



Government
Security
Profession

Career framework

For security professionals
in government

A user guide

Contents

User guide overview	3	Skill levels and role levels	11
Career pathways overview	4	Skill expectations and success profiles	12
Grade to role mapping	5	Career pathways	13
Example career profiles	6	Recruitment	14
Learning and development	7	Framework guidance	15
Personal development	8	Resources overview	16
Roles and role level expectations	9	Curious? Get in touch	17
Skills	10		

User guide overview

This document supports departmental capability leads, career framework Champions and line managers to embed the career framework.

What is the purpose of this document?

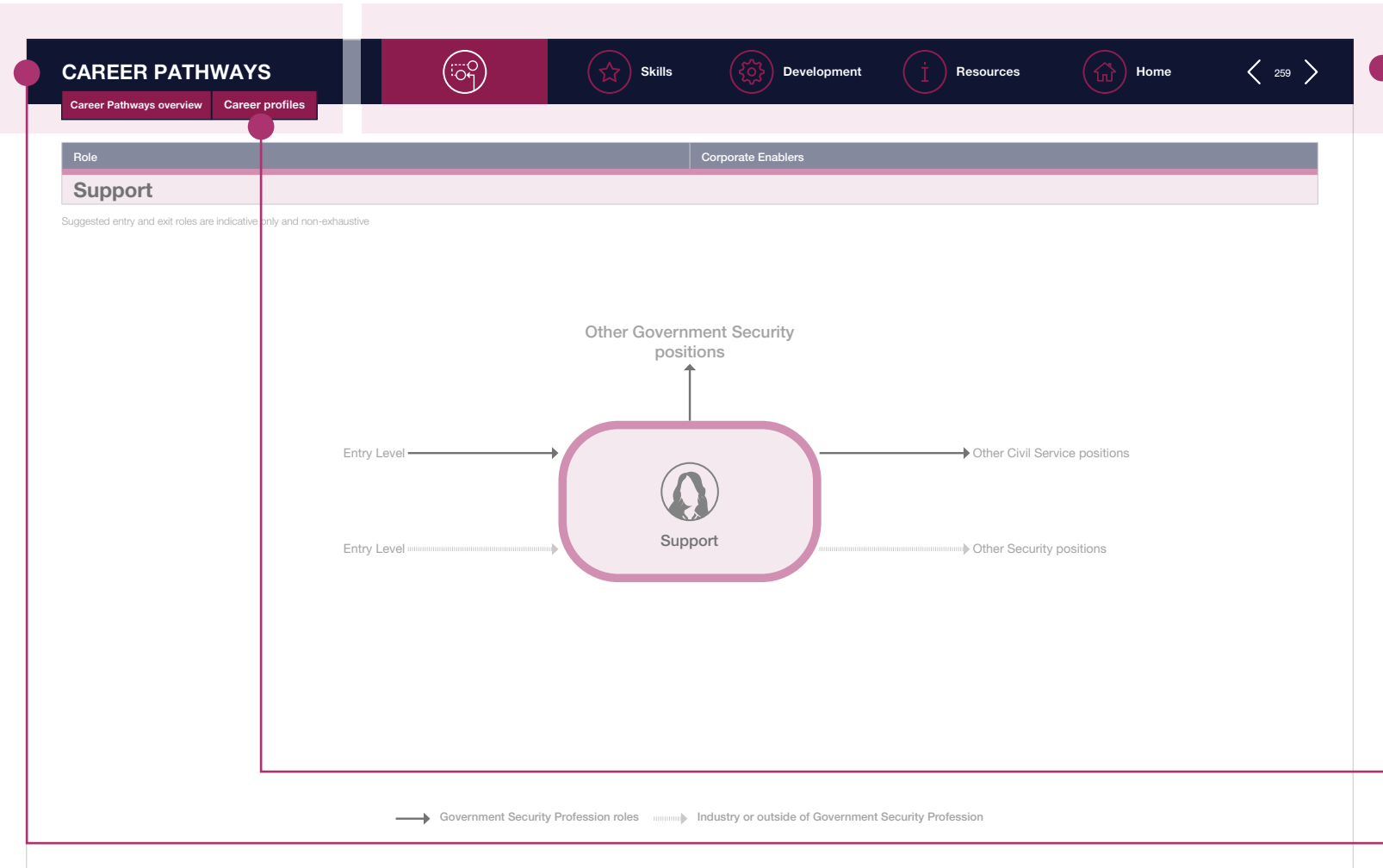
To help departmental capability leads, career framework Champions and line managers navigate the career framework so they can successfully embed it within their departments. It includes an explanation of how to access each component of the career framework, what each component contains and frequently asked questions for each component. It is also a useful reference tool.

