FITSI Exam Development Guide

An Overview of how to Develop Exam Questions for the FITSP Certification Exams

Version 2.2

Published 4/27/2020

This page is left intentionally blank

TABLE OF CONTENTS

1. Document Overview

The FITSI Exam Development Guide is for individuals who are responsible for exam question development for one of the four FITSP certification roles. FITSI item writing committees and FITSI members will use this guide to help write and develop questions that are consistent and compatible with the tasks and objectives that the FITSP certification exam measures.

First, this document includes a discussion of the schema used for exam item development efforts. The schema provides a logical framework for tracking how questions map back to the exam, topic area, and objectives.

Second, the document includes a discussion of Bloom's Taxonomy of Educational Objectives. Bloom's Taxonomy is used as the standard in education circles and uses six types of cognitive skills to be measured. The FITSP certification questions can be mapped back into one of these six cognitive skills.

Third, this document provides some sample questions that are categorized by the six cognitive skills within Bloom's Taxonomy. This section is meant to guide test writers who have never written a question based on these six skill areas.

Four, this document includes an outline of all the objectives for the four FITSI certifications (FITSP-Auditor, FITSP-Designer, FITSP-Manager, and FITSP-Operator) broken down by security topic number and objectives number.

Finally, the last section provides a worksheet template that provides guidance on how questions should be formatted, which allows tracking to the schema and taxonomy as well as includes the answers and references used in question development. Providing this level of detail is important as it helps audit the linkage of the question and answers.

2. FITSI Exam Development Schema

The FITSI exam development framework uses a schema represented in a numerical format. Each question can be tracked based on its schema reference. The FITSP exam development schema is broken down into three levels: 1) Exam 2) Security Topic Area and 3) Objective.

Four exams are represented numerically from 1-4: Auditor, Designer, Manager, and Operator.

18 Security Topic areas are represented numerically from 1-18: Access Control, Media Protection, Continuity Planning, etc.

There are up to 5 objectives that are represented numerically from 1-5: Objective #1, Objective #2, Objective #3, Objective #4, and Objective #5.

Below is an example of the FITSI exam development schema:

1. Exam
    1. Security Topic Area
        1. Objective

This schema means that a question will have schema reference in the form of ***X.X.X***. For example, the first objective for the FITSP-Manager exam in the Access Control topic is:

- "Manage 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."

Because the FITSP-Manager exam is the third in the group, it is listed with the number "3" in the first ***X***.

Since Access Control is the first security topic area, it is listed with the number "1" in the second ***X***.

Since this is the first objective in the security topic area, it is listed with the number "1" in the third ***X***.

Therefore, the schema reference for this objective is ***3.1.1***.

3. Use of Bloom's Taxonomy of Educational Objectives

The FITSP exam uses questions that follow Bloom's taxonomy of educational objectives. This taxonomy was first introduced in 1956 is a classification of learning objectives that have become the standard model for assessing knowledge used within education. It is broken into three basic domains; affective, psychomotor, and cognitive. Academia is predominantly focused on the cognitive domain, which deals with knowledge, comprehension, and critical thinking. Within the cognitive domain, six skills are identified. These six skills are used to help measure whether a candidate understands an idea, concept, or theory at a sufficiently deep enough level. Questions that are developed for the FITSP certification are based upon one of the six skill levels.

The six skills levels are:

1. Knowledge
2. Comprehension
3. Application
4. Analysis
5. Synthesis
6. Evaluation

Below are the areas that each of these skills focuses on:

- Knowledge – This is the ability to use rote memorization and recall certain facts.

- Comprehension – This is the ability to read course content, extrapolate, and interpret important information and put other's ideas into their own words.

- Application – This is the ability to take new concepts and apply them to another situation.

- Analysis – This is the ability to take new information and break it down into parts to differentiate between them.

- Synthesis – This is the ability to take various pieces of information and form a whole creating a pattern where one did not previously exist.

- Evaluation – This is the ability to look at someone else's ideas or principles and see the worth of the work and the value of the conclusions.

