Government
Security
Profession

Career framework

For security professionals
in government

Welcome

We have developed a vision for the future of Government Security and are working to bring that vision to life. One of the 5 key components of that vision is "**an exciting and rewarding profession**", and this career framework is a key part in making this central component real for all of us.

An exciting and rewarding profession

Security is all about people – whether they are threat actors, those we seek to protect or those who are doing the protecting. Building the Government Security Profession is therefore one of Government Security's strategic priorities.

The Government Security Profession aim is to:

"create a world-leading and dynamic Government Security Profession which enables and inspires our security professionals, while building a diverse, inclusive and thriving Security community"

Expert

“We are constantly curious, believe deeply in learning and development and bringing the outside in. We have achieved deep, evidence-based knowledge of the state of Government Security. Our people, and their behaviours, are critical to the delivery of our vision. Investment in learning and development will build a skilled, motivated and committed workforce and enable government security professionals to develop themselves through continual professional development, secondments and shadowing to gain understanding and broaden experience.”

Diverse

“Our vision is of a diverse community of Government Security professionals who are exceptionally situationally aware, and who work with pace and urgency. Our diversity comes, in part, from our investment in people, but also because more colleagues represent the diversity of those we protect and want to work with us. Our diversity also enriches our perspectives – informing our responses.”

Outward-looking

“We need to build our expertise and understanding through strong connections across government, and with the private sector. The private sector enriches, and is enriched by, those who work in Government Security through shared learning, secondments and career progression between our two sectors.”

Currently, expertise in Government Security is in short supply and patchily spread. The Government Security Profession framework is a critical first step in beginning to address that. It offers you an opportunity to chart a career in Government Security, working across government and beyond, to develop your skills and expertise.

Security is at the cutting edge of modern organisations. Your journey starts here!

Dominic Fortescue, Director General and Government Chief Security Officer

Who is in the Government Security Profession?

The Government Security Profession is part of the Government Security Function, which seeks to build the capacity and capabilities of security professionals across government, covering Physical, Personnel, Cyber, Technical Security and Corporate Enablers. We aim to:

- Attract and recruit the best talent into the Government Security Profession
- Retain a responsive, highly skilled and motivated workforce
- Develop a clear learning offer with external accreditation and interchange with industry
- Support and align clear career pathways across the profession and wider government
- Ensure future talent pipelines including Cyber Apprenticeships and graduate schemes

The Government Security Profession brings together all security professionals working in government to help them gain the skills and knowledge they need to carry out their roles.

As part of the Government Security Profession, you have a critical role to play by helping us to protect HM Government and our citizens both at home and overseas.

The Government Security Profession career framework has been developed for government departments, the armed forces, the police service and the security services.

What are government functions?

- **The Government Security Function is 1 of 12 functions across government.** Functions work in partnerships across departments to apply a consistent approach and support better decisions, efficiencies and ensure the right capabilities are in place for departments to achieve their priorities.
- The Government Security Function is headed by the Government Chief Security Officer. Government Security is one of the newest arrivals to the functions family. We are responsible for the delivery of security services through a talented group of security professionals across government.
- **A government profession develops the capability of a group of people with particular skills and expertise across government**, on behalf of departments and the functions. An individual can belong to more than one government profession and is employed by a department or arm's length body.

What will I find in the career framework?

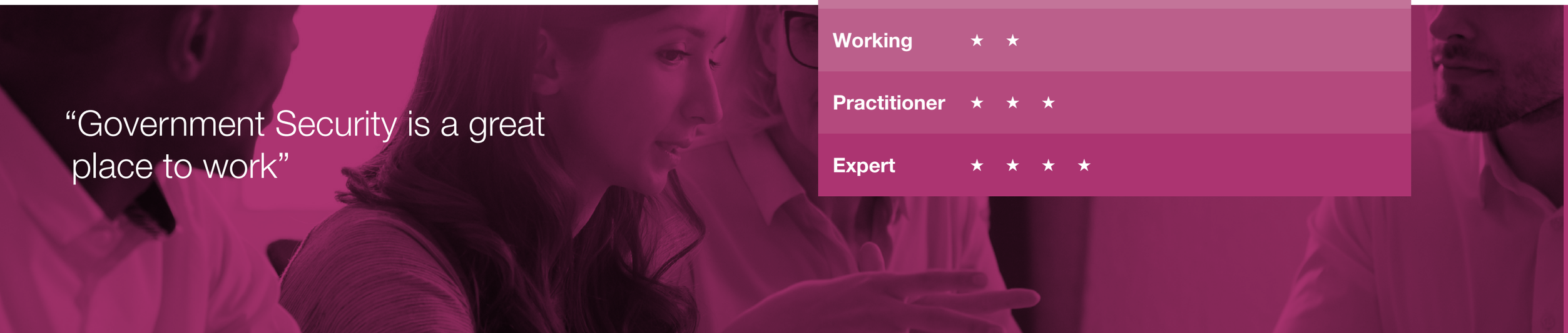
The Government Security Profession career framework defines, for all security professionals across government:

Career pathways

Role-level expectations

Skills and skill level definitions

Indicative training mapped to these skills



As this is the first career framework we have put together, training is indicative rather than recommended. Managers and employees are, however, still encouraged to use the framework to tailor the development journey and make decisions about which training to undertake. In future versions we hope to include a formal learning offer for each of the security specialisms.

How should I use the career framework?

The career framework enables you to align yourself to one of the 46 security roles. Each role lists the required expectations, skills and skill levels for the role and it is recommended that you assess yourself against these to identify areas of strength and for development.

You should have regular conversations with your line manager about possible interventions, using the indicative training where relevant, at periodic intervals throughout the performance year. We aim to complete the skills library of recommended training by 2021, and this will further support these career conversations.

It is particularly important to regularly review your career with your line manager to agree the skill level you should be progressing towards. The skill levels are:

Awareness	★
Working	★ ★
Practitioner	★ ★ ★
Expert	★ ★ ★ ★

Career Pathways

What is a career pathway?

A career pathway is a series of defined and connected roles. It often features roles at different levels. Career pathways also describe the expectations, skills and development required for each role at each level.

A career pathway enables security professionals to identify what is expected for each role at each level, and how they can progress through different levels or roles. You may use a career pathway to advance to successively higher levels. This progression can happen in the same role or a different one. Each step on a career pathway is designed to help you gain the right skills and experiences to be effective at that level, and prepare to progress to the next.

The Career Pathways align to Corporate Enablers and the 4 specialisms:

- Physical Security
- Personnel Security
- Cyber Security
- Technical Security

Who is it for?

The Government Security Profession career framework is for all government colleagues working in a security role, or anyone who wants to find out more about what is required for different security roles.

How do I access it?

It is available on GOV.UK.

When should I do this?

You should regularly review the career pathway and make sure you are familiar with it. It is particularly important to do this when you are considering a role move, when you discuss your personal development plan with your line manager and during your regular performance reviews. The Government Security Profession career framework also offers a range of development opportunities to help you progress to the next level of your role or move to a different area of expertise.

Links with other professions

The 46 roles featured in the career framework are the core roles of the Government Security Profession.

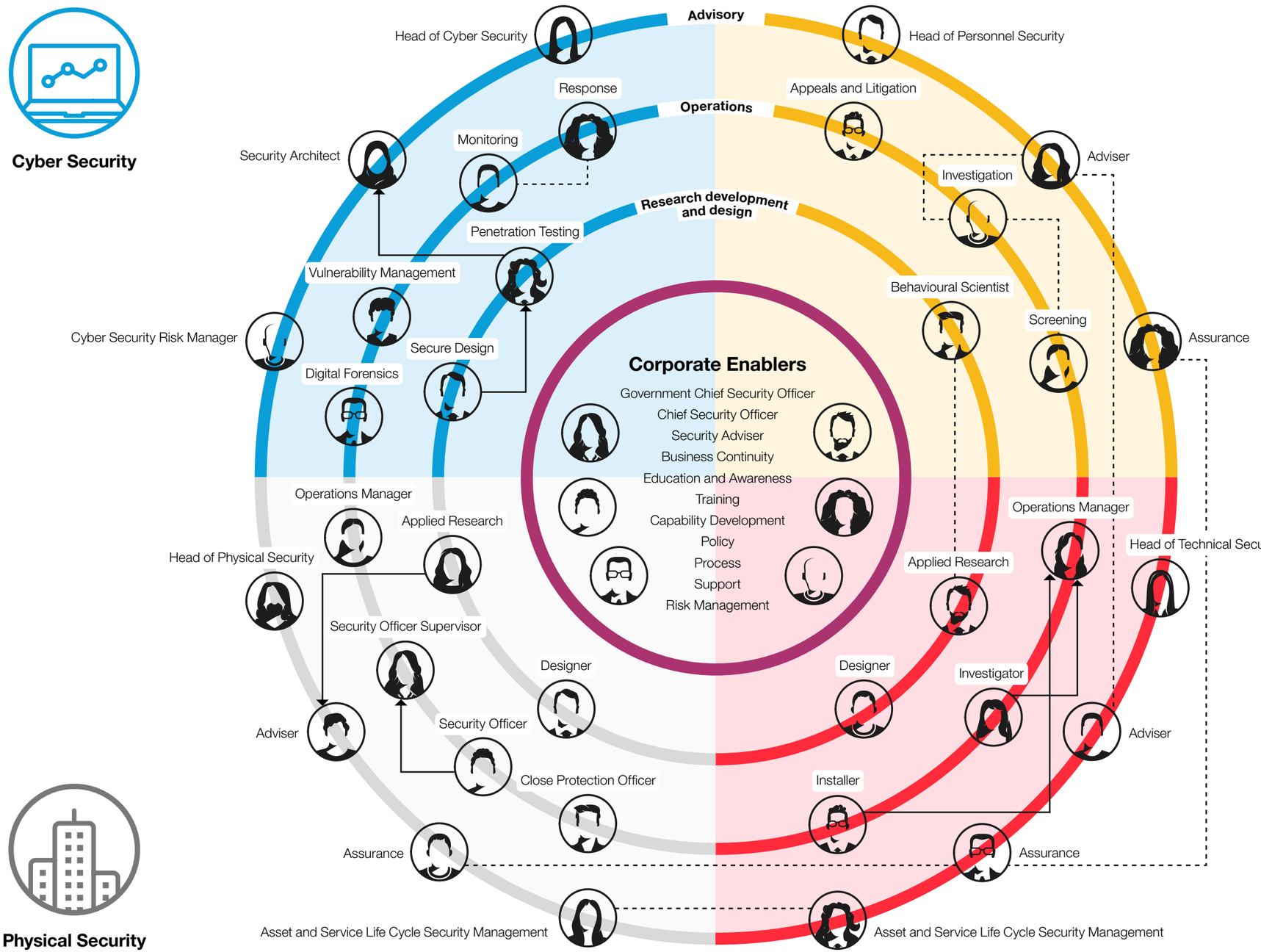
However, there are many more roles that are needed to successfully deliver projects. These roles are not included here, but you can find information on them within the frameworks of other professions, such as **Digital, Data and Technology**, **Project Delivery**, **Analysis**, **Commercial**, **Finance** and **Policy**.

Roles

Example career movement

Example career progression

This diagram illustrates examples of career pathways for security professionals. If you click on any of the 46 roles, you will be taken to a more detailed career pathway unique to the role. If you click on any of the specialisms, you will be taken to its role family menu.



Physical Security career pathways

		Indicative grades									
	Civil Service grades	AA/ Apprentice	AO	EO	EO-HEO	HEO	SEO	SEO-G7	G7-G6	SCS 1	SCS 2
	Indicative tri-service military ranks (NATO)	OR Recruit and OF Cadet	OR2-OR3	OR3-OR4	OR5-OF1	OR9-OF3	OF3	OF4	OF5	OF6	OF7
Government Security Profession career pathways	Physical Security	**Advisory**	Head of Physical Security							■	■	■
			Adviser				■	■	■	■	■	
			Assurance				■	■	■	■	■	
			Asset and Service Life Cycle Security Management	■	■	■	■	■	■			
		Operations	Operations Manager			■	■	■	■	■	■	
			Security Officer Supervisor				■	■	■	■	■	
			Close Protection Officer			■	■	■	■			
			Security Officer	■	■	■	■					
		Research, development and design	Applied Research	■	■	■	■	■	■	■	■	■
			Designer			■	■	■	■	■		

The grades listed are indicative and intended as a starting point. Depending on the job being advertised, appropriate skills should be added. Specific grades should be determined by departments using grading guidance or, if appropriate, the job evaluation grading support process.

Personnel Security career pathways

		Indicative grades									
Civil Service grades		AA/Apprentice	AO	EO	EO-HEO	HEO	SEO	SEO-G7	G7-G6	SCS 1	SCS 2
Indicative tri-service military ranks (NATO)		OR Recruit and OF Cadet	OR2-OR3	OR3-OR4	OR5-OF1	OR9-OF3	OF3	OF4	OF5	OF6	OF7
Government Security Profession career pathways											
Personnel Security											
Advisory	Head of Personnel Security								■	■	■
	Adviser				■	■	■	■	■		
	Assurance				■	■	■	■	■		
Operations	Appeals and Litigation			■	■	■	■	■	■		
	Investigation			■	■	■	■	■	■		
	Screening	■	■	■	■	■	■	■	■		
Research, development and design	Behavioural Scientist				■	■	■	■	■		

The grades listed are indicative and intended as a starting point. Depending on the job being advertised, appropriate skills should be added. Specific grades should be determined by departments using Grading Guidance or if appropriate job evaluation grading support process.

Cyber Security career pathways

		Indicative grades									
	Civil Service grades	AA/Apprentice	AO	EO	EO-HEO	HEO	SEO	SEO-G7	G7-G6	SCS 1	SCS 2
	Indicative tri-service military ranks (NATO)	OR Recruit and OF Cadet	OR2-OR3	OR3-OR4	OR5-OF1	OR9-OF3	OF3	OF4	OF5	OF6	OF7
Government Security Profession career pathways	Cyber Security	Advisory	Head of Cyber Security							■	■	■
			Security Architect					■	■	■		
			Risk Manager				■	■	■	■		
		Operations	Monitoring			■	■	■	■	■		
			Response			■	■	■	■	■		
			Vulnerability Management			■	■	■	■	■		
			Digital Forensics			■	■	■	■	■		
		Research, development and design	Penetration testing				■	■	■	■		
			Secure Design				■	■	■			

The grades listed are indicative and intended as a starting point. Depending on the job being advertised, appropriate skills should be added. Specific grades should be determined by departments using grading guidance or, if appropriate, job evaluation grading support process.

Technical Security career pathways

		Indicative grades							
	Civil service grades	AA/Apprentice	AO	EO	EO-HEO	HEO	SEO	SEO-G7	G7-G6
	Indicative tri-service military ranks (NATO)	OR Recruit and OF Cadet	OR2-OR3	OR3-OR4	OR5-OF1	OR9-OF3	OF3	OF4	OF5
Government Security Profession career pathways	Technical Security	Advisory	Head of Technical Security						■	■
			Adviser			■	■	■	■	■
			Assurance			■	■	■	■	■
			Asset and Service Life Cycle Security Management	■	■	■	■	■	■	■	■
		Operations	Operations Manager			■	■	■	■	■	■
			Investigator		■	■	■	■			
			Installer	■	■	■	■	■	■	■	
		Research, development and design	Applied Research	■	■	■	■	■	■	■	■
			Designer				■	■	■	■	

The grades listed are indicative and intended as a starting point. Depending on the job being advertised, appropriate skills should be added. Specific grades should be determined by departments using Grading Guidance or if appropriate job evaluation grading support process.

Corporate Enablers career pathways

		Indicative grades										
	Civil service grades	AA/Apprentice	AO	EO	EO-HEO	HEO	SEO	SEO-G7	G7-G6	SCS 1	SCS 2	SCS 3
	Indicative tri-service military ranks (NATO)	OR Recruit and OF Cadet	OR2-OR3	OR3-OR4	OR5-OF1	OR9-OF3	OF3	OF4	OF5	OF6	OF7	OF8
Government Security Profession career pathways	Government Chief Security Officer											■
	Chief Security Officer										■	
	Security Adviser							■	■	■		
Corporate Enablers	Policy	■	■	■	■	■	■	■	■	■		
	Risk Management				■	■	■	■	■			
	Capability Development				■	■	■	■	■			
	Training	■	■	■	■	■	■	■	■			
	Education and Awareness	■	■	■	■	■	■	■	■			
	Business Continuity	■	■	■	■	■	■	■				
	Process	■	■	■	■	■	■	■				
	Support	■	■									

The grades listed are indicative and intended as a starting point. Depending on the job being advertised, appropriate skills should be added. Specific grades should be determined by departments using grading guidance or, if appropriate, job evaluation grading support process.

Career profiles

Deborah Smith-Dunlop

Head of Vetting Appeals and Litigation

Cluster 2

Mahbubul Islam

Deputy Chief Information Security Officer

HMCTS

Tom Meadows

Head of Technical Services Security Services Group

MoD

Robert Boscot

Business Continuity Policy Lead

DExEU

Charlotte Roe

Cyber Security Apprentice

NHS Digital

Deborah Smith-Dunlop

I came into security from an HR background. I was drawn into Personnel Security because I like learning about people, their behaviours and motivations – and I felt my HR skills would be transferable.

My government career has been varied. I started as a summer temp in an investigation team while I decided what I wanted to do. I went on to work in VAT which was a good grounding in analytics and how people behave.

From a corporate role within HM Revenues and Customs (HMRC) I took a secondment to the National Criminal Intelligence Service where I began my HR career. I was fortunate to be on various teams designing corporate services functions for Serious Organised Crime Agency (SOCA) and then the National Crime Agency (NCA).

Security experience

My experiences led me to become Head of Personnel Security in the NCA, delivering services across government, including the police and agencies.

I was then lucky to get an opportunity to move to the Government Security Profession unit where I brought my passion, experience and skills together as part of the early work to design this career framework.

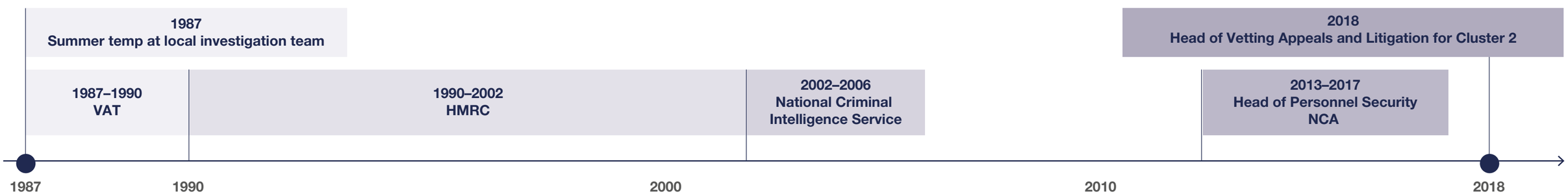
Today, I am Head of Vetting appeals and litigation in Cluster 2 which continues to test my subject matter expertise.

Career highlights

I am really proud of the work I did as Head of Personnel Security in the NCA to better assess vulnerability and move away from being far too risk averse. It was great to work more closely and openly with HR, occupational health, professional standards on specific people issues and to collectively look for ways of managing risk.

And finally, I am honoured to have refreshed the level 4 Cyber Security apprenticeship scheme and doubling the number of women entering the scheme. We are really lucky to have these talented people and I hope we can get more schemes across all of our specialisms.

> "As Head of Personnel Security in the NCA I delivered services we now have in clusters, and across government, including the police and agencies."



Mahbubul Islam

My Civil Service journey started in 2001 in an operational capacity, a part-time role that was flexible to allow me to complete my undergraduate degree in Computing and Business Information Technology.

Security experience

My first role in security was as a Special Projects Business Analyst on the National Identity Cards Programme. After this, I went on to become a Trainee Information Assurance Specialist. I started with zero knowledge of security, but rapidly upskilled through the training programme and soon was delivering practical security delivery outcomes. My trainee colleagues and I were able to create a programme built on knowledge, experience and exposure to cover as many functional security areas as possible in 2 years. My functional security roles have been both in the Physical and Cyber Security specialisms.

It was at HM Passport Office that I was able to work on cross-government security projects with Foreign and Commonwealth Office (FCO), Home Office, Government Digital Service (GDS), Driving and Vehicle Licensing Agency (DVLA), Crown Dependency and British Overseas Territories and others. I often found myself switching functional security roles from assurance to delivery and vice versa based on the engagements.

I then became the Head of the Government Transformational Security at GDS, which oversees and supports all of its security aspects.

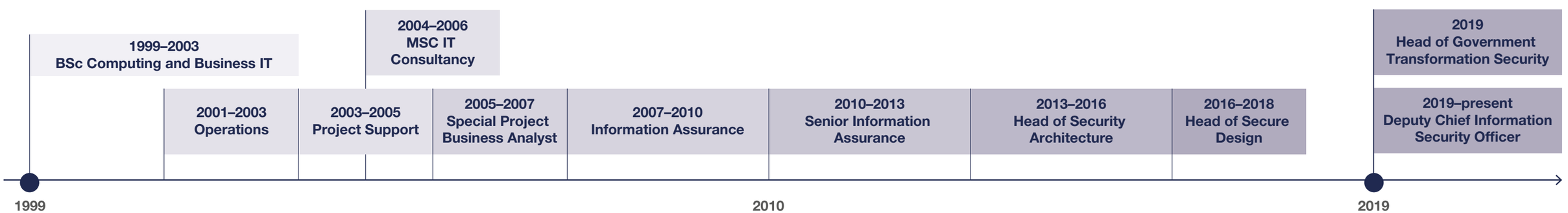
I have now been promoted to Deputy Director/Deputy Chief Information Security Officer, doing 1st Line and 2nd Line Security for HM Courts and Tribunal Services (HMCTS); I also ensure the department is aligned to transformational security strategy from Cabinet Office, Ministry of Justice and National Cyber Security Centre (NCSC).

Career highlights

Firstly, achieving the Chartered Security Professional qualification through my experience of working on 2 major IT programmes (National Identity Cards and Universal Credit).

A close second was working on supply chain security management for the Next Generation Passport Programme and being able learn new dimensions of security, namely Secure Print.

> “I was provided a safe environment by management to develop, and found myself well supported by experienced security mentors. This all helped me become a well-rounded security practitioner.”



Tom Meadows

I joined the Security Services Group (SSG) as an apprentice in August 1974 and have never looked back. Over the last 45 years I have had a varied career holding most roles in the SSG covering manufacture, installation and maintenance of security systems. This has included such roles as: systems adviser, commercial officer, and designer of HMG's in-house high security AC12M intruder alarm system. I have served as a consultant on integrated security systems from intrusion detection systems, perimeter intrusion detection systems, CCTV, automatic access control systems, and Physical Security measures. I led the Protective Security Advisory Team (PSAT), SSG assurance and compliance team and continue as SSG Group Security Adviser.

Security experience

In December 2016, I was appointed to the role of Head of SSG Technical Services, where I still lead specialist teams in SSG delivering high security advice, professional support including quality and compliance services to the customers across HM Government departments, the Ministry of Defence (MOD) estate, and critical national infrastructure.

I'm also responsible for SSG's research and development, technical support and training, production and for SSG security furniture services.

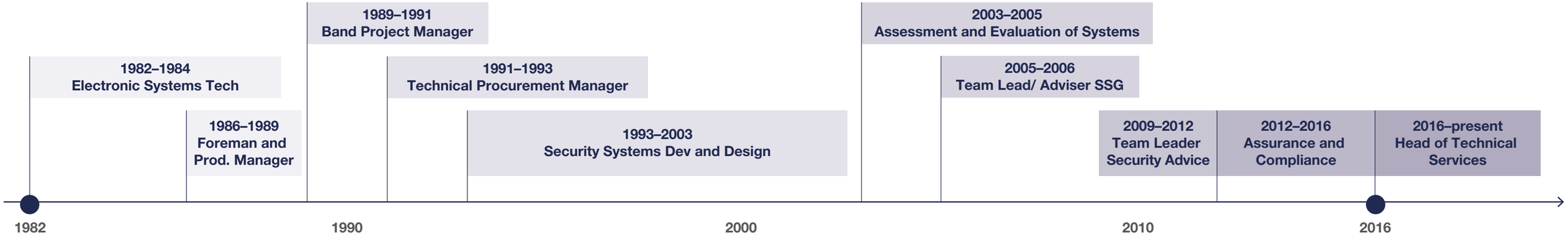
Career highlights

I've been lucky to travel countless miles across the globe; including Cyprus, Kathmandu, Belize and the Falklands. By aeroplanes, trains and automobiles – not to forget the odd helicopter ride and a submarine!

My fondest memories are a flight around Everest and on another occasion, being flown to a facility on a coral island, after doing the survey and awaiting the return flight, swimming on a coral reef, walking around the island 6 inches above an aquamarine sea, white sand with palm trees and huts on stilts – and I really did buy the T-shirt.

So, 45 years and counting – how fast they have passed. I'd do it all again given the chance.

"So far it's been an eclectic, challenging and at times both exciting and scary career, one that I hadn't planned, but as the opportunities arose I've embraced them and been rewarded both with promotion, life experience and memories of times shared with equally minded colleagues."



Robert Boscot

I left school at 16 and, like my father, went to work on a dairy farm where I stayed for 9 years. Then I accompanied a friend to night school on a university course, an event that changed my life. I was soon accepted as a mature student completing a Humanities degree.

In 1993 I joined the Civil Service, spending 7 years in Customs and Excise (VAT and drugs policy), 3 years in Prison Service (drugs and security policy), 12 years in the Home Office (counter terrorism and protective security) and 3 years in the Department for Transport (emergency response and business continuity). Although it took me a bit of time to find my business continuity niche, thinking about the "what if" elements of protective security was always central.

My time on the farm taught me that unless I was prepared for any eventuality then I wasn't going to get very far. This and the desire to want to make a difference is something which I brought with me and it became more pronounced when I became disabled after a fall. It is only right that the Civil Service is an amalgam of the people we serve and I am immensely proud to be a Co-chair of the enAble network in Department for Exiting the European Union (DExEU).

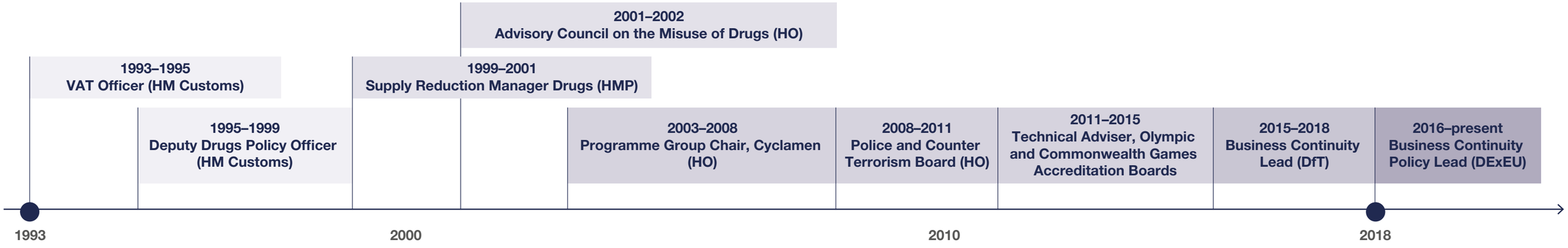
Career highlights

For the past year I have been the Business Continuity Policy Lead in DExEU. I love being part of big projects and have worked on the Olympic Games, Commonwealth Games, the Children of Problem Drug Users report, briefing for approximately 100 Cabinet Office Briefing Room (COBR) meetings and Programme Cyclamen.

Highlights

Working on the 2012 Olympic Games. I worked on accrediting athletes and games family members. It was a special time and showed the value of having a really simple common goal: "make it happen". People suddenly all became part of a massive team pulling in the same way.

"Name me another profession which would give you this variety. Moving around keeps you fresh and helps you develop new skills and you will always enrich what is already there."



Charlotte Roe

After attending a CyberFirst career fair, I got to see the opportunities available and applied for a Cyber Security apprentice. I was really excited when I left college and entered into an unknown world as a Cyber Security apprentice. Two years on I have experience in operating in multiple teams, building up my knowledge and most importantly meeting a lot of great new faces.

Security experience

Since completing my 2 year Cyber Security apprenticeship in 2019, I was given the opportunity to transition into a security operations role within NHS Digital. I was introduced into a fascinating world of networking and Security Information and Event Management (SIEM), and even got to grips with learning the cyber language (there are quite a few acronyms). I think of how far I have come since some of the "silly" questions I would ask – but we do all have to start from somewhere!

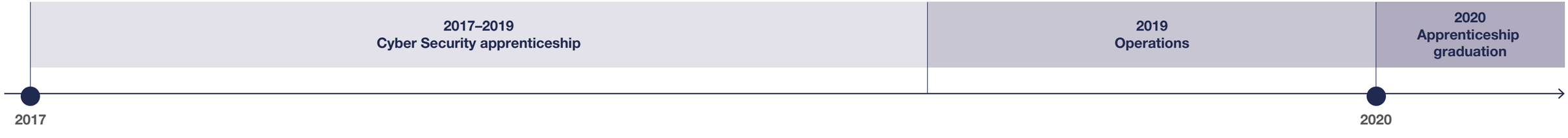
Career highlights

A great aspect about working in Government Security is I have had the opportunity to travel around the UK, attend many networking and social events. But, ultimately the best thing is I sometimes reflect back at what I have done and my achievements, and think "wow, look at me, helping the NHS".

Cyber Security had never been a career I had thought of entering, but I have developed a sense of place and personal development. I have also had the opportunity to explore myself and set goals. I aim to gain more qualifications such as System Security Certified Professional and continue to pursue a future career within security.

Last thing I would say is, Cyber Security is a brilliant field to work in and if you can hack it, no pun intended, then you will be amazed at what you can do.

"Cyber Security had never been a career I had thought of entering, but I have developed a sense of place and personal development."



Physical Security – role families and roles

Physical Security protects assets, including people, services, infrastructure, systems, places, equipment and networks. Effective Physical Security is achieved by multi-layering different measures – commonly referred to as ‘defence in depth’. The concept is based on the principle that the security of an asset is not significantly reduced with the loss of any single layer.

Advisory


Head of Physical Security


Adviser


Assurance


Asset and Service Life Cycle Security Management

Operations


Operations Manager


Security Officer Supervisor


Security Officer


Close Protection Officer

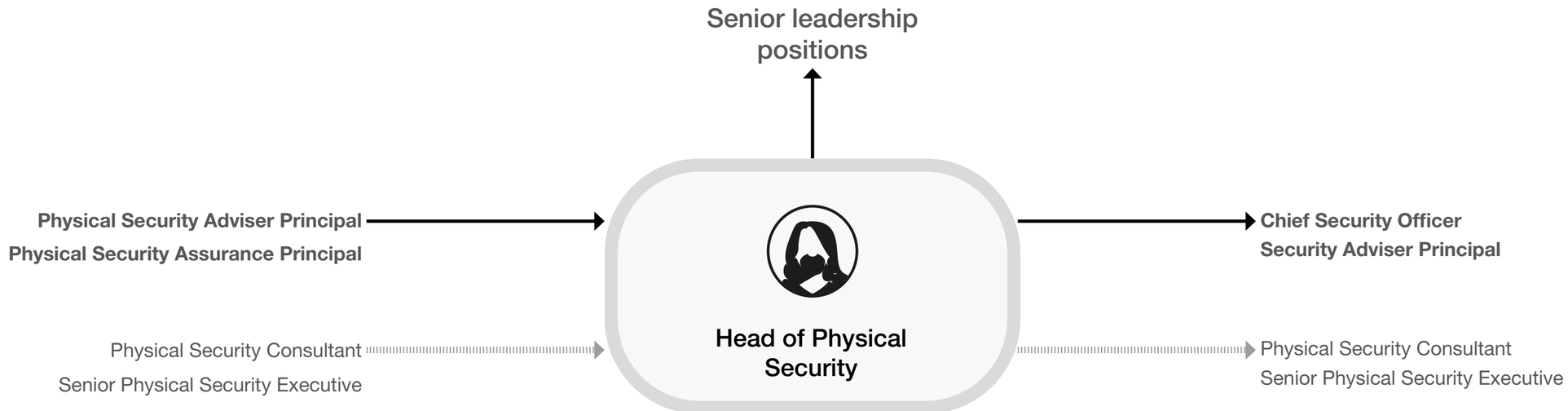
Research, development and design


Applied Research


Designer

Role	Role family	Security specialism
Head of Physical Security	Advisory	Physical Security

Suggested entry and exit roles are indicative only and non-exhaustive



Role	Role family	Security specialism
Head of Physical Security	Advisory	Physical Security

Role summary

The Head of Physical Security is responsible for the Physical Security specialism, anticipating challenges, providing strategic direction, driving performance and building the capability required to ensure the security of new and existing services.

Typical role level expectations

- Be the primary point of contact on Physical Security issues with key stakeholders, including external parties, and actively develop strong working relationships in relation to Physical Security
- Ensure that the Physical Security policies and security controls employed remain appropriate and proportionate to the assessed risks, and are responsive and adaptable to the changing threat environment, business requirements and central government policies
- Champion learning, development and accreditation, cultivate talent and foster an inclusive, diverse and motivated workforce
- Work with the heads of specialism to promote cross-government security mindedness
- Influence, change and impact decisions with both internal and external stakeholders
- Promote the Government Physical Security Profession and advise on Physical Security risks
- Work with industry, including security manufacturers and security consultants, to drive best practice
- Drive professional development by working with Government Security Function to set and drive continuous learning standards

Entry route

Internal

Suitable for an individual from the Government Security Profession

External

Suitable for an individual from a senior management position in the private sector

Role	Role family	Security specialism
Head of Physical Security	Advisory	Physical Security

Minimum skill expectations

Skill	Skill level	Training	Success profiles
Applied Physical Security	Expert	**Repository**	Leadership*
Risk understanding and mitigation	Working	**Repository**	Communicating and influencing
Protective security	Awareness	**Repository**	Developing self and others
Threat understanding	Awareness	**Repository**	Seeing the big picture
			Working together

*Principal behaviour

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

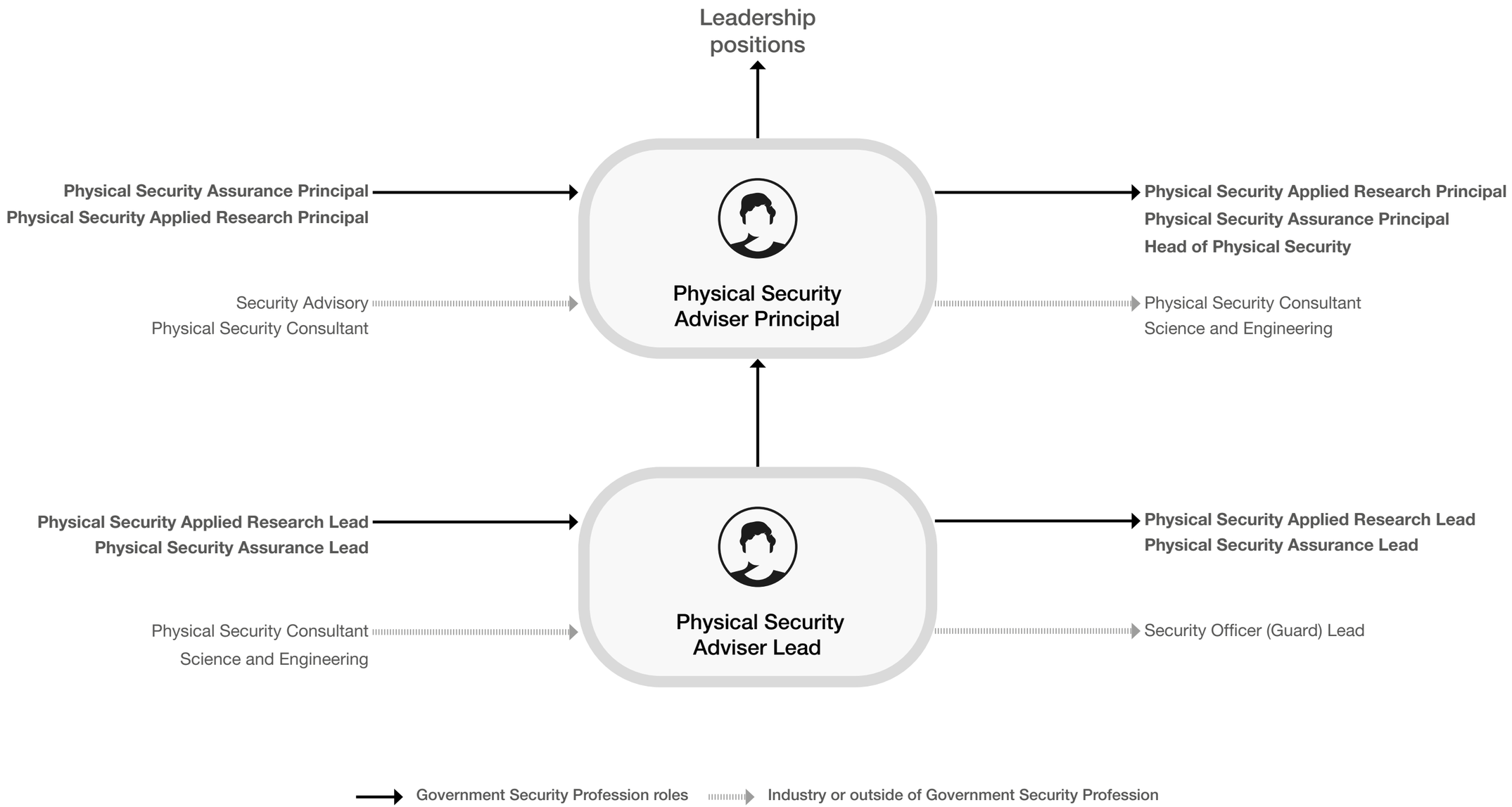
Development

Suggested training	Indicative professional qualifications/accreditations
• Physical Security leadership course • Risk management and information risk management course • Threat to government and industry training	• Membership of a relevant institution or body • Relevant industry or government qualifications or accreditations

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC

Role	Role family	Security specialism
Physical Security Adviser	Advisory	Physical Security

Suggested entry and exit roles are indicative only and non-exhaustive



Role	Role family	Security specialism
Physical Security Adviser Lead	Advisory	Physical Security

Role summary

The role of a Physical Security Adviser is to provide Physical Security advice to identify and mitigate security risks in line with business needs. This role includes the overseas security adviser cadre.

Typical role level expectations

- Provide expert advice on Physical Security to the Government Security Profession and wider public and/or private sector
- Conduct risk assessments in the local environment, extracting insights to provide an informed opinion on Physical Security risks and the adequacy of controls in place
- Align with relevant regulation, policy and standards to provide proportional, practical advice, tailored to the local environment, and advise on any residual risk
- Monitor the efficiency and effectiveness of the Physical Security processes across the organisation, and make recommendations for continual improvement
- Maintain awareness of current and emerging technologies and their impact on existing security practices

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. Science and Engineering Profession)

External

Suitable for an individual who has worked as a Physical Security consultant in industry

Role	Role family	Security specialism
Physical Security Adviser Principal	Advisory	Physical Security

Role summary

The role of a Physical Security Adviser is to provide Physical Security advice to identify and mitigate security risks in line with business needs. This role includes the overseas security adviser cadre.

Typical role level expectations

- Provide expert advice on Physical Security to the Government Security Profession and wider public and/or private sector
- Manage and commission risk assessments in the local environment, extracting insights to provide an informed opinion on Physical Security risks and the adequacy of controls in place
- Create organisational vision for aligning with regulation, policy and standards to provide proportional, practical advice, tailored to the local environment, and advise on any residual risk
- Create and monitor standards regarding efficiency and effectiveness of the Physical Security processes across the organisation, and make recommendations for continual improvement
- Maintain awareness of current and emerging technologies and their impact on existing security practices

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession

External

Suitable for an individual who has worked as a Physical Security consultant in industry

Role	Role family	Security specialism
Physical Security Adviser	Advisory	Physical Security

Minimum skill expectations

Skill	Skill level	Training	Success profiles
Applied Physical Security	Practitioner	**Repository**	Communicating and influencing*
Risk understanding and mitigation	Practitioner	**Repository**	Changing and improving
Protective security	Working	**Repository**	Delivering at pace
Threat understanding	Working	**Repository**	Making effective decisions
Legal and regulatory environment and compliance	Working	**Repository**	Managing a quality service

*Principal behaviour

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Development

Suggested training	Indicative professional qualifications/accreditations
• Risk management leadership course • Security management course • Threat awareness course • Security framework course • Security strategy course	• Membership of a relevant institution or body, e.g. Register of Security Engineers and Specialists, American Society for Industrial Security, The Security Institute • Relevant government-recognised qualifications and accreditations • Relevant industry qualifications and accreditations e.g. PMI Risk Management Professional, Physical Security Professional

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC

Role	Role family	Security specialism
Physical Security Adviser	Advisory	Physical Security

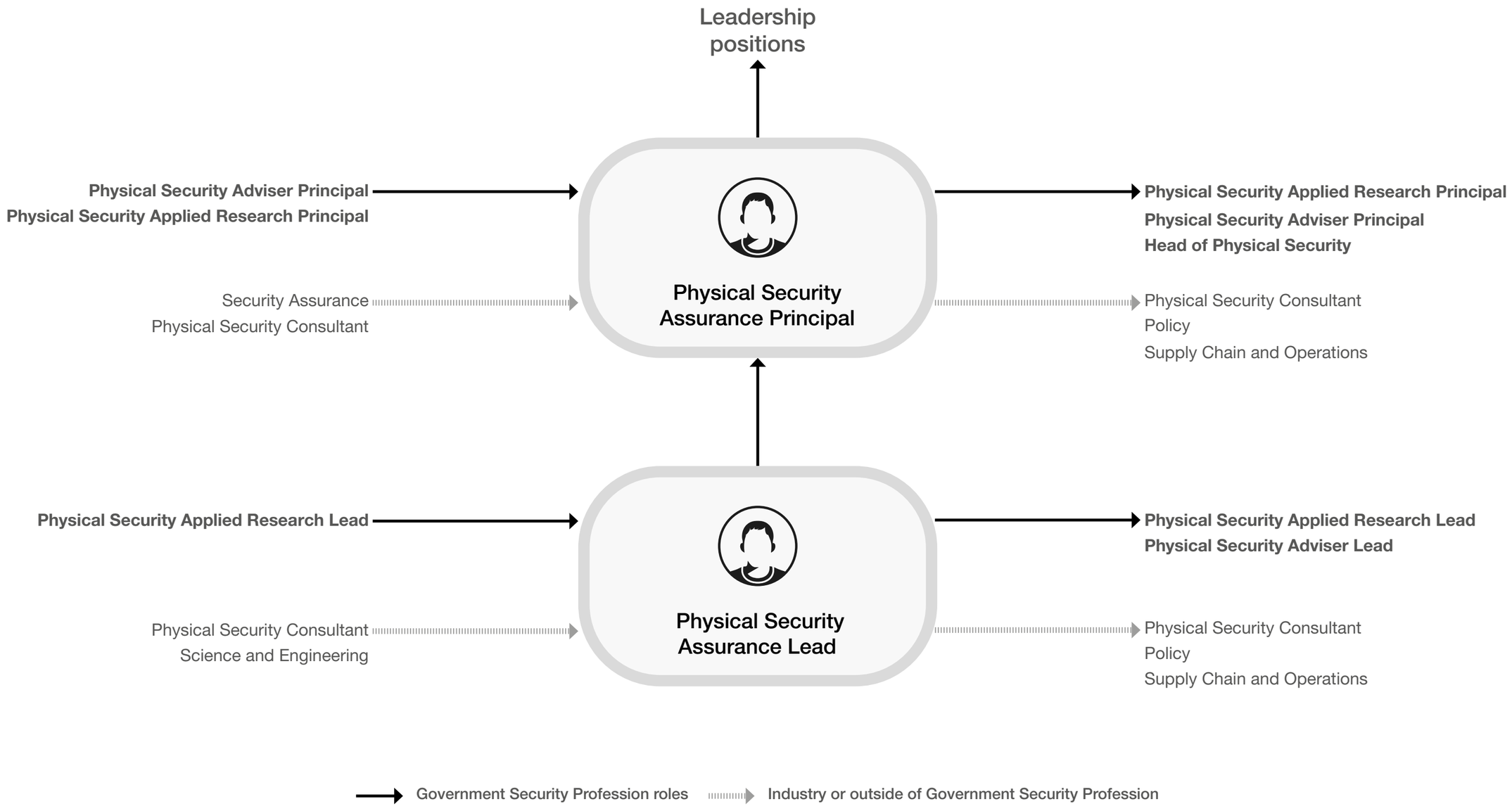
Minimum skill expectations

Skill	Role level	
	Adviser Lead	Adviser Principal
	Skill level	
Applied Physical Security	Practitioner	Expert
Risk understanding and mitigation	Practitioner	Expert
Protective security	Working	Practitioner
Threat understanding	Working	Practitioner
Legal and regulatory environment and compliance	Working	Working

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Role	Role family	Security specialism
Physical Security Assurance	Advisory	Physical Security

Suggested entry and exit roles are indicative only and non-exhaustive



Role	Role family	Security specialism
Physical Security Assurance Lead	Advisory	Physical Security

Role summary

The role of Physical Security assurance is to identify Physical Security risks and highlight non-compliance and vulnerabilities to enable others to manage residual risk.

Typical role level expectations

- Deliver Physical Security assurance processes, including providing audit information to risk owners
- Assess, record, and monitor the introduction, maintenance, through-life performance, and removal of physical infrastructure and systems
- Monitor and report on the delivery of Physical Security services against requirements, with the use of key performance indicators
- Ensure alignment with government and industry objectives and standards, proactively reviewing and assuring security risk and highlighting non-conformance

Entry route

Internal

Suitable for an individual from the Government Security Profession

External

Suitable for an individual who has worked within Physical Security in industry

Role	Role family	Security specialism
Physical Security Assurance Principal	Advisory	Physical Security

Role summary

The role of Physical Security assurance is to identify Physical Security risks and highlight non-compliance and vulnerabilities to enable others to manage residual risk.

Typical role level expectations

- Manage delivery and life cycle of Physical Security assurance processes, including sharing audit information to senior leadership, and setting assurance standards across government
- Manage the assessment, recording, and monitoring of the introduction, maintenance, through-life performance, and removal of physical infrastructure and systems
- Review reporting, including key performance indicators, and act as key decision maker for the delivery of Physical Security services against requirements
- Ensure alignment with government and/or industry objectives and standards, and liaise with senior stakeholders on how these objectives and standards can be met

Entry route

Internal

Suitable for an individual from the Government Security Profession

External

Suitable for an individual who has worked within Physical Security in industry

Role	Role family	Security specialism
Physical Security Assurance	Advisory	Physical Security

Minimum skill expectations

Skill	Skill level	Training	Success profiles
Applied Physical Security	Practitioner	**Repository**	Communicating and influencing*
Legal and regulatory environment and compliance	Practitioner	**Repository**	Changing and improving
Risk understanding and mitigation	Practitioner	**Repository**	Making effective decisions
Protective security	Awareness	**Repository**	Managing a quality service
Threat understanding	Awareness	**Repository**	Seeing the big picture

*Principal behaviour

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Development

Suggested training	Indicative professional qualifications/accreditations
• Regulatory, compliance or legislative course • Threat awareness course • Risk management leadership course	• Membership of a relevant institution or body, e.g. American Society for Industrial Security, Register of Security Engineers and Specialists • Relevant industry qualifications and accreditations, e.g. ISO27001 Lead Auditor, Physical Security Professional, Certified Information Systems Auditor • Relevant government qualifications and accreditations

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC

Role	Role family	Security specialism
Physical Security Assurance	Advisory	Physical Security

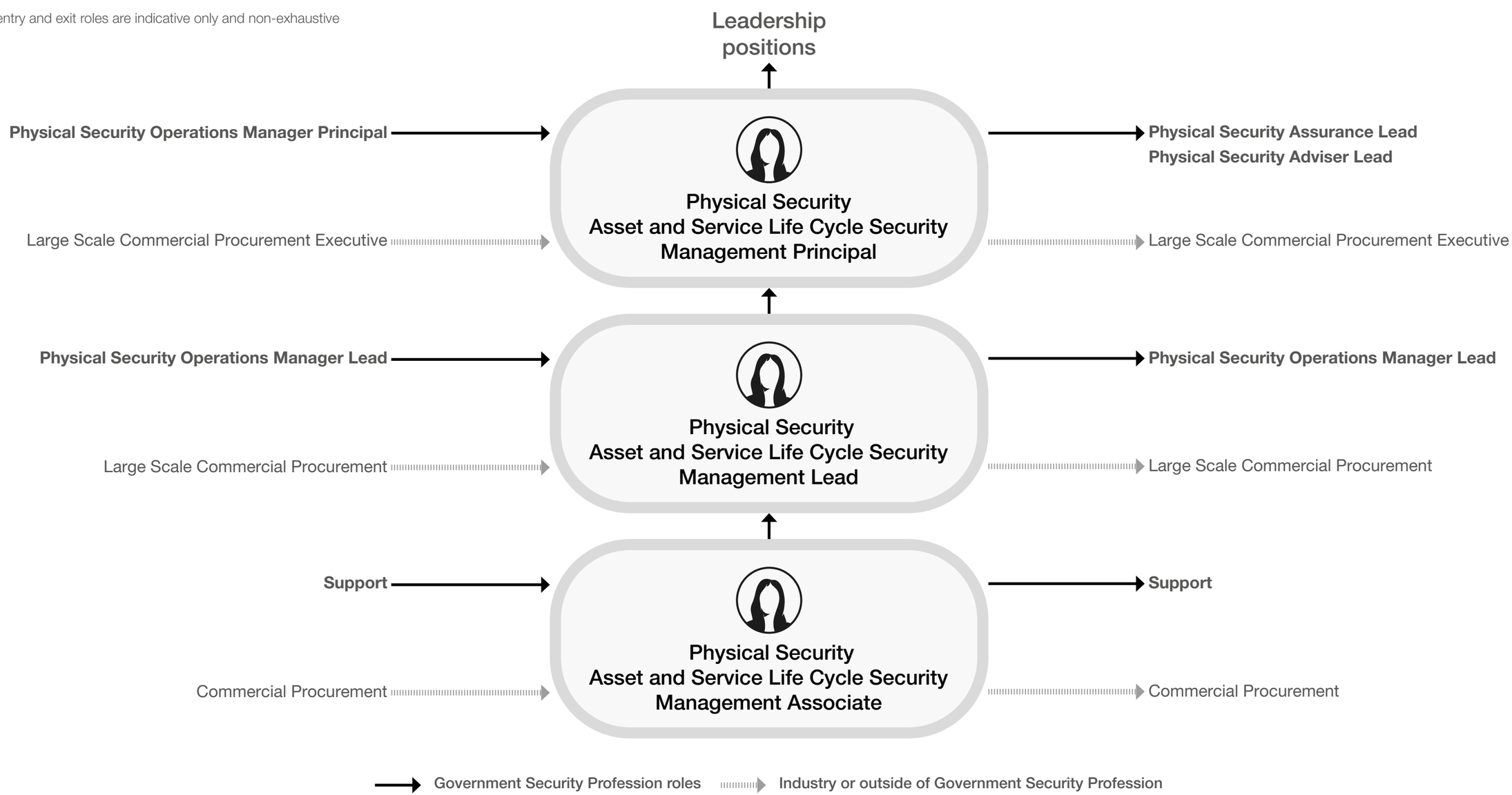
Minimum skill expectations

Skill	Role level	
	Assurance Lead	Assurance Principal
	Skill level	
Applied Physical Security	Practitioner	Expert
Legal and regulatory environment and compliance	Practitioner	Expert
Risk understanding and mitigation	Practitioner	Expert
Protective security	Awareness	Working
Threat understanding	Awareness	Working

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Role	Role family	Security specialism
Physical Security Asset and Service Life Cycle Security Management	Advisory	Physical Security

Suggested entry and exit roles are indicative only and non-exhaustive



Role	Role family	Security specialism
Physical Security Asset and Service Life Cycle Security Management Associate	Advisory	Physical Security

Role summary

The role of Physical Security Asset and Service Life Cycle Security Management is to oversee and provide advice throughout the procurement cycle, minimising the security risks associated with the procurement of assets or services, from concept to disposal.

Typical role level expectations

- Support identification and management of assets developed, processed or shared with suppliers, including with domestic and international partners
- Support supplier compliance with all relevant security legislation and regulatory requirements
- Support governance structures to manage all security risks from conception to disposal of assets
- Support with the implementation of secure logistics of assets in development, transportation and at rest

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. Commercial Function Profession or Procurement Profession)

External

Suitable for an individual who has worked in contract management

Role	Role family	Security specialism
Physical Security Asset and Service Life Cycle Security Management Lead	Advisory	Physical Security

Role summary

The role of Physical Security Asset and Service Life Cycle Security Management is to oversee and provide advice throughout the procurement cycle, minimising the security risks associated with the procurement of assets or services, from concept to disposal.

Typical role level expectations

- Identify and manage the assets developed, processed or shared with suppliers, including with domestic and international partners
- Ensure acquisitions/service programmes and suppliers comply with all relevant security legislation and regulatory requirements
- Implement governance structures to manage all security risks from conception to disposal of assets
- Act on intelligence indicating any risk to the supply chain, including providing advice and assurance on supplier's security across acquisitions and services, and encourage continuous improvement
- Develop and maintain effective stakeholder relationships with both internal and external stakeholders in order to influence and change security decisions and manage the delivery of the required security assets

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. Commercial Function Profession or Procurement Profession)

External

Suitable for an individual who has worked in contract management

Role	Role family	Security specialism
Physical Security Asset and Service Life Cycle Security Management Principal	Advisory	Physical Security

Role summary

The role of Physical Security Asset and Service Life Cycle Security Management is to oversee and provide advice throughout the procurement cycle, minimising the security risks associated with the procurement of assets or services, from concept to disposal.

Typical role level expectations

- Oversee life cycle standards for assets developed for the organisation, processed or shared with suppliers, including with domestic and international partners
- Create and manage standards for acquisitions/service programmes and ensure suppliers comply with all relevant security legislation and regulatory requirements
- Oversee the implementation of governance structures to manage all security risks from conception to disposal of assets
- Aggregate and prioritise intelligence indicating any risk to the supply chain, including providing advice and assurance on supplier's security across acquisitions and services, and encourage continuous improvement
- Develop and maintain effective stakeholder relationships with both internal and external stakeholders in order to influence and change security decisions and manage the delivery of the required security assets

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. Commercial Function Profession or Procurement Profession)

External

Suitable for an individual who has worked in contract management

Role	Role family	Security specialism
Physical Security Asset and Service Life Cycle Security Management	Advisory	Physical Security

Minimum skill expectations

Skill	Skill level	Training	Success profiles
Applied Physical Security	Working	**Repository**	Communicating and influencing*
Risk understanding and mitigation	Working	**Repository**	Making effective decisions
Secure supply chain management	Working	**Repository**	Managing a quality service
Legal and regulatory environment and compliance	Awareness	**Repository**	Seeing the big picture
Protective security	Awareness	**Repository**	Working together
Threat understanding	Awareness	**Repository**	

*Principal behaviour

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Development

Suggested training	Indicative professional qualifications/accreditations
• Risk management course • Secure procurement and supply chain management course • Threat awareness course • Regulatory, compliance or legislative course	• Membership of a relevant institution or body, e.g. Register of Security Engineers and Specialists • Relevant industry qualifications and accreditations • Relevant government qualifications and accreditations, e.g. from UK National Authority for Counter Eavesdropping Academy or Centre for the Protection of National Infrastructure

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC

Role	Role family	Security specialism
Physical Security Asset and Service Life Cycle Security Management	Advisory	Physical Security

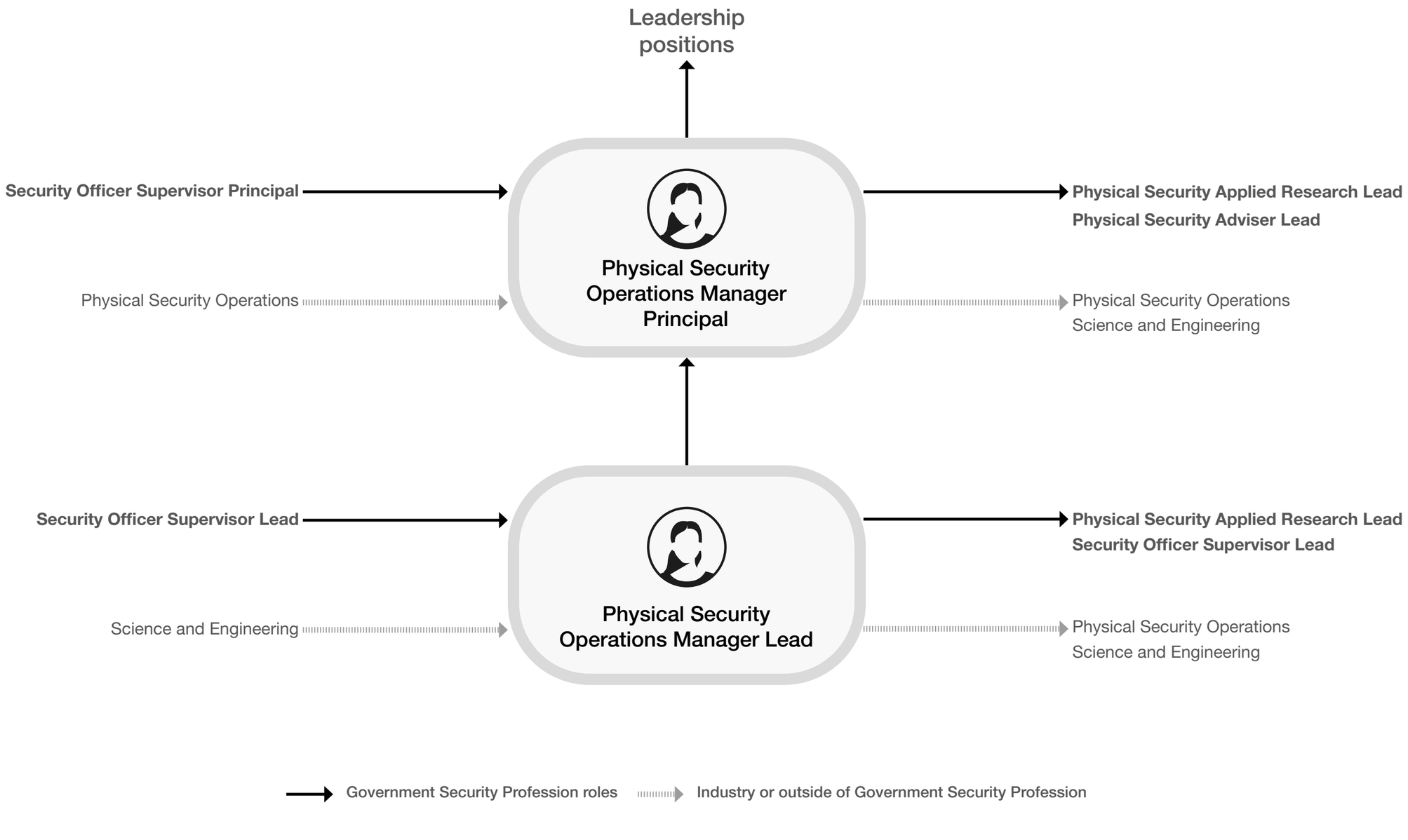
Minimum skill expectations

Skill	Role level		
	Asset and Service Life Cycle Security Management Associate	Asset and Service Life Cycle Security Management Lead	Asset and Service Life Cycle Security Management Principal
	Asset and Service Life Cycle Security Management Lead		
Applied Physical Security	Working	Practitioner	Expert
Risk understanding and mitigation	Working	Practitioner	Expert
Secure supply chain management	Working	Practitioner	Expert
Legal and regulatory environment and compliance	Awareness	Working	Practitioner
Protective security	Awareness	Working	Working
Threat understanding	Awareness	Working	Working

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Role	Role family	Security specialism
Physical Security Operations Manager	Operations	Physical Security

Suggested entry and exit roles are indicative only and non-exhaustive



Role	Role family	Security specialism
Physical Security Operations Manager Lead	Operations	Physical Security

Role summary

The role of a Physical Security Operations Manager is to ensure the correct posture of physical and tactical resources to manage sites and maintain operational preparedness for security incidents. This role includes the overseas/regional overseas security manager cadre.

Typical role level expectations

- Maintain Physical Security operations and governance structures to manage risk and deploy Physical Security effectively to protect assets and people throughout the estate
- Plan, test and respond to security/emergency incidents or concerns, including those raised by third parties, to include preparing briefs on security issues for internal and external stakeholders
- Comply with relevant regulation and legislation
- Manage resources, including people, and expenditure while promoting a positive and inclusive working environment

Entry route

Internal

Suitable for an individual from the Government Security Profession

External

Suitable for an individual who has worked in policing or the military or in operations management in industry

Role	Role family	Security specialism
Physical Security Operations Manager Principal	Operations	Physical Security

Role summary

The role of a Physical Security Operations Manager is to ensure the correct posture of physical and tactical resources to manage sites and maintain operational preparedness for security incidents.