How do I navigate the career framework?

There are 5 main components to the Government Security Profession Career Framework:

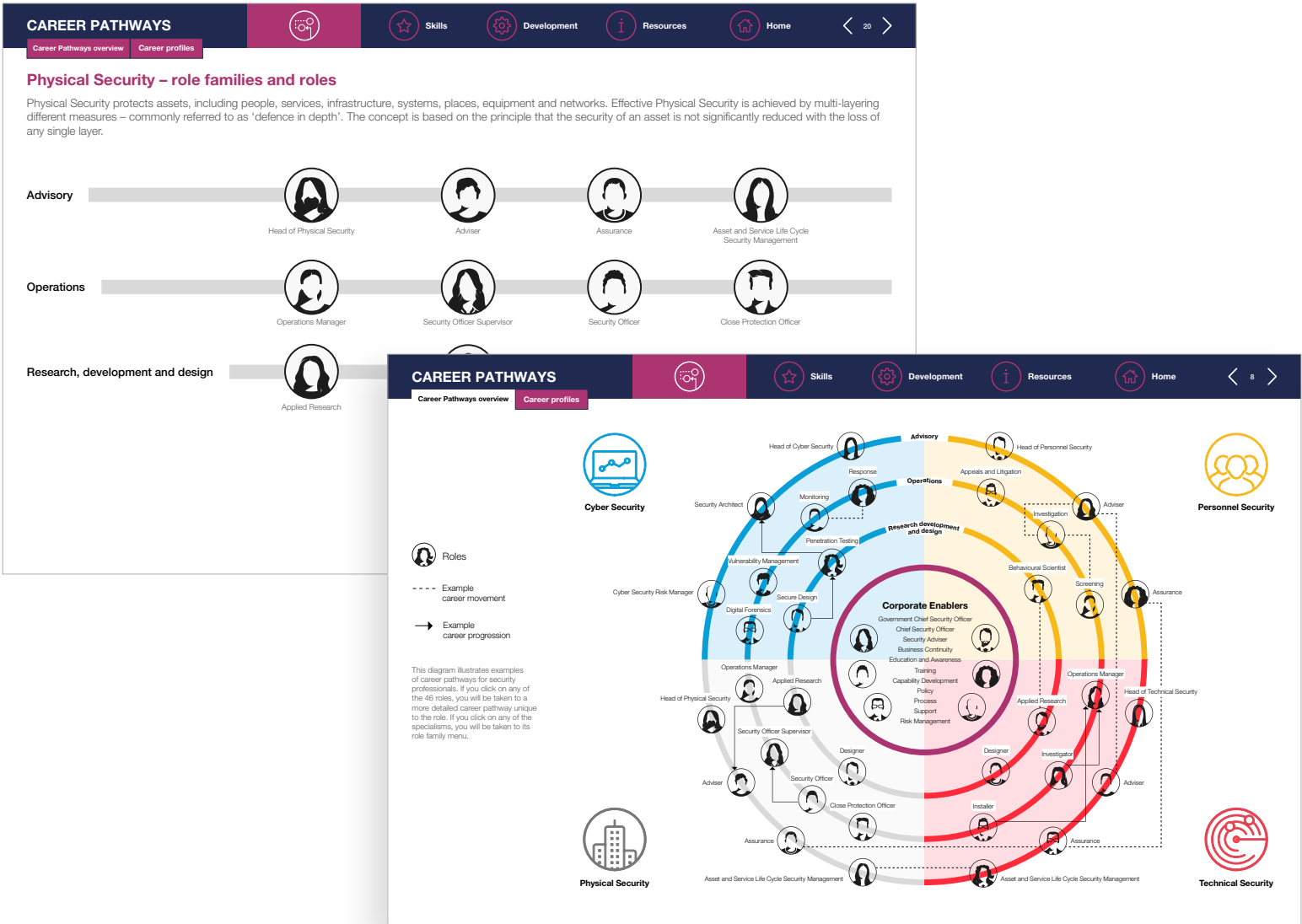
- Home
- Career pathways
- Skills
- Development
- Resources

To navigate between each, click through the navigation bar at the top of the career framework.



