FITSI Next Generation FITSP Certification Scheme Handbook

Certification Scheme
for the Next
Generation of The
Federal IT Security
Institute (FITSI)
Sponsored
Certifications

Version 1.1

Published 10/26/2021

This page is left intentionally blank

TABLE OF CONTENTS

1. Overview

This handbook describes the certification scheme details for the Next Generation FITSP Certification Program. This document covers the scheme of the four following certification roles:

- FITSP-Auditor-NG
- FITSP-Designer-NG
- FITSP-Manager-NG
- FITSP-Operator-NG

2. Applicability

FITSI has put together this handbook to document the formal structure of the Next Generation FITSP Certification scheme. This FITSP certification scheme conforms with ISO 17024: 2012 - Conformity assessment — General requirements for bodies operating certification of persons.

The most up-to-date *FITSI Next Generation FITSP Certification Scheme Handbook* can be found at http://www.fitsi.org/documents.html.

3. FITSP-Auditor-NG Certification Scheme Details

A. Scope of Certification

The FITSP-Auditor-NG certification is designed to demonstrate the federal workforce member (civilian personnel, military, and contractors) possess the knowledge of federal information technology (IT) security requirements necessary to successfully ***audit*** and ***assess*** the management, operational, and technical IT security controls for systems owned by, or operated on behalf of, the federal government of the United States.

B. Job Description

The following list highlights, but may not comprehensively capture, the commonly articulated roles characterized within federal statutory, regulatory, standards, and guidance documents that relate to the FITSP-Auditor-NG certification.

- Assessor
- External IT auditor
- Evaluator
- Internal IT auditor
- Reviewer
- Risk/Vulnerability Analyst

C. Task Description

The Federal Information Security Management Act of 2002 and the Federal Information Modernization Act of 2014 require federal agencies to follow NIST standards and guidance for cybersecurity. NIST defines minimum security standards for federal information and information systems (FIPS). FITSI will use FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, as the basis for the FITSP Certification Program. The FITSP-Auditor-NG certification describes the auditor requirements of the FIPS 200 standard based upon the following descriptions: audit, review, inspect, evaluate, or assess.

FITSI develops a job task analysis (JTA) report, and the Scheme Committee reviews the report and approves it for usage by the certification program.

The FITSP-Auditor-NG certification currently uses the *FITSI Job Task Analysis Report 2017* published and approved on August 8th, 2017, to map job tasks to specific domain concentrations.

D. Required Competence

The most current FITSP-Auditor Exam Blueprint defines the required competence for the FITSP-Auditor-NG certification. This document links the tasks identified in section C above to the Body of Knowledge below in section E. This linkage is done by using domain concentrations identified in the Job Task Analysis (JTA) by Subject Matter Experts who contribute to the process and other industry professionals representing the Auditor role.

The FITSP-Auditor-NG certification currently uses the *FITSP-Auditor Exam Blueprint* published and approved on January 18th, 2018.

E. Body of Knowledge

Candidates of all four certification roles (Auditor, Designer, Manager, and Operator) are tested on a comprehensive Federal Body of Knowledge (FBK) which consists of a library of federal statutes, regulations, standards, and guidelines. The FBK consists of 6 domains and 18 IT security topic areas.

1. Domains
    a. Domain 1 – National Institute of Standards and Technology (NIST) Special Publications (SPs)
    b. Domain 2 – NIST Federal Information Processing Standards (FIPS)
    c. Domain 3 – NIST Control Families (CFs)
    d. Domain 4 – Governmental Laws and Regulations
    e. Domain 5 – NIST Risk Management Framework (RMF)
    f. Domain 6 – NIST Interagency Reports (NISTIRs)
2. IT security topic areas
    a. Access Control
    b. Audit and Accountability
    c. Awareness and Training
    d. Configuration Management
    e. Contingency Planning
    f. Identification and Authentication
    g. Incident Response
    h. Maintenance
    i. Media Protection
    j. Personnel Security
    k. Physical and Environmental Protection
    l. Planning
    m. Program Management
    n. Risk Assessment
    o. Security Assessment and Authorization
    p. System and Communications Protection
    q. System and Information Integrity
    r. System and Services Acquisition

FITSI publishes a formal Federal Body of Knowledge (FBK) Guide. The most current version of the FBK Guide can be found at the following website: http://www.fitsi.org/documents.html.

