

Profile title			
INFORMATION SECURITY SPECIALIST ROLE (12)			
Summary statement			
Ensures the implementation of the organisation's information security policy by the secure and appropriate use of ICT resources.			
Mission			
Defines, proposes and implements necessary information security techniques and practices in compliance with information security standards and procedures. Contributes to security practices, awareness and compliance by providing advice, support, information and training.			
Deliverables			
	Accountable	Responsible	Contributor
	<ul style="list-style-type: none"> <li>Knowledge or Information Base (Security)</li> </ul>	<ul style="list-style-type: none"> <li>Solution and Critical Business Process Integration Proposal (Security)</li> <li>Information Security Risk Assessment</li> </ul>	<ul style="list-style-type: none"> <li>Risk Management Policy</li> <li>Information Security Risk Treatment Plan</li> <li>Information Security Policy</li> </ul>
Main task/s			
<ul style="list-style-type: none"> <li>Evaluate information security risks, threats and consequences and take appropriate action</li> <li>Provide information security training and education</li> <li>Provide technical validation of security tools, implement, configure and manage appropriate tools</li> <li>Contribute to the definition of and actively promote information security standards and procedures throughout the IT and IT user communities</li> <li>Identify and remediate security vulnerabilities</li> <li>Monitor security developments to ensure the continued efficiency and effectiveness of information security processes and controls</li> <li>Proactively evaluate new threats and counter potential information security incidents</li> <li>Implements security techniques on all or part of an application, process, network or system within area of responsibility</li> </ul>			

The table above is an extract from *European ICT professionals role profiles* Ref. No. CWA 16458-1:2018 E © 2018 CEN

The following pages map SFIA skills and competency levels to the role profile. There are 2 parts to the mapping:

• **The Level of responsibility.**

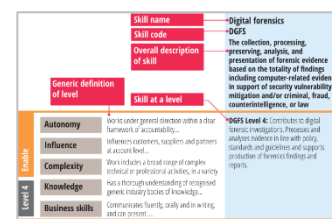
A common language is used to describe levels of responsibility across roles in all professional disciplines. The SFIA Framework consists of seven levels of responsibility; Level 1, the lowest, to Level 7, the highest. The levels describe the behaviours, values, knowledge and characteristics that an individual should have in order to be identified as competent at the level. Each of the levels is also labelled with a phrase to summarise the level of responsibility.

Level 7	Set strategy, inspire, mobilise
Level 6	Initiate, influence
Level 5	Ensure, advise
Level 4	Enable
Level 3	Apply
Level 2	Assist
Level 1	Follow

• **The Professional skills.**

SFIA 7 consists of 102 professional skills. Each skill description is made up of an overall definition of the skill and a description of the skill at each of up to seven levels.

The skill level descriptions provide a detailed definition of what it means to practice the skill at each level of competency. The skill level descriptions are aligned to the 7 levels of responsibility which ensures consistency throughout the SFIA framework making it solid and robust across professional disciplines.



NB: This is an illustrative skills profile only. It may not be the best fit for your organization. Anyone using this document should take care to apply the principles of SFIA to their own organisation and role design. See the [SFIA website](#) for further guidance.

**EU ICT Security Specialist role (12) (NB this could be a multi-level role)****SFIA Generic Responsibility Levels for the Role****Autonomy - Level 5**

- Works under broad direction
- Work is often self-initiated
- Is fully responsible for meeting allocated technical and/or project/supervisory objectives
- Establishes milestones and has a significant role in the assignment of tasks and/or responsibilities

**Influence - Level 5**

- Influences organisation, customers, suppliers, partners and peers on the contribution of own specialism
- Builds appropriate and effective business relationships
- Makes decisions which impact the success of assigned work, i.e. results, deadlines and budget
- Has significant influence over the allocation and management of resources appropriate to given assignments
- Leads on user/customer collaboration throughout all stages of work
- Ensures users' needs are met consistently through each work stage

**Complexity - Level 5**

- Performs an extensive range and variety of complex technical and/or professional work activities
- Undertakes work which requires the application of fundamental principles in a wide and often unpredictable range of contexts
- Understands the relationship between own specialism and wider customer/organisational requirements

**Knowledge - Level 5**

- Is fully familiar with recognised industry bodies of knowledge both generic and specific
- Actively seeks out new knowledge for own personal development and the mentoring or coaching of others
- Develops a wider breadth of knowledge across the industry or business
- Applies knowledge to help to define the standards which others will apply

