FITSI Certification Application

Application for The
Federal IT Security
Institute (FITSI)
Sponsored
Certifications

Version 2.2

Published 01/05/23

This page is left intentionally blank

TABLE OF CONTENTS

1. FITSP Certification Process Overview

FITSI uses several certification processes to manage the FITSP Certification Program. These processes include:

1. An examination process
2. An application process
3. An assessment process
4. A certification decision process

The diagram below illustrates how these processes work together. Depending upon where the person seeking certification is in the process, they are either considered a Certification Candidate, Certification Applicant, or a Certification Holder.

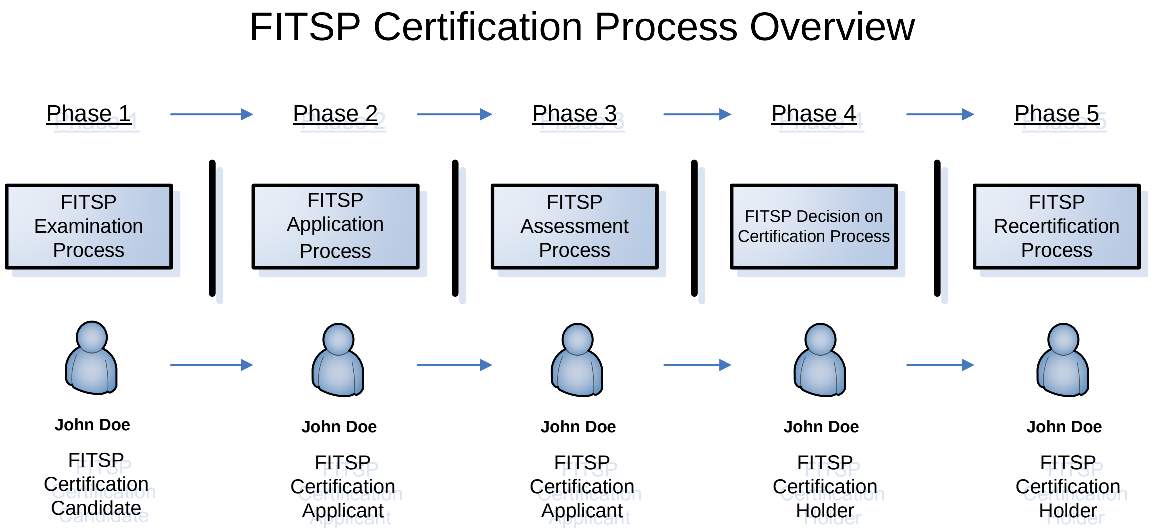
FITSP Certification Process Overview
Phase 1
Phase 2
Phase 3
Phase 4
Phase 5
FITSP Examination Process
FITSP Application Process
FITSP Assessment Process
FITSP Decision on Certification Process
FITSP Recertification Process
John Doe
FITSP Certification Candidate
John Doe
FITSP Certification Applicant
John Doe
FITSP Certification Applicant
John Doe
FITSP Certification Holder
John Doe
FITSP Certification Holder

Figure 1: FITSP Certification Process Overview

As part of earning a Federal IT Security Professional (FITSP) certification, FITSP Certification Candidates must successfully pass a certification exam (Phase 1) and submit a formal FITSI Certification application and supporting documentation (Phase 2). Once the FITSP Certification Application is submitted, FITSI will assess all the items in the application (Phase 3) and render a formal certification decision (Phase 4). During this formal certification decision phase, a determination is made on whether the FITSP certification will be granted to the individual. Certification Applicants who become Certification Holders in Phase 4 move to Phase 5, where they must meet certain criteria to be recertified. This process is visually represented in Figure 1 above.

2. Instructions for the FITSP Certification Applicant

This document provides instructions and a method for FITSP Certification Applicants to submit this FITSI Certification Application as part of Phase 2. FITSI requires three components, at a minimum, to be a part of this application:

1. Documentation of a Certification Applicant's background, including details of each job held to support a minimum of five years of Information Technology (IT) security experience. This requirement is documented in the application, and ***a current resume or curriculum vitae (CV) from the Certification Applicant must be submitted*** simultaneously.
2. A third-party endorsement from two colleagues who can verify the Certification Applicant's experience. An Endorser can be a supervisor, employer, manager, or certified peer. A certified peer must hold one of the certifications listed in Section 5.B of this application.
3. A formal attestation by the Certification Applicant that the information provided in this application is true and correct and agrees to several other terms and conditions regarding participation in the FITSP Certification Program.