Typical role level expectations

- Lead Physical Security operations and set governance structures to appropriately meet the risk appetite, overseeing effective Physical Security to protect assets and people throughout the estate
- Oversee the planning, testing and response to security/emergency incidents or concerns, and provide informed recommendations on Physical Security issues to internal and external stakeholders
- Ensure compliance with relevant regulation and legislation
- Oversee the management of resources, including people, and expenditure while ensuring a positive and inclusive working environment

Entry route

Internal

Suitable for an individual from the Government Security Profession

External

Suitable for an individual who has worked in policing or the military or in operations management in industry

Role	Role family	Security specialism
Physical Security Operations Manager	Operations	Physical Security

Minimum skill expectations

Skill	Skill level	Training	Success profiles
Applied Physical Security	Working	Repository	Making effective decisions*
Risk understanding and mitigation	Working	Repository	Changing and improving
Secure operations management	Working	Repository	Leadership
Protective security	Awareness	Repository	Managing a quality service
Threat understanding	Awareness	Repository	
Legal and regulatory environment and compliance	Awareness	Repository	

*Principal behaviour

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Development

Suggested training	Indicative professional qualifications/accreditations
• Secure operations, project management and controls course • Risk management course • Threat awareness course • Regulatory, compliance or legislative course	• Membership of a relevant institution or body • Relevant industry qualifications and accreditations e.g. America Society for Industrial Security, Physical Security Professional, ISO27001 • Relevant government qualifications and accreditations, e.g. from the Centre for the Protection of National Infrastructure

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC

Role	Role family	Security specialism
Physical Security Operations Manager	Operations	Physical Security

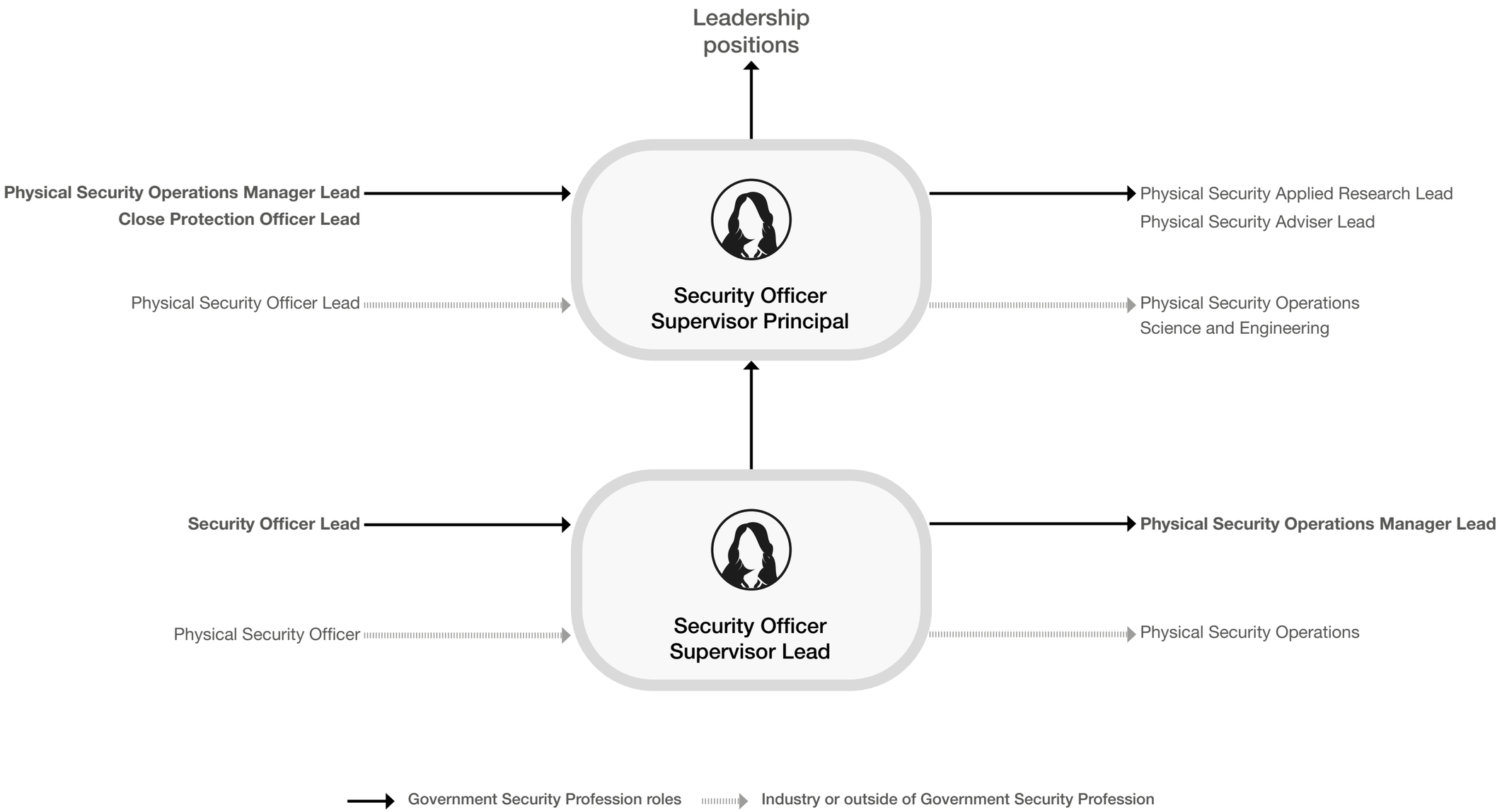
Minimum skill expectations

Skill	Role level	
	Operations Manager Lead	Operations Manager Principal
	Skill level	
Applied Physical Security	Working	Practitioner
Risk understanding and mitigation	Working	Practitioner
Secure operations management	Working	Practitioner
Protective security	Awareness	Working
Threat understanding	Awareness	Working
Legal and regulatory environment and compliance	Awareness	Awareness

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Role	Role family	Security specialism
Security Officer Supervisor	Operations	Physical Security

Suggested entry and exit roles are indicative only and non-exhaustive



Role	Role family	Security specialism
Security Officer Supervisor Lead	Operations	Physical Security

Role summary

The role of a Security Officer Supervisor is to supervise security officers to protect people, property, information, and assets from damage, destruction, or unauthorised removal from an organisation.

Typical role level expectations

- Manage the protection of premises against unauthorised access or occupation, outbreaks of disorder, damage or perceived threat, and unwanted egress and ingress
- Operate security systems in line with standard operating procedures
- Align assigned teams of security officers to protect property or information against compromise, destruction or damage, maintaining integrity of performance through effective management, fostering a positive and inclusive working environment, and addressing concerns in a timely and sensitive manner
- Respond appropriately to security concerns raised, including by third parties, and work with the first responder to incidents or emergencies, escalating and reporting issues as required

Entry route

Internal

Suitable for an individual from the Government Security Profession

External

Suitable for an individual who has worked in military or policing or within security officer supervision in industry

Role	Role family	Security specialism
Security Officer Supervisor Principal	Operations	Physical Security

Role summary

The role of a Security Officer Supervisor is to supervise security officers to protect people, property, information, and assets from damage, destruction, or unauthorised removal from an organisation.

Typical role level expectations

- Supervise the protection of large scale premises against unauthorised access or occupation, outbreaks of disorder, damage or perceived threat, and unwanted egress and ingress
- Oversee the operation security systems in line with standard operating procedures
- Ensure assigned teams of security officers are aligned to protect property or information against compromise, destruction, or damage, maintaining integrity of performance through effective management, ensuring a positive and inclusive working environment is maintained, and concerns are appropriately addressed in a timely and sensitive manner
- Ensure responses to security concerns raised, including by third parties, are appropriately addressed, reviewing escalations and response reports to drive continuous improvement and best practice

Entry route

Internal

Suitable for an individual from the Government Security Profession

External

Suitable for an individual who has worked in military or policing or within security officer supervision in industry

Role	Role family	Security specialism
Security Officer Supervisor	Operations	Physical Security

Minimum skill expectations

Skill	Skill level	Training	Success profiles
Applied Physical Security	Practitioner	Repository	Managing a quality service*
Secure operations management	Practitioner	Repository	Developing self and others
Risk understanding and mitigation	Working	Repository	Making effective decisions
Protective security	Working	Repository	Working together
Threat understanding	Awareness	Repository	
Legal and regulatory environment and compliance	Awareness	Repository	

*Principal behaviour

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Development

Suggested training	Indicative professional qualifications/accreditations
• Protective security course • Customer service course • Operational risk management course • Team leadership and management course	• Membership of a relevant institution or body • Relevant industry qualifications and accreditations e.g. American Society for Industrial Security Associate Protection Professional qualification, Security Industry Authority licence, Certified Protection Professional • Relevant government qualifications and accreditations, e.g. from the Centre for the Protection of National Infrastructure

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC

Role	Role family	Security specialism
Security Officer Supervisor	Operations	Physical Security

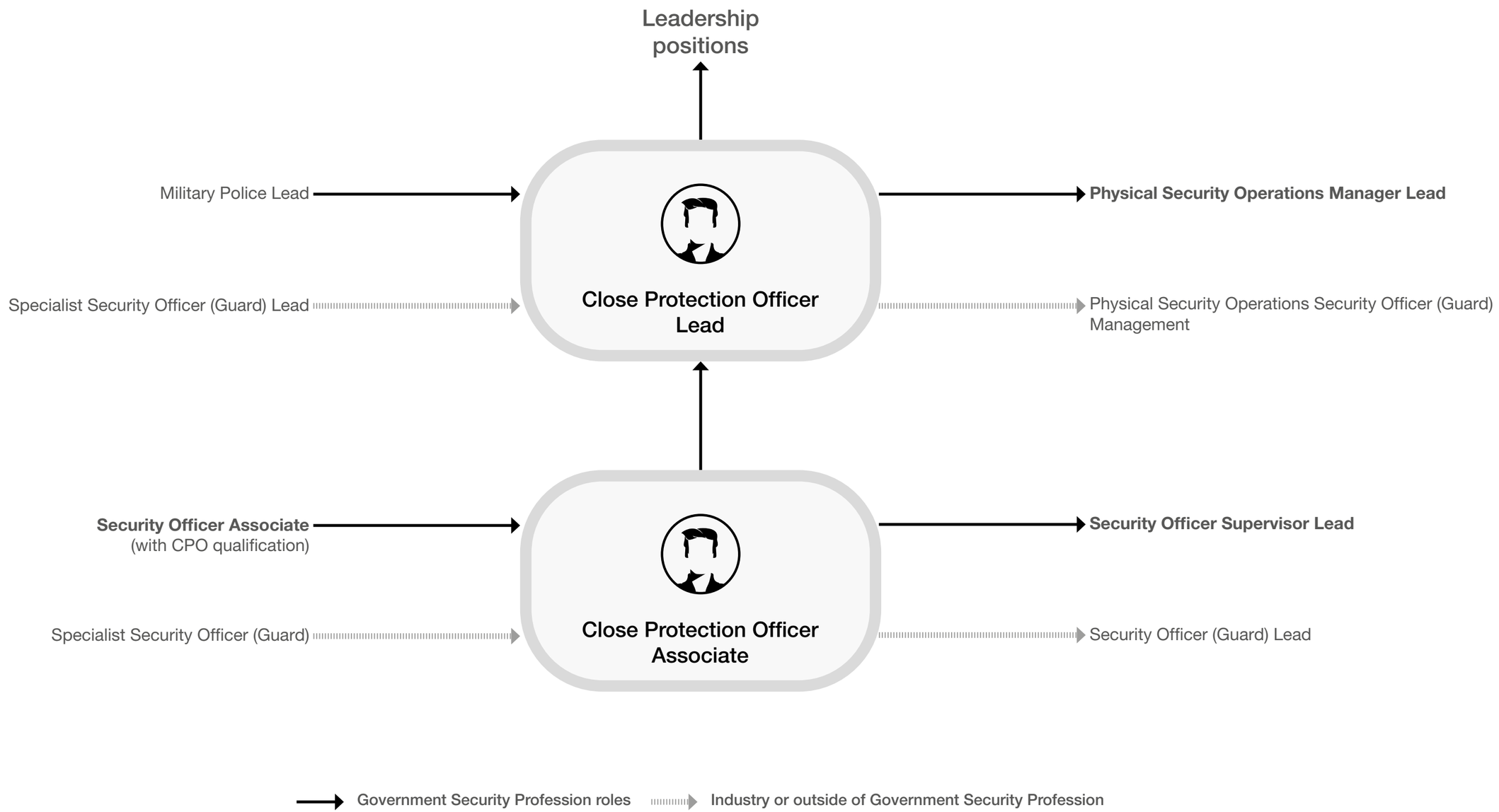
Minimum skill expectations

Skill	Role level	
	Security Officer Supervisor Lead	Security Officer Supervisor Principal
	Skill level	
Applied Physical Security	Practitioner	Practitioner
Secure operations management	Practitioner	Practitioner
Risk understanding and mitigation	Working	Practitioner
Protective security	Working	Practitioner
Threat understanding	Awareness	Working
Legal and regulatory environment and compliance	Awareness	Awareness

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Role	Role family	Security specialism
Close Protection Officer	Operations	Physical Security

Suggested entry and exit roles are indicative only and non-exhaustive



Role	Role family	Security specialism
Close Protection Officer Associate	Operations	Physical Security

Role summary

The role of a Close Protection Officer is to protect principles from the threat of kidnap, assassination and general crime.

Typical role level expectations

- Protect clients from various physical threats while accompanying them on business and social visits
- Follow procedural expectations and requirements, including vulnerability assessments, risk profiling and advance premises screenings
- Identify and prevent potential threats or disruption

Entry route

Internal

Suitable for an individual with a UK military or civilian policing background, who has completed the Royal Military Police's CPO course or the Civilian Police's National Protection Officer's Course

External

Suitable for an individual who has a military policing or civilian policing background or equivalent UK Special Forces experience

Role	Role family	Security specialism
Close Protection Officer Lead	Operations	Physical Security

Role summary

The role of a Close Protection Officer is to protect principles from the threat of kidnap, assassination and general crime.

Typical role level expectations

- Manage a close protection team securing a variety of clients against various physical threats
- Review and action outcomes from procedural activities or processes, including vulnerability assessments, risk profiling, and advance premises screenings
- Lead on the identification and prevention of potential threats or disruption

Entry route

Internal

Suitable for an individual with a UK military or civilian policing background, who has completed the Royal Military Police's CPO course or the Civilian Police's National Protection Officer's Course

External

Suitable for an individual who has a military policing or civilian policing background or equivalent UK Special Forces experience

Role	Role family	Security specialism
Close Protection Officer	Operations	Physical Security

Minimum skill expectations

Skill	Skill level	Training	Success profiles
Risk understanding and mitigation	Practitioner	**Repository**	Communicating and influencing*
Threat understanding	Working	**Repository**	Delivering at pace
Protective security	Working	**Repository**	Leadership
Applied Physical Security	Awareness	**Repository**	Making effective decisions
Secure operations management	Awareness	**Repository**	Managing a quality service
Legal and regulatory environment and compliance	Awareness	**Repository**	Seeing the big picture

*Principal behaviour

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Development

Suggested training	Indicative professional qualifications/accreditations
• Hostile environment course and on-site training • D13.1 Enhanced First Aid Training/Medic • Post Incident Manager's course • National Protection Officers and National Protection Driving courses • Royal Military Police Close Protection course	• Relevant industry or government qualifications and accreditations, e.g. Level 3 Certificate for Working as a Close Protection Operative within the Private Security Industry • Membership of a relevant institution or body

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC

Role	Role family	Security specialism
Close Protection Officer	Operations	Physical Security

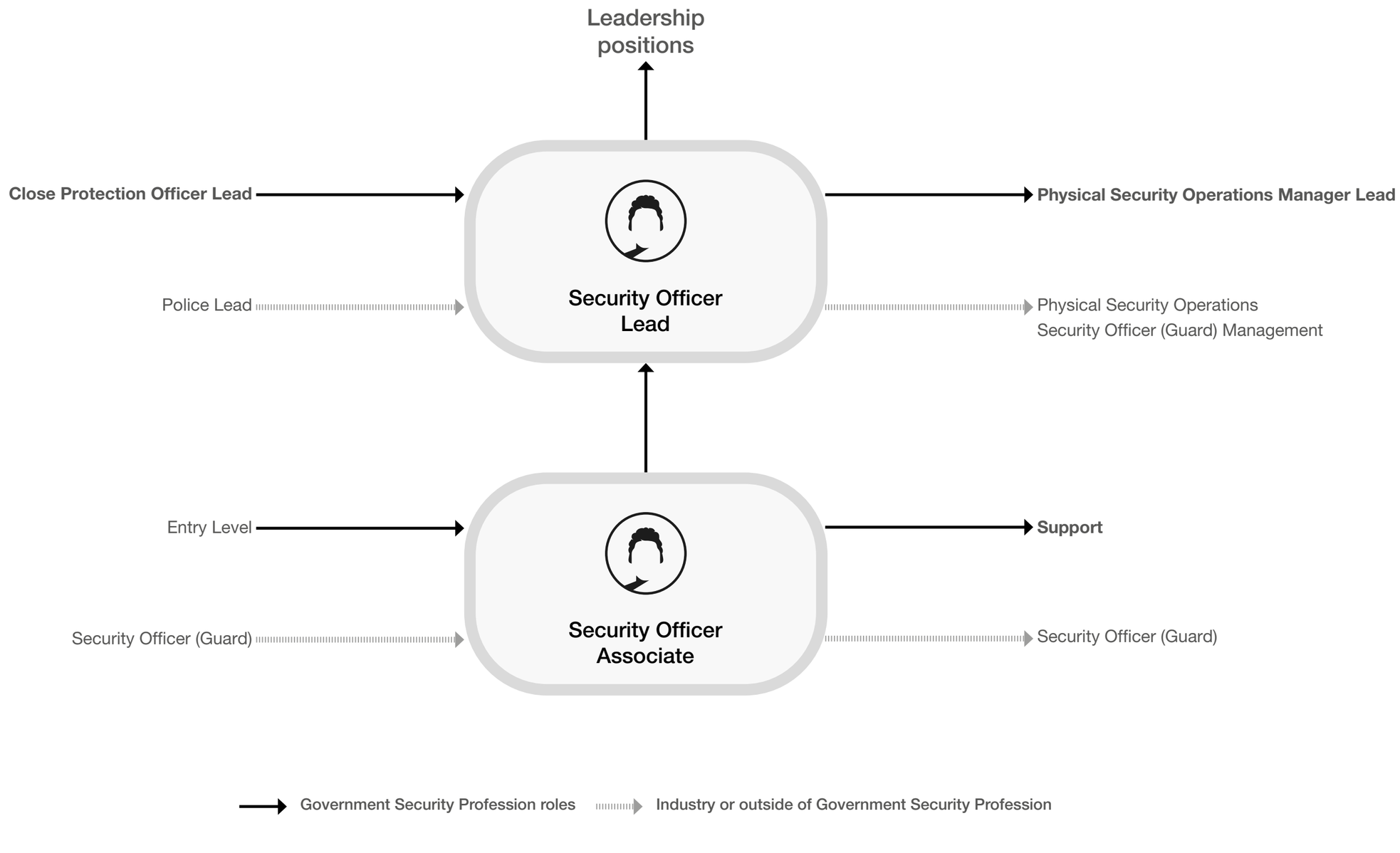
Minimum skill expectations

Skill	Role level	
	Close Protection Officer Associate	Close Protection Officer Lead
	Skill level	
Risk understanding and mitigation	Practitioner	Practitioner
Threat understanding	Working	Practitioner
Protective security	Working	Working
Applied Physical Security	Awareness	Working
Secure operations management	Awareness	Working
Legal and regulatory environment and compliance	Awareness	Awareness

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Role	Role family	Security specialism
Security Officer	Operations	Physical Security

Suggested entry and exit roles are indicative only and non-exhaustive



Role	Role family	Security specialism
Security Officer Associate	Operations	Physical Security

Role summary

The role of a Security Officer is to protect people, property, information and assets from damage, destruction, or unauthorised removal from an organisation.

Typical role level expectations

- Undertake the protection of premises against unauthorised access or occupation, against outbreaks of disorder, and against damage or perceived threat, and against unwanted egress and ingress
- Use security systems in line with standard operating procedures, to monitor and review the activities of individuals of interest
- Respond to security/emergency incidents in a proactive manner, including those raised by third parties, escalating and reporting issues as necessary

Entry route

Internal

Entry level

External

Suitable for an individual who has worked as a Security Officer in industry

Role	Role family	Security specialism
Security Officer Lead	Operations	Physical Security

Role summary

The role of a Security Officer is to protect people, property, information and assets from damage, destruction or unauthorised removal from an organisation.

Typical role level expectations

- Undertake and support with the management of the protection of premises against unauthorised access or occupation, against outbreaks of disorder, and against damage or perceived threat, and against unwanted egress and ingress
- Oversee the use of security systems in line with standard operating procedures, to monitor and review the activities of individuals of interest
- Respond to security/emergency incidents in a proactive manner, including those raised by third parties, reviewing escalations or reports of concerns or issues as necessary

Entry route

Internal

Entry level

External

Suitable for an individual who has worked as a Security Officer in industry

Role	Role family	Security specialism
Security Officer	Operations	Physical Security

Minimum skill expectations

Skill	Skill level	Training	Success profiles
Protective security	Working	**Repository**	Communicating and influencing*
Applied Physical Security	Awareness	**Repository**	Making effective decisions
Risk understanding and mitigation	Awareness	**Repository**	Managing a quality service
Secure operations management	Awareness	**Repository**	Working together
Threat understanding	Awareness	**Repository**	
Legal and regulatory environment and compliance	Awareness	**Repository**	

*Principal behaviour

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Development

Suggested training	Indicative professional qualifications/accreditations
• First aid course • Threat awareness course • Risk management course • Hostile environment course and on-site training • Post Incident Manager's course	• Membership of a relevant institution or body, e.g. Security Industry Authority • Relevant industry qualifications and accreditations, e.g. from American Society for Industrial Security Associate Protection Professional qualification • Relevant government qualifications and accreditations

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC

Role	Role family	Security specialism
Security Officer	Operations	Physical Security

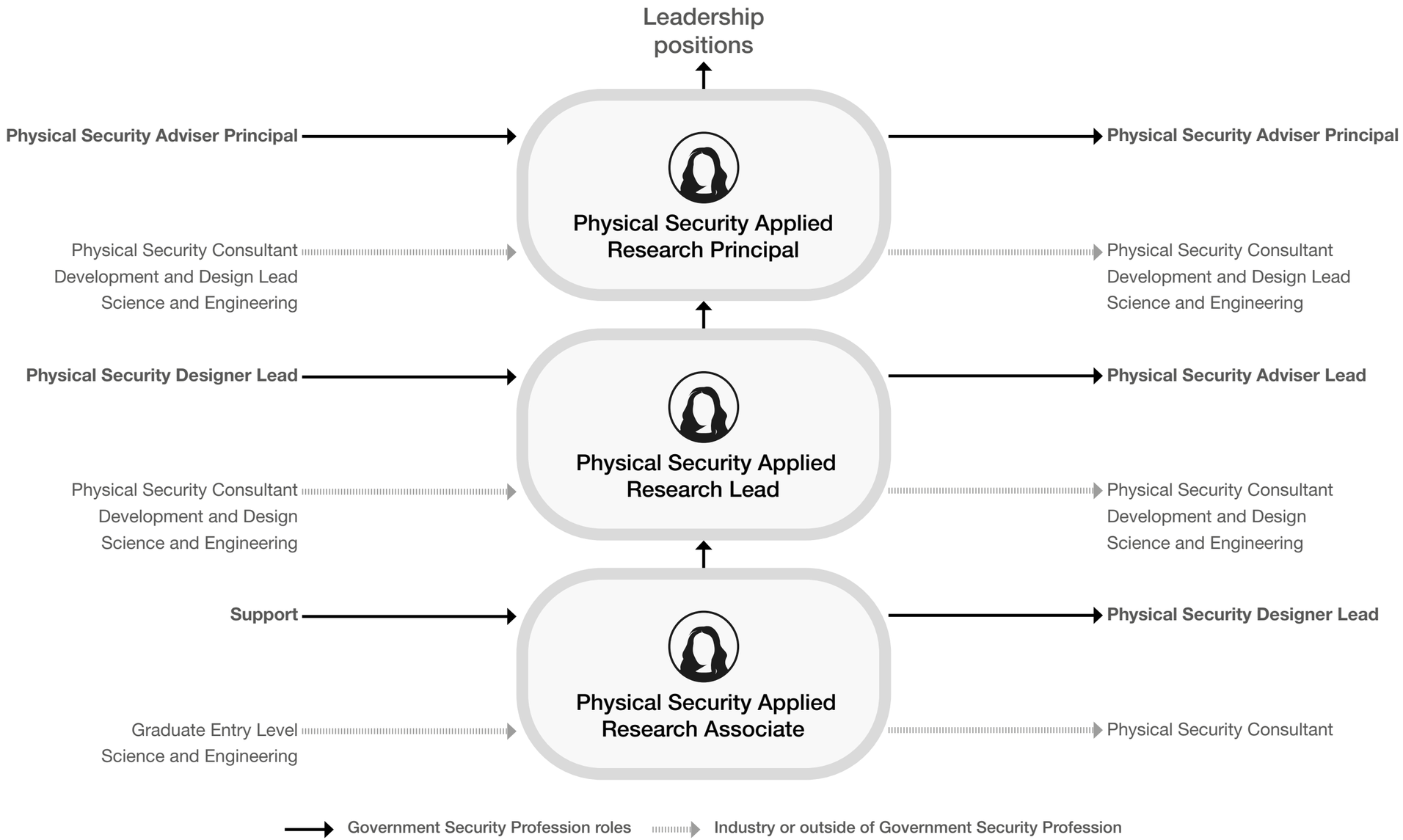
Minimum skill expectations

Skill	Role level	
	Security Officer Associate	Security Officer Lead
	Skill level	
Protective security	Working	Practitioner
Applied Physical Security	Awareness	Working
Risk understanding and mitigation	Awareness	Working
Secure operations management	Awareness	Working
Threat understanding	Awareness	Working
Legal and regulatory environment and compliance	Awareness	Awareness

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Role	Role family	Security specialism
Physical Security Applied Research	Research, development and design	Physical Security

Suggested entry and exit roles are indicative only and non-exhaustive



Role	Role family	Security specialism
Physical Security Applied Research Associate	Research, development and design	Physical Security

Role summary

The role of Physical Security Applied Research is to inform the development of products and services to mitigate Physical Security risks.

Typical role level expectations

- Support a team of researchers to inform the development of products and services, utilising science and/or engineering, adhering to research and development best practices and frameworks to mitigate Physical Security risks
- Maintain awareness of current and emerging technologies and their impact on existing security practices

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. Science and Engineering Profession)

External

Suitable for an individual from an applied research, engineering or scientific background

Role	Role family	Security specialism
Physical Security Applied Research Lead	Research, development and design	Physical Security

Role summary

The role of Physical Security Applied Research is to inform the development of products and services to mitigate Physical Security risks.

Typical role level expectations

- Conduct research to inform the development of products and services, utilising science and/or engineering, adhering to research and development best practices and frameworks to mitigate Physical Security risks
- Provide technical guidance on emerging or existing issues
- Contribute to national and international Physical Security standards
- Maintain awareness of current and emerging technologies and their impact on existing security practices

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. Science and Engineering Profession)

External

Suitable for an individual from an applied research, engineering or scientific background

Role	Role family	Security specialism
Physical Security Applied Research Principal	Research, development and design	Physical Security

Role summary

The role of Physical Security Applied Research is to inform the development of products and services to mitigate Physical Security risks.

Typical role level expectations

- Commission and lead a team undertaking research to inform the development of products and services, utilising science and/or engineering, adhering to research and development best practices and frameworks to mitigate Physical Security risks
- Provide technical guidance on emerging or existing issues, providing thought leadership and foresight of future evolving threats, and advising on the development and implementation of countermeasures
- Initiate, influence, and lead the continuous improvement of national and international Physical Security standards
- Define the standard current and emerging technologies and their impact on existing security practices for the whole specialism, inside and outside the organisation

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. Science and Engineering Profession)

External

Suitable for an individual from an applied research, engineering or scientific background

Role	Role family	Security specialism
Physical Security Applied Research	Research, development and design	Physical Security

Minimum skill expectations

Skill	Skill level	Training	Success profiles
Applied research	Working	Repository	Managing a quality service*
Legal and regulatory environment and compliance	Working	Repository	Changing and improving
Applied Physical Security	Working	Repository	Developing self and others
Risk understanding and mitigation	Awareness	Repository	Seeing the big picture
Threat understanding	Awareness	Repository	
Protective security	Awareness	Repository	

*Principal behaviour

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Development

Suggested training	Indicative professional qualifications/accreditations
• Research based regulatory, compliance or legislative course • Risk management course • Threat awareness course • Research methodologies course	• Membership of a relevant institution or body e.g. Register of Security Engineers and Specialists • Relevant industry qualifications and accreditations • Relevant HM Government qualifications and accreditations e.g. from the Centre for the Protection of National Infrastructure

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC

Role	Role family	Security specialism
Physical Security Applied Research	Research, development and design	Physical Security

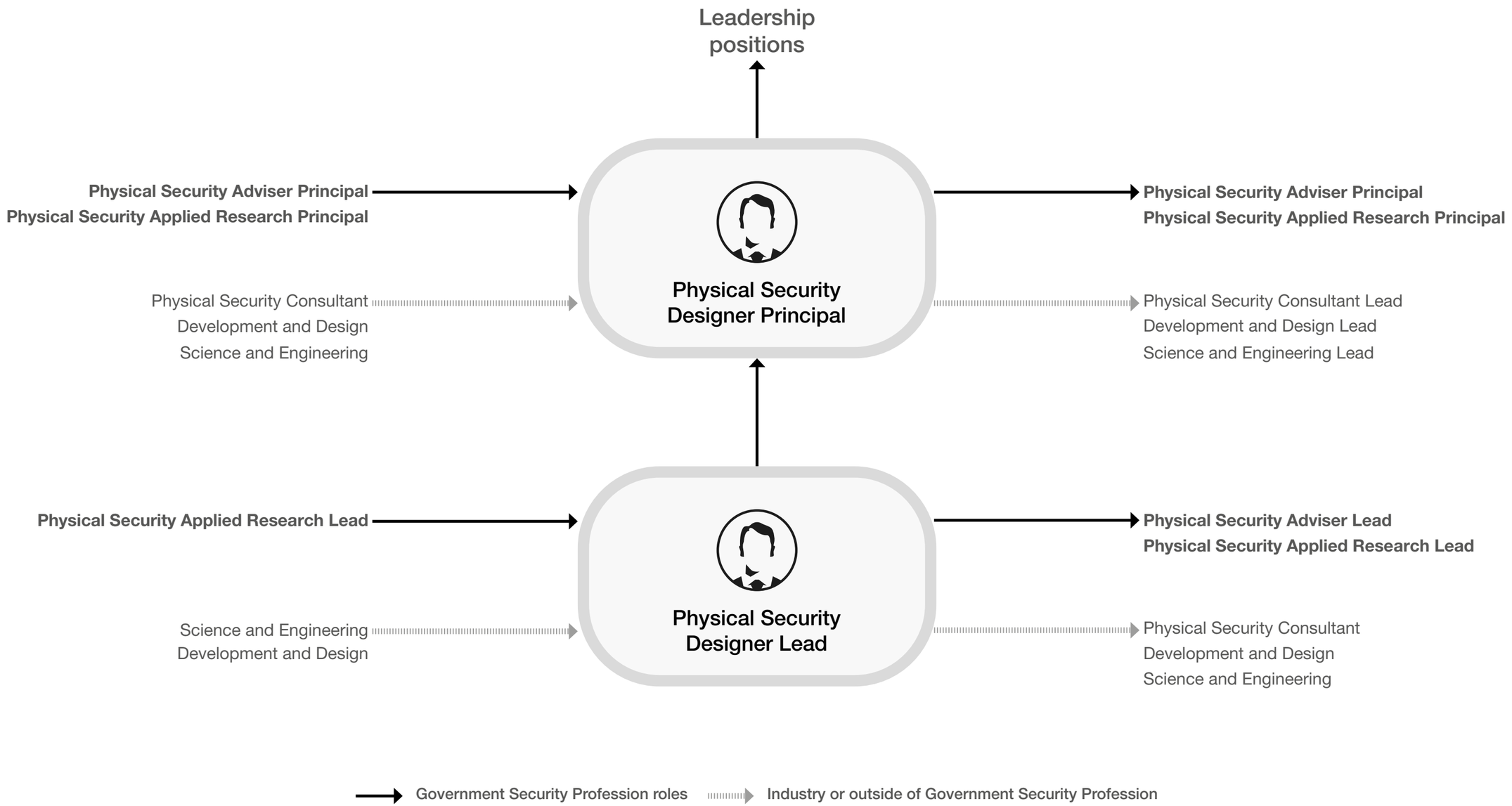
Minimum skill expectations

Skill	Role level		
	Applied Research Associate	Applied Research Lead	Applied Research Principal
	Skill level		
Applied research	Working	Practitioner	Expert
Legal and regulatory environment and compliance	Working	Practitioner	Expert
Applied Physical Security	Working	Practitioner	Practitioner
Risk understanding and mitigation	Awareness	Working	Practitioner
Threat understanding	Awareness	Awareness	Working
Protective security	Awareness	Awareness	Awareness

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Role	Role family	Security specialism
Physical Security Designer	Research, development and design	Physical Security

Suggested entry and exit roles are indicative only and non-exhaustive



Role	Role family	Security specialism
Physical Security Designer Lead	Research, development and design	Physical Security

Role summary

The role of Physical Security Designer is to provide advice and expertise on the design and implementation of Physical Security measures.

Typical role level expectations

- Issue and produce specifications or requirements for Physical Security design
- Review and quality assure local Physical Security solutions for an environment
- Share best practice advice with the wider research, development and design community
- Leverage understanding of local level risks and threat environment to inform relevant advice

Entry route

Internal

Suitable for an individual from the Government Security specialism or other relevant profession (e.g. Science and Engineering Profession)

External

Suitable for an individual from an applied research, engineering or scientific background

Role	Role family	Security specialism
Physical Security Designer Principal	Research, development and design	Physical Security

Role summary

The role of Physical Security Designer is to provide advice and expertise on the design and implementation of Physical Security measures.

Typical role level expectations

- Lead teams issuing and producing specifications or requirements for Physical Security design across an organisation or across wider government
- Oversee, quality assure, and commission local Physical Security solutions for multiple environments
- Shape best practice advice and share with the wider research, development and design community
- Develop and lead organisational understanding of local-level risks and threat environment to inform relevant advice

Entry route

Internal

Suitable for an individual from the Government Security specialism or other relevant profession (e.g. Science and Engineering Profession)

External

Suitable for an individual from an applied research, engineering or scientific background

Role	Role family	Security specialism
Physical Security Designer	Research, development and design	Physical Security

Minimum skill expectations

Skill	Skill level	Training	Success profiles
Design	Practitioner	**Repository**	Managing a quality service*
Legal and regulatory environment and compliance	Practitioner	**Repository**	Changing and improving
Applied Physical Security	Practitioner	**Repository**	Developing self and others
Protective security	Working	**Repository**	Seeing the big picture
Risk understanding and mitigation	Working	**Repository**	
Secure operations management	Working	**Repository**	
Threat understanding	Awareness	**Repository**	

*Principal behaviour

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Development

Suggested training	Indicative professional qualifications/accreditations
• Secure design course • Risk management course • Threat awareness course • Design-based regulatory, compliance or legislative course	• Membership of a relevant institution or body e.g. the Register of Security Engineers and Specialists • Relevant industry qualifications/accreditations e.g. Certified Information Systems Auditor, ISO27001 Lead Auditor • Relevant HM Government qualifications and accreditations e.g. from the Centre of the Protection of National Infrastructure

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC

Role	Role family	Security specialism
Physical Security Designer	Research, development and design	Physical Security

Minimum skill expectations

Skill	Role level	
	Designer Lead	Designer Principal
	Skill level	
Design	Practitioner	Expert
Legal and regulatory environment and compliance	Practitioner	Expert
Applied Physical Security	Practitioner	Practitioner
Protective security	Working	Practitioner
Risk understanding and mitigation	Working	Practitioner
Secure operations management	Working	Practitioner
Threat understanding	Awareness	Awareness

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Personnel Security – role families and roles

Personnel Security is a system of policies and procedures that seek to mitigate the risk of workers (insiders) exploiting their legitimate access to an organisation's assets for unauthorised purposes.

Advisory


Head of Personnel Security


Adviser


Assurance

Operations


Appeals and Litigation


Investigation

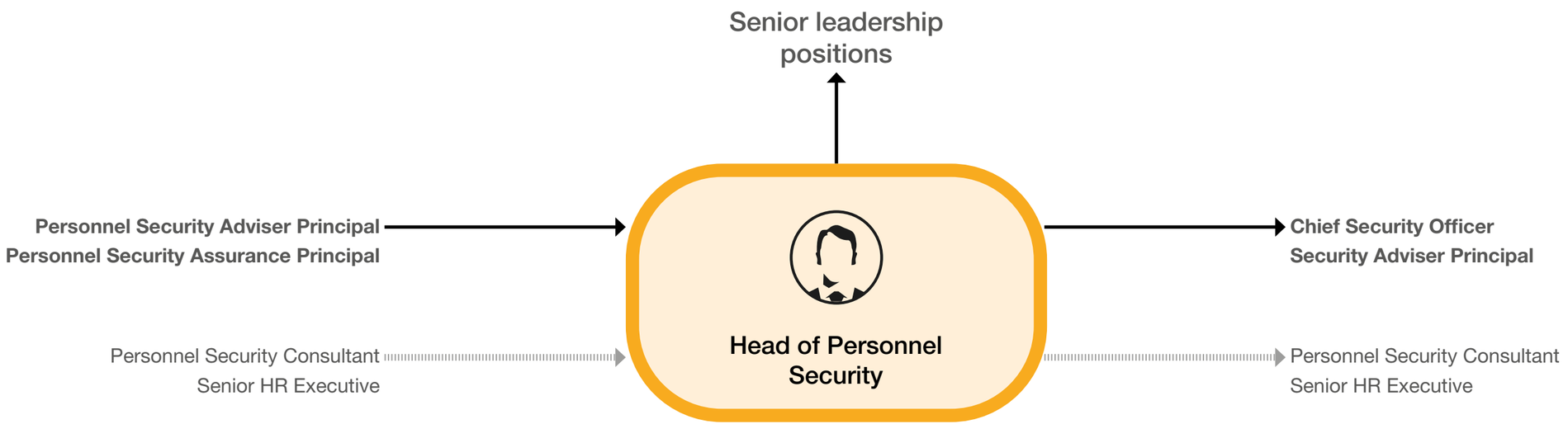

Screening

Research, development and design


Behavioural Scientist

Role	Role family	Security specialism
Head of Personnel Security	Advisory	Personnel Security

Suggested entry and exit roles are indicative only and non-exhaustive



Role	Role family	Security specialism
Head of Personnel Security	Advisory	Personnel Security

Role summary

The Head of Personnel Security is responsible for the Personnel Security specialism, providing strategic direction, anticipating challenges, driving performance and building the capability required to ensure the security of new and existing services.

Typical role level expectations

- Be the primary point of contact on Personnel Security issues with key stakeholders, including external parties, and actively develop strong working relationships in relation to Personnel Security
- Ensure that Personnel Security policies and security controls remain appropriate and proportionate to the assessed risks, and are responsive and adaptable to the changing threat environment, business requirements and central government policies
- Champion learning, development and accreditation, cultivate talent and foster an inclusive, diverse and motivated workforce
- Promote cross-government security mindedness
- Promote the Government Personnel Security Profession and advise on Personnel Security risks
- Work with industry, including security manufacturers and security consultants, to drive best practice
- Drive professional development by working with Government Security Function to set and drive continuous learning standards

Entry route

Internal

Suitable for an individual from the Government Security Profession

External

Suitable for an individual from a senior management position in the private sector

Role	Role family	Security specialism
Head of Personnel Security	Advisory	Personnel Security

Minimum skill expectations

Skill	Skill level	Training	Success profiles
Applied Personnel Security	Expert	**Repository**	Leadership*
Protective security	Working	**Repository**	Communicating and influencing
Risk understanding and mitigation	Awareness	**Repository**	Developing self and others
Threat understanding	Awareness	**Repository**	Seeing the big picture
			Working together

*Principal behaviour

Skill levels are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

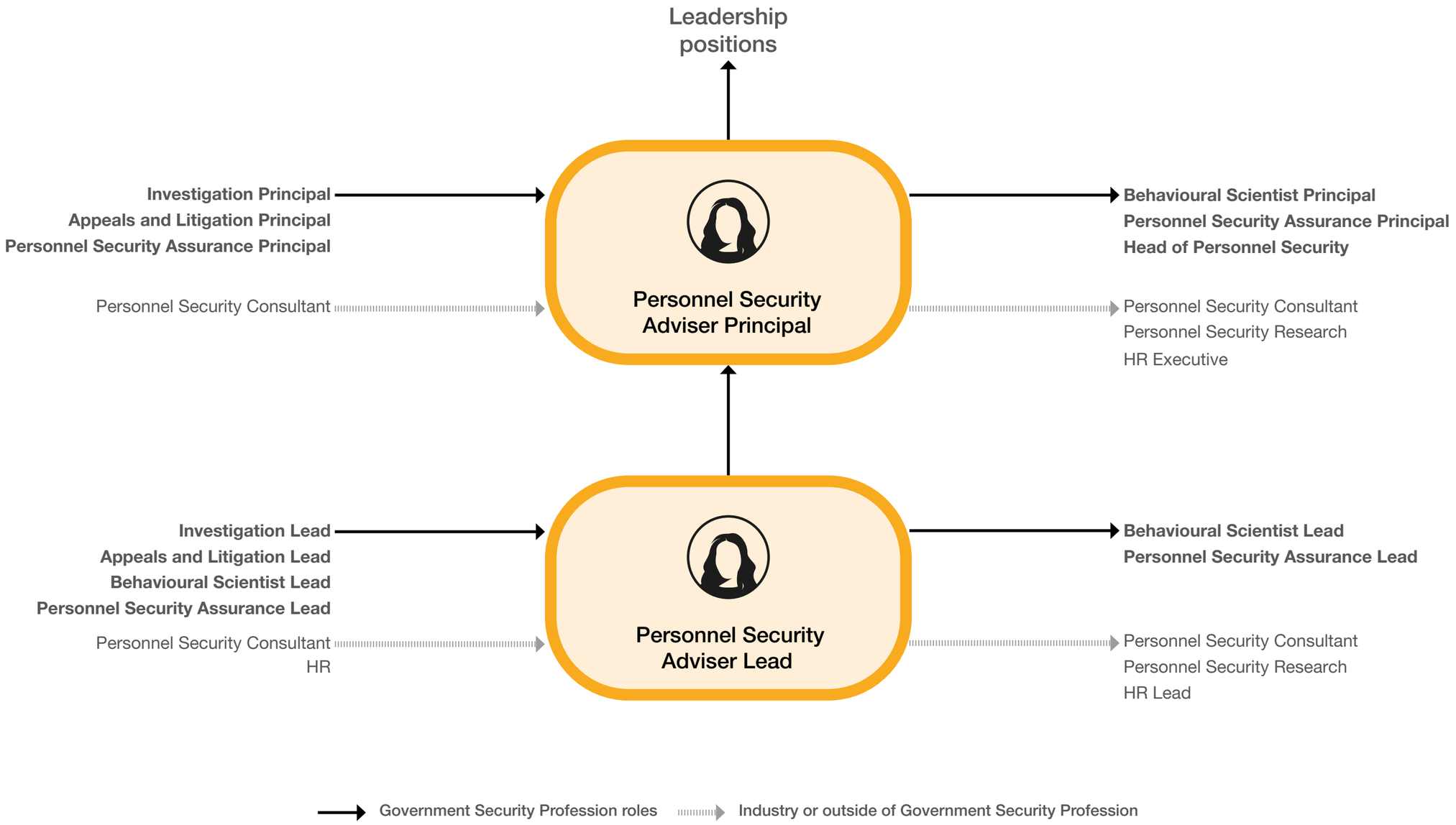
Development

Suggested training	Indicative professional qualifications/accreditations
• Personnel Security leadership course • Risk management and information risk management course • Threat to HM Government/industry training	• Membership of a relevant institution or body • Relevant industry or government qualifications and accreditations

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC

Role	Role family	Security specialism
Personnel Security Adviser	Advisory	Personnel Security

Suggested entry and exit roles are indicative only and non-exhaustive



Role	Role family	Security specialism
Personnel Security Adviser Lead	Advisory	Personnel Security

Role summary

The role of a Personnel Security Adviser is to provide expert tailored Personnel Security advice to the public and private sectors to mitigate the insider risk.

Typical role level expectations

- Provide expert advice on Personnel Security to the Government Security Profession and wider public and/or private sector
- Conduct risk assessments in the local environment, extracting insights to provide an informed opinion on Personnel Security risks and the adequacy of controls in place
- Align with relevant regulation, policy and standards to provide proportional, practical advice, tailored to the local environment, and advise on any residual risk
- Monitor the efficiency and effectiveness of the Personnel Security processes across the organisation, and make recommendations for continual improvement
- Maintain awareness of current and emerging technologies and their impact on existing security practices

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. HR, Behavioural Sciences or Research and Development)

External

Suitable for an individual who has worked as a Personnel Security consultant in industry

Role	Role family	Security specialism
Personnel Security Adviser Principal	Advisory	Personnel Security

Role summary

The role of a Personnel Security Adviser is to provide expert tailored Personnel Security advice to the public and private sectors to mitigate the insider risk.

Typical role level expectations

- Provide expert advice on Personnel Security to the Government Security Profession and wider public and/or private sector
- Manage and commission risk assessments in the local environment, extracting insights to provide an informed opinion on Personnel Security risks and the adequacy of controls in place
- Create organisational vision for aligning with regulation, policy and standards to provide proportional, practical advice, tailored to the local environment, and advise on any residual risk
- Create and monitor standards regarding efficiency and effectiveness of the Personnel Security processes across the organisation, and make recommendations for continual improvement
- Maintain awareness of current and emerging technologies and their impact on existing security practices

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. HR, Behavioural Sciences or Research and Development)

External

Suitable for an individual who has worked as a Personnel Security consultant in industry

Role	Role family	Security specialism
Personnel Security Adviser	Advisory	Personnel Security

Minimum skill expectations

Skill	Skill level	Training	Success profiles
Applied Personnel Security	Practitioner	**Repository**	Making effective decisions*
Risk understanding and mitigation	Practitioner	**Repository**	Changing and improving
Protective security	Working	**Repository**	Communicating and influencing
Threat understanding	Working	**Repository**	Managing a quality service
Legal and regulatory environment and compliance	Working	**Repository**	Seeing the big picture
			Working at pace

*Principal behaviour

Skill levels are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Development

Suggested training	Indicative professional qualifications/accreditations
• Risk management leadership course • Security management course • Threat awareness course • Security framework course • Security strategy course	• Chartered psychologist/HR • Membership of a relevant institution or body, e.g. Chartered Institute of Personnel and Development, Register of Security Engineers and Specialists • Relevant industry or government qualifications and accreditations e.g. from the Centre for the Protection of National Infrastructure

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC

Role	Role family	Security specialism
Personnel Security Adviser	Advisory	Personnel Security

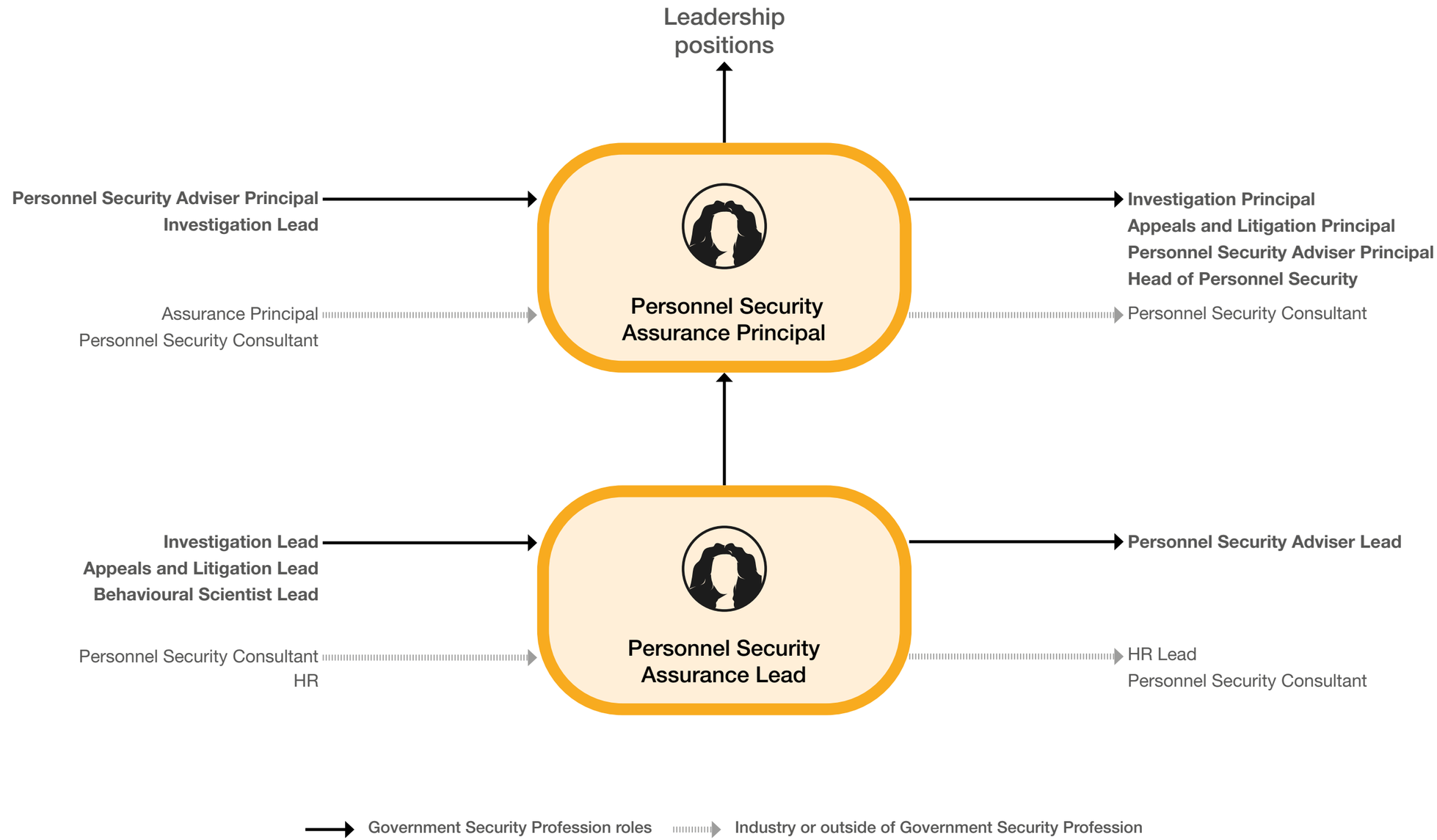
Minimum skill expectations

Skill	Role level	
	Adviser Lead	Adviser Principal
	Skill level	
Applied Personnel Security	Practitioner	Expert
Risk understanding and mitigation	Practitioner	Expert
Protective security	Working	Practitioner
Threat understanding	Working	Practitioner
Legal and regulatory environment and compliance	Working	Working

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Role	Role family	Security specialism
Personnel Security Assurance	Advisory	Personnel Security

Suggested entry and exit roles are indicative only and non-exhaustive



Role	Role family	Security specialism
Personnel Security Assurance Lead	Advisory	Personnel Security

Role summary

The role of Personnel Security Assurance is to establish the appropriate Personnel Security organisational posture to deliver an effective risk-based approach to mitigate the insider risk.

Typical role level expectations

- Deliver Personnel Security assurance processes, including providing audit information to risk owners
- Monitor and report on the delivery of Personnel Security processes against requirements, with the use of key performance indicators
- Review current personnel risk reduction methods, including those which are technological or procedural, and highlight areas of concern
- Ensure alignment with government and/or industry objectives and standards, proactively reviewing and assuring security risk and highlighting non-conformance

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. HR, Behavioural Sciences or Research and Development)

External

Suitable for an individual who has worked as a Personnel Security consultant in industry

Role	Role family	Security specialism
Personnel Security Assurance Principal	Advisory	Personnel Security

Role summary

The role of Personnel Security Assurance is to establish the appropriate Personnel Security organisational posture to deliver an effective risk-based approach to mitigate the insider risk.

Typical role level expectations

- Manage delivery and life cycle of Personnel Security assurance processes, including sharing audit information to senior leadership, and setting assurance standards across government
- Manage the assessment, recording and monitoring of Personnel Security processes
- Review reporting, including key performance indicators, and act as key decision maker for the delivery of Personnel Security processes against requirements
- Ensure alignment with government and/or industry objectives and standards, and liaise with senior stakeholders on how these objectives and standards can be met

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. HR, Behavioural Sciences or Research and Development)

External

Suitable for an individual who has worked as a Personnel Security consultant in industry

Role	Role family	Security specialism
Personnel Security Assurance	Advisory	Personnel Security

Minimum skill expectations

Skill	Skill level	Training	Success profiles
Applied Personnel Security	Practitioner	Repository	Making effective decisions*
Legal and regulatory environment and compliance	Practitioner	Repository	Changing and improving
Risk understanding and mitigation	Practitioner	Repository	Communicating and influencing
Protective security	Awareness	Repository	Managing a quality service
Threat understanding	Awareness	Repository	Seeing the big picture

*Principal behaviour

Skill levels are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Development

Suggested training	Indicative professional qualifications/accreditations
• Regulatory, compliance or legislative course • Threat awareness course • Risk management leadership course	• Chartered psychologist/HR • Membership of a relevant institution or body e.g. Chartered Institute of Personnel and Development, Register of Security Engineers and Specialists • Relevant industry or government qualifications and accreditations e.g. from the Centre for the Protection of National Infrastructure

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC

Role	Role family	Security specialism
Personnel Security Assurance	Advisory	Personnel Security

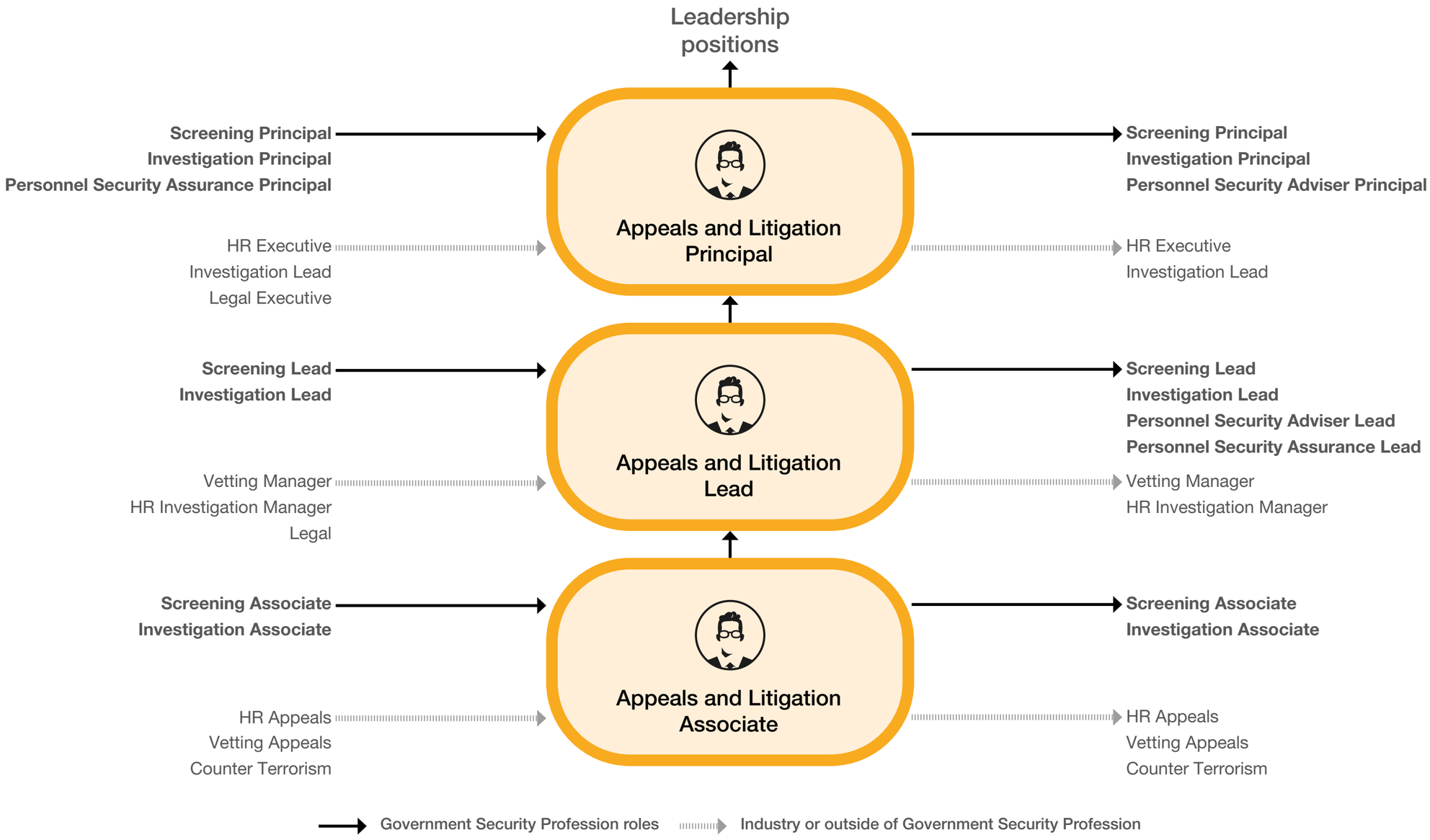
Minimum skill expectations

Skill	Role level	
	Assurance Lead	Assurance Principal
	Skill level	
Applied Personnel Security	Practitioner	Expert
Legal and regulatory environment and compliance	Practitioner	Expert
Risk understanding and mitigation	Practitioner	Expert
Protective security	Awareness	Working
Threat understanding	Awareness	Working

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Role	Role family	Security specialism
Appeals and Litigation	Operations	Personnel Security

Suggested entry and exit roles are indicative only and non-exhaustive



Role	Role family	Security specialism
Appeals and Litigation Associate	Operations	Personnel Security

Role summary

The role of Appeals and Litigation is to manage the appeals and litigation processes in accordance with internal and regulatory policies.

Typical role level expectations

- Collaborate with a wider team on the appeals and litigation processes and assist in all elements of the litigation process
- Deal with complex and non-routine cases exercising appropriate levels of delegation and risk management, and provide sound analysis of issues
- Provide sound advice with regards to appeals and litigation risk
- Share best legal practice with the wider organisation, and share data-driven status updates to team leadership

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. Counter-Fraud, Counter-Terrorism, HR or Behavioural Sciences)

External

Suitable for an individual who has industry vetting or HR experience, or experience in counter terrorism advisory

Role	Role family	Security specialism
Appeals and Litigation Lead	Operations	Personnel Security

Role summary

The role of Appeals and Litigation is to manage the appeals and litigation processes in accordance with internal and regulatory policies.

Typical role level expectations

- Manage and align a team regarding appeals and litigation processes
- Manage complex and non-routine cases exercising appropriate levels of delegation and risk management, and provide sound analysis of issues
- Provide specialised advice with regards to appeals and litigation risk
- Share best legal practice with a local team and with the wider organisation, and present data-driven status updates to Personnel Security leadership

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. Counter-Fraud, Counter-Terrorism, HR or Behavioural Sciences)

External

Suitable for an individual who has industry vetting or HR experience, or experience in counter terrorism advisory

Role	Role family	Security specialism
Appeals and Litigation Principal	Operations	Personnel Security

Role summary

The role of Appeals and Litigation is to manage the appeals and litigation processes in accordance with internal and regulatory policies.