F. Code of Conduct

Candidates must agree to abide by the FITSI Code of Ethics defined in the FITSI Code of Ethics Handbook.

G. Criteria for Initial Certification

A minimum of five years of information security experience is required to qualify for any FITSP certification. This experience can be obtained from employment in the federal government or civilian sector. FITSP-Auditor-NG certification candidates can waive portions of the experience requirements if the candidate possesses other complimentary security certifications or education.

- Educational waivers – Candidates may waive one year of experience for a bachelor's degree in any discipline. Candidates may waive one year of experience for a bachelor's degree and a second year with a master's degree with an IT or information assurance focus. Each degree allows for one year of experience to be waived. Degrees must be issued by a fully accredited institution.
- Complimentary security certifications – Candidates are eligible to waive one year of experience by possessing one or more of the following IT security certifications:
    - CompTIA Advanced Security Practitioner (CASP+)
    - CompTIA Cybersecurity Analyst (CySA+)
    - CompTIA Security+
    - EC-Council Certified Ethical Hacker Security+ (CEH)
    - Global Information Assurance Certified (GIAC)
    - ISACA Certified Information Security Manager (CISM)
    - ISACA Certified Information Systems Auditor (CISA)
    - ISC2 Certified Information Systems Security Professional (CISSP)
    - ISC2 Certified Authorization Professional (CAP)
    - ISC2 System Security Certified Practitioner (SSCP)

Candidates may not waive more than three years of experience with any combination of education and complimentary security certifications. All FITSP-Auditor-NG candidates are required to provide documented details of experience after passing the exam through the *FITSI Certification Application Form*.

H. Criteria for Recertification

Federal standards are constantly changing, which requires a candidate to maintain knowledge currency. FITSP-Auditor-NG candidates must retest every six years.

I. Assessment Methods for Initial Certification and Recertification

A multiple-choice exam consisting of 150 multiple choice items is the assessment method for initial certification and recertification activities. Certification holders that are recertifying must take the most current version of the exam available at the time of recertification.

J. Surveillance Methods

Certification holders are required to pay an annual maintenance fee (AMF). Failure to stay current on AMFs may result in suspension or withdrawal of a certification holder's certification.

K. Criteria for Suspending and Withdrawing Certification

Certification holders must keep their certifications in good standing for the entire six-year cycle. A FITSP certification can be suspended or withdrawn (revoked) for a certification holder due to non-compliance with the certification maintenance requirements.

Certification may be put into a suspended state for the following reasons:

- Failure to stay current with AMF
- Having an active complaint for violation of the FITSI Code of Ethics

The suspension period can last for up to 90 days. During this time, the certification holder must refrain from promoting the certification while it is suspended. To remove the certification from a suspended state, the certification holder must address the issue causing the suspension.

If the certification holder does not address the issue causing the suspension after 90 days, the certification will be withdrawn (revoked).

Reasons for withdrawal (revocation) of the certification are:

- Continued failure to bring outstanding AMFs current after 90 days
- Substantiated violation of the FITSI Code of Ethics as determined through the FITSI complaint process

When a certification is withdrawn (revoked), the certification holder must discontinue the use of all claims and references to the certification and discontinue the use of the FITSI Certification Logo.

L. Exam Blue Print Requirements

FITSI develops the FITSP-Auditor-NG blueprint, which maps the certification exam items (questions) to the tasks and the six domains. The item distribution for the domains is linked back to domain concentrations identified in the *FITSI Job Task Analysis Report 2017*. The Scheme Committee reviews the exam blueprint and approves it for usage by the certification program.

M. Cut-Score Requirements

FITSI employs professional psychometricians to ensure exam items perform correctly and help determine the necessary cut-score of the FITSP-Auditor-NG certification. The psychometrician conducts a cut-score study with FITSI recruited Subject Matter Experts (SMEs) using the Angoff method. The Scheme Committee reviews the recommended cut-score and approves it for usage by the certification program.

4. FITSP-Designer-NG Certification Scheme Details

A. Scope of Certification

The FITSP-Designer-NG certification is designed to demonstrate the federal workforce member (civilian personnel, military, and contractors) possess the knowledge of federal information technology (IT) security requirements necessary to successfully ***design*** and ***develop*** the management, operational, and technical IT security controls for systems owned by, or operated on behalf of, the federal government of the United States.

