

BCS Learning & Development SG



WE ARE
RECORDING



PUT QUESTIONS
INTO CHAT



WE WILL BE
STARTING AT 7PM



WELCOME

**IT SKILLS FRAMEWORKS
HOW DO THEY ALL FIT TOGETHER?
JUL 2022**

BCS Learning & Development Specialist Group

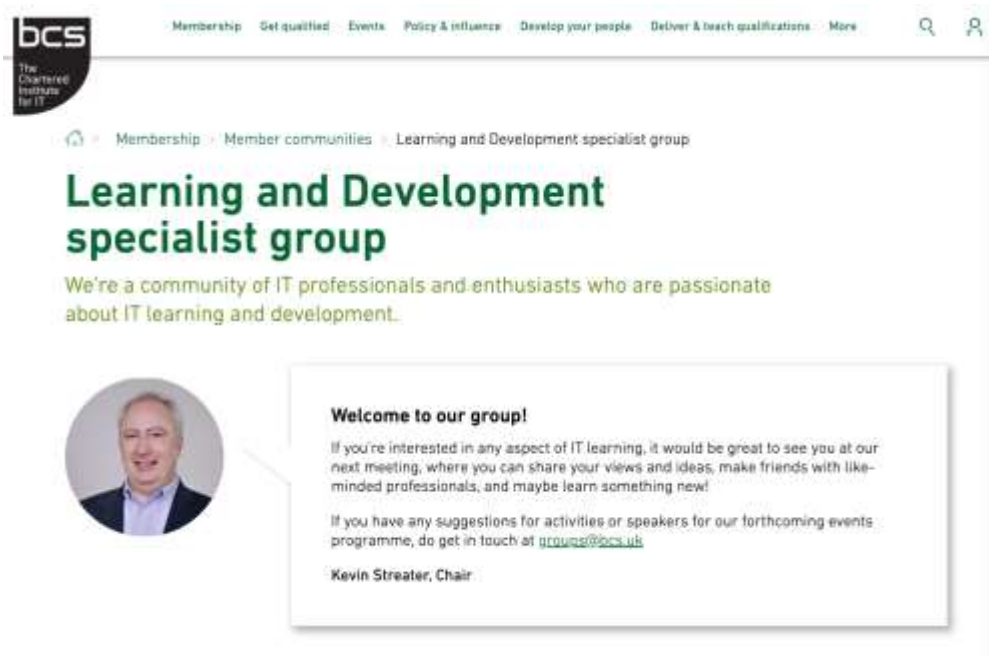
“The BCS Learning & Development Specialist Group is for those involved in the development, delivery or management of learning to IT and communications professionals and users.”

BCS L&D SG Member Specialisms

Members are specialists in:

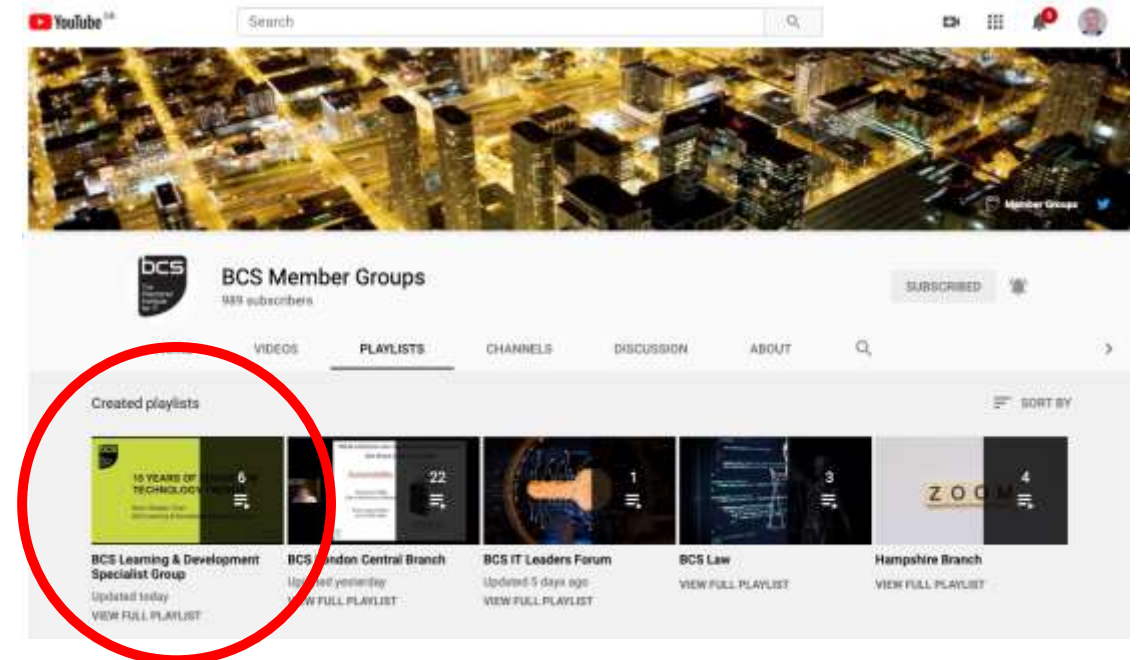
- **IT End User Skills Training (18%)**
- **IT Professional Skills Training (18%)**
- **IT Technical Skills Training (16%)**
- **University/Education Sector (16%)**
- **General Interest in IT Skills Topics (32%)**

