



*SFIA defines the skills and competencies required by professionals who design, develop, implement, manage and protect the data and technology that power the digital world.*

## **SFIA, enhancing adaptability and professionalism across the Royal Air Force Cyberspace Profession**

**Flight Lieutenant Amy Phillips- Mahon  
Flight Sergeant Debz Roberts  
RAF Cyberspace Profession Implementation Team**



Please use the Q&A facility to ask questions – we will try to answer some of these as we go along

Chat is available for other comments

This webinar is being recorded – Delegates will be muted with video off

Please complete the form at the end of this webinar

**The Webinar will start shortly ...**

Facilitators: Peter Leather, Ian Seward

To contact the SFIA Foundation: [ops@sfia-online.org](mailto:ops@sfia-online.org)

Please use the chat to  
tell us which country  
you are from

**Independent Global Not-for-Profit Foundation – *driven by industry and employers:***

Purpose

To enable greater capability and capacity within the global digital workforce

1. Active stewardship of the global skills and competency framework and its ecosystem to meet the needs of professionals and employers

2. Increase visibility and adoption of SFIA globally

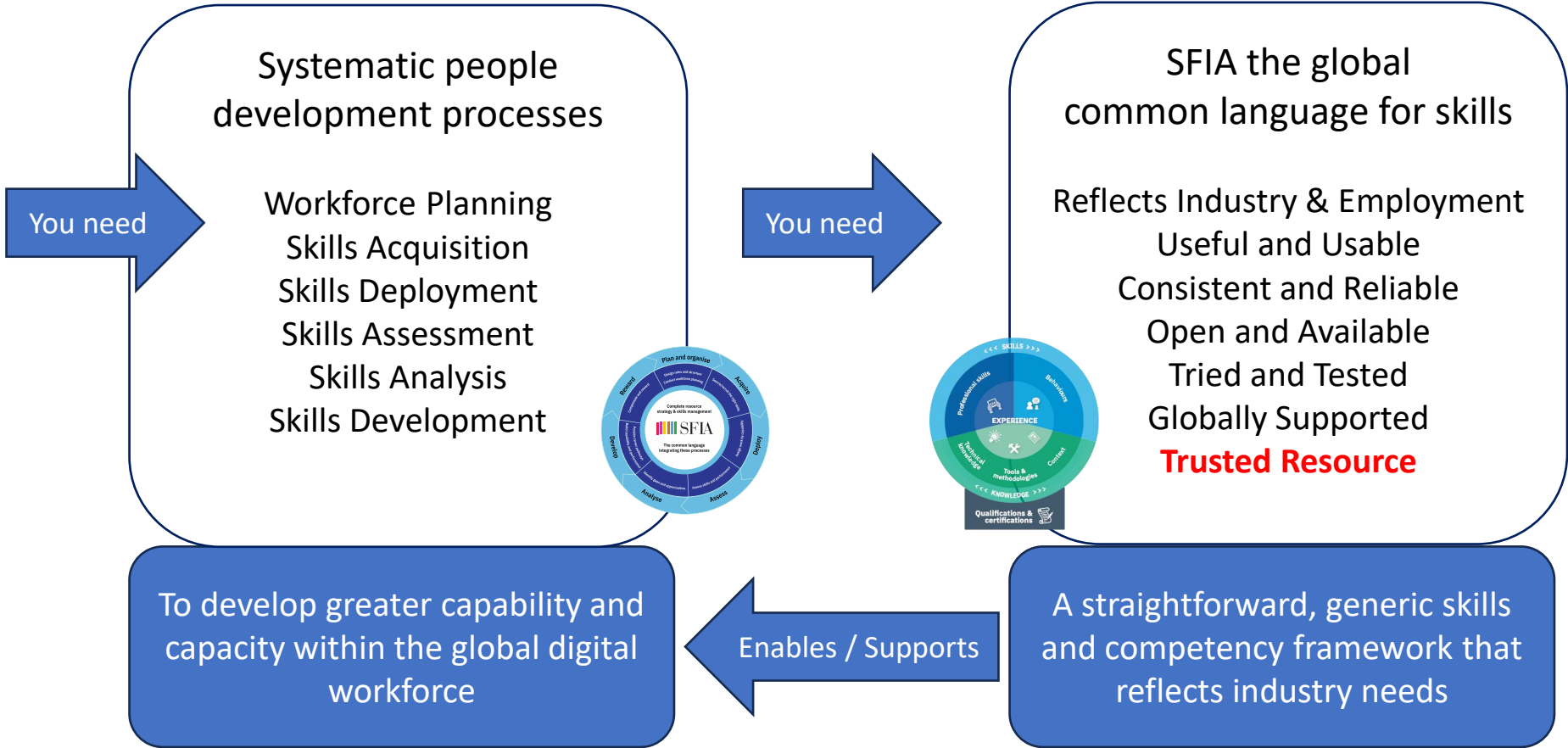
3. Facilitate effective use and consumption of SFIA via an engaged community and supporting ecosystem

4. Ensure sufficient and sustainable funding to deliver the strategic imperatives

SFIA – essential to skills-based workforce development in the digital world

Skills-based recruitment  
 Career paths  
 Talent management  
**Reskilling** Capability  
**Skills first Upskilling**  
**Skills-based organisation**  
 Workforce management  
 Job mobility

What Industry Wants



Generative AI Solutions **Essential for** Consistent & Trusted Resource

## SFIA first created in 2000

- Existing frameworks were not useful to industry and workforce development

## SFIA is refreshed every 3 years

- To remain current and relevant – to ensure that SFIA meets industry needs
- All updates are incremental and come from experience of use by industry

## SFIA changes and input comes directly from industry

- Organisations that are focussed on developing their workforce to meet current or future needs

## Industry finds SFIA useful and usable

- SFIA has been widely adopted internationally
- SFIA covers a broad range of professional practices – across professional activities

## Engaged global community

- An enthusiasm to share and develop more and more support assets

## SFIA's track-record: usable, consistent and reliable


- People know SFIA is kept updated and available so know they can use it with confidence

# SFIA views – updates or in progress

- The conventional view of SFIA used for the summary chart and framework reference guide
- Categories & sub-categories

**SFIA 9**


Full framework



- A framework for Agile
- Specific guidance for use of SFIA skills within an Agile environment

**SFIA 9**

Agile



- A framework for DevOps
- Specific guidance for use of SFIA skills within a DevOps environment