Typical role level expectations

- Provide leadership for teams within appeals and litigation during high profile or non-standard litigation processes
- Provide leadership to complex and non-routine cases exercising appropriate levels of delegation and risk management, and provide expert analysis of issues
- Provide expert advice with regards to appeals and litigation risk
- Share best legal practice with the wider appeals and litigation community and with the wider organisation, and present data-driven status updates to Personnel Security leadership

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. Counter-Fraud, Counter-Terrorism, HR or Behavioural Sciences)

External

Suitable for an individual who has industry vetting or HR experience, or experience in counter terrorism advisory

Role	Role family	Security specialism
Appeals and Litigation	Operations	Personnel Security

Minimum skill expectations

Skill	Skill level	Training	Success profiles
Applied Personnel Security	Working	**Repository**	Making effective decisions*
Risk understanding and mitigation	Working	**Repository**	Changing and improving
Legal and regulatory environment and compliance	Awareness	**Repository**	Communicating and influencing
Threat understanding	Awareness	**Repository**	Managing a quality service
Protective security	Awareness	**Repository**	Seeing the big picture

*Principal behaviour

Skill levels are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Development

Suggested training	Indicative professional qualifications/accreditations
• Tribunals training • Risk management training • Threat awareness training • Regulatory, compliance or legislative course	• Chartered psychologist/HR • Membership of a relevant institution or body, e.g. Chartered Institute of Personnel and Development, Register of Security Engineers and Specialists • Relevant industry or government qualifications and accreditations e.g. from the Centre for the Protection of National Infrastructure

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC

Role	Role family	Security specialism
Appeals and Litigation	Operations	Personnel Security

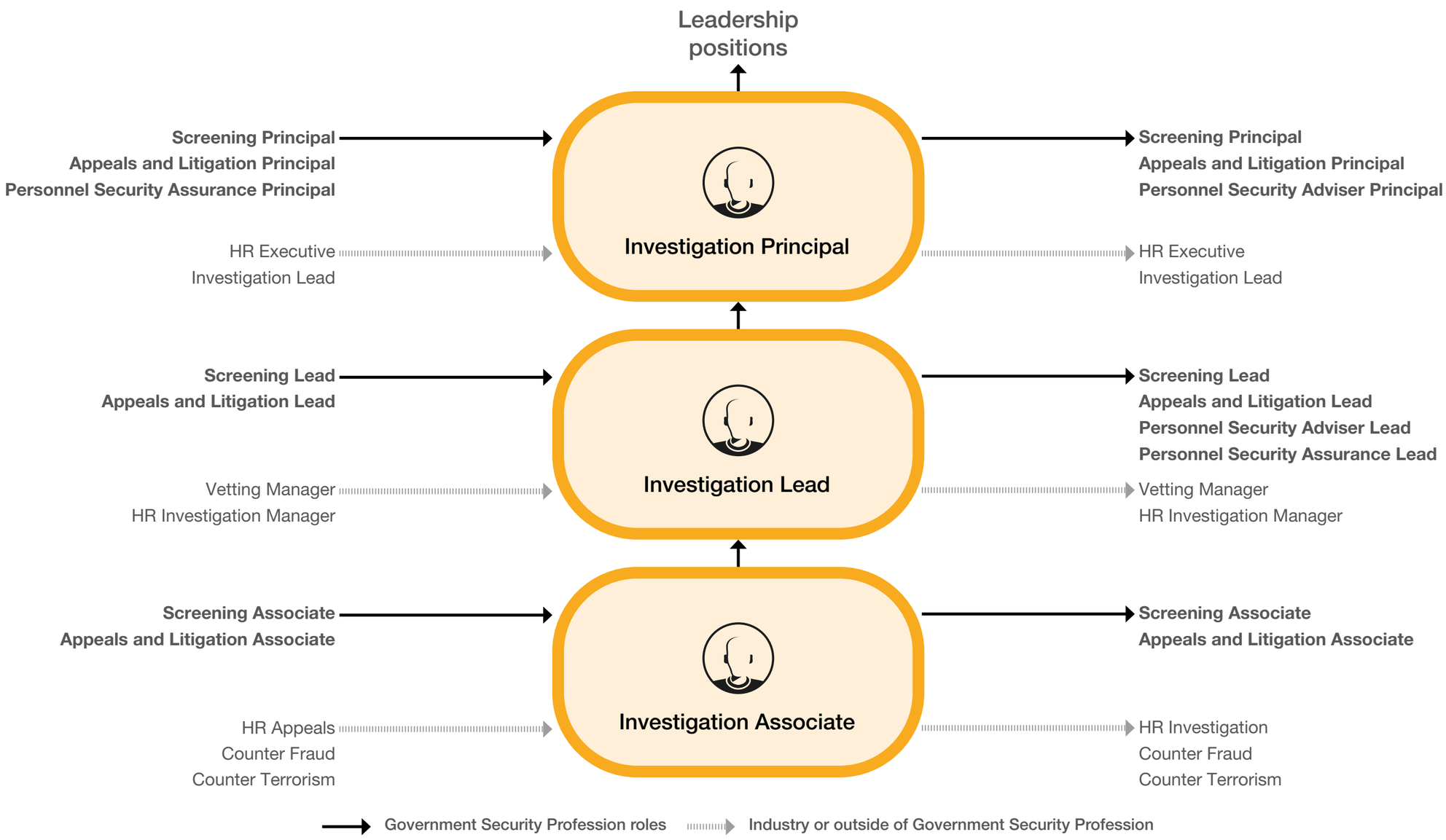
Minimum skill expectations

Skill	Role level		
	Appeals and Litigation Associate	Appeals and Litigation Lead	Appeals and Litigation Principal
	Skill level		
Applied Personnel Security	Working	Practitioner	Expert
Risk understanding and mitigation	Working	Practitioner	Expert
Legal and regulatory environment and compliance	Awareness	Working	Practitioner
Threat understanding	Awareness	Working	Practitioner
Protective security	Awareness	Working	Working

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Role	Role family	Security specialism
Investigation	Operations	Personnel Security

Suggested entry and exit roles are indicative only and non-exhaustive



Role	Role family	Security specialism
Investigation Associate	Operations	Personnel Security

Role summary

The role of Investigation is to investigate and analyse Personnel Security incidents, provide tailored recommendations of actions to resolve issues, feed back lessons learned to the appropriate risk groups, and ensure new mitigations can be instigated to reduce the likelihood of a repeat incident.

Typical role level expectations

- Design impact assessment documents prior to initiating investigations to assess whether an investigation is necessary
- Conduct investigations into Personnel Security incidents in line with relevant organisational HR and security policies
- Produce comprehensive reports on the outcome of investigations and recommend disciplinary action where necessary
- Contribute to the creation and maintenance of policies and procedures

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. Counter-Fraud, Counter-Terrorism, HR or Behavioural Sciences)

External

Suitable for an individual who has industry vetting or HR experience, or experience in counter terrorism advisory

Role	Role family	Security specialism
Investigation Lead	Operations	Personnel Security

Role summary

The role of Investigation is to investigate and analyse Personnel Security incidents, provide tailored recommendations of actions to resolve issues, feed back lessons learned to the appropriate risk groups, and ensure new mitigations can be instigated to reduce the likelihood of a repeat incident.

Typical role level expectations

- Review impact assessment documents before initiating investigations to assess whether an investigation is necessary
- Manage investigations into Personnel Security incidents in line with relevant organisational HR and security policies
- Lead on the delivery of comprehensive reports on the outcome of investigations
- Lead on the creation and maintenance of policies and procedures associated with the investigation process

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. Counter-Fraud, Counter-Terrorism, HR or Behavioural Sciences)

External

Suitable for an individual who has industry vetting or HR experience, or experience in counter terrorism advisory

Role	Role family	Security specialism
Investigation Principal	Operations	Personnel Security

Role summary

The role of Investigation is to investigate and analyse Personnel Security incidents, provide tailored recommendations of actions to resolve issues, feed back lessons learned to the appropriate risk groups, and ensure new mitigations can be instigated to reduce the likelihood of a repeat incident.

Typical role level expectations

- Review non-standard impact assessment documents prior to initiating investigations to assess whether an investigation is necessary
- Provide leadership and oversight to Personnel Security incidents and mandate compliance to relevant organisational HR and security policies
- Lead on the review of comprehensive reports on the outcome of investigations
- Provide leadership for and ensure substantial reviews are held on policies and procedures associated with the investigation process

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. Counter-Fraud, Counter-Terrorism, HR or Behavioural Sciences)

External

Suitable for an individual who has industry vetting or HR experience, or experience in counter terrorism advisory

Role	Role family	Security specialism
Investigation	Operations	Personnel Security

Minimum skill expectations

Skill	Skill level	Training	Success profiles
Investigative interviewing	Practitioner	**Repository**	Making effective decisions*
Applied Personnel Security	Practitioner	**Repository**	Changing and improving
Risk understanding and mitigation	Working	**Repository**	Communicating and influencing
Legal and regulatory environment and compliance	Working	**Repository**	Managing a quality service
Protective security	Awareness	**Repository**	Seeing the big picture
Threat understanding	Awareness	**Repository**	

*Principal behaviour

Skill levels are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Development

Suggested training	Indicative professional qualifications/accreditations
• Insider threat identification and management course • Threat awareness course • Risk management course • Regulatory, compliance or legislative course	• Chartered psychologist/HR • Membership of a relevant institution or body, e.g. Chartered Institute of Personnel and Development, Register of Security Engineers and Specialists • Relevant industry or government qualifications and accreditations e.g. from the Centre for the Protection of National Infrastructure

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC

Role	Role family	Security specialism
Investigation	Operations	Personnel Security

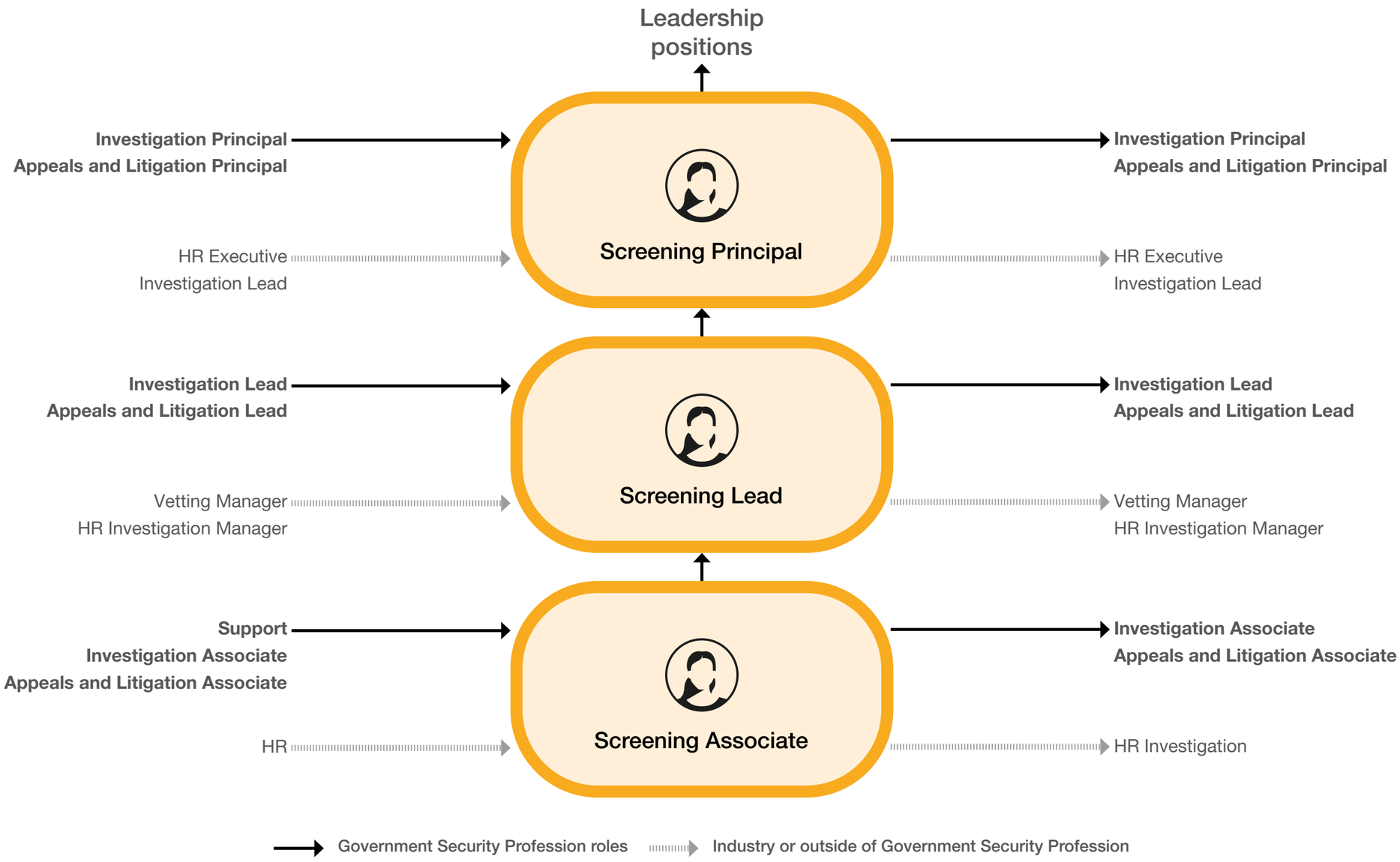
Minimum skill expectations

Skill	Role level		
	Investigation Associate	Investigation Lead	Investigation Principal
	Skill level		
Investigative interviewing	Practitioner	Practitioner	Expert
Applied Personnel Security	Practitioner	Practitioner	Practitioner
Risk understanding and mitigation	Working	Practitioner	Practitioner
Legal and regulatory environment and compliance	Working	Working	Practitioner
Protective security	Awareness	Working	Practitioner
Threat understanding	Awareness	Working	Working

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Role	Role family	Security specialism
Screening	Operations	Personnel Security

Suggested entry and exit roles are indicative only and non-exhaustive



Role	Role family	Security specialism
Screening Associate	Operations	Personnel Security

Role summary

Screening's role is to align the screening processes (including vetting) with a risk-based approach to assure that incoming individuals (and any subsequent internal movers) have been appropriately assessed.

Typical role level expectations

- Conduct pre-employment and post-employment screenings in line with relevant regulation, policy, and standards
- Produce comprehensive reports on the outcome of screening procedures
- Support the implementation of a proportionate, multi-disciplinary approach to countering insider threats
- Contribute to creating and maintaining policies and procedures associated with the screening process

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. HR, Behavioural Sciences or Research and Development)

External

Suitable for an individual who has industry vetting or HR experience, or experience in counter terrorism advisory

Role	Role family	Security specialism
Screening Lead	Operations	Personnel Security

Role summary

Screening's role is to align the screening processes (including vetting) with a risk-based approach to assure that incoming individuals (and any subsequent internal movers) have been appropriately assessed.

Typical role level expectations

- Manage a team of screening professionals to deliver appropriate decisions in line with risk appetite and relevant regulation, policy, and standards
- Develop and design the implementation of a proportionate, multi-disciplinary approach to countering insider threats
- Manage corporate reviews after any significant incidents
- Lead on creating and maintaining policies and procedures associated with the screening process

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. HR, Behavioural Sciences or Research and Development)

External

Suitable for an individual who has industry vetting or HR experience, or experience in counter terrorism advisory

Role	Role family	Security specialism
Screening Principal	Operations	Personnel Security

Role summary

Screening's role is to align the screening processes (including vetting) with a risk-based approach to assure that incoming individuals (and any subsequent internal movers) have been appropriately assessed.

Typical role level expectations

- Manage a team of Screening Leads and their teams to deliver appropriate decisions in line with risk appetite and relevant regulation, policy, and standards
- Review and make decisions based on comprehensive reports on the outcome of screening procedures
- Lead the implementation of a proportionate, multi-disciplinary approach to countering insider threats
- Lead and provide oversight to cross-team corporate reviews after any significant incidents

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. HR, Behavioural Sciences or Research and Development)

External

Suitable for an individual who has industry vetting or HR experience, or experience in counter terrorism advisory

Role	Role family	Security specialism
Screening	Operations	Personnel Security

Minimum skill expectations

Skill	Skill level	Training	Success profiles
Applied Personnel Security	Working	Repository	Making effective decisions*
Risk understanding and mitigation	Working	Repository	Changing and improving
Legal and regulatory environment and compliance	Awareness	Repository	Communicating and influencing
Threat understanding	Awareness	Repository	Managing a quality service
Investigative interviewing	Awareness	Repository	Seeing the big picture
Protective security	Awareness	Repository	

*Principal behaviour

Skill levels are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Development

Suggested training	Indicative professional qualifications/accreditations
• Threat awareness course • Risk management course • Regulatory, compliance, or legislative course	• Chartered psychologist/HR • Membership of a relevant institution or body e.g. Chartered Institute of Personnel and Development, Register of Security Engineers and Specialists • Relevant industry/HM Government qualifications/accreditations e.g. from the Centre for the Protection of National Infrastructure

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC

Role	Role family	Security specialism
Screening	Operations	Personnel Security

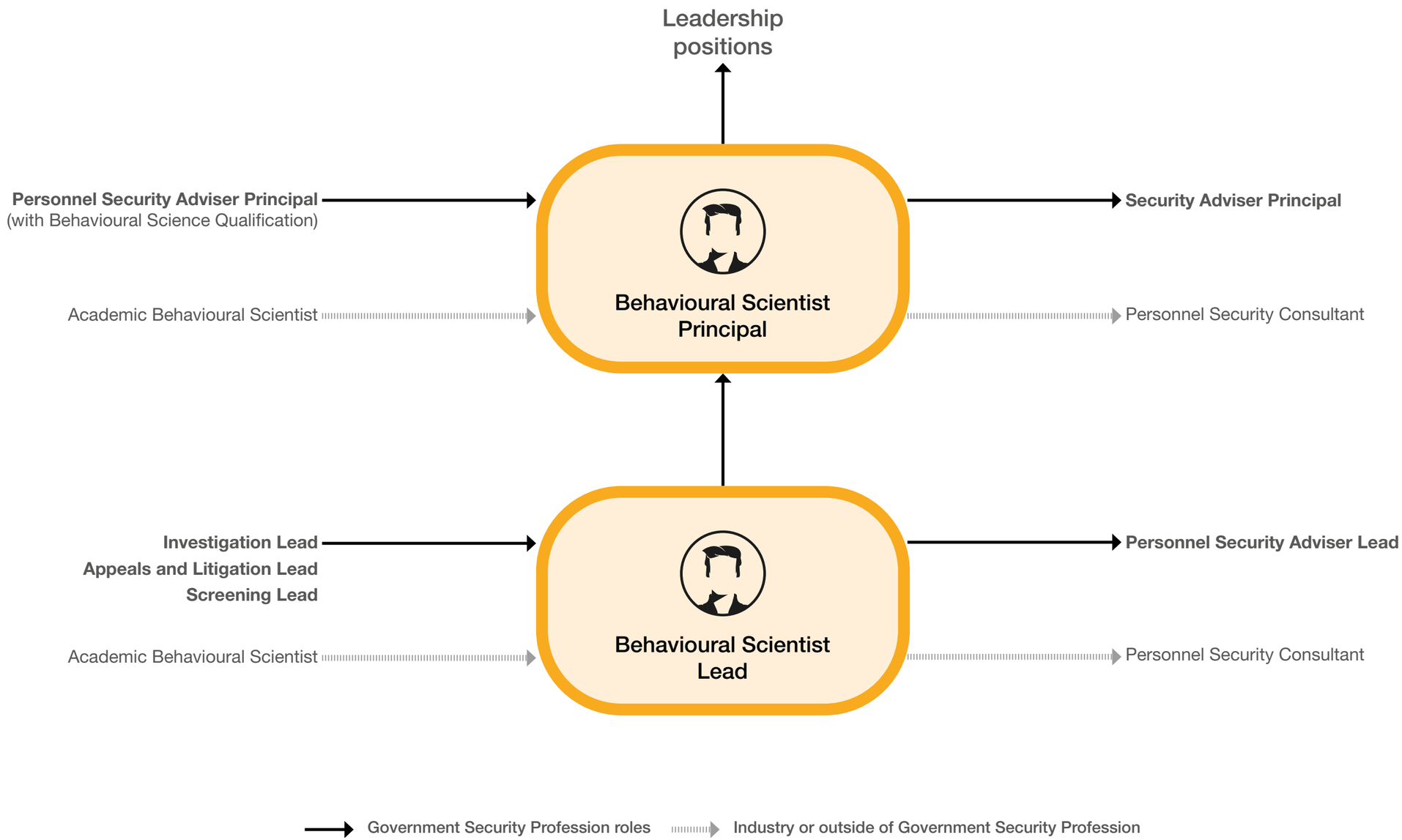
Minimum skill expectations

Skill	Role level		
	Screening Associate	Screening Lead	Screening Principal
	Skill level		
Applied Personnel Security	Working	Practitioner	Expert
Risk understanding and mitigation	Working	Practitioner	Expert
Legal and regulatory environment and compliance	Awareness	Working	Practitioner
Threat understanding	Awareness	Working	Practitioner
Investigative interviewing	Awareness	Working	Working
Protective security	Awareness	Working	Working

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Role	Role family	Security specialism
Behavioural Scientist	Research, development and design	Personnel Security

Suggested entry and exit roles are indicative only and non-exhaustive



Role	Role family	Security specialism
Behavioural Scientist Lead	Research, development and design	Personnel Security

Role summary

The role of a Behavioural Scientist is to enhance the department's effectiveness in mitigating the insider risk. They provide behavioural science assessments and advice that is evidence based and practitioner focused.

Typical role level expectations

- Deliver robust applied behavioural insights to security programmes and projects
- Identify areas for improvement in current security assessment and development tools
- Design and implement new approaches to security programmes to increase uptake and impact
- Influence, change, and impact security decisions with both internal and external stakeholders

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. HR, Behavioural Sciences or Research and Development)

External

Suitable for an individual who has studied or worked in industry as a Behavioural Scientist

Role	Role family	Security specialism
Behavioural Scientist Principal	Research, development and design	Personnel Security

Role summary

The role of a Behavioural Scientist is to enhance the department's effectiveness in mitigating the insider risk. They provide behavioural science assessments and advice that is evidence based and practitioner focused.

- Typical role level expectations
- Manage and provide an expert point of view into robust applied behavioural insights delivered to security programmes and projects
- Provide expert advice on areas for improvement in current security assessment and development tools
- Lead on the design and implementation of new approaches to security programmes to increase uptake and impact
- Influence, change, and impact security decisions with both internal and external stakeholders

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. HR, Behavioural Sciences or Research and Development)

External

Suitable for an individual who has studied or worked in industry as a Behavioural Scientist

Role	Role family	Security specialism
Behavioural Scientist	Research, development and design	Personnel Security

Minimum skill expectations

Skill	Skill level	Training	Success profiles
Applied Personnel Security	Practitioner	Repository	Changing and improving*
Applied research	Practitioner	Repository	Communicating and influencing
Legal and regulatory environment and compliance	Practitioner	Repository	Delivering at pace
Risk understanding and mitigation	Working	Repository	Seeing the big picture
Protective security	Working	Repository	
Threat understanding	Awareness	Repository	

*Principal behaviour

Skill levels are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Development

Suggested training	Indicative professional qualifications/accreditations
• Research-based regulatory, compliance, or legislative course • Risk management course • Threat awareness course • Research methodologies course	• Chartered psychologist/HR • Membership of a relevant institution or body, e.g. Chartered Institute of Personnel and Development, Register of Security Engineers and Specialists • Relevant industry or government qualifications and accreditations e.g. from the Centre for the Protection of National Infrastructure

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC

Role	Role family	Security specialism
Behavioural Scientist	Research, development and design	Personnel Security

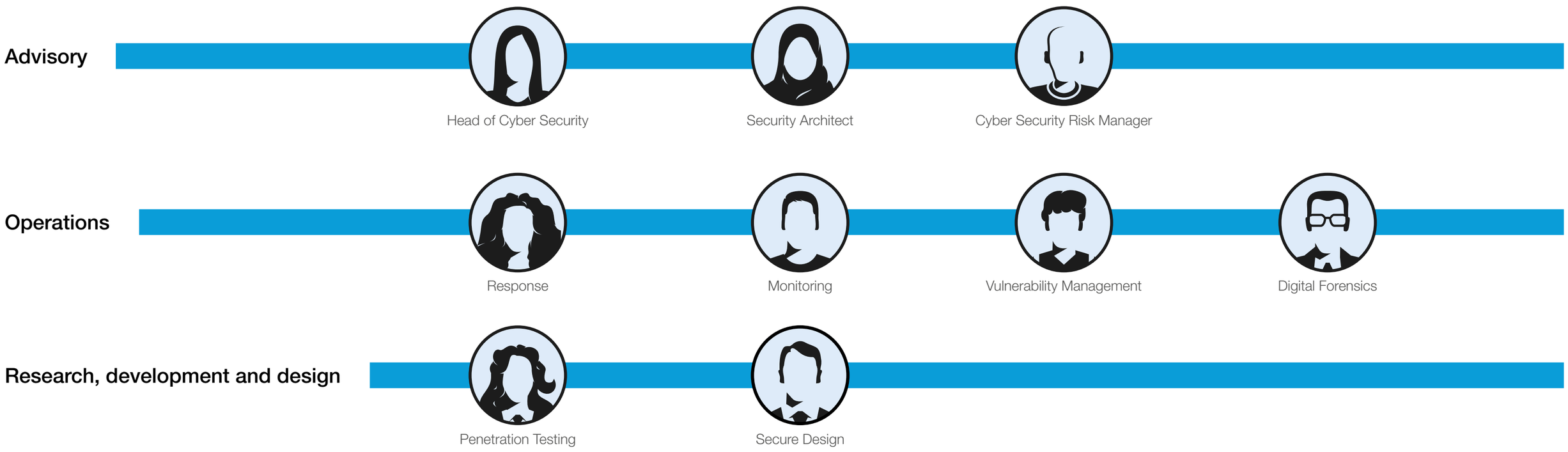
Minimum skill expectations

Skill	Role level	
	Behavioural Scientist Lead	Behavioural Scientist Principal
	Skill level	
Applied Personnel Security	Practitioner	Expert
Applied research	Practitioner	Expert
Legal and regulatory environment and compliance	Practitioner	Expert
Risk understanding and mitigation	Working	Practitioner
Protective security	Working	Working
Threat understanding	Awareness	Working

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

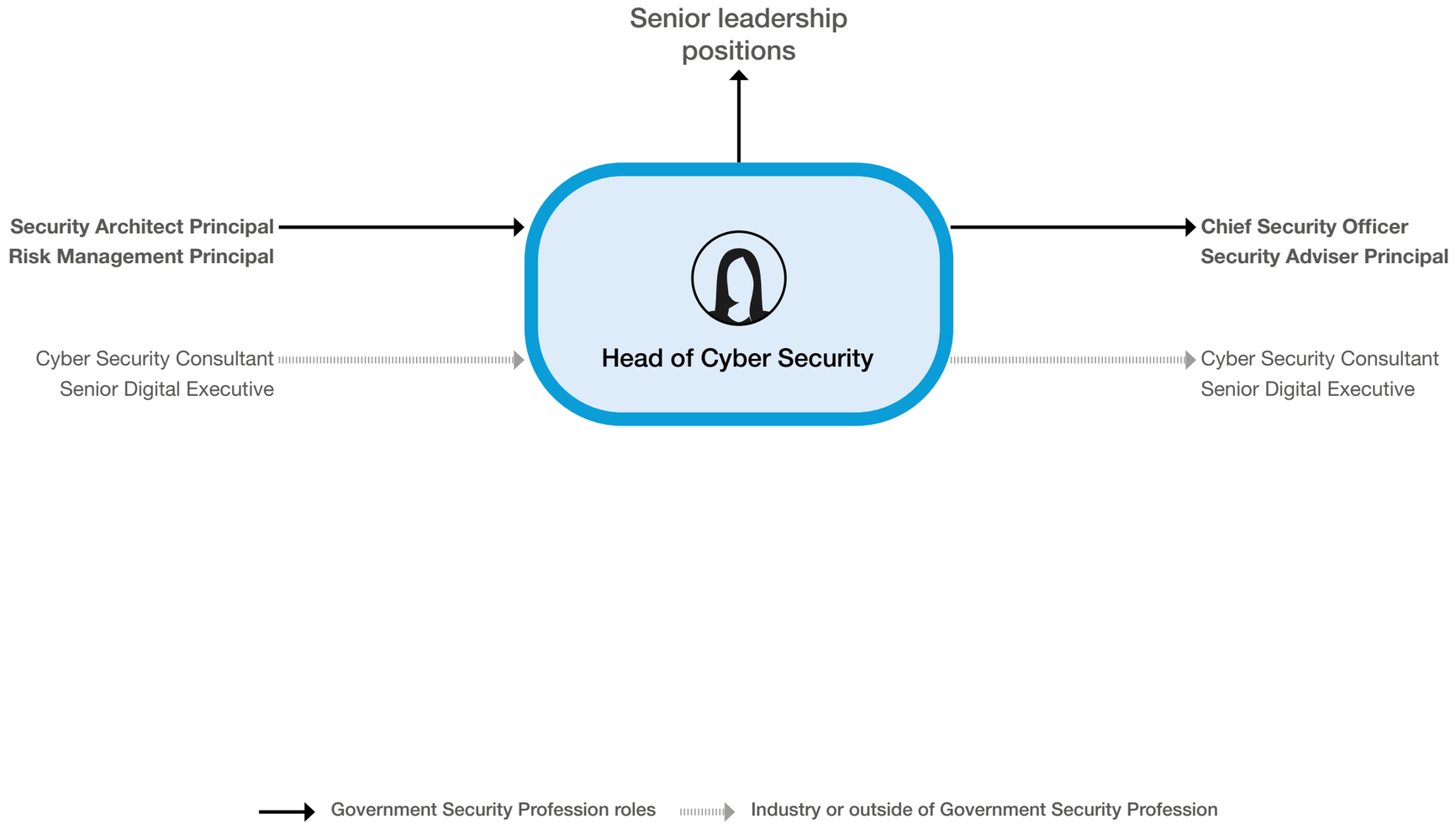
Cyber Security – role families and roles

Cyber Security protects information systems (hardware, software and their associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes intentional harm by the operator of the system, or accidental harm as a result of failing to follow security procedures.



Role	Role family	Security specialism
Head of Cyber Security	Advisory	Cyber Security

Suggested entry and exit roles are indicative only and non-exhaustive



Role	Role family	Security specialism
Head of Cyber Security	Advisory	Cyber Security

Role summary

The Head of Cyber Security is responsible for the Cyber Security specialism. They provide strategic direction, anticipate challenges, drive performance and build the capability required to ensure the security of new and existing services.

Typical role level expectations

- Be the primary point of contact on Cyber Security issues with key stakeholders, including external parties, and actively develop strong working relationships in relation to Cyber Security
- Ensure that the Cyber Security policies and security controls remain appropriate and proportionate to the assessed risks, and are responsive and adaptable to the changing threat environment, business requirements and central government policies
- Champion learning, development and accreditation, cultivate talent and foster an inclusive, diverse and motivated workforce
- Work with the heads of specialisms to promote cross-government security mindedness
- Influence, change and impact decisions with both internal and external stakeholders
- Promote the Government Cyber Security Profession and advise on Cyber Security risks
- Work with industry, including security manufacturers and security consultants, to drive best practice
- Drive professional development by working with the Government Security Function to set and drive continuous learning standards

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. Science and Engineering Profession)

External

Suitable for an individual from a senior management position in the private sector

Role	Role family	Security specialism
Head of Cyber Security	Advisory	Cyber Security

Minimum skill expectations

Skill	Skill level	Training	Success profiles
Applied security capability	Expert	**Repository**	Leadership*
Protective security	Working	**Repository**	Communicating and influencing
Threat understanding	Awareness	**Repository**	Developing self and others
Information risk assessment and risk management	Awareness	**Repository**	Seeing the big picture
			Working together

*Principal behaviour

Skill levels are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

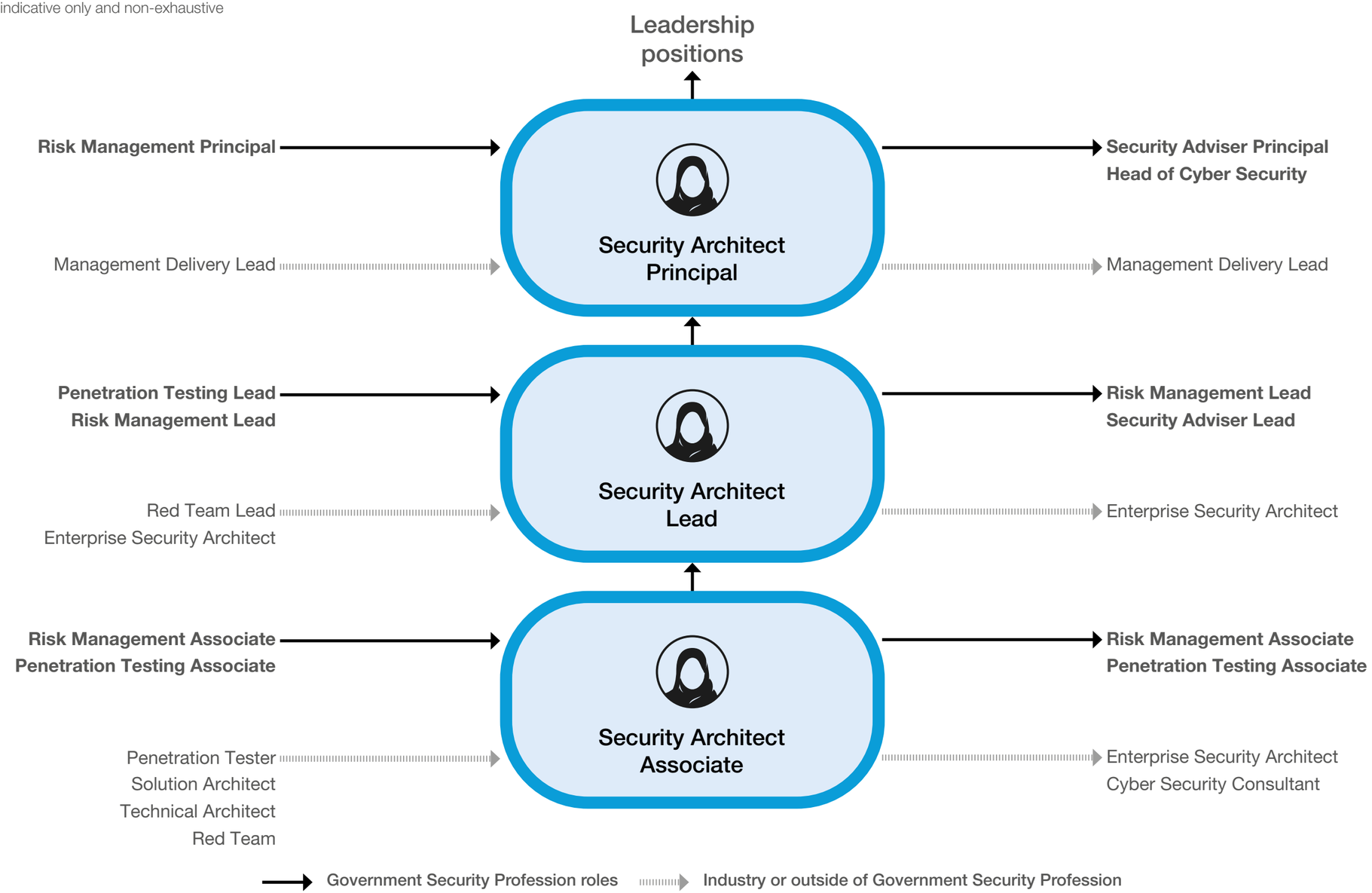
Development

Suggested training	Indicative professional qualifications/accreditations
• Cyber Security leadership course • Risk management and information risk management course • Threat to HM Government and industry training	• Membership of a relevant institution or body • Relevant industry and government qualifications and accreditations

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC

Role	Role family	Security specialism
Security Architect	Advisory	Cyber Security

Suggested entry and exit roles are indicative only and non-exhaustive



Role	Role family	Security specialism
Security Architect Associate	Advisory	Cyber Security

Role summary

The Security Architect advises and enables technical teams to make security decisions. They provide advice and guidance to ensure common tools and patterns are used effectively to deliver secure systems, and they implement proportionate controls to enable business outcomes.

Typical role level expectations

- Recommend security controls and identify solutions that support a business objective
- Provide specialist advice and recommendations regarding approaches and technologies across teams and various stakeholders, assessing the risk associated with proposed changes
- Inspire and influence others to execute security principles, communicating widely with other stakeholders
- Help review ongoing security architectural activities

Entry route

Internal

Suitable for an individual from a technical role within the Government Security Profession

External

Suitable for an individual who has worked in the private sector in both a managerial and a technical capacity, especially from the technology sector

Role	Role family	Security specialism
Security Architect Lead	Advisory	Cyber Security

Role summary

The Security Architect advises and enables technical teams to make security decisions. They provide advice and guidance to ensure common tools and patterns are used effectively to deliver secure systems, and implement proportionate controls to enable business outcomes.

Typical role level expectations

- Lead the technical design of systems and services, justifying and communicating all design decisions, applying research and innovative security architecture solutions to new or existing problems
- Communicate the vision, principles and strategy for security architects for one project or technology
- Decipher subtle security needs and understand the impact of decisions, balancing requirements and deciding between approaches
- Lead on quality assurance, and act as the point of escalation for Security Architects within a team
- Interact with stakeholders across organisations, teams, or communities

Entry route

Internal

Suitable for an individual from a technical role within the Government Security Profession

External

Suitable for an individual who has worked in the private sector in both a managerial and a technical capacity, especially from the technology sector

Role	Role family	Security specialism
Security Architect Principal	Advisory	Cyber Security

Role summary

The Security Architect advises and enables technical teams to make security decisions. They provide advice and guidance to ensure common tools and patterns are used effectively to deliver secure systems, and implement proportionate controls to enable business outcomes.

Typical role level expectations

- Lead projects with high strategic impact, setting a strategy that can be used in the long term and across the whole organisation
- Develop vision, principles and strategy for Security Architects for multiple projects or technologies
- Recommend security design across several projects or technologies, up to an organisational or inter-organisational level, solving unprecedented issues and problems
- Influence key organisational and architectural decisions, and interact with senior stakeholders across organisations to reach and influence a wide range of people across larger teams and communities

Entry route

Internal

Suitable for an individual from a technical role within the Government Security Profession

External

Suitable for an individual who has worked in the private sector in both a managerial and a technical capacity, especially from the technology sector

Role	Role family	Security specialism
Security Architect	Advisory	Cyber Security

Minimum skill expectations

Skill	Skill level	Training	Success profiles
Security architecture	Working	Repository	Making effective decisions*
Applied security capability	Working	Repository	Changing and improving
Information risk assessment and risk management	Working	Repository	Communicating and influencing
Protective security	Working	Repository	Leadership
Threat understanding	Working	Repository	Seeing the big picture
			Working together

*Principal behaviour

Skill levels are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Development

Suggested training	Indicative professional qualifications/accreditations
• Information security management principles course • Information risk management course • Cyber Security Development Programme • Security architecture course or programme	• Membership in a professional association • Relevant industry qualifications/accreditations e.g. Certified Information Systems Security Professional, Certified Information Security Management Principles • Relevant HM Government qualifications or accreditations

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC

Role	Role family	Security specialism
Security Architect	Advisory	Cyber Security

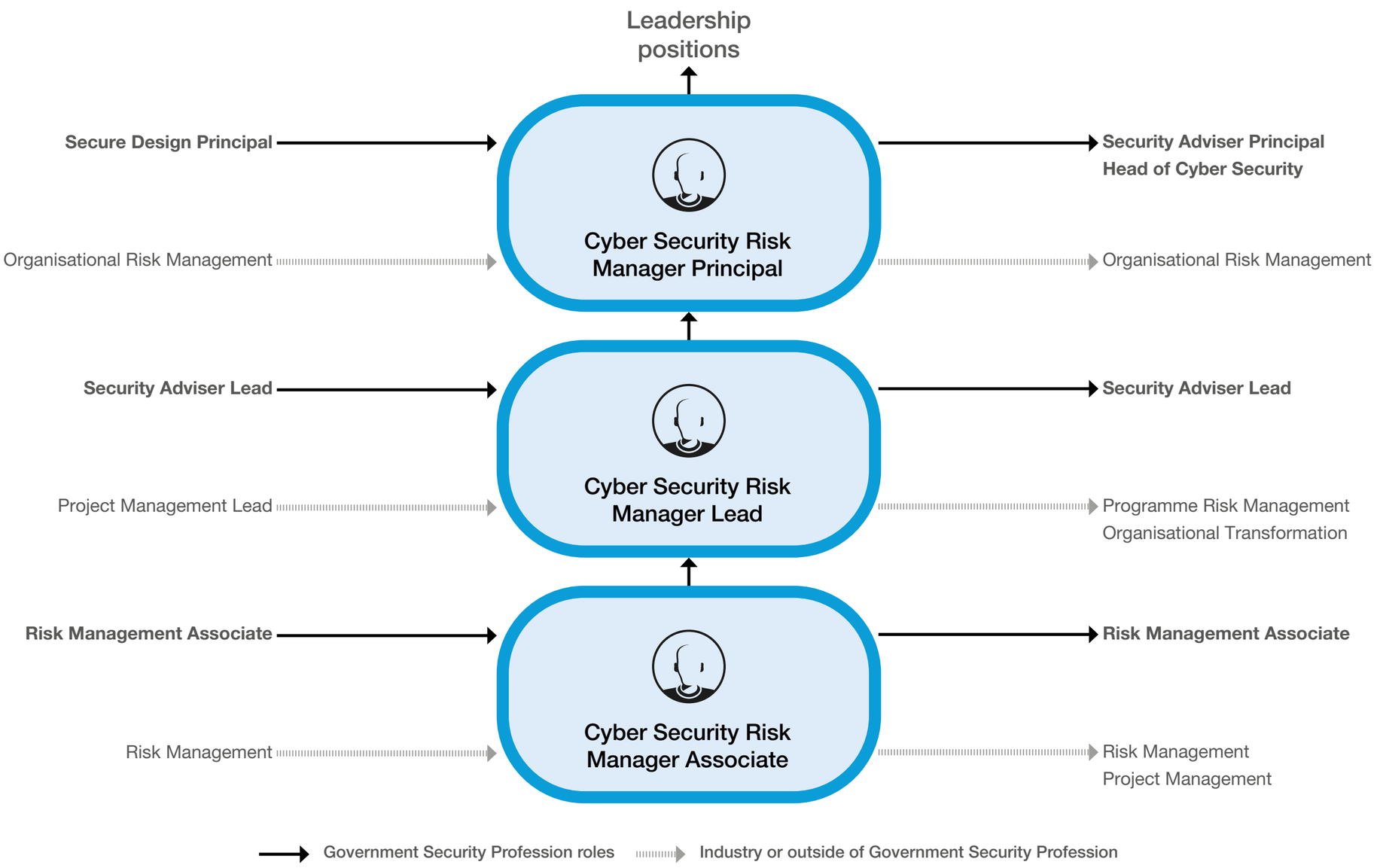
Minimum skill expectations

Skill	Role level		
	Security Architect Associate	Security Architect Lead	Security Architect Principal
	Skill level		
Security architecture	Working	Practitioner	Expert
Applied security capability	Working	Practitioner	Expert
Information risk assessment and risk management	Working	Practitioner	Practitioner
Protective security	Working	Working	Working
Threat understanding	Working	Working	Working

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Role	Role family	Security specialism
Cyber Security Risk Manager	Advisory	Cyber Security

Suggested entry and exit roles are indicative only and non-exhaustive



Role	Role family	Security specialism
Cyber Security Risk Manager Associate	Advisory	Cyber Security

Role summary

The Cyber Security Risk Manager identifies, understands and mitigates cyber-related risks. They provide risk or service owners with advice to help them make well informed risk-based decisions.

Typical role level expectations

- Work within established security and risk management governance structures, usually under supervision to support, review and undertake straightforward risk management activities such as:
  - helping with the analysis and derivation of business-supporting security needs
  - undertaking Cyber Security related risk assessments, basic threat assessments and other risk management activities
- Have an understanding of the applicability of appropriate legislation and regulations
- Provide advice to address identified Cyber Security related risks by applying of a variety of security capabilities, which may include using published guidance, standards or experts as appropriate
  - The scenarios will be straightforward, and the advice given will be proportionate and contextualised to the use case
- Provide straightforward advice to validate the effectiveness of risk mitigation measures, including an understanding of how to use different assurance activities (such as a pen test) and make recommendations for improvement
- Help risk or service owners to make decisions that are well informed by good and clear security advice, including contributing to reports or working within established reporting chains in a security team

Role	Role family	Security specialism
Cyber Security Risk Manager Associate	Advisory	Cyber Security

Entry route

Internal

Suitable for an individual from a role within the Government Security Profession or those with a clear interest and aptitude for technology and security risk management

External

Suitable for an individual who has worked in a Cyber Security risk management role in industry. More junior roles will be suitable for those with a clear interest and aptitude for technology and security risk management

Role	Role family	Security specialism
Cyber Security Risk Manager Lead	Advisory	Cyber Security

Role summary

The Cyber Security Risk Manager identifies, understands and mitigates cyber-related risks. They provide risk or service owners with advice to help them make well informed risk-based decisions.

Typical role level expectations

- Independently undertake risk management activities within a given area of practice or expertise, usually within established security and risk management governance structures
- Lead the analysis and derivation of business-supporting security needs, undertake Cyber Security related risk assessments, conduct tailored threat assessment and other risk management activities, and ensure activities are consistent with applicable regulations and legislation
- Provide tailored advice to a range of stakeholders on how to remedy identified risks by proportionately applying security capabilities, using published guidance, standards, and drawing on a range of experts as well as personal expertise
- Provide expert security advice that highlights Cyber Security related risks, so risk or service owners can make well-informed and auditable decisions

Entry route

Internal

Suitable for an individual from a role within the Government Security Profession or those with a clear interest and aptitude for technology and security risk management

External

Suitable for an individual who has worked in a Cyber Security risk management role in industry. More junior roles will be suitable for those with a clear interest and aptitude for technology and security risk management

Role	Role family	Security specialism
Cyber Security Risk Manager Principal	Advisory	Cyber Security

Role summary

The Cyber Security Risk Manager identifies, understands and mitigates cyber-related risks. They provide risk or service owners with advice to help them make well informed risk-based decisions.

Typical role level expectations

- Lead and undertake risk management activities against the hardest or most novel scenarios, while applying the fundamental principles of risk management to a range of complex scenarios, and lead regulatory or legislative compliance activities
- Guide and direct specialist activities of others, actively promoting development in the applicable skills, providing leadership to other risk managers, and sharing best practice widely across government, the public sector, and industry
- Lead the analysis and derivation of complex security needs
- Lead Cyber Security related risk assessments and other expert risk management activities, including providing guidance on establishing the organisation's Cyber Security-related governance arrangements
- Provide guidance to ensure ongoing confidence that fundamental organisational security needs have been met, including integrating a range of assurance approaches and techniques to give continued confidence to the risk, service or system owner
- Shape leadership decision-making through:
  - effective reporting and communication regarding the effectiveness of security processes across an organisation
  - providing recommendations to highly complex problems
  - acting as an SME for complex cyber risk management concerns, issues and problems

Role	Role family	Security specialism
Cyber Security Risk Manager Principal	Advisory	Cyber Security

Entry route

Internal

Suitable for an individual from a role within the Government Security Profession or those with a clear interest and aptitude for technology and security risk management

External

Suitable for an individual who has worked in a Cyber Security risk management role in industry. More junior roles will be suitable for those with a clear interest and aptitude for technology and security risk management

Role	Role family	Security specialism
Cyber Security Risk Manager	Advisory	Cyber Security

Minimum skill expectations

Skill	Skill level	Training	Success profiles
Information risk assessment and risk management	Practitioner	**Repository**	Making effective decisions*
Applied security capability	Practitioner	**Repository**	Changing and improving
Protective security	Working	**Repository**	Communicating and influencing
Threat understanding	Working	**Repository**	Delivering at pace
			Seeing the big picture

*Principal behaviour

Skill levels are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Development

Suggested training	Indicative professional qualifications/accreditations
• Technical Reconnect • Risk Reconnect • Cyber Security Development Programme • Threat awareness course • Information risk management course	• Membership of a relevant institution or body • Relevant industry qualifications and accreditations e.g. Cyber Security Professional, Certified Information Systems Security Professional, ISO27001 Lead Auditor • Relevant government qualifications or accreditations

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC

Role	Role family	Security specialism
Cyber Security Risk Manager	Advisory	Cyber Security

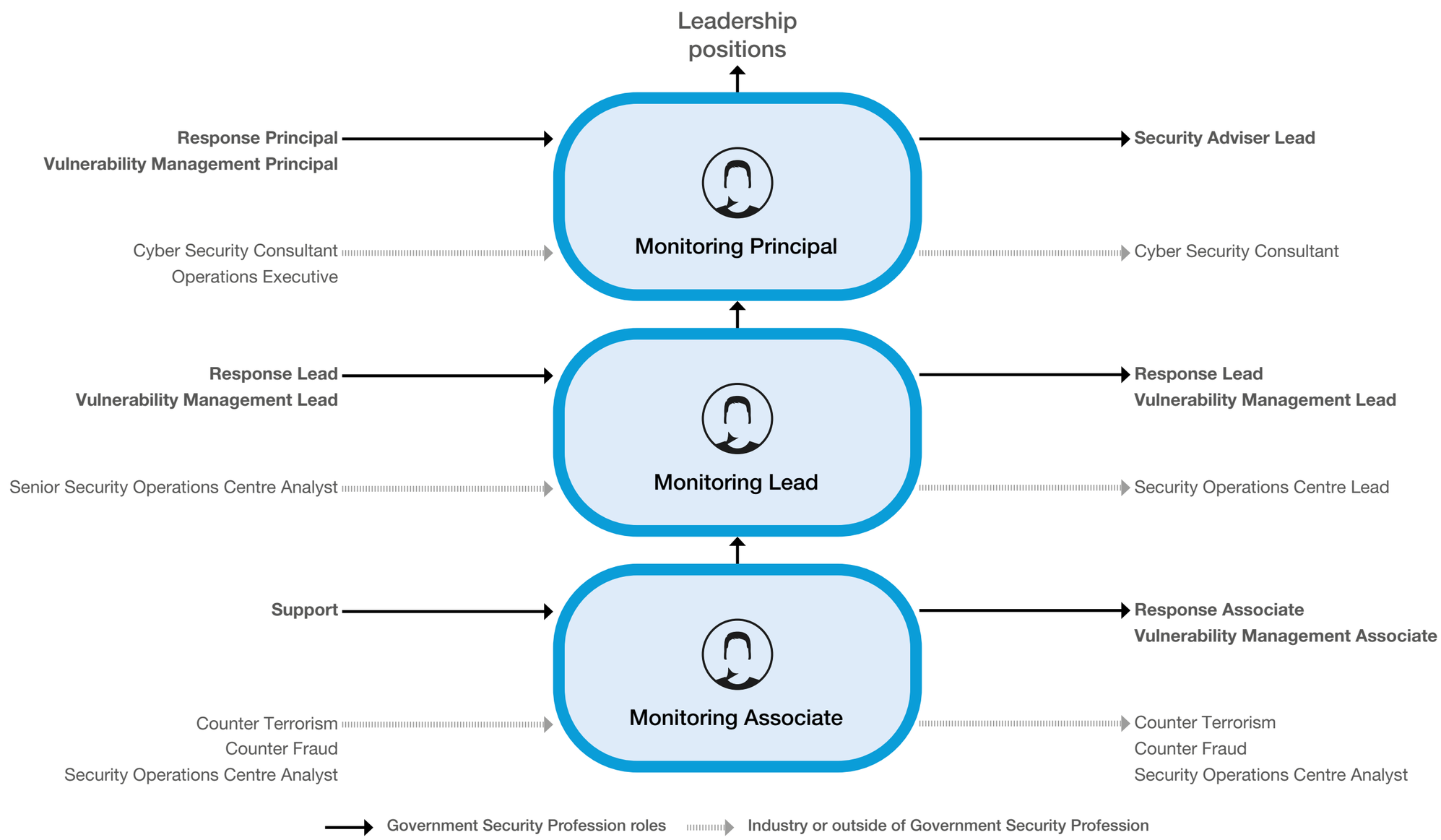
Minimum skill expectations

Skill	Role level		
	Risk Manager Associate	Risk Manager Lead	Risk Manager Principal
	Skill level		
Information risk assessment and risk management	Practitioner	Practitioner	Expert
Applied security capability	Practitioner	Practitioner	Practitioner
Protective security	Working	Practitioner	Expert
Threat understanding	Working	Practitioner	Practitioner

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Role	Role family	Security specialism
Monitoring	Operations	Cyber Security

Suggested entry and exit roles are indicative only and non-exhaustive



Role	Role family	Security specialism
Monitoring Associate	Operations	Cyber Security

Role summary

The role of Monitoring is to collect and analyse security event data arising from activity across the organisation, tune and improve rules generating security alerts, and follow up by investigating indicators of potentially malicious activity, escalating incidents or initiating responses.

Typical role level expectations

- Support implementation of the monitoring roadmap to enhance monitoring in line with requirements, policies and standards to govern all activities and outputs
- Monitor, triage and investigate security alerts on protective monitoring platforms to identify security incidents and perform analysis of security event data to support the response, reporting or escalating where appropriate
- Design, develop and support automated monitoring processes, using a variety of the latest SIEM (Security Information and Event Management) and network analysis tools, techniques and procedures to:
  - detect malicious activity
  - ensure continuous improvement through dashboard monitoring or retrospective assessment

Entry route

Internal

Suitable for an individual from the Government Security Profession, Digital, Data and Technology Profession, or Analytics Profession

External

Suitable for an individual who has worked as a Cyber Security intelligence analyst, monitoring specialist and/or response specialist, or in big data or data science, artificial intelligence or machine learning, or digital forensics, in the private sector

Role	Role family	Security specialism
Monitoring Lead	Operations	Cyber Security

Role summary

The role of Monitoring is to collect and analyse security event data arising from activity across the organisation, tune and improve rules generating security alerts, and follow up by investigating indicators of potentially malicious activity, escalating incidents or initiating responses.

Typical role level expectations

- Manage the implementation of the monitoring roadmap
- Support the shaping of the monitoring strategy, ensuring requirements, policies and standards to govern all activities and outputs are met
- Manage the monitoring, triaging, and investigation of security alerts on protective monitoring platforms to identify security incidents, and reviewing analysis of security event data to manage security incident response, reporting, or escalation where appropriate
- Lead small monitoring teams in the design, development and enablement of automated monitoring processes, recommending and implementing the latest SIEM (Security Information and Event Management) and network analysis tools, techniques and procedures to:
  - detect malicious activity
  - ensure continuous improvement through dashboard monitoring or retrospective assessment

Entry route

Internal

Suitable for an individual from the Government Security Profession, Digital, Data and Technology Profession, or Analytics Profession

External

Suitable for an individual who has worked as a Cyber Security intelligence analyst, monitoring specialist and/or response specialist, or in big data or data science, artificial intelligence or machine learning, or digital forensics, in the private sector

Role	Role family	Security specialism
Monitoring Principal	Operations	Cyber Security

Role summary

The role of Monitoring is to collect and analyse security event data arising from activity across the organisation, tune and improve rules generating security alerts, and follow up by investigating indicators of potentially malicious activity, escalating incidents or initiating responses.

Typical role level expectations

- Lead wider implementation of a monitoring strategy, ensuring roadmaps are achieved as expected, ensuring requirements, policies and standards to govern all activities and outputs are met
- Lead monitoring, triaging, and investigation of security alerts on protective monitoring platforms to identify security incidents
- Review high-priority or high-complexity analysis of security event data to manage security incident response, making key decisions on reporting or escalations for monitoring
- Lead large, cross-functional monitoring teams in the design, development and enablement of automated monitoring processes, advising on the latest SIEM (Security Information and Event Management) and network analysis tools, techniques and procedures to detect malicious activity, while communicating directly with leadership on the progress and status of monitoring

Entry route

Internal

Suitable for an individual from the Government Security Profession, Digital, Data and Technology Profession, or Analytics Profession

External

Suitable for an individual who has worked as a Cyber Security intelligence analyst, monitoring specialist and/or response specialist, or in big data or data science, artificial intelligence or machine learning, or digital forensics, in the private sector

Role	Role family	Security specialism
Monitoring	Operations	Cyber Security

Minimum skill expectations

Skill	Skill level	Training	Success profiles
Intrusion detection and analysis	Working	Repository	Delivering at pace*
Threat intelligence and threat assessment	Working	Repository	Changing and improving
Threat understanding	Working	Repository	Making effective decisions
Applied security capability	Awareness	Repository	Managing a quality service
Cyber Security operations	Awareness	Repository	Working together
Secure operations management	Awareness	Repository	
Protective security	Awareness	Repository	
Forensics	Awareness	Repository	
Information risk assessment and risk management	Awareness	Repository	

*Principal behaviour

Skill levels are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Development

Suggested training	Indicative professional qualifications/accreditations
• Continuous Monitoring course • Security Operations Centre course • Information risk management course • Threat awareness course • Threat intelligence course	• Membership of a relevant institution or body e.g. Institute of Information Security Professionals, Council for Registered Ethical Security Testers • Relevant industry qualifications and accreditations e.g. Certified Security Operations Centre Analyst • Relevant HM Government qualifications or accreditations

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC

Role	Role family	Security specialism
Monitoring	Operations	Cyber Security

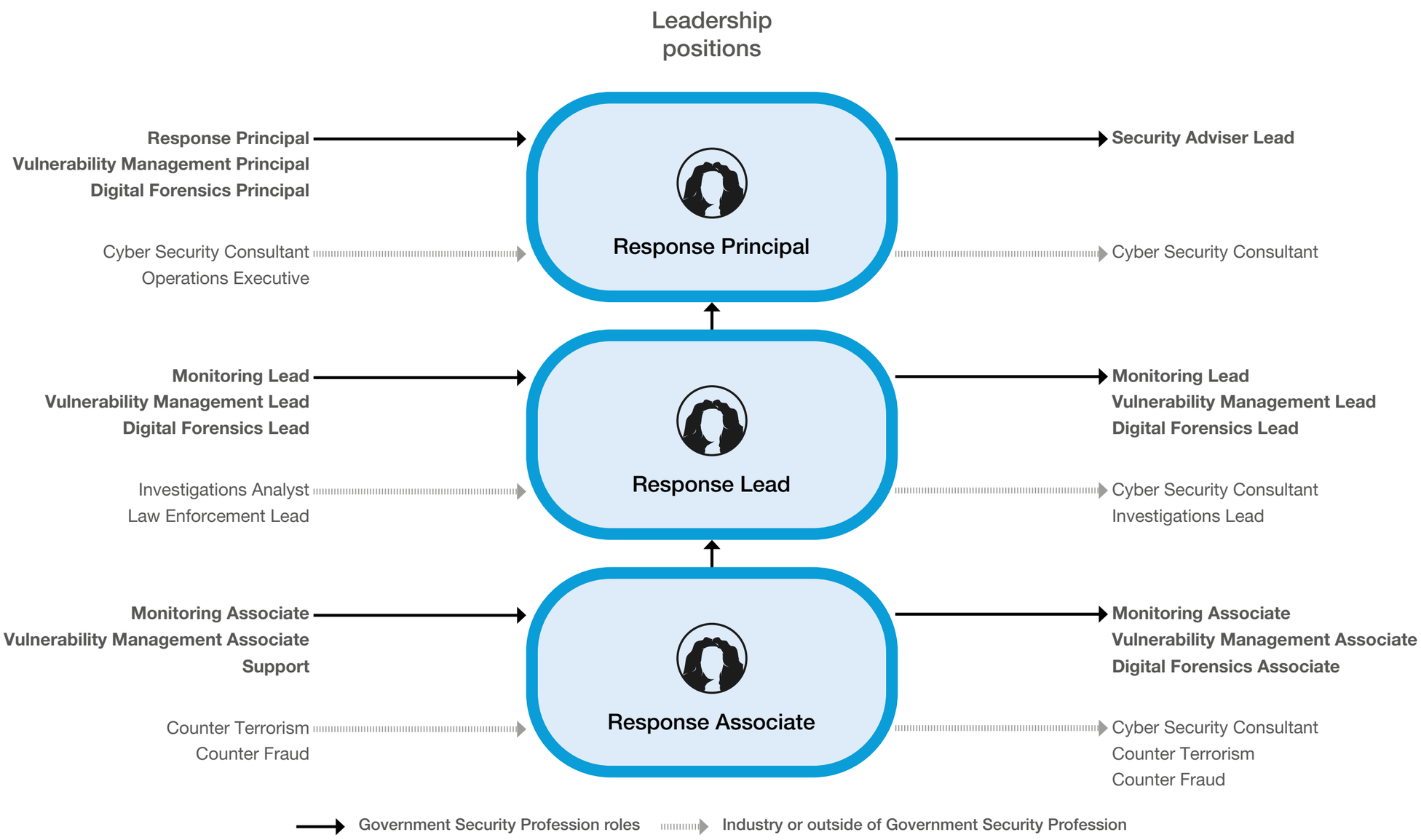
Minimum skill expectations

Skill	Role level		
	Monitoring Associate	Monitoring Lead	Monitoring Principal
	Skill level		
Intrusion detection and analysis	Working	Practitioner	Expert
Threat intelligence and threat assessment	Working	Practitioner	Practitioner
Threat understanding	Working	Practitioner	Practitioner
Cyber Security operations	Awareness	Working	Working
Secure operations management	Awareness	Working	Working
Protective security	Awareness	Awareness	Working
Forensics	Awareness	Awareness	Awareness
Information risk assessment and risk management	Awareness	Awareness	Awareness

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Role	Role family	Security specialism
Response	Operations	Cyber Security

Suggested entry and exit roles are indicative only and non-exhaustive



Role	Role family	Security specialism
Response Associate	Operations	Cyber Security

Role summary

The role of Response is to manage the response procedures and investigations of security events or incidents. Response colleagues must contain and remediate those incidents, identify potential process improvements, and maintain organisational readiness through preparedness exercises and co-ordinating red team activity. Response also advise product and service owners of potential mitigations.

Typical role level expectations

- Carry out an organisation's response policies and processes to meet the needs in line with appropriate standards
- Help conduct incident response exercises including scoping, design, and governance of red teaming and threat-hunting activity
- Communicate the results of investigations and risk mitigation outcomes, supporting an organisation to improve and maintain a robust response to new threats and attack vectors
- Conduct post-incident review, including root cause analysis, to feed back information and so improve monitoring
- Provide standardised advice on mitigation, escalating to a team leader where appropriate

Entry route

Internal

Suitable for an individual from the Government Security Profession, Digital, Data and Technology Profession, or Analytics Profession

External

Suitable for an individual who has worked as a Cyber Security intelligence analyst, or monitoring and response specialist, or in digital forensics, in the private or third sector

Role	Role family	Security specialism
Response Lead	Operations	Cyber Security

Role summary

The role of Response is to manage the response procedures and investigations of security events or incidents. Response colleagues must contain and remediate those incidents, identify potential process improvements, and maintain organisational readiness through preparedness exercises and co-ordinating red team activity. Response also advise product and service owners of potential mitigations.

Typical role level expectations

- Manage an organisation's response policies and processes to meet the needs in line with appropriate standards
- Manage incident response exercises and scoping, design and governance of red-teaming and threat-hunting activity
- Communicate the significance of the results of investigations and risk mitigation outcomes, guiding the organisation in the improvement and maintenance of a robust response to new threats and attack vectors
- Manage post-incident review, including root cause analysis, to feed back information and so improve monitoring
- Provide specialist, tailored advice on mitigation, handling escalations with risk and service owners as appropriate

Entry route

Internal

Suitable for an individual from the Government Security Profession, Digital, Data and Technology Profession, or Analytics Profession

External

Suitable for an individual who has worked as a Cyber Security intelligence analyst, or monitoring and response specialist, or in digital forensics, in the private or third sector

Role	Role family	Security specialism
Response Principal	Operations	Cyber Security

Role summary

The role of Response is to manage the response procedures and investigations of security events or incidents. Response colleagues must contain and remediate those incidents, identify potential process improvements, and maintain organisational readiness through preparedness exercises and co-ordinating red team activity. Response also advise product and service owners of potential mitigations.

