assessing security controls.
        - Knowledge of information systems.
        - Knowledge of environmental hazards.
    - Skill Statements
        - Ability to audit controls for protection.
- Task #24 – Assess the provision of appropriate environmental controls in facilities containing information systems.
    - Knowledge Statements
        - Knowledge of auditing and assessing security controls.
        - Knowledge of environmental controls.
        - Knowledge of different types of facilities.
        - Knowledge of information systems.
    - Skill Statements
        - Ability to audit environmental controls.

Topic #12 - Planning

- Task #25 – Inspect the development, documentation, periodic update, and 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.
    - Knowledge Statements
        - Knowledge of auditing and assessing security controls.
        - Knowledge of security plans.
        - Knowledge of information systems.
        - Knowledge of security controls.
        - Knowledge of rules of behavior.
    - Skill Statements
        - Ability to audit security plans.

Topic #13 - Program Management

- Task #26 – Assess elements that ensure that security processes and controls are compatible and consistent with an organization's information security program.
    - Knowledge Statements
        - Knowledge of auditing and assessing security controls.

        - Knowledge of security processes.
        - Knowledge of security controls.
        - Knowledge of an information security program.
    - Skill Statements
        - Ability to audit controls for conformity with an information security program.

Topic #14 - Risk Assessment

- Task #27 – Assess the 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.
    - Knowledge Statements
        - Knowledge of auditing and assessing security controls.
        - Knowledge of risk.
        - Knowledge of conducting risk assessments.
        - Knowledge of organizational operations.
        - Knowledge of organizational assets.
        - Knowledge of information processing, storage, and transmission.
    - Skill Statements
        - Ability to audit elements that conduct risk assessments.

Topic #15 - Security Assessments and Authorization

- Task #28 – Inspect the periodic assessment of security controls in organizational information systems to determine if the controls are effective in their application.
    - Knowledge Statements
        - Knowledge of auditing and assessing security controls.
        - Knowledge of security controls.
        - Knowledge of information systems.
        - Knowledge of conducting security control assessments.
    - Skill Statements
        - Ability to audit security control assessments.
- Task #29 – Evaluate the development and implementation of plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems.
    - Knowledge Statements
        - Knowledge of auditing and assessing security controls.
        - Knowledge of POAMs.
        - Knowledge of vulnerabilities.
        - Knowledge of information systems.

    - Skill Statements
        - Ability to audit the correction of deficiencies and elimination of vulnerabilities.
- Task #30 – Audit the authorization of operation of organizational information systems and any associated information system connections.
    - Knowledge Statements
        - Knowledge of auditing and assessing security controls.
        - Knowledge of ATOs.
        - Knowledge of information systems.
        - Knowledge of information system connections.
    - Skill Statements
        - Ability to audit elements supporting the authorization of an information system.
- Task #31 – Review the monitoring of information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.
    - Knowledge Statements
        - Knowledge of auditing and assessing security controls.
        - Knowledge of security controls.
        - Knowledge of continuous monitoring methods.
    - Skill Statements
        - Ability to audit controls to ensure continued effectiveness.

Topic #16 - System and Communication Protection

- Task #32 – Assess the monitoring, controlling, and protection of organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
    - Knowledge Statements
        - Knowledge of auditing and assessing security controls.
        - Knowledge of organizational communications.
        - Knowledge of external boundaries.
        - Knowledge of internal boundaries.
        - Knowledge of information systems.
    - Skill Statements
        - Ability to audit controls for appropriate communication protections.
- Task #33 – Inspect the employment of architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.
    - Knowledge Statements
        - Knowledge of auditing and assessing security controls.
        - Knowledge of architectural designs.
        - Knowledge of software development techniques.

        - Knowledge of systems engineering principles.
        - Knowledge of information security.
        - Knowledge of information systems.
    - Skill Statements
        - Ability to audit elements for control effectiveness.

Topic #17 - System and Information Integrity

- Task #34 – Evaluate the identification, reporting, and correction of information and information system flaws in a timely manner.
    - Knowledge Statements
        - Knowledge of auditing and assessing security controls.
        - Knowledge of information systems.
        - Knowledge of information system flaws.
        - Knowledge of information.
    - Skill Statements
        - Ability to audit the identification, reporting, and correction of flaws.
- Task #35 – Audit the provision of protections from malicious code at appropriate locations within organizational information systems.
    - Knowledge Statements
        - Knowledge of auditing and assessing security controls.
        - Knowledge of malicious code.
        - Knowledge of information systems.
        - Knowledge of countermeasures to malicious code.
    - Skill Statements
        - Ability to audit malicious code protection.
- Task #36 – Review the monitoring of information system security alerts and advisories and take appropriate actions in response.
    - Knowledge Statements
        - Knowledge of auditing and assessing security controls.
        - Knowledge of information systems.
        - Knowledge of security alerts and advisories.
        - Knowledge of monitoring.
    - Skill Statements
        - Ability to audit alerts and responses.

Topic #18 - System and Services Acquisition

- Task #37 – Review the allocation of sufficient resources to adequately protect organizational information systems.
    - Knowledge Statements
        - Knowledge of auditing and assessing security controls.
        - Knowledge of information systems.
        - Knowledge of system resources.

        - Knowledge of protection methods (security controls).
    - Skill Statements
        - Ability to audit resources.
- Task #38 – Audit elements that employ system development life cycle processes that incorporate information security considerations.
    - Knowledge Statements
        - Knowledge of auditing and assessing security controls.
        - Knowledge of SDLC.
        - Knowledge of information systems.
        - Knowledge of information security.
    - Skill Statements
        - Ability to audit controls.
- Task #39 – Evaluate the use of software usage and installation restrictions.
    - Knowledge Statements
        - Knowledge of auditing and assessing security controls.
        - Knowledge of software.
        - Knowledge of software usage tracking methods.
        - Knowledge of ways to restrict software installation and usage.
    - Skill Statements
        - Ability to audit software usage controls.
- Task #40 – Audit elements that ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.
    - Knowledge Statements
        - Knowledge of auditing and assessing security controls.
        - Knowledge of third-party providers.
        - Knowledge of security controls.
        - Knowledge of information system outsourcing methods.
    - Skill Statements
        - Ability to audit elements to provide assurance from third-party providers.