Personnel Certification

Swiss Association for Quality

Federation of Swiss IT Experts

A program of the EXPERT FSIE .ch series.

D465 EN

Expert FSIE™ Security (ICT and Cyber Security)

Public Version 1.0

Authored by: security@fsie.ch (Specialized Commission, Lead a.i. U. Annino)

Classification: Public

Status: Release

Document-ID: **D465_S3_EN**

Table of Contents

1. Scope

The certification is processed as per the generic SAQ Expert FSIE™ certification scheme (D500) and detailed regulation (D420 including all referenced documents therein). The document at hand describes the specific practices (competences) and requirements for the program **Security.**

These must be demonstrated by work testimonials, advanced education graduations, the handed-in case study and in the oral exam. The re-certification encompasses work testimonials and continuing education requirements.

Additional to traditional specialisation certifications, each Expert FSIE™

- requires basic IT competences common for each of the specialisations
- knows how to efficiently collaborate with other IT experts (context and role models)
- can integrate his existing diploma and certifications into the FSIE title
- adheres to a common Code of Conduct
- follows the same pattern of periodical competences updates by practice and education

2. Summary of the Profile Security

The Expert FSIE™ Security takes the responsibility for reliable IT services by managing risks to security objectives such as availability, confidentiality and integrity of systems and data. He/she is developing policies and IT security management systems (ISMS) as well as providing assurance and awareness to IT, business and management.

swissICT "Berufe der ICT" profiles covered:

- ICT Security Officer (also: Information Security Manager, Information Security Officer, Chief Security Officer/CSO, Chief Information Security Officer/CISO, Data Protection Officer/DPO)
- ICT-Security-Specialist (ICT Security Engineer, ICT Security Expert)
- ICT Security Architect
- ICT-Security-Operations-Manager (ICT Security Operations Analyst, Security Operations Engineer, ICT Security Incidents Manager)
- ICT-Consultant (Security)
- ICT-System-Engineer (Security) or ICT-Platform-Engineer (Security) or Systems Development Engineer (Security)

Agile profiles covered:

- Expert IT Security
- Engineer IT Security

3. Catalog of IT Security Practices and Collaboration Requirements

The practices are further refined in an FSIE-internal document which contains detailed competences description, methods, techniques and sample examination questions.

3.1. IT Security Practices

Practice-ID	Title	Description
sBOC 01	Strategy-driven security objectives	Understand business and IT strategies as well as enterprise risk policies to define IT security objectives
sBOC 02	IT Security Architecture	Understand business architecture and processes to define IT security architecture
sBOC 03	IT Security Risks and Threats	Define IT security risk categories and understand current threats both global and specific to the enterprise
sBOC 04	ISMS	Develop holistic IT security management systems based on current standards
sBOC 05	Regulations Impacts	Understand national and international regulations and their impacts on the "security minded" development, engineering and operation of IT services
sBOC 06	IT Security Controls	Capability to develop and implement IT security controls for processes, people and technology as well as conduct awareness programs to impacted persons
sBOC 07	Assessments and Reviews	Perform assessments and reviews of effectiveness, efficiency and maturity of IT security controls
qsBOC 08	Quality and Security minded ICT-Framework	Cooperation and collaboration of the quality and security experts for the holistic view and design of a "quality and security minded" ICT-Framework.
sBOC 09	IT Security Reporting	Report IT security status and risks to all management levels

The IT Expert FSIE™ Security is required to reach a level of competence according to Bloom[1] of 4, 5 or 6 (analysis, synthesis, evaluation) for 7 out of the 9 practices. The 2 remaining he/she should master at level 3 (application).

[1] https://en.wikipedia.org/wiki/Bloom%27s_taxonomy

3.2. Security Collaboration Requirements

Topic	Description
Expert FSIE™ BRIDGE	Typically, the Expert FSIE™ Security is involved in the preparation or execution of a project by the respective expert. This expert understands the business context, owns the business requirements, prepares business cases and guides the overall project execution.
Expert FSIE™ Engineering	The tasks of software/hardware design and development are delegated to the respective experts in coordination of an eventually involved Expert FSIE™ BRIDGE.
Expert FSIE™ Quality	The tasks of quality management, measurement and reporting for continuous process improvement tailored to the enterprise architecture and objectives are delegated to the respective experts.
Expert FSIE™ Strategy	The Expert FSIE™ Security takes inputs and coordinates with this expert. The respective expert delegates strategic IT security topics to the Expert FSIE™ Security.
Expert FSIE™ Operations	IT operational and platform tasks are delegated to or coordinated with these respective experts.
Expert FSIE™ Management	IT Management / CIO is involved in the strategic positioning of IT security and receives the IT security reports (as are possibly all other management roles up to CEO as per enterprise directives)

When delegating, holders of the titles Expert FSIE™ <xy> in provider lead roles are preferred.