FITSP Certification Applicants can waive portions of the experience requirements if the FITSP Certification Applicant possesses other complimentary security certifications or education. The acceptable complimentary security certifications are listed in the *FITSI Certification Candidate Handbook*. FITSP Certification Applicants may not waive more than three years of experience with any combination of education or certifications. FITSP Certification Applicant 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. FITSP Certification Applicants may not waive more than three years of experience with any combination of education and complimentary security certifications. The request to waive professional experience is included in Section 5 of this application.

The FITSP Certification Applicant must review, complete, and sign this application by hand (wet signature) or electronically (a public key digital signature or typed signature) and submit the application electronically by emailing it to applications@fitsi.org. FITSP Certification Applicants must complete Sections 3, 4, and 6 in their entirety and submit this application in total (all pages). If the Certification Applicant wishes to waive professional experience, Section 5 must also be completed.

Please note: The FITSP Certification Applicant is responsible for collecting and submitting all files to FITSI. Necessary items include 1) this *FITSI Certification Application Form* filled out (all 17 pages), 2) the FITSP Certification Applicant's current resume or curriculum vitae (CV), and 3) two separate third-party endorsements. All of these documents, in total, constitute the FITSI Certification Application Package.

If the FITSI Certification Application Package is not completed in full and submitted in total (this *FITSI Certification Application Form* (all 17 pages), the FITSP Certification Applicant's current resume or curriculum vitae (CV), and two separate third-party endorsements), FITSI will deny the application and notify the FITSP Certification Applicant via email.

FITSI endeavors to grant certification to FITSP Certification Applicants within 60 calendar days from the receipt of the application (and all supporting documentation).

FITSP Certification Candidates may take the certification exam before the five years of experience have been met and be allowed to earn the experience over the next five years. Once the FITSP Certification Candidate obtains the necessary experience during the five years after passing the exam, the FITSP Certification Applicant can submit the certification application.

Once the certification application is submitted, FITSI can conduct the Assessment and the Decision on Certification phases listed above in Figure 1 and grant the FITSP credential.

3. FITSP Certification Applicant Background

FITSP Certification Applicants must have five years of information security experience as part of the application process. This section provides FITSI with the key elements to determine if the Certification Applicant meets the minimum professional experience requirements.

A. General FITSP Certification Applicant Information

First Name: ____ Middle Initial: __________

Last Name: ____

Preferred Mailing Address: ____

____

____

Certification Applicant Contact Email: _________________________

Certification Applicant Contact Phone: _________________________

FITSI ID: ______________ (leave blank if unknown or unassigned)

Desired Certification Applying for: ______ Select One ____________

B. FITSP Certification Applicant Experience

Please provide background information for each position for which you had significant IT security responsibility. Under the "Areas of work" section, **annotate "P" for primary for each topic the position required as part of daily duties. Annotate an "S" for secondary for each topic that encompassed less than 50% of your job tasks.** At the end of Organization #10, in the "Total Amount of Time" section C, please sum up the total time for all collective experiences.

Organization #1

Organization: ____________________________ Position: ________________________

Years performing this work: ____

Areas of work:

• ____ Access Control	• ____ Awareness/Training	• ____ Audit/Accountability
• ____ Assessment & Authorization	• ____ Configuration Management	• ____ Contingency Planning
• ____ Identification & Authentication	• ____ Incident Response	• ____ Maintenance
• ____ Media Protection	• ____ Physical Environmental Protection	• ____ Planning
• ____ Personnel Security	• ____ Risk Assessment	• ____ System and Services Acquisition
• ____ System and Communication Protection	• ____ System and Information Integrity	• ____ Program Management

Organization #2

Organization: ______________________________ Position: _________________________

Years performing this work: ____

Areas of work:

• ____ Access Control	• ____ Awareness/Training	• ____ Audit/Accountability
• ____ Assessment & Authorization	• ____ Configuration Management	• ____ Contingency Planning
• ____ Identification & Authentication	• ____ Incident Response	• ____ Maintenance
• ____ Media Protection	• ____ Physical Environmental Protection	• ____ Planning
• ____ Personnel Security	• ____ Risk Assessment	• ____ System and Services Acquisition
• ____ System and Communication Protection	• ____ System and Information Integrity	• ____ Program Management

Organization #3

Organization: ______________________________ Position: _________________________

Years performing this work: ____

Areas of work:

• ____ Access Control	• ____ Awareness/Training	• ____ Audit/Accountability
• ____ Assessment & Authorization	• ____ Configuration Management	• ____ Contingency Planning
• ____ Identification & Authentication	• ____ Incident Response	• ____ Maintenance
• ____ Media Protection	• ____ Physical Environmental Protection	• ____ Planning
• ____ Personnel Security	• ____ Risk Assessment	• ____ System and Services Acquisition
• ____ System and Communication Protection	• ____ System and Information Integrity	• ____ Program Management