B. Job Description

The following list highlights, but may not comprehensively capture, the commonly articulated roles characterized within federal statutory, regulatory, standards, and guidance documents that relate to the FITSP-Designer-NG certification.

- IT Security Engineer
- Programmer
- Security Engineer
- System Designer
- System Developer

C. Task Description

The Federal Information Security Management Act of 2002 and the Federal Information Modernization Act of 2014 require federal agencies to follow NIST standards and guidance for cybersecurity. NIST defines minimum security standards for federal information and information systems (FIPS). FITSI uses FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, as the basis for the FITSP Certification Program. The FITSP-Designer-NG certification describes the designer requirements of the FIPS 200 standard based upon the following descriptions: design, develop, construct, or create.

FITSI develops a job task analysis (JTA) report, and the Scheme Committee reviews the report and approves it for usage by the certification program.

The FITSP-Designer-NG certification currently uses the *FITSI Job Task Analysis Report 2017* published and approved on August 8th, 2017, to map job tasks to specific domain concentrations.

D. Required Competence

The most current FITSP-Designer Exam Blueprint defines the required competence for the FITSP-Designer-NG certification. This document links the tasks identified in section C above to the Body of knowledge below in section E. This linkage is done by using domain concentrations identified in the Job Task Analysis (JTA) by Subject Matter Experts who contribute to the process and other industry professionals representing the Designer role.

The FITSP-Designer-NG certification currently uses the *FITSP-Designer Exam Blueprint* published and approved on January 18th, 2018.

E. Body of Knowledge

Candidates of all four certification roles (Auditor, Designer, Manager, and Operator) are tested on a comprehensive Federal Body of Knowledge (FBK) which consists of a library of federal statutes, regulations, standards, and guidelines. The FBK consists of 6 domains and 18 IT security topic areas.

1. Domains
   a. Domain 1 – NIST Special Publications (SPs)
   b. Domain 2 – NIST Federal Information Processing Standards (FIPS)
   c. Domain 3 – NIST Control Families (CFs)
   d. Domain 4 – Governmental Laws and Regulations
   e. Domain 5 – NIST Risk Management Framework (RMF)
   f. Domain 6 – NIST Interagency Reports (NISTIRs)
2. IT security topic areas
   a. Access Control
   b. Audit and Accountability
   c. Awareness and Training
   d. Configuration Management
   e. Contingency Planning
   f. Identification and Authentication
   g. Incident Response
   h. Maintenance
   i. Media Protection
   j. Personnel Security
   k. Physical and Environmental Protection
   l. Planning
   m. Program Management
   n. Risk Assessment
   o. Security Assessment and Authorization
   p. System and Communications Protection
   q. System and Information Integrity
   r. System and Services Acquisition

FITSI publishes a formal Federal Body of Knowledge (FBK) Guide. The most current version of the FBK Guide can be found at the following website: http://www.fitsi.org/documents.html.

F. Code of Conduct

Candidates must agree to abide by the FITSI Code of Ethics defined in the FITSI Code of Ethics Handbook.

G. Criteria for Initial Certification

A minimum of five years of information security experience is required to qualify for any FITSP certification. This experience can be obtained from employment in the federal government or civilian sector. FITSP-Designer-NG certification candidates can waive portions of the experience requirements if the candidate possesses other complimentary security certifications or education.

- Educational waivers – Candidates may waive one year of experience for a bachelor's degree in any discipline. Candidates may waive one year of experience for a bachelor's degree and a second year with a master's degree with an IT or information assurance focus. Each degree allows for one year of experience to be waived. Degrees must be issued by a fully accredited institution.
- Complimentary security certifications – Candidates are eligible to waive one year of experience by possessing one or more of the following IT security certifications:
  - CompTIA Advanced Security Practitioner (CASP+)
  - CompTIA Cybersecurity Analyst (CySA+)
  - CompTIA Security+
  - EC-Council Certified Ethical Hacker Security+ (CEH)
  - Global Information Assurance Certified (GIAC)
  - ISACA Certified Information Security Manager (CISM)
  - ISACA Certified Information Systems Auditor (CISA)
  - ISC2 Certified Information Systems Security Professional (CISSP)
  - ISC2 Certified Authorization Professional (CAP)
  - ISC2 System Security Certified Practitioner (SSCP)

Candidates may not waive more than three years of experience with any combination of education and complimentary security certifications. All FITSP-Designer-NG candidates are required to provide documented details of experience after passing the exam through the *FITSI Certification Application Form*.

o

H. Criteria for Recertification

Federal standards are constantly changing, which requires a candidate to maintain knowledge currency. FITSP-Designer-NG candidates must retest every six years.