Reference:

Hellyer, S. (n.d.). *A teaching handbook for university faculty. Chapter 1: Course objectives.* Retrieved October 1, 1998, from Indiana University Purdue University Indianapolis Website: http://www.iupui.edu/~profdev/handbook/chap1.html

Zimmaro, Dawn M., Writing Good Multiple-Choice Exams. August 19, 2004, from University of Texas at Austin Website: http://www.utexas.edu/academic/mec/research/pdf/writingmcexamshandout.pdf

The FITSP exam questions focus on validating the following types of cognitive abilities:

Knowledge – Test questions focus on identification and recall of information
Comprehension – Test questions focus on the use of facts, rules, and principles
Application – Test questions focus on applying facts or principles
Analysis – Test questions focus on the separation of a whole into component parts
Synthesis – Test questions focus on combining ideas to form a new whole
Evaluation – Test questions focus on developing opinions, judgments or decisions

Reference:

Hellyer, S. (n.d.). *A teaching handbook for university faculty. Chapter 1: Course objectives.* Retrieved October 1, 1998, from Indiana University Purdue University Indianapolis Website: http://www.iupui.edu/~profdev/handbook/chap1.html

Zimmaro, Dawn M., Writing Good Multiple-Choice Exams. August 19, 2004, from University of Texas at Austin Website: http://www.utexas.edu/academic/mec/research/pdf/writingmcexamshandout.pdf

4. Sample Multiple-Choice Items Related to Bloom's Taxonomy

Listed below are some examples using non-FITSP related content to illustrate the ways of writing multiple-choice questions that work within the six levels of Bloom's Taxonomy of Educational Objectives.

Knowledge

1. Reliability is the same as:
   A. consistency.
   B. relevancy.
   C. representativeness.
   D. usefulness.

Outcome: Identifies the meaning of a term.

2. What is the first step in constructing an achievement test?
   A. Decide on test length.
   B. Identify the intended learning outcomes.
   C. Prepare a table of specifications.
   D. Select the item types to use.

Outcome: Identifies the order of events.

3. In the area of physical science, which one of the following definitions describes the term "polarization"?
   A. The separation of electric charges by friction.
   B. The ionization of atoms by high temperatures.
   C. The interference of sound waves in a closed chamber.
   D. The excitation of electrons by high-frequency light.
   E. The vibration of transverse waves in a single plane.

A simple recall of the correct definition of polarization is required.

Comprehension

1. Which one of the following statements contains a specific determiner?
   A. America is a continent.
   B. America was discovered in 1492.
   C. America has some big industries.
   D. America's population is increasing.

Outcome: Identifies an example of a term.

2. The statement that "test reliability is a necessary but not sufficient condition of test validity" means that:
   A. a reliable test will have a certain degree of validity.
   B. a valid test will have a certain degree of reliability.
   C. a reliable test may be completely invalid and a valid test completely unreliable.

Outcome: Interprets the meaning of an idea.

3. Which of the following is an example of a criterion-referenced interpretation?

A. Derik earned the highest score in science.
B. Erik completed his experiment faster than his classmates.
C. Edna's test score was higher than 50 percent of the class.
D. Tricia set up her laboratory equipment in five minutes.

Outcome: Identifies an example of a concept or principle.

4. What is most likely to happen to the reliability of the scores for a multiple-choice test, where the number of alternatives for each item is changed from three to four?

A. It will decrease.
B. It will increase.
C. It will stay the same.
D. There is no basis for making a prediction.

Outcome: Predicts the most probable effect of an action.

5. Which one of the following describes what takes place in the so-called PREPARATION stage of the creative process, as applied to the solution of a particular problem?

A. The problem is identified and defined.
B. All available information about the problem is collected.
C. An attempt is made to see if the proposed solution to the problem is acceptable.
D. The person goes through some experience leading to a general idea of how the problem can be solved.
E. The person sets the problem aside and gets involved with some other unrelated activity.

The knowledge of the five stages of the creative process must be recalled (knowledge), and the student is tested

Application

Which one of the following memory systems does a piano-tuner mainly use in his occupation?