Typical role level expectations

- Shape the entire organisation's response policies and processes to ensure that these meet the organisation's need, in line with appropriate standards
- Communicate with a broad range of senior stakeholders and be responsible for defining the vision, principles and strategy for incident response
- Aggregate and evaluate post-incident feedback to inform board-level reporting on security incidents
- Be a recognised expert and adviser to investigators and senior leadership across government

Entry route

Internal

Suitable for an individual from the Government Security Profession, Digital, Data and Technology Profession, or Analytics Profession

External

Suitable for an individual who has worked as a Cyber Security intelligence analyst, monitoring and response specialist or digital forensics, in the private or third sector

Role	Role family	Security specialism
Response	Operations	Cyber Security

Minimum skill expectations

Skill	Skill level	Training	Success profiles
Incident management, incident investigation and response	Practitioner	**Repository**	Making effective decisions*
Information risk assessment and risk management	Practitioner	**Repository**	Changing and improving
Intrusion detection and analysis	Working	**Repository**	Communicating and influencing
Threat intelligence and threat assessment	Working	**Repository**	Delivering at pace
Applied security capability	Awareness	**Repository**	Leadership
Protective security	Awareness	**Repository**	Managing a quality service
Threat understanding	Awareness	**Repository**	

*Principal behaviour

Skill levels are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Development

Suggested training	Indicative professional qualifications/accreditations
• Incident response and planning course • Threat hunting course • Advanced threat methodologies course • Information risk management course • Threat awareness course	• Membership of a relevant institution or body e.g. Institute of Information Security Professionals • Relevant industry qualifications or accreditations, e.g. Offensive Security Certified Professional, Certified Information Security Management Principles, Certified Information Systems Security Professional

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC

Role	Role family	Security specialism
Response	Operations	Cyber Security

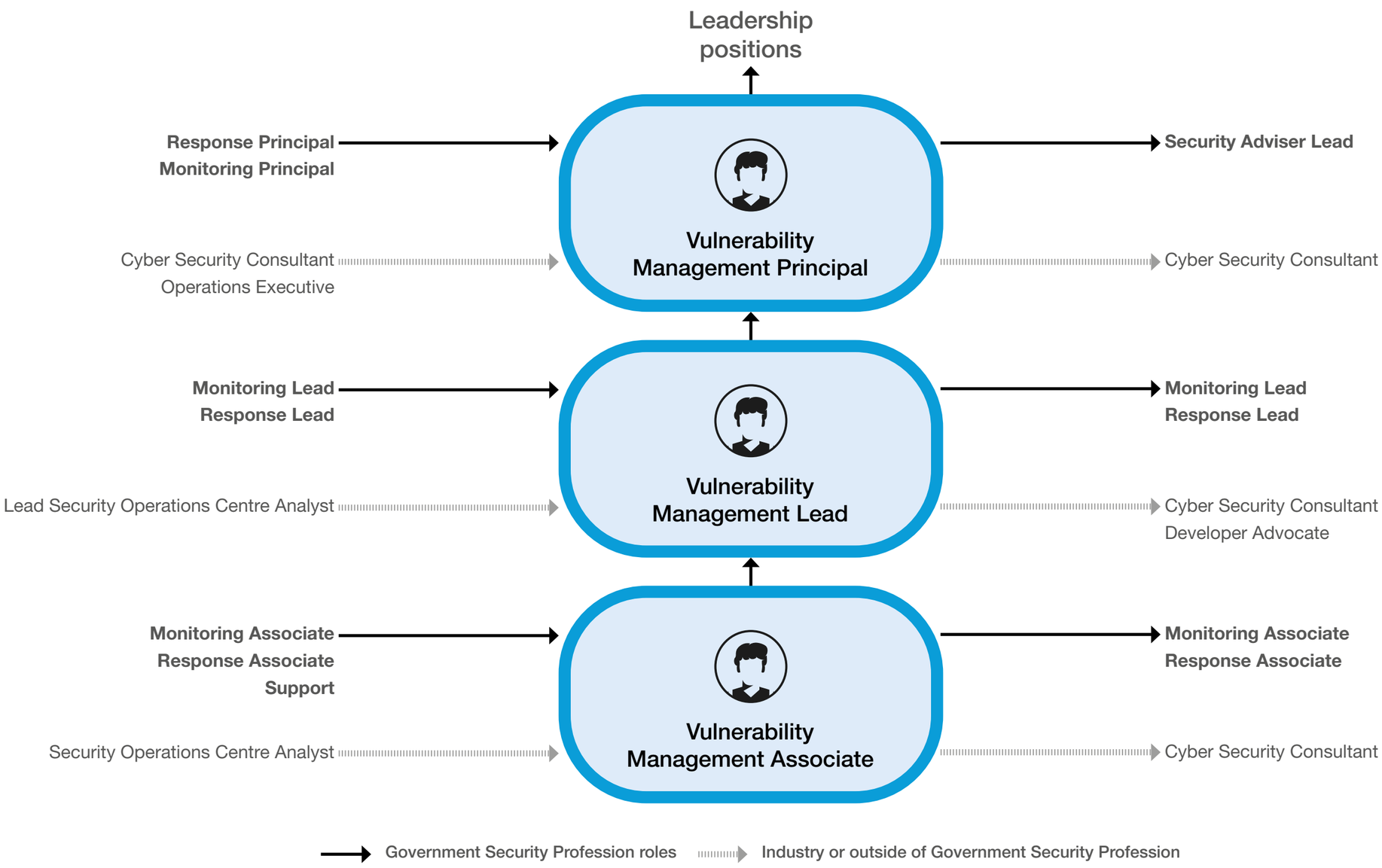
Minimum skill expectations

Skill	Role level		
	Response Associate	Response Lead	Response Principal
	Skill level		
Incident management, incident investigation and response	Practitioner	Practitioner	Expert
Information risk assessment and risk management	Practitioner	Practitioner	Practitioner
Intrusion detection and analysis	Working	Practitioner	Expert
Threat intelligence and threat assessment	Working	Practitioner	Practitioner
Applied security capability	Awareness	Working	Working
Protective security	Awareness	Awareness	Awareness
Threat understanding	Awareness	Awareness	Awareness

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Role	Role family	Security specialism
Vulnerability Management	Operations	Cyber Security

Suggested entry and exit roles are indicative only and non-exhaustive



Role	Role family	Security specialism
Vulnerability Management Associate	Operations	Cyber Security

Role summary

The role of Vulnerability Management is to triage vulnerabilities by relevance and criticality to the organisation. Vulnerability Management then identify mitigations for those vulnerabilities and advise on implementing them.

Typical role level expectations

- Analyse complex information systems to understand the associated Cyber Security risks, audit requirements, and data value
- Support the creation and implementation of vulnerability assessments of enterprise assets to a predefined scope and schedule using predetermined templates and test scripts, including but not limited to:
  - application vulnerability assessments
  - infrastructure vulnerability assessments
- Assist in the prioritisation of those vulnerabilities through a risk-based approach
- Triage and prioritise vulnerabilities, implement mitigating measures, and support in the life cycle of vulnerability management, providing standardised advice on ways to improve control mechanisms and mitigate risk
- Collaborate with stakeholders to manage vulnerabilities and undertake remediation activities
- Communicate common mitigation strategies such as patching and basic configuration change (system hardening)
- Understand how local protective security measures can be applied to reduce vulnerability exposure
- Demonstrate knowledge of common approaches and tooling to perform vulnerability assessment and to validate system configuration
- Perform vulnerability assessments of enterprise assets with limited supervision to a predefined scope and schedule using predetermined templates and test scripts
- Develop and implement schedules for performing vulnerability assessments to meet organisational objectives and compliance requirements

Role	Role family	Security specialism
Vulnerability Management Associate	Operations	Cyber Security

Entry route

Internal

Suitable for an individual from the Government Security Profession, Digital, Data and Technology Profession, or Analytics Profession

External

Suitable for an individual who has worked in penetration testing, application security and development security operations in the private sector

Role	Role family	Security specialism
Vulnerability Management Lead	Operations	Cyber Security

Role summary

The role of Vulnerability Management is to triage vulnerabilities by relevance and criticality to the organisation. Vulnerability Management then identify mitigations for those vulnerabilities and advise on implementing them.

Typical role level expectations

- Manage complex information systems to understand and prioritise actions on Cyber Security risks, audit requirements and data value, and provide guidance to vulnerability management team members
- Manage the creation and implementation and lead development of vulnerability assessments for IT estates, including but not limited to application vulnerability assessments and infrastructure vulnerability assessments
- Drive prioritisation of those vulnerabilities through a risk-based approach, to meet common organisational objectives such as regulatory compliance and audit functions
- Manage the triage of vulnerabilities, ensuring mitigation measures are implemented, and managing the life cycle of vulnerability management for a set of assets, providing tailored advice on ways to improve control mechanisms and mitigate risks
- Recommend remediation strategies and provide advice on complex configuration changes in support of vulnerability remediation
- Proactively identify and leverage threat intelligence sources to inform strategic vulnerability mitigation measures
- Manage collaboration with stakeholders to create tactical plans relating to managing vulnerabilities, and oversee subsequent activities
- Demonstrate developed knowledge and understanding of approaches and tooling for performing vulnerability assessment against large and complex infrastructure
- Validate system configuration across multiple and complex interlinking systems
- Translate vulnerability management standards and best practice into organisation-specific policies, procedures and guidelines and champion standards and best practice outside security functions
- Explain the need for effective vulnerability management processes and implications of poor performances
- Lead development and implementation of effective vulnerability management programs across the enterprise to meet organisational and regulatory and compliance requirements
- Develop vulnerability assessment templates and test scripts to meet common organisational objectives such as regulatory compliance and internal audit functions

Role	Role family	Security specialism
Vulnerability Management Lead	Operations	Cyber Security

Entry route

Internal

Suitable for an individual from the Government Security Profession, Digital, Data and Technology Profession, or Analytics Profession

External

Suitable for an individual who has worked in penetration testing, application security and development security operations in the private sector

Role	Role family	Security specialism
Vulnerability Management Principal	Operations	Cyber Security

Role summary

The role of Vulnerability Management is to triage vulnerabilities by relevance and criticality to the organisation. Vulnerability Management then identify mitigations for those vulnerabilities and advise on implementing them.

Typical role level expectations

- Lead complex information systems to understand and prioritise actions on Cyber Security risks, audit requirements and data value, and provide specialist or complex guidance to vulnerability management teams and external senior stakeholders
- Lead the development and implementation of multiple vulnerability assessments and enterprise-wide scanning strategies across multiple complex environments, while leading in prioritising those vulnerabilities through a risk-based approach
- Lead the triage of vulnerabilities, ensuring mitigation measures are implemented, and oversee the life cycle of vulnerability management for a set of assets, providing tailored specialist or complex advice on ways to improve control mechanisms and mitigate risks
- Lead senior stakeholder engagement across government to create strategic plans for managing vulnerabilities and remediation activities
- Create organisational principles and vision that will provide the basis for triaging vulnerabilities
- Provide advice to senior leadership on ways to improve control mechanisms, identify, evaluate, and mitigate risks
- Develop bespoke templates and test scripts to meet uncommon or complex organisational objectives
- Set the organisation’s vulnerability management strategy including people, process and technology elements
- Ensure organisation-specific vulnerability management policies, procedures and guidelines are aligned with organisational objectives and risk appetite
- Set direction and approve investment in strategic tooling and capability to address strategic enterprise-wide risk
- Develop bespoke templates and test scripts to meet uncommon or complex organisational objectives

Role	Role family	Security specialism
Vulnerability Management Principal	Operations	Cyber Security

Entry route

Internal

Suitable for an individual from the Government Security Profession, Digital, Data and Technology Profession, or Analytics Profession

External

Suitable for an individual who has worked in penetration testing, application security or development security operations in the private sector

Role	Role family	Security specialism
Vulnerability Management	Operations	Cyber Security

Minimum skill expectations

Skill	Skill level	Training	Success profiles
Penetration testing	Working	**Repository**	Making effective decisions*
Information risk assessment and risk management	Working	**Repository**	Changing and improving
Threat intelligence and threat assessment	Working	**Repository**	Delivering at pace
Cyber Security operations	Working	**Repository**	Managing a quality service
Threat understanding	Working	**Repository**	Seeing the big picture
Legal and regulatory environment and compliance	Awareness	**Repository**	
Protective security	Awareness	**Repository**	

*Principal behaviour

Skill levels are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Development

Suggested training	Indicative professional qualifications/accreditations
• Vulnerability management course • Secure evaluation and testing course • Threat awareness course • Advanced threat methodologies course • Information risk management course	• Membership of a relevant institution or body e.g. Institute of Information Security Professionals • Relevant industry qualifications and accreditations e.g. Certified Information Security Management Principles, Certified Information Systems Security Professional • Relevant HM Government qualifications and accreditations

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC

Role	Role family	Security specialism
Vulnerability Management	Operations	Cyber Security

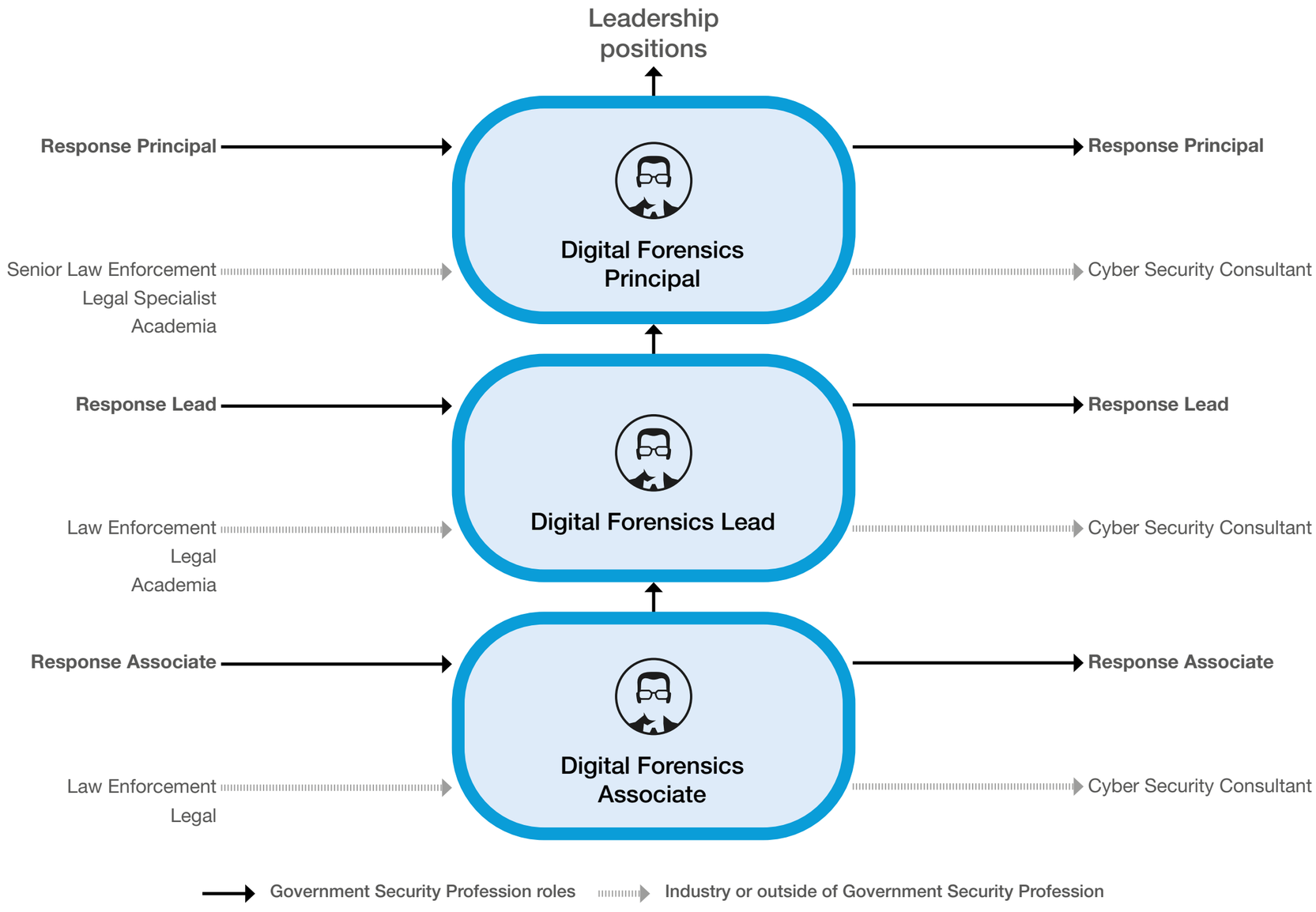
Minimum skill expectations

Skill	Role level		
	Vulnerability Management Associate	Vulnerability Management Lead	Vulnerability Management Principal
	Skill level		
Penetration testing	Working	Practitioner	Expert
Information risk assessment and risk management	Working	Practitioner	Practitioner
Threat intelligence and threat assessment	Working	Practitioner	Practitioner
Cyber Security operations	Working	Practitioner	Practitioner
Threat understanding	Working	Practitioner	Practitioner
Legal and regulatory environment and compliance	Awareness	Awareness	Awareness
Protective security	Awareness	Awareness	Awareness

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Role	Role family	Security specialism
Digital Forensics	Operations	Cyber Security

Suggested entry and exit roles are indicative only and non-exhaustive



Role	Role family	Security specialism
Digital Forensics Associate	Operations	Cyber Security

Role summary

The role of Digital Forensics is to scope, co-ordinate and undertake forensic activity to gather forensic evidence from devices, systems and the internet in compliance with law and organisational investigation requirements.

Typical role level expectations

- Conduct forensic activity using specialist equipment as appropriate, following the relevant organisational processes
- Work with specialist forensic personnel or a wider team to support the digital aspects of their investigation
- Support the application of forensic readiness policy and work with other teams to ensure its implementation
- Analyse evidence to identify breaches of policy, regulation or law
- Present evidence as appropriate, acting as an expert witness if necessary

Entry route

Internal

Suitable for an individual from the Government Security Profession, Digital, Data and Technology Profession, or Analytics Profession

External

Suitable for an individual who has worked in digital forensics in the private sector

Role	Role family	Security specialism
Digital Forensics Lead	Operations	Cyber Security

Role summary

The role of Digital Forensics is to scope, co-ordinate and undertake forensic activity to gather forensic evidence from devices, systems and the internet in compliance with law and organisational investigation requirements.

Typical role level expectations

- Assess the need for (and co-ordinate) forensic activity within the overall response initiative, including managing a team, ensuring that forensic services are deployed appropriately
- Manage forensic readiness policy and work with other teams to ensure appropriate implementation
- Co-ordinate team scene investigation and capture evidence in accordance with legal guidelines to minimise disruption to the business and preserve evidentiary integrity, using specialist equipment as appropriate
- Review evidence to identify breaches of policy, regulation or law
- Present evidence as appropriate, acting as an expert witness if necessary

Entry route

Internal

Suitable for an individual from the Government Security Profession, Digital, Data and Technology Profession, or Analytics Profession

External

Suitable for an individual who has worked in digital forensics in the private sector

Role	Role family	Security specialism
Digital Forensics Principal	Operations	Cyber Security

Role summary

The role of Digital Forensics is to scope, co-ordinate and undertake forensic activity to gather forensic evidence from devices, systems and the internet in compliance with law and organisational investigation requirements.

Typical role level expectations

- Define and lead digital forensics strategy through the assessment and communication of forensic requirements within an organisation
- Define the organisational approach to evidence capture in line with legal guidelines, to minimise disruption to the business and preserve evidentiary integrity, using specialist equipment as appropriate
- Lead forensic readiness policy and guide teams to ensure its implementation
- Provide thought leadership and deliver specialist advice to others within and beyond the organisation
- Present evidence as appropriate, acting as an expert witness if necessary

Entry route

Internal

Suitable for an individual from the Government Security Profession, Digital, Data and Technology Profession, or Analytics Profession

External

Suitable for an individual who has worked in digital forensics in the private sector

Role	Role family	Security specialism
Digital Forensics	Operations	Cyber Security

Minimum skill expectations

Skill	Skill level	Training	Success profiles
Forensics	Working	**Repository**	Making effective decisions*
Intrusion detection and analysis	Working	**Repository**	Changing and improving
Information risk assessment and risk management	Working	**Repository**	Delivering at pace
Threat intelligence and threat assessment	Working	**Repository**	Managing a quality service
Threat understanding	Working	**Repository**	Seeing the big picture
Legal and regulatory environment and compliance	Awareness	**Repository**	
Protective security	Awareness	**Repository**	

*Principal behaviour

Skill levels are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Development

Suggested training	Indicative professional qualifications/accreditations
• Digital Forensic Analysis course (Windows, Mac, iOS) • Threat detection course • Information risk management course • Threat awareness course	• Membership of a relevant institution or body e.g. Institute of Information Security Professionals • Relevant industry qualifications and accreditations e.g. Certified Information Security Management Principles, Certified Information Systems Security Professional • Relevant HM Government qualifications and accreditations

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC

Role	Role family	Security specialism
Digital Forensics	Operations	Cyber Security

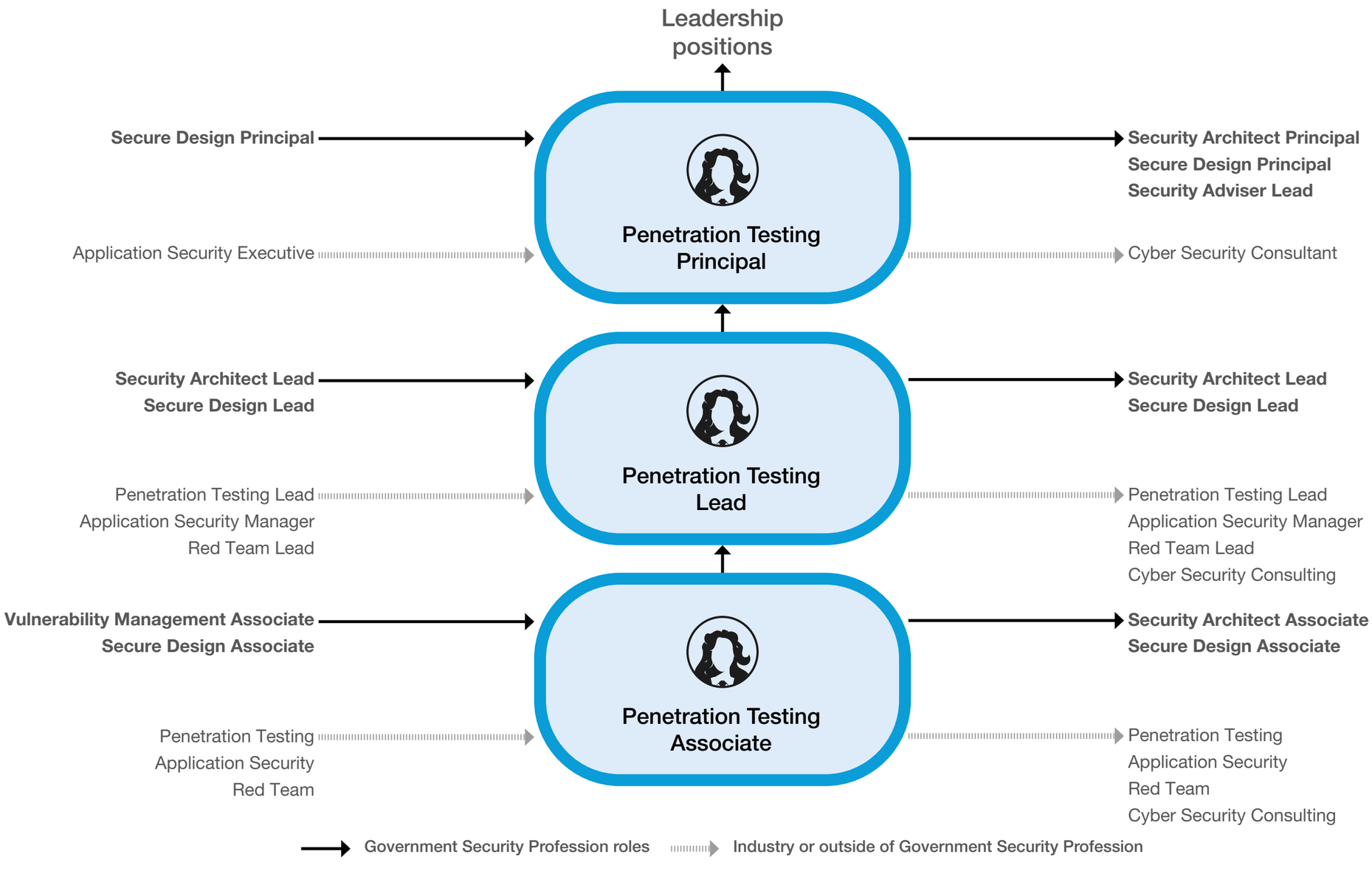
Minimum skill expectations

Skill	Role level		
	Digital Forensics Associate	Digital Forensics Lead	Digital Forensics Principal
	Skill level		
Forensics	Working	Practitioner	Expert
Intrusion detection and analysis	Working	Practitioner	Expert
Information risk assessment and risk management	Working	Practitioner	Practitioner
Threat intelligence and threat assessment	Working	Practitioner	Practitioner
Threat understanding	Working	Practitioner	Practitioner
Legal and regulatory environment and compliance	Awareness	Awareness	Awareness
Protective security	Awareness	Awareness	Awareness

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Role	Role family	Security specialism
Penetration Testing	Research, development and design	Cyber Security

Suggested entry and exit roles are indicative only and non-exhaustive



Role	Role family	Security specialism
Penetration Testing Associate	Research, development and design	Cyber Security

Role summary

Penetration Testing provides Cyber Security assurance by attempting to penetrate existing defences, to feed back on potential vulnerabilities (whether in a system, an application or across the entire IT estate) and co-ordinate the production of a remediation action plan.

Typical role level expectations

- Support the scoping, conducting and procurement of penetration tests, red team exercises, vulnerability assessments of IT assets, and other tests to assess the robustness of a system, product or technology
- Disseminate the implications of test findings, relaying the potential business impact if vulnerabilities are exploited
- Engage with internal and external stakeholders to provide appropriate Cyber Security assurance in accordance with policy and regulations
- Report potential issues and mitigation options to appropriate stakeholders or governance forums
- Contribute to the review and interpretation of reports and contribute to remediation action plan production

Entry route

Internal

Suitable for an individual from the Government Security Profession, Digital, Data and Technology Profession, or Analytics Profession

External

Suitable for an individual who has worked in penetration testing or application security

Role	Role family	Security specialism
Penetration Testing Lead	Research, development and design	Cyber Security

Role summary

Penetration Testing provides Cyber Security assurance by attempting to penetrate existing defences, to feed back on potential vulnerabilities (whether in a system, an application or across the entire IT estate) and co-ordinate the production of a remediation action plan.

Typical role level expectations

- Scope, conduct and procure penetration tests, red team exercises, vulnerability assessments of IT assets, and other tests to assess the robustness of a system, product or technology
- Disseminate the implications of test findings and explain the potential business impact if vulnerabilities are exploited
- Co-ordinate engagement with internal and external stakeholders to manage and provide appropriate Cyber Security assurance to the required standard and in accordance with policy and regulations
- Advise on potential issues and mitigation options to appropriate stakeholders or governance forums
- Review and interpret reports and co-ordinate and manage remediation action plan production

Entry route

Internal

Suitable for an individual from the Government Security Profession, Digital, Data and Technology Profession, or Analytics Profession

External

Suitable for an individual who has worked in penetration testing or application security

Role	Role family	Security specialism
Penetration Testing Principal	Research, development and design	Cyber Security

Role summary

Penetration Testing provides Cyber Security assurance by attempting to penetrate existing defences, to feed back on potential vulnerabilities (whether in a system, an application or across the entire IT estate) and co-ordinate the production of a remediation action plan.

Typical role level expectations

- Lead large-scale, cross-functional or highly complex penetration tests, red team exercises, vulnerability assessments of IT assets, and other tests to assess the robustness of a system, product or technology
- Disseminate the implications of test findings and explain the potential business impact if vulnerabilities are exploited to senior level leadership across government
- Lead engagement with senior internal and external stakeholders to manage and provide appropriate Cyber Security assurance to the required standard and in accordance with policy and regulations
- Advise on complex issues and mitigation options to appropriate stakeholders or governance forums, acting as an SME across government, the public sector, and industry
- Be the key decision maker on reports, overseeing the remediation of vulnerabilities post-penetration testing

Entry route

Internal

Suitable for an individual from the Government Security Profession, Digital, Data and Technology Profession, or Analytics Profession

External

Suitable for an individual who has worked in penetration testing or application security

Role	Role family	Security specialism
Penetration Testing	Research, development and design	Cyber Security

Minimum skill expectations

Skill	Skill level	Training	Success profiles
Penetration testing	Working	**Repository**	Managing a quality service*
Information risk assessment and risk management	Working	**Repository**	Changing and improving
Protective security	Awareness	**Repository**	Communicating and influencing
Threat understanding	Awareness	**Repository**	Delivering at pace
			Making effective decisions
			Seeing the big picture
			Working together

*Principal behaviour

Skill levels are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Development

Suggested training	Indicative professional qualifications/accreditations
• Penetration testing, tools and techniques course • Red teaming course • Threat awareness course • Information risk management course	• Membership of a relevant institution or body, e.g. Institute of Information Security Professionals, Council for Registered Ethical Security Testers • Relevant industry qualifications and accreditations e.g. Offensive Security Certified Professional, Certified Information Systems Security Professional, Tigerscheme

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC

Role	Role family	Security specialism
Penetration Testing	Research, development and design	Cyber Security

Minimum skill expectations

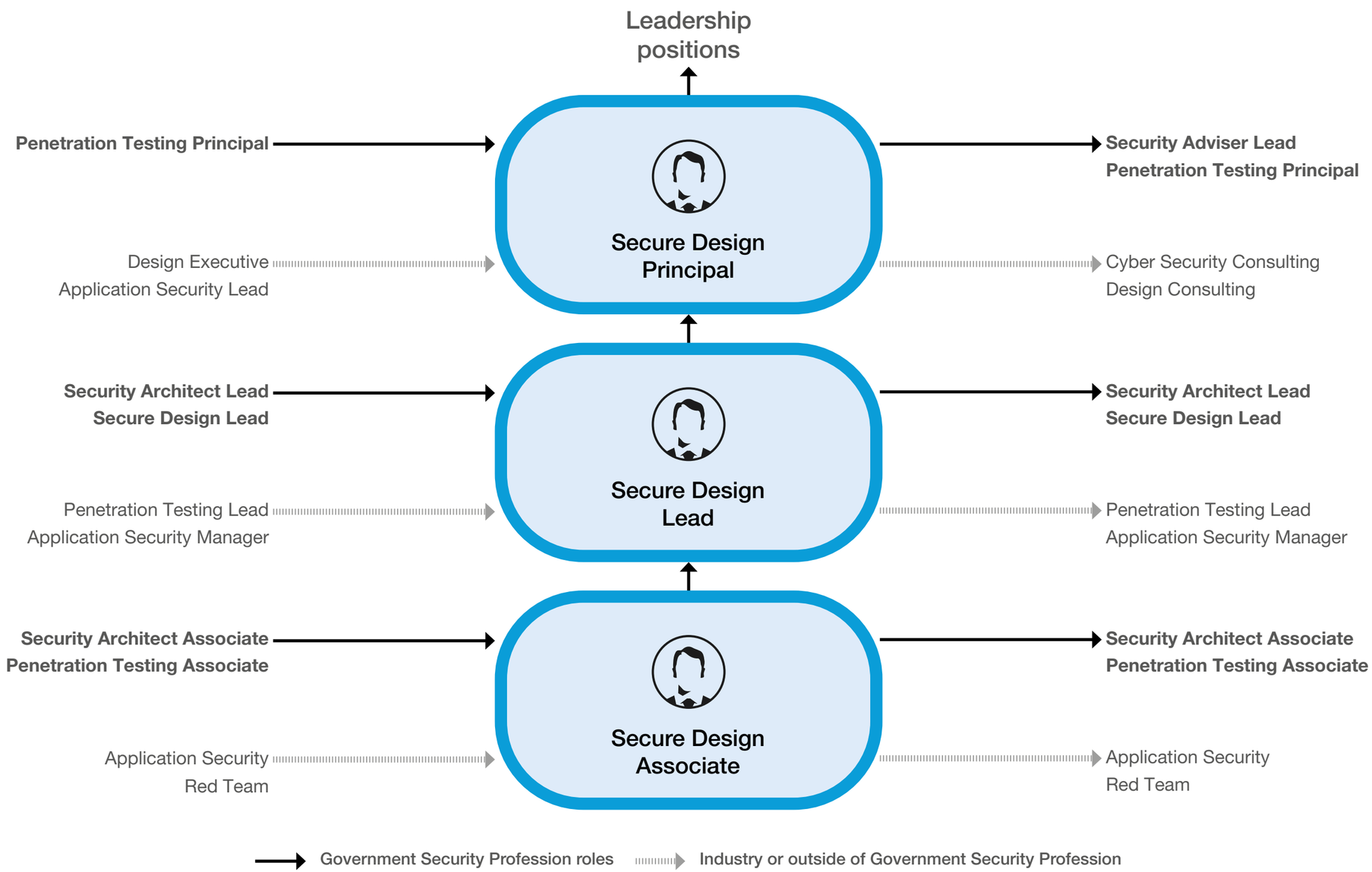
Skill	Role level		
	Penetration Testing Associate	Penetration Testing Lead	Penetration Testing Principal
	Skill level		
Penetration testing	Working	Practitioner	Expert
Information risk assessment and risk management	Working	Practitioner	Expert
Protective security	Awareness	Working	Practitioner
Threat understanding	Awareness	Working	Practitioner

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

amework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC

Role	Role family	Security specialism
Secure Design	Research, development and design	Cyber Security

Suggested entry and exit roles are indicative only and non-exhaustive



Role	Role family	Security specialism
Secure Design Associate	Research, development and design	Cyber Security

Role summary

The role of Secure Design covers testing or assurance to ensure that security is embedded in all stages of the application development life cycle, and that there is continuous monitoring through use. Roles in this area will also advise on and test the efficacy of measures to build security into continuous integration and deployment pipelines.

Typical role level expectations

- Embed ‘secure by design’ principles into application development, integrating security tools, standards, and processes into product life cycles
- Support the assessment of application resilience throughout an IT estate, generating regular application security reports to provide information about statistics and trends
- Follow processes, provide standardised advice on tooling for, and conduct dynamic and static analysis in the product development life cycle
- Work with development teams to embed secure development life cycle and security awareness, and ensure appropriate tools and skills exist

Entry route

Internal

Suitable for an individual from the Government Security Profession, Digital, Data and Technology Profession, or Analytics Profession

External

Suitable for an individual who has worked in penetration testing, application security or development security operations

Role	Role family	Security specialism
Secure Design Lead	Research, development and design	Cyber Security

Role summary

The role of Secure Design covers testing or assurance to ensure that security is embedded in all stages of the application development life cycle, and that there is continuous monitoring through use. Roles in this area will also advise on and test the efficacy of measures to build security into continuous integration and deployment pipelines.

Typical role level expectations

- Manage the embedment of ‘secure by design’ principles into application development by providing specialist internal consultancy and integrating security tools, standards, and processes into product life cycles
- Manage the assessment of application resilience throughout an IT estate, reviewing regular application security reports, and prioritising based on risk appetite and business requirements
- Manage processes, provide tailored advice on tooling for, and conduct dynamic and static analysis in the product development life cycle
- Ensure appropriate channels for vulnerability disclosure exist in line with policy, and any bounty programme is effectively managed to ensure identified vulnerabilities are quickly remediated

Entry route

Internal

Suitable for an individual from the Government Security Profession, Digital, Data and Technology Profession, or Analytics Profession

External

Suitable for an individual who has worked in penetration testing, application security or development security operations

Role	Role family	Security specialism
Secure Design Principal	Research, development and design	Cyber Security

Role summary

The role of Secure Design covers testing or assurance to ensure that security is embedded in all stages of the application development life cycle, and that there is continuous monitoring through use. Roles in this area will also advise on and test the efficacy of measures to build security into continuous integration and deployment pipelines.

Typical role level expectations

- Lead the embedment of ‘secure by design’ principles into application development by providing advice and internal consultancy on highly complex criteria and contexts
- Lead multi-team assessment of application resilience throughout an IT estate, reviewing regular application security reports, holding accountability and responsibility for secure design implementation
- Lead and assure processes, and provide SME thought leadership on tooling and dynamic and static analysis in the product development life cycle
- Lead development teams alongside senior cross-government decision makers to embed secure development life cycle and security awareness, and ensure appropriate tools and skills exist

Entry route

Internal

Suitable for an individual from the Government Security Profession, Digital, Data and Technology Profession, or Analytics Profession

External

Suitable for an individual who has worked in penetration testing, application security or development security operations

Role	Role family	Security specialism
Secure Design	Research, development and design	Cyber Security

Minimum skill expectations

Skill	Skill level	Training	Success profiles
Secure design	Working	**Repository**	Delivering at pace*
Secure development	Working	**Repository**	Changing and improving
Information risk assessment and risk management	Working	**Repository**	Communicating and influencing
Threat understanding	Awareness	**Repository**	Making effective decisions
Protective security	Awareness	**Repository**	Seeing the big picture
			Working together

*Principal behaviour

Skill levels are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Development

Suggested training	Indicative professional qualifications/accreditations
• Secure design course • Application security course • Web applications, services and servers security course • Information risk management course • Threat awareness course	• Membership of a relevant institution or body, e.g. British Computer Society, Institute of Engineering and Technology, Council for Registered Ethical Security Testers • Relevant industry qualifications or accreditations, e.g. Offensive Security Certified Professional, Certified Information Systems Security Professional, Tigerscheme

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC

Role	Role family	Security specialism
Secure Design	Research, development and design	Cyber Security

Minimum skill expectations

Skill	Role level		
	Secure Design Associate	Secure Design Lead	Secure Design Principal
	Skill level		
Secure design	Working	Practitioner	Expert
Secure development	Working	Practitioner	Expert
Information risk assessment and risk management	Working	Working	Working
Threat understanding	Awareness	Working	Practitioner
Protective security	Awareness	Awareness	Awareness

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Technical Security – role families and roles

Technical Security holistically protects sensitive information and technology from close access acquisition or exploitation by hostile actors, as well as any other forms of technical manipulation.

Advisory


Head of Technical Security


Adviser


Assurance


Asset and Service Life Cycle Security Management

Operations


Operations Manager


Investigator


Installer

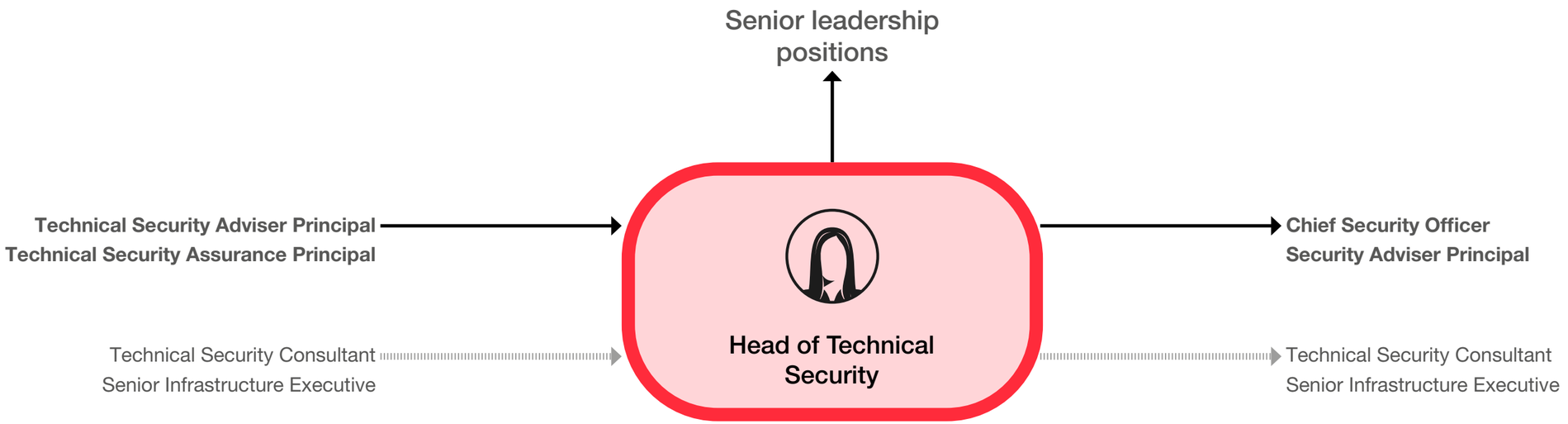
Research, development and design


Applied Research


Designer

Role	Role family	Security specialism
Head of Technical Security	Advisory	Technical Security

Suggested entry and exit roles are indicative only and non-exhaustive



Role	Role family	Security specialism
Head of Technical Security	Advisory	Technical Security

Role summary

The Head of Technical Security is responsible for the Technical Security specialism. They anticipate challenges, provide strategic direction, drive performance and build the capability required to ensure the security of new and existing services.

Typical role level expectations

- Be the primary point of contact on Technical Security issues with key stakeholders, including external parties, and actively develop strong working relationships in relation to Technical Security
- Ensure that the Technical Security policies and security controls remain appropriate and proportionate to the assessed risks, and are responsive and adaptable to the changing threat environment, business requirements and government policies
- Champion learning, development and accreditation, cultivate talent and foster an inclusive, diverse and motivated workforce
- Work with the heads of specialism to promote cross-government security mindedness
- Influence, change and impact decisions with both internal and external stakeholders
- Promote the Technical Security specialism and advise on Technical Security risks
- Work with industry, including security manufacturers and security consultants, to drive best practice
- Drive professional development by working with the Government Security Function to set and drive continuous learning standards

Entry route

Internal

Suitable for an individual from the Government Security Profession

External

Suitable for an individual from a senior management position in the private sector

Role	Role family	Security specialism
Head of Technical Security	Advisory	Technical Security

Minimum skill expectations

Skill	Skill level	Training	Success profiles
Applied Technical Security	Expert	**Repository**	Leadership*
Protective security	Working	**Repository**	Communicating and influencing
Risk understanding and mitigation	Awareness	**Repository**	Developing self and others
Threat understanding	Awareness	**Repository**	Seeing the big picture
			Working together

*Principal behaviour

Skill levels are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

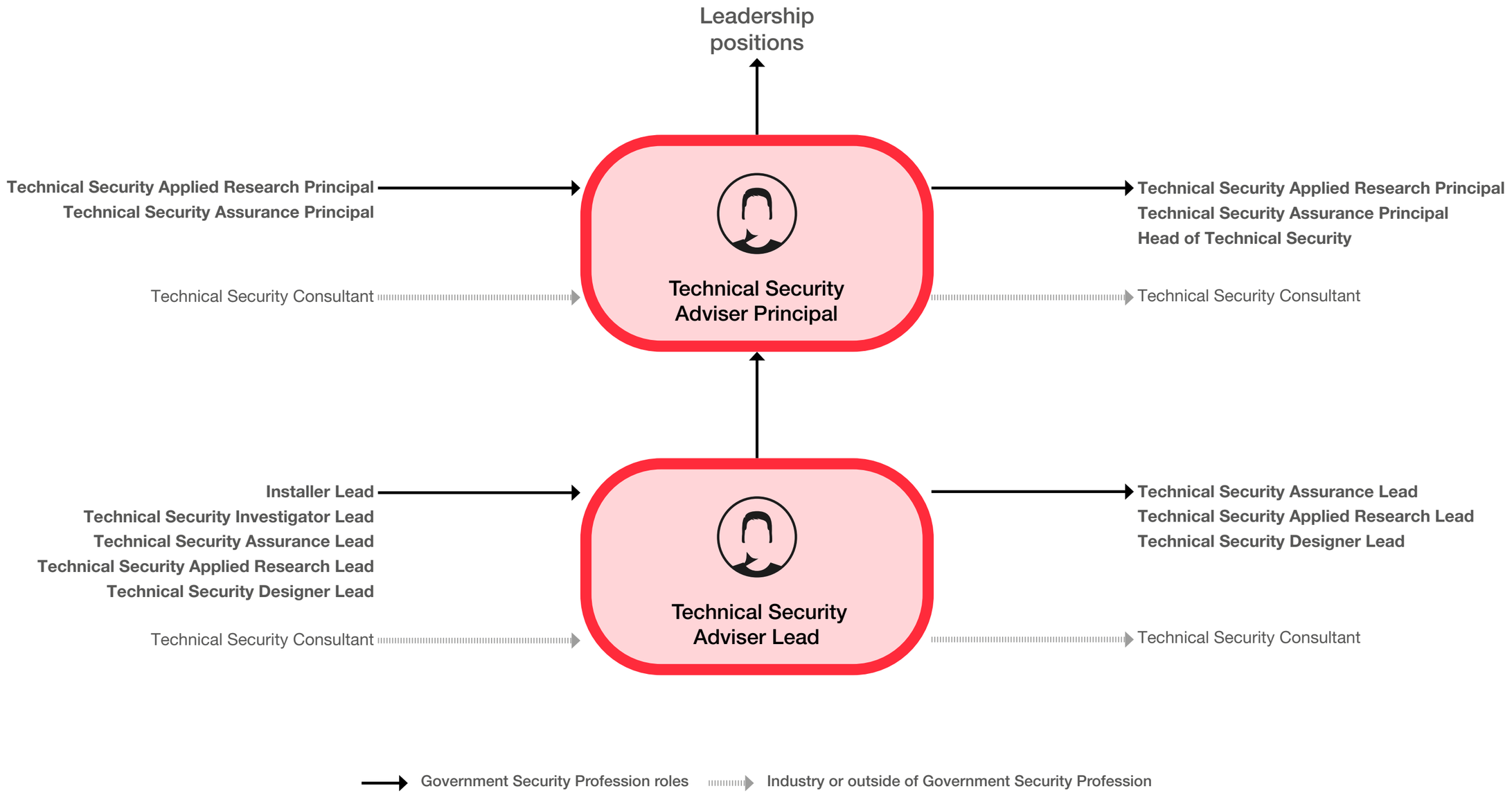
Development

Suggested training	Indicative professional qualifications/accreditations
• Technical Security leadership course • Risk management and information risk management course • Threat to government and industry training	• Membership of a relevant institution or body • Relevant industry or government qualifications and accreditations

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC

Role	Role family	Security specialism
Technical Security Adviser	Advisory	Technical Security

Suggested entry and exit roles are indicative only and non-exhaustive



Role	Role family	Security specialism
Technical Security Adviser Lead	Advisory	Technical Security

Role summary

The role of a Technical Security Adviser is to provide Technical Security advice to identify and mitigate security risks in line with business needs.

Typical role level expectations

- Provide expert advice on Technical Security to the Government Security Profession and wider public and private sectors
- Conduct risk assessments in the local environment, extracting insights to provide an informed opinion on Technical Security risks and the adequacy of controls in place
- Align with relevant regulation, policy and standards to provide proportional, practical advice that is tailored to the local environment, and advise on any residual risk
- Monitor the efficiency and effectiveness of the Technical Security processes across the organisation, and make recommendations for continual improvement
- Maintain awareness of current and emerging technologies and their impact on existing security practices

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. Science and Engineering Profession)

External

Suitable for an individual who has worked as a Technical Security consultant in industry

Role	Role family	Security specialism
Technical Security Adviser Principal	Advisory	Technical Security

Role summary

The role of a Technical Security Adviser is to provide Technical Security advice to identify and mitigate security risks in line with business needs.

Typical role level expectations

- Provide expert advice on Technical Security to the Government Security Profession and wider public and private sectors
- Manage and commission risk assessments in the local environment, extracting insights to provide an informed opinion on Technical Security risks and the adequacy of controls in place
- Create an organisational vision for aligning regulation, policy and standards to provide proportional, practical advice that is tailored to the local environment, and advise on any residual risk
- Create and monitor standards regarding efficiency and effectiveness of the Technical Security processes across the organisation, and make recommendations for continual improvement
- Maintain awareness of current and emerging technologies and their impact on existing security practices

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. Science and Engineering Profession)

External

Suitable for an individual who has worked as a Technical Security consultant in industry

Role	Role family	Security specialism
Technical Security Adviser	Advisory	Technical Security

Minimum skill expectations

Skill	Skill level	Training	Success profiles
Applied Technical Security	Practitioner	**Repository**	Making effective decisions*
Risk understanding and mitigation	Practitioner	**Repository**	Changing and improving
Protective security	Working	**Repository**	Communicating and influencing
Threat understanding	Working	**Repository**	Managing a quality service
Legal and regulatory environment and compliance	Working	**Repository**	Seeing the big picture

*Principal behaviour

Skill levels are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Development

Suggested training	Indicative professional qualifications/accreditations
• UK National Authority for Counter Eavesdropping Academy course • Risk management leadership course • Security management course • Threat awareness course • Security framework course	• Membership of a relevant institution or body • Relevant industry qualifications and accreditations • Relevant government qualifications and accreditations e.g. from UK National Authority for Counter Eavesdropping Academy, and the Centre for the Protection of National Infrastructure

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC

Role	Role family	Security specialism
Technical Security Adviser	Advisory	Technical Security

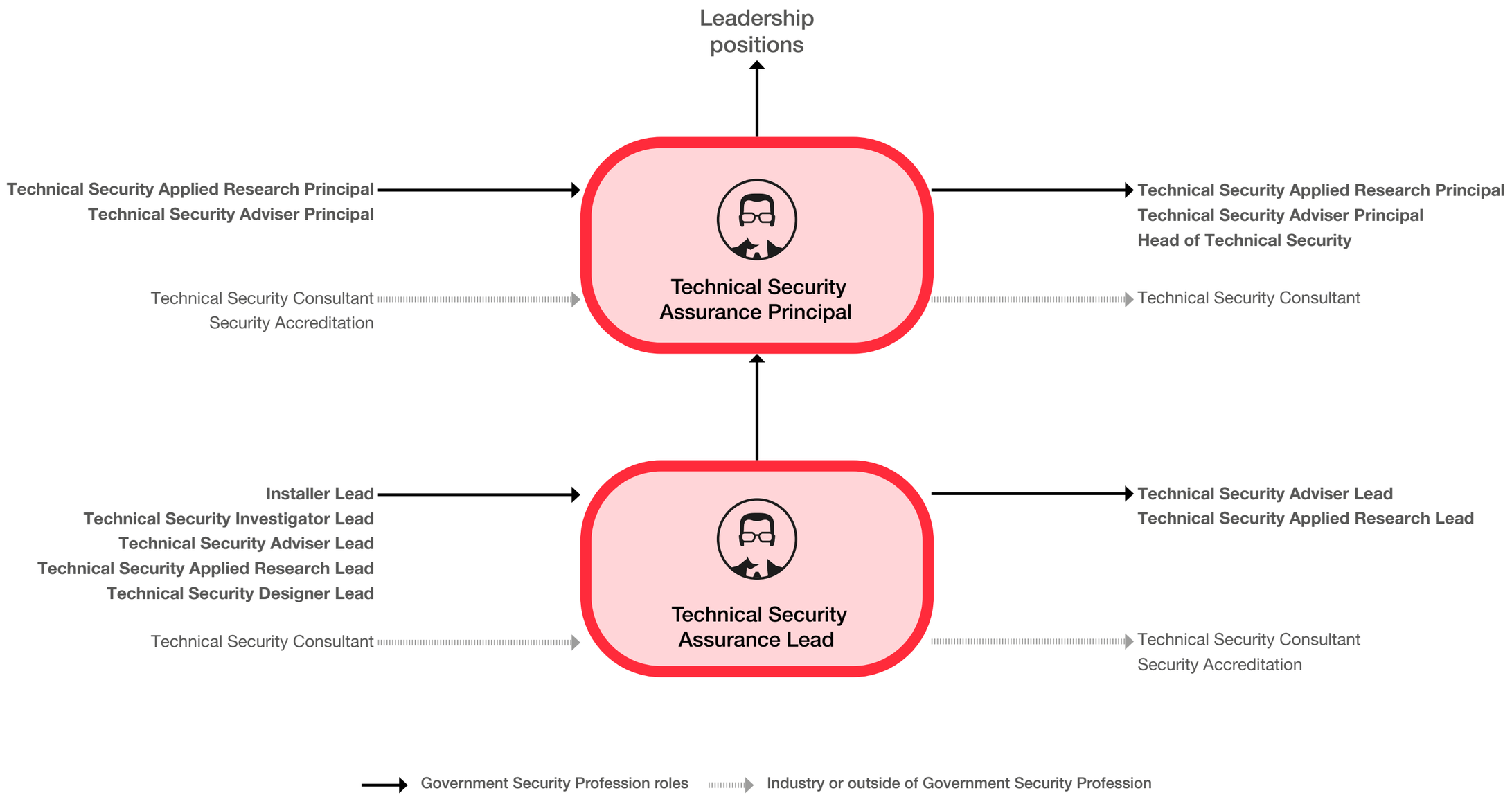
Minimum skill expectations

Skill	Role level	
	Adviser Lead	Adviser Principal
	Skill level	
Applied Technical Security	Practitioner	Expert
Risk understanding and mitigation	Practitioner	Expert
Protective security	Working	Practitioner
Threat understanding	Working	Practitioner
Legal and regulatory environment and compliance	Working	Working

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Role	Role family	Security specialism
Technical Security Assurance	Advisory	Technical Security

Suggested entry and exit roles are indicative only and non-exhaustive



Role	Role family	Security specialism
Technical Security Assurance Lead	Advisory	Technical Security

Role summary

The role of Technical Security Assurance is to identify Technical Security risks and highlight non-compliance and vulnerabilities to enable others to manage residual risk.

Typical role level expectations

- Deliver Technical Security assurance processes, including providing audit information to risk owners
- Assess, record, and monitor the introduction, maintenance, through-life performance, and removal of technical services, systems, platforms and infrastructure
- Monitor and report on the delivery of Technical Security services against requirements, using key performance indicators
- Ensure alignment with government and industry objectives and standards, proactively reviewing and assuring security risk and highlighting non-conformance

Entry route

Internal

Suitable for an individual from the Government Security Profession

External

Suitable for an individual who has worked within Technical Security in industry

Role	Role family	Security specialism
Technical Security Assurance Principal	Advisory	Technical Security

Role summary

The role of Technical Security Assurance is to identify Technical Security risks and highlight non-compliance and vulnerabilities to enable others to manage residual risk.

Typical role level expectations

- Manage delivery and life cycle of Technical Security assurance processes, including sharing audit information with senior leadership, and setting assurance standards across government
- Manage the assessment, recording, and monitoring of the introduction, maintenance, through-life performance, and removal of technical services, systems, platforms and infrastructure
- Review reporting, including key performance indicators, and act as key decision maker for the delivery of Technical Security services against requirements
- Ensure alignment with government and industry objectives and standards, and liaise with senior stakeholders on how these can be met

Entry route

Internal

Suitable for an individual from the Government Security Profession

External

Suitable for an individual who has worked within Technical Security in industry

Role	Role family	Security specialism
Technical Security Assurance	Advisory	Technical Security

Minimum skill expectations

Skill	Skill level	Training	Success profiles
Applied Technical Security	Practitioner	Repository	Making effective decisions*
Legal and regulatory environment and compliance	Practitioner	Repository	Changing and improving
Risk understanding and mitigation	Practitioner	Repository	Communicating and influencing
Protective security	Awareness	Repository	Managing a quality service
Threat understanding	Awareness	Repository	Seeing the big picture

*Principal behaviour

Skill levels are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Development

Suggested training	Indicative professional qualifications/accreditations
• UK National Authority for Counter Eavesdropping Academy course • Regulatory, compliance, or legislative course • Threat awareness course • Risk management leadership course	• Membership of a relevant institution or body • Relevant industry qualifications and accreditations e.g. Certified Information Systems Auditor • Relevant government qualifications or accreditations, e.g. from UK National Authority for Counter Eavesdropping Academy, and the Centre for the Protection of National Infrastructure

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC

Role	Role family	Security specialism
Technical Security Assurance	Advisory	Technical Security

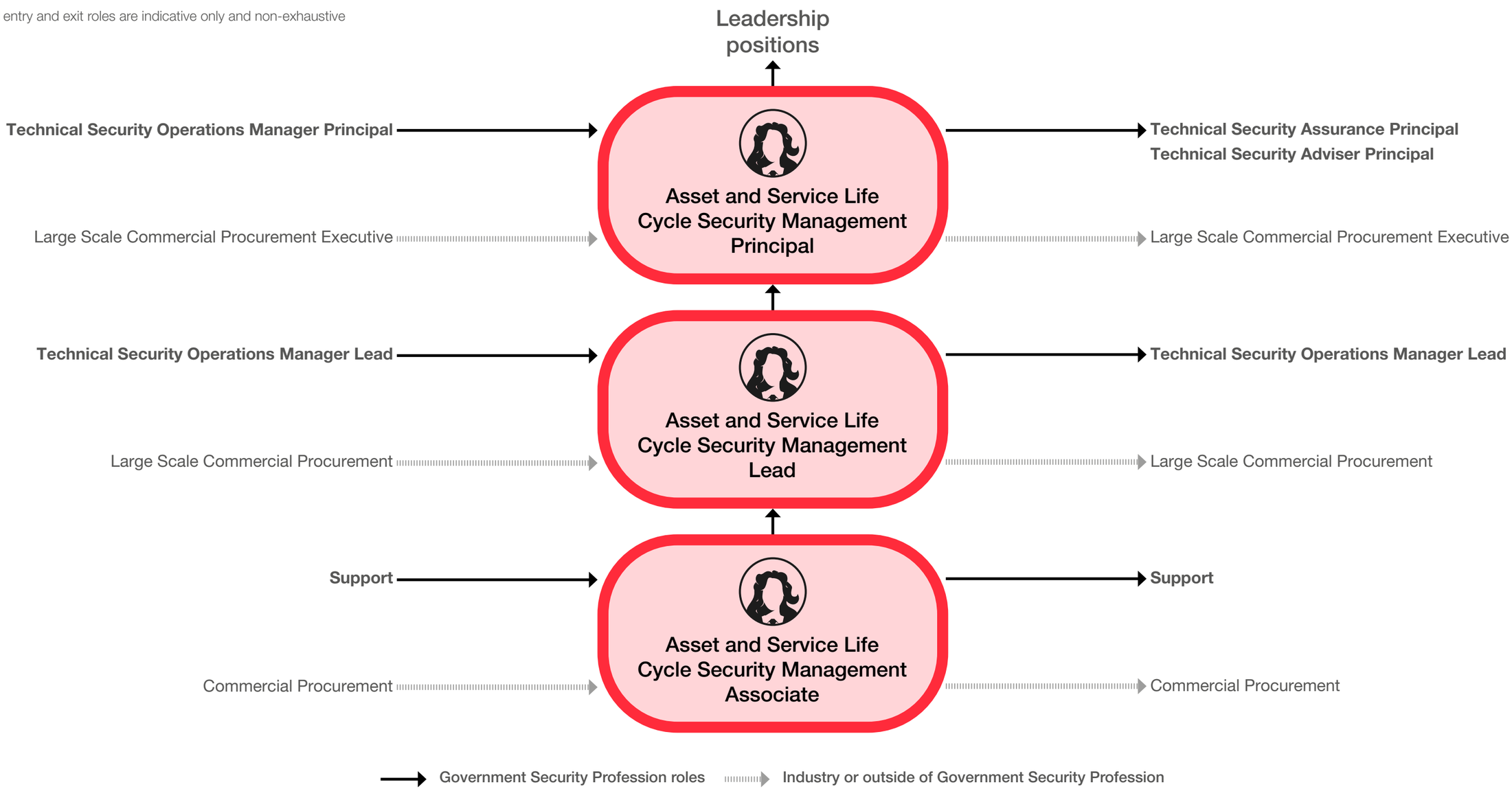
Minimum skill expectations

Skill	Role level	
	Assurance Lead	Assurance Principal
	Skill level	
Applied Technical Security	Practitioner	Expert
Legal and regulatory environment and compliance	Practitioner	Expert
Risk understanding and mitigation	Practitioner	Expert
Protective security	Awareness	Working
Threat understanding	Awareness	Working

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Role	Role family	Security specialism
Technical Security Asset and Service Life Cycle Security Management	Advisory	Technical Security

Suggested entry and exit roles are indicative only and non-exhaustive



Role	Role family	Security specialism
Technical Security Asset and Service Life Cycle Security Management Associate	Advisory	Technical Security

Role summary

The role of Technical Security Asset and Service Life Cycle Security Management is to oversee and provide advice throughout the procurement cycle, minimising the security risks associated with the procurement of assets or services, from concept to disposal.

Typical role level expectations

- Support identification and management of assets developed, processed or shared with suppliers, including with domestic and international partners
- Support supplier compliance with all relevant security legislation and regulatory requirements
- Support governance structures to manage all security risks from conception to disposal of assets, products or services, and the wider supply chain
- Support with the implementation of secure logistics of assets in development, transportation and at rest

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant government profession (e.g. Commercial or Procurement)

External

Suitable for an individual who has worked in contract management

Role	Role family	Security specialism
Technical Security Asset and Service Life Cycle Security Management Lead	Advisory	Technical Security

Role summary

The role of Technical Security Asset and Service Life Cycle Security Management is to oversee and provide advice throughout the procurement cycle, minimising the security risks associated with the procurement of assets or services, from concept to disposal.