Organization #4

Organization: ______________________________ Position: _________________________

Years performing this work: ____

Areas of work:

• ____ Access Control	• ____ Awareness/Training	• ____ Audit/Accountability
• ____ Assessment & Authorization	• ____ Configuration Management	• ____ Contingency Planning
• ____ Identification & Authentication	• ____ Incident Response	• ____ Maintenance
• ____ Media Protection	• ____ Physical Environmental Protection	• ____ Planning
• ____ Personnel Security	• ____ Risk Assessment	• ____ System and Services Acquisition
• ____ System and Communication Protection	• ____ System and Information Integrity	• ____ Program Management

Organization #5

Organization: ______________________________ Position: _________________________

Years performing this work: ____

Areas of work:

• ____ Access Control	• ____ Awareness/Training	• ____ Audit/Accountability
• ____ Assessment & Authorization	• ____ Configuration Management	• ____ Contingency Planning
• ____ Identification & Authentication	• ____ Incident Response	• ____ Maintenance
• ____ Media Protection	• ____ Physical Environmental Protection	• ____ Planning
• ____ Personnel Security	• ____ Risk Assessment	• ____ System and Services Acquisition
• ____ System and Communication Protection	• ____ System and Information Integrity	• ____ Program Management

Organization #6

Organization: ______________________________ Position: _________________________

Years performing this work: ____

Areas of work:

• ____ Access Control	• ____ Awareness/Training	• ____ Audit/Accountability
• ____ Assessment & Authorization	• ____ Configuration Management	• ____ Contingency Planning
• ____ Identification & Authentication	• ____ Incident Response	• ____ Maintenance
• ____ Media Protection	• ____ Physical Environmental Protection	• ____ Planning
• ____ Personnel Security	• ____ Risk Assessment	• ____ System and Services Acquisition
• ____ System and Communication Protection	• ____ System and Information Integrity	• ____ Program Management

Organization #7

Organization: ______________________________ Position: _________________________

Years performing this work: ____

Areas of work:

• ____ Access Control	• ____ Awareness/Training	• ____ Audit/Accountability
• ____ Assessment & Authorization	• ____ Configuration Management	• ____ Contingency Planning
• ____ Identification & Authentication	• ____ Incident Response	• ____ Maintenance
• ____ Media Protection	• ____ Physical Environmental Protection	• ____ Planning
• ____ Personnel Security	• ____ Risk Assessment	• ____ System and Services Acquisition
• ____ System and Communication Protection	• ____ System and Information Integrity	• ____ Program Management

Organization #8

Organization: ______________________________ Position: _________________________

Years performing this work: ____

Areas of work:

• ____ Access Control	• ____ Awareness/Training	• ____ Audit/Accountability
• ____ Assessment & Authorization	• ____ Configuration Management	• ____ Contingency Planning
• ____ Identification & Authentication	• ____ Incident Response	• ____ Maintenance
• ____ Media Protection	• ____ Physical Environmental Protection	• ____ Planning
• ____ Personnel Security	• ____ Risk Assessment	• ____ System and Services Acquisition
• ____ System and Communication Protection	• ____ System and Information Integrity	• ____ Program Management

Organization #9

Organization: ______________________________ Position: _________________________

Years performing this work: ____

Areas of work:

• ____ Access Control	• ____ Awareness/Training	• ____ Audit/Accountability
• ____ Assessment & Authorization	• ____ Configuration Management	• ____ Contingency Planning
• ____ Identification & Authentication	• ____ Incident Response	• ____ Maintenance
• ____ Media Protection	• ____ Physical Environmental Protection	• ____ Planning
• ____ Personnel Security	• ____ Risk Assessment	• ____ System and Services Acquisition
• ____ System and Communication Protection	• ____ System and Information Integrity	• ____ Program Management

Organization #10

Organization: ______________________________ Position: _________________________

Years performing this work: ____

Areas of work:

• ____ Access Control	• ____ Awareness/Training	• ____ Audit/Accountability
• ____ Assessment & Authorization	• ____ Configuration Management	• ____ Contingency Planning
• ____ Identification & Authentication	• ____ Incident Response	• ____ Maintenance
• ____ Media Protection	• ____ Physical Environmental Protection	• ____ Planning
• ____ Personnel Security	• ____ Risk Assessment	• ____ System and Services Acquisition
• ____ System and Communication Protection	• ____ System and Information Integrity	• ____ Program Management

C. Total Amount of Time (in Years): _______________________________________

4. Third-Party Endorsements

FITSI requires that FITSP Certification Applicants submit two endorsements by colleagues or employees that can validate the FITSP Certification Applicant's experience identified in Section 2 above. The endorsers do not need to validate every organization where the FITSP Certification Applicant has worked. The purpose of the endorser is to help validate the five years of IT security experience in a commercial or government environment. An Endorser can be a supervisor, employer, manager, or certified peer. A certified peer must hold one of the certifications listed in Section 5.B below.