Career pathways overview

The career framework contains specialisms, role families and roles. You can see these all on one page in the career pathway overview.



What is the career pathway overview?

A visual representation of the specialisms, role families and roles, all on the same page. The definitions for each of these are in the glossary of terms, in the resources.

What are the key elements?

The career pathway overview includes indicative career pathways, which are examples of career progression and horizontal movement 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. The career pathway includes indicative entry and exit routes, linked to the rest of the career framework where the role is in the Government Security Profession.

How should it be used?

It is a good entry point into the career framework. You can navigate to the rest of the career framework from it, by clicking on specialisms or individual roles.

Grade to role mapping

The career framework includes indicative grade to role mapping for the 4 specialisms and corporate enablers.

Why is indicative grade to role mapping included?

Indicative grade to role mapping is included in the career framework at the request of Government Security Professionals, and to adhere to Civil Service HR career framework guidelines.

Why are there two different sets of indicative grades?

The grade to role mapping includes Civil Service grades and indicative military grades. The latter are sourced from NATO and recognised across the armed forces, Royal Air Force and Royal Navy.

How should I use the grade to role mapping?

Use the grade to role mapping to identify roughly what grades you would expect to see a role to be employed at. Click on a role to view the career pathway and role expectations. You will notice that a range of grades is given for each role. This is because each career framework role has between 2 and 3 levels. We would expect the different role levels to map to different grades.

CAREER PATHWAYS

Career Pathways overview

Career profiles

Skills

Development

Resources

Home

< 10 >

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	Head of Personnel Security									
		Advisory									
		Adviser									
	Operations	Assurance									
		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.

Example career profiles

The career framework includes career profiles from professionals working in Government Security.

CAREER PATHWAYS

Career Pathways overviewCareer profiles

Skills

Development

Resources

Home

<14>

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

Why did you include example career profiles?

To share examples of security professionals who work across the 4 security specialisms and corporate enablers. The individuals have all contributed to the development of the career framework.

What do the career profiles contain?

The career profiles contain the career journeys to date of different security professionals. For example, Deborah Smith-Dunlop’s career profile demonstrates that it’s possible to move into the security profession from a different profession, as Deborah explains that she started her career in Human Resources.

How should I use the career profiles?

You should use the career profiles to identify the diversity of the career opportunities available to Government Security Professionals. You can hyperlink back to the career pathways, skills or development by clicking on the bar at the top of the page.

Learning and development

Each skill has a repository of indicative training. This training is not endorsed by the Government Security Profession. A full learning suite will be developed to support the framework.

SKILLS

Skill level definitionsList of skills

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	NCSO 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	
Information risk assessment and risk management	Cyber Security	
Intrusion detection and analysis	Cyber Security	
Investigative interviewing	Personnel Security	
Legal and regulatory environment and compliance	Cross-specialism	
Penetration testing	Cyber Security	
Protective security	Cross-specialism	
Risk understanding and mitigation	Cross-specialism	
Secure design	Cyber Security	
Secure development	Cyber Security	
Secure operations management	Cross-specialism	
Secure supply chain management	Cross-specialism	
Security architecture	Cyber Security	
Threat intelligence and threat assessment	Cyber Security	
Threat understanding	Cross-specialism	

DEVELOPMENT

Personal development planning

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.

10

20

70

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.

What is 70/20/10?

70/20/10 is a widely used learning and development model. According to it, 70% of development is learning through experience, 20% is learning through others and 10% is learning through structured education. The career framework training repositories address the 10%.