Typical role level expectations

- Identify and manage the assets developed, processed or shared with suppliers, including with domestic and international partners
- Ensure acquisitions, service programmes and suppliers comply with all relevant security legislation and regulatory requirements
- Implement governance structures to manage all security risks from conception to disposal of assets, products or services, and the wider supply chain
- Act on intelligence that indicates any risk to the supply chain, including providing advice and assurance on supplier's security across acquisitions and services, and encourage continuous improvement
- Develop and maintain effective stakeholder relationships with both internal and external stakeholders in order to influence and change security decisions and manage the delivery of the required security assets

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant government profession (e.g. Commercial or Procurement)

External

Suitable for an individual who has worked in contract management

Role	Role family	Security specialism
Technical Security Asset and Service Life Cycle Security Management Principal	Advisory	Technical Security

Role summary

The role of Technical Security Asset and Service Life Cycle Security Management is to oversee and provide advice throughout the procurement cycle, minimising the security risks associated with the procurement of assets or services, from concept to disposal.

Typical role level expectations

- Oversee life cycle standards for assets developed for the organisation, processed or shared with suppliers, including with domestic and international partners
- Create and manage standards for acquisitions, service programmes and suppliers that comply with all relevant security legislation and regulatory requirements
- Oversee the implementation of governance structures to manage all security risks from conception to disposal of assets, products or services, and the wider supply chain
- Aggregate and prioritise intelligence that indicates any risk to the supply chain, including providing advice and assurance on supplier's security across acquisitions and services, and encourage continuous improvement
- Develop and maintain effective stakeholder relationships with both internal and external stakeholders in order to influence and change security decisions and manage the delivery of the required security assets

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant government profession (e.g. Commercial or Procurement)

External

Suitable for an individual who has worked in contract management

Role	Role family	Security specialism
Technical Security Asset and Service Life Cycle Security Management	Advisory	Technical Security

Minimum skill expectations

Skill	Skill level	Training	Success profiles
Applied Technical Security	Working	**Repository**	Communicating and influencing*
Risk understanding and mitigation	Working	**Repository**	Making effective decisions
Secure supply chain management	Working	**Repository**	Managing a quality service
Legal and regulatory environment and compliance	Awareness	**Repository**	Seeing the big picture
Protective security	Awareness	**Repository**	Working together
Threat understanding	Awareness	**Repository**	

*Principal behaviour

Skill levels are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Development

Suggested training	Indicative professional qualifications/accreditations
• UK National Authority for Counter Eavesdropping Academy course • Risk management course • Secure procurement and supply chain management course • Threat awareness course • Regulatory, compliance, or legislative course	• Membership of a relevant institution or body e.g. Register of Security Engineers and Specialists • Relevant industry qualifications and accreditations • Relevant government qualifications and accreditations e.g. from UK National Authority for Counter Eavesdropping Academy, and the Centre for the Protection of National Infrastructure

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC

Role	Role family	Security specialism
Technical Security Asset and Service Life Cycle Security Management	Advisory	Technical Security

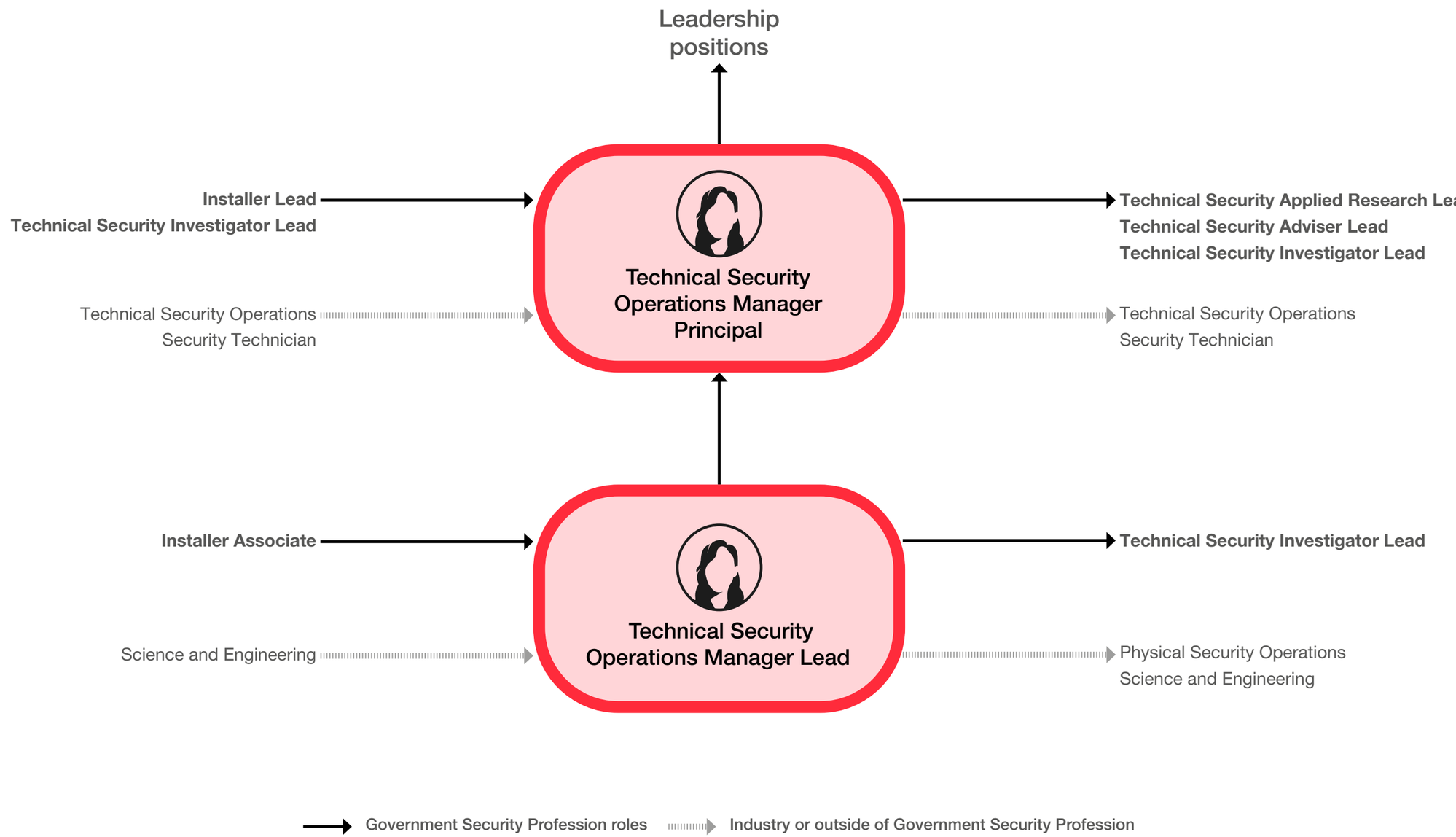
Minimum skill expectations

Skill	Role level		
	Asset and Service Life Cycle Security Management Associate	Asset and Service Life Cycle Security Management Lead	Asset and Service Life Cycle Security Management Principal
	Skill level		
Applied Technical Security	Working	Practitioner	Expert
Risk understanding and mitigation	Working	Practitioner	Expert
Secure supply chain management	Working	Practitioner	Expert
Legal and regulatory environment and compliance	Awareness	Working	Practitioner
Protective security	Awareness	Working	Working
Threat understanding	Awareness	Working	Working

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Role	Role family	Security specialism
Technical Security Operations Manager	Operations	Technical Security

Suggested entry and exit roles are indicative only and non-exhaustive



Role	Role family	Security specialism
Technical Security Operations Manager Lead	Operations	Technical Security

Role summary

The role of a Technical Security Operations Manager is to ensure operational preparedness for security incidents and the effective deployment of resources.

Typical role level expectations

- Maintain Technical Security operations and governance structures to appropriately manage risk
- Deploy Technical Security countermeasures to maintain technical integrity throughout the estate
- Plan, test, and respond to security and emergency incidents or concerns, including those raised by third parties, to include preparing briefs on security issues for internal and external stakeholders
- Comply with relevant regulation and legislation
- Manage resources, including people, and expenditure while promoting a positive and inclusive working environment

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. Science and Engineering Profession)

External

Suitable for an individual who has worked in security operations management in industry

Role	Role family	Security specialism
Technical Security Operations Manager Principal	Operations	Technical Security

Role summary

The role of a Technical Security Operations Manager is to ensure operational preparedness for security incidents and the effective deployment of resources.

Typical role level expectations

- Lead Technical Security operations and set governance structures to appropriately meet the risk appetite, overseeing effective Technical Security countermeasures to maintain technical integrity throughout the estate
- Oversee the planning, testing, and response to security and emergency incidents or concerns, and providing informed recommendations on Technical Security issues to internal and external stakeholders
- Mandate compliance with relevant regulation and legislation
- Oversee the management of resources, including people, and expenditure while ensuring a positive and inclusive working environment

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. Science and Engineering Profession)

External

Suitable for an individual who has worked in security operations management in industry

Role	Role family	Security specialism
Technical Security Operations Manager	Operations	Technical Security

Minimum skill expectations

Skill	Skill level	Training	Success profiles
Applied Technical Security	Working	Repository	Managing a quality service*
Risk understanding and mitigation	Working	Repository	Changing and improving
Secure operations management	Working	Repository	Communicating and influencing
Protective security	Working	Repository	Working together
Threat understanding	Working	Repository	
Legal and regulatory environment and compliance	Awareness	Repository	

*Principal behaviour

Skill levels are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Development

Suggested training	Indicative professional qualifications/accreditations
• UK National Authority for Counter Eavesdropping Academy course • Secure operations, project management and controls course • Threat awareness course • Regulatory, compliance, or legislative course	• Membership of a relevant institution or body • Relevant industry qualifications and accreditations • Relevant government qualifications and accreditations, e.g. from the UK National Authority for Counter Eavesdropping Academy, and the Centre for the Protection of National Infrastructure

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC

Role	Role family	Security specialism
Technical Security Operations Manager	Operations	Technical Security

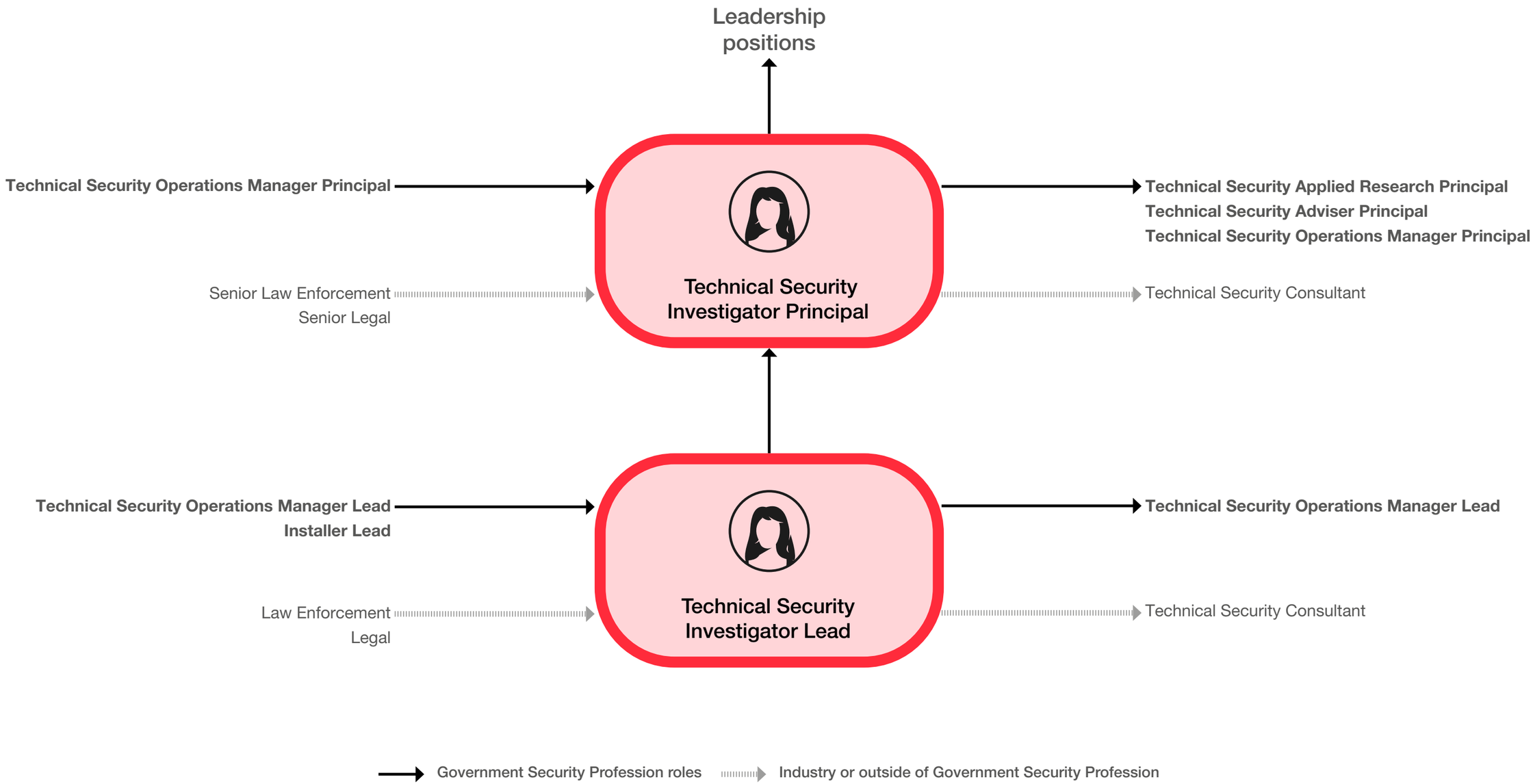
Minimum skill expectations

Skill	Role level	
	Operations Manager Lead	Operations Manager Principal
	Skill level	
Applied Technical Security	Working	Practitioner
Risk understanding and mitigation	Working	Practitioner
Secure operations management	Working	Practitioner
Protective security	Awareness	Working
Threat understanding	Awareness	Working
Legal and regulatory environment and compliance	Awareness	Awareness

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Role	Role family	Security specialism
Technical Security Investigator	Operations	Technical Security

Suggested entry and exit roles are indicative only and non-exhaustive



Role	Role family	Security specialism
Technical Security Investigator Lead	Operations	Technical Security

Role summary

The role of a Technical Security Investigator is to conduct Technical Security inspections in line with the latest developments in Technical Security, resolving or reporting any anomalies.

Typical role level expectations

- Support Technical Security inspections to identify potential tampering or manipulation
- Support the creation of situation reports outlining notable Technical Security anomalies and events
- Perform radio frequency heatmapping of estate and trace the sources of unidentified radio signals detected by in place monitoring systems
- Perform Technical Security baseline activities

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. Science and Engineering Profession)

External

Suitable for an individual with science and engineering investigative experience

Role	Role family	Security specialism
Technical Security Investigator Principal	Operations	Technical Security

Role summary

The role of a Technical Security Investigator is to conduct Technical Security inspections in line with the latest developments in Technical Security, resolving or reporting any anomalies.

Typical role level expectations

- Supervise, commission, or lead Technical Security inspections
- Commission, review, or lead situation reports on notable Technical Security anomalies and events
- Oversee teams performing radio frequency heat mapping of estate and tracing the sources of unidentified radio signals detected by in place monitoring systems
- Set standards for Technical Security baseline activities

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. Science and Engineering Profession)

External

Suitable for an individual with science and engineering investigative experience

Role	Role family	Security specialism
Technical Security Investigator	Operations	Technical Security

Minimum skill expectations

Skill	Skill level	Training	Success profiles
Applied Technical Security	Working	Repository	Making effective decisions*
Risk understanding and mitigation	Working	Repository	Communicating and influencing
Secure operations management	Awareness	Repository	Developing self and others
Legal and regulatory environment and compliance	Awareness	Repository	Managing a quality service
Protective security	Awareness	Repository	
Threat understanding	Awareness	Repository	

*Principal behaviour

Skill levels are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Development

Suggested training	Indicative professional qualifications/accreditations
• UK National Authority for Counter Eavesdropping Academy course • Secure operations course • Threat awareness course • Regulatory, compliance, or legislative course	• Membership of a relevant institution or body • Industry qualifications and accreditations • Government qualifications and accreditations e.g. from the UK National Authority for Counter Eavesdropping Academy, and the Centre for the Protection of National Infrastructure

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC

Role	Role family	Security specialism
Technical Security Investigator	Operations	Technical Security

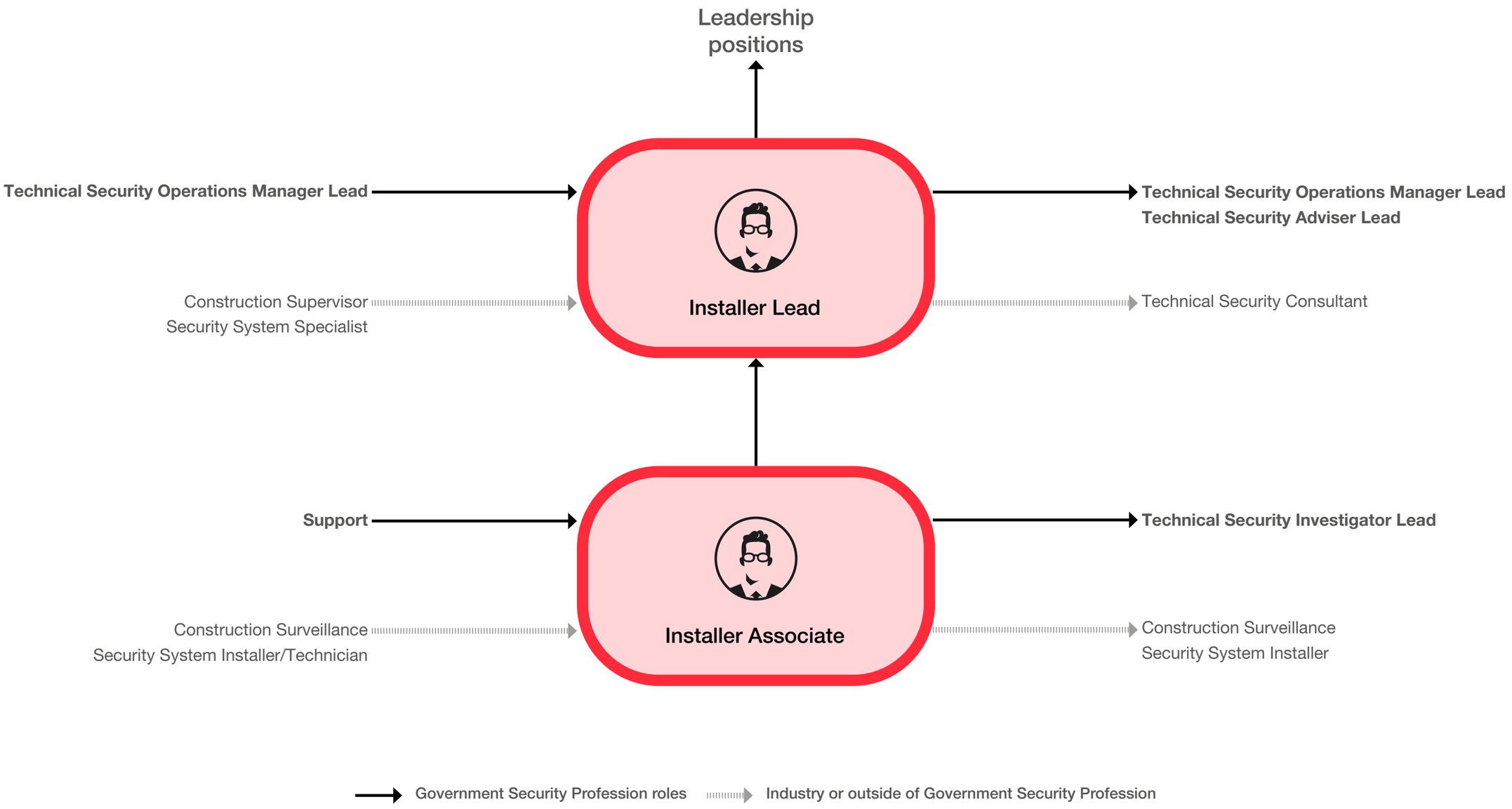
Minimum skill expectations

Skill	Role level	
	Investigator Lead	Investigator Principal
	Skill level	
Applied Technical Security	Working	Practitioner
Risk understanding and mitigation	Working	Practitioner
Secure operations management	Awareness	Working
Legal and regulatory environment and compliance	Awareness	Awareness
Protective security	Awareness	Awareness
Threat understanding	Awareness	Awareness

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Role	Role family	Security specialism
Installer	Operations	Technical Security

Suggested entry and exit roles are indicative only and non-exhaustive



Role	Role family	Security specialism
Installer Associate	Operations	Technical Security

Role summary

The role of an Installer is to install and maintain protective security mitigations in sensitive environments, maintain building systems and infrastructure, and baseline and mitigate Technical Security risks.

Typical role level expectations

- Inspect and maintain protective security installations to prevent potential tampering and manipulation
- Follow and interpret security installation design protocols
- Contribute to local protective security solutions and provide technical support
- Provide technical surveillance countermeasures using appropriate tooling

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. Science and Engineering Profession)

External

Suitable for an individual who has worked as an external security systems installer

Role	Role family	Security specialism
Installer Lead	Operations	Technical Security

Role summary

The role of an Installer is to install and maintain protective security mitigations in sensitive environments, maintain building systems and infrastructure, and baseline and mitigate Technical Security risks.

Typical role level expectations

- Manage a team undertaking protective security installations to prevent potential tampering and manipulation
- Share knowledge of security installation design protocols with others, and oversee team operations
- Oversee and quality assure local protective security solutions and provide technical support
- Provide technical surveillance countermeasures using appropriate tooling

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. Science and Engineering Profession)

External

Suitable for an individual who has worked as an external security systems installer

Role	Role family	Security specialism
Installer	Operations	Technical Security

Minimum skill expectations

Skill	Skill level	Training	Success profiles
Risk understanding and mitigation	Working	**Repository**	Managing a quality service*
Applied Technical Security	Working	**Repository**	Delivering at pace
Legal and regulatory environment and compliance	Awareness	**Repository**	Developing self and others
Protective security	Awareness	**Repository**	Working together
Threat understanding	Awareness	**Repository**	

*Principal behaviour

Skill levels are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Development

Suggested training	Indicative professional qualifications/accreditations
• Centre for the Protection of National Infrastructure • Equipment-specific training • Health and safety • Industry training courses	• Membership of a relevant institution or body • Relevant industry qualifications and accreditations • Relevant government qualifications and accreditations

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC

Role	Role family	Security specialism
Installer	Operations	Technical Security

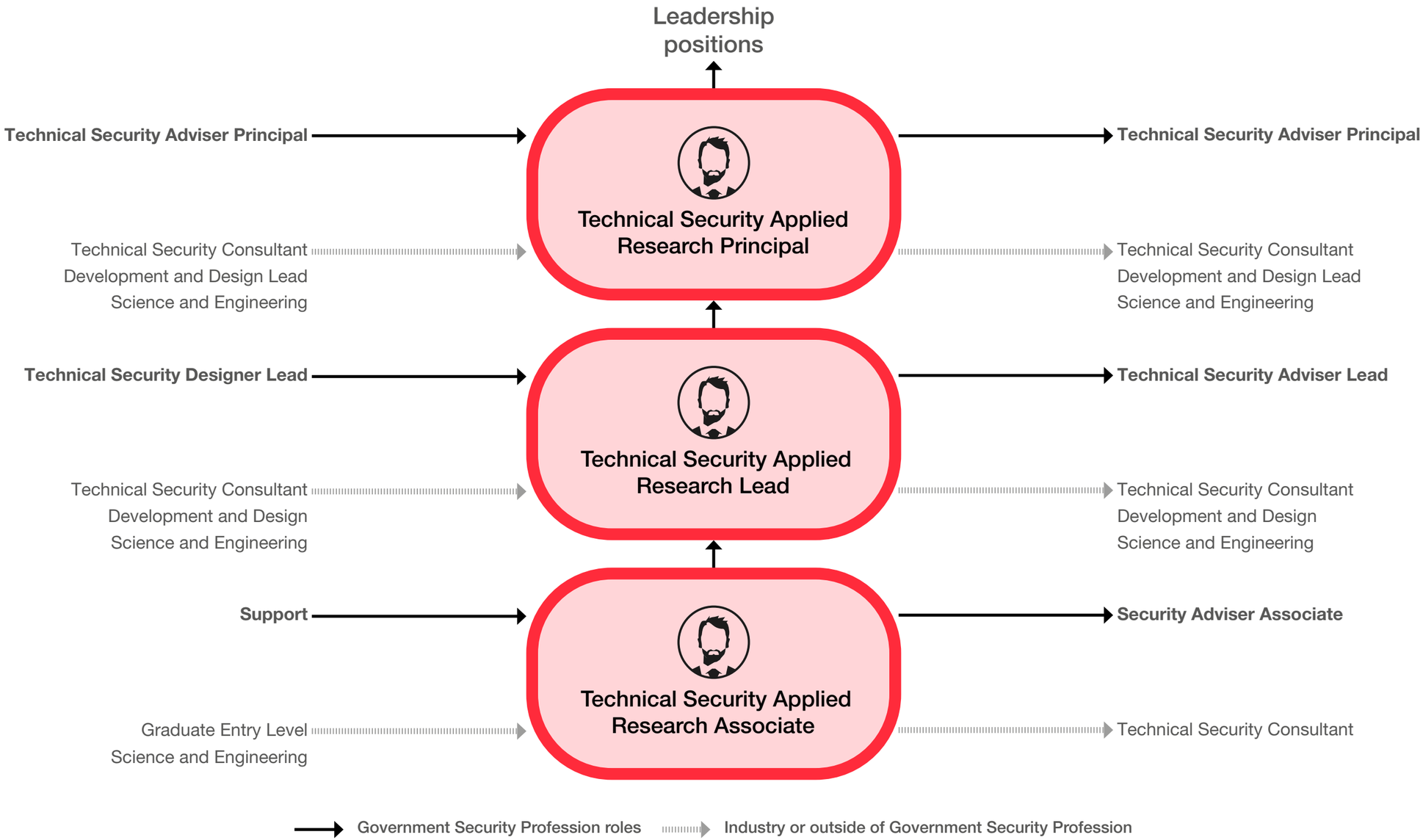
Minimum skill expectations

Skill	Role level	
	Installer Associate	Installer Lead
	Skill level	
Risk understanding and mitigation	Working	Practitioner
Applied Technical Security	Working	Working
Legal and regulatory environment and compliance	Awareness	Awareness
Protective security	Awareness	Awareness
Threat understanding	Awareness	Awareness

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Role	Role family	Security specialism
Technical Security Applied Research	Research, development and design	Technical Security

Suggested entry and exit roles are indicative only and non-exhaustive



Role	Role family	Security specialism
Technical Security Applied Research Associate	Research, development and design	Technical Security

Role summary

The role of Technical Security Applied Research is to inform the development of products and services to mitigate Technical Security risks.

Typical role level expectations

- Support a team of researchers to inform the development of products and services, utilising science and/or engineering, adhering to research and development best practices and frameworks to mitigate Physical Security risks
- Maintain awareness of current and emerging technologies and their impact on existing security practices

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. Science and Engineering Profession)

External

Suitable for an individual from an applied research, engineering or scientific background

Role	Role family	Security specialism
Technical Security Applied Research Lead	Research, development and design	Technical Security

Role summary

The role of Technical Security Applied Research is to inform the development of products and services to mitigate Technical Security risks.

Typical role level expectations

- Conduct research to inform the development of products and services, utilising science and/or engineering, adhering to research and development best practices and frameworks to mitigate Technical Security risks
- Provide technical guidance on emerging or existing issues
- Contribute to national and international Technical Security standards
- Maintain awareness of current and emerging technologies and their impact on existing security practices

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. Science and Engineering Profession)

External

Suitable for an individual from an applied research, engineering or scientific background

Role	Role family	Security specialism
Technical Security Applied Research Principal	Research, development and design	Technical Security

Role summary

The role of Technical Security Applied Research is to inform the development of products and services to mitigate Technical Security risks.

Typical role level expectations

- Commission and lead a team undertaking research to inform the development of products and services, utilising science and/or engineering, and adhering to research and development best practices and frameworks to mitigate Technical Security risks
- Provide technical guidance on emerging or existing issues, providing thought leadership and foresight of future evolving threats, and advising on the development and implementation of countermeasures
- Initiate, influence and lead the continuous improvement of national and international Technical Security standards
- Define the standard current and emerging technologies and their impact on existing security practices for the whole specialism, inside and outside the organisation

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. Science and Engineering Profession)

External

Suitable for an individual from an applied research, engineering or scientific background

Role	Role family	Security specialism
Technical Security Applied Research	Research, development and design	Technical Security

Minimum skill expectations

Skill	Skill level	Training	Success profiles
Applied research	Working	Repository	Managing a quality service*
Legal and regulatory environment and compliance	Working	Repository	Changing and improving
Applied Technical Security	Working	Repository	Developing self and others
Risk understanding and mitigation	Awareness	Repository	Seeing the big picture
Threat understanding	Awareness	Repository	
Protective security	Awareness	Repository	

*Principal behaviour

Skill levels are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Development

Suggested training	Indicative professional qualifications/accreditations
• UK National Authority for Counter Eavesdropping Academy course • Research based regulatory, compliance or legislative course • Threat awareness course • Research methodologies course	• Membership of a relevant institution or body, e.g. Register of Security Engineers and Specialists • Relevant industry qualifications and accreditations • Relevant government qualifications and accreditations e.g. from the Centre for the Protection of National Infrastructure

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC

Role	Role family	Security specialism
Technical Security Applied Research	Research, development and design	Technical Security

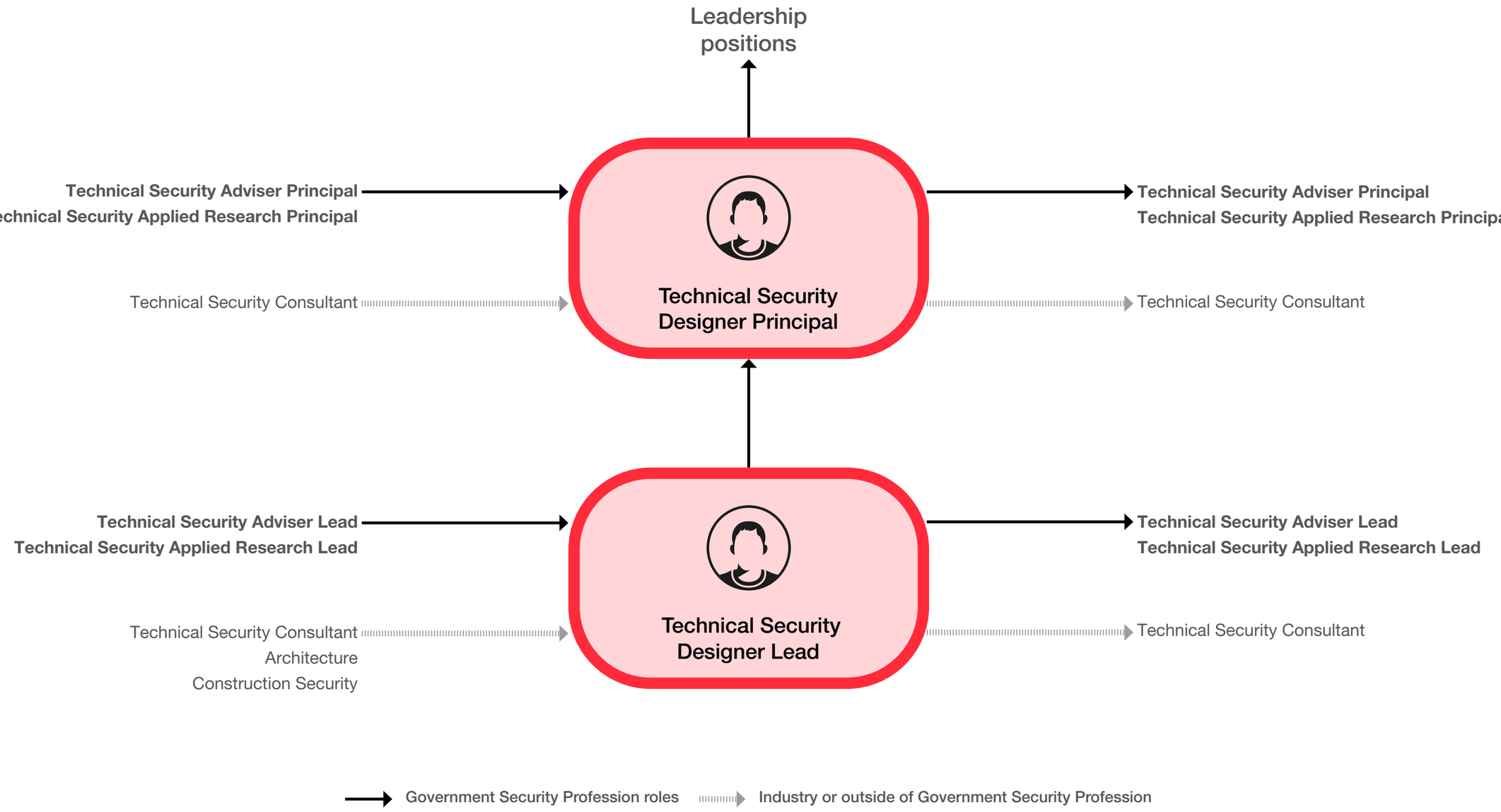
Minimum skill expectations

Skill	Role level		
	Applied Research Associate	Applied Research Lead	Applied Research Principal
	Skill level		
Applied research	Working	Practitioner	Expert
Legal and regulatory environment and compliance	Working	Practitioner	Expert
Applied Technical Security	Working	Practitioner	Practitioner
Risk understanding and mitigation	Awareness	Working	Practitioner
Threat understanding	Awareness	Awareness	Working
Protective security	Awareness	Awareness	Awareness

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Role	Role family	Security specialism
Technical Security Designer	Research, development and design	Technical Security

Suggested entry and exit roles are indicative only and non-exhaustive



Role	Role family	Security specialism
Technical Security Designer Lead	Research, development and design	Technical Security

Role summary

The role of Technical Security Designer is to provide advice and expertise on the design and implementation of Technical Security measures.

Typical role level expectations

- Conduct research to inform the development of products and services, utilising science and/or engineering, adhering to research and development best practices and frameworks to mitigate Technical Security risks
- Provide technical guidance on emerging or existing issues
- Contribute to national and international Technical Security standards
- Maintain awareness of current and emerging technologies and their impact on existing security practices

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. Science and Engineering Profession)

External

Suitable for an individual from an applied research, engineering or scientific background

Role	Role family	Security specialism
Technical Security Designer Principal	Research, development and design	Technical Security

Role summary

The role of Technical Security Designer is to provide advice and expertise on the design and implementation of Technical Security measures.

Typical role level expectations

- Commission and lead a team undertaking research to inform the development of products and services, utilising science and/or engineering, and adhering to research and development best practices and frameworks to mitigate Technical Security risks
- Provide technical guidance on emerging or existing issues, providing thought leadership and foresight of future evolving threats, and advising on the development and implementation of countermeasures
- Initiate, influence and lead the continuous improvement of national and international Technical Security standards
- Define the standard current and emerging technologies and their impact on existing security practices for the whole specialism, inside and outside the organisation

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. Science and Engineering Profession)

External

Suitable for an individual from an applied research, engineering or scientific background

Role	Role family	Security specialism
Technical Security Designer	Research, development and design	Technical Security

Minimum skill expectations

Skill	Skill level	Training	Success profiles
Design	Practitioner	**Repository**	Changing and improving*
Legal and regulatory environment and compliance	Practitioner	**Repository**	Developing self and others
Applied Technical Security	Practitioner	**Repository**	Managing a quality service
Protective security	Working	**Repository**	
Risk understanding and mitigation	Working	**Repository**	
Secure operations management	Working	**Repository**	
Threat understanding	Awareness	**Repository**	

*Principal behaviour

Skill levels are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Development

Suggested training	Indicative professional qualifications/accreditations
• UK National Authority for Counter Eavesdropping Academy course • Secure design course • Design-based regulatory, compliance or legislative course • Risk management course • Threat awareness course	• Membership of a relevant institution or body, e.g. the Register of Security Engineers and Specialists • Relevant industry qualifications and accreditations • Relevant government qualifications and accreditations e.g. from the Centre of the Protection of National Infrastructure

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC

Role	Role family	Security specialism
Technical Security Designer	Research, development and design	Technical Security

Minimum skill expectations

Skill	Role level	
	Designer Lead	Designer Principal
	Skill level	
Design	Practitioner	Expert
Legal and regulatory environment and compliance	Practitioner	Expert
Applied Technical Security	Practitioner	Practitioner
Protective security	Working	Practitioner
Risk understanding and mitigation	Working	Practitioner
Secure operations management	Working	Practitioner
Threat understanding	Awareness	Awareness

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Corporate Enablers – role families and roles

In addition to the Government Security Profession career framework's 4 security specialisms, the career framework also has Government Security Profession corporate enablers. The corporate enablers span the specialisms and are pivotal to the growth, development and success of the Government Security Profession. Individuals working in a corporate enabler role may belong to more than one government function and profession. The corporate enablers included in the career framework are leadership, business continuity, education and awareness, training, capability development, policy, process, support, and risk management. This list is non-exhaustive.


Government Chief Security Officer


Chief Security Officer


Security Adviser


Business Continuity


Education and Awareness


Training


Capability Development


Policy


Process

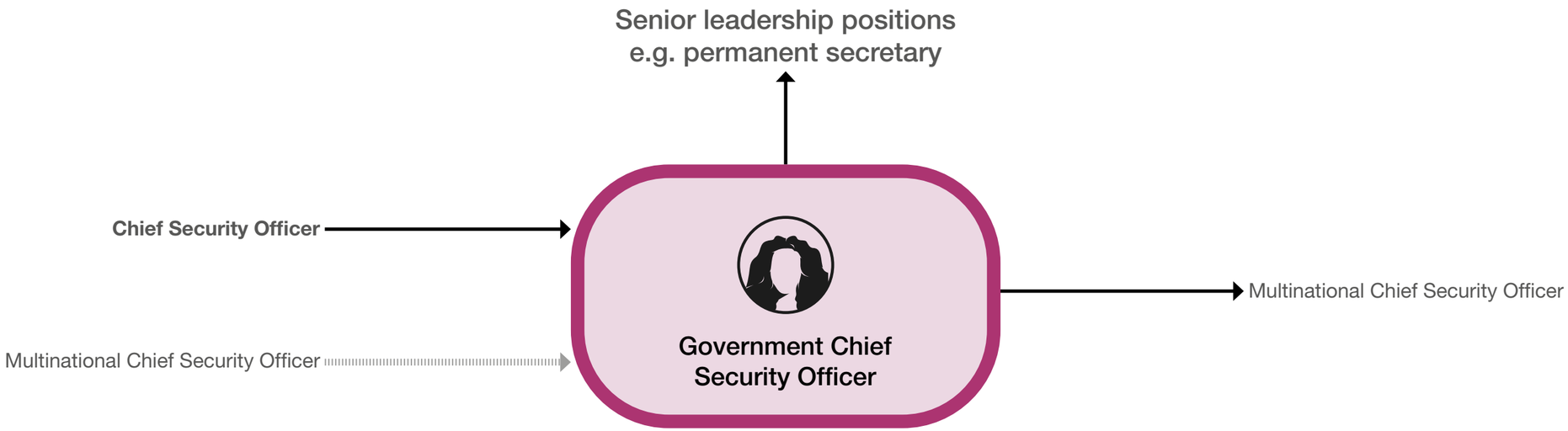

Support


Risk Management

Role	Corporate Enablers

Government Chief Security Officer

Suggested entry and exit roles are indicative only and non-exhaustive



Role	Corporate Enablers

Government Chief Security Officer

Role summary

The Government Chief Security Officer is recognised as the lead government security official. They are responsible for leading the Government Security Group, defining its high-level vision, objectives and strategy, as well as overseeing day-to-day operations in support of security across government. They are accountable to the Chief Executive of the Civil Service and the wider Civil Service Board.

Typical role level expectations

- Anticipate changing conditions and trends, and influence government to adjust and respond appropriately
- Champion a positive security culture across government, ensuring appropriate resource allocation into initiatives within the Government Security Function
- Champion and promote the Government Security Profession as well as other relevant wider government and industry communities
- Actively develop and manage relationships and interdependencies with key internal and external stakeholders

Entry route

Internal

Suitable for an individual who has completed the Government Security Profession pathway

External

May be suitable for a former Chief Security Officer of a multinational organisation

Role	Corporate Enablers

Government Chief Security Officer

Minimum skill expectations

Skill	Skill level	Training	Success profiles
Protective security	Expert	**Repository**	Leadership*
Risk understanding and mitigation	Awareness	**Repository**	Communicating and influencing
Threat understanding	Awareness	**Repository**	Developing self and others
			Seeing the big picture
			Working together

*Principal behaviour

Skill levels are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Development

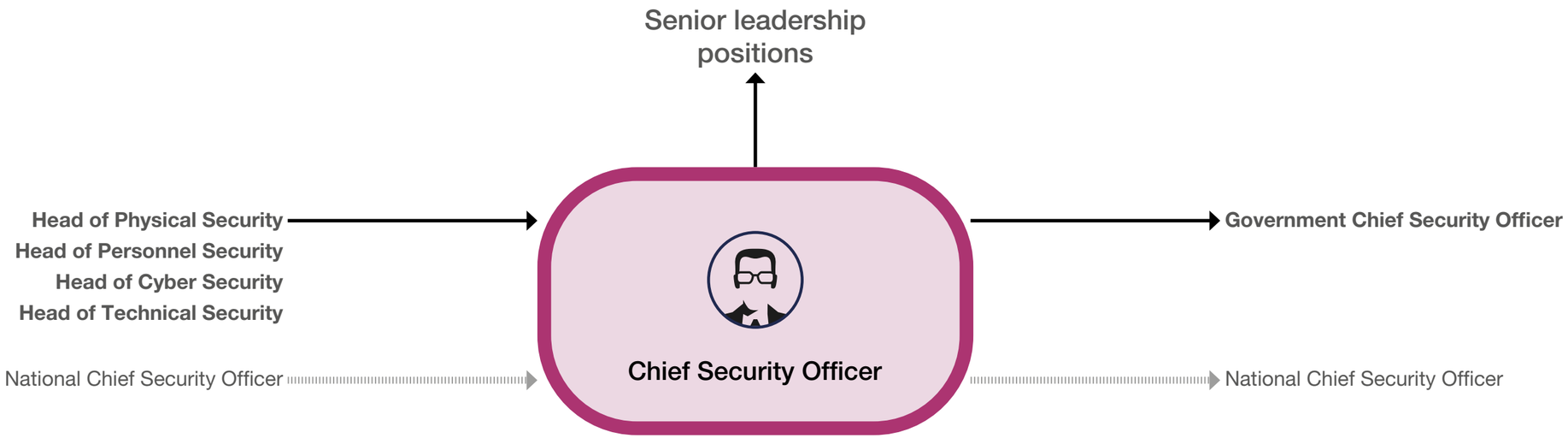
Suggested training	Indicative professional qualifications/accreditations
• HM Government Security leadership course • Risk management and information risk management course • Threat to HM Government/industry training	• Membership of a relevant institution or body • Relevant industry or government qualifications and accreditations

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC

Role	Corporate Enablers

Chief Security Officer

Suggested entry and exit roles are indicative only and non-exhaustive



Government Security Profession roles | Industry or outside of Government Security Profession

Role	Corporate Enablers

Chief Security Officer

Role summary

The Chief Security Officer is responsible for leading the Cluster Security Unit, in addition to the responsibilities of a Security Adviser.

Typical role level expectations

- Champion a positive security culture at a departmental and wider government level
- Lead a Cluster Security Unit/Centre of Excellence, overseeing day-to-day service delivery and ensuring that the Cluster Security Unit/ Centre of Excellence has the skills and resources to meet agreed standards and service level agreements as required by Security Advisers in the departments and agencies
- Define clear goals, strategic objectives, performance delivery outcomes and timelines for security in the Cluster Security Unit/Centre of Excellence

Entry route

Internal

Suitable for an individual from the Government Security Profession

External

May be suitable for an individual who has worked as an industry Chief Security Officer

Role	Corporate Enablers

Chief Security Officer

Minimum skill expectations

Skill	Skill level	Training	Success profiles
Protective security	Expert	**Repository**	Leadership*
Risk understanding and mitigation	Awareness	**Repository**	Communicating and influencing
Threat understanding	Awareness	**Repository**	Developing self and others
			Seeing the big picture
			Working together

*Principal behaviour

Skill levels are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Development

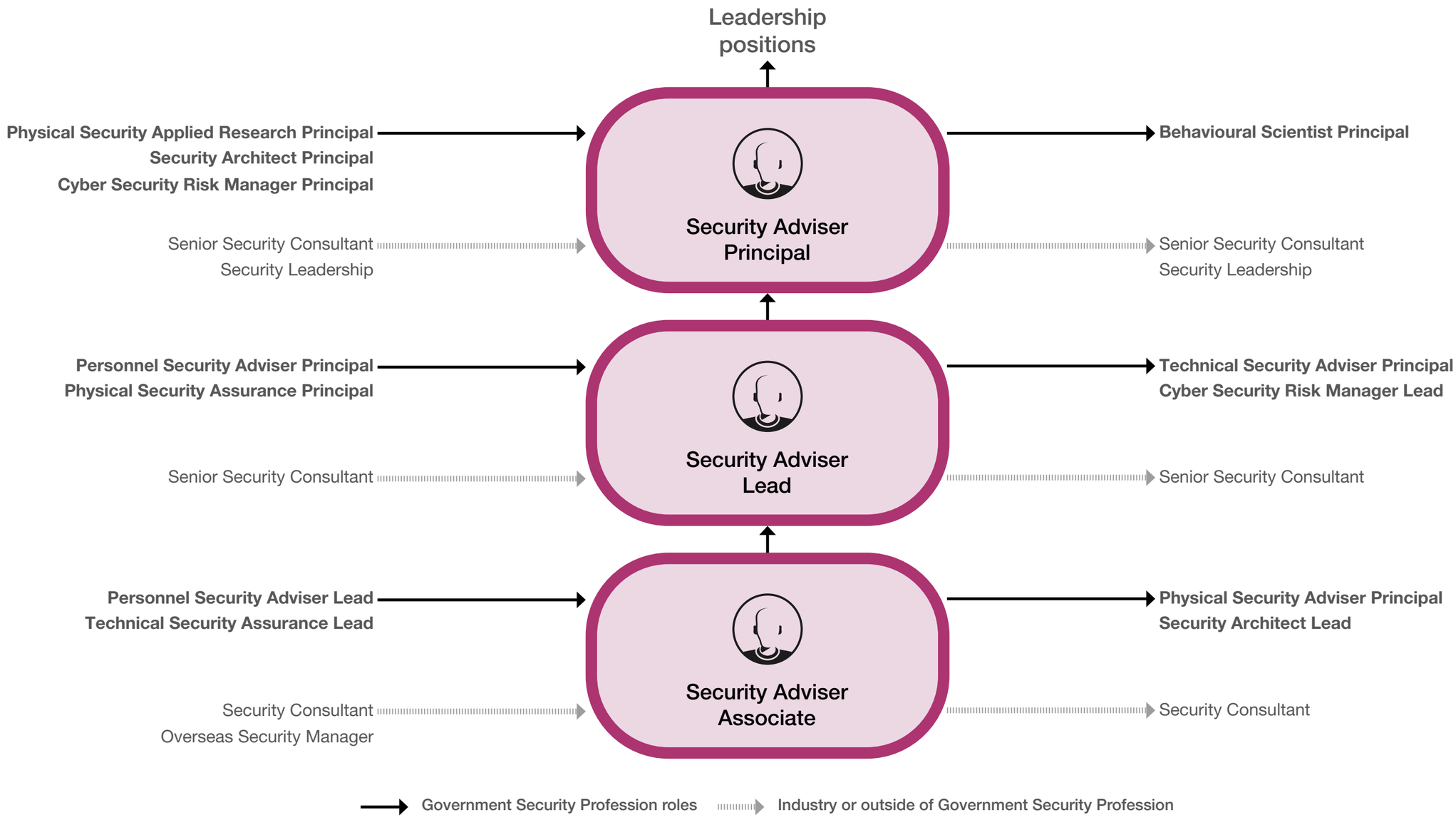
Suggested training	Indicative professional qualifications/accreditations
• Security leadership course • Risk management and information risk management course • Threat to HM Government/industry training	• Membership of a relevant institution or body • Relevant industry or government qualifications and accreditations

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC

Role	Corporate Enablers

Security Adviser

Suggested entry and exit roles are indicative only and non-exhaustive



Role	Corporate Enablers

Security Adviser Associate

Role summary

The role of the Security Adviser is to support the Government Chief Security Officer to ensure departmental security requirements are being met and provide ongoing monitoring of services delivered by the Cluster Security Unit.

Typical role level expectations

- Support the co-ordination of security requirements and service requests for a government organisation, acting as an intelligent customer to the relevant Cluster Security Unit/ Centre of Excellence and offering a strategic picture
- Support the provision of security advice to an assigned government organisation, including addressing and mitigating security risks and issues, and supporting the maintenance of a security culture
- Support the development and maintenance of organisational policies, products and methodologies to drive continuous improvement
- Support building a network of security partners across government and national technical authorities, and within industry, with a goal to share best practice
- Actively participate, on behalf of a government organisation, with the Cluster Security Unit/Centre of Excellence to ensure security consistency and maintain security and risk standards across government

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. Risk Management Profession)

External

May be suitable for an individual who has worked in risk management

Role	Corporate Enablers

Security Adviser Lead

Role summary

The role of the Security Adviser is to support the Government Chief Security Officer to ensure departmental security requirements are being met and provide ongoing monitoring of services delivered by the Cluster Security Unit.

Typical role level expectations

- Co-ordinate security requirements and service requests for a government organisation of small to medium size and complexity, acting as an intelligent customer to the respective Cluster Security Unit/Centre of Excellence and offering a strategic picture
- Provide security advice to one or more assigned government organisations, including to address and mitigate security risks and issues, and establish and maintain a security culture
- Manage the development and maintenance of organisational policies, products and methodologies to drive continuous improvement
- Build a network of security partners across government, national technical authorities and within industry, with a goal to share best practice
- Actively participate, on behalf of a government organisation, with the Cluster Security Unit/Centre of Excellence to ensure security consistency and maintain security and risk standards across government

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. Risk Management Profession)

External

May be suitable for an individual who has worked in risk management

Role	Corporate Enablers

Security Adviser Principal

Role summary

The role of the Security Adviser is to support the Government Chief Security Officer to ensure departmental security requirements are being met and provide ongoing monitoring of services delivered by the Cluster Security Unit.

Typical role level expectations

- Co-ordinate security requirements and service requests for a large or high-complexity government organisation, acting as an intelligent customer to the respective Cluster Security Unit/Centre of Excellence and offering a strategic picture
- Provide security advice to one or more assigned government organisations, including to address and mitigate security risks and issues, and establish and maintain a security culture
- Lead the development and maintenance of organisational policies, products and methodologies to drive continuous improvement
- Lead a network of security partners across government, national technical authorities and within industry, with a goal to share best practice
- Actively lead engagement, on behalf of multiple government organisations, with the Cluster Security Unit/Centre of Excellence to ensure security consistency and maintain security and risk standards across government

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. Risk Management Profession)

External

May be suitable for an individual who has worked in risk management

Role	Corporate Enablers

Security Adviser

Minimum skill expectations

Skill	Skill level	Training	Success profiles
Protective security	Practitioner	**Repository**	Leadership*
Risk understanding and mitigation	Working	**Repository**	Communicating and influencing
Legal and regulatory environment and compliance	Awareness	**Repository**	Developing self and others
Threat understanding	Awareness	**Repository**	Seeing the big picture
			Working together

*Principal behaviour

Skill levels are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Development

Suggested training	Indicative professional qualifications/accreditations
• Security leadership course • Risk management and information risk management course • Threat to HM Government/industry training	• Membership of a relevant institution or body • Relevant industry or government qualifications and accreditations

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC

Role	Corporate Enablers

Security Adviser

Minimum skill expectations

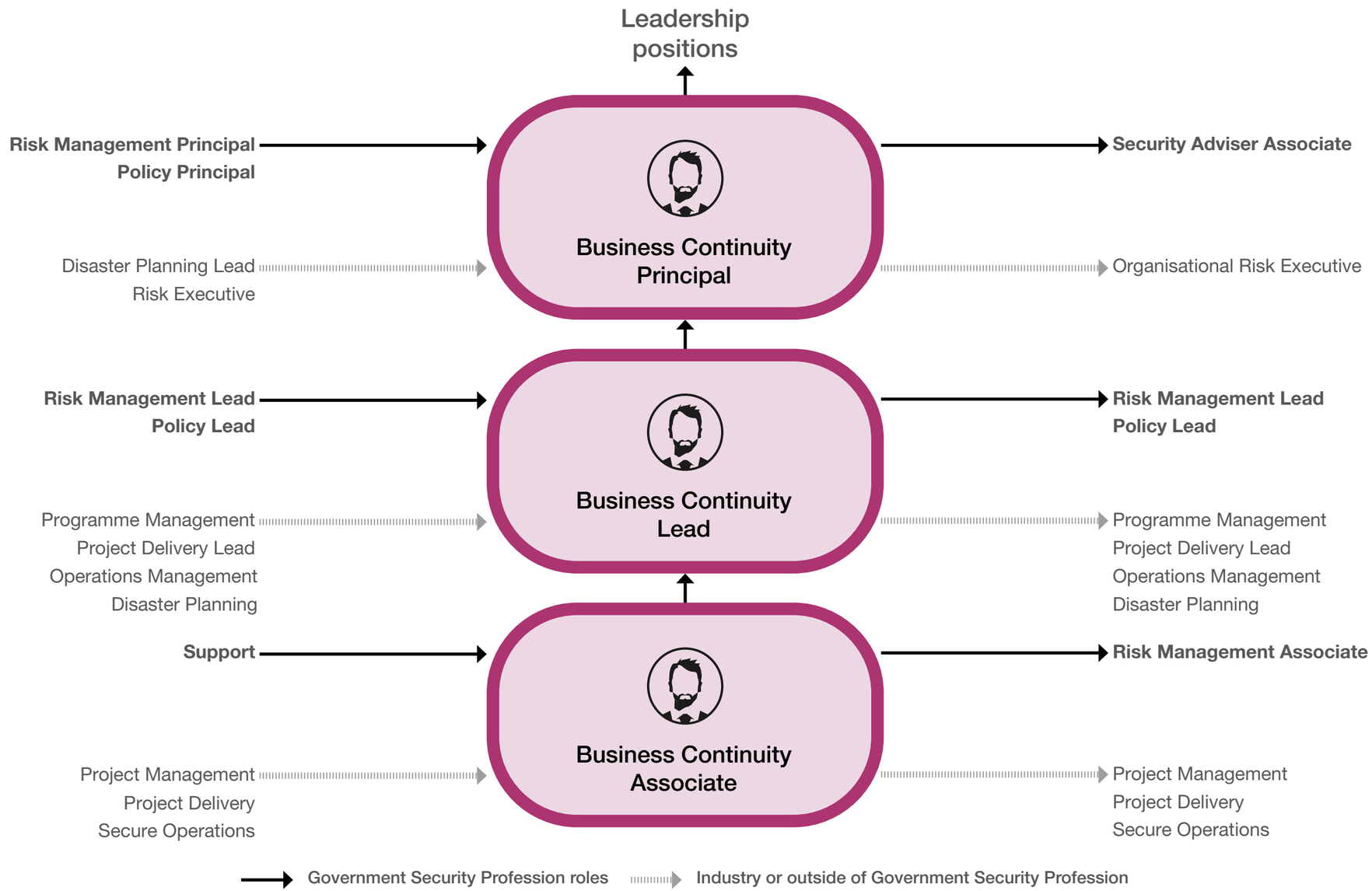
Skill	Role level		
	Security Adviser Associate	Security Adviser Lead	Security Adviser Principal
	Skill level		
Protective security	Practitioner	Practitioner	Expert
Risk understanding and mitigation	Working	Practitioner	Practitioner
Legal and regulatory environment and compliance	Awareness	Working	Practitioner
Threat understanding	Awareness	Working	Practitioner

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Role	Corporate Enablers

Business Continuity

Suggested entry and exit roles are indicative only and non-exhaustive



Role	Corporate Enablers

Business Continuity Associate

Role summary

The role of Business Continuity is to work across the Business Continuity Management Life Cycle in completing policy and programme management, embedding, analysis, design, implementation and validation of business continuity management-related initiatives, policies, programmes and services to aid improved resilience.

Typical role level expectations

- Identify and document business continuity risks and issues and escalate as required
- Contribute to an accurate and up-to-date organisational picture to include risk owners and lines of accountability
- Support incident response structures for strategic, tactical and operational disruptions
- Support implementation of the business continuity capability by establishing, maintaining and reviewing the organisation's policy and programme activities for each stage of the business continuity life cycle

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. Policy and Programme Management Profession)

External

Suitable for an individual from a business continuity/resilience, risk management or related role in industry or with a business continuity-related qualification e.g. the Business Continuity Diploma

Role	Corporate Enablers

Business Continuity Lead

Role summary

The role of Business Continuity is to work across the Business Continuity Management Life Cycle in completing policy and programme management, embedding, analysis, design, implementation and validation of business continuity management-related initiatives, policies, programmes and services to aid improved resilience.

Typical role level expectations

- Co-ordinate the identification and documentation of business continuity risks and issues, and act as an escalation point for mitigation
- Maintain an accurate and up-to-date organisational picture to include risk owners and lines of accountability
- Collaborate with incident response on structures for strategic, tactical and operational disruptions, identifying all participants involved in the response process, including their roles, responsibilities and authorities
- Implement the business continuity capability by establishing, maintaining and reviewing the organisation's policy and programme activities for each stage of the business continuity life cycle

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. Policy and Programme Management Profession)

External

Suitable for an individual from a business continuity/resilience, risk management or related role in industry

Role	Corporate Enablers

Business Continuity Principal

Role summary

The role of Business Continuity is to work across the Business Continuity Management Life Cycle in completing policy and programme management, embedding, analysis, design, implementation and validation of business continuity management-related initiatives, policies, programmes and services to aid improved resilience.

Typical role level expectations

- Champion business continuity in the Government Security Profession and wider government
- Drive continuous improvement through the sharing of knowledge, best practice and lessons learned
- Lead business continuity exercising programmes through engagement with stakeholders
- Promote training and awareness campaigns to ensure the successful embedding of business continuity practices

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. Policy and Programme Management Profession)

External

Suitable for an individual from a business continuity/resilience, risk management or related role in industry

Role	Corporate Enablers

Business Continuity

Minimum skill expectations

Skill	Skill level	Training	Success profiles
Business continuity management	Working	**Repository**	Seeing the big picture*
Protective security	Working	**Repository**	Changing and improving
Risk understanding and mitigation	Working	**Repository**	Communicating and influencing
Threat understanding	Working	**Repository**	Leadership
			Managing a quality service
			Working together

*Principal behaviour

Skill levels are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Development

Suggested training	Indicative professional qualifications/accreditations
• Business Continuity Institute courses • Risk management course • Threat awareness course	• Membership of a relevant institution or body, e.g. Business Continuity Institute • Relevant industry or government qualifications and accreditations

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC

Role	Corporate Enablers

Business Continuity

Minimum skill expectations

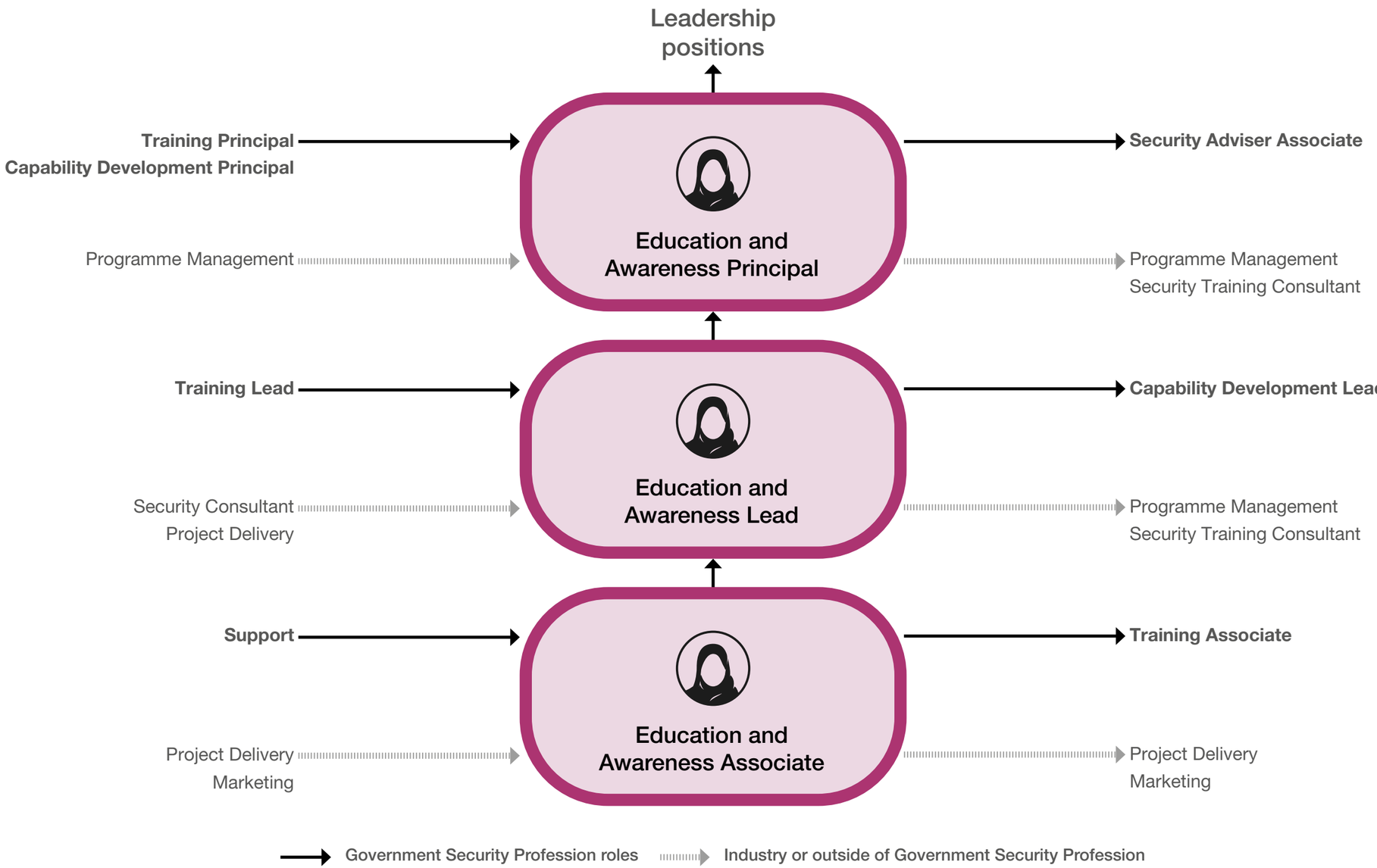
Skill	Role level		
	Business Continuity Associate	Business Continuity Lead	Business Continuity Principal
	Skill level		
Business continuity management	Working	Practitioner	Expert
Protective security	Working	Practitioner	Practitioner
Risk understanding and mitigation	Working	Practitioner	Practitioner
Threat understanding	Working	Practitioner	Practitioner

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Role	Corporate Enablers

Education and Awareness

Suggested entry and exit roles are indicative only and non-exhaustive



Role	Corporate Enablers

Education and Awareness Associate

Role summary

The role of Education and Awareness is to identify education and awareness programmes, projects and engagements to develop the security culture of an organisation.