A. Echoic memory
B. Short-term memory
C. Long-term memory
D. Mono-auditory memory
E. None of the above

This question tests for the application of previously acquired knowledge (the various memory systems).

Analysis

Read carefully through the paragraph below and decide which of the options A-D is correct.

"The basic premise of pragmatism is that questions posed by speculative metaphysical propositions can often be answered by determining what the practical consequences of the acceptance of a particular metaphysical proposition are in this life. Practical consequences are taken as the criterion for assessing the relevance of all statements or ideas about truth, norm, and hope."

A. The word "acceptance" should be replaced by "rejection."
B. The word "often" should be replaced by "only."
C. The word "speculative" should be replaced by hypothetical."
D. The word "criterion" should be replaced by "measure."

This question requires prior knowledge of and understanding of the concept of pragmatism. The student is tested on his/her ability to analyze whether a word fits the accepted definition of pragmatism.

Synthesis

Evaluation

Judge the sentence in italics according to the criteria given below:
"The United States took part in the Gulf War against Iraq BECAUSE of the lack of civil liberties imposed on the Kurds by Saddam Hussein's regime."

A. The assertion and the reason are both correct, and the reason is valid.
B. The assertion and the reason are both correct, but the reason is invalid.
C. The assertion is correct, but the reason is incorrect.
D. The assertion is incorrect, but the reason is correct.
E. Both the assertion and the reason are incorrect.

Knowledge and understanding of Middle East politics are assumed. The student is tested on the ability to evaluate between cause and effect in the sentence regarding predefined criteria.

References:

Carneson, J., Delpierre, G., & Masters, K. (n.d.). *Designing and managing multiple-choice questions: Appendix C, multiple-choice questions, and Bloom's taxonomy.* Retrieved November 3, 2003, from the University of Cape Town Website: http://www.uct.ac.za/projects/cbe/mcqman/mcqappc.html

Gronlund, N. E. (1998). *Assessment of student achievement*. Boston: Allyn and Bacon.

Zimmaro, Dawn M., Writing Good Multiple-Choice Exams. August 19, 2004, from University of Texas at Austin Website: http://www.utexas.edu/academic/mec/research/pdf/writingmcexamshandout.pdf

5. 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.

6. FITSP-Designer Exam Objectives Outline

This section provides the objectives that are measured by the FITSP-Designer 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 #2

Topic #1 - Access Control

- Objective #1 – Design 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 – Develop 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 – Design 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 – Develop 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 – Construct 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 – Construct 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 – Create the establishment and enforcement of security configuration settings for information technology products employed in organizational information systems.

Topic #5 - Contingency Planning

- Objective #1 – Design 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 – Develop 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 – Construct 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 – Create the tracking, documentation, and reporting of incidents to appropriate organizational officials or authorities.

Topic #8 - Maintenance

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

Topic #9 - Media Protection

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

Topic #10 - Personnel Security

- Objective #1 – Design 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 – Develop elements to ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers.
- Objective #3 – Develop the employment of formal sanctions for personnel failing to comply with organizational security policies and procedures.

Topic #11 - Physical and Environmental Protection

- Objective #1 – Design the limitation of physical access to information systems, equipment, and the respective operating environments to authorized individuals.
- Objective #2 – Design the protection of the physical plant and supporting infrastructure for information systems.
- Objective #3 – Develop 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 – Create 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 – Develop 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 – Design 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 – Design the periodic assessment of security controls in organizational information systems to determine if the controls are effective in their application.

- Objective #2 – Design the development and implementation of plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems.
- Objective #3 – Design the authorization of operation of organizational information systems and any associated information system connections.
- Objective #4 – Develop 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 – Design 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 – Develop 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 – Design the identification, reporting, and correction of information and information system flaws in a timely manner.
- Objective #2 – Develop elements to provision protections from malicious code at appropriate locations within organizational information systems.
- Objective #3 – Construct elements to monitor information system security alerts and advisories and take appropriate actions in response.