Learning and Development Specialist Group



The screenshot shows the BCS website's 'Learning and Development specialist group' page. At the top left is the BCS logo. The navigation bar includes links for Membership, Get qualified, Events, Policy & influence, Develop your people, Deliver & teach qualifications, and More. Below the navigation, the breadcrumb trail reads: Membership > Member communities > Learning and Development specialist group. The main heading is 'Learning and Development specialist group' in green. Below it is a sub-heading: 'We're a community of IT professionals and enthusiasts who are passionate about IT learning and development.' A circular profile picture of Kevin Streater is on the left. To its right is a white box with the text: 'Welcome to our group! If you're interested in any aspect of IT learning, it would be great to see you at our next meeting, where you can share your views and ideas, make friends with like-minded professionals, and maybe learn something new! If you have any suggestions for activities or speakers for our forthcoming events programme, do get in touch at groups@bcs.uk Kevin Streater, Chair

<https://www.bcs.org/membership/member-communities/learning-and-development-specialist-group/>



The screenshot shows the YouTube channel page for 'BCS Member Groups'. The channel has 989 subscribers and is marked as 'SUBSCRIBED'. The page is set to the 'PLAYLISTS' tab. A red circle highlights the 'Created playlists' section, which lists five playlists: 'BCS Learning & Development Specialist Group' (6 videos, updated today), 'BCS London Central Branch' (22 videos, updated yesterday), 'BCS IT Leaders Forum' (1 video, updated 5 days ago), 'BCS Law' (3 videos), and 'Hampshire Branch' (4 videos). Each playlist entry includes a thumbnail image and a 'VIEW FULL PLAYLIST' link.