Typical role level expectations

- Support the development of a security culture within an organisation
- Undertake activities to deliver and assure security education and awareness programmes across the Government Security Profession
- Promote security-conscious behaviours and good security risk management practices within the Government Security Profession and wider government

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. Training, Communication, or Policy and Programme Management)

External

Suitable for an individual who has worked in security training, policy or marketing in industry

Role	Corporate Enablers

Education and Awareness Lead

Role summary

The role of Education and Awareness is to identify education and awareness programmes, projects and engagements to develop the security culture of an organisation.

Typical role level expectations

- Lead the development of a security culture within an organisation
- Lead activities to deliver and assure security education awareness programmes across the Government Security Profession
- Promote security-conscious behaviours and good security risk management practices within the Government Security Profession and wider government

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. Training, Communication, or Policy and Programme Management)

External

Suitable for an individual who has worked in security training, policy or marketing in industry

Role	Corporate Enablers

Education and Awareness Principal

Role summary

The role of Education and Awareness is to identify education and awareness programmes, projects and engagements to develop the security culture of an organisation.

Typical role level expectations

- Champion the development of a security culture within an organisation
- Lead on the delivery of security education and awareness programmes and initiatives across the Government Security Profession
- Promote security education and awareness programmes across the Government Security Profession and wider government

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. Training, Communication, or Policy and Programme Management)

External

Suitable for an individual who has worked in security training, policy or marketing in industry

Role	Corporate Enablers

Education and Awareness

Minimum skill expectations

Skill	Skill level	Training	Success profiles
Protective security	Working	**Repository**	Seeing the big picture*
Threat understanding	Awareness	**Repository**	Changing and improving
Applied research	Awareness	**Repository**	Communicating and influencing
Risk understanding and mitigation	Awareness	**Repository**	Developing self and others
Legal and regulatory environment and compliance	Awareness	**Repository**	

*Principal behaviour

Skill levels are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Development

Suggested training	Indicative professional qualifications/accreditations
• Workforce engagement course • Risk management course • Threat awareness course	• Membership of a relevant institution or body • Relevant industry or government qualifications and accreditations

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC

Role	Corporate Enablers

Education and Awareness

Minimum skill expectations

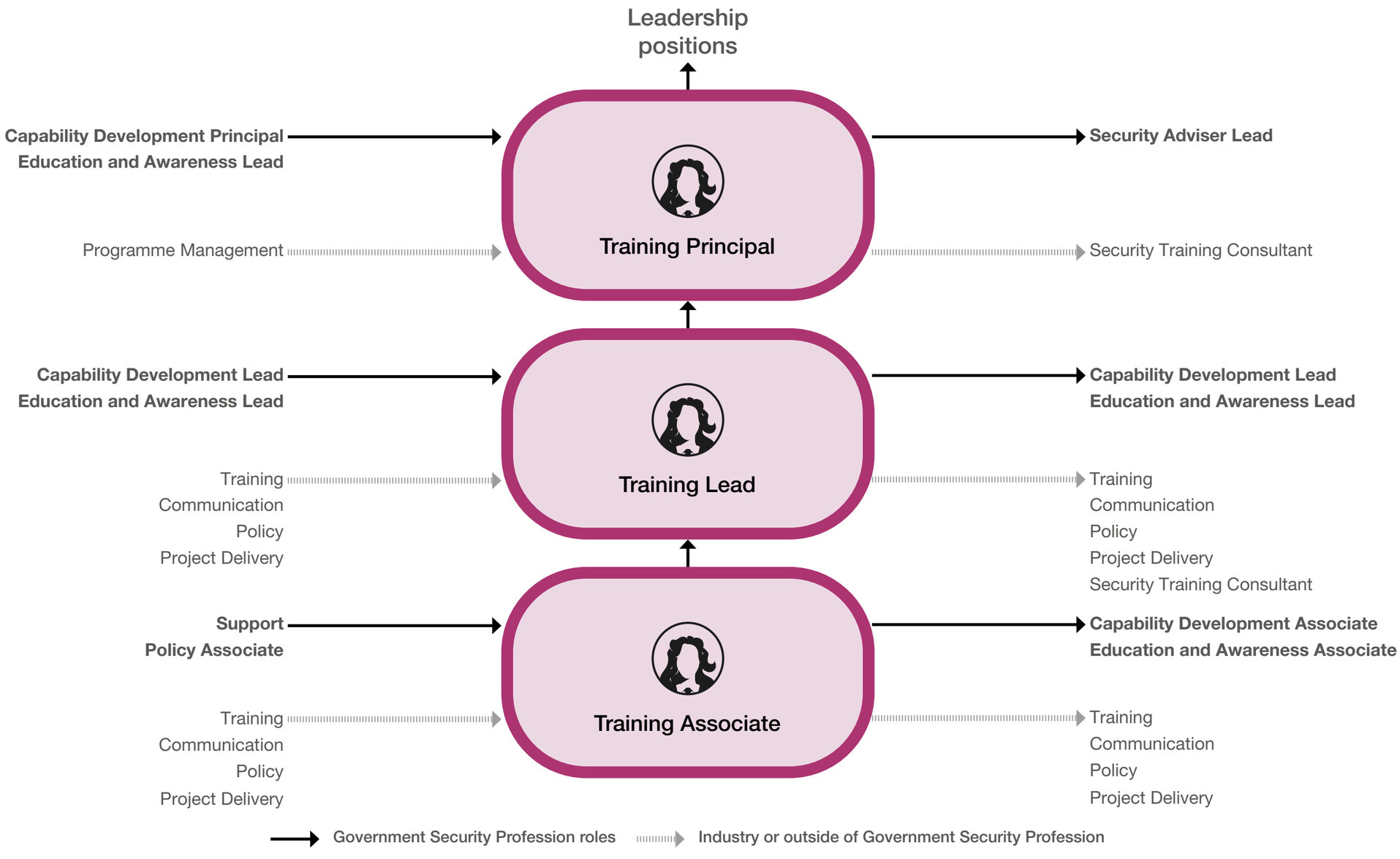
Skill	Role level		
	Education and Awareness Associate	Education and Awareness Lead	Education and Awareness Principal
	Skill level		
Protective security	Working	Practitioner	Expert
Threat understanding	Awareness	Working	Practitioner
Applied research	Awareness	Working	Working
Risk understanding and mitigation	Awareness	Working	Working
Legal and regulatory environment and compliance	Awareness	Awareness	Awareness

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Role	Corporate Enablers

Training

Suggested entry and exit roles are indicative only and non-exhaustive



Role	Corporate Enablers

Training Associate

Role summary

The role of Training is to deliver, co-ordinate and/or direct security training programmes for government security professionals.

Typical role level expectations

- Promote security-conscious behaviours and good security risk management practices within the Government Security Profession
- Work with the Government Security Profession to develop training courses, potentially across a range of platforms (classroom, eLearning, self-paced) to meet the needs of the Government Security Profession

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. Training, Communication or Policy and Programme Management)

External

Suitable for an individual who has worked in security training in industry

Role	Corporate Enablers

Training Lead

Role summary

The role of Training is to deliver, co-ordinate and/or direct security training programmes for government security professionals.

Typical role level expectations

- Promote security-conscious behaviours and good security risk management practices within the Government Security Profession and wider government
- Lead on the development of training courses across a range of platforms (classroom, eLearning, self-paced) to meet the needs of the Government Security Profession
- Maintain up-to-date knowledge of the latest security developments and trends, to incorporate into security training

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. Training, Communication or Policy and Programme Management)

External

Suitable for an individual who has worked in security training in industry

Role	Corporate Enablers

Training Principal

Role summary

The role of Training is to deliver, co-ordinate and/or direct security training programmes for government security professionals.

Typical role level expectations

- Champion security-conscious behaviours and good security risk management practices within the Government Security Profession, wider government and externally
- Lead on the strategy for training of practitioners across the Government Security Profession
- Oversee teams develop training courses across a range of platforms (classroom, eLearning, self-paced) to meet the needs of the Government Security Profession
- Share training best practices with wider government and across industry
- Maintain up-to-date knowledge of the latest security developments and trends, to incorporate into security training

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. Training, Communication or Policy and Programme Management)

External

Suitable for an individual who has worked in security training in industry

Role	Corporate Enablers

Training

Minimum skill expectations

Skill	Skill level	Training	Success profiles
Protective security	Working	**Repository**	Seeing the big picture
Threat understanding	Awareness	**Repository**	Changing and improving
Risk understanding and mitigation	Awareness	**Repository**	Communicating and influencing
			Delivering at pace
			Developing self and others
			Leadership
			Making effective decisions
			Managing a quality service
			Working together

*Principal behaviour

Skill levels are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Development

Suggested training	Indicative professional qualifications/accreditations
• Workforce engagement course • Risk management course • Threat awareness course	• Membership of a relevant institution or body • Relevant industry or government qualifications and accreditations

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC

Role	Corporate Enablers

Training

Minimum skill expectations

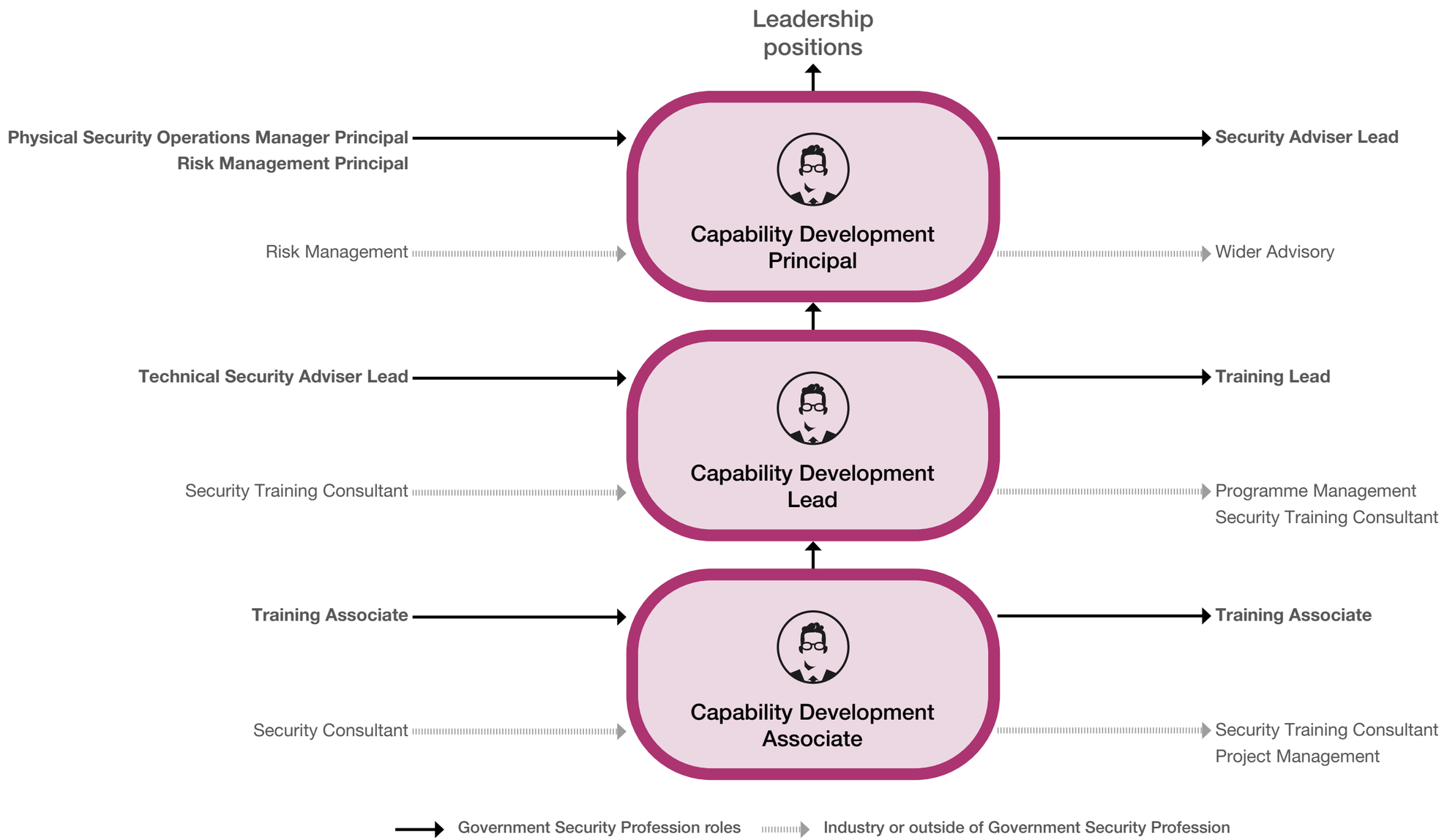
Skill	Role level		
	Training Associate	Training Lead	Training Principal
	Skill level		
Protective security	Working	Practitioner	Expert
Threat understanding	Awareness	Working	Practitioner
Risk understanding and mitigation	Awareness	Working	Working

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Role	Corporate Enablers

Capability Development

Suggested entry and exit roles are indicative only and non-exhaustive



Role	Corporate Enablers

Capability Development Associate

Role summary

The role of Capability Development refers to the development of policies and procedures relating to the employment of personnel and equipment including recruitment and procurement. It also refers to how these are modified according to threat as part of a process of continuous review.

Typical role level expectations

- Support colleagues within capability development on their liaison regarding security issues with key stakeholders, including external parties, and contribute to the development of strong working relationships with external stakeholders who have interests in relation to security
- Ensure that the security policies and security controls employed locally remain appropriate and proportionate to the assessed risks, and are responsive and adaptable to the changing threat environment, business requirements and central government policies
- Promote cross-government security-mindedness

Entry route

Internal

Suitable for an individual from the Government Security Profession

External

Suitable for an individual who has worked in security talent management in industry

Role	Corporate Enablers

Capability Development Lead

Role summary

The role of Capability Development refers to the development of policies and procedures relating to the employment of personnel and equipment including recruitment and procurement. It also refers to how these are modified according to threat as part of a process of continuous review.

Typical role level expectations

- Be the primary point of contact on security issues with key stakeholders, including external parties, and develop strong working relationships with external stakeholders who have interests in relation to security
- Ensure that the security policies and security controls employed across an organisation remain appropriate and proportionate to the assessed risks, and are responsive and adaptable to the changing threat environment, business requirements and central government policies
- Manage the uptake and endorsement of learning, development and accreditation; cultivate talent and foster an inclusive, diverse and motivated workforce; and promote cross-government security-mindedness

Entry route

Internal

Suitable for an individual from the Government Security Profession

External

Suitable for an individual who has worked in security talent management in industry

Role	Corporate Enablers

Capability Development Principal

Role summary

The role of Capability Development refers to the development of policies and procedures relating to the employment of personnel and equipment including recruitment and procurement. It also refers to how these are modified according to threat as part of a process of continuous review.

Typical role level expectations

- Be the primary point of contact on complex or large-scale security issues with key stakeholders, including external parties, and develop strong working relationships with external stakeholders who have interests in relation to security
- Ensure that the security policies and security controls employed across multiple organisations or highly complex organisations remain appropriate and proportionate to the assessed risks, and are responsive and adaptable to the changing threat environment, business requirements and central government policies
- Lead uptake and endorsement of learning, development and accreditation; cultivate talent and foster an inclusive, diverse and motivated workforce; and promote cross-government security-mindedness

Entry route

Internal

Suitable for an individual from the Government Security Profession

External

Suitable for an individual who has worked in security talent management in industry

Role	Corporate Enablers

Capability Development

Minimum skill expectations

Skill	Skill level	Training	Success profiles
Risk understanding and mitigation	Working	**Repository**	Leadership*
Protective security	Awareness	**Repository**	Communicating and influencing
Threat understanding	Awareness	**Repository**	Developing self and others
Legal and regulatory environment and compliance	Awareness	**Repository**	Seeing the big picture
			Working together

*Principal behaviour

Skill levels are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Development

Suggested training	Indicative professional qualifications/accreditations
• Risk management course • Threat awareness course • Regulatory, compliance or legislative course • Project management course	• Membership of a relevant institution or body • Relevant industry or government qualifications and accreditations

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC

Role	Corporate Enablers

Capability Development

Minimum skill expectations

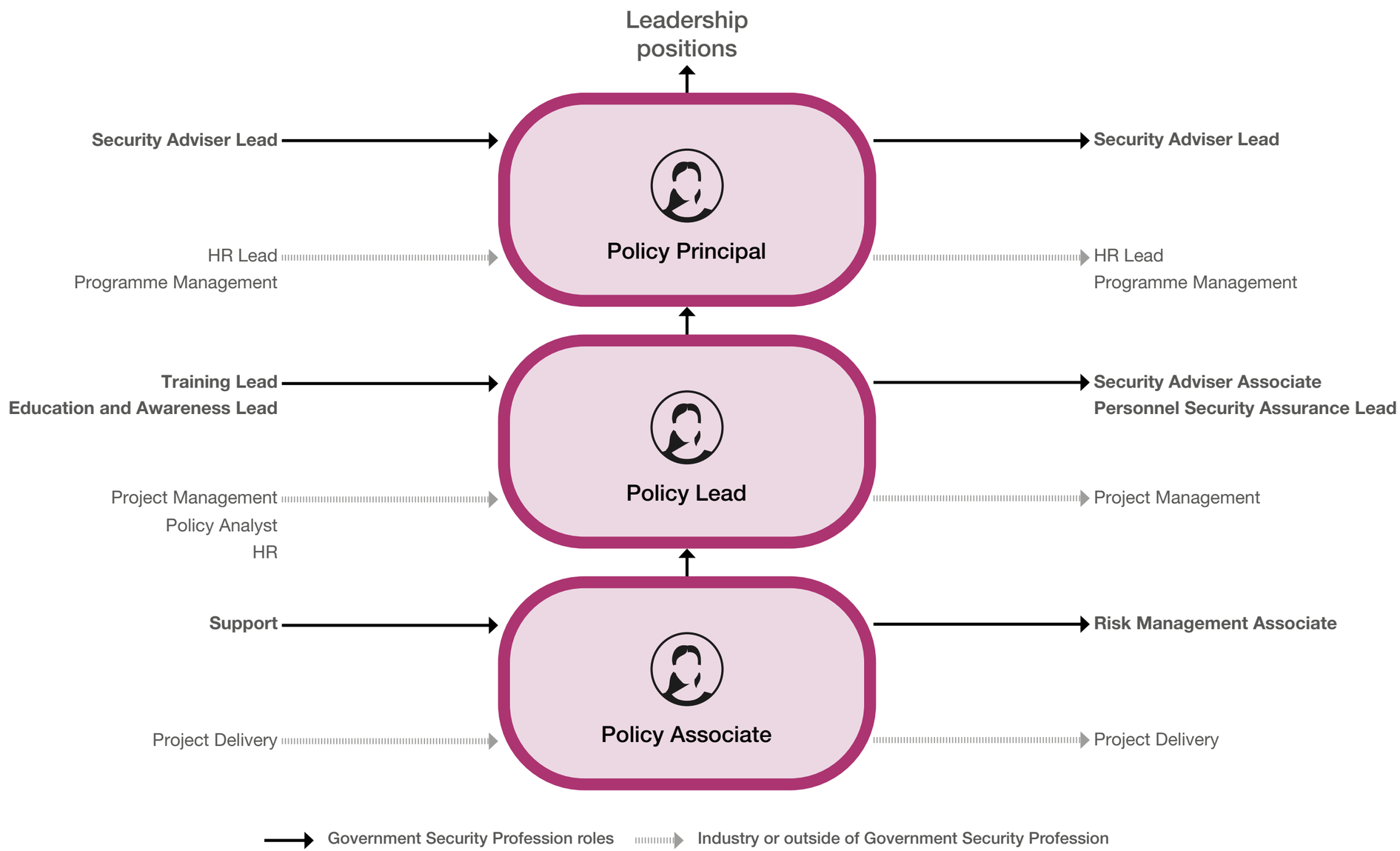
Skill	Role level		
	Capability Development Associate	Capability Development Lead	Capability Development Principal
	Skill level		
Risk understanding and mitigation	Working	Practitioner	Practitioner
Protective security	Awareness	Working	Practitioner
Threat understanding	Awareness	Working	Practitioner
Legal and regulatory environment and compliance	Awareness	Working	Working

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Role	Corporate Enablers

Policy

Suggested entry and exit roles are indicative only and non-exhaustive



Role	Corporate Enablers

Policy Associate

Role summary

The role of Security Policy is to develop, implement and maintain business-enabling policies and processes relevant to the Government Security Profession, taking into account local requirements and ensuring adherence to applicable regulation and wider departmental and government policies.

Typical role level expectations

- Support the establishment of an appropriate protective security organisational posture to encourage an effective risk-based approach to security across the estate, taking into account political, economic, social, technological, legal and environmental considerations
- Demonstrate sound understanding of the intended outcomes of the policy and what successful end-to-end delivery looks like
- Support the development of mechanisms to drive continuous improvement within wider government and across national and international standards, enforce sanctions and encourage the sharing of best practice
- Assess quantitative and qualitative data to support the creation of evidence-based policy, evaluating and presenting evidence within the appropriate tooling

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. Training, Communication or Policy and Programme Management)

External

Suitable for an individual who has worked in security policy in industry

Role	Corporate Enablers

Policy Lead

Role summary

The role of Security Policy is to develop, implement and maintain business-enabling policies and processes relevant to the Government Security Profession, taking into account local requirements and ensuring adherence to applicable regulation and wider departmental and government policies.

Typical role level expectations

- Manage the establishment of an appropriate protective security organisational posture to ensure an effective risk-based approach to security across the estate, taking into account political, economic, social, technological, legal and environmental considerations
- Communicate to both technical and non-technical senior audiences the intended outcomes of the policy and what successful end-to-end delivery looks like
- Manage the development of mechanisms to drive continuous improvement within wider government and across national and international standards, enforce sanctions and encourage the sharing of best practice
- Review quantitative and qualitative data to support the creation of evidence-based policy, evaluating and presenting evidence within the appropriate tooling

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. Training, Communication or Policy and Programme Management)

External

Suitable for an individual who has worked in security policy in industry

Role	Corporate Enablers

Policy Principal

Role summary

The role of Security Policy is to develop, implement and maintain business-enabling policies and processes relevant to the Government Security Profession, taking into account local requirements and ensuring adherence to applicable regulation and wider departmental and government policies.

Typical role level expectations

- Lead the establishment of an appropriate protective security organisational posture and encourage an effective risk-based approach to security across the estate
- Provide policy leadership and thought leadership to technical and non-technical stakeholders
- Lead the development of mechanisms to drive continuous improvement within wider government and across national and international standards, enforce sanctions, and encourage the sharing of best practice
- Shape strategic direction based on quantitative and qualitative data to support the creation of evidence-based policy

Entry route

Internal

Suitable for an individual from the Government Security Profession or other relevant profession (e.g. Training, Communication or Policy and Programme Management)

External

Suitable for an individual who has worked in security policy in industry

Role	Corporate Enablers

Policy

Minimum skill expectations

Skill	Skill level	Training	Success profiles
Protective security	Working	**Repository**	Seeing the big picture*
Legal and regulatory environment and compliance	Working	**Repository**	Communicating and influencing
Applied research	Awareness	**Repository**	Leadership
Risk understanding and mitigation	Awareness	**Repository**	
Threat understanding	Awareness	**Repository**	

*Principal behaviour

Skill levels are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Development

Suggested training	Indicative professional qualifications/accreditations
• Risk management course • Threat awareness course • Regulatory, compliance or legislative course • Policy and report writing course	• Membership of a relevant institution or body • Relevant industry or government qualifications and accreditations

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC

Role	Corporate Enablers

Policy

Minimum skill expectations

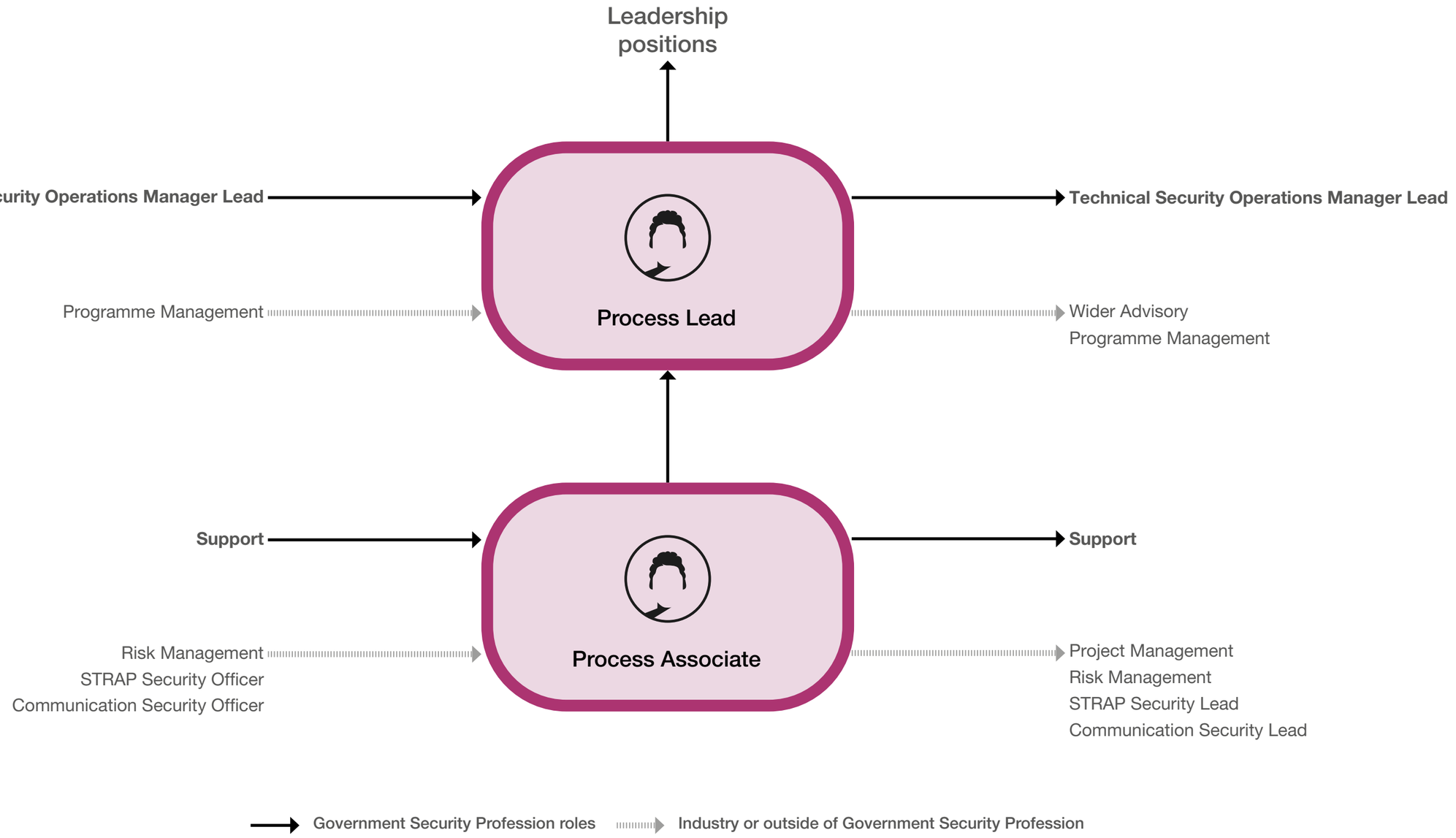
Skill	Role level		
	Policy Associate	Policy Lead	Policy Principal
	Skill level		
Protective security	Working	Practitioner	Expert
Legal and regulatory environment and compliance	Working	Practitioner	Expert
Applied research	Awareness	Working	Working
Risk understanding and mitigation	Awareness	Working	Working
Threat understanding	Awareness	Working	Working

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Role	Corporate Enablers

Process

Suggested entry and exit roles are indicative only and non-exhaustive



Role	Corporate Enablers

Process Associate

Role summary

The role of Process is to oversee certain specialist security processes, including processes related to STRAP assets and the provision of oversight of communications device security throughout the organisation, to facilitate compliance with security procedures and safeguard organisational information and technology assets.

Typical role level expectations

- Support adequate protection of assets by rigorous controls and audit, ensuring procedures for controlling access, use, and decommissioning of equipment and information are robust
- Ensure communications devices and STRAP and CRYPTO materials are appropriately secured where necessary, and support user access management processes and technologies
- Document procedures for administration and use of communication security equipment, STRAP and CRYPTO materials
- Support operation of appropriate improvement plans and work with organisations to establish STRAP and CRYPTO requirements to achieve their objectives
- Support the secure use, custody, movement or destruction of classified STRAP material, and account for communications security material and associated key material
- Support the organisation's regular inventory and audit of communications and communication security equipment, and carry out cryptographic security tasks, including ordering key materials from the Key Production Agency and co-ordinating with National Cyber Security Centre on IS4 audit

Entry route

Internal

Suitable for an individual from the Government Security Profession

External

Suitable for an individual who has worked in information security in the private sector with particularly high assurance requirements

Role	Corporate Enablers

Process Lead

Role summary

The role of Process is to oversee certain specialist security processes, including processes related to STRAP assets and the provision of oversight of communications device security throughout the organisation, to facilitate compliance with security procedures and safeguard organisational information and technology assets.

Typical role level expectations

- Manage protection of assets by rigorous controls and audit, ensuring procedures for controlling access, use, and decommissioning of equipment and information are robust
- Manage a team in ensuring communications devices and STRAP and CRYPTO materials are appropriately secured where necessary, and lead on user access management processes and technologies
- Manage the documentation procedures for administration and use of communication security equipment, STRAP or CRYPTO materials
- Lead operations of appropriate improvement plans and lead organisations to establish STRAP or CRYPTO requirements to achieve their objectives
- Manage and lead the use, custody, movement or destruction of classified STRAP material, and account for communications security material and associated key material
- Oversee a team's support to organisation's regular inventory and audit of communications and communication security equipment, and manage cryptographic security tasks

Entry route

Internal

Suitable for an individual from the Government Security Profession

External

Suitable for an individual who has worked in information security in the private sector with particularly high assurance requirements

Role	Corporate Enablers

Process

Minimum skill expectations

Skill	Skill level	Training	Success profiles
Legal and regulatory environment and compliance	Working	Repository	Seeing the big picture*
Compliance monitoring and controls testing	Awareness	Repository	Communicating and influencing
Risk understanding and mitigation	Awareness	Repository	Making effective decisions
Secure operations management	Awareness	Repository	Working together
Protective security	Awareness	Repository	
Threat understanding	Awareness	Repository	

*Principal behaviour

Skill levels are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Development

Suggested training	Indicative professional qualifications/accreditations
• STRAP Security Officer course • Communication security course • Risk management course • Threat awareness course • Regulatory, compliance or legislative course	• Membership of a relevant institution or body • Relevant industry or government qualifications and accreditations

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC

Role	Corporate Enablers

Process

Minimum skill expectations

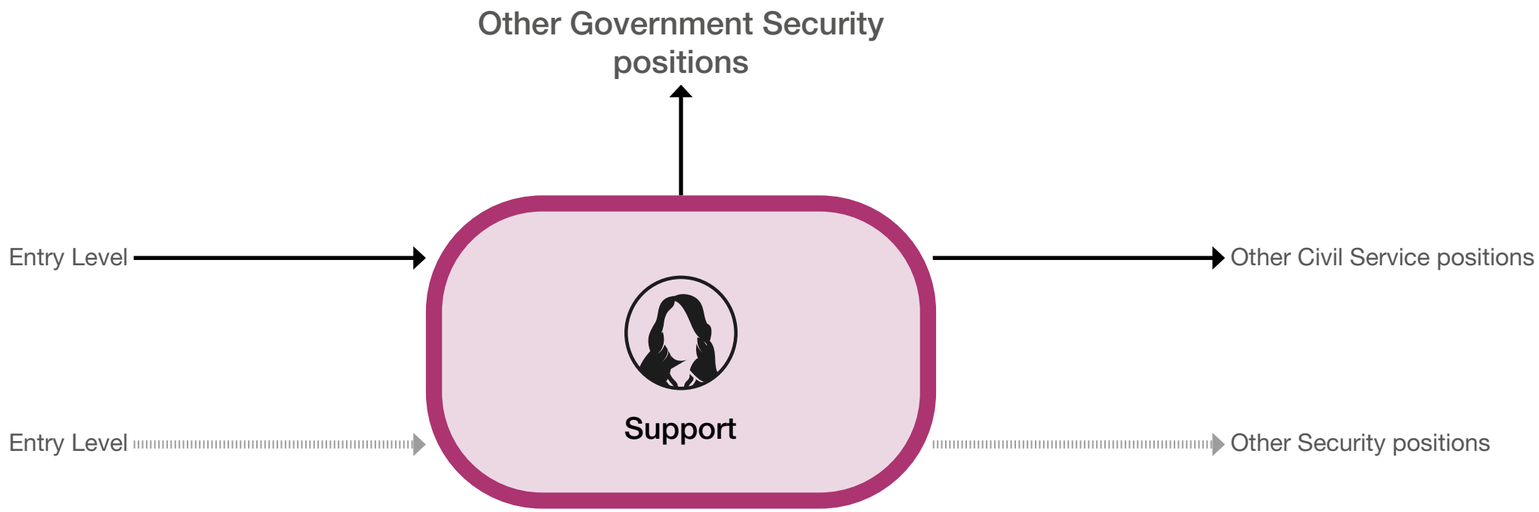
Skill	Role level	
	Process Associate	Process Lead
	Skill level	
Legal and regulatory environment and compliance	Working	Practitioner
Compliance monitoring and controls testing	Awareness	Working
Risk understanding and mitigation	Awareness	Working
Secure operations management	Awareness	Working
Protective security	Awareness	Awareness
Threat understanding	Awareness	Awareness

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Role	Corporate Enablers

Support

Suggested entry and exit roles are indicative only and non-exhaustive



Government Security Profession roles

Industry or outside of Government Security Profession

Role	Corporate Enablers

Support

Role summary

The role of Support is to provide efficient and effective administration, as well as assistance to protective security teams, ensuring the successful mitigation of security risks.

Typical role level expectations

- Provide support to the Government Security Profession, effectively managing multiple workloads with conflicting priorities
- Act as the focal point for security queries, collating and communicating necessary policies, procedures and threat information
- Ensure compliance to local security operations, policy and procedures

Entry route

Internal

Entry level

External

Entry level

Role	Corporate Enablers

Support

Minimum skill expectations

Skill	Skill level	Training	Success profiles
Applied Personnel Security	Awareness	**Repository**	Working together*
Applied Physical Security	Awareness	**Repository**	Delivering at pace
Applied security capability	Awareness	**Repository**	Developing self and others
Applied Technical Security	Awareness	**Repository**	Managing a quality service
Legal and regulatory environment and compliance	Awareness	**Repository**	
Protective security	Awareness	**Repository**	
Risk understanding and mitigation	Awareness	**Repository**	
Threat understanding	Awareness	**Repository**	

*Principal behaviour

Skill levels are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Development

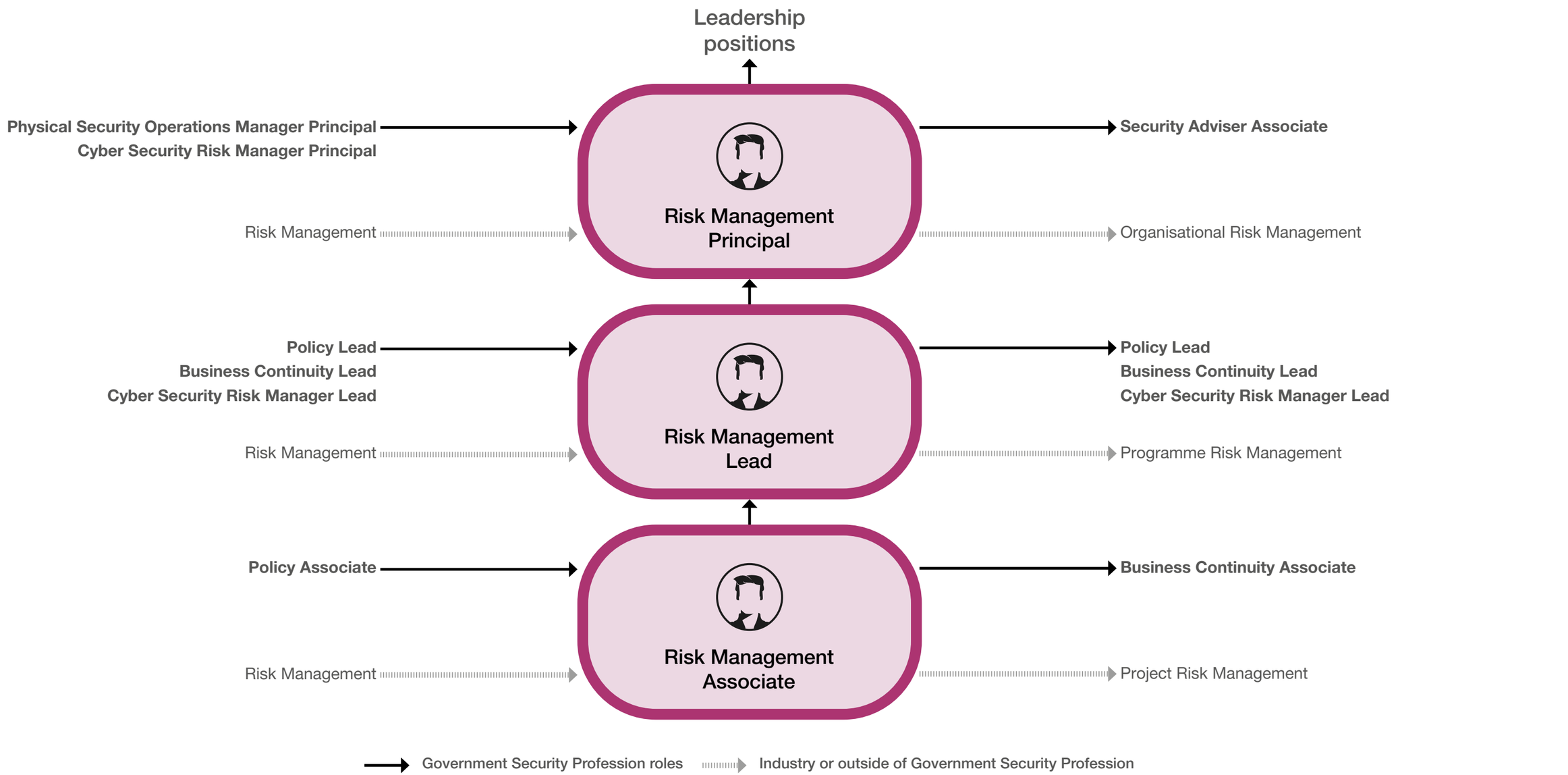
Suggested training	Indicative professional qualifications/accreditations
• Risk management course • Threat awareness course • Regulatory, compliance or legislative course	• Membership of a relevant institution or body • Relevant industry or government qualifications and accreditations

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC

Role	Corporate Enablers

Risk Management

Suggested entry and exit roles are indicative only and non-exhaustive



Role	Corporate Enablers

Risk Management Associate

Role summary

The role of Risk Management is to identify and evaluate security risks to information, systems and processes owned by the organisation, and proactively provide appropriate advice, drawing on a wide variety of sources, to stakeholders across the organisation and at a variety of levels.

Typical role level expectations

- Communicate risk assessment outcomes to stakeholders in ways that support effective security, risk management and decision-making, and advise stakeholders on their approach to risk assessment in the context of their business outcomes
- Monitor the efficiency and effectiveness of the risk management processes across the organisation, and make recommendations for continuous improvement
- Conduct reviews and risk assessments when necessary and feed back findings to the relevant parties
- Interpret and contribute to the development of risk management-related policy, and assure the ongoing appropriateness of policy in accordance with regulation and wider departmental and government policies

Entry route

Internal

Suitable for an individual from a role within the Government Security Profession

External

Suitable for an individual who has worked in a risk management role in industry

Role	Corporate Enablers

Risk Management Lead

Role summary

The role of Risk Management is to identify and evaluate security risks to information, systems and processes owned by the organisation, and proactively provide appropriate advice, drawing on a wide variety of sources, to stakeholders across the organisation and at a variety of levels.

Typical role level expectations

- Communicate risk assessment outcomes to senior stakeholders in ways that support effective security, risk management and decision-making, and advise senior stakeholders on their approach to risk assessment in the context of their organisational outcomes
- Manage risk management processes across an organisation, reviewing their efficiency and effectiveness, leading recommendations for continuous improvement
- Assess reviews and risk assessments and communicate effectively to relevant senior stakeholders
- Develop risk management-related policy, and assure the ongoing appropriateness of policy in accordance with regulation and wider organisational and government policies

Entry route

Internal

Suitable for an individual from a role within the Government Security Profession

External

Suitable for an individual who has worked in a risk management role in industry

Role	Corporate Enablers

Risk Management Principal

Role summary

The role of Risk Management is to identify and evaluate security risks to information, systems and processes owned by the organisation, and proactively provide appropriate advice, drawing on a wide variety of sources, to stakeholders across the organisation and at a variety of levels.

Typical role level expectations

- Communicate risk assessment outcomes to leaders across government in ways that support effective security strategy, risk management and decision-making, and advise leaders on their approach to risk assessment in the context of their organisational outcomes
- Lead complex risk management processes across an organisation, reviewing their efficiency and effectiveness, leading recommendations for continuous improvement
- Draw key conclusions from reviews and risk assessments for prioritised concerns and communicate effectively to relevant leadership
- Lead and champion risk management-related policy, and assure the ongoing appropriateness of policy in accordance with regulation and wider organisational and government policies

Entry route

Internal

Suitable for an individual from a role within the Government Security Profession

External

Suitable for an individual who has worked in a risk management role in industry

Role	Corporate Enablers

Risk Management

Minimum skill expectations

Skill	Skill level	Training	Success profiles
Risk understanding and mitigation	Working	**Repository**	Seeing the big picture*
Legal and regulatory environment and compliance	Working	**Repository**	Communicating and influencing
Protective security	Working	**Repository**	Making effective decisions
Threat understanding	Working	**Repository**	Working together

*Principal behaviour

Skill levels are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Development

Suggested training	Indicative professional qualifications/accreditations
• Threat awareness course • Risk management course	• Membership of a relevant institution or body • Relevant industry or government qualifications and accreditations

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC

Role	Corporate Enablers

Risk Management

Minimum skill expectations

Skill	Role level		
	Risk Management Associate	Risk Management Lead	Risk Management Principal
	Skill level		
Risk understanding and mitigation	Working	Practitioner	Expert
Legal and regulatory environment and compliance	Working	Practitioner	Practitioner
Protective security	Working	Practitioner	Practitioner
Threat understanding	Working	Working	Working

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert

Skills

What are skills?

Skills refer to expertise or aptitude in a capability that is needed to do something successfully. There are 25 security skills.

The security skills are used to indicate the typical knowledge and experience required for each of the 46 security roles in the career framework.

Who are they for?

The security skills are for all government staff working in a security role, or anyone who wants to find out more about what is required for different security roles. They are also for some members of the wider public sector who have adopted our model.

How do I access them?

You can access the skills through clicking on the ‘Skills’ bar at the top of this page. Click on any skill to see skill level definitions at awareness, working practitioner and expert level.

What is a skills profiling tool?

A skills profiling tool is an online tool accessible across government that maps training to skill levels to help you navigate your career. It will be made available as part of the next career framework. Government Security Profession will inform the community when it is available.

How do I use the career framework skills?

It is important to link the skills to your development and use them to inform career and development discussions with your line manager. This will help you to agree which development areas to focus on.

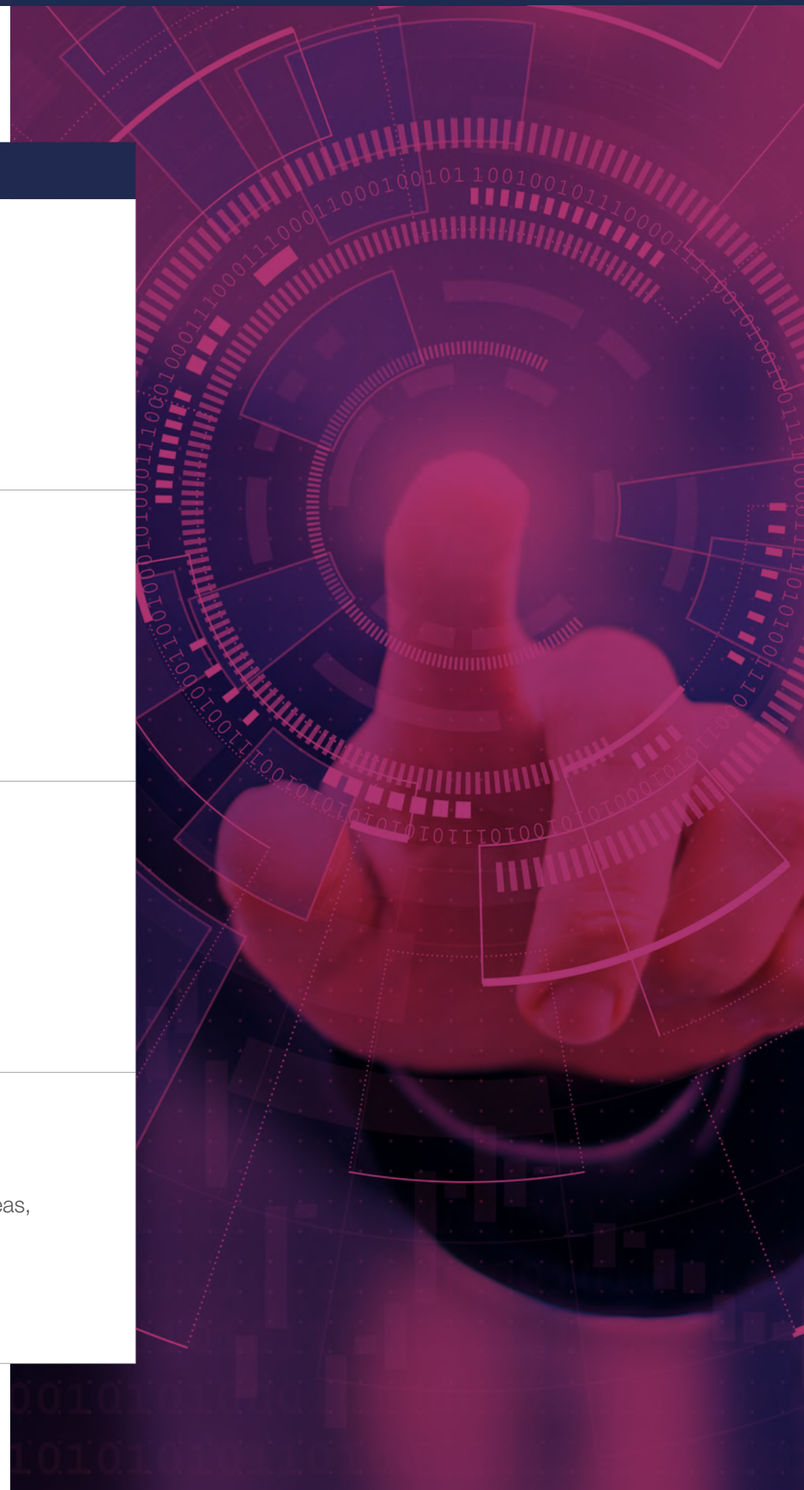
It is important to remember the following:

- the skill profiles are for guidance only and shouldn’t be used as an exact measure for a particular role
- achieving the skill profile for a role at a different grade level does not entitle someone to that grade, but it may enhance their chances when applying for that role
- you don’t need to achieve all aspects of the skill profile for a role before you can apply for it – we often learn best by stretching ourselves to take on new responsibilities
- the indicative training mapped to the career framework skills refers to only 10% of development – click on ‘Development’ to learn about the 70/20/10 approach

Skill level definitions

Skill level	Description
Awareness ★	Applies knowledge and experience of the skill, including tools and techniques, adopting those most appropriate for the environment.
Working ★★	Applies knowledge and experience of the skill with others, including tools and techniques, adopting those most appropriate for the environment.
Practitioner ★★★	Shares knowledge and experience of the skill with others, including tools and techniques, defining those most appropriate for the environment.
Expert ★★★★	Has knowledge and experience in the application of this skill. Is a recognised specialist and adviser in this skill including user needs, generation of ideas, methods, tools and leading or guiding others in best practice use.

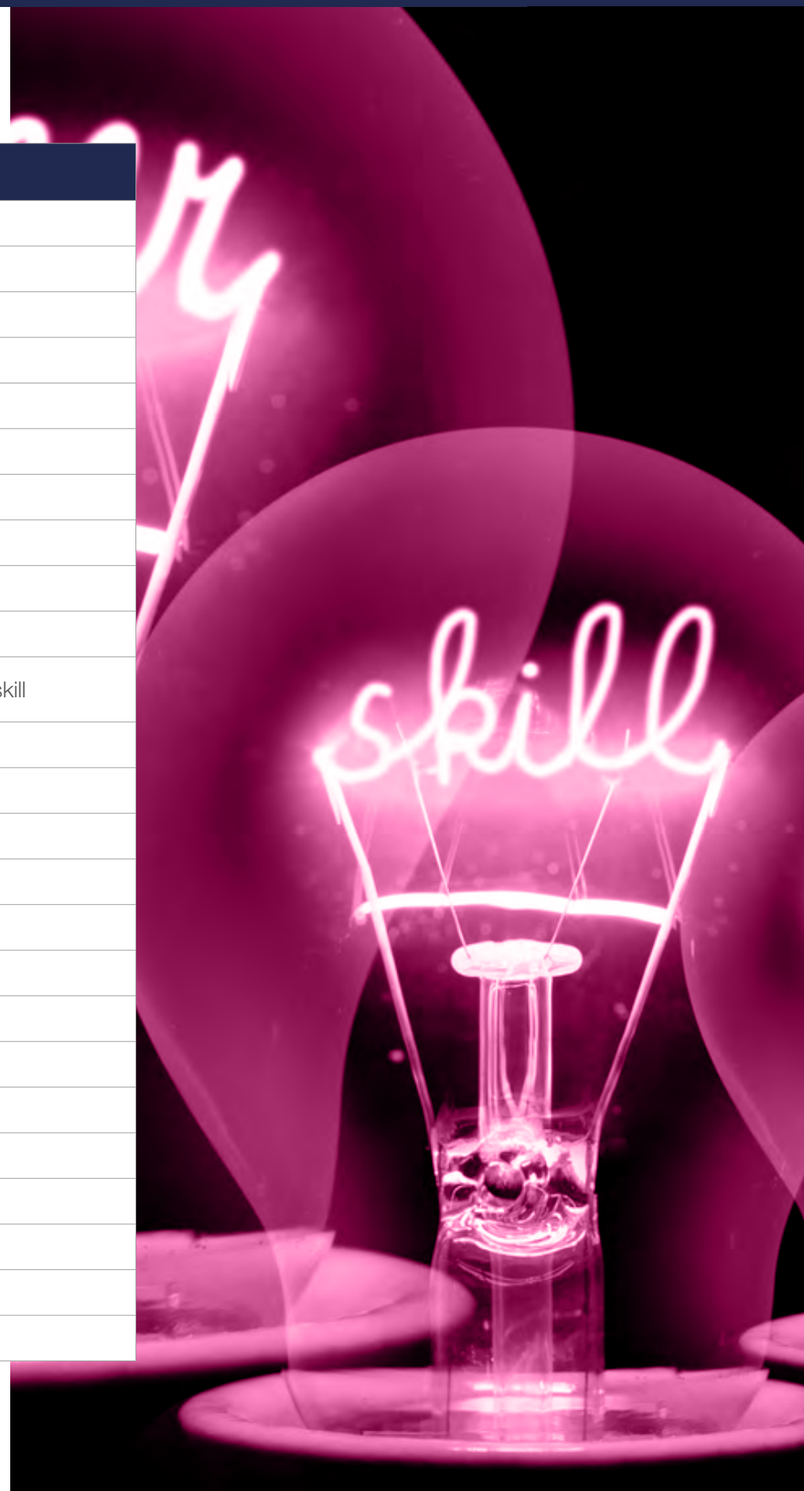
Skill source: Digital, Data and Technology **Capability Framework**



List of skills

Skill	Specialism	Source
Applied Personnel Security	Personnel Security	**CPNI**
Applied Physical Security	Physical Security	**CPNI**
Applied research	Cross-specialism	**CIISEC Framework** I2 skill
Applied security capability	Cyber Security	NCSC Information Risk Assurance skill 5.5
Applied Technical Security	Technical Security	CPNI
Business continuity management	Cross-specialism	**Business Continuity Institute**
Compliance monitoring and controls testing	Cyber Security	**CIISEC Framework** D2 skill
Cyber Security operations	Cyber Security	**CIISEC Framework** E2 skill
Design	Cross-specialism	**Digital, Data and Technology**
Forensics	Cyber Security	**CIISEC Framework** F3 skill
Incident management, incident investigation and response	Cyber Security	**NCSC** (skill definition), **CIISEC Framework** F2 skill
Information risk assessment and risk management	Cyber Security	NCSC Information Risk Assurance skill 5.2
Intrusion detection and analysis	Cyber Security	**CIISEC Framework** F1 skill
Investigative interviewing	Personnel Security	College of Policing Investigation
Legal and regulatory environment and compliance	Cross-specialism	**CIISEC Framework** A6 skill
Penetration testing	Cyber Security	**CIISEC Framework** D4 skill
Protective security	Cross-specialism	**CPNI**
Risk understanding and mitigation	Cross-specialism	**CIISEC Framework** B3 skill
Secure design	Cyber Security	**Digital, Data and Technology**
Secure development	Cyber Security	**Digital, Data and Technology**
Secure operations management	Cross-specialism	**CIISEC Framework** E1 skill
Secure supply chain management	Cross-specialism	**CPNI**
Security architecture	Cyber Security	NCSC Information Assurance skill 6.3
Threat intelligence and threat assessment	Cyber Security	**CIISEC Framework** B1 skill
Threat understanding	Cross-specialism	**NIST**, **CPNI**

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profession or the NCSC, CPNI or UKNACE.



Applied Personnel Security

Skill	Skill source	Skill type
Applied Personnel Security	CPNI	Personnel Security

Skill definition	
Applied Personnel Security refers to the policies, practices and methodologies that seek to mitigate the risk of workers (insiders) exploiting legitimate access to an organisation's assets for unauthorised purposes.	
Awareness ★	Describes concepts of Personnel Security, including the significance of the Personnel Security specialism, the relationship between all specialisms and how the specialisms relate to the security function across government Promotes Personnel Security within the local working environment
Working ★★	Applies concepts of Personnel Security within the context of the other specialisms/enablers Champions Personnel Security within the wider security function, providing advice to others
Practitioner ★★★	Develops and applies new concepts in Personnel Security, involving the other specialisms/enablers Develops individuals and contributes to the development of the specialism Promotes Personnel Security as a business enabler throughout the organisation Engages with the UK security community
Expert ★★★★	Leads innovation in Personnel Security, taking into account other specialisms/enablers and business drivers Promote the development of individuals against the career framework Promote the use of Personnel Security as a business enabler at board or senior management level Active member of the UK security community

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert. Skill levels are cumulative – for example, to hold a 'practitioner' level in this skill, you must meet the requirements of 'working' level too.

Applied Personnel Security

Skill	Skill source	Skill type
Applied Personnel Security	**CPNI**	**Personnel Security**

Indicative training

Indicative training	Format	Length	Provider type
CERT Insider Threat Program Evaluator Certificate	Certification, Classroom, eLearning	2 days	External
Fundamentals of Employment Law	Classroom	2 days	External
Grievance, Discipline and Dismissals	Classroom	2 days	External
How to Prepare for an Employment Tribunal	Classroom	2 days	External
Security Management Course Level 3	eLearning	Self-paced	External
Social Media and Employment Law	Classroom	1 day	External
The role of national security vetting and aftercare	To be defined	To be defined	HM Government

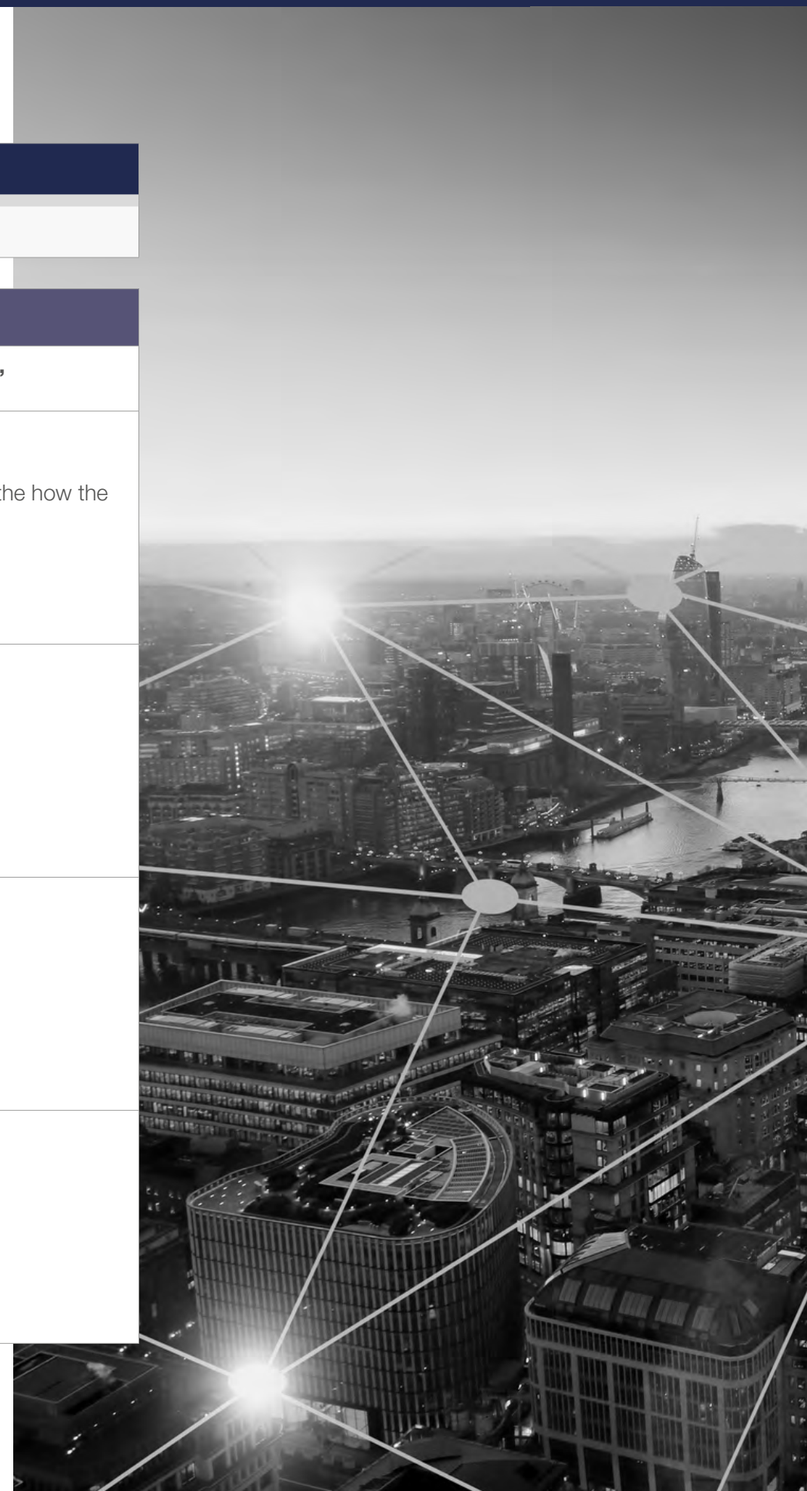
Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profression of the NCSC, CPNI or UKNACE.