**SFIA 9**


DevOps



- A framework for Data/Data Science
- Specific guidance for use of SFIA skills within a data and data science environment

**SFIA 9**


Big data/Data science



- A framework for Enterprise IT
- Specific guidance for use of SFIA skills within an enterprise IT environment

**SFIA 9**

Enterprise IT



- A framework for Digital transformation
- Specific guidance for use of SFIA skills within a digital transformation environment

**SFIA 9**

Digital transformation




- A framework for Digital Health Roles
- Specific guidance for use of SFIA skills within a digital health environment
- Illustrative Digital Health Role Profiles

**SFIA 9 In Dev**

Digital Health

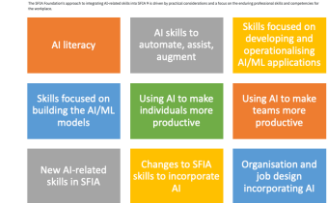
- [A framework for cloud computing skills](#)



**SFIA 8 to 9 In Progress**

Cloud Computing

- A framework for AI skills (BETA)



**SFIA 9 In Dev**

AI - Beta In Development

- [A framework for cyber security skills](#)



**SFIA 9**

Cyber security InfoSec



# The RAF Cyberspace Journey with SFIA

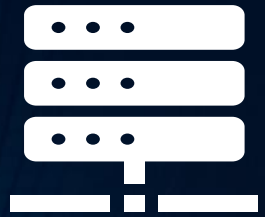
FLT LT AMY PHILLIPS-MAHON & FLT SGT DEBRA ROBERTS



# Scope

- Introduction and problem overview
- The desired end point
- The plan: strategy and approach
- How we implemented the plan
- Recommendations
- Benefits and early results
- Q&A

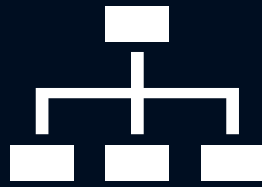
# Introduction to RAF Cyberspace



Build



Secure



Manage



Develop



Exploit





PROBLEM  
OVERVIEW:

THE RAF'S URGENT  
NEED FOR  
MODERNISATION:

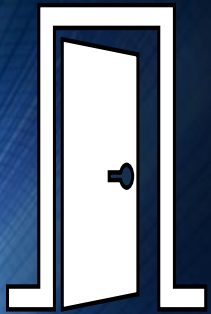
The digital skills crisis



# TRANSFORMING AT SCALE:

## REIMAGINING RAF CAREERS THROUGH SFIA

- 121 distinct conditions.
- 3000 People and Job roles located across 4 Continents.
- Multiple Governmental and External Stakeholders.
- 9 Months to deliver!



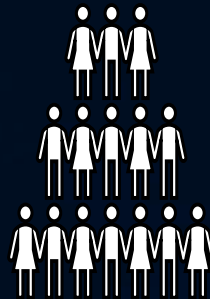
Recruit



Select



Train



Sustain



Retain



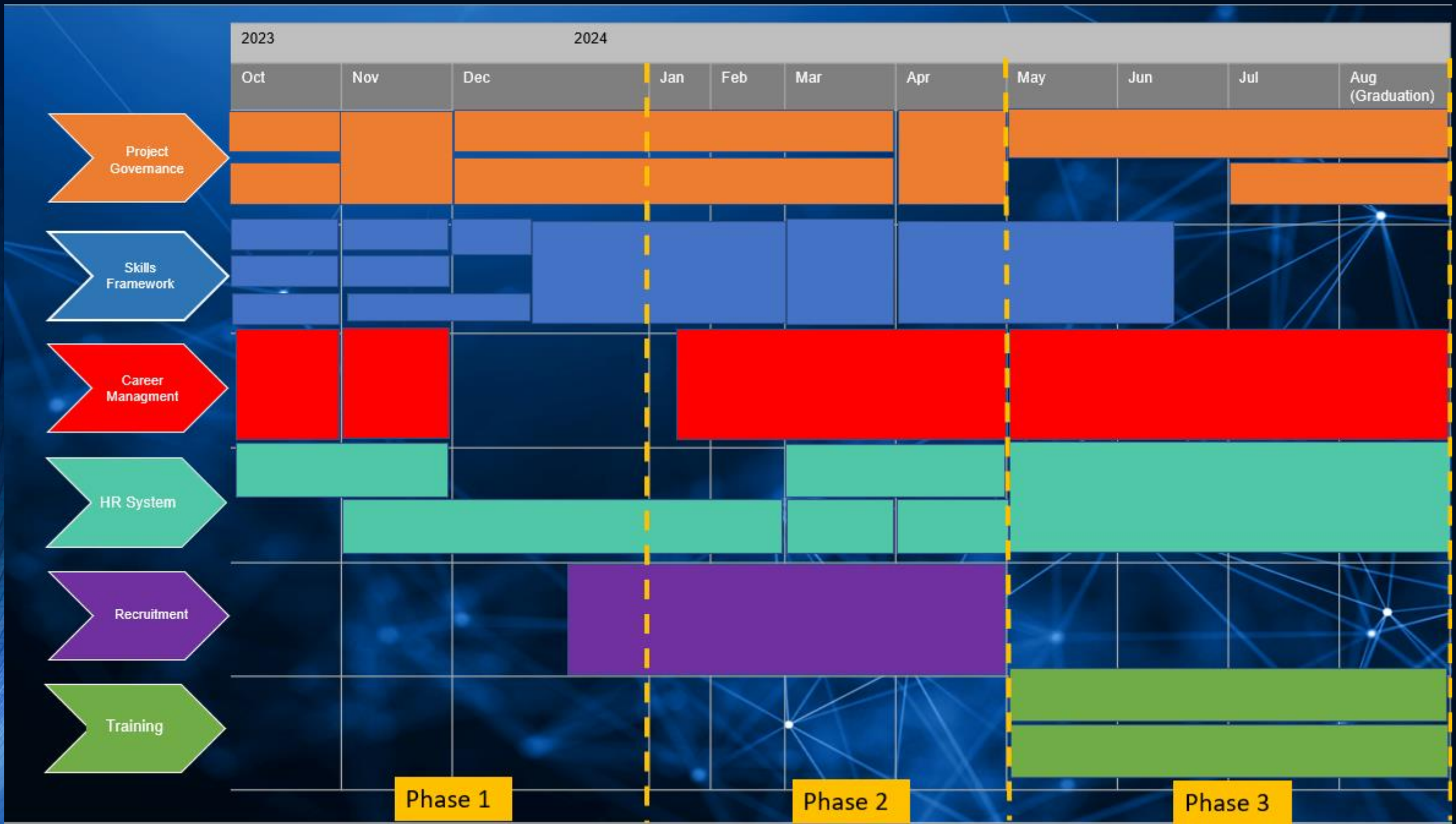
Resettle

Why SFIA?