The endorsement forms are available as separate documents to provide by email to colleagues or employers. These endorsement forms are part of the .zip file that includes this application and is available for download at http://www.fitsi.org/documents.html.

5. Optional – Waiving up to Three Years of Professional Experience

FITSP Certification Applicants can waive portions of the experience requirements if the FITSP Certification Applicant possesses other complimentary security certifications or education.

FITSP Certification Applicants may not waive more than three years of experience with any combination of education or certifications.

A. Advanced Degree Waiver Criteria

FITSP Certification Applicants 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.

This waiver process allows for a maximum of two degrees (one undergraduate and one graduate). Advanced degrees can only be used to waive up to two years of professional experience.

B. Existing IT Security Certification Waiver Criteria

FITSP Certification Applicants 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)

This waiver process allows a maximum of two certifications. Industry certifications can only be used to waive up to two years of professional experience.

For FITSP Certification Applicants planning on waiving experience via academic experience, Certification Applicants must include a copy of their official college transcripts with this application.

For FITSP Certification Applicants planning on waiving experience via other industry certifications, Certification Applicants must include a URL (or electronic copy of certification) from a certification body (see below) where FITSI can independently verify that the FITSP Certification Applicant does possess that certification.

Please complete the following section:

I am requesting a waiver of ___________ (write in one or two) year(s) of professional experience by using my advanced degree(s) in IT or information assurance. I have attached my college transcript(s) to this application.

I am requesting a waiver of ___________ (write in one or two) year(s) of professional experience by using existing IT security certifications. The certifications I am using are listed below:

1. ____
   a. URL for verification: ____
   b. An Electronic Copy of the Certification is attached: □
2. ____
   a. URL for verification: ____
   b. An Electronic Copy of the Certification is attached: □

6. FITSP Certification Applicant Attestation

Dear FITSI,

As part of the application process to be awarded a FITSP certification, I have included details regarding my professional experience to demonstrate the necessary five years of information security experience.

I attest that this information is correct and accurate and that I have not intentionally misled or falsified any aspect of this application, either intentionally or via accident. I understand that if I am audited, and FITSI finds that my information is not accurate, I may have my certification suspended and/or withdrawn. I will not be entitled to any form of a refund of either examination or annual maintenance fees.

By signing this application, I also agree to the following:

1. Comply with relevant provisions of the FITSP certification scheme.
2. Comply with the FITSP certification requirements and supply any information (or additional information) needed for the assessment.
3. Comply with all requirements and guidelines documented in the *FITSI Certification Holder Handbook*.
4. Adhere to the FITSI Code of Ethics.
5. Make claims regarding FITSP certification only with respect to the scope for which I have been granted certification.
6. Refrain from using the FITSP certification in any manner that brings FITSI into disrepute.
7. Refrain from using the FITSP certification in a misleading manner.
8. Refrain from making any misleading or unauthorized statements about the FITSP certification.
9. Discontinue the use of all claims and references to FITSP certification upon suspension, withdrawal, or revocation of certification and return any certificates issued by FITSI.
10. Refrain from further promotion of the FITSP certification during anytime the FITSP certification is suspended, withdrawn, or revoked.
11. Discontinue the use of all claims to FITSP certification upon resigning my FITSP certification and return any FITSP certification certificates issued by FITSI.
12. Notify FITSI, without delay, of matters that affect my capability to continue to fulfill the FITSP certification requirements.
13. Discontinue use of the FITSP Certification Logo if my FITSP certification is withdrawn (revoked).
14. Comply with the most current policies documented in the *FITSI Logo and Mark Usage Requirements Handbook* when using the FITSP Certification Logo or FITSP Certification Text Mark.

By my signature below, I hereby accept and acknowledge all of above attestations and intend to be legally bound. I acknowledge that this application may be electronically signed and agree that an electronic signature shall have the same force and effect as a handwritten signature for the purposes of validity, enforceability, and admissibility.

____
Printed Name

____
Signature Date