Why is the training indicative and not recommended? Why isn't it endorsed by the National Technical Authorities?

The training is sourced from cross-government security professionals. The validation of whether the training is fit for purpose is planned for the next phase. We will be working closely with NTAs and other security experts to deliver a comprehensive learning offer in late 2020. In the meantime, robust development conversations are essential to ensure that you are achieving the appropriate development for your chosen career path.

How do I access the 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.

Personal development

The career framework development plan should be used to structure regular performance achievement conversations.



Why is development in the career framework?

Development is a key aspect of the career framework. We encourage you to use the career framework in performance conversations with your line manager to discuss your target role and agree the skill levels you should be progressing towards over the performance year.

What is the personal development planning cycle?

There are 6 elements to the personal development planning cycle:

- understanding your strengths and gaps
- investigating career opportunities
- holding career conversations
- creating your action plan
- putting your plan into action
- reviewing

Access each area in the career framework by clicking on the icon. Key points for line managers are called out in a blue box on each page.

Roles and role level expectations

Each of the 46 career framework roles has a role summary and role level expectations.

CAREER PATHWAYS

Career Pathways overview

Career profiles

Skills

Development

Resources

Home

<

30

>

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

Why does each role level have expectations?

The 46 career framework roles each have role level expectations because the typical responsibilities a professional carries out will differ, depending on their skill levels. The skills for each role are the same; the skill levels progress with the role level progression.

What are role level expectations?


Role level expectations are mapped to associate, principal and lead role levels. The role level expectations are aligned to the progression of skill levels. They reflect the typical responsibilities a professional with the skill levels would carry out.

How can I access the role level expectations?

You can access role level expectations for each of the 46 career framework roles by clicking on the role in the career pathway overview, and then scrolling through the role levels mapped to the role.

Skills

The 25 career framework skills each have 4 levels.



SKILLS

Skill level definitions

List of skills

Career Pathways

Development

Resources

Home

272

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.

Why are there fewer skills than roles in the career framework?

There are 25 skills in the career framework, shared across 46 roles. Many of the skills can appear in more than one role. Each skill has 4 levels: awareness, working, practitioner and expert.

What is a skill type?

‘Skill type’ refers to which of the 4 specialisms or corporate enablers the skill can be found in. Where a skill appears in a role in more than one specialism, it is labelled as a cross-specialism skill. For example, ‘design’ appears in a physical security role and a technical security role, so its skill type is cross-specialism.

How should I use the skills?

You should consider the skills for your role in parallel to the role expectations. Use the skills to structure regular development conversations, ideally with your line manager.


Skill levels and role levels


Career framework skill level expectations increase as the role level increases.


CAREER PATHWAYS


Career Pathways overview

Career profiles

 Skills

 Development

 Resources

 Home

< 131 >

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

What is a role level?

Each of the 46 career framework roles has 2 or more role levels. Role levels are a hierarchy of levels within a role. Examples include associate, lead and principal.

What is the difference between a skill level and a role level?

There are 4 skill levels to each skill: awareness, working, practitioner and expert. Skill level expectations increase as the role level increases. For example, the Principal Security Architect has higher skill level expectations than the Lead Security Architect, which has higher skill level expectations than the Associate Security Architect.

How can I access the skill levels and role levels?

The career framework visually presents the role levels mapped to the skills and skill levels. [Click on a skill](#) to view the definition of the skill at awareness, working, practitioner and expert.

Skill expectations and success profiles

Each career framework role has minimum skill expectations and success profile Civil Service behaviours.

CAREER PATHWAYS

Career Pathways overview

Career profiles

Skills

Development

Resources

Home

< 130 >

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
<ul style="list-style-type: none">Continuous Monitoring courseSecurity Operations Centre courseInformation risk management courseThreat awareness courseThreat intelligence course	<ul style="list-style-type: none">Membership of a relevant institution or body e.g. Institute of Information Security Professionals, Council for Registered Ethical Security TestersRelevant industry qualifications and accreditations e.g. Certified Security Operations Centre AnalystRelevant 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

Why does the career framework need success profile Civil Service behaviours?