**Business Skills - Level 5**

- Demonstrates leadership
- Communicates effectively, both formally and informally
- Facilitates collaboration between stakeholders who have diverse objectives
- Analyses, designs, plans, executes and evaluates work to time, cost and quality targets
- Analyses requirements and advises on scope and options for continuous operational improvement
- Takes all requirements into account when making proposals
- Demonstrates creativity, innovation and ethical thinking in applying solutions for the benefit of the customer/stakeholder
- Advises on the available standards, methods, tools and applications relevant to own specialism and can make appropriate choices from alternatives
- Maintains an awareness of developments in the industry
- Takes initiative to keep skills up to date
- Mentors colleagues
- Assesses and evaluates risk
- Proactively ensures security is appropriately addressed within their area by self and others
- Engages or works with security specialists as necessary
- Contributes to the security culture of the organisation

**EU ICT Security Specialist role (12)** (NB this could be a multi-level role)**SFIA Professional Skills for the Role**

Core - all people performing this job will need this skill. Optional - some people performing this job will need the skill.

**Core: Information Security @ Level 5**

- Provides advice and guidance on security strategies to manage identified risks and ensure adoption and adherence to standards
- Obtains and acts on vulnerability information and conducts security risk assessments, business impact analysis and accreditation on complex information systems
- Investigates major breaches of security, and recommends appropriate control improvements
- Contributes to development of information security policy, standards and guidelines

**Core: Information Assurance @ Level 5**

- Interprets information assurance and security policies and applies these in order to manage risks
- Provides advice and guidance to ensure adoption of and adherence to information assurance architectures, strategies, policies, standards and guidelines
- Uses testing to support information assurance
- Contributes to the development of policies, standards and guidelines

**Core: Relationship management @ Level 5**

- Identifies the communications and relationship needs of stakeholder groups
- Translates communications / stakeholder engagement strategies into specific activities and deliverables
- Facilitates open communication and discussion between stakeholders, acting as a single point of contact by developing, maintaining and working to stakeholder engagement strategies and plans
- Provides informed feedback to assess and promote understanding
- Facilitates business decision-making processes
- Captures and disseminates technical and business information

**Core: Learning delivery @ Level 4**

- Prepares or customises and delivers learning activities and the learning environment for a variety of audiences
- Teaches, instructs, trains students/learners in order to develop knowledge, techniques and skills using appropriate methods, tools, online environments, equipment and materials
- Oversees students/learners in performing practical activities and work, advising and assisting where necessary, and ensuring that maximum learning benefit is gained from the practical experience
- Provides detailed instruction as necessary and responds to wide-ranging and detailed questioning in own area(s) of specialisation
- Assesses objectively, against pre-set criteria, the ability levels of students and reports as appropriate
- Develops examples and case study material for use in pre-defined courses
- Adapts simple course material to meet the needs of students

**Optional: Security administration @ Level 5**

- Monitors the application and compliance of security administration procedures and reviews information systems for actual or potential breaches in security
- Ensures that all identified breaches in security are promptly and thoroughly investigated and that any system changes required to maintain security are implemented
- Ensures that security records are accurate and complete and that request for support are dealt with according to set standards and procedures
- Contributes to the creation and maintenance of policy, standards, procedures and documentation for security

**Optional: Conformance review @ Level 4**

- Conducts formal reviews of activities, processes, products or services
- Collects, collates and examines records as part of specified testing strategies for evidence of compliance with management directives, or the identification of abnormal occurrences
- Analyses evidence collated and drafts part or all of formal reports commenting on the conformance found to exist in the reviewed part of an information systems environment

**Optional: Continuity management @ Level 4**

- Implements and contributes to the development of a continuity management plan
- Coordinates the assessment of risks to the availability, integrity and confidentiality of systems that support critical business processes
- Coordinates the planning, designing, testing of maintenance procedures and contingency plans

**Optional: Business risk management @ Level 4**

- Investigates and reports on hazards and potential risk events within a specific function or business area

**Optional: Learning design and development @ Level 4**

- Specifies the content and structure of learning and development materials
- Takes responsibility for design, creation, packaging and maintenance and manages development to deliver agreed outcomes
- Where required, designs, configures and tests learning environments, including population of simulated databases, and replication of external systems, interfaces, and assessment systems
- Secures external accreditations as appropriate