<https://www.youtube.com/c/BCSMemberGroups/playlists>

Follow us on Social Media



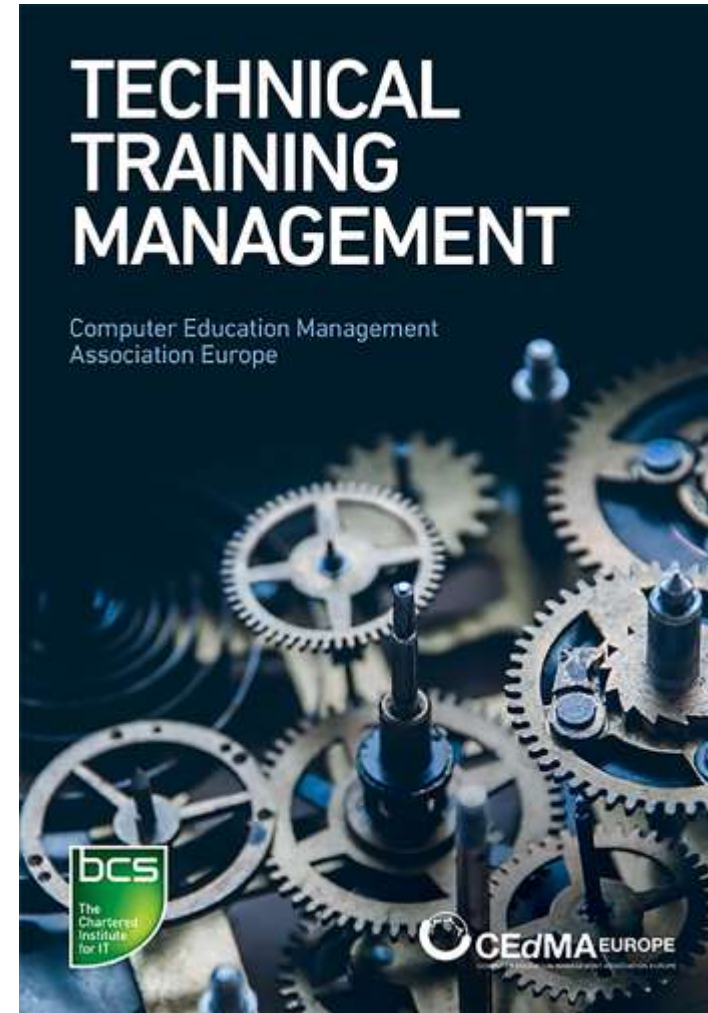
@BCSLandDSG

- We currently have over 600 followers
- Over 4,700 tweets have been posted

Anyone interested in helping to increase our social media and marketing activity is most welcome to join us

Technical Training Management Book

- Launched in April 2019
- Available on BCS Bookshop as hardcopy or ePub



Planned Future Events

Our webinars for 2022 support the 4 BCS priorities:

- **Community;** promoting a diverse membership community of professionals
- **Inspiration;** influencing and improving computer education in all its forms
- **Progression;** providing opportunities for learning and development to bring out the best in people
- **Influence;** campaigning to ensure IT is used to solve the biggest problems of society

Ideas are always welcome

If you have any other ideas
please send to:

