

Applying SFIA's skills to cybersecurity focus areas

Attribution-ShareAlike 4.0
International (CC BY-SA 4.0)

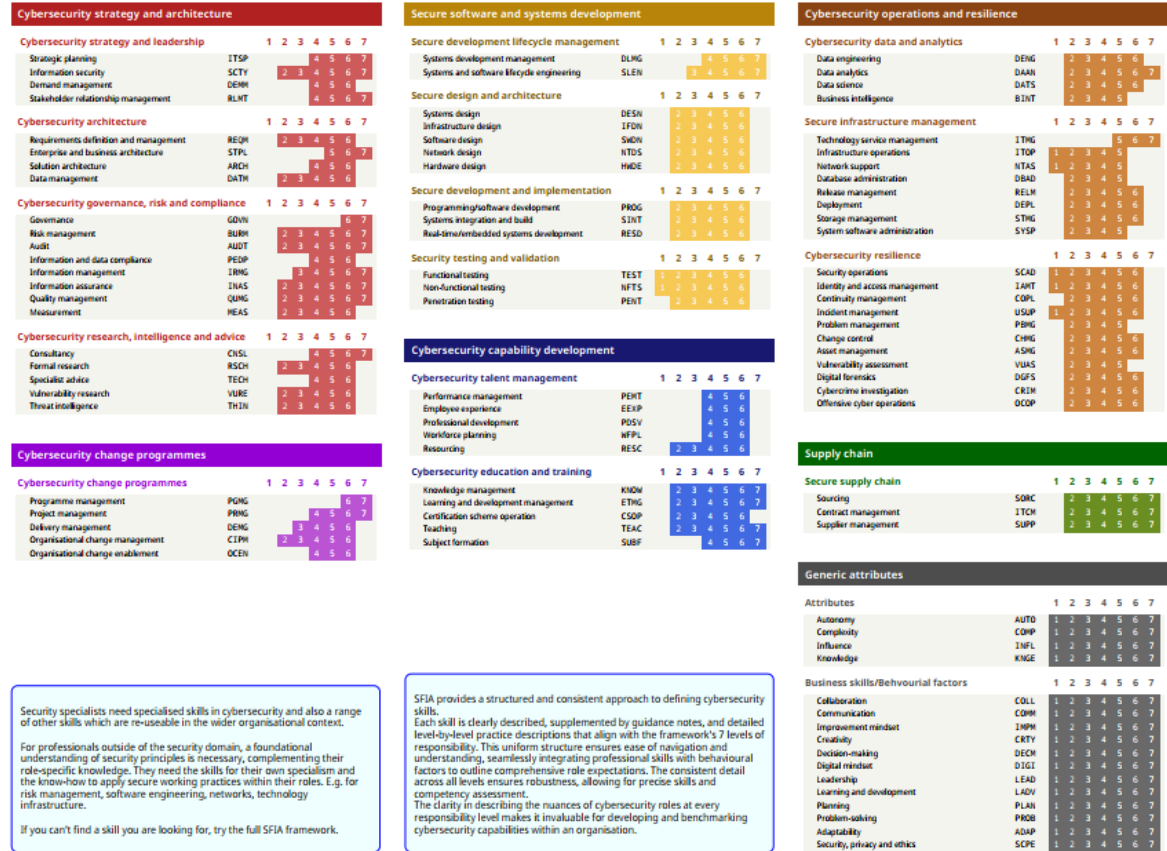


Security specialists need specialised skills in cybersecurity and also a range of other skills which are re-useable in the wider organisational context.

For **professionals outside of the security domain**, a foundational understanding of security principles is necessary, complementing their role-specific knowledge. They need the skills for their own specialism and the know-how to apply secure working practices within their roles. E.g. for risk management, software engineering, networks, technology infrastructure.

Registered members can get a [high-resolution interactive pdf version](#) of this graphic

SFIA 9 – a framework for cybersecurity skills



Security specialists need specialised skills in cybersecurity and also a range of other skills which are re-useable in the wider organisational context.

For professionals outside of the security domain, a foundational understanding of security principles is necessary, complementing their role-specific knowledge. They need the skills for their own specialism and the know-how to apply secure working practices within their roles. E.g. for risk management, software engineering, networks, technology infrastructure.

If you can't find a skill you are looking for, try the full SFIA framework.

SFIA provides a structured and consistent approach to defining cybersecurity skills. Each skill is clearly described, supplemented by guidance notes, and detailed level-by-level practice descriptions that align with the framework's 7 levels of responsibility. This uniform structure ensures ease of navigation and understanding, seamlessly integrating professional skills with behavioural factors to outline comprehensive role expectations. The consistent detail across all levels ensures robustness, allowing for precise skills and competency assessment.

The clarity in describing the nuances of cybersecurity roles at every responsibility level makes it invaluable for developing and benchmarking cybersecurity capabilities within an organisation.

SFIA Levels of responsibility	SFIA Level 1 Follow	SFIA Level 2 Assist	SFIA Level 3 Apply	SFIA Level 4 Enable	SFIA Level 5 Ensure, advise	SFIA Level 6 Initiate, influence	SFIA Level 7 Set strategy, inspire, mobilise
SFIA's attributes of Autonomy, Influence and Complexity are the key to determining level of impact, responsibility and accountability. Click the SFIA level to find the details.	Follows instructions, completes routine tasks under close supervision, and requires guidance. Learns and applies basic skills and knowledge.	Assists and supports others, works under routine supervision, and uses discretion to solve routine problems. Actively learns through training and on-the-job experiences.	Performs varied tasks, including complex and non-routine, using standard methods. Plans and manages own work, exercises discretion, and meets deadlines. Proactively enhances skills and impact in the workplace.	Performs diverse complex activities, supports and guides others, delegates tasks when appropriate, works autonomously under general direction, and contributes expertise to deliver team objectives.	Provides authoritative guidance in their field and works under broad direction. Accountable for delivering significant work outcomes, from analysis through execution to evaluation.	Influences the organisation significantly, makes high-level decisions, shapes policies, demonstrates thought leadership, fosters collaboration, and accepts accountability for strategic initiatives and outcomes.	Determines overall organisational vision and strategy, operates at the highest level, and assumes accountability for overall success.

The SFIA Foundation is the global not-for-profit organisation which owns the Skills Framework for the Information Age. SFIA is a registered trademark of the SFIA Foundation. © copyright SFIA Foundation 2024.