Applied Physical Security

Skill	Skill source	Skill type
Applied Physical Security	CPNI	Physical Security

Skill definition	
Applied Physical Security refers to the policies, practices and methodologies used to protect assets, including people, services, infrastructure, systems, places, equipment and networks.	
Awareness ★	Describes concepts of Physical Security, including the significance of the Physical Security specialism, the relationship between all specialisms, and the how the specialisms relate to the security function across government Promotes Physical Security within the local working environment
Working ★★	Applies concepts of Physical Security within the context of the other specialisms/enablers Champions Physical Security within the wider security function, providing advice to others
Practitioner ★★★	Develops and applies new concepts in Physical Security, involving the other specialisms/enablers Develops individuals and contributes to the development of the specialism Promotes Physical Security as a business enabler throughout the organisation Engages with the UK security community
Expert ★★★★	Leads innovation in Physical Security, taking into account other specialisms/enablers and business drivers Promotes the development of individuals against the career framework Promotes the use of Physical Security as a business enabler at board or senior management level Is an active member of the UK security community

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert. Skill levels are cumulative – for example, to hold a ‘practitioner’ level in this skill, you must meet the requirements of ‘working’ level too.



Applied Physical Security

Skill	Skill source	Skill type
Applied Physical Security	CPNI	Physical Security

Indicative training

Indicative training	Format	Length	Provider type
IQ Level 5 Physical Security Professional	eLearning	Self-paced	External
Physical Security Professional	Certification	Self-paced	External
Security Management Course Level 3	eLearning	Self-paced	External

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profression of the NCSC, CPNI or UKNACE.

Applied research

Skill	Skill source	Skill type
Applied research	**CIISEC Framework** I2 skill	Cross-specialism

Skill definition	
Applied research is the understanding and application of research methods to assure and maintain best practice within an organisation. The principles of applied research are vulnerability research and discovery. They lead to the development of exploits; reverse engineering and researching mitigation bypasses; cryptographic research leading to the assessment of existing algorithms; and the use of existing knowledge in experimental development to produce new or substantially improved devices, products and processes.	
Awareness ★	Describes the basic principles of applied research and how it applies to security Conducts basic applied research under supervision Understands the principles of applied research in information security and may have undertaken some directed practical examples in a training environment
Working ★★	Explains the principal requirements of applied research and applies methods correctly Conducts basic applied research without supervision, e.g. leading to the development of simple exploits or an assessment of an existing cryptographic algorithm
Practitioner ★★★	Leads teams conducting applied research Advises colleagues on choice and application of research methods to assure best practice
Expert ★★★★	Leads applied research activities for an organisation Undertakes advanced research Helps an organisation adopt a wide range of research methods Leads a community of practice to help an organisation continually assure, improve and innovate their research

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert. Skill levels are cumulative – for example, to hold a ‘practitioner’ level in this skill, you must meet the requirements of ‘working’ level too.

Applied research

Skill	Skill source	Skill type
Applied research	**CIISEC Framework** I2 skill	Cross-specialism

Indicative training

Indicative training	Format	Length	Provider type
SEC402: Cybersecurity Writing: Hack the Reader	eLearning	2 days	External

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profression of the NCSC, CPNI or UKNACE.

Applied security capability

Skill	Skill source	Skill type
Applied security capability	NCSC Information Risk Assurance Skill 5.5	Cyber Security

Skill definition
Applied security capability is formed of a set of complementary security skills. Individual roles may have a requirement for a different profile across these skills. Applied security capability involves 4 elements: **1. Security requirement elicitation: gathering and deriving meaningful security requirements to support an identified need** **2. Application of security capabilities: apply standardised or unique security capabilities to address security needs** **3. Provision or assurance and confidence: provide confidence that business priorities are appropriately protected** **4. Security and risk reporting: communicate security and risk effectively**

Awareness ★	Understands why security must support business needs and the importance of being able to demonstrate that relationship Aware of some key, well-understood, security principles and can demonstrate an awareness of some Cyber Security relevant technologies Understands why it is important to gain confidence in security measures and can describe some straightforward mechanisms such as pen-tests Understands and can describe basic security concepts
Working ★★	Aware of the need to provide traceability between business need and security requirements. Gathers and derives simple or obvious security requirements for highly standardised use cases, using well-established guidance that is unlikely to be contentious Provides basic security advice to address standard security needs. Advice could be written or verbal. Knows the limitations and scope for what advice can be given and when to draw on others' expertise Is aware of and follows appropriate process such as quality control arrangements Understands and can apply a range of basic approaches to assurance and understands their applicability Meaningfully describes straightforward security concepts and their business applicability Ensures security recommendations and risk statements developed are reasonably and well contextualised to the business need under consideration

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert. Skill levels are cumulative – for example, to hold a 'practitioner' level in this skill, you must meet the requirements of 'working' level too.

Applied security capability

Skill	Skill source	Skill type
Applied security capability	NCSC Information Risk Assurance Skill 5.5	Cyber Security

Skill definition
Applied security capability is formed of a set of complementary security skills. Individual roles may have a requirement for a different profile across these skills. Applied security capability involves 4 elements: **1. Security requirement elicitation: gathering and deriving meaningful security requirements to support an identified need** **2. Application of security capabilities: apply standardised or unique security capabilities to address security needs** **3. Provision or assurance and confidence: provide confidence that business priorities are appropriately protected** **4. Security and risk reporting: communicate security and risk effectively**

Practitioner ★★★	Elicits security requirements based on straightforward approaches such as threat/vulnerability/impact analysis. Security needs will include an understanding of the user as part of the overall system Helps organisations to derive and reason about their security needs, such as understanding and applying security principles to particular business scenarios Interprets and clarifies management or organisational intention with regards to security, such as described in risk appetite statements. This includes interpreting such statements into meaningful and appropriate security requirements Provides security advice to non-standard use cases, drawing on and using experts in specific topics or technologies Uses standardised control frameworks (such as 27001/2) appropriately, with awareness of their strengths and limitations Understands when security measures might impact on users or business needs and provides effective advice to help the business make an appropriate decision Applies a range of assurance approaches, with a clear understanding of the strengths and limitations of each approach. There is a clear ability to map the assurance options recommended directly to the security need to be addressed Assurance and confidence is not limited to a point in time, but seeks to address confidence across the system/service life cycle Provides meaningful security and risk communication in a range of scenarios. Understands and takes account of the limitations of various risk communication mechanisms such qualitative v quantitative approaches

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert. Skill levels are cumulative – for example, to hold a ‘practitioner’ level in this skill, you must meet the requirements of ‘working’ level too.

Applied security capability

Skill	Skill source	Skill type
Applied security capability	NCSC Information Risk Assurance Skill 5.5	Cyber Security

Skill definition
Applied security capability is formed of a set of complementary security skills. Individual roles may have a requirement for a different profile across these skills. Applied security capability involves 4 elements: **1. Security requirement elicitation: gathering and deriving meaningful security requirements to support an identified need** **2. Application of security capabilities: apply standardised or unique security capabilities to address security needs** **3. Provision or assurance and confidence: provide confidence that business priorities are appropriately protected** **4. Security and risk reporting: communicate security and risk effectively**

Expert ★★★★	Considers complicated, non-obvious security needs, e.g. where the connections between business need, the technology that supports that need and how it might be impacted are important to work out Works closely with those who 'own' business needs, deduces their tolerances with regard to things they care about and turns those into meaningful security statements that can be applied. This might be either complicated and specific, or simple scenarios with broad applicability Delivers security advice that is contextualised and appropriate for the strategic customer need Avoids providing 'point' solutions or advice that does not address the overall key need. Looks at the wider 'system' including sociotechnical considerations (e.g. the role the user plays in meeting the desired security outcomes) Provides security advice that extends beyond particular technologies of which the candidate is familiar and draws upon and directs appropriate expertise to solve the bigger security problem. Ensures the overall technical coherence and quality of advice Together with assurance experts, develops and applies novel approaches to assurance of products/systems/services Understands and applies different approaches to product, implementation and operational assurance. Uses each appropriately to derive a genuine understanding of confidence that the overall business objective is protected Provides technical leadership for specific experts (be they pen-testers, product or behavioural assurance, for example) in the context of a specific technical assurance or confidence challenge Effectively communicates difficult risk and security concepts in accessible ways that can be clearly understood by business leaders. Contributes to and develops risk communication strategies

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert. Skill levels are cumulative – for example, to hold a 'practitioner' level in this skill, you must meet the requirements of 'working' level too.

Applied security capability

Skill	Skill source	Skill type
Applied security capability	NCSC Information Risk Assurance Skill 5.5	Cyber Security

Indicative training

Indicative training	Format	Length	Provider type
BCS Certificate in Information Security Management Principles	Classroom	5 days	External
Board-level Cyber Security Strategy Training	Classroom	1 hour	External
Certified Information Systems Security Professional	Certification, Classroom	5 days	External
Certified ISO27001 Practitioner	Classroom	5 days	External
Certified Protection Professional	Certification	Self-paced	External
CompTIA Advanced Security	Certification, Classroom	5 days	External
CompTIA Security+	Certification, Classroom	5 days	External
Cyber 101	eLearning	2–6 hours	HM Government
Cyber Essentials Consultancy	eLearning	1 day	External
Cyber Security Development Programme	Classroom, Onsite	4 years	HM Government
Cyber Security for Senior Executives and Senior Information Risk Owners	Classroom	1 day	External
Cyber Security Fundamentals	Classroom	2 days	External
Cyber Security Technologist NVQ Level 4 Apprenticeship	Apprenticeship	To be defined	External
Cyber Security – An Introduction	eLearning	2 months	External
Foundation Certificate in Cyber Security	Classroom	5 days	External
Fundamentals of Information Assurance in Her Majesty's Government	Classroom	2 days	External
Introduction to Security	eLearning	Self-paced	HM Government
MGT525: IT Project Management, Effective Communication, and PMP Exam Prep	Classroom	6 days	External
SEC402: Cybersecurity Writing: Hack the Reader	eLearning	2 days	External
Security Management Course Level 3	eLearning	Self-paced	External

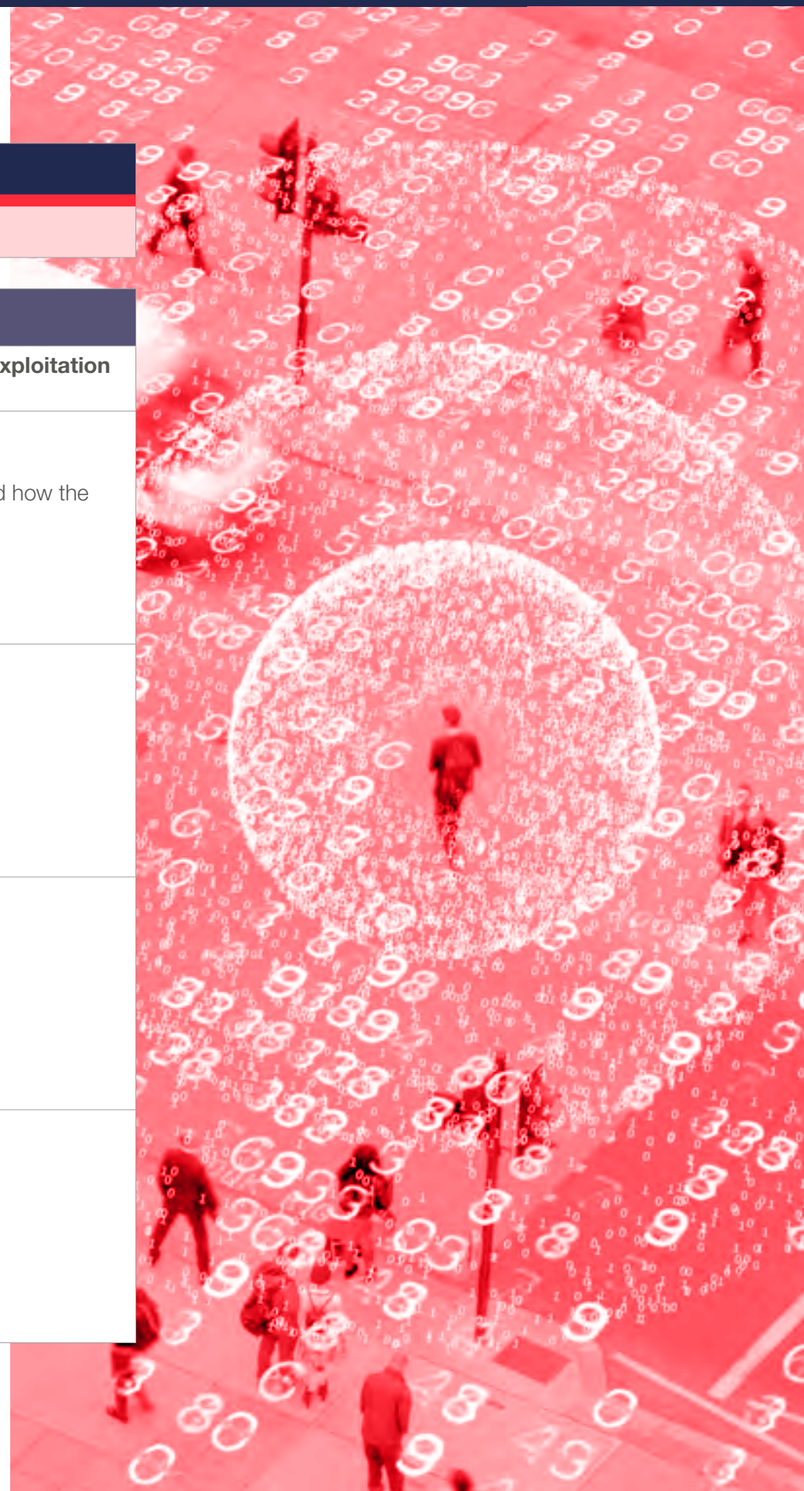
Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profression of the NCSC, CPNI or UKNACE.

Applied Technical Security

Skill	Skill source	Skill type
Applied Technical Security	CPNI	Technical Security

Skill definition	
Applied Technical Security refers to the policies, practices, and methodologies used to protect sensitive information and technology from close acquisition or exploitation by hostile actors, as well as other forms of technical manipulation.	
Awareness ★	Describes concepts of Technical Security, including the significance of the Technical Security specialism, the relationship between all specialisms, and how the specialisms relate to the security function across government Promotes Technical Security within the local working environment
Working ★★	Applies concepts of Technical Security within the context of the other specialisms/enablers Champions Technical Security within the wider security function, providing advice to others
Practitioner ★★★	Develops and applies new concepts in Technical Security, involving the other specialisms/enablers Develops individuals and contributes to the development of the specialism Promotes Technical Security as a business enabler throughout the organisation Engages with the UK security community
Expert ★★★★	Leads innovation in Technical Security, taking into account other specialisms/enablers and business drivers Promotes the development of individuals against the career framework Promotes the use of Technical Security as a business enabler at board or senior management level Active member of the UK security community

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert. Skill levels are cumulative – for example, to hold a ‘practitioner’ level in this skill, you must meet the requirements of ‘working’ level too.



Applied Technical Security

Skill	Skill source	Skill type
Applied Technical Security	CPNI	Technical Security

Indicative training

Indicative training	Format	Length	Provider type
EMS-TEMPEST: EM Security and TEMPEST Fundamentals	Classroom	2 days	HM Government
Infrastructure Technical NVQ – Level 3 Apprenticeship	Apprenticeship	3 year	HM Government
Security Management Course Level 3	eLearning	Self-paced	External
Technical Reconnect	To be defined	To be defined	HM Government
Technical Surveillance Countermeasures Awareness	Classroom	1 day	HM Government
Technical Engineering NVQ – Level 3 Apprenticeship	Apprenticeship	3 year	HM Government
TSCM-DRMP: TSCM Defensive Radio Monitoring Principles	Classroom	5 days	HM Government
TSCM-RBS: Rising Building Security	Classroom	1 day	HM Government
TSCM-SK: TSCM Search Kit	Classroom, Onsite	3 days	HM Government
TSCM-VIT: TSCM for VoIP Telephony	Classroom	4 days	HM Government
TSCM-FX: TSCM Field Exercise	Classroom, Onsite	2 days	HM Government

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profression of the NCSC, CPNI or UKNACE.

Business continuity management

Skill	Skill source	Skill type
Business continuity management	Business Continuity Institute	Cross-specialism

Skill definition	
Business continuity management helps mitigate risks to the disruption of an organisation or service, by identifying critical elements including information, assets and infrastructure, and then planning to ensure that the organisation or service can operate to the extent required in the event of a disruption.	
Awareness ★	Describes the basic principles of business continuity management Follows documented business continuity management principles and guidelines
Working ★★	Explains the importance of business continuity management Follows documented principles and guidelines for business continuity management activities with limited direction/supervision Assists with the design, development and implementation of business continuity management Assists with the implementation and execution of business continuity management
Practitioner ★★★	Leads business continuity management activities Advises others on principles and guidelines for business continuity management activities Leads teams designing, developing and implementing of business continuity management Leads teams implementing and executing business continuity management Promotes the sharing of business continuity management best practice
Expert ★★★★	Leads business continuity management activities for an organisation Promotes business continuity management principles and guidelines Advises others on business continuity management processes providing thought leadership to the field Champions business continuity management best practice

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert. Skill levels are cumulative – for example, to hold a ‘practitioner’ level in this skill, you must meet the requirements of ‘working’ level too.

Business continuity management

Skill	Skill source	Skill type
Business continuity management	**Business Continuity Institute**	Cross-specialism

Indicative training

Indicative training	Format	Length	Provider type
BCI – Business Impact Analysis	Classroom	2 days	External
BCI – Designing Business Continuity Solutions	Classroom	1 day	External
BCI – Designing and Delivering Effective Exercises	Classroom	1 day	External
BCI – Developing and Managing the Business Continuity Plan	Classroom	1 day	External
BCI – Embedding Business Continuity	Classroom	1 day	External
BCI – Incident Response and Crisis Management	Classroom	2 days	External
BCI – Introduction to Business Continuity	Classroom	2 days	External
BCI – Introduction to Organizational Resilience	Classroom	1 day	External
BCI – Policy and Programme Management	Classroom	2 days	External
BCI – Supply Chain Resilience	Classroom	1 day	External
BCI – Validating your BCM Programme	Classroom	2 days	External
EPC – Business Continuity	Classroom	Varied	External
EPC – Emergency and Crisis Management	Classroom	Varied	External
EPC – Emergency and Crisis Management – Planning and Preparedness	Classroom	Varied	External
EPC – Emergency and Crisis Management – Response and Recovery	Classroom	Varied	External
EPC – Emergency and Crisis Management – Risk	Classroom	Varied	External

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profression of the NCSC, CPNI or UKNACE.

Compliance monitoring and controls testing

Skill	Skill source	Skill type
Compliance monitoring and controls testing	**CIISEC Framework** D2 skill	Cyber Security

Skill definition	
Compliance monitoring and controls testing refers to the implementations and processes used to verify ongoing conformance to security and/or legal and regulatory requirements against technical, physical, procedural and personnel controls. The principles of the skill are to define and implement processes to verify ongoing conformance to security and/or legal and regulatory requirements, and carry out security compliance checks in accordance with an appropriate methodology. Compliance monitoring and controls testing covers compliance checks and tests against technical, physical, procedural and personnel controls.	
Awareness ★	Describes the benefits of compliance monitoring and controls testing and can list the common compliance monitoring standards, e.g. ISO/IEC 27001, PCI DSS, IAMM Maintains understanding of statutes and regulations Follows documented procedures for compliance or regulations
Working ★★	Explains the main principles and processes involved in conducting a compliance monitoring and controls testing exercise Reviews and implements alterations to operating procedures in response to changes in regulations or statutes Educates/provides guidance on the implementation of regulations
Practitioner ★★★	Conducts compliance monitoring and controls testing Understands wider regulatory context and how it can be applied to best meet the business needs of the organisation Designs and leads implementation of business change, where required by regulation Leads the implementation of regulations within the security function
Expert ★★★★	Leads compliance monitoring and controls testing activities for an organisation Champions opportunities that regulation and compliance can provide to an organisation at senior manager or board level Promotes compliance or regulation within the security function Reports significant non-compliance issues to senior management

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert. Skill levels are cumulative – for example, to hold a ‘practitioner’ level in this skill, you must meet the requirements of ‘working’ level too.

Compliance monitoring and controls testing

Skill	Skill source	Skill type
Compliance monitoring and controls testing	**CIISEC Framework** D2 skill	Cyber Security

Indicative training

Indicative training	Format	Length	Provider type
CompTIA Advanced Security	Certification, Classroom	5 days	External
Cyber Security for Information Asset Owners	Classroom	1 day	External
Fundamentals of Information Assurance in Her Majesty's Government	Classroom	1 day	HM Government
MGT512: Security Leadership Essentials for Managers	Classroom	5 days	External
SEC566: Implementing and Auditing the Critical Security Controls – In-Depth	Classroom	5 days	External

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profression of the NCSC, CPNI or UKNACE.

Cyber Security operations

Skill	Skill source	Skill type
Cyber Security operations	**CIISEC Framework** E2 skill	Cyber Security

Skill definition	
Cyber Security operations are the secure configuration and maintenance of information, controls and communications equipment in accordance with relevant security policies, standards and guidelines. This includes the configuration of information security devices (e.g. firewalls) and protective monitoring tools (e.g. Security Information and Event Management (SIEM)). Principles include implementing security policy (e.g. patching policies) and security operating procedures in respect of system and/or network management, maintaining security records and documentation in accordance with security operating procedures, and monitoring processes for violations of relevant security policies (e.g. acceptable use, security).	
Awareness ★	Recognises the need for information systems and services to be operated and monitored securely and can list some of the main policies and practices involved in achieving this Explains the main principles of secure configuration of role specific security components and devices, including firewalls and protective monitoring tools (e.g. SIEM)
Working ★★	Demonstrates experience applying the principles of secure configuration of role-specific security components and devices in a training or academic environment, for example through participation in syndicate exercises, undertaking practical exercises, and/or passing a test or examination Supports the overall aims of a Cyber Security operations-related team, e.g. a monitoring team Applies routine security procedures appropriate to the role, such as patching, managing access rights, malware, protection or vulnerability testing under direction/supervision Develops and tests rules for detecting violations of security operating procedures under supervision
Practitioner ★★★	Develops security operating procedures for use across multiple information systems or maintains compliance with them Applies routine security procedures appropriate to the role, such as patching, managing access rights, malware protection or vulnerability testing with autonomy Develops and tests rules for detecting violations of security operating procedures with autonomy Leads small teams managing Cyber Security operations within an organisation
Expert ★★★★	Leads teams managing Cyber Security operations within an organisation Identifies the need for, and implements, new security operating procedures and practices to meet changing requirements Is a subject matter expert in developing and operationalising techniques for Cyber Security operations, e.g. detecting anomalous activity, automating orchestration and configuration of IT

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert. Skill levels are cumulative – for example, to hold a ‘practitioner’ level in this skill, you must meet the requirements of ‘working’ level too.

Cyber Security operations

Skill	Skill source	Skill type
Cyber Security operations	**CIISEC Framework** E2 skill	Cyber Security

Indicative training

Indicative training	Format	Length	Provider type
No indicative training identified	To be defined	To be defined	To be defined

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profression of the NCSC, CPNI or UKNACE.

Design

Skill	Skill source	Skill type
Design	Digital, Data and Technology	Cross-specialism

Skill definition	
Design is the ability to visualise, articulate and solve complex problems and concepts, making disciplined decisions based on available information and research evidence.	
Awareness ★	Describes the basic principles of design Assists with the design of systems to use across services
Working ★★	Explains concepts, principles, processes and risks of design Designs systems to balance security with business objectives
Practitioner ★★★	Leads design teams Designs systems for use across services Advises on the design of systems to balance security with business objectives
Expert ★★★★	Leads design activities for an organisation Designs systems for use across multiple services and can identify the simplest approach out of a variety of approaches Leads a community of practice to help an organisation continually assure, improve and innovate their design practices

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert. Skill levels are cumulative – for example, to hold a ‘practitioner’ level in this skill, you must meet the requirements of ‘working’ level too.

Design

Skill	Skill source	Skill type
Design	Digital, Data and Technology	Cross-specialism

Indicative training

Indicative training	Format	Length	Provider type
No indicative training identified	To be defined	To be defined	To be defined

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profression of the NCSC, CPNI or UKNACE.

Forensics

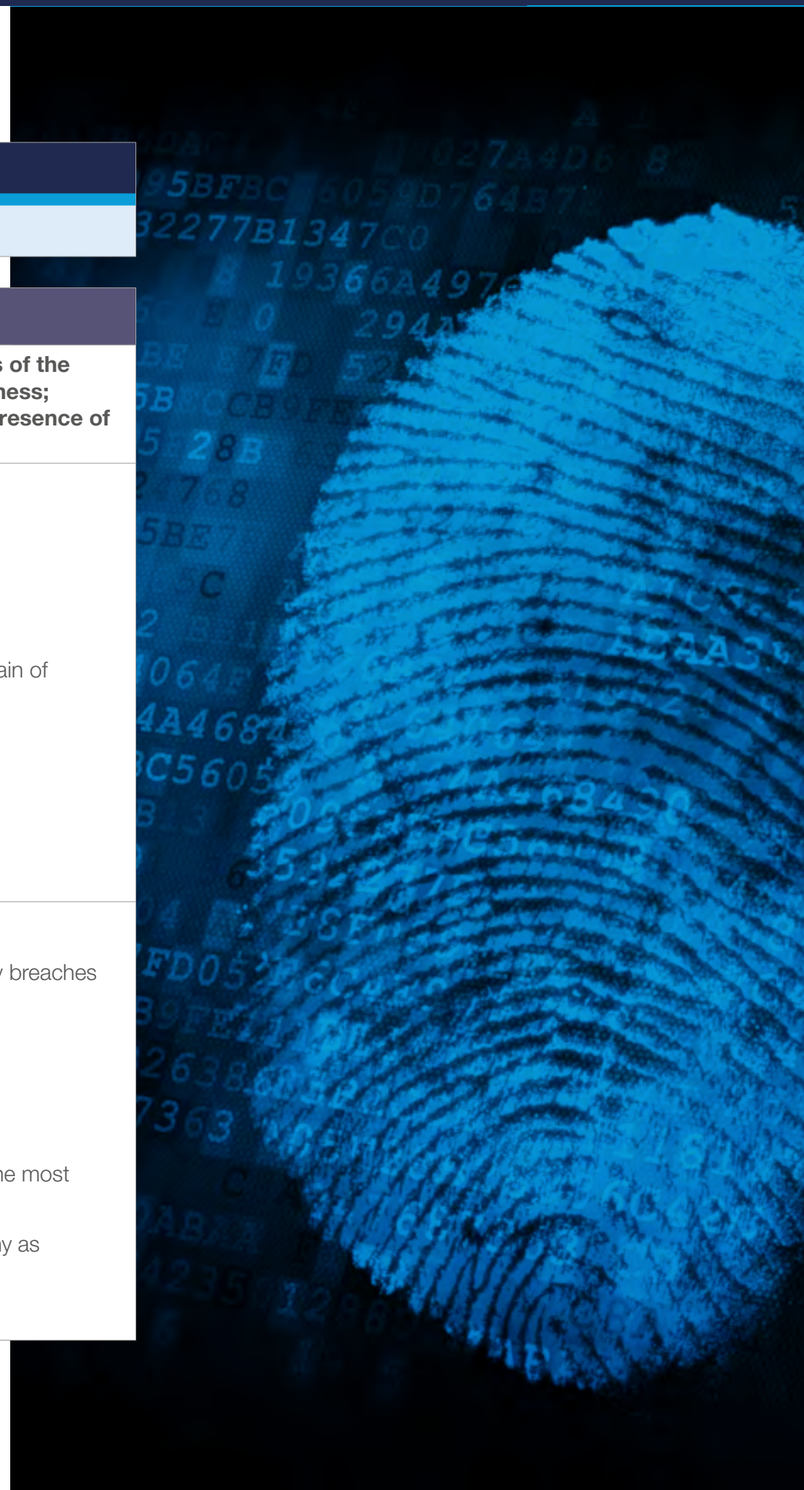
Skill	Skill source	Skill type
Forensics	**CIISEC Framework** F3 skill	Cyber Security

Skill definition

Forensics refers to the capture, analysis and reporting of evidence in accordance with legal guidelines, to minimise disruption to an organisation. The principles of the skill include securing the scene and capturing evidence in accordance with legal guidelines and in the most effective manner to minimise disruption to the business; maintaining evidential weight using specialist equipment as appropriate; analysing the evidence to identify breaches of policy, regulatory or law, including the presence of malware, and presenting evidence as appropriate; and acting as an expert witness as appropriate.

Awareness ★	Describes basic forensic principles and is capable of using agreed tools and techniques in support of an investigation Contributes to forensic activities with supervision Follows documented forensic principles and guidelines such as those related to acquisition and handling of forensic artefacts and maintaining the chain of custody Can identify suitable tools for use, and considers the impact on forensic integrity Considers the difference in intelligence and evidential requirements
Working ★★	Analyses digital evidence and investigates computer security incidents to derive information required to help resolve security incidents, and/or identify breaches of policy, regulation or law Understands legislative requirements and implications of actions within the organisation context Undertakes real-time analysis of ongoing incidents on live systems to identify relevant artefacts, understand the incident and facilitate resolution Able to identify suspicious software, including potential malware sources Secures the scene of an incident, with little requirement for supervision, acquiring and handling evidence in accordance with legal guidelines and in the most effective manner to minimise disruption to the business, ensuring that the chain of custody is maintained Presents conclusions in a manner suited to the context (written or oral), and is able to effectively defend conclusions, and provide evidence and testimony as required

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert. Skill levels are cumulative – for example, to hold a ‘practitioner’ level in this skill, you must meet the requirements of ‘working’ level too.



Forensics

Skill	Skill source	Skill type
Forensics	**CIISEC Framework** F3 skill	Cyber Security

Skill definition	
Forensics refers to the capture, analysis and reporting of evidence in accordance with legal guidelines, to minimise disruption to an organisation. The principles of the skill include securing the scene and capturing evidence in accordance with legal guidelines and in the most effective manner to minimise disruption to the business; maintaining evidential weight using specialist equipment as appropriate; analysing the evidence to identify breaches of policy, regulatory or law, including the presence of malware, and presenting evidence as appropriate; and acting as an expert witness as appropriate.	
Practitioner ★★★	Supervises others and manages teams in undertaking complex forensic investigations, and defines working procedures Analyses technically complex digital evidence and investigates complicated computer security incidents to derive information required to help resolve security incidents, and/or identify breaches of policy, regulation or law Undertakes real-time analysis of sophisticated ongoing incidents on live systems to identify relevant artefacts, understand the incident and facilitate resolution Secures the scene of an incident, without supervision, acquiring and handling evidence in accordance with legal guidelines and in the most effective manner to minimise disruption to the business, ensuring that the chain of custody is maintained Adapts techniques, modifies tools and creates scripts to address atypical situations. Addresses forensic requirements arising from Cloud and distributed environments, and emerging technologies Identifies indicators of compromise on an infrastructure, malicious software and any Tactics, Techniques and Procedures (TTPs) associated Collates artefacts from a wide range of sources to develop conclusions Presents conclusions in a manner suited to the context (written or oral), and effectively defends conclusions under scrutiny Provides clear explanations to senior stakeholders, detailed explanations to technical specialists and, if required, provides testimony and evidence as an expert witness in legal cases
Expert ★★★★	Sets direction within the organisation for all aspects of computer forensic activity. Defines policy and formulates the overarching digital forensics strategy, engaging with other relevant departments and stakeholders Leads forensic teams Contributes to the development of the field Analyses technically complex digital evidence and investigates highly complicated and novel computer security incidents to derive information required to help resolve security incidents, and/or identify breaches of policy, regulation or law Undertakes and oversees real-time analysis of very sophisticated ongoing incidents on live systems to identify relevant artefacts, understand the incident and facilitate resolution Secures or oversees the securing of the scene of an incident, acquiring and handling evidence in accordance with legal guidelines and in the most effective manner to minimise disruption to the business, ensuring that the chain of custody is maintained, compliant with relevant standards, policies, procedures and legislation Creates and adapts techniques and tools to address atypical and novel situations. Addresses forensic requirements arising from Cloud and distributed environments, and emerging technologies Reverses engineer malware to further investigative and intelligence opportunities Presents conclusions in a manner suited to the context (written or oral), and effectively defends conclusions under scrutiny Provides clear explanations to senior stakeholders (including the highest levels of management), detailed explanations to technical specialists and, if required, provides testimony and evidence as an expert witness in legal cases (including cases that break new ground and set precedent in terms of forensic evidence)

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert. Skill levels are cumulative – for example, to hold a ‘practitioner’ level in this skill, you must meet the requirements of ‘working’ level too.

Forensics

Skill	Skill source	Skill type
Forensics	**CIISEC Framework** F3 skill	Cyber Security

Indicative training

Indicative training	Format	Length	Provider type
Introduction to Digital Forensics	Classroom	3 days	External
FOR500: Windows Forensic Analysis	Classroom	6 days	External
FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting	Classroom	6 days	External
FOR518: Mac and iOS Forensic Analysis and Incident Response	Classroom	5 days	External
FOR526: Advanced Memory Forensics and Threat Detection	Classroom	6 days	External
FOR572: Advanced Network Forensics: Threat Hunting, Analysis and Incident Response	Classroom	6 days	External
FOR578: Cyber Threat Intelligence	Classroom	5 days	External
FOR585: Advanced Smartphone Forensics	Classroom	6 days	External
MGT512: Security Leadership Essentials for Managers	Classroom	5 days	External

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profression of the NCSC, CPNI or UKNACE.

Incident management, incident investigation and response

Skill	Skill source	Skill type
Incident management, incident investigation and response	**NCSC** (skill definition), **CIISEC Framework** F2 skill	Cyber Security

Skill definition	
Incident management, incident investigation and response refers to the set of processes, procedures and systems used to reduce the harm caused to victims of cyber incidents and deter future attacks. The principles of the skill include engagement with the overall organisation incident management process to ensure that information security incidents are handled appropriately, defining and implementing processes, procedures and configuring system policies for responding to and investigating information security incidents, establishing and maintaining a Computer Emergency Response Team (CERT) and systems to deal with information security incidents.	
Awareness ★	Describes the basic principles of incident management, incident investigation and response. Implements processes, procedures and systems for responding to and investigating incidents Follows documented principles and guidelines for incident management, incident investigation and response activities with supervision
Working ★★	Contributes to incident management, incident investigation and response policy and/or incident management processes, procedures and systems Follows documented principles and guidelines for incident management, incident investigation and response activities with limited direction/supervision
Practitioner ★★★	Defines incident management, incident investigation and response policy and/or incident management and investigation processes, procedures and systems Follows documented principles and guidelines for incident management, incident investigation and response activities Advises others on incident management, incident investigation and response processes
Expert ★★★★	Champions incident management, incident investigation and response policy and/or incident management and investigation processes, procedures and systems Shapes incident management, system response, incident investigation and response principles and guidelines for incident management activities Advises on corporate and systems response to an incident Promotes incident management, incident investigation and response best practice Monitors the effectiveness of reporting

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert. Skill levels are cumulative – for example, to hold a ‘practitioner’ level in this skill, you must meet the requirements of ‘working’ level too.

Incident management, incident investigation and response

Skill	Skill source	Skill type
Incident management, incident investigation and response	**NCSC** (skill definition), **CIISEC Framework** F2 skill	Cyber Security

Indicative training

Indicative training	Format	Length	Provider type
Cyber Incident Planning and Response	Classroom	1 day	External
Cyber Security for Information Asset Owners	Classroom	1 day	External
ICS515: ICS Active Defence and Incident Response	Classroom	5 days	External
Incident Response for IT Professionals	Classroom	6 days	External
MGT512: Security Leadership Essentials for Managers	Classroom	5 days	External
SEC503: Intrusion Detection In-Depth	Classroom	6 days	External

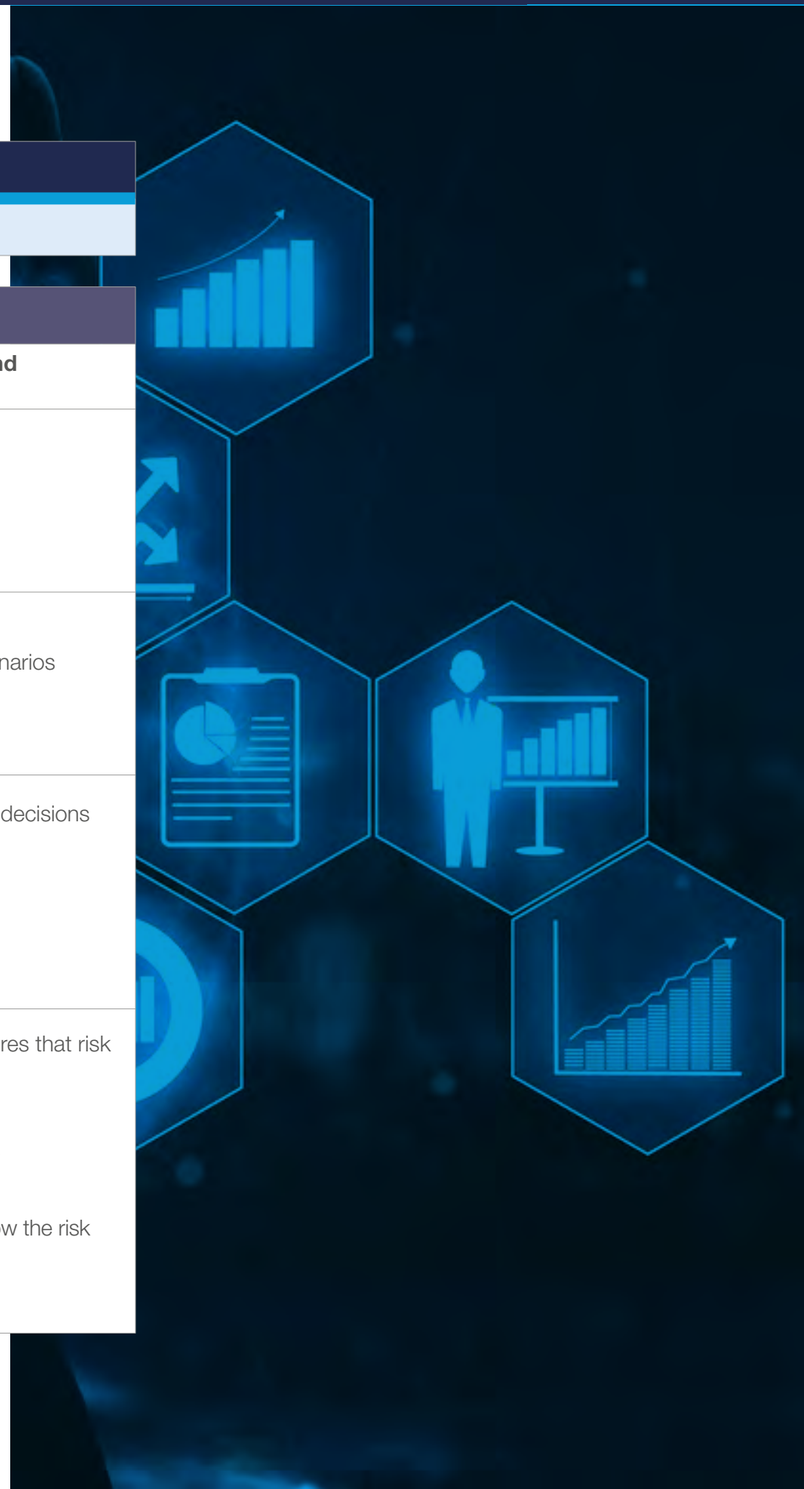
Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profression of the NCSC, CPNI or UKNACE.

Information risk assessment and risk management

Skill	Skill source	Skill type
Information risk assessment and risk management	NCSC Information Risk Assurance Skill 5.2	Cyber Security

Skill definition	
Information risk assessment and risk management identifies and evaluates security risks to information, systems, and processes owned by the organisation, and proactively provides appropriate advice, drawing on a wide variety of sources, to stakeholders across the organisation and at a variety of levels.	
Awareness ★	Demonstrates knowledge of risk assessment and risk management theory and approaches Understands how risk management supports business or organisational objectives Understands and can follow routine organisational governance processes for security and risk management
Working ★★	Supports security professionals in carrying out risk assessments and developing mitigation strategies for relatively common and well-understood scenarios Has an understanding of, and can apply, the fundamental principles of risk assessment, risk management processes and decision-making
Practitioner ★★★	Understands the organisation's business drivers and approach to managing risk to support delivery of balanced and cost-effective risk management decisions on situations with a relatively well-defined scope. Relates risk to corporate governance, organisational strategic direction and planning Delivers or reviews risk assessments using appropriate risk assessment methods for common scenarios such as enterprise IT systems Inspects and reports on the security characteristics of systems with straightforward scope Has a good understanding of how assessed risks are addressed as part of an approach to risk treatment
Expert ★★★★	Enables the organisation to deliver balanced and cost-effective risk management decisions on situations with complex scope or significant risk. Ensures that risk is embedded into corporate governance processes Integrates risk management processes into appropriate business activities such as system development, security architecture or procurement Develops approaches to effectively report risk (including through system life cycles) to management who are responsible for risk to a given system or capability. This includes the ability to interpret management risk direction to others (such as developers or other security professionals) Delivers comprehensive risk assessments for complicated or novel scenarios, using methodologies appropriate to the situation. Understands in detail how the risk assessment output dovetails into the risk management process Determines and understands the security characteristics of complicated or novel systems

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert. Skill levels are cumulative – for example, to hold a 'practitioner' level in this skill, you must meet the requirements of 'working' level too.



Information risk assessment and risk management

Skill	Skill source	Skill type
Information risk assessment and risk management	NCSC Information Risk Assurance Skill 5.2	Cyber Security

Indicative training

Indicative training	Format	Length	Provider type
BCS Certificate in Information Security Management Principles	Classroom	5 days	External
Certified Information Systems Security Professional	Certification, Classroom	5 days	External
Cyber Incident Planning and Response	Classroom	1 day	External
Cyber Security for Information Asset Owners	Classroom	1 day	External
Cyber Security Risk Assessment and Management	Classroom	4 days	External
Fundamentals of Information Assurance in Her Majesty's Government	Classroom	1 day	HM Government
Information Assurance Risk Management for HMG	Classroom	1 day	External
Introduction to Risk Management	eLearning	Self-paced	HM Government
MGT512: Security Leadership Essentials for Managers	Classroom	5 days	External
PMI Risk Management Professional	Certification	To be defined	External
Risk in the Boardroom	Classroom	1 day	External
Risky Business: Managing your Information Risk	eLearning	3 months	External

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profression of the NCSC, CPNI or UKNACE.

Intrusion detection and analysis

Skill	Skill source	Skill type
Intrusion detection and analysis	**CIISEC Framework** F1 skill	Cyber Security

Skill definition
Intrusion detection and analysis consists of network and system activities to identify potential intrusion or other anomalous behaviour. Processes, methods and procedures include information analysis, security analytics including outputs from intelligence analysis, predictive research, and root cause analysis, vulnerability report analysis, and the production of warning materials. Further principles of the skill include monitoring, collating and filtering external vulnerability reports for organisational relevance, ensuring that relevant vulnerabilities are rectified through formal change processes, and ensuring that disclosure processes are put in place to restrict the knowledge of new vulnerabilities until appropriate remediation or mitigation is available.

Awareness ★	Describes the basic principles of intrusion detection and analysis including the difference between intrusion prevention and intrusion detection Follows documented principles and guidelines for intrusion detection and analysis activities Implements intrusion detection and analysis processes and procedures
Working ★★	Understands and explains the basic principles of monitoring network and system activity to identify potential intrusion or other anomalous behaviour Uses information provided from various sources to identify, analyse, and report events that occur or might occur within the network. Uses a range of methods and procedures to identify, acquire, and preserve artefacts by means of controlled and documented analytical and investigative techniques Understands the business context of the activities Educates others on policies, procedures and guidelines relating to monitoring and analysing network and system activity
Practitioner ★★★	Understands and explains advanced principles of monitoring network and system activity to identify potential intrusion or other anomalous behaviour and applies the results in investigations Collects information from a variety of sources (e.g. data from cyber defence tools, system logs) and uses it to identify, analyse, and report events that occur or might occur within the network. Uses a range of advanced methods and procedures (including intelligence analysis, predictive research, root cause analysis, vulnerability report analysis) to identify, acquire, analyse and preserve artefacts by means of controlled and documented analytical and investigative techniques Supervises and manages teams undertaking intrusion detection and analysis Creates policies, procedures and guidelines based on intrusion detection and analysis standards Advises others on intrusion detection and analysis Tailors and refines systems and processes to meet the organisation's needs

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert. Skill levels are cumulative – for example, to hold a 'practitioner' level in this skill, you must meet the requirements of 'working' level too.

Intrusion detection and analysis

Skill	Skill source	Skill type
Intrusion detection and analysis	**CIISEC Framework** F1 skill	Cyber Security

Skill definition
Intrusion detection and analysis consists of network and system activities to identify potential intrusion or other anomalous behaviour. Processes, methods and procedures include information analysis, security analytics including outputs from intelligence analysis, predictive research, and root cause analysis, vulnerability report analysis, and the production of warning materials. Further principles of the skill include monitoring, collating and filtering external vulnerability reports for organisational relevance, ensuring that relevant vulnerabilities are rectified through formal change processes, and ensuring that disclosure processes are put in place to restrict the knowledge of new vulnerabilities until appropriate remediation or mitigation is available.

Expert	★★★★	Understands and explains advanced monitoring of network and system activity to identify potential intrusion or other anomalous behaviour and applies the results in complex investigations Collects or oversees collection of information from a variety of sources (e.g. data from cyber defence tools, system logs) and uses it to identify, analyse, and report events that occur or might occur within the network. Uses a range of advanced methods and procedures (including intelligence analysis, predictive research, root cause analysis, vulnerability report analysis), developing techniques and tools where necessary, to identify, acquire, analyse and preserve artefacts by means of specialist analytical and investigative techniques Leads and oversees intrusion detection and analysis function and activities for an organisation Shapes intrusion detection and analysis strategy, policy, procedures and guidelines within the organisation and influences developments in the field at a national level Advises and influences senior management on intrusion detection and analysis matters Defines, articulates and communicates required capabilities and tools

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert. Skill levels are cumulative – for example, to hold a ‘practitioner’ level in this skill, you must meet the requirements of ‘working’ level too.

Intrusion detection and analysis

Skill	Skill source	Skill type
Intrusion detection and analysis	**CIISEC Framework** F1 skill	Cyber Security

Indicative training

Indicative training	Format	Length	Provider type
Certified Ethical Hacker	Certification, eLearning	Self-paced	External
CompTIA Advanced Security	Certification, Classroom	5 days	External
CompTIA Cybersecurity Analyst+	Certification, Classroom	5 days	External
CSOCA – Certified Security Operations Centre Analyst	Certification, Classroom	5 days	External
FOR500: Windows Forensic Analysis	Classroom	6 days	External
FOR518: Mac and iOS Forensic Analysis and Incident Response	Classroom	5 days	External
FOR572: Advanced Network Forensics: Threat Hunting, Analysis and Incident Response	Classroom	6 days	External
FOR578: Cyber Threat Intelligence	Classroom	5 days	External
MGT512: Security Leadership Essentials for Managers	Classroom	5 days	External
SEC503: Intrusion Detection In-Depth	Classroom	6 days	External
Security Operations Centre Analyst Foundation	Classroom	4 days	External

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profression of the NCSC, CPNI or UKNACE.

Investigative interviewing

Skill	Skill source	Skill type
Investigative interviewing	College of Policing Investigation	Personnel Security

Skill definition	
Investigative interviewing refers to a process of gathering, retaining and analysing information for investigative purposes in a manner that maintains the integrity of vetting information.	
Awareness ★	Follows documented investigative interviewing procedures and guidelines and applies them to practice Adapts working practices to meet changes in relevant policies, procedures and guidelines Supports the investigative interviewing process with supervision
Working ★★	Inputs into the development of investigative interviewing policies, procedures and guidelines Assures working practices are meeting relevant policies, procedures and guidelines Supports the investigative interviewing process without supervision Educates others on relevant policies, procedures and guidelines
Practitioner ★★★	Translates investigative interviewing policies, procedures and guidelines into practice Responds to challenges to relevant policies, procedures and guidelines and implements continuous improvements Leads and manages the investigative interviewing process Explains the need for and implications of relevant policies, procedures and guidelines outside the security function
Expert ★★★★	Shapes investigative interviewing policies, procedures and guidelines within the organisation and at a national level Implements business change as a result of relevant policies, procedures and guidelines Directs the investigative interviewing process Champions the need for and the business benefits of relevant policies, procedures and guidelines

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert. Skill levels are cumulative – for example, to hold a ‘practitioner’ level in this skill, you must meet the requirements of ‘working’ level too.

Investigative interviewing

Skill	Skill source	Skill type
Investigative interviewing	College of Policing Investigation	Personnel Security

Indicative training

Indicative training	Format	Length	Provider type
Conducting Investigations (via Civil Service Learning)	Classroom	1 day	External

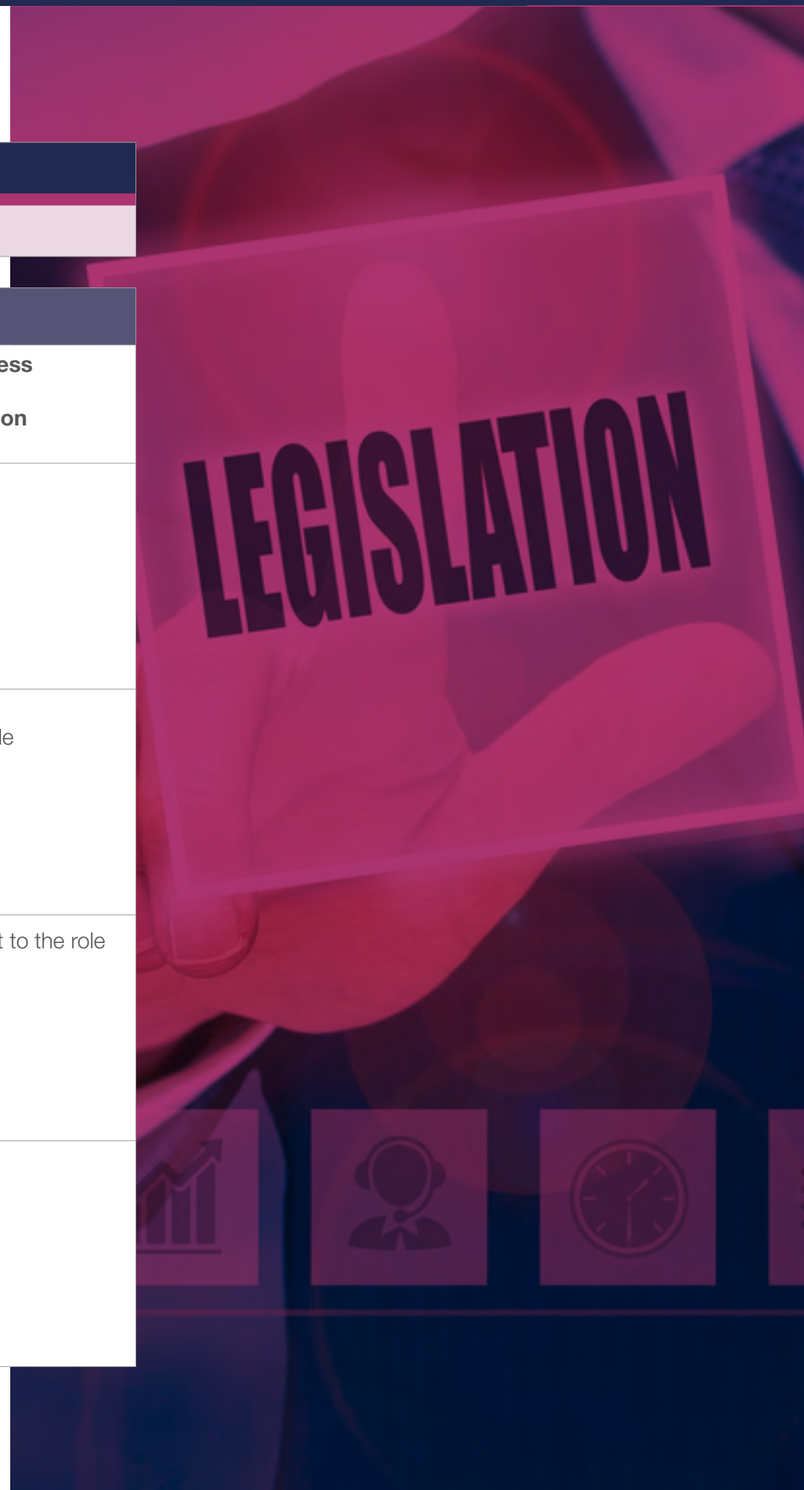
Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profression of the NCSC, CPNI or UKNACE.

Legal and regulatory environment and compliance

Skill	Skill source	Skill type
Legal and regulatory environment and compliance	**CIISEC Framework** A6 skill	Cross-specialism

Skill definition	
Legal and regulatory environment and compliance refers to an organisation's adherence to laws, regulations, guidelines and specifications relevant to its business processes. It consists of a blend of compliance requirements and assurance capabilities. Principles of the skill include understanding the legal and regulatory environment within which the business operates, ensuring that information security governance arrangements are appropriate, and ensuring that the organisation complies with legal and regulatory requirements.	
Awareness ★	Describes the major legislative regulatory instruments relevant to security legislation and regulation relevant to the role Maintains understanding of regulations that will impact the role Follows documented procedures for compliance or regulations
Working ★★	Explains the principal requirements of major legislation and regulations relevant to security, and the legal and regulatory instruments relevant to the role Reviews and implements alterations to operating procedures in response to changes in regulations Educates/provides guidance on the implementation of regulations Reports residual non-compliance to management in accordance with organisation procedures
Practitioner ★★★	Advises others on the principal requirements of major legislation and regulations relevant to security, and the legal and regulatory instruments relevant to the role Provides oversight of the range of regulations that impact the security function and the interactions between them Designs and leads implementation of business change, where required by regulation Leads the implementation of regulations within the security function Reports residual non-compliance to senior management in accordance with organisational procedures
Expert ★★★★	Leads the application of major legislation and regulations relevant to security, to ensure security is a business enabler Champions opportunities that regulation and compliance can provide to an organisation at senior manager or board level Promotes regulation and compliance within the security function Advises on the development of new legislation and regulation Lobbies external authorities, e.g. for niche regulation

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert. Skill levels are cumulative – for example, to hold a 'practitioner' level in this skill, you must meet the requirements of 'working' level too.



Legal and regulatory environment and compliance

Skill	Skill source	Skill type
Legal and regulatory environment and compliance	**CIISEC Framework** A6 skill	Cross-specialism

Indicative training

Indicative training	Format	Length	Provider type
Assessing GDPR As Part of the IASME Standard	Classroom	2 days	External
Certified ISO27001 Practitioner	Classroom	5 days	External
Fundamentals of Information Assurance in Her Majesty's Government	Classroom	1 day	HM Government
Information and Cyber Law/Data Protection Legislation (including GDPR)	Classroom	0.5 days	External
Information Assurance Risk Management for HMG	Classroom	1 day	External
NIST Security Framework Foundation	Classroom	2 days	External
SEC566: Implementing and Auditing the Critical Security Controls – In-Depth	Classroom	5 days	External

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profression of the NCSC, CPNI or UKNACE.

Penetration testing

Skill	Skill source	Skill type
Penetration testing	**CIISEC Framework** D4 skill	Cyber Security

Skill definition

Penetration testing is a method for gaining assurance in the security of an IT system by attempting to breach some or all of that system's security, using the tools and techniques that an adversary might employ. Principles of the skill include contributing to the scoping and conduct of vulnerability assessments; knowing the tools and techniques needed to enumerate an environment and assess asset configuration; identifying and testing for public domain vulnerabilities, assessing the potential for exploitation, and conducting exploits where appropriate; reporting potential issues and mitigation options; contributing to the review and interpretation of reports; and co-ordinating and managing remediation action plan responses. This skill has broad applicability across many roles.

Awareness ★	Understands and can explain the difference between vulnerability assessment and penetration testing and their purpose, and recognises the value of testing in supporting information security and configuration compliance Understands the basic principles, processes and components of penetration testing and can describe how these are applied in practice. Appreciates the risks of testing and the governance associated in executing such tests Understands the difference between red, blue and purple team simulated attack exercises and can explain the objectives and goals for each Has studied penetration exercises that illustrate scenarios based on threat intelligence and is able to list common types of vulnerabilities for infrastructure and web application targets Has training in penetration testing and has experience of using a limited number of testing tools 'out of the box' with basic functionality May have successfully completed simulated exercises in penetration testing within a training or academic environment or participated in syndicated exercises, undertaking practical exercises, or passing a test or examination (although there are no mandatory qualifications)
Working ★★	Explains the principles of penetration testing, the main components of an infrastructure penetration test and the high-level processes involved, to practitioners and non-practitioners alike Provides pragmatic input to assist in the development of penetration testing policies, procedures and guidelines and understands their business context Helps ensure compliance of working practices by educating colleagues in basic penetration testing policies, procedures and guidelines Performs basic tests or attack exercises by following documented principles and guidelines for penetration testing activities and interprets results, with little or no supervision Uses preconfigured commercial and bespoke tools to conduct vulnerability assessments and basic penetration tests without supervision and complex infrastructure penetration testing under supervision Understands the potential risks of security testing in different operational environments and takes them into account while developing plans Makes contributions to assessment reports that are factual and literal, rather than interpretive Has solid rather than wide platform knowledge being strong on a single platform (e.g. Windows, Mac) Has achieved recognised qualifications in appropriate and relevant subjects, including Offensive Security Certified Professional, CHECK Team Member or equivalent

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert. Skill levels are cumulative – for example, to hold a 'practitioner' level in this skill, you must meet the requirements of 'working' level too.

Penetration testing

Skill	Skill source	Skill type
Penetration testing	**CIISEC Framework** D4 skill	Cyber Security

Skill definition

Penetration testing is a method for gaining assurance in the security of an IT system by attempting to breach some or all of that system's security, using the tools and techniques that an adversary might employ. Principles of the skill include contributing to the scoping and conduct of vulnerability assessments; knowing the tools and techniques needed to enumerate an environment and assess asset configuration; identifying and testing for public domain vulnerabilities, assessing the potential for exploitation, and conducting exploits where appropriate; reporting potential issues and mitigation options; contributing to the review and interpretation of reports; and co-ordinating and managing remediation action plan responses. This skill has broad applicability across many roles.

Practitioner ★★★	Leads teams undertaking complex penetration tests Follows documented principles and guidelines for high-complexity penetration testing activities Designs and implements test programmes for mid-complexity systems, products, applications or processes, selecting suitable techniques, tools and test strategies without supervision Identifies vulnerabilities, and determines whether they are exploitable, adapting testing approach based on findings Detects and investigates result aberrations, or absences of expected results Creates assessment reports, confirming technology compliance with standards and policies and vulnerabilities, and provides suggested remediation actions Advises others on penetration testing processes, the implications of testing, and sharing penetration testing best practice Has a broader platform knowledge and conducts assessments from a multi-platform perspective Has achieved recognised qualifications in appropriate and relevant subjects, to a high-functioning level, including CHECK Team Leader, CREST Certified Simulated Attack Specialist or equivalent
Expert ★★★★	Takes a multi-customer approach to establishing penetration testing policies, procedures and guidelines, taking into account organisational and national level perspectives Has responsibility for penetration testing services and drives organisational and business change to better comply with policies, procedures and guidelines Ensures effective delivery of penetration testing assessments for organisational benefit Leads organisational teams in various stages of test design, execution, and assessment, for multiple customers, potentially across multiple organisations, and that comply with policies, procedures and guidelines Improves organisational penetration testing processes, achieving high standards of excellence Champions the organisational recognition of value of penetration testing services, and the benefits of addressing the results Authoritatively influences the organisational management regarding penetration testing concepts and activities Builds on, and advances, practitioner level skills for self and colleagues Communicates complex issues at the appropriate level for the audience Has achieved appropriate level of qualifications, including CREST Certified Simulated Attack Manager or equivalent

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert. Skill levels are cumulative – for example, to hold a 'practitioner' level in this skill, you must meet the requirements of 'working' level too.

Penetration testing

Skill	Skill source	Skill type
Penetration testing	**CIISEC Framework** D4 skill	Cyber Security

Indicative training

Indicative training	Format	Length	Provider type
Advanced Infrastructure Hacking	Classroom	5 days	External
Certified Ethical Hacker	Certification, eLearning	Self-paced	External
CompTIA Advanced Security	Certification, Classroom	5 days	External
CompTIA PenTest+	Classroom	5 days	External
FOR578: Cyber Threat Intelligence	Classroom	5 days	External
Hands-on Penetration Testing and Ethical Hacking	eLearning	To be defined	External
Hands-on Web Application Penetration Testing Training Course	eLearning	To be defined	External
ICS515: ICS Active Defense and Incident Response	Classroom	5 days	External
MGT512: Security Leadership Essentials for Managers	Classroom	5 days	External
Offensive Security Certified Professional + Penetration testing with Kali Linux	Certification, eLearning	Self-paced	External
Penetration Testing – Tools and Techniques	Classroom, eLearning	5 days	External
SEC460: Enterprise Threat and Vulnerability Assessment	Classroom	6 days	External

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profression of the NCSC, CPNI or UKNACE.