Kevin.Streater@bcs.org



TALK: KEVIN STREATER

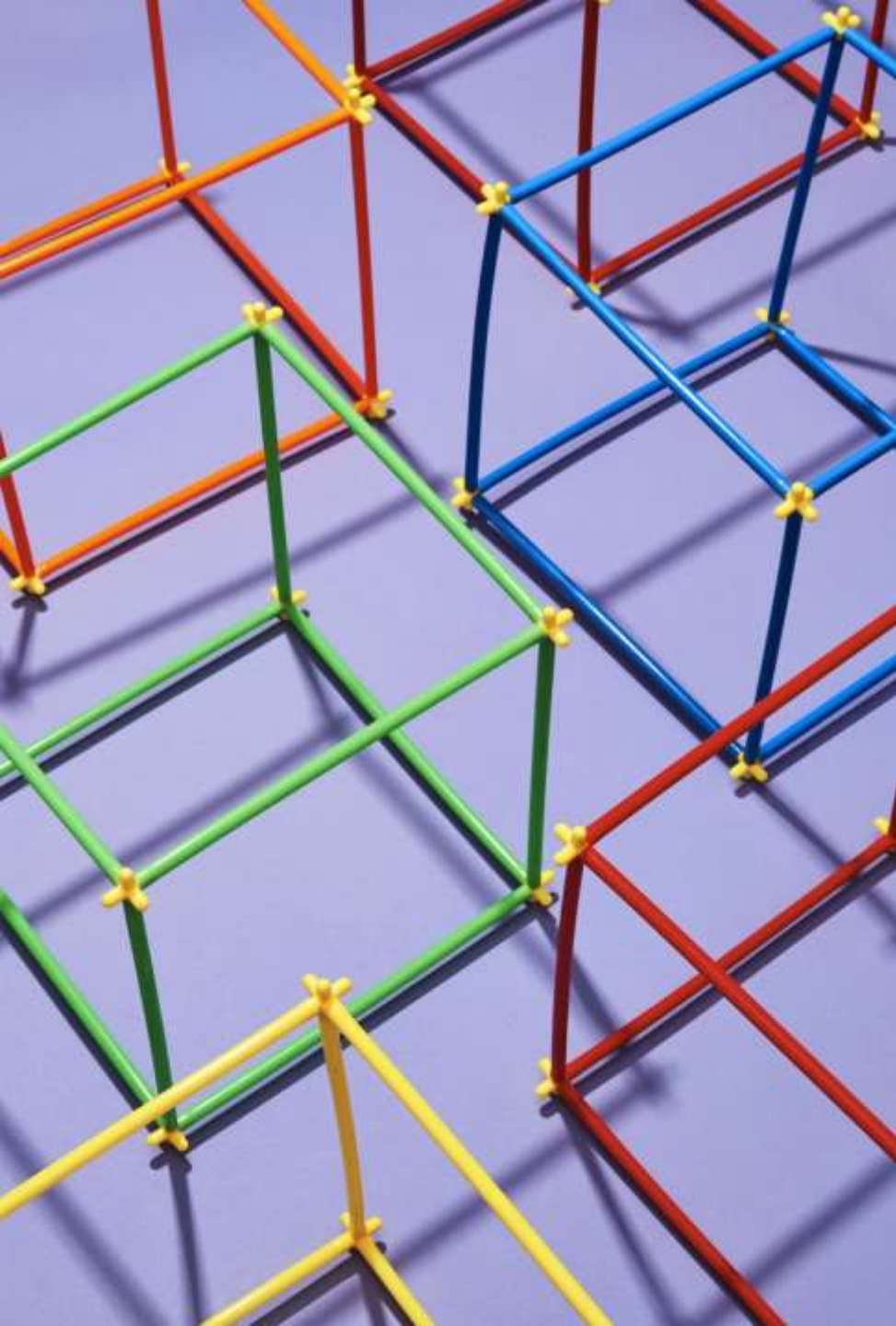


IT Skills Frameworks

How do they all fit together?

- What IT skills frameworks do you know of?





What types of frameworks are there?

- Knowledge frameworks
- Skills frameworks
- Competency frameworks
- Technical skills frameworks