Civil Service behaviours are the actions and activities that people do that result in effective performance in a job. The career framework includes success profile behaviours mapped to each role to guide professionals in the set of behaviours that, when demonstrated, are associated with job success.

What are success profiles?

The success profile framework was introduced across government to attract and retain people of talent and experience from a range of talent, in line with the Civil Service Workforce Plan. There are 5 elements of the success profiles: ability, technical, behaviours, strengths and experience. The Government Security Profession Career Framework focuses on success profile behaviours only.

How do I find out more about Civil Service behaviours?

Click on ‘success profiles’ on the role summary of any career framework role to access the GOV.UK Success Profiles: Civil Service Behaviours guidance pack. This is a 21-page document that gives examples of each behaviour, mapped to grade.

Career pathways

Each role has an indicative career pathway, including internal and external entry and exit routes.

Why does each role have a career pathway?

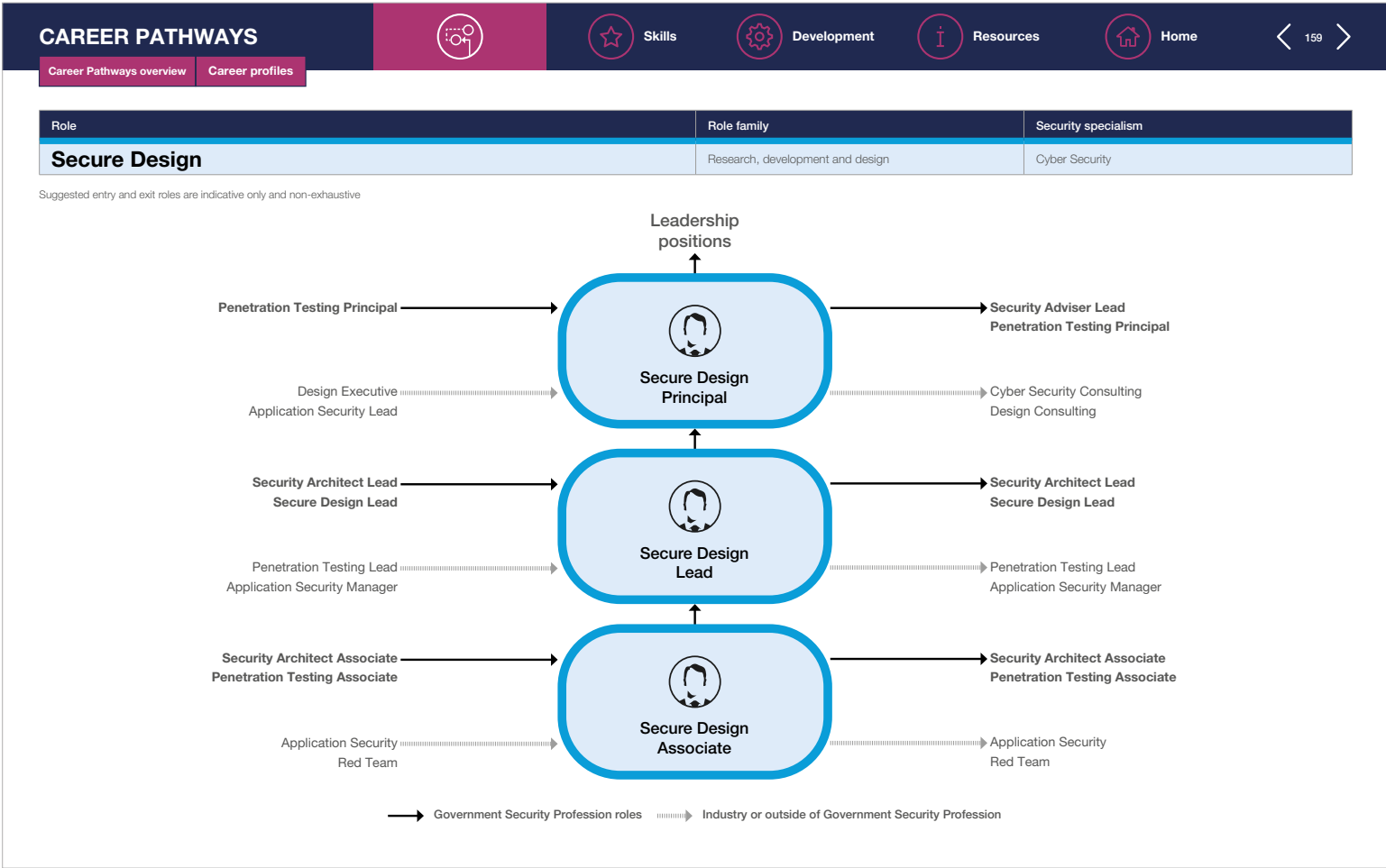
Career pathways are designed to facilitate progression within a role, and movement between roles and security specialisms. Each role has a career pathway with entry and exit routes, which include routes within and outside of the Government Security Profession, and routes in and out of industry.