Protective security

Skill	Skill source	Skill type
Protective security	CPNI	Cross-specialism

Skill definition	
Protective security encompasses the combination and multi-layering of appropriate and proportionate Physical, Personnel and Cyber Security measures to help identify and respond to any attack. Security requirements will change accordingly with the locally identified threats and vulnerabilities.	
Awareness ★	Maintains an up-to-date understanding of fundamentals of all areas of security (especially in the context of government), and appreciates the importance of making use of a combination and multi-layering of appropriate and proportionate Physical, Personnel and Cyber Security measures to protect assets Identifies aspects from across the breadth of the security field Promotes protective security, providing advice to others
Working ★★	Applies concepts of protective security within the context of the other specialisms/enablers, and keeps knowledge up to date Champions protective security within the wider security function, providing advice to others
Practitioner ★★★	Develops and applies new concepts in protective security, involving the other specialisms, including the Corporate Enablers Develops individuals and contributes to the development of protective security practices Promotes protective security as a business enabler throughout the organisation Engages with the UK security community
Expert ★★★★	Leads innovation in protective security, taking into account other specialisms/enablers and business drivers Promotes the development of individuals against the career framework Promotes the use of protective security as a business enabler at board or senior management level Is an active member of the UK security community

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert. Skill levels are cumulative – for example, to hold a ‘practitioner’ level in this skill, you must meet the requirements of ‘working’ level too.

Protective security

Skill	Skill source	Skill type
Protective security	CPNI	Cross-specialism

Indicative training

Indicative training	Format	Length	Provider type
Certified Information Security Management Principles	Certification, Classroom	5 days	External
Certified Information Systems Security Professional	Certification, Classroom	5 days	External
Certified Protection Professional	Certification, Classroom	3 days	External
Defence Strategic Cyber Awareness	Classroom	1 day	HM Government
Fundamentals of Information Assurance in Her Majesty's Government	Classroom	1 day	HM Government
Information Assurance Risk Management for HMG	Classroom	1 day	External
Introduction to Security	eLearning	Self-paced	HM Government
MGT512: Security Leadership Essentials for Managers	Classroom	5 days	External
MGT514: Security Strategic Planning, Policy and Leadership	Classroom	5 days	External
Security Management Course Level 3	eLearning	Self-paced	External

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profression of the NCSC, CPNI or UKNACE.

Risk understanding and mitigation

Skill	Skill source	Skill type
Risk understanding and mitigation	**CIISEC Framework** B3 skill	Cross-specialism

Skill definition
Risk understanding and mitigation identifies and evaluates security risks to information, systems and processes owned by the organisation, and proactively provides appropriate advice, drawing on a wide variety of sources, to stakeholders across the organisation and at a variety of levels. Principles of the skill include developing cyber and information security risk management strategies and controls, taking into account business needs and risk assessments, and balancing technical, physical, procedural and personnel controls.

Awareness ★	Describes the basic principles of risk understanding and mitigation Supports security professionals in carrying out risk assessments and developing mitigation strategies Follows documented principles and guidelines for risk understanding and mitigation
Working ★★	Develops basic cost-effective risk management plans Supports risk assessment and mitigation plan development Follows documented principles and guidelines for risk understanding and mitigation Relates risk to corporate governance, organisational strategic direction and planning
Practitioner ★★★	Develops complex and innovative risk management plans, enabling the organisation to deliver balanced and cost–effective risk management decisions based on advanced threat principles and concepts Leads risk assessment and mitigation plan development Ensures that risk is embedded into corporate governance processes and integrates risk management processes into appropriate business activities
Expert ★★★★	Leads risk management within an organisation, enabling senior leadership to make effective risk-based business decisions Leads on the provision of top-end risk understanding and mitigation advice Integrates risk understanding and mitigation processes into appropriate business activities Develops approaches to effectively report risks and delivers comprehensive risk assessments

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert. Skill levels are cumulative – for example, to hold a ‘practitioner’ level in this skill, you must meet the requirements of ‘working’ level too.

Risk understanding and mitigation

Skill	Skill source	Skill type
Risk understanding and mitigation	**CIISEC Framework** B3 skill	Cross-specialism

Indicative training

Indicative training	Format	Length	Provider type
Enterprise Risk Management for leaders, influencers and decision makers	Classroom	3 days	External
Fundamentals of Information Assurance in Her Majesty's Government	Classroom	1 day	HM Government
Information Assurance Risk Management for HMG	Classroom	1 day	External
Introduction to Risk Management	eLearning	Self-paced	HM Government
PMI Risk Management Professional	Certification	To be defined	External
Risk in the Boardroom	Classroom	5 days	External
Risky Business: Managing your Information Risk	eLearning	3 months	External

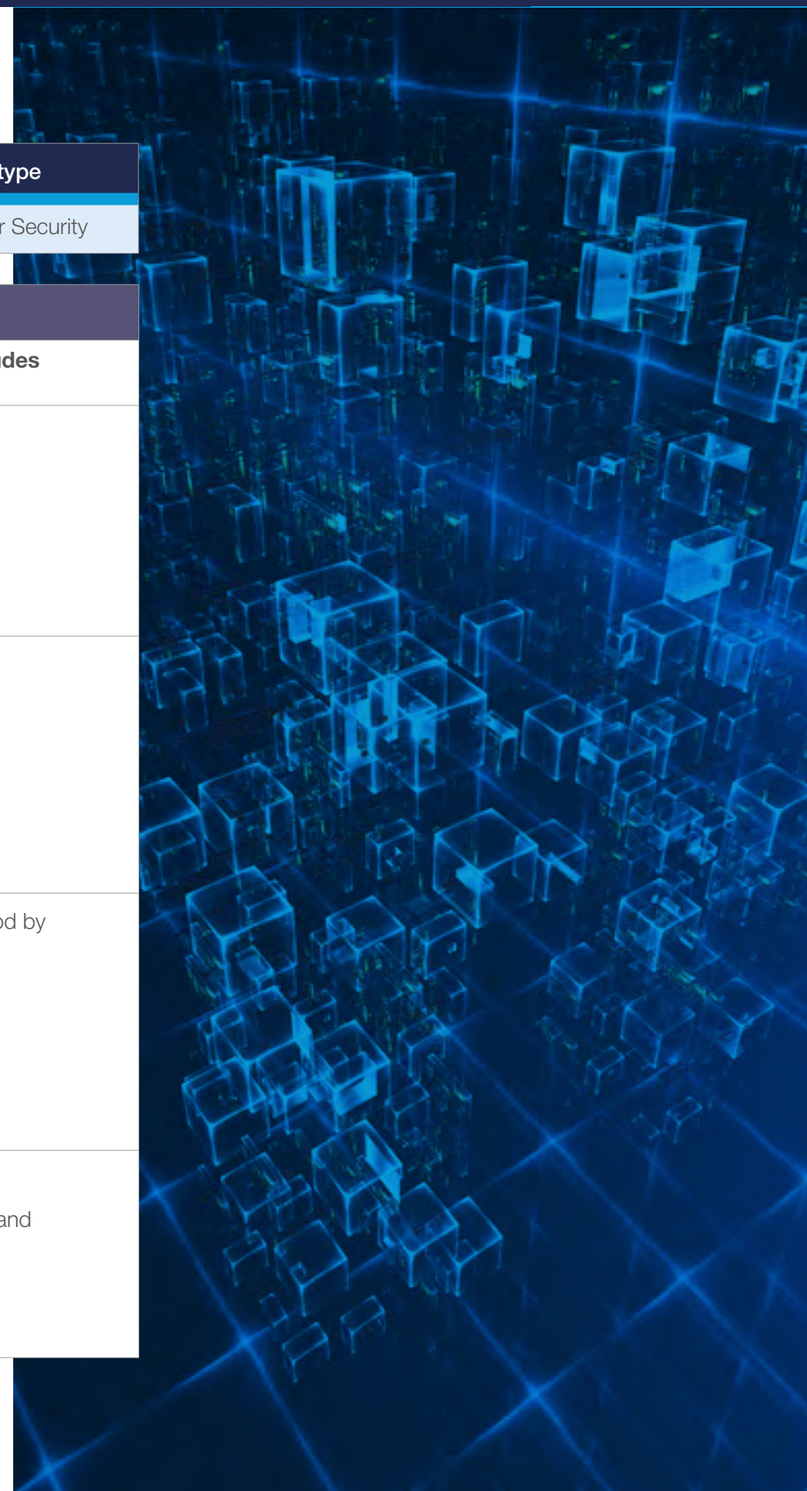
Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profression of the NCSC, CPNI or UKNACE.

Secure design

Skill	Skill source	Skill type
Secure design	Digital, Data and Technology	Cyber Security

Skill definition	
Secure design is the ability to apply Cyber Security functions or designs to reduce high-level to low-level service exploitation opportunities. Secure design includes designing countermeasures and mitigations against potential exploitations of service weaknesses for applications, systems, hardware and/or services.	
Awareness ★	Understands a number of secure design principles, frameworks and standards for designing a digital service Supports the definition of secure design requirements based on business drivers and attributes Is aware of several methods of design such as agile delivery Is familiar with hardware and software languages that can be used on a digital service Is aware of security audit frameworks for digital services
Working ★★	Produces high-level design and develops processes for maintaining the security of a service through its full life cycle Understands and can define secure design principles, frameworks and standards for designing a digital service Explains processes that maintain the required level of security of a component, product, or system through its life cycle Applies secure code/hardware documentation Confers with stakeholders such as engineers and programmers to design high-level applications/services Scopes security audits in accordance with a digital service framework
Practitioner ★★★	Leads and creates documentation of a digital service and subsequent revisions, inserting comments in the coded instructions so it can be understood by others, including engineers Leads the preparation of detailed workflow and diagrams that describe input, output and logical operation of a digital service Produces low-level design and develops processes for maintaining the security of a service through its full life cycle Leads and translates security requirements into application design elements including documenting specific security criteria Creates audit points in the software development life cycle process by designing audit compliance
Expert ★★★★	Champions secure design principles, frameworks and standards for a digital service or programme Sponsors and directs design of detailed low-level workflows, diagrams that describe input, output and logical operation of a digital service. Designs and develops the processes of a digital service through its full life cycle Leads and translates security requirements into application design elements including documenting specific security criteria Designs advanced audit points into digital services

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert. Skill levels are cumulative – for example, to hold a ‘practitioner’ level in this skill, you must meet the requirements of ‘working’ level too.



Secure design

Skill	Skill source	Skill type
Secure design	Digital, Data and Technology	Cyber Security

Indicative training

Indicative training	Format	Length	Provider type
No indicative training identified	To be defined	To be defined	To be defined

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profression of the NCSC, CPNI or UKNACE.

Secure development

Skill	Skill source	Skill type
Secure development	Digital, Data and Technology	Cyber Security

Skill definition	
Secure development allows for the implementation of secure systems, products and components, using appropriate methodologies and frameworks. It includes the development, creation, maintenance and coding of new (or modification of existing) computer applications, software or bespoke utility programs for business outcomes.	
Awareness ★	Understands basic application/hardware/service development life cycle Familiar with application, fraud, error and business logic exploits Recognises basic to advanced languages to create a digital service Comprehends the common Technical Security controls
Working ★★	Develops services by writing programming and scripting language Takes a lead in conducting software debugging and guides developers/engineers to resolve issues Creates and delivers automated assurance against Technical Security guidance and configurations Implements business logic and technical solutions to design out fraud and error Builds and implements security audit points in digital services Drives secure coding practices and champions them in the engineering community
Practitioner ★★★	Develops services by writing programming and scripting language Leads software debugging and guides developers/engineers to resolve issues Creates and delivers automated assurance against Technical Security guidance and configurations Implements business logic and technical solutions to design out fraud and error Builds and implements security audit points in digital services Drives secure coding practices and champions them, including in the engineering community
Expert ★★★★	Leads the implementation of secure development principles, software and hardware debugging. Guides developers/engineers Develops services by writing advanced programming and scripting language Creates and delivers automated assurance against Technical Security guidance and configurations Implements security remediations and performs root cause analysis Leads the development of advanced security audit points in digital services Drives secure coding practices and champions them, including in the engineering community

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert. Skill levels are cumulative – for example, to hold a ‘practitioner’ level in this skill, you must meet the requirements of ‘working’ level too.

Secure development

Skill	Skill source	Skill type
Secure development	Digital, Data and Technology	Cyber Security

Indicative training

Indicative training	Format	Length	Provider type
No indicative training identified	To be defined	To be defined	To be defined

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profression of the NCSC, CPNI or UKNACE.

Secure operations management

Skill	Skill source	Skill type
Secure operations management	**CIISEC Framework** E1 skill	Cross-specialism

Skill definition	
Secure operations management refers to the ongoing operation, management and continuous improvement of security capabilities throughout an organisation through policies, procedures and guidelines. Principles of the skill include creating and maintaining system understanding, including hardware and software inventories; establishing processes for maintaining the security of information throughout its existence, including establishing and maintaining security operating procedures in accordance with security policies, standards and procedures; assessing and responding to new technical, physical, personnel or procedural vulnerabilities; engaging with suppliers, penetration testers and the change management process to ensure that vulnerabilities are mediated; and managing the implementation of information security programmes, co-ordinating security activities across the organisation.	
Awareness ★	Describes the basic principles of secure operations management Follows documented principles and guidelines for secure operations management activities Implements secure operations management processes and procedures
Working ★★	Explains the main processes for secure operations management Understands the business context in which policies, procedures and guidelines sit Implements secure operations management processes and procedures
Practitioner ★★★	Applies standards into secure operations management processes Responds to challenges to policies, procedures and guidelines and implements continuous improvements Identifies and implements new management controls to reflect changes in factors such as threat levels and legislation
Expert ★★★★	Shapes policies, procedures and guidelines within the organisation and at a national level Implements business change as a result of policies, procedures and guidelines Champions the need for and the business benefits of management controls

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert. Skill levels are cumulative – for example, to hold a ‘practitioner’ level in this skill, you must meet the requirements of ‘working’ level too.

Secure operations management

Skill	Skill source	Skill type
Secure operations management	**CIISEC Framework** E1 skill	Cross-specialism

Indicative training

Indicative training	Format	Length	Provider type
ICS515: ICS Active Defence and Incident Response	Classroom	5 days	External
MGT525: IT Project Management, Effective Communication, and PMP Exam Prep	Classroom	6 days	External
SEC402: Cybersecurity Writing: Hack the Reader	eLearning	2 days	External

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profression of the NCSC, CPNI or UKNACE.

Secure supply chain management

Skill	Skill source	Skill type
Secure supply chain management	CPNI	Cross-specialism

Skill definition	
Secure supply chain management refers to the activities, processes and procedures related to protecting the operations across a logistics network regarding the moving of a product or service from supplier to customer and from concept to disposal. Secure supply chain management can be divided into 4 sections: (1) understand the risks; (2) establish control; (3) check your arrangements; and (4) continuous improvement.	
Awareness ★	Describes the basic principles of secure supply chain management Follows documented principles and guidelines for secure supply chain management activities Implements secure supply chain management processes and procedures within their areas of responsibility
Working ★★	Explains and can develop processes for secure supply chain management Understands the business context in which policies, procedures and guidelines sit, tailoring processes to suit business needs Implements secure supply chain management processes and procedures
Practitioner ★★★	Develops secure supply chain management processes to meet standards or changes to standards Responds to challenges to policies, procedures and guidelines and implements continuous improvements Identifies and implements new secure supply chain management controls to reflect changes in factors such as threat levels and legislation
Expert ★★★★	Shapes policies, procedures and guidelines within the organisation and at a national level Implements business change as a result of policies, procedures and guidelines Champions the need for and the business benefits of secure supply chain management controls

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert. Skill levels are cumulative – for example, to hold a ‘practitioner’ level in this skill, you must meet the requirements of ‘working’ level too.

Secure supply chain management

Skill	Skill source	Skill type
Secure supply chain management	CPNI	Cross-specialism

Indicative training

Indicative training	Format	Length	Provider type
ICS515: ICS Active Defence and Incident Response	Classroom	5 days	External
Project Management Professional	Certification	To be defined	External

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profression of the NCSC, CPNI or UKNACE.

Security architecture

Skill	Skill source	Skill type
Security architecture	NCSC Information Assurance skill 6.3	Cyber Security

Skill definition	
Security architecture relates to the secure design of computer systems. It combines technical architecture and risk management, along with knowledge of how systems can be compromised to help design systems that (among other things) are sufficiently hard to compromise or disrupt while being sufficiently easy to monitor and maintain.	
Awareness ★	Demonstrates knowledge of internal and external sources of published security architecture guidance, including secure design principles and patterns Demonstrates broad-ranging Technical Security knowledge necessary to understand system architectures, including common server roles, cryptography, key management, security technologies, virtual private networks (VPNs), load balancers, Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS)
Working ★★	Supports the design and/or review of common system architecture problems (e.g. typical website architectures or remote access solutions), using knowledge of common vulnerabilities, threats and methods of attack to identify recommended security controls, working under supervision Has broad-ranging Technical Security knowledge necessary to understand system architectures that include common technologies (e.g. Windows and Linux servers, end user compute platforms, databases, common server roles, cryptography, security technologies, load balancers, cloud services) Understands the application of security architecture in one or more domains – digital services, enterprise IT, operational technologies etc., as well as the other relevant inputs to architectural design in those domains (regulatory, government policy, standards etc.)
Practitioner ★★★	Has experience of reviewing system architectures to: • identify single points of vulnerability and common architectural flaws • identify security issues relating to configuration of components in an architecture • validate and explain how common attack methods are mitigated by the design identify areas where detailed technical analysis will be required to understand important nuances that could have significant security implications Articulates security issues identified, proposes and prioritises appropriate mitigation options, taking into consideration other potential constraints (functional impact, cost etc.) Contributes to the design of system architectures that solve common business problems, including specifying required security controls Understands the context and has required domain knowledge to tailor advice to the specific need of the customer
Expert ★★★★	Designs and reviews system architectures for a broad range of complex or uncommon requirements to identify security weaknesses and recommend mitigations Designs (or significantly influences) the technical design of a system to enforce security properties that have been derived from first principles to meet a complex or uncommon set of requirements Follows a methodical and repeatable approach to reviewing the security of a system architecture, and can describe that approach Advises on security architecture implications of technological trends when applied to existing systems, such as migration to the cloud. Can explain how those technologies change the security approach required Contributes to new and innovative security architecture guidance for others to re-use May have one or more technology specialisms where they are regarded as an expert in how their specialism supports security architecture design (e.g. telecoms, power, microservice architectures, identity)

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert. Skill levels are cumulative – for example, to hold a ‘practitioner’ level in this skill, you must meet the requirements of ‘working’ level too.

Security architecture

Skill	Skill source	Skill type
Security architecture	NCSC Information Assurance skill 6.3	Cyber Security

Indicative training

Indicative training	Format	Length	Provider type
CompTIA Advanced Security	Certification, Classroom	5 days	External
Cyber Security Development Programme	Classroom, Onsite	4 years	HM Government
Cyber Security for Information Asset Owners	Classroom	1 day	External
MGT512: Security Leadership Essentials for Managers	Classroom	5 days	External
SEC511: Continuous Monitoring and Security Operations	Classroom	6 days	External

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profression of the NCSC, CPNI or UKNACE.

Threat intelligence and threat assessment

Skill	Skill source	Skill type
Threat intelligence and threat assessment	**CIISEC Framework** B1 skill	Cyber Security

Skill definition
Threat intelligence and threat assessment encompasses evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging concern or risk that has been aggregated, transformed, analysed, interpreted or enriched to provide the necessary context for decision-making processes. Principles of the skill include assessing and validating information from several sources on current and potential cyber and information security threats to the business, analysing trends and highlighting information security issues relevant to the organisation, including security analytics for big data; processing, collating and exploiting data, taking into account relevance and reliability to develop and maintain 'situational awareness'; predicting and prioritising threats to an organisation and their methods of attack; analysing the significance and implication of processed intelligence to identify significant trends, potential threat agents and their capabilities, predicting and prioritising threats to an organisation and their methods of attack; using human factor analysis in the assessment of threats; using threat intelligence to develop attack trees; and preparing and disseminating intelligence reports, providing threat indicators and warnings.

Awareness ★	Understands and utilises basic threat principles and concepts
Working ★★	Understands and can explain threat intelligence and threat assessment principles and concepts Uses prescribed tools and techniques to acquire, validate and analyse threat information from multiple sources Under direction enriches threat information by providing context, assessing possible implications and summarising the behaviour, capabilities and activities of threat actors Uses approved techniques to model routine threats, under supervision, to identify common enterprise attack vector, identify critical organisational functions, and protect organisational assets and goals Applies knowledge to prioritise remediation of identified vulnerabilities for a single asset or system
Practitioner ★★★	Has an advanced understanding of threat intelligence and threat assessment principles and concepts, and leads threat intelligence and assessment activities Identifies sources of threat information and utilises a variety of techniques, without supervision, to acquire, validate and analyse threat information, enterprise attack vectors, and critical organisational functions from multiple sources. Synthesises and places intelligence in context Applies expertise and insight to enrich threat information, including understanding the behaviour, capabilities and activities of threat actors and assessing possible implications, prioritising remediation of identified vulnerabilities for multiple systems Disseminates enriched threat intelligence Applies threat intelligence to model threats and protects organisational assets and goals, including informing the selection of security controls, developing indicators of compromise, detecting illicit behaviour (including evidence of fraud and crime), providing context for undertaking investigations and responding to events Directs others in undertaking threat intelligence activities

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert. Skill levels are cumulative – for example, to hold a 'practitioner' level in this skill, you must meet the requirements of 'working' level too.

Threat intelligence and threat assessment

Skill	Skill source	Skill type
Threat intelligence and threat assessment	**CIISEC Framework** B1 skill	Cyber Security

Skill definition
Threat intelligence and threat assessment encompasses evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging concern or risk that has been aggregated, transformed, analysed, interpreted or enriched to provide the necessary context for decision-making processes. Principles of the skill include assessing and validating information from several sources on current and potential cyber and information security threats to the business, analysing trends and highlighting information security issues relevant to the organisation, including security analytics for big data; processing, collating and exploiting data, taking into account relevance and reliability to develop and maintain 'situational awareness'; predicting and prioritising threats to an organisation and their methods of attack; analysing the significance and implication of processed intelligence to identify significant trends, potential threat agents and their capabilities, predicting and prioritising threats to an organisation and their methods of attack; using human factor analysis in the assessment of threats; using threat intelligence to develop attack trees; and preparing and disseminating intelligence reports, providing threat indicators and warnings.

Expert	★★★★	Demonstrates a highly advanced understanding of threat principles and concepts. Identifies sources of threat information and selections and, where required, develops techniques to acquire, validate and analyse threat information from multiple sources Synthesises and places complex intelligence in context, understanding relevance in the context of organisational strategy Applies and directs others in application of expertise and insight to enrich threat information, including understanding the behaviour, capabilities and activities of threat actors and assessing possible implications Is responsible for disseminating enriched threat intelligence Directs and is responsible for the application of threat intelligence to model threats, including sophisticated and complex threats, to protect organisational assets and goals, including informing the selection of security controls, developing indicators of compromise, detecting illicit behaviour (including evidence of fraud and crime), and providing context for undertaking investigations and responding to events Leads and oversees the threat intelligence function and activities for an organisation Is responsible for strategy, policy, procedures, guidelines and selection of relevant tools and techniques within the organisation Advises and influences senior management when required, and influences developments in the field at a national level

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert. Skill levels are cumulative – for example, to hold a 'practitioner' level in this skill, you must meet the requirements of 'working' level too.

Threat intelligence and threat assessment

Skill	Skill source	Skill type
Threat intelligence and threat assessment	**CIISEC Framework** B1 skill	Cyber Security

Indicative training

Indicative training	Format	Length	Provider type
Advanced Threat Methodology	Classroom	6 days	External
CompTIA Cybersecurity Analyst+	Certification, Classroom	5 days	External
FOR500: Windows Forensic Analysis	Classroom	6 days	External
FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting	Classroom	6 days	External
FOR572: Advanced Network Forensics: Threat Hunting, Analysis and Incident Response	Classroom	6 days	External
FOR578: Cyber Threat Intelligence	Classroom	5 days	External
MGT512: Security Leadership Essentials for Managers	Classroom	5 days	External
SEC460: Enterprise Threat and Vulnerability Assessment	Classroom	6 days	External

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profression of the NCSC, CPNI or UKNACE.

Threat understanding

Skill	Skill source	Skill type
Threat understanding	**NIST**, CPNI	Cross-specialism

Skill definition	
Threat understanding encompasses evidence-based knowledge, including context, about an existing or emerging threat to assets that can be used to inform decisions.	
Awareness ★	Describes specific threats and how they may manifest themselves in a local environment Maintains understanding of local threat environment and can apply to inform and provide context for wider activities Uses local threat information in decision-making and planning Demonstrates knowledge of current threats and trends affecting the landscape
Working ★★	Interprets sources of threat information for the local environment and applies knowledge of the external environment Maintains understanding of local and strategic threat environments, and trends affecting the landscape, and can apply to inform and provide context Uses local and strategic threat information in decision-making and planning Communicates tailored threat information to relevant local stakeholders within the organisation
Practitioner ★★★	Proactively identifies, interprets and leverages a range of relevant sources of threat information, using a variety of techniques, to understand the threat environment (local and strategic), including its nature, capability, focuses of interest and other factors associated with relevant threats Uses lessons learned to maintain an understanding of the organisation's attack surface, and uses local and strategic threat information in decision-making and planning Communicates tailored threat information to relevant senior stakeholders across multiple sites and/or business functions Combines external threat information, organisational context and situational awareness to provide a holistic threat understanding capability
Expert ★★★★	Uses a range of techniques and sources to develop, maintain and direct an understanding of the operating threat environment, including its nature, capability, focuses of interest and other factors associated with relevant threat sources/threat actors Combines external threat information, organisational context and situational awareness to provide a holistic threat understanding capability, including the use of threat models Communicates tailored threat information to relevant senior stakeholders at the board level across multiple sites and/or business functions Combines external threat information, organisational context and situational awareness to provide a holistic threat understanding capability to teams and organisations

Security skills are measured using the Digital, Data and Technology skill level ranging from Awareness to Expert. Skill levels are cumulative – for example, to hold a 'practitioner' level in this skill, you must meet the requirements of 'working' level too.

Threat understanding

Skill	Skill source	Skill type
Threat understanding	**NIST**, CPNI	Cross-specialism

Indicative training

Indicative training	Format	Length	Provider type
Security Management Course Level 3	eLearning	Self-paced	External
The Cyber Threat to UK Businesses	eLearning	3 months	External

Training included in the career framework is for illustrative purposes only and is not endorsed by the Government Security Profression of the NCSC, CPNI or UKNACE.

Development

What is development?

Development activities can be undertaken to improve a particular skill or area in your current role and as you progress through or towards different roles.

There are many fantastic support mechanisms and development opportunities available within government. The Civil Service Reform Plan guarantees each individual a minimum of 5 working days for development each year. There is mandatory training we are all required to do, alongside a multitude of other opportunities.

Your career is your responsibility, but there is help and support available to aid your career progression.

To develop your career, you will need to gain a breadth and depth of experience. The specifics will depend on the career aspirations that you have. The career framework will help you identify this in discussion with your line manager, or a mentor or coach.

You do not necessarily need a long-term career plan to manage your career proactively. You do, however, need to be clear on what aspirations you have so that you can identify opportunities and plan when to move on from an existing role or area.

Who is it for?

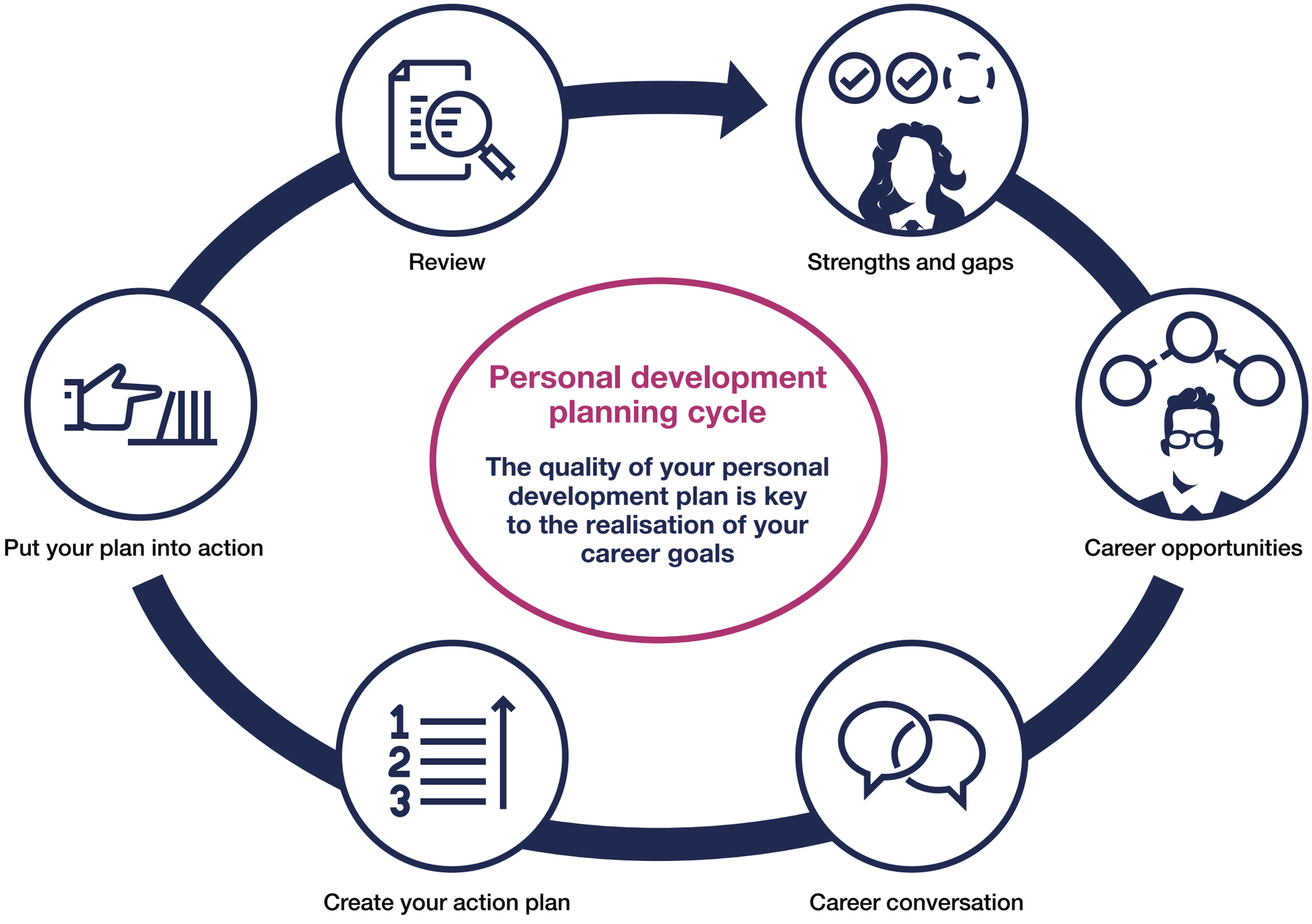
The Government Security Profession career framework is for all security professionals or aspiring professionals.

How do I access it?

- Through discussions with your line manager
- Through Civil Service Learning (or equivalent if your organisation is not aligned to CSL)
- Through internal capability initiatives within your own department or organisation
- On the job – use this tool to complete your profile

When should I do this?

As you discuss your personal development plan with your line manager to agree the skill level (awareness, working, practitioner or expert level) you should be progressing towards during the performance year, or during your regular performance reviews.


Review
Strengths and gaps
Career opportunities
Personal development planning cycle
The quality of your personal development plan is key to the realisation of your career goals
Put your plan into action
Create your action plan
Career conversation

Strengths and gaps

Career opportunities

Career conversation

Create your action plan

Put your plan into action

Review

Understand your strengths and gaps

Questions to think about

- Where are you in your career now?
- What are you good at?
- What do you like doing?
- How do you get feedback on your strengths and weaknesses?
- How do you like to learn?
- What would you like to improve?
- What 3 skills would enable you to be more effective?
- What 3 experiences would help broaden your knowledge?
- What are the barriers that could impact your performance at work?
- If you could rate yourself 1 to 10 (10 being outstanding), where are you in your current role?
- How could you improve on that number?

People who can help you

- Line manager
- Role model
- Mentor
- Coach
- Peers
- Government Security Profession team
- Subject matter expert
- Senior security professional

When you need to think about this

- Regularly with your informal support network
- Periodically through seeking feedback and honest self-assessment
- Revisit skills and development regularly in line with annual reviews

Tools that can support you

- Success profiles
- Government Security Profession career framework
- 360 degree feedback (where appropriate)
- Personal development/action plan
- Skills profiling tool

Key points for line managers

» Familiarise yourself with the Government Security Profession career framework

» Ensure regular one to ones with individuals

» Take the opportunity to give and receive regular, honest and fair feedback

» Remember to encourage and endorse skills in the online skills tool

Strengths and gaps

Career opportunities

Career conversation

Create your action plan

Put your plan into action

Review

Investigate career opportunities

Questions to think about

- What security projects or areas interest you?
- How do your specific goals match your career path?
- What skills and experience should you be looking to obtain?
- How would you describe your ideal development opportunities?
- What other areas of the business would you like to know more about?
- When assessing yourself against your skills, which do you struggle to meet?
- Even if you are doing the same role, how will you have evolved in 12 months?
- Can you talk to people in areas of interest?
- Can you job shadow to gain experience?
- Are there secondment/loan opportunities?

People who can help you

- Line manager
- Peers
- Mentor
- Coach
- Government Security Profession team

When you need to think about this

- Any time – it's smart to stay current
- Before holding your performance or development review
- When you are contemplating a change in your role

Tools that can support you

- Internal and external publications
- Civil Service Jobs
- Conferences and seminars
- Career profiles
- Career conversations

Key points for line managers

» Be supportive and give guidance

» Talk about short, medium and long-term goals

» Connect individuals to other people

» See the bigger picture – think of the future of the business and what would support ongoing business needs

Strengths and gaps

Career opportunities

Career conversation

Create your action plan

Put your plan into action

Review

Hold career conversation

Questions to think about

- What progress have you made in the past 12 months?
- Are your career objectives realistic? Have they changed?
- Are your skills up to date?
- Have you gathered sufficient feedback?
- Have you thought about possible training needs and opportunities?
- If you could choose any role, what would that look like?
- What type of role would you like to be doing in 2, 5 and 10 years?
- What 3 skills will help you move towards this goal?
- What can you do now to prepare for your short, medium and long-term goals?

People who can help you

- Line manager
- Mentor
- Coach
- Government Security Profession team

When you need to think about this

- At least once a year, normally in the first quarter
- You should hold this conversation at any time if you feel you need to refresh your career plans

Tools that can support you

- Career pathways
- Skills
- Personal development/action plan
- Civil Service Learning
- Government skills profiling tool

Key points for line managers

» Talk about values, ambitions and motivations

» Talk about strengths, limitations and development needs

» Encourage individuals to think beyond what they are doing now

» Find out what motivates and inspires individuals

Strengths and gaps

Career opportunities

Career conversation

Create your action plan

Put your plan into action

Review

Create your action plan

Questions to think about

- What development opportunities would be of assistance to you?
- Is your development plan realistic?
- Does it challenge you?
- How do you get the support to implement the plan?

People who can help you

- Line manager
- Mentor
- Coach
- Role model
- Peers
- Government Security Profession team

When you need to think about this

- During and after your annual conversation with your line manager
- In conversations with your mentor
- In self-initiated conversations with role models or others

Tools that can support you

- Career pathways
- Skills
- 360 degree feedback (where appropriate)
- Personal development/action plan
- 70/20/10 opportunities

Key points for line managers

» Help to create a realistic and challenging personal development/action plan

» Help to identify resources and opportunities

» Encourage individuals to get direction and advice from other sources (i.e. their mentor)

» Provide opportunities to help learning through experience

Strengths and gaps
Career opportunities
Career conversation
Create your action plan
Put your plan into action
Review

Put your plan into action

Questions to think about

- How do you make personal development an everyday activity?
- How do you ensure your development/ action plan is not compromised when you are too busy?
- How do you engage the right people to help you?

People who can help you

- Mentor
- Coach
- Role model
- Government Security Profession team

When you need to think about this

- Following directly from your development conversations
- In follow-up conversations with your line manager, mentor and others involved

Tools that can support you

- Government skills profiling tool
- 360 degree feedback (where appropriate)
- Personal development/action plan
- Civil Service Jobs

Key points for line managers

» Support individuals by recommending specific actions they could do to get started

» Follow up and give them time and space to focus on development

Strengths and gaps

Career opportunities

Career conversation

Create your action plan

Put your plan into action

Review

Review

Questions to think about

- Are you satisfied with your progress?
- What have you learned recently?
- Is there anything missing?
- Are you delivering on your objectives?

People who can help you

- Line manager
- Role model
- Government Security Profession team
- Mentor
- Coach

Tools that can support you

- Career pathways
- Skills
- 360 degree feedback (where appropriate)
- Personal development/action plan
- Online skills tool

When you need to think about this

- Advised monthly, spend a few minutes thinking about achievements and required steps

Key points for line managers

» Informal checking in with individual can be useful to help reinforce the need to keep their own development in view

» Encourage regular reviews

» Provide support throughout the process

What is continuous personal development?

As someone working in a security environment you will already be involved to some degree with continuous professional development (CPD). Searching the internet for information, doing something new and sharing knowledge either formally or informally with colleagues are all part of CPD.

Making CPD a more formal part of the development process will help you make the most of available learning opportunities and have these recognised as part of your personal development plan. The vast majority of continuous professional development relates to 'near the job' learning. See the detail of the 70/20/10 principle for more information on the different types of learning.

Length of CPD

We recommend that those working in a security role or those wanting to maintain their security skills undertake a minimum of 5 days CPD per annum. This aligns with the Civil Service's "5 days learning per year". CPD should be logged and discussed with line managers as part of regular development discussions.

Types of CPD

Some examples of CPD for the Government Security Profession are listed below. This list is not exhaustive. We also recommend that you consider a varied approach to your CPD learning choices and try new things each year.

Shadowing and networking

- Work-shadowing a fellow security professional
- Acting as a mentor or coach for a fellow security professional
- Being mentored or coached by a fellow security professional
- Attending a meeting of a relevant security professional association
- Undertaking a security review as either a review team member or review team leader
- Being an assessor at a security Fast Track or Fast Stream assessment centre
- Attending security community events
- Delivering a presentation at a security community event

Self study

- Attending internal masterclass or learning event
- Reading security literature or internet material

Formal learning

- Accredited training course (including its ongoing maintenance if the certification requires it)
- E-learning – e.g. through Civil Service Learning

Advice on successful CPD

CPD works best for individuals when it is:

Relevant

“The experiences are those that enable you to use CPD at work to immediately improve on performance”

Collaborative (i.e. done with other people)

“Presenting my work to colleagues produced positive feedback and a lively debate on my findings”

Recognised

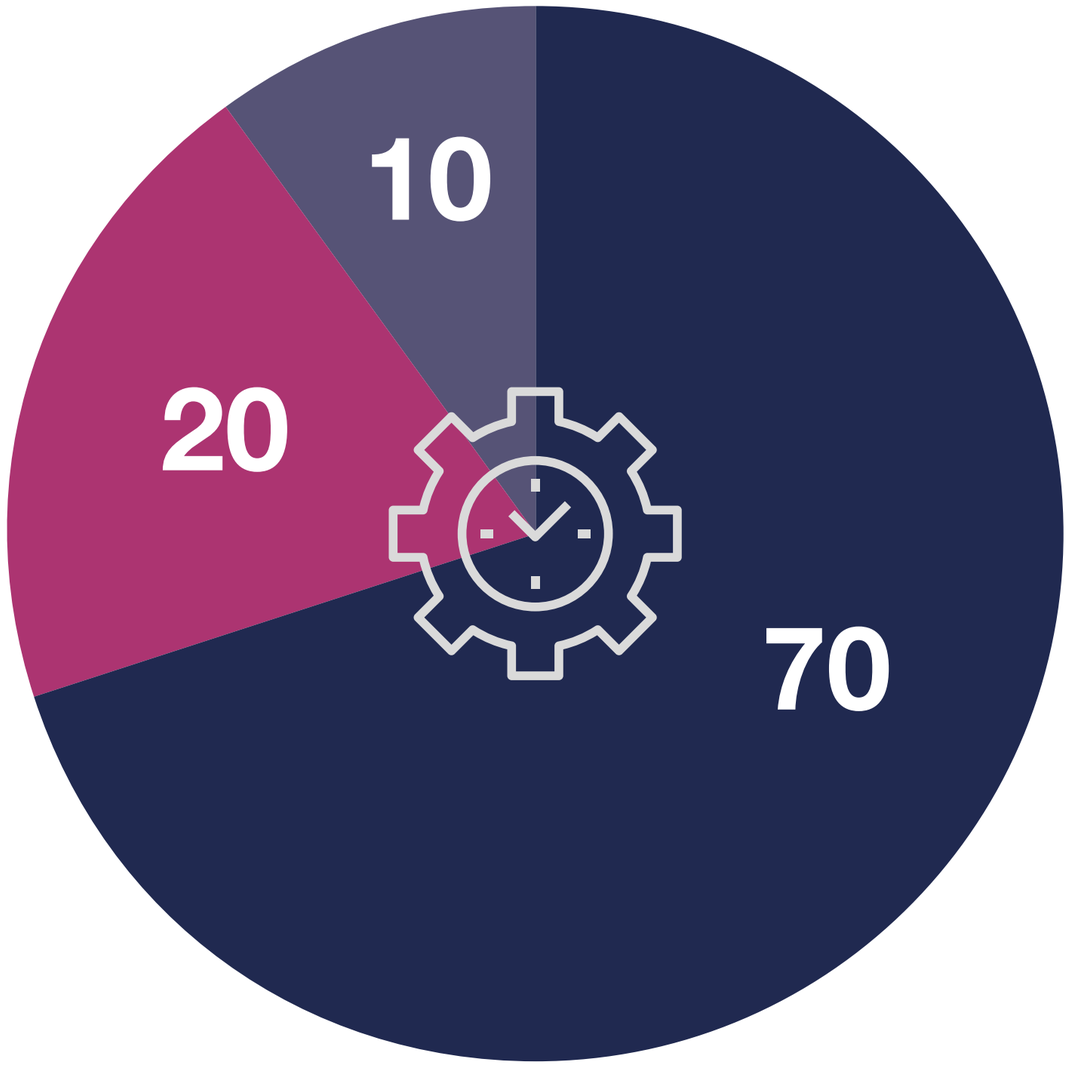
“The trouble with CPD is that you have to do it, you do it on your own, and it’s not recognised”

Personal

“CPD works best if it is led by the individual”

What is 70/20/10?

70/20/10 is a widely used learning and development model. The three numbers represent the relative amount of learning time a person typically spends on the following three activities to optimise their development. These ratios should not be taken literally but are a relative indication of time.



70% ‘Learning through experience’

On the job

This is often regarded as the most beneficial as it enables you to put your knowledge into practice and embed learning. It’s about stretching ourselves to take on areas of work responsibilities that are new to us and learning through these experiences.

20% ‘Learning through others’

Near the job

This is sometimes referred to as ‘Social Learning’. It’s about how we share our knowledge and experiences with others and also how we learn from them. There are many ways to do this. We refer to this as continuous professional development (CPD) and you can see some of the many examples of this on our CPD page.

10% ‘Learning through structured education’

Off the job

This covers all forms of formal courses and learning programmes. These may be delivered through e-learning, in a classroom or through distance learning.

Spotlight on career framework training

How does the career framework training link to 70/20/10?

According to the 70/20/10 model, 70% of learning is through experience, 20% is learning through others and 10% is learning through structured education. The content of the career framework 'training repositories' is structured education, whether within government or externally supplied. It therefore addresses only the 10%.

Why is the career framework training indicative and not recommended?

The training is sourced from security professionals from government departments. It has not been validated as fit for purpose, so is included in the career framework for illustrative purposes only. The validation of whether the training is fit for purpose is planned for the Government Security Profession's next phase.

How do I access the career framework training?

The career framework training is mapped to skills. Click on the 'repository' after the skill minimum expectations to access the indicative training. Here you can view the training format (e.g. eLearning, certifications, classroom based), length and provider type of each indicative training course.

When can I expect to access validated training?

The Government Security Profession is working to develop a suite of tools to support security professionals develop their careers. Contact **gsp@cabinetoffice.gov.uk** for the latest information on where we are in the skills profiling tool mobilisation and training validation journey.

What will the complete Government Security Profession offering look like?

The Government Security Profession career framework is one of many government security capability building blocks. The complete Government Security Profession offering will include validated training mapped to each career framework skill and a skills profiling tool. This skills profiling tool will enable security professionals to access and navigate training mapped to each career framework skill.

Resources

Glossary of terms

Asset	Anything that has value to the organisation, including software, information, people and reputation.
Attack	Any attempt to destroy, expose, alter, disable, steal or gain unauthorised access to or make unauthorised use of an asset.
Availability	The attribute of being accessible and usable upon demand by an authorised entity.
Career framework	Career frameworks developed within and for a profession articulate in one place the skill, experience and capabilities needed for each role for that profession.
Career pathways	Internal entry routes outline the typical government jobs from which individuals can transfer into Government Security Profession roles. External entry routes outline the typical industry jobs from which individuals can transfer into Government Security Profession roles.
Confidentiality	When information is not made available or disclosed to unauthorised individuals, entities or processes.
Consequence	The outcome of an event affecting objectives.
Control	A means of managing risk, including policies, procedures, guidelines, practices or organisational structures, which can be of an administrative, technical, management or legal nature.
Corporate Enablers	Corporate Enablers span the specialisms and are pivotal to the growth, development and success of the Government Security Profession.
Integrity	The attribute of protecting the accuracy and completeness of assets.
Likelihood	The chance of something happening.
Risk	Possible future outcomes that we can describe in terms of their chances of occurrence, and what impact they would have on us (**NCSC**) or the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation (ISO27005).
Role	High-level job groupings which detail the position an individual plays in an organisation or department. Roles are not job descriptions.
Role family	High-level grouping of associated roles within a security specialism.
Role level	Role levels are the hierarchy of levels within a role. Examples include associate, lead and principal.
Security specialism	The Government Security Profession career framework is made up of 4 security specialisms: Physical Security, Personnel Security, Cyber Security and Technical Security.
Skill	The expertise or aptitude in a capability. Can be relevant across specialisms (Physical, Personnel, Cyber, Technical) or specific to one specialism.
Threat	Anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage or destroy an asset.

Design principles

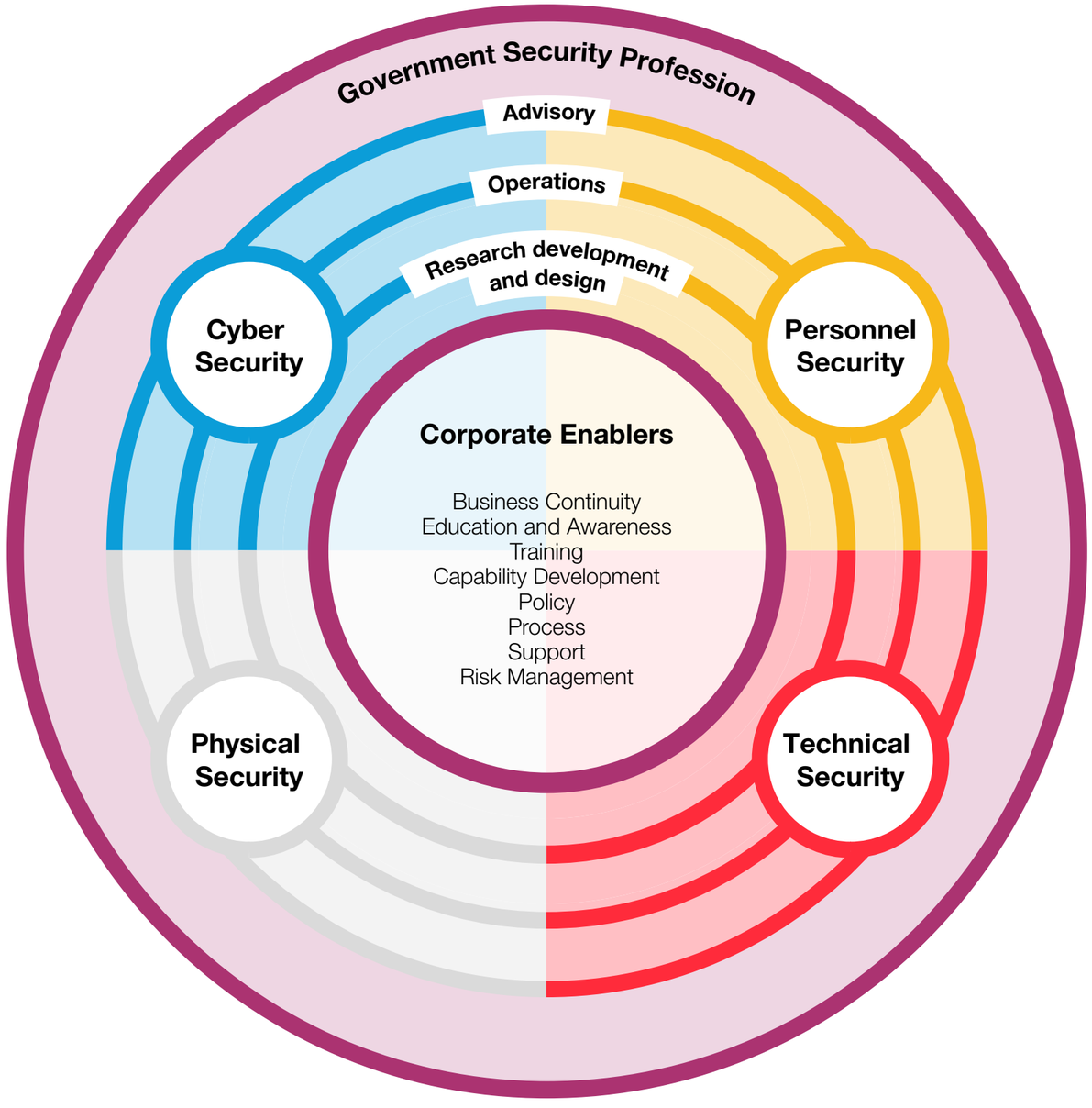
Principles governing the Government Security Profession career framework

Civil Service Code or equivalent*	In addition to meeting the role, skill and success profiles outlined, all roles should adhere to the Civil Service Code or organisational equivalent, where appropriate. The Civil Service Code forms part of the terms and conditions of every civil servant. It outlines the core values of the Civil Service. These core values are honesty, integrity, impartiality and objectivity.*
Continuous development	As the Government Security Profession has a vocational nature, practitioners are expected to continuously develop themselves. Suggested training and development activities and professional qualifications are indicative, and do not replace organisational experience.
Framework-campaign relationship	The Government Security Profession career framework provides the basis for organisation-led recruitment campaigns, which will then be built upon with the addition of specific requirements.
Qualification equivalency	Work is ongoing to develop a benchmark of equivalencies between Cyber Security qualifications (e.g. Certified Information Systems Security Professional/Certified Information Security Manager).
Scope of the Government Security Profession	The Government Security Profession is comprised of security professionals from the Civil Service, the armed forces, HM Inspectorate of Constabulary and Fire and Rescue Services, the security services and private sector contractors employed by the government. All are bound by a common framework and a set of values and standards.

*Taken from the Civil Service Code

Career framework structure

The Government Security Profession career framework has 4 security specialisms: Personnel, Physical, Technical and Cyber Security. The career framework also has Government Security Profession Corporate Enablers. The Corporate Enablers span the specialisms and are pivotal to the growth, development and success of the Government Security Profession. Individuals working in a corporate enabler role may belong to more than one government function and profession. The Corporate Enablers included in the career framework are leadership, business continuity, education and awareness, training, capability development, policy, process, support, and risk management. This list is non-exhaustive.



Government Security Profession specialisms

The Government Security Profession career framework is composed of 4 specialisms. Each specialism contains 3 role families.

Physical Security	Physical Security protects assets, including people, services, infrastructure, systems, places, equipment and networks. Effective Physical Security is achieved by multi-layering different measures, which is commonly referred to as ‘defence in depth’. The concept is based on the principle that the security of an asset is not significantly reduced with the loss of any single layer.
Personnel Security	Personnel Security is a system of policies and procedures that seeks to identify, understand and mitigate the risk of workers (insiders) exploiting their legitimate access to an organisation’s assets for unauthorised purposes.
Cyber Security	Cyber Security protects information systems (hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures.
Technical Security	Technical Security holistically protects sensitive information and technology from close access acquisition or exploitation by hostile actors, as well as any other forms of technical manipulation.

Physical Security – role families

Role family	Role family definition
Advisory	Responsible for providing Physical Security advice and assurance internally, to the government and industry partners, and externally, including to the private sector.
Operations	Responsible for the efficient and effective management of all aspects of physical operations, including outsourced capability (e.g. services and people) of physical and personal security from the places where people work and the people themselves, to the locations of systems, services and networks.
Research, development and design	Responsible for research and knowledge development of Physical Security countermeasures and associated guidance.

Personnel Security – role families

Role family	Role family definition
Advisory	Responsible for providing Personnel Security advice and assurance internally, to the government and industry partners, and externally, including to the private sector.
Operations	Responsible for conducting and facilitating people screening, implementing, reviewing and assessing security monitoring policies and investigating breaches or incidents of concern.
Research, development and design	Responsible for research and knowledge development of Personnel Security countermeasures and associated guidance.

Cyber Security – role families

Role family	Role family definition
Advisory	Responsible for advising and enabling teams to make security decisions. This includes providing advice and guidance about technical matters and the identification of cyber-related risks, and how to mitigate and manage risks.
Operations	Responsible for monitoring, responding to and proactively managing threats facing the organisation, including by monitoring event data, collecting and disseminating actionable intelligence, and managing identified vulnerabilities across the organisation.
Research, development and design	Responsible for ensuring development and design of applications is done with sensitivity to threats facing the organisation, and building security in the development process. This includes, for example, conducting penetration tests and social engineering tests.

Technical Security – role families

Role family	Role family definition
Advisory	Responsible for identifying and mitigating security risks relating to Technical Security, including ensuring the appropriate implementation of effective countermeasures, while ensuring that mitigations are aligned to the risk register at both the corporate and tactical levels.
Operations	Responsible for delivering the protection of sensitive information and technology from close access acquisition or exploitation by hostile actors.
Research, development and design	Responsible for research and knowledge development of Technical Security countermeasures and associated guidance.

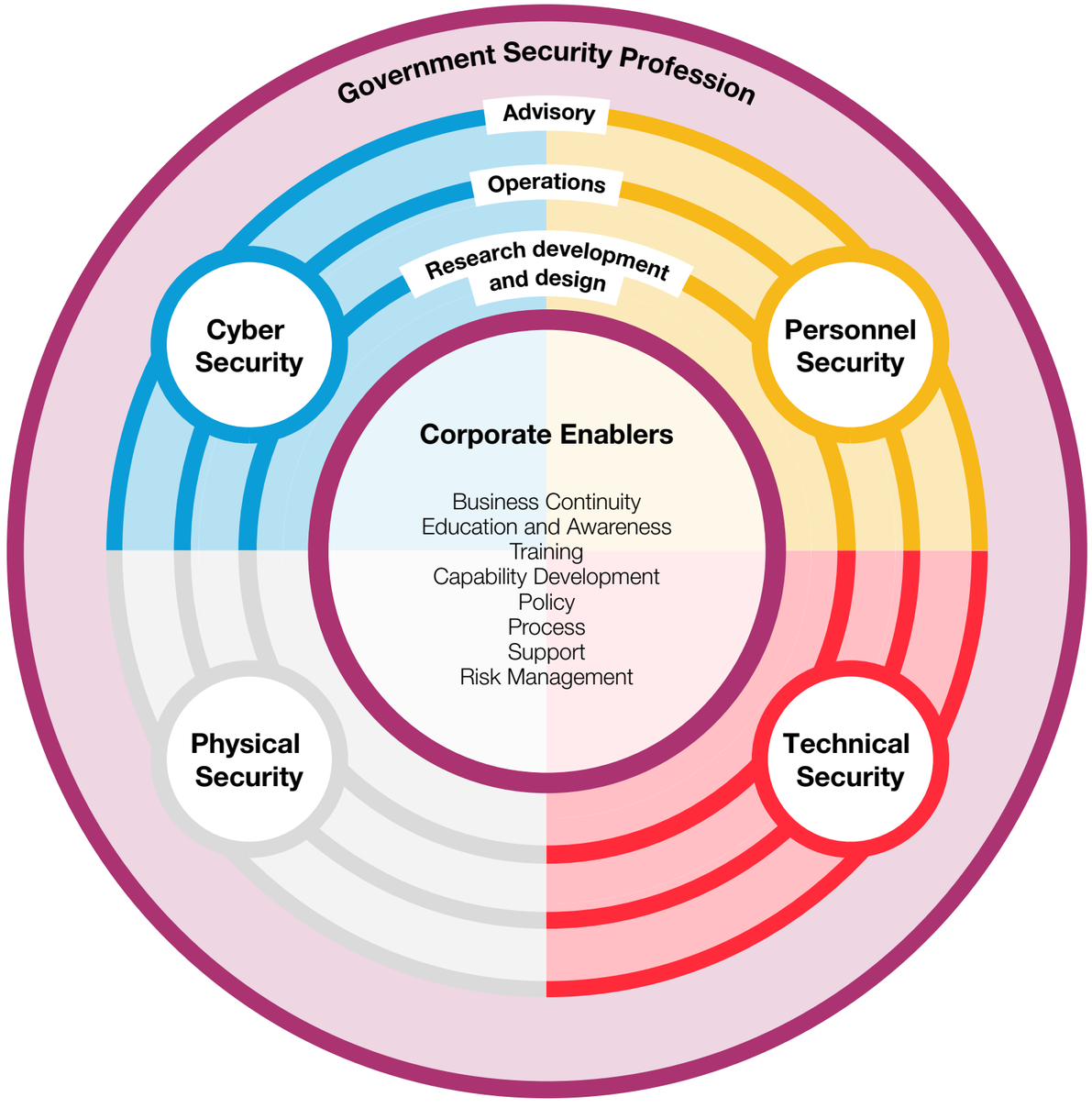
Government Security Profession – role levels

Role level	Role level definition
Associate	An individual with limited relevant prior experience.
Lead	An individual with relevant prior experience.
Principal	An individual with significant relevant prior experience.

Government Security Profession Corporate Enablers

What is a corporate enabler?

In addition to the Government Security Profession career framework's 4 security specialisms, the career framework also includes Government Security Profession Corporate Enablers. The Corporate Enablers span the specialisms and are pivotal to the growth, development and success of the Government Security Profession. An individual working in a corporate enabler role may belong to more than one government function and profession. The Corporate Enablers included in the career framework are leadership, business continuity, education and awareness, capability development, policy, process, support and risk management. This list is non-exhaustive.



Success profiles

What are the elements of the success profile?

Ability

The aptitude or potential to perform to the required standard.

Technical

The demonstration of specific professional skills, knowledge or qualifications.

Behaviours

The actions and activities that people do which result in effective performance in a job.

The Government Security Profession career framework focuses on success profile behaviours.

Strengths

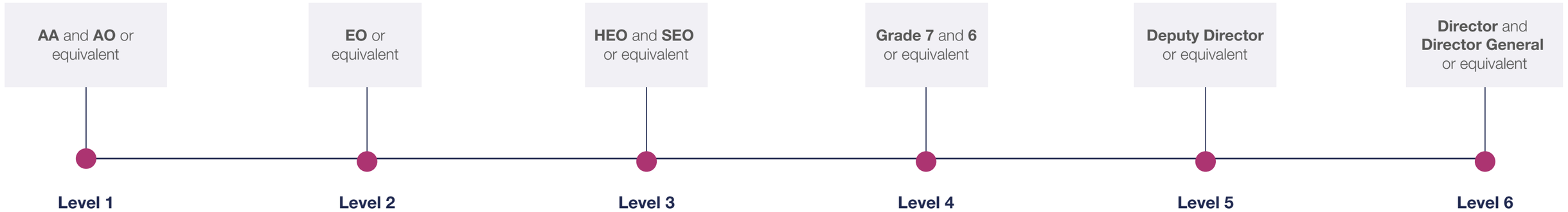
The things we do regularly, do well and that motivate us.

Experience

The knowledge or mastery of an activity or subject gained through involvement in or exposure to it.

Success profiles

Civil Service behaviours	General description
Seeing the big picture	Understand how your role fits with and supports organisational objectives. Recognise the wider Civil Service priorities and ensure work is in the national interest.
Changing and improving	Seek out opportunities to create effective change and suggest innovative ideas for improvement. Review ways of working, including seeking and providing feedback.
Making effective decisions	Use evidence and knowledge to support accurate, expert decisions and advice. Carefully consider alternative options, implications and risks of decisions.
Leadership	Show pride and passion for public service. Create and engage others in delivering a shared vision. Value difference, diversity and inclusion, ensuring fairness and opportunity for all.
Communicating and influencing	Communicate purpose and direction with clarity, integrity and enthusiasm. Respect the needs, responses and opinions of others.
Working together	Form effective partnerships and relationships with people both internally and externally, from a range of diverse backgrounds, sharing information, resources and support.
Developing self and others	Focus on continuous learning and development for self, others and the organisation as a whole.
Managing a quality service	Deliver service objectives with professional excellence, expertise and efficiency, taking account of diverse customer needs.
Delivering at pace	Take responsibility for delivering timely and quality results with focus and drive.



Curious? Get in touch

Email the Government Security team at
gsp@cabinetoffice.gov.uk

Find out about Government Security careers:
www.civil-service-careers.gov.uk/professions/working-in-security/

Subscribe to the Government Security blog:
securityprofession.blog.gov.uk