I. Assessment Methods for Initial Certification and Recertification

A multiple-choice exam consisting of 150 multiple choice items is the assessment method for initial certification and recertification activities. Certification holders that are recertifying must take the most current version of the exam available at the time of recertification.

J. Surveillance Methods

Certification holders are required to pay an annual maintenance fee (AMF). Failure to stay current on AMFs may result in suspension or withdrawal of a certification holder's certification.

K. Criteria for Suspending and Withdrawing Certification

Certification holders must keep their certifications in good standing for the entire six-year cycle. A FITSP certification can be suspended or withdrawn (revoked) for a certification holder due to non-compliance with the certification maintenance requirements.

Certification may be put into a suspended state for the following reasons:

- Failure to stay current with AMF
- Having an active complaint for violation of the FITSI Code of Ethics

The suspension period can last for up to 90 days. During this time, the certification holder must refrain from promoting the certification while it is suspended. To remove the certification from a suspended state, the certification holder must address the issue causing the suspension.

If the certification holder does not address the issue causing the suspension after 90 days, the certification will be withdrawn (revoked).

Reasons for withdrawal (revocation) of the certification are:

- Continued failure to bring outstanding AMFs current after 90 days
- Substantiated violation of the FITSI Code of Ethics as determined through the FITSI complaint process

When a certification is withdrawn (revoked), the certification holder must discontinue the use of all claims and references to the certification and discontinue the use of the FITSI Certification Logo.

L. Exam Blue Print Requirements

FITSI develops the FITSP-Designer-NG blueprint, which maps the certification exam items (questions) to the tasks and the six domains. The item distribution for the domains is linked back to domain concentrations identified in the *FITSI Job Task Analysis Report 2017*. The Scheme Committee reviews the exam blueprint and approves it for usage by the certification program.

M. Cut-Score Requirements

FITSI employs professional psychometricians to ensure exam items perform correctly and help determine the necessary cut-score of the FITSP-Designer-NG certification. The psychometrician conducts a cut-score study with FITSI recruited Subject Matter Experts (SMEs) using the Angoff method. The Scheme Committee reviews the recommended cut-score and approves it for usage by the certification program.

5. FITSP-Manager-NG Certification Scheme Details

A. Scope of Certification

The FITSP-Manager-NG certification is designed to demonstrate the federal workforce member (civilian personnel, military, and contractors) possess the knowledge of federal information technology (IT) security requirements necessary to successfully ***manage*** and ***oversee*** the management, operational, and technical IT security controls for systems owned by, or operated on behalf of, the federal government of the United States.

B. Job Description

The following list highlights, but may not comprehensively capture, the commonly articulated roles characterized within federal statutory, regulatory, standards, and guidance documents that relate to the FITSP-Manager-NG certification.

- Authorizing Official
- Chief Information Officer
- Senior Agency Information Security Officer
- Chief Information Security Officer
- Chief Technology Officer
- Freedom of Information Act Official
- Information Resource Manager
- Information Assurance Manager
- Information Security Manager
- Information Security Program Manager
- Information Systems Security Officers
- IT Security Compliance Officer
- Mission or Business Owner
- Privacy Act Official (Privacy Officers)
- Program and Functional Managers
- Procurement Officers
- Risk Executive
- Senior Accountable Official for Risk Management
- Senior Agency Official for Privacy
- Senior/Executive Agency Leader
- System Owner

C. Task Description

The Federal Information Security Management Act of 2002 and the Federal Information Modernization Act of 2014 require federal agencies to follow NIST standards and guidance for cybersecurity. NIST defines minimum security standards for federal information and information systems (FIPS). FITSI uses FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, as the basis for the FITSP Certification Program. The FITSP-Manager-NG certification uses the tasks in FIPS 200 and applies a managerial focus to these tasks. The following descriptions are used to provide managerial focus: manage, oversee, govern, supervise, direct, or administer.

FITSI develops a job task analysis (JTA) report, and the Scheme Committee reviews the report and approves it for usage by the certification program.

The FITSP-Manager-NG certification currently uses the *FITSI Job Task Analysis Report 2017* published and approved on August 8th, 2017, to map job tasks to specific domain concentrations.