What is a career pathway?

A career pathway has internal and external entry routes, to demonstrate what a career journey within a role could look like. Internal entry routes outline the typical government jobs from which professionals can transfer into Government Security Profession Career Framework roles. External entry routes outline the typical industry jobs from which individuals can transfer into Government Security Profession career framework roles. Suggested entry and exit routes are indicative only and non-exhaustive.

How do I access the career pathways?

Click on the [career framework overview](#) to view all 46 roles in one place. Click on any role to view the career pathway for that role. Where an entry or exit route links to a career framework role, this is hyperlinked.



Recruitment

The career framework should be used when recruiting for new roles.

CAREER PATHWAYS

Career Pathways overview

Career profiles

Skills

Development

Resources

Home

< 161 >

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

How can I use the framework for recruitment?

This framework is ideal for building consistency across role descriptions and levels of ability, within and across teams. This means you have a readily understood information base on which to construct your advertising.

The recruitment toolkit (available from our Knowledge Hub and our website) has the details you require, speeding up the task with content that has been prepared and cross-checked for you.

Used effectively, this framework will drive career pathways, guide development, and in time we will have associated accreditation; all of this increases promotion potential and is part of your recruitment offer.

It provides recruiting sifters with criteria to use in assessing applications and gives interviewers cues for Success Profiles questions to judge potential ability in a given role.

Above all, the framework can give you consistency of approach to apply to regular processes, making your life easier and your actions more effective.

Framework guidance

Most frequently asked questions are referenced in the introduction of the career framework document.



Why can't I find my job in the career framework?

The Government Security Profession Career Framework refers to roles rather than jobs. A role is an organised set of behaviours, responsibilities and activities granted to a person or team. One person or team may have multiple roles. Roles are about people, whereas jobs are about tasks and duties. Depending on the size of your organisation, you may carry out different aspects of multiple career framework roles on a day-to-day basis.

How can I request an amendment to the career framework?

To make an amendment you need to contact gsp@cabinetoffice.gov.uk to ask for a change request form.

Resources overview

The resources includes a glossary of key terms, design principles, an overview of the career framework structure and a description of the success profiles.

RESOURCES

Career Pathways

Skills

Development

i

Home

<

348

>

Success profiles

Experience

Ability

Technical

Behaviours

Strengths

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.

Why does the career framework have a resources?

The career framework includes a resources as a home for important information that doesn't fall under career pathways, skills or development. The resources includes a glossary of terms, the career framework design principles, the career framework structure overview and additional information on Civil Service success profiles. The purpose of the glossary of terms is to enable consistent use of key terms, such as 'asset', 'risk' and 'threat', across the security landscape and career framework.

What additional information can I find in the resources?

The resources gives additional information about the career framework structure, including definitions of the 4 security specialisms and their 3 role families. These role families are advisory, operations, and research and development and design. These 3 role families are consistent across physical, personnel, cyber and technical security. The appendix also shares the definition of the corporate enabler group, which cuts across all security specialisms.

How do I access the resources?

Click on 'resources' in the navigation bar. Alternatively, you can access the descriptions of each role family and specialism by clicking on the career framework overview and following the links to each definition.

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/](http://www.civil-service-careers.gov.uk/professions/working-in-security/)**

Subscribe to the Government Security blog:
securityprofession.blog.gov.uk