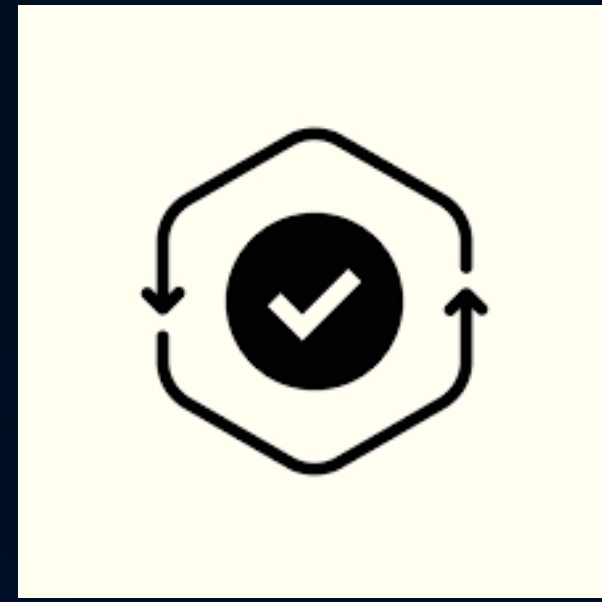
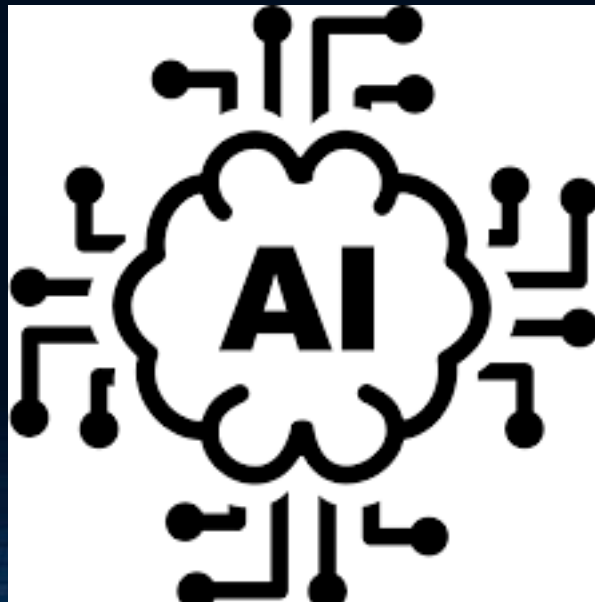
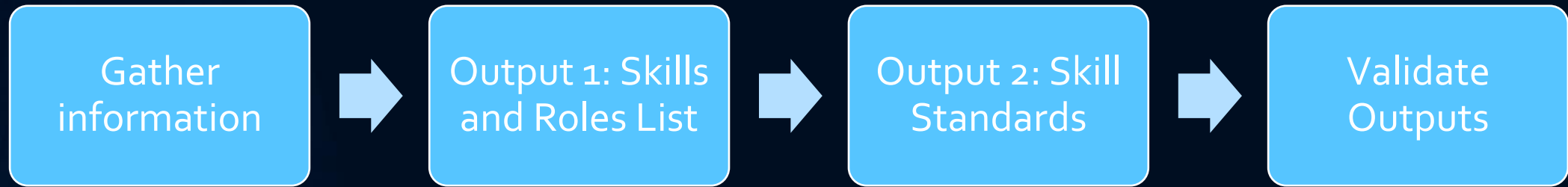
Phase 1

Phase 2

Phase 3



# Phase 1 overview










Application Support professionals are responsible for maintaining and supporting the software applications used by an organisation. This includes a wide range of tasks, such as:

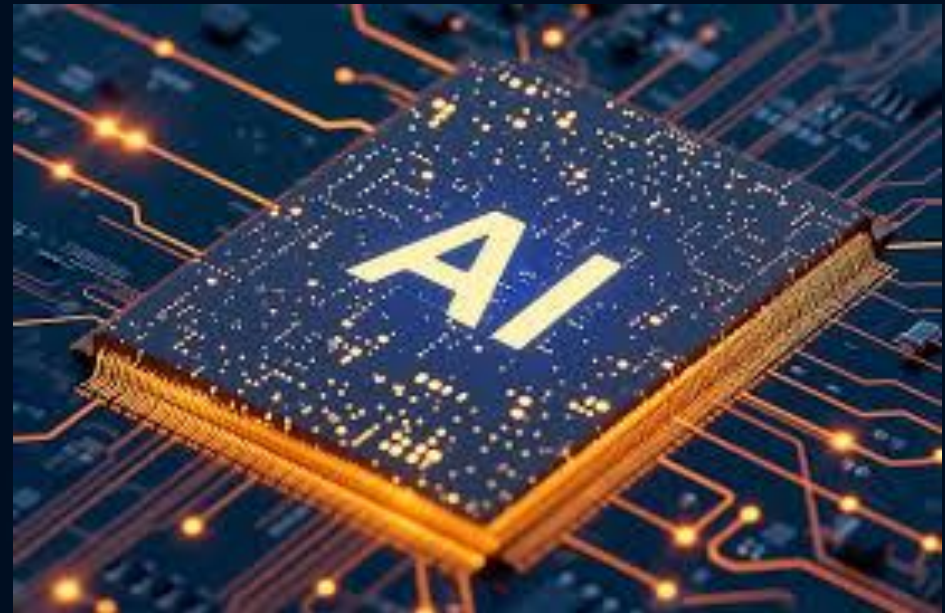
- Investigating and resolving issues reported by users
- Monitoring application performance and identifying potential problems
- Providing advice and training to users on how to use the applications effectively
- Devising and implementing corrections for faults
- Making general or site-specific modifications to applications
- Updating documentation
- Manipulating data
- Defining enhancements to applications
- Development of Applications (Such as Power Apps)

Application Support professionals often work closely with the developers of the applications they support, as well as with colleagues in other IT disciplines, such as database administration and network support.