D. Required Competence

The most current FITSP-Manager Exam Blueprint defines the required competence for the FITSP-Manager-NG certification. This document links the tasks identified in section C above to the Body of knowledge below in section E. This linkage is done by using domain concentrations identified in the Job Task Analysis (JTA) by Subject Matter Experts who contribute to the process and other industry professionals representing the Manager role.

The FITSP-Manager-NG certification currently uses the *FITSP-Manager Exam Blueprint* published and approved on January 18th, 2018.

E. Body of Knowledge

Candidates of all four certification roles (Auditor, Designer, Manager, and Operator) are tested on a comprehensive Federal Body of Knowledge (FBK) which consists of a library of federal statutes, regulations, standards, and guidelines. The FBK consists of 6 domains and 18 IT security topic areas.

1. Domains
    a. Domain 1 – NIST Special Publications (SPs)
    b. Domain 2 – NIST Federal Information Processing Standards (FIPS)
    c. Domain 3 – NIST Control Families (CFs)
    d. Domain 4 – Governmental Laws and Regulations
    e. Domain 5 – NIST Risk Management Framework (RMF)
    f. Domain 6 – NIST Interagency Reports (NISTIRs)
2. IT security topic areas
    a. Access Control
    b. Audit and Accountability
    c. Awareness and Training
    d. Configuration Management
    e. Contingency Planning
    f. Identification and Authentication
    g. Incident Response
    h. Maintenance
    i. Media Protection
    j. Personnel Security
    k. Physical and Environmental Protection
    l. Planning
    m. Program Management
    n. Risk Assessment

o. Security Assessment and Authorization
p. System and Communications Protection
q. System and Information Integrity
r. System and Services Acquisition

FITSI publishes a formal Federal Body of Knowledge (FBK) Guide. The most current version of the FBK Guide can be found at the following website: http://www.fitsi.org/documents.html.

F. Code of Conduct

Candidates must agree to abide by the FITSI Code of Ethics defined in the FITSI Code of Ethics Handbook.

G. Criteria for Initial Certification

A minimum of five years of information security experience is required to qualify for any FITSP certification. This experience can be obtained from employment in the federal government or civilian sector. FITSP-Manager-NG certification candidates can waive portions of the experience requirements if the candidate possesses other complimentary security certifications or education.

- Educational waivers – Candidates may waive one year of experience for a bachelor's degree in any discipline. Candidates may waive one year of experience for a bachelor's degree and a second year with a master's degree with an IT or information assurance focus. Each degree allows for one year of experience to be waived. Degrees must be issued by a fully accredited institution.
- Complimentary security certifications – Candidates are eligible to waive one year of experience by possessing one or more of the following IT security certifications:
    - CompTIA Advanced Security Practitioner (CASP+)
    - CompTIA Cybersecurity Analyst (CySA+)
    - CompTIA Security+
    - EC-Council Certified Ethical Hacker Security+ (CEH)
    - Global Information Assurance Certified (GIAC)
    - ISACA Certified Information Security Manager (CISM)
    - ISACA Certified Information Systems Auditor (CISA)
    - ISC2 Certified Information Systems Security Professional (CISSP)
    - ISC2 Certified Authorization Professional (CAP)
    - ISC2 System Security Certified Practitioner (SSCP)

Candidates may not waive more than three years of experience with any combination of education and complimentary security certifications. All FITSP-Manager-NG candidates are required to provide documented details of experience after passing the exam through the *FITSI Certification Application Form*.

o

H. Criteria for Recertification

Federal standards are constantly changing, which requires a candidate to maintain knowledge currency. FITSP-Manager-NG candidates must retest every six years.

I. Assessment Methods for Initial Certification and Recertification

A multiple-choice exam consisting of 150 multiple choice items is the assessment method for initial certification and recertification activities. Certification holders that are recertifying must take the most current version of the exam available at the time of recertification.

J. Surveillance Methods

Certification holders are required to pay an annual maintenance fee (AMF). Failure to stay current on AMFs may result in suspension or withdrawal of a certification holder's certification.

K. Criteria for Suspending and Withdrawing Certification

Certification holders must keep their certifications in good standing for the entire six-year cycle. A FITSP certification can be suspended or withdrawn (revoked) for a certification holder due to non-compliance with the certification maintenance requirements.

