# FITSI Certification Application

Application Form for
after a FITSI
Examination has been
Successfully
Completed

Version 1.3

Published 7/24/2015


This page is left intentionally blank

# TABLE OF CONTENTS

## 1. Instructions for the Certification Candidate

As part of earning a FITSI certification, candidates must successfully pass a certification exam and submit this certification application before being awarded the credential. FITSI requires three components at a minimum as a part of this application:

1. Documentation of a candidate's background including details of each job they have held to support the minimum five years of IT security experience.
2. A third party endorsement from two colleagues who can verify the candidate's experience.
3. A formal attestation by the candidate that the information provided in this application is true and correct.

Optionally, a candidate may waive up to three years of experience with one of several industry IT security certifications and/or a bachelor's and/or master's degree in information technology or information assurance from an accredited college. The ability to waive professional experience can be done in Section 4 of this application.

This document can be filled out electronically and emailed to FITSI. Candidates must fill out section 2, 3 and 5 in its entirety and submit this application in total (all pages) by faxing it to 703-754-8215 or emailing it contactus@fitsi.org. If section 4 is used (waiving up to three years of professional experience) that must be filled out as well.

***If the application is not completed in full and returned in total (all 17 pages), the application will be denied and the candidate will be notified via email.***

FITSI endeavors to award certification of candidates within 60 calendar days from the time this application (and all supporting documentation) is submitted.

***Effective 1/10/2014, FITSP candidates are allowed to take the certification exam before the 5 years of experience has been meet and allowed to earn it over the next 5 years. Once the candidate obtains the necessary experience during the 5 years after taking the exam, the candidate can fill out the certification application and be awarded the FITSP credential.***

## 2. Candidate Background

As part of the application process candidates must have 5 years of information security experience. This section provides FITSI with the key elements to determine if the minimum professional experience requirements of candidates are being met.

### A. General Candidate Information

First Name: _____ Middle Initial: _____

Last Name: _____

Preferred Mailing Address: _____

_____

_____

Candidate Contact Email: _____

Candidate Contact Phone: _____

FITSI ID: _____ (put N/A if no FITSI ID has been assigned yet)

Certification Role Applying for: **Please Select a Role from the Drop Down** _____

## B. Candidate Experience

Please provide background information for each position where you have had significant IT security responsibility. Under the "Areas of work" section **please place a "P" for primary, for each topic this position has dealt with as part of daily duties. Please place an "S" for secondary, for each topic that encompasses less than 50% of your job tasks.** At the end of Organization #10 please sum up the total amount of time that all of these jobs have included.

### 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):** _____

## 3. Third-Party Endorsements

FITSI requires that candidates must get two endorsements by colleagues or employees that can validate the candidate experience identified in section #2 above. The endorsers do not need to validate every organization that a candidate has worked at. They must help validate the five years of IT security experience in the commercial or government environment.

The endorsement forms are available as separate documents to be able to email to colleagues or employers. These separate copies of the endorsement forms can be found at http://www.fitsi.org/documents.

## A. Endorser #1

The following is an endorsement for (FITSI Certification Candidate full name):

_____

The following information is to be completed by the person providing the endorsement

Endorser's Information:

Endorser's Name: _____
Profession and Title: _____
Business Address: _____
_____
Daytime Phone: _____
Contact Email: _____

Years professionally associated with Applicant: _____

To the best of your knowledge does the candidate possess at least five years of information security experience? _____

Do you consider the candidate to be a personal of good moral character? _____

Brief description of the professional relationship with the applicant and applicant duties: (Include supporting professional details specific to the Certification Role)

_____
_____
_____
_____
_____
_____
_____
_____
_____

I, _____, attest that the information given above is accurate and true. I agree to provide any additional information requested by FITSI.

_____
Signature of Endorser Date

## B. Endorser #2

The following is an endorsement for (FITSI Certification Candidate full name):

_____

The following information is to be completed by the person providing the endorsement

Endorser's Information:

Endorser's Name: _____
Profession and Title: _____
Business Address: _____
_____
Daytime Phone: _____
Contact Email: _____

Years professionally associated with Applicant: _____

To the best of your knowledge does the candidate possess at least five years of information security experience? _____

Do you consider the candidate to be a personal of good moral character? _____

Brief description of the professional relationship with the applicant and applicant duties: (Include supporting professional details specific to the Certification Role)

_____
_____
_____
_____
_____
_____
_____
_____
_____

I, _____, attest that the information given above is accurate and true. I agree to provide any additional information requested by FITSI.

_____
Signature of Endorser Date

## 4. Optional – Waiving up to Three Years of Professional Experience

FITSI candidates are able to waive some experience requirements if the candidate possesses other advanced degrees and/or other complimentary IT security certifications.

***Candidates cannot waive more than 3 years of professional experience in total (with both advanced degrees and certifications).***

### A. Advanced Degree Waiver Criteria

Candidates can waive one year of experience for a bachelor degree with an information technology or information assurance focus. Candidates can waive a second year with a master's degree in an information technology or information assurance focus. Degrees must be issued by a fully accredited institution.

A maximum of 2 degrees (1 undergraduate and 1 graduate) can be used for this waiver process. This means advanced degrees can only be used to waive up to two years of professional experience.

### B. Existing IT Security Certification Waiver Criteria

Candidates can waive one year of experience for each of the following IT security certifications:

- CISM - Certified Information Security Manager
- CISSP - Certified Information Systems Security Professional
- CISA - Certified Information Systems Auditor
- GIAC - Global Information Assurance Certified
- CEH - Certified Ethical Hacker
- Security+
- SSCP - System Security Certified Practitioner
- SCNA - Security Certified Network Architect
- SCNS - Security Certified Network Specialist
- CAP - Certification and Accreditation Professional

A maximum of 2 certifications can be used for this waiver process. This means industry certifications can only be used to waive up to two years of professional experience.

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

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

Please fill out the below section:

I am requesting a waiver of _____ (write in one or two) year(s) of professional experience by using my advanced degree(s) in information technology 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. Electronic Copy of Certification is attached: ☐
2. _____
   a. URL for verification: _____
   b. Electronic Copy of Certification is attached: ☐

## 5. Candidate Attestation

This form must be filled out and signed by the candidate.

Dear FITSI

As part of the application process to be awarded a FITSI 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 mislead or falsified any aspect of this application either intentionally or via accident. I understand that if I am audited and it is determined that my information is not accurate I can have my certification revoked and I will not be entitled to any form of refund of either examination or annual maintenance fees.

_____
Printed Name

_____
Signature

_____
Date