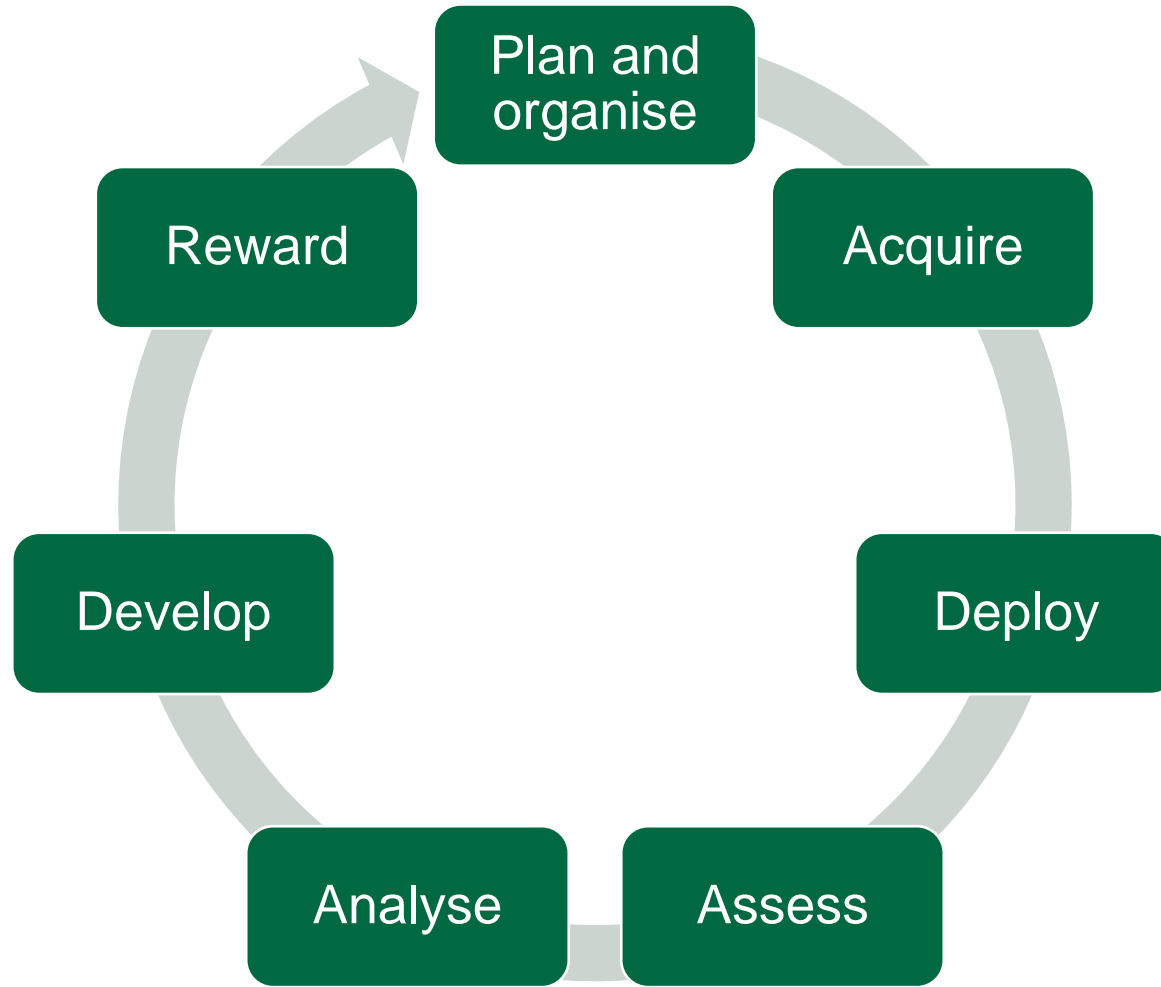
THE SKILLS MANAGEMENT CYCLE

What is skills management about?

Skills Management is about:

- Planning and organising your workforce
- Sourcing and recruiting talent
- Assigning resources by capability
- Assessing skills, performance and capability
- Identifying gaps, skills development needs and opportunities
- Planning and executing development activities to build capability and performance
- Rewarding and compensating individuals for their skills and competencies

The Skills Management Cycle



Use of the Skills Management Cycle

- The use of the skills management cycle improves communication and understanding for all involved e.g. line management, HR and employees.
- By using specialist skills frameworks organisations can achieve a consistent and integrated skills and people management approach.



AN APPROACH TO DEFINING SKILLS

ISO-23773-1 for beginners!

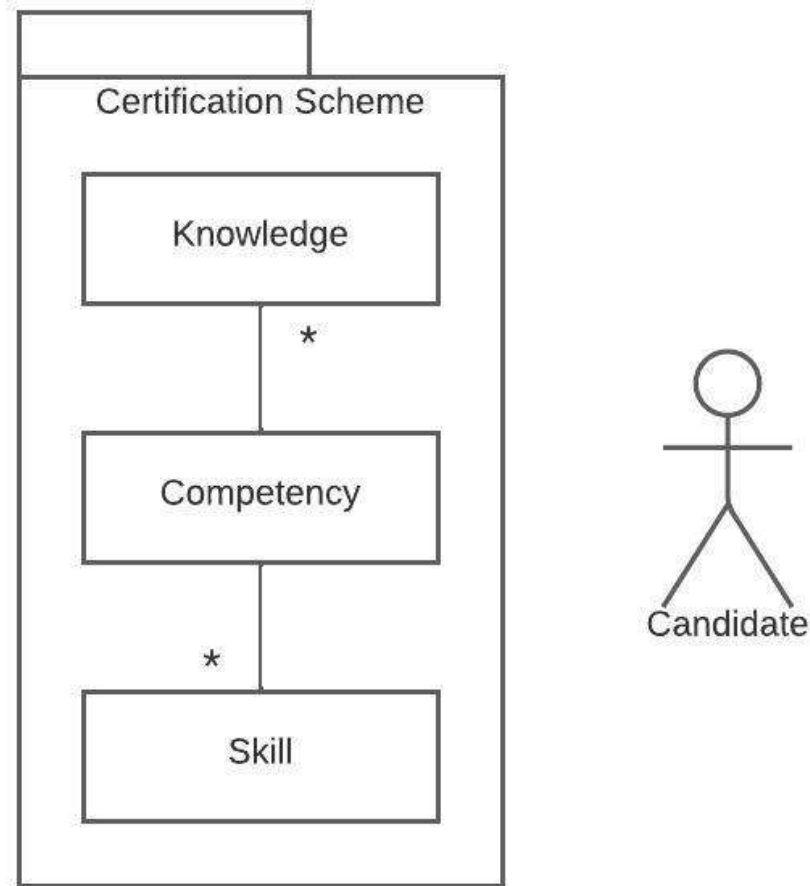
ISO/IEC-24773-01

- ISO/IEC-24773-1:
 - Software and systems engineering – Certification of software and systems engineering professionals
 - Part 1: General requirements
- Part of a broader series of standards to address the certification of professionals in software engineering and systems engineering
- Related to ISO-17024 which is about how to deliver certification schemes