Skill Name	Description	Link to Associated Framework
Digital Incident Management (USUP)	Coordinating responses to incident reports, minimising negative impacts and restoring service as quickly as possible.	Digital Incident Management (sfia-online.org) 
Digital Information Assurance (INAS)	Protecting against and managing risks related to the use, storage and transmission of data and information systems.	Digital Information Assurance (sfia-online.org) 
Configuration Management (CFMG)	Planning, identifying, controlling, accounting for and auditing of configuration items (CIs) and their interrelationships.	Configuration management (sfia-online.org) 
Service Level Management (SLMO)	Agreeing targets for service levels and assessing, monitoring, and managing the delivery of services against the targets.	Service level management (sfia-online.org) 
Customer Service Support (CSMG)	Managing and operating customer service or service desk functions.	Customer service support (sfia-online.org) 
Application Support (ASUP)	Delivering management, technical and administrative services to support and maintain live applications.	Application support (sfia-online.org) 
Programming/Software Development (PROG)	Developing software components to deliver value to stakeholders.	Programming/software development (sfia-online.org) 
Digital Information Security (SCTY)	Defining and operating a framework of security controls and security management strategies.	Digital Information Security (sfia-online.org) 
Database Administration (DBAD)	Installing, configuring, monitoring, maintaining and improving the performance of databases and data stores.	Database administration (sfia-online.org) 

# Use of AI – benefits and lessons learnt

- Reduced the number of full time employees required
- Reduced time taken to author a skill
- Human validation critical
- Seed data quality is essential
- Creating an auditable trail is key



# Making SFIA useable for the RAF – Proficiency levels and KSEB

<b>SFIA</b>	Follow	Assist	Apply	Enable	Ensure/ Advise	Initiate/ Influence	Set Strategy
<b>CYBERSPACE</b>	Awareness		Practitioner		Senior Practitioner	Expert	