An Expert FSIE™ Security must demonstrate the understanding and practical application of the above collaborations with

- Strategy
- Operations
- BRIDGE (Project)

3.3. IT Security Work Context Requirements

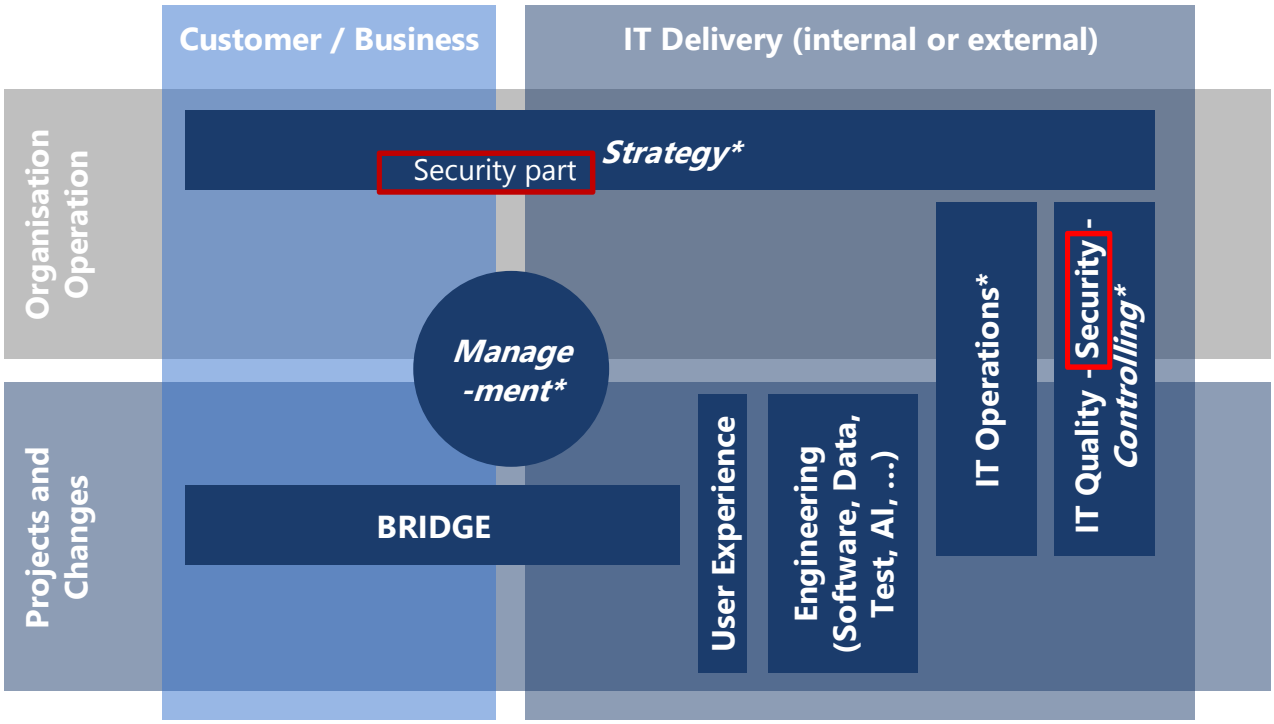
"Run the enterprise" / operations tasks	The Expert FSIE™ Security is involved in governance activities related to IT security. He/she defines and implements a holistic control framework and management system to address and also sensitize process, people and technology-related security risks. In this role, he/she typically performs “2nd line of defence” duties e.g. as an Information/IT Security Officer or Data Protection Officer DPO. But also “1st line of defence” activities to ensure information/IT security in day-to-day IT

	service delivery processes as a security manager/administrator are common. With a risk-based approach, the Expert FSIE™ Security consults operational as well as "2nd LoD" units regarding information/IT security. He/she performs security assessments, assists in running security systems as well as remediation processes within a Security Operation Centre SOC and serves as point of contact for internal and external (security) auditors.
"Change the enterprise" / Project tasks	The Expert FSIE™ Security is involved in all phases of a project. During project initiation and requirement specification phases, he/she ensures the specification of appropriate security requirements which typically are non-functional and reviews them for compliance to company policies. During the solution design phase, he/she performs the security risk analysis. Also, security aspects of the design are defined, and security testing requirements are specified. In the implementation phase, the Expert FSIE™ Security plans and provides independent security tests and eventually gives the security sign-off. Finally, in the first operational phase, he/she ensures that proper security incident, response and event management processes are in place and time-critical requirements for example "data breach notifications" are compliant.