Topic #18 - System and Services Acquisition

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

7. FITSP-Manager Exam Objectives Outline

This section provides the objectives that are measured by the FITSP-Manager 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 #3

Topic #1 - Access Control

- Objective #1 – Manage 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 #3 - Audit and Accountability

- Objective #1 – Supervise 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 – Oversee 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 #2 - Awareness and Training

- Objective #1 – Direct 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 – Govern 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 – Administer 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 – Manage the establishment and enforcement of security configuration settings for information technology products employed in organizational information systems.

Topic #5 - Contingency Planning

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

Topic #8 - Maintenance

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

Topic #9 - Media Protection

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

Topic #10 - Personnel Security

- Objective #1 – Administer 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 – Direct elements to ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers.
- Objective #3 – Govern the employment of formal sanctions for personnel failing to comply with organizational security policies and procedures.

Topic #11 - Physical and Environmental Protection

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

Topic #12 - Planning

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

- Objective #2 – Administer the development and implementation of plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems.
- Objective #3 – Manage the authorization of operation of organizational information systems and any associated information system connections.
- Objective #4 – Direct 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 – Manage 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 – Direct 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 – Govern the identification, reporting, and correction of information and information system flaws in a timely manner.
- Objective #2 – Supervise the provision of protections from malicious code at appropriate locations within organizational information systems.
- Objective #3 – Oversee the monitoring of information system security alerts and advisories and take appropriate actions in response.

Topic #18 - System and Services Acquisition

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

8. FITSP-Operator Exam Objectives Outline

This section provides the objectives that are measured by the FITSP-Operator 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 #4

Topic #1 - Access Control

- Objective #1 – Configure 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 – Enable 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 – Facilitate 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 – Implement 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 – Execute 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 – Facilitate 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 – Enable the establishment and enforcement of security configuration settings for information technology products employed in organizational information systems.

Topic #5 - Contingency Planning

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

Topic #8 - Maintenance

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

Topic #9 - Media Protection

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

Topic #10 - Personnel Security

- Objective #1 – Enable 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 – Implement elements to ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers.
- Objective #3 – Operate the employment of formal sanctions for personnel failing to comply with organizational security policies and procedures.

Topic #11 - Physical and Environmental Protection

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

Topic #12 - Planning

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

- Objective #2 – Enable the development and implementation of plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems.
- Objective #3 – Facilitate the authorization of operation of organizational information systems and any associated information system connections.
- Objective #4 – Execute 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 – Execute 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 – Execute 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 – Enable the identification, reporting, and correction of information and information system flaws in a timely manner.
- Objective #2 – Facilitate the provision of protections from malicious code at appropriate locations within organizational information systems.
- Objective #3 – Configure the monitoring of information system security alerts and advisories and take appropriate actions in response.

Topic #18 - System and Services Acquisition

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

9. Sample FITSI Exam Development Worksheet

Exam: FITSP-Manager

Security Topic Area: Identification and Authentication

Objective: Govern 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.

Schema Reference: 3.6.1

Taxonomy Reference: Knowledge
(Possible selections: Knowledge, Comprehension, Application, Analysis, Synthesis or Evaluation)

Exam Question: You are an IT security manager working at a federal agency. As part of a new system that is being developed based on the SDLC methodology, you are helping select and acquire the necessary controls to limit access to authorized users. Which of the following references would be used as the basis-selecting multifactor authentication to the system?

Exam Answer Choices:

a) HSPD-5
b) NIST SP 800-60
c) OMB Memo 07-16
d) NIST SP 800-63

Explanation:
The correct answer is d) NIST SP 800-63. This document focuses on Electronic authentication for information systems and the different types of multifactor authentication based upon the type of system. Answer a) is incorrect as it deals with the management of domestic incidents. Answer b) is incorrect; it deals with the classification of information types. Answer c) is incorrect as it deals with defining how federal agencies are expected to protect personally identifiable information.

FITSP Domain (select one): NIST Special Publications
(Possible selections: NIST Special Publications, NIST Federal Information Processing Standards, Government Laws and Regulations, NIST Control Families, NIST Risk Management Framework, NIST Interagency Reports)

References: http://csrc.nist.gov, NIST Special Publication 800-63 Rev3