A Model for Skills

- ISO/IEC-24773-1 defines a relationship model for the major concepts relating to technical certification which can help navigate the skills landscape
- Major concepts are:
 - *Knowledge*
 - *Skill*
 - *Competence*

A Model for Skills



For a certification scheme to work, candidates must demonstrate that they have:

- Competency in the domain
- The skills necessary to be able to be competent
- The knowledge that underpins the skills

Source: BS ISO/IEC-24773-1:2019

Knowledge, Skills and Competence

Knowledge

- Items that are generally agreed to be essential to understanding a particular subject at a specific cognitive level

Skills

- A skill is the ability to apply knowledge to perform a simple operation in a controlled environment

Competence

- The ability to apply knowledge and skills in order to achieve a successful result on an ongoing basis



Knowledge, Skills and Performance

Knowledge	Cognitive Level
Knowledge 1	Cognitive level description
Knowledge 2	Cognitive level description
...	



Skill	Knowledge	Performance Level
Skill 1	List of knowledge required to demonstration skill 1	Performance level description
Skill 2	List of knowledge required to demonstration skill 1	Performance level description
...		

Source: BS ISO/IEC-24773-1:2019

Competency and Proficiency

Competency	Knowledge	Skill	Proficiency level
Competency 1	List of knowledge required to demonstrate competency 1	List of skills required to demonstrate competency 1	Proficiency level description
Competency 2	List of knowledge required to demonstrate competency 2	List of skills required to demonstrate competency 2	Proficiency level description
...			



Skill	Knowledge	Performance Level Requirements
Role 1	Competency 1 required to fulfil role 1	Performance level required to fulfil role 1
	Competency 2 required to fulfil role 1	Performance level required to fulfil role 1
	...	

Source: BS ISO/IEC-24773-1:2019

Generic Competence

ISO/IEC 24773-1 includes a list of generic competencies expected of a professional in the environment they are operating in.

These are:

- Ability to communicate effectively
- Ability to identify, formulate and solve problems
- Ability to function effectively as an individual and in a team
- Ability to evaluate the probable social, commercial, cultural, ethical and environmental consequences of an engineering professional's work

Code of ethics and professional practices

ISO/IEC 24773-1 describes that any professional certification scheme shall include a code of ethics and professional practices which should be consistent with:

- An assertion that the certified person shall obey the laws of the community in which they operate;
- A commitment to the principle of individual autonomy, comprising freedom of action in the workplace;
- A commitment to non-discrimination on any basis other than merit;
- A commitment to treat competitors and suppliers respectfully and honestly;
- An intention to exercise care to avoid conflicts of interest as well as the appearance of conflicts of interest;
- An integrity statement, asserting that the certified person shall tell the truth and do what they say they do;
- A commitment that the certified person shall only undertake work they are competent to undertake;
- A commitment that the certified person shall undertake their work conscientiously, striving for efficiency and effectiveness;
- A commitment to build one's professional reputation based on merit;
- A commitment to continuous professional development and currency of competence;
- A commitment to report any failure to meet the standards established by the Scheme;
- A commitment to the complaint and discipline process