Certification may be put into a suspended state for the following reasons:

- Failure to stay current with AMF
- Having an active complaint for violation of the FITSI Code of Ethics

The suspension period can last for up to 90 days. During this time, the certification holder must refrain from promoting the certification while it is suspended. To remove the certification from a suspended state, the certification holder must address the issue causing the suspension.

If the certification holder does not address the issue causing the suspension after 90 days, the certification will be withdrawn (revoked).

Reasons for withdrawal (revocation) of the certification are:

- Continued failure to bring outstanding AMFs current after 90 days
- Substantiated violation of the FITSI Code of Ethics as determined through the FITSI complaint process

When a certification is withdrawn (revoked), the certification holder must discontinue the use of all claims and references to the certification and discontinue the use of the FITSI Certification Logo.

L. Exam Blue Print Requirements

FITSI develops the FITSP-Manager-NG blueprint, which maps the certification exam items (questions) to the tasks and the six domains. The item distribution for the domains is linked back to domain concentrations identified in the *FITSI Job Task Analysis Report 2017*. The Scheme Committee reviews the exam blueprint and approves it for usage by the certification program.

M. Cut-Score Requirements

FITSI employs professional psychometricians to ensure exam items perform correctly and help determine the necessary cut-score of the FITSP-Manager-NG certification. The psychometrician conducts a cut-score study with FITSI recruited Subject Matter Experts (SMEs) using the Angoff method. The Scheme Committee reviews the recommended cut-score and approves it for usage by the certification program.

6. FITSP-Operator-NG Certification Scheme Details

A. Scope of Certification

The FITSP-Operator-NG certification is designed to demonstrate the federal workforce member (civilian personnel, military, and contractors) possess the knowledge of federal information technology (IT) security requirements necessary to successfully ***implement*** and ***operate*** the management, operational, and technical IT security controls for systems owned by, or operated on behalf of, the federal government of the United States.

B. Job Description

The following list highlights, but may not comprehensively capture, the commonly articulated roles characterized within federal statutory, regulatory, standards, and guidance documents that relate to the FITSP-Operator-NG certification.

- Data Center Manager
- Database Administrator
- IT Security Operations
- Maintenance Professional
- Network Administrator
- Network Security Specialists
- Security Administrator
- System Administrators
- System Operations Personnel
- Technical Support Professionals
- Telecommunications Personnel

C. Task Description

The Federal Information Security Management Act of 2002 and the Federal Information Modernization Act of 2014 require federal agencies to follow NIST standards and guidance for cybersecurity. NIST defines minimum security standards for federal information and information systems (FIPS). FITSI uses FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, as the basis for the FITSP Certification Program. The FITSP-Operator-NG certification describes the operator requirements of the FIPS 200 standard based upon the following descriptions: implement, operate, configure, enable, facilitate, or execute.

FITSI develops a job task analysis (JTA) report, and the Scheme Committee reviews the report and approves it for usage by the certification program.

The FITSP-Operator-NG certification currently uses the *FITSI Job Task Analysis Report 2017* published and approved on August 8th, 2017, to map job tasks to specific domain concentrations.

D. Required Competence

The most current FITSP-Operator Exam Blueprint defines the required competence for the FITSP-Operator-NG certification. This document links the tasks identified in section C above to the Body of knowledge below in section E. This linkage is done by using domain concentrations identified in the Job Task Analysis (JTA) by Subject Matter Experts who contribute to the process and other industry professionals representing an Operator role.

The FITSP-Operator-NG certification currently uses the *FITSP-Operator Exam Blueprint* published and approved on January 18th, 2018.

E. Body of Knowledge

Candidates of all four certification roles (Auditor, Designer, Manager, and Operator) are tested on a comprehensive Federal Body of Knowledge (FBK) which consists of a library of federal statutes, regulations, standards, and guidelines. The FBK consists of 6 domains and 18 IT security topic areas.

1. Domains
    a. Domain 1 – NIST Special Publications (SPs)
    b. Domain 2 – NIST Federal Information Processing Standards (FIPS)
    c. Domain 3 – NIST Control Families (CFs)
    d. Domain 4 – Governmental Laws and Regulations
    e. Domain 5 – NIST Risk Management Framework (RMF)
    f. Domain 6 – NIST Interagency Reports (NISTIRs)
2. IT security topic areas
    a. Access Control
    b. Audit and Accountability
    c. Awareness and Training
    d. Configuration Management
    e. Contingency Planning
    f. Identification and Authentication
    g. Incident Response
    h. Maintenance
    i. Media Protection
    j. Personnel Security
    k. Physical and Environmental Protection
    l. Planning
    m. Program Management
    n. Risk Assessment
    o. Security Assessment and Authorization
    p. System and Communications Protection
    q. System and Information Integrity
    r. System and Services Acquisition

FITSI publishes a formal Federal Body of Knowledge (FBK) Guide. The most current version of the FBK Guide can be found at the following website: http://www.fitsi.org/documents.html.