**Description:** Defining and operating a framework of security controls and security management strategies. (SCTY)

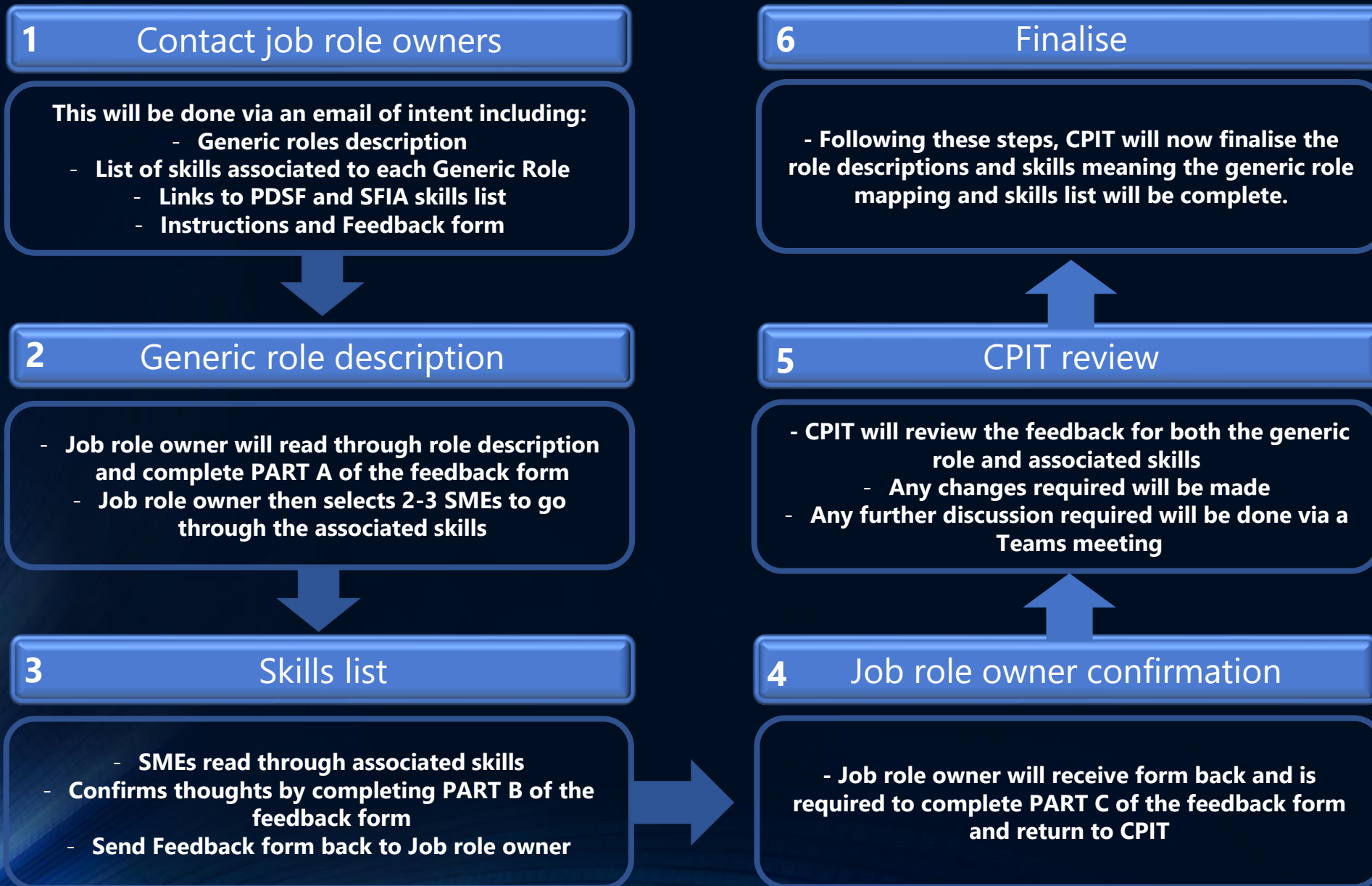
Awareness	Practitioner	Senior Practitioner	Expert
<p><b>Knowledge:</b></p> <ul style="list-style-type: none"> <li>Basic security controls and IAW regulatory standards (e.g. JSP440, JSP441).</li> <li>Known vulnerabilities and associated risks.</li> <li>Initial incident response and IAW policy.</li> </ul> <p><b>Skill Application:</b></p> <ul style="list-style-type: none"> <li>Applies and maintains specific security controls as required by organisational policy and local risk assessments.</li> <li>Communicates security risks and issues to business managers and others. Performs basic risk assessments for small information systems.</li> <li>Contributes to the identification of risks that arise from potential technical solution architectures. Suggests alternate solutions or countermeasures to mitigate risks.</li> <li>Defines secure systems configurations in compliance with intended architectures.</li> <li>Supports investigation of suspected attacks and security breaches.</li> </ul> <p><b>Experience:</b></p> <ul style="list-style-type: none"> <li>Minimal real-world experience of undertaking routine Information Security tasks with supervision.</li> </ul> <p><b>Behaviour:</b></p> <ul style="list-style-type: none"> <li>Shows willingness to learn and develop in the area of Information Security.</li> </ul>	<p><b>Knowledge:</b></p> <ul style="list-style-type: none"> <li>Security controls and management strategies in the context of confidentiality, integrity, availability, and accountability of information systems.</li> <li>Data Protection principles (GDPR Article 5) and Data Protection Impact Assessment (DPIA) process.</li> <li>Security control frameworks such as Secure by Design.</li> </ul> <p><b>Skill Application:</b></p> <ul style="list-style-type: none"> <li>Provides guidance on the application and operation of elementary physical, procedural and technical security controls.</li> <li>Explains the purpose of security controls and performs security risk and business impact analysis for medium complexity information systems.</li> <li>Identifies risks that arise from potential technical solution architectures. Designs alternate solutions or countermeasures and ensures they mitigate identified risks.</li> <li>Investigates suspected attacks and supports security incident management.</li> </ul> <p><b>Experience:</b></p> <ul style="list-style-type: none"> <li>Real-world experience on a variety of tasks worked as part of a team on Information Security tasks.</li> </ul> <p><b>Behaviour:</b></p> <ul style="list-style-type: none"> <li>Supports and develops junior operators through guidance and mentorship.</li> </ul>	<p><b>Knowledge:</b></p> <ul style="list-style-type: none"> <li>Organisational strategies that address information control requirements.</li> <li>How to identify, assess and monitor operational threats, their impact on business and associated risks.</li> <li>Design principles to mitigate security threats (e.g. ISO 27001, NIST).</li> </ul> <p><b>Skill Application:</b></p> <ul style="list-style-type: none"> <li>Provides advice and guidance on security strategies to manage identified risks and ensure adoption and adherence to standards.</li> <li>Contributes to development of information security policy, standards and guidelines.</li> <li>Obtains and acts on vulnerability information and conducts security risk assessments, business impact analysis and accreditation on complex information systems. Investigates major breaches of security and recommends appropriate control improvements.</li> <li>Develops new architectures that mitigate the risks posed by new technologies and business practices.</li> </ul> <p><b>Experience:</b></p> <ul style="list-style-type: none"> <li>Real world operational experience undertaking a wide variety of complex tasks both independently and through leading a team.</li> </ul> <p><b>Behaviour:</b></p> <ul style="list-style-type: none"> <li>Thinks creatively to overcome complex challenges or problems.</li> <li>Supports and develops practicing operators through guidance and mentorship.</li> </ul>	<p><b>Knowledge:</b></p> <ul style="list-style-type: none"> <li>Procedures to develop, implement, deliver, and support enterprise-wide data protection and information security strategies.</li> <li>Methods to ensure compliance between business strategies and data protection and information security.</li> <li>Security controls that can be used to mitigate threats within solutions and services.</li> <li>Solutions with embedded security controls specifically engineered for mitigating data protection and information security threats.</li> </ul> <p><b>Skill Application:</b></p> <ul style="list-style-type: none"> <li>Develops and communicates corporate information security policy, standards and guidelines.</li> <li>Ensures architectural principles are applied during design to reduce risk. Drives adoption and adherence to policy, standards and guidelines.</li> <li>Contributes to the development of organisational strategies that address information control requirements. Identifies and monitors environmental and market trends and proactively assesses impact on business strategies, benefits and risks.</li> <li>Leads the provision of authoritative advice and guidance on the requirements for security controls in collaboration with subject matter experts.</li> </ul> <p><b>Experience:</b></p> <ul style="list-style-type: none"> <li>Real-world experience of leading and directing complex activities and providing wider domain support.</li> </ul> <p><b>Behaviour:</b></p> <ul style="list-style-type: none"> <li>Supports and develops future senior practitioners through guidance and mentorship, with focus on future leadership.</li> </ul>
<b>Corresponding competency framework</b>			
SFIA 8 Framework - Information Security – Level 3	SFIA 8 Framework - Information Security – Level 4	SFIA 8 Framework - Information Security – Level 5	SFIA 8 Framework - Information Security – Level 6
<b>Courses, licenses, qualifications</b>			



# Phase 2 – Jan 24 – Mar 24

- Foster relationships with key stakeholders
- Begin generic role verification and skill authoring in earnest
- Complete supporting work (e.g. internal policy updates, recruitment material etc)
- Continue comms (bi-weekly drop-in clinics, all ranks dial ins, unit visits)

# Generic Role Verification



## Job Role Owner Generic Role Instructions and Feedback

### 1. APPLICABILITY

- a. This feedback form is applicable to Cyberspace job role owners.

### 2. AIM

- a. This feedback form is to ensure the involvement of job role owners within a certain area within cyberspace giving them situational awareness as well as their welcomed opinion on the profession work completed by CPIT. We need the role owners to revalidate and or scrutinise the definition of the generic role and associated skills outline below to ensure the job role is still correct and any changes to the role are accounted for.

### 3. TASKS AND RESPONISBILITES

#### JOB ROLE OWNER

The job role owners' task is to confirm and or scrutinise the descriptions of the job roles as defined by CPIT.