Continuing Professional Development

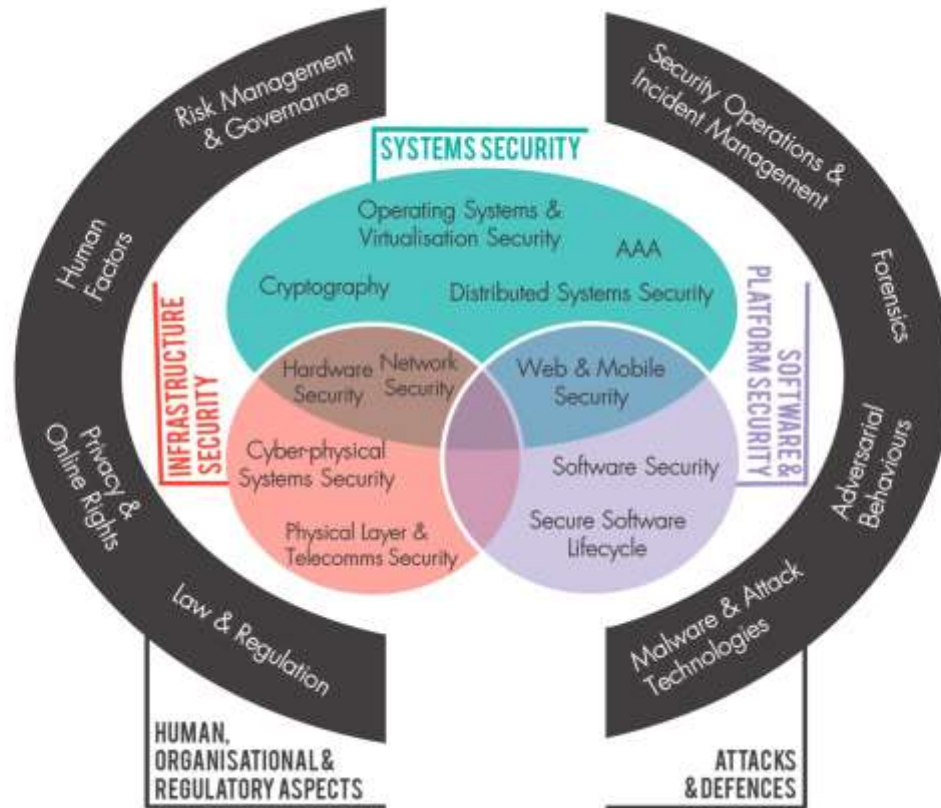
ISO/IEC 24773-1 describes how any form of certification scheme should include a requirement for continuous professional development.

This should include:

- A requirement for continuing professional development (CPD) appropriate to the titles that are certified
- Include the number of hours or CPD points required
- A justification for the CPD requirement, especially in relation to any risks that the requirement is designed to minimize

EXAMPLE – CYBER SECURITY

CyBOK Knowledge Areas



- CyBOK has categorised cyber security knowledge into 2 top level areas under the broad headings of:
 - Human, organisational and regulatory aspects
 - Attacks and defences
 - Systems security
 - Software and platform security
 - Infrastructure security
- As a framework, CyBOK has great depth, but is not written to support the skills management cycle.

CIISec Skills Framework



- The CIISec Skills Framework breaks down the skills required to be successful in the cyber domain down into:
 - 9 technical domains
 - 2 responsibility domains.
- The CIISec Skills Framework provides a detailed, specialist definition for each practical area of cyber security.

CIISec Skills Framework – Skills A to F

SECTION A Security Discipline – Information Security Governance and Management
A1 – Governance
A2 – Policy and Standards
A3 – Information Security Strategy
A4 – Innovation and Business Improvement
A5 – Behavioural Change
A6 – Legal & Regulatory Environment and Compliance
A7 – Third Party Management
SECTION B Security Discipline – Threat Assessment and Information Risk Management
B1 – Threat Intelligence, Assessment and Threat Modelling
B2 – Risk Assessment
B3 – Information Risk Management
SECTION C Security Discipline – Implementing Secure Systems
C1 – Enterprise Security Architecture
C2 – Technical Security Architecture
C3 – Secure Development
SECTION D Security Discipline – Assurance: Audit, Compliance and Testing
D1 – Internal and Statutory Audit
D2 – Compliance Monitoring and Controls Testing
D3 – Security Evaluation and Functionality Testing
D4 – Penetration Testing and conducting Simulated Attack Exercises
SECTION E Security Discipline – Operational Security Management
E1 – Secure Operations Management
E2 – Secure Operations and Service Delivery
SECTION F Security Discipline – Incident Management, Investigation and Digital Forensics
F1 – Intrusion Detection and Analysis
F2 – Incident Management, Incident Investigation and Response
F3 – Forensics

CIISec Skills Framework – Skills G to K

SECTION G Security Discipline – Data Protection, Privacy and Identity Management

G1 – Data Protection

G2 – Privacy

G3 – Identity and Access Management (IAM/IdM)

SECTION H Security Discipline – Business Resilience

H1 – Business Continuity and Disaster Recovery Planning

H2 – Business Continuity and Disaster Recovery Management

H3 – Cyber Resilience

SECTION I Security Discipline – Information Security Research

I1 – Research

I2 – Applied Research

SECTION J Security Discipline – Management, Leadership, Business and Communications

J1 – Management, Leadership and Influence

J2 – Business Skills

J3 – Communication and Knowledge Sharing

SECTION K Security Discipline – Contributions to the Information Security Profession and Professional Development