An Expert FSIE™ Security must demonstrate to have taken the lead in both of the 2 above-mentioned contexts at least once.

3.4. The Expert FSIE™ Security in the FSIE profiles collaboration and work model

An Expert FSIE™ Security has primarily an operations-oriented (continuing duties and tasks) role but is involved in projects/changes (ITIL: service creation) as the respective expert.



4. Work Testimonials

The work testimonials are reported using the standard regulation and electronic form (D450) valid for every Expert FSIE™.

4.1. Requirements

The required minimum is 40% capacity in the past 6 years, i.e. 3'840 hours of practical work covering the 9 practices as per chapter 3.1 not older than 6 years must be reported.

For each of the 9 practices, he/she must have a record of >=160 hours.

The collaboration requirements as per chapter 3.2 must be demonstrated.

The work context requirements as per chapter 3.3 must be demonstrated.

5. Advanced Education Requirements

The Expert FSIE™ Security has graduated >=15 attributed Security ECTS worth of any of the following advanced education programs (or certificates). The graduation certificates must be provided (scanned).

Education Provider	Name	Link	Attributed Security ECTS
EPFL - Ecole Polytechnique Federale Lausanne	Master-Specialisation: Information security (from September 2018: Cyber security)		20
FHNW - Fachhochschule Nordwestschweiz	CAS Information Security & Risk Management		10
FH/ZHAW	Master-Specialisation: Information Security	X	20
GSE	GIAC Security Expert		4
Hochschule Luzern	CAS Information Security		10
	MAS Information Security		20
ibW - Südostschweiz	Eidg. Dipl. ICT Security Experte (ICT-Berufsbildung)	X	20
ISACA	CISM		2
	CISA		2
	CRISC		4
ISC	CISSP		5
	CCSP		5
	CSSLP		5
diverse - Diverse	Eidg. Dipl. ICT Security Experte (ICT-Berufsbildung)		20

Important Note: The list above only encompasses Swiss Security advanced education offerings known to the FSIE Security specialisation commission. If a candidate is a graduate of a non-listed course that presumably covers all or some of the Security practices, he/she shall submit it and the FSIE Security specialisation commission will assess the validity and eventually attributable ECTS. Also, if you are a provider of advanced education that is not listed, please send it in for assessment and listing to security@fsie.ch.

The graduations must not be older than 6 years or maintained in the past 6 years, if the advanced education has a re-certification regulation (e.g. CISSP).

Temporary regulation:
The non-re-certifiable graduations can be older than 6 years. Also, they can stem from no longer existing education providers and/or be titles/programs that do no longer exist but were appropriately covering the educational aspects of the Security practices as listed in chapter 3.1.

6. Case Study

The case study is written using the standard template (D423) valid for every Expert FSIE™.

Specific Security requirement:
The case study must encompass the development and implementation of an ISMS (sBOC 04) i.e. a holistic IT Security Management System.

7. Oral Exam

The oral exam is conducted using the standard structure and assessment scheme valid for every Expert FSIE™ (D421).

6 of the 9 practices must be covered in the 2nd and 3rd exam parts of the case study and specialisation questionings.

8. Re-Certification

The re-certification requirements are checked every 3 years.

8.1. Continued work testimonials

The continued work testimonials are reported using the standard regulation and electronic form (D450) valid for every Expert FSIE™.

The required minimum is 40% capacity in the past 3 years, i.e. 1'920 hours of practical work covering the 9 practices as per chapter 3.1 not older than 3 years must be reported by the Expert FSIE™ Security.

For 7 of the 9 practices, he/she must have a record of >=80 hours.

The collaboration requirements as per chapter 3.2 must be demonstrated.

The work context requirements as per chapter 3.3 must be demonstrated.

If feasible, a onetime extension of 0.5 years to reach the above requirements can be granted.

8.2. Continuing education

The Expert FSIE™ Security must achieve the standard amount of 18 CEP with IT security-specific or generic continuing education in 3 years conforming to the FSIE CEP regulation (D440). Note: 18 CEP can be achieved by attending 9 full-day IT security or generic refresher courses. However, the CEP regulation attributes CEP also to other continuing education measures.

If feasible, a onetime extension of 0.5 years to reach the above requirement can be granted.

9. Title

- The title is valid for 3 years after the initial certification and after each successfully completed re-certification.
- As long as valid, the holder is licensed to use the following title:

  [IT] Expert FSIE™ Security

  Note: [] denotes optional parts, ¦ separates options.

For the other language variants refer to D465_DE, D465_FR and D465_IT