F. Code of Conduct

Candidates must agree to abide by the FITSI Code of Ethics defined in the FITSI Code of Ethics Handbook.

G. Criteria for Initial Certification

A minimum of five years of information security experience is required to qualify for any FITSP certification. This experience can be obtained from employment in the federal government or civilian sector. FITSP-Operator-NG certification candidates can waive portions of the experience requirements if the candidate possesses other complimentary security certifications or education.

- Educational waivers – Candidates may waive one year of experience for a bachelor's degree in any discipline. Candidates may waive one year of experience for a bachelor's degree and a second year with a master's degree with an IT or information assurance focus. Each degree allows for one year of experience to be waived. Degrees must be issued by a fully accredited institution.
- Complimentary security certifications – Candidates are eligible to waive one year of experience by possessing one or more of the following IT security certifications:
    - CompTIA Advanced Security Practitioner (CASP+)
    - CompTIA Cybersecurity Analyst (CySA+)
    - CompTIA Security+
    - EC-Council Certified Ethical Hacker Security+ (CEH)
    - Global Information Assurance Certified (GIAC)
    - ISACA Certified Information Security Manager (CISM)
    - ISACA Certified Information Systems Auditor (CISA)
    - ISC2 Certified Information Systems Security Professional (CISSP)
    - ISC2 Certified Authorization Professional (CAP)
    - ISC2 System Security Certified Practitioner (SSCP)

Candidates may not waive more than three years of experience with any combination of education and complimentary security certifications. All FITSP-Operator-NG candidates are required to provide documented details of experience after passing the exam through the *FITSI Certification Application Form*.

o

H. Criteria for Recertification

Federal standards are constantly changing, which requires a candidate to maintain knowledge currency. FITSP-Operator-NG candidates must retest every six years.

I. Assessment Methods for Initial Certification and Recertification

A multiple-choice exam consisting of 150 multiple choice items is the assessment method for initial certification and recertification activities. Certification holders that are recertifying must take the most current version of the exam available at the time of recertification.

J. Surveillance Methods

Certification holders are required to pay an annual maintenance fee (AMF). Failure to stay current on AMFs may result in suspension or withdrawal of a certification holder's certification.

K. Criteria for Suspending and Withdrawing Certification

Certification holders must keep their certifications in good standing for the entire six-year cycle. A FITSP certification can be suspended or withdrawn (revoked) for a certification holder due to non-compliance with the certification maintenance requirements.

Certification may be put into a suspended state for the following reasons:

- Failure to stay current with AMF
- Having an active complaint for violation of the FITSI Code of Ethics

The suspension period can last for up to 90 days. During this time, the certification holder must refrain from promoting the certification while it is suspended. To remove the certification from a suspended state, the certification holder must address the issue causing the suspension.

If the certification holder does not address the issue causing the suspension after 90 days, the certification will be withdrawn (revoked).

Reasons for withdrawal (revocation) of the certification are:

- Continued failure to bring outstanding AMFs current after 90 days
- Substantiated violation of the FITSI Code of Ethics as determined through the FITSI complaint process

When a certification is withdrawn (revoked), the certification holder must discontinue the use of all claims and references to the certification and discontinue the use of the FITSI Certification Logo.

L. Exam Blue Print Requirements

FITSI develops the FITSP-Operator-NG blueprint, which maps the certification exam items (questions) to the tasks and the six domains. The item distribution for the domains is linked back to domain concentrations identified in the *FITSI Job Task Analysis Report 2017*. The Scheme Committee reviews the exam blueprint and approves it for usage by the certification program.

M. Cut-Score Requirements

FITSI employs professional psychometricians to ensure exam items perform correctly and help determine the necessary cut-score of the FITSP-Operator-NG certification. The psychometrician conducts a cut-score study with FITSI recruited Subject Matter Experts (SMEs) using the Angoff method. The Scheme Committee reviews the recommended cut-score and approves it for usage by the certification program.