1. Read through the generic role description and list of associated skills.
2. Carefully answer the questions outlined within **Part A** of this feedback form. In the event there is anything within the description that you disagree with, please add as much explanation as you can into the boxes provided.
3. Please complete the details outlined in **Part B** of this feedback form and return to CPIT

**From:**  
**To:**  
**Subject:**

Good morning/afternoon (insert who)

As the job role owner of (enter job role name) the Cyberspace Professions Implementation Team (CPIT) requires you to confirm and or scrutinise the description of the generic role: (enter generic role) as part of the revalidation process to ensure the information is still a true reflection of the role. The generic role sets the foundation for associated specialist roles. A Job Specification draws on the generic role profile providing the next level of detail to articulate the requirement for a specific job at a given unit. Once reviewed, please complete Part A of the attached feedback form

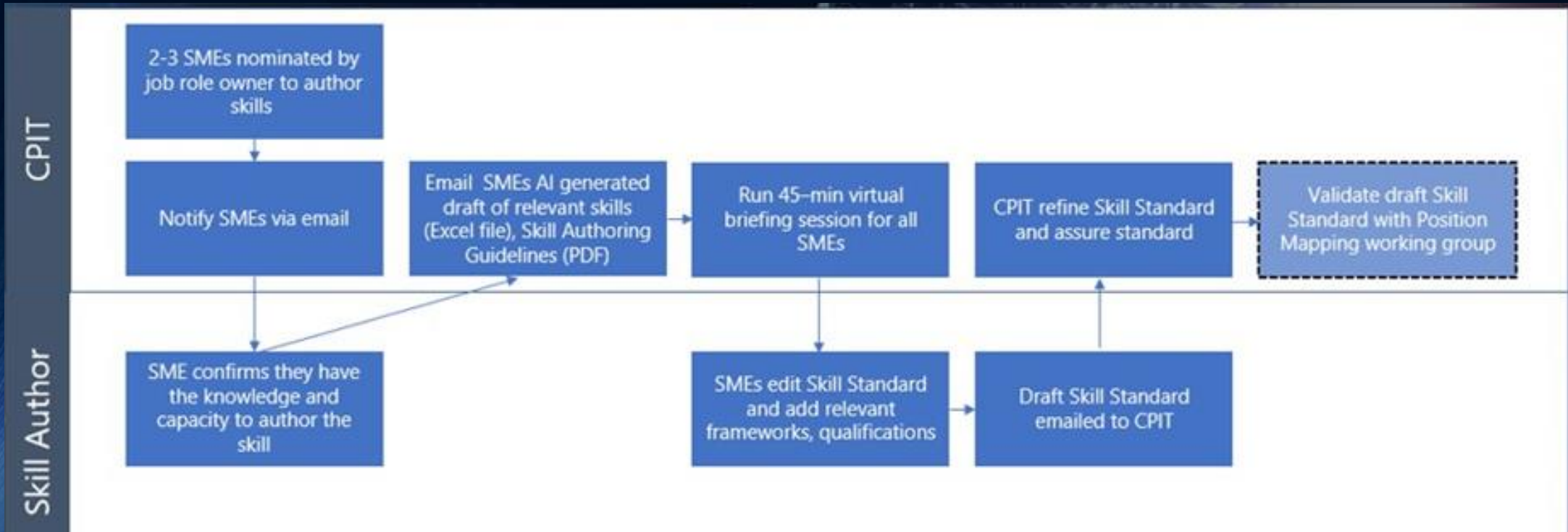
Once you have reviewed the description of the generic role and the skills associated with it complete Part A of the feedback form. After you have completed Part A please fill in your details on Part B in case a more in depth review of the role is required as a result of your feedback.

Once the form has been completed please attach the document and submit your response to the email address referenced in paragraph 3c.

We thank you in advance for you cooperation,

Kind regards,

# Skill Authoring





## 26 Generic Roles

1. Application Support
2. Change & Transformation
3. Cloud Services
4. Cryptography
5. Cyber Protection
6. Cyber Incident Response
7. Cyberspace Training & Support
8. Data & Analytics
9. Governance, Risk & Assurance
10. Infra Provision & Assurance
11. Information Service Management
12. Information Service Operations
13. Network Delivery & Operations
14. Network Security
15. Radar & Radio Management
16. Satellite & Radio
17. Software Development
18. Solutions Architect
19. Strategy & Planning
20. User Interface & User Experience



