FITSP-Auditor Exam Objectives

A Breakdown of the
Exam Objectives
Measured on the
FITSP-Auditor Exam

Version 2.1

Published 1/18/2018

This page is left intentionally blank

TABLE OF CONTENTS

1. FITSP-Auditor Exam Objectives Outline

This section provides the objectives that are measured by the FITSP-Auditor exam. The purpose here is to provide both the objectives as well as the schema framework to easily identify where an exam objective should fit within the schema.

Exam #1

Topic #1 - Access Control

- Objective #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.

Topic #2 - Audit and Accountability

- Objective #1 – 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.
- Objective #2 – 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.

Topic #3 - Awareness and Training

- Objective #1 – 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.
- Objective #2 – Assess elements to ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

Topic #4 - Configuration Management

- Objective #1 – 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.
- Objective #2 – Review the establishment and enforcement of security configuration settings for information technology products employed in organizational information systems.

Topic #5 - Contingency Planning

- Objective #1 – 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.

Topic #6 - Identification and Authentication

- Objective #1 – 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.

Topic #7 - Incident Response

- Objective #1 – 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.
- Objective #2 – Inspect the tracking, documentation, and reporting of incidents to appropriate organizational officials or authorities.

Topic #8 - Maintenance

- Objective #1 – Audit the performability of periodic and timely maintenance on organizational information systems.
- Objective #2 – Review the provision of effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

Topic #9 - Media Protection

- Objective #1 – Evaluate the protection of information system media, both paper and digital.
- Objective #2 – Audit the limitation of access to information or information system media to authorized users.
- Objective #3 – Review the sanitization or destruction of information system media before disposal or release for reuse.

Topic #10 - Personnel Security

- Objective #1 – 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.

- Objective #2 – Audit elements to ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers.
- Objective #3 – Review the employment of formal sanctions for personnel failing to comply with organizational security policies and procedures.

Topic #11 - Physical and Environmental Protection

- Objective #1 – Inspect the limitation of physical access to information systems, equipment, and the respective operating environments to authorized individuals.
- Objective #2 – Evaluate the protection of the physical plant and supporting infrastructure for information systems.
- Objective #3 – Audit the provision of supporting utilities for information systems.
- Objective #4 – Review the protection of information systems against environmental hazards.
- Objective #5 – Assess the provision of appropriate environmental controls in facilities containing information systems.

Topic #12 - Planning

- Objective #1 – 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.

Topic #13 - Program Management

- Objective #1 – Assess elements that ensure that security processes and controls are compatible and consistent with an organization's information security program.

Topic #14 - Risk Assessment

- Objective #1 – 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.

Topic #15 - Security Assessments and Authorization

- Objective #1 – Inspect the periodic assessment of security controls in organizational information systems to determine if the controls are effective in their application.

- Objective #2 – Evaluate the development and implementation of plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems.
- Objective #3 – Audit the authorization of operation of organizational information systems and any associated information system connections.
- Objective #4 – Review the monitoring of information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

Topic #16 - System and Communication Protection

- Objective #1 – 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.
- Objective #2 – Inspect the employment of architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

Topic #17 - System and Information Integrity

- Objective #1 – Evaluate the identification, reporting, and correction of information and information system flaws in a timely manner.
- Objective #2 – Audit the provision of protections from malicious code at appropriate locations within organizational information systems.
- Objective #3 – Review the monitoring of information system security alerts and advisories and take appropriate actions in response.

Topic #18 - System and Services Acquisition

- Objective #1 – Review the allocation of sufficient resources to adequately protect organizational information systems.
- Objective #2 – Audit elements that employ system development life cycle processes that incorporate information security considerations.
- Objective #3 – Evaluate the use of software usage and installation restrictions.
- Objective #4 – Audit elements that ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

	Revision History				
Version	Description of Change	Author	Approved By	Approval Date	Effective Date
2.0	Initial Release	Jim Wiggins	Jim Wiggins	12/1/2017	12/1/2017
2.1	1) Fixed order of Exam Objective Topics to make sure they are in alphabetical order	Jim Wiggins	Jim Wiggins	1/18/2018	1/18/2018