Profile title	INFORMATION SECURITY MANAGER ROLE (11)		
Summary statement	Leads and manages the organisation information security policy.		
Mission	Defines the information security strategy and manages implementation across the organisation. Embeds proactive information security protection by assessing, informing, alerting and educating the entire organisation.		
Deliverables	**Accountable**	**Responsible**	**Contributor**
	• Information Security Policy	• Knowledge or Information Base • Information Security Strategy	• Risk Management Policy • New Solution and Critical Business Integration Proposal
Main task/s	• Define the information security strategy and standards • Contribute to the development of the organisation's security policy • Manages security audits • Evaluate risks, threats and consequences • Establish and manage prevention, detection, correction and remediation plans • Inform and raise awareness among general management and across all IT users and professionals • Conduct information security operations		

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:

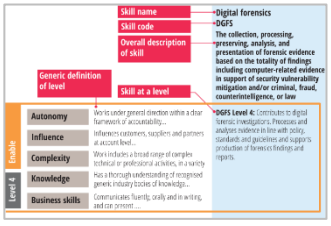
- ***The Level of responsibility.***

  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.

- ***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.



EU ICT Security Manager role (11) *(NB this could be a multi-level role)*

SFIA Generic Responsibility Levels for the Role

Autonomy - Level 6

• Has defined authority and accountability for actions and decisions within a significant area of work, including technical, financial and quality aspects
• Establishes organisational objectives and assigns responsibilities

Influence - Level 6

• Influences policy and strategy formation
• Initiates influential relationships with internal and external customers, suppliers and partners at senior management level, including industry leaders
• Makes decisions which impact the work of employing organisations, achievement of organisational objectives and financial performance

Complexity - Level 6

• Has a broad business understanding and deep understanding of own specialism(s)
• Performs highly complex work activities covering technical, financial and quality aspects
• Contributes to the implementation of policy and strategy
• Creatively applies a wide range of technical and/or management principles

Knowledge - Level 6

• Promotes the application of generic and specific bodies of knowledge in own organisation
• Has developed business knowledge of the activities and practices of own organisation and those of suppliers, partners, competitors and clients

Businesss Skills - Level 6

• Demonstrates clear leadership
• Communicates effectively at all levels to both technical and non-technical audiences
• Understands the implications of new technologies
• Understands and communicates industry developments, and the role and impact of technology in the employing organisation
• Absorbs complex information
• Promotes compliance with relevant legislation and the need for services, products and working practices to provide equal access and equal opportunity to people with diverse abilities
• Takes the initiative to keep both own and colleagues' skills up to date
• Manages and mitigates risk
• Takes a leading role in promoting security throughout own area of responsibilities and collectively in the organisations

EU ICT Security Manager role (11) *(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 6

• Develops and communicates corporate information security policy, standards and guidelines
• Contributes to the development of organisational strategies that address information control requirements
• Identifies and monitors environmental and market trends and pro-actively assesses impact on business strategies, benefits and risks
• Leads the provision of authoritative advice and guidance on the requirements for security controls in collaboration with experts in other functions eg legal, technical support
• Ensures architectural principles are applied during design to reduce risk and drives adoption and adherence to policy, standards and guidelines

Core: Information Assurance @ Level 6

• Develops corporate Information assurance policy, standards and guidelines
• Contributes to the development of organisational strategies that address the evolving business risk and information control requirements
• Drives adoption of and adherence to policies and standards through the provision of expert advice and guidance in order to ensure architectural principles are applied, requirements are defined and rigorous security testing is applied
• Monitors environmental and market trends and pro-actively assesses impact on business strategies, benefits and risks

Core: Enterprise IT governance @ Level 5

• Reviews current and proposed information systems for compliance with the organisations obligations (including legislation, regulatory, contractual and agreed standards/policies) and adherence to overall strategy
• Provides specialist advice to those accountable for governance to correct compliance issues

Core: Security administration @ Level 6

• Develops policies, standards, processes, guidelines for ensuring the physical and electronic security of automated systems
• Ensures that the policy and standards for security administration are fit for purpose, current and are correctly implemented
• Reviews new business proposals and provides specialist advice on security issues and implications

Core: Relationship management @ Level 6

• Leads the development of comprehensive stakeholder management strategies and plans
• Builds long-term, strategic relationships with senior stakeholders (internal and external)
• Facilitates the engagement of stakeholders and delivery of services and change projects, acting as a single point of contact for senior stakeholders, facilitating relationships between them
• Negotiates to ensure that stakeholders understand and agree what will meet their needs, and that appropriate agreements are defined
• Oversees monitoring of relationships including lessons learned and appropriate feedback
• Leads actions to improve relations and open communications with and between stakeholders

Optional: Business risk management @ Level 6

• Plans and manages the implementation of organisation-wide processes and procedures, tools and techniques for the identification, assessment, and management of risk inherent in the operation of business processes and of potential risks arising from planned change

Optional: Conformance review @ Level 6

• Specifies organisational procedures for the internal or third-party assessment of an activity, process, product or service, against recognised criteria
• Develops plans for review of management systems, including the review of implementation and use of standards and the effectiveness of operational and process controls
• May manage the review, conduct the review or manage third party reviewers
• Identifies areas of risk and specifies interrogation programs
• Recommends improvements in processes and control procedures
• Authorises the issue of formal reports to management on the extent of compliance of systems with standards, regulations and/or legislation