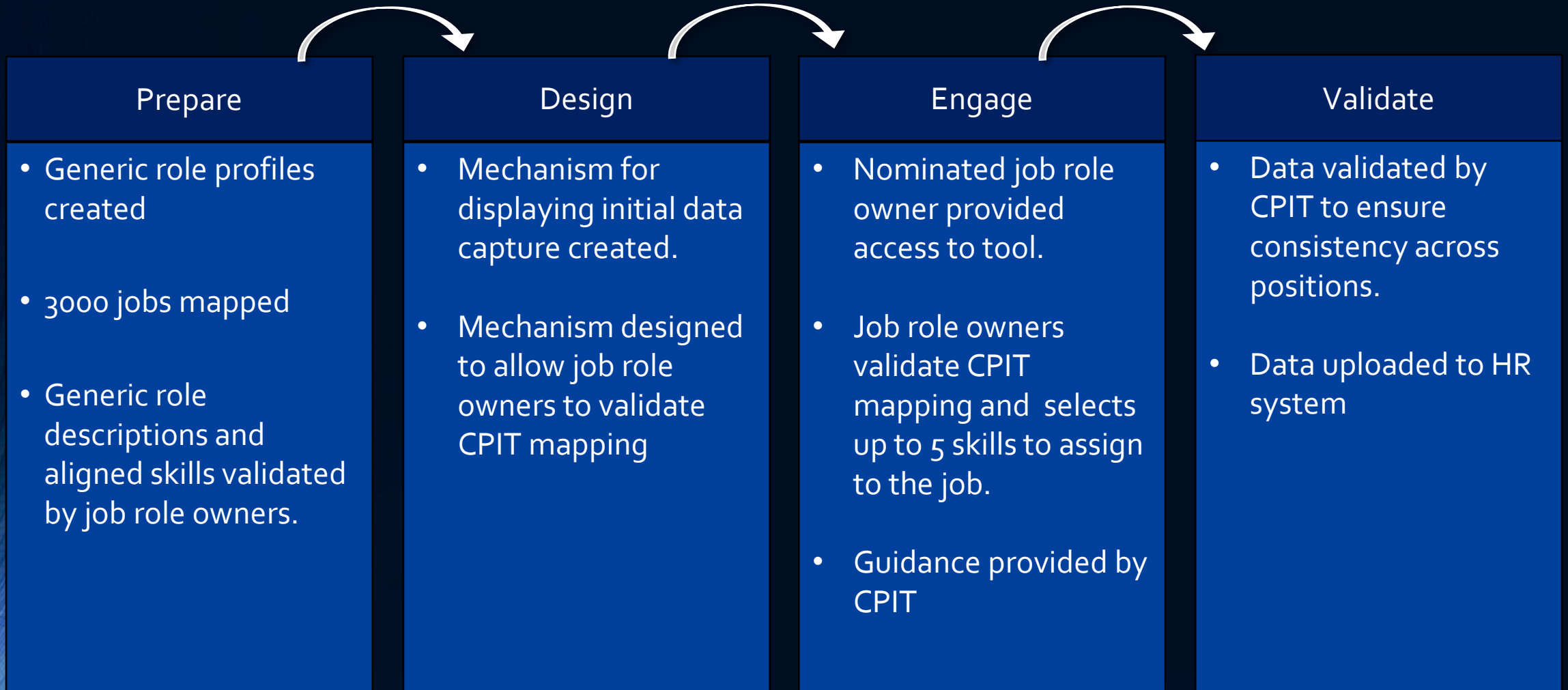
## 65 Skills

1. Application Support
2. Audit
3. Availability Management
4. Business Modelling
5. Business Situation Analysis
6. Competency Assessment
7. Configuration Management
8. Content Authoring
9. Customer Service Support
10. Data Engineering
11. Data Management
12. Data Modelling and Design
13. Data Science
14. Data Visualisation
15. Database Administration
16. Digital Demand Management
17. Digital Forensics
18. Enterprise and Business Architecture
19. Digital Governance
20. Digital Incident Management
21. Information Assurance
22. Information Security
23. IT Infrastructure
24. Learning Delivery
25. Learning Design and Development
26. Machine Learning
27. Network Design
28. Network Security
29. Network Support
30. Organisation Facilitation
31. Penetration Testing
32. Performance Management
33. Technology Problem Management
34. Professional Development
35. Programming and Software Development
36. Project Management
37. Quality Assurance
38. Quality Management
39. Radar System Management
40. Radio Frequency Engineering
41. Requirements Definition & Management
42. Risk Management
43. Satellite Communication Systems Operation
44. Communication Security
45. Service Acceptance
46. Service Level Management
47. Software Configuration
48. Software Design
49. Solution Architecture
50. Strategic Planning
51. Subject Formation
52. Supplier Management
53. Systems and Software Lifecycle Engineering
54. Digital Systems Design
55. Digital Systems Development
56. Teaching
57. Technology Testing
58. Digital Threat Intelligence
59. User Experience Analysis
60. User Experience Design
61. User Experience Evaluation
62. User Research
63. Vulnerability Assessment
64. Workforce Planning
65. Working at Height

# Phase 3 – Apr 24 – Aug 24

- Job roles mapped to framework
- Training mapped to framework
- Mapping individuals to the framework
- Skill framework document and quality system creation
- Creation of defined career pathways based on skills

# Process Overview – Position Mapping



# Mapping individuals to the framework

## Skills Application Form

To apply, please complete and submit this form along with any supporting evidence to your Line Manager.

Rank		Service number	
First name		Surname	
JPAN			
Line Manger Details			
Rank		Service Number	
First name		Surname	
MOD Email			

## Skill applying for

The [Cyberspace Skills Framework](#) provides detailed information on each Skill.

Skill Name			
Current Skill proficiency level			
Awareness	Practitioner	Senior Practitioner	Expert
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requested Skill proficiency Level			
Awareness	Practitioner	Senior Practitioner	Expert
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## Supporting Evidence

Use the following sections to provide written evidence of how you have demonstrated the skill you are applying for, at the appropriate proficiency level.

The Cyberspace Skills Framework provides information on the different proficiency levels and K.S.E.B.

Situation
Task
Action
Result

## Any other supporting evidence

*Eg. Provide details of any course attended and attach certificates that support your application.*

## Declaration by Applicant-

I confirm that all details are correct and true

Forward application to Line Manager

## Line Manager Verification

I agree with the evidence in this application

Yes

No

Completed form to be emailed to Cyberspace Skills Framework Managers



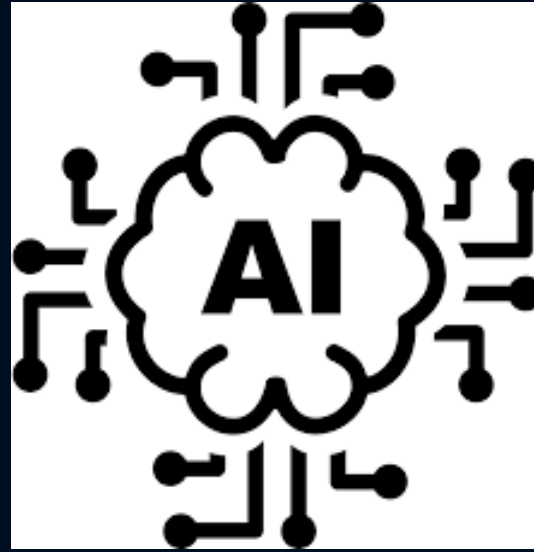
# Recommendations

The background features a dark blue gradient on the left, transitioning into a complex, glowing blue structure on the right. This structure consists of numerous thin, parallel lines that curve and spiral inward, creating a sense of depth and movement, similar to a tunnel or a data stream visualization. The lines are more densely packed and brighter in the center-right area, fading towards the edges.



**JUST GET ON WITH  
IT**

**LOOK TO EXPEDITE BUT NOT  
AT THE EXPENSE OF SME  
ENGAGEMENT**



# COMMUNICATIONS:

MAKING PEOPLE PART OF THE CHANGE





# CREATING A DIGITAL SKILLS FRAMEWORK

Flight Lieutenant Amy Phillips-Mahon CEng MIET MBCS of the Cyberspace Professions Implementation Team, RAF Digital, explains how organisational transformation in line with SFIA is helping the RAF face its challenges against the backdrop of a rapidly evolving digital landscape.

Maintaining a highly skilled workforce in today's fast-paced digital world is more challenging than ever before. With technology evolving at an unprecedented pace, traditional methods of preparing for future trends quickly become outdated. Professionals need to ensure they continue to possess the skills that will ensure continuous employability, while organisations need to create an environment that is successful in recruiting and retaining top talent. This has prompted the Royal Air Force (RAF) to undertake a significant organisational transformation program.

The organisational structure of the RAF has not changed substantially for the last 70 years. Currently, officers are employed within a branch which represents a specific area of expertise—for example logistics or engineering. Enlisted aviators are employed within trade groups and these encompass sub-trades representing a distinct occupation; for example, Trade Group 4 is responsible for telecommunications and information systems. This is subdivided into two sub-trades of information communication and technology technicians, and communication infrastructure technicians. Enlisted aviators must currently remain within the trade they joined. This lack of workforce flexibility is limiting from a career development perspective.

### A NEW APPROACH TO RAF CAREER MANAGEMENT

Programme professions will transition the RAF from a structure of 80 branches and trades to 11 distinct professions, each being supported by a comprehensive skills framework. This will facilitate a new approach to career management within the armed forces. For the cyberspace profession, this transformation programme

Primarily the Skills Framework for the Information Age (SFIA) was used as the backbone, but was also supported by several other frameworks such as the Digital and Data Profession Capability Framework and the Mast and Tower Safety Framework, to capture the broad range of skills within the profession.

### THE RAF CYBERSPACE PROFESSION: SCOPE AND AMBITION

The RAF cyberspace profession is dedicated to building, operating, managing and defending critical digital and technological capabilities and infrastructure. The profession encompasses a wide range of responsibilities, including radar maintenance, coding, network infrastructure and cybersecurity. Given the profession's diverse nature, developing a skills framework to cover the breadth of these activities was a monumental task.

To tackle this, the Cyberspace Profession Implementation Team (CPIT) was established in October 2023. The team was tasked with creating and implementing a skills framework for the cyberspace profession and set a compressed timeline of nine months to meet the ambitious targets set by the overarching professions programme. Aligning to SFIA and other industry frameworks was crucial for meeting such a strict timeframe, as the team were able to leverage a globally recognised model for describing skills, significantly expediting the project by accelerating the skill authoring process.

### A NOVEL APPROACH TO FRAMEWORK DEVELOPMENT

The initial step in creating the framework involved defining all roles within the cyberspace profession through the

# COLLABORATION: BUILDING RELATIONSHIPS ACROSS THE UK IT SECTOR



The Cyberspace Profession Conference 2024



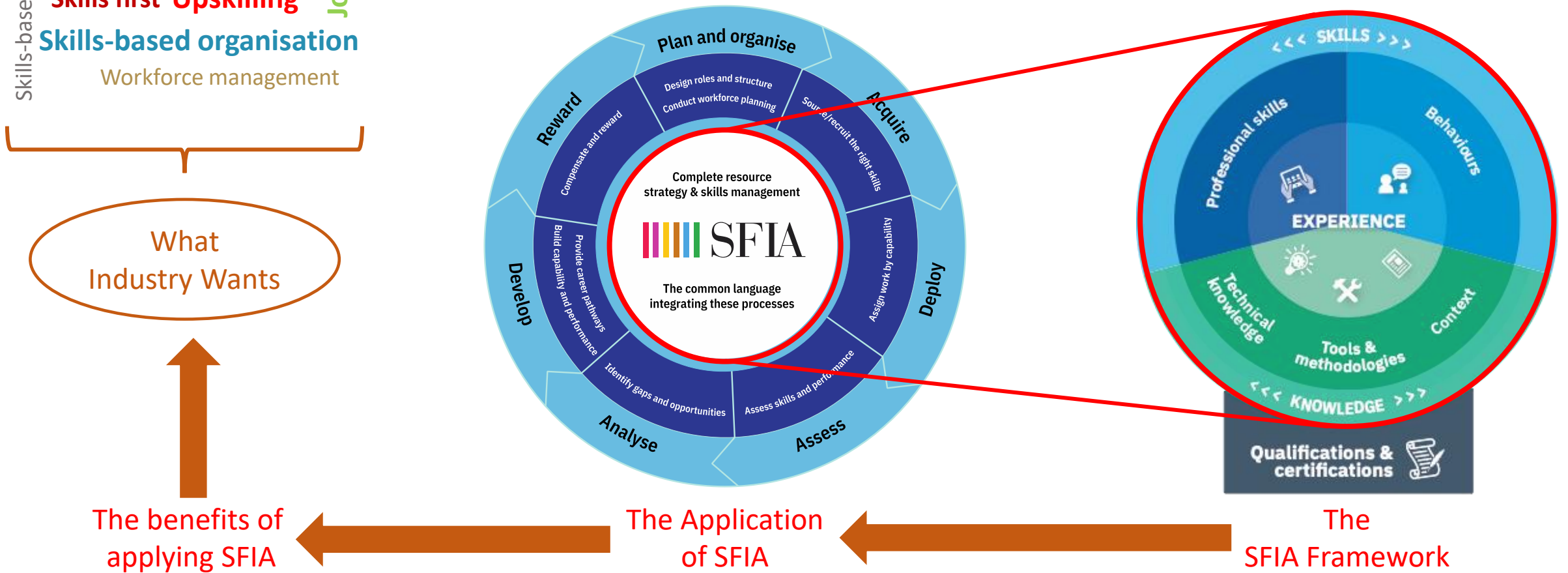
# Benefits of the Approach

- **Professionalisation:** SFIA backbone creates pathways to professional registration, simplifies CPD, and fosters a motivated, professional workforce.
- **Talent Management:** Objective skill measurement for clear talent distribution to facilitate skill-based career management in the RAF.
- **Transferable Skills:** Formal skill progression recording enhances employability and serves as a recruitment tool for Cyberspace careers.
- **Sector Alignment:** Use of SFIA ensures alignment across Defence, Government, and wider sector.
- **Lateral Entry:** Facilitates clear skill articulation for lateral moves within RAF and civilian sectors, provides bespoke training pathways, and enhances recruitment and employment of Reserve forces.



# Q&A







*SFIA defines the skills and competencies required by professionals who design, develop, implement, manage and protect the data and technology that power the digital world.*

## Contact the SFIA Foundation directly:

- For and questions or queries you may have about SFIA
- Tell us your story, tell us about how you use SFIA
- Tell us about the issues you face in developing skills and competencies
- Tell us what you would like to see in the future

Remember to register on the SFIA Website ... and talk to us about your use of SFIA

Complete the short form to tell us what you want to see:

Peter Leather  
[updates@sfia-online.org](mailto:updates@sfia-online.org)  
[LinkedIn](#)

Ian Seward  
[ops@sfia-online.org](mailto:ops@sfia-online.org)  
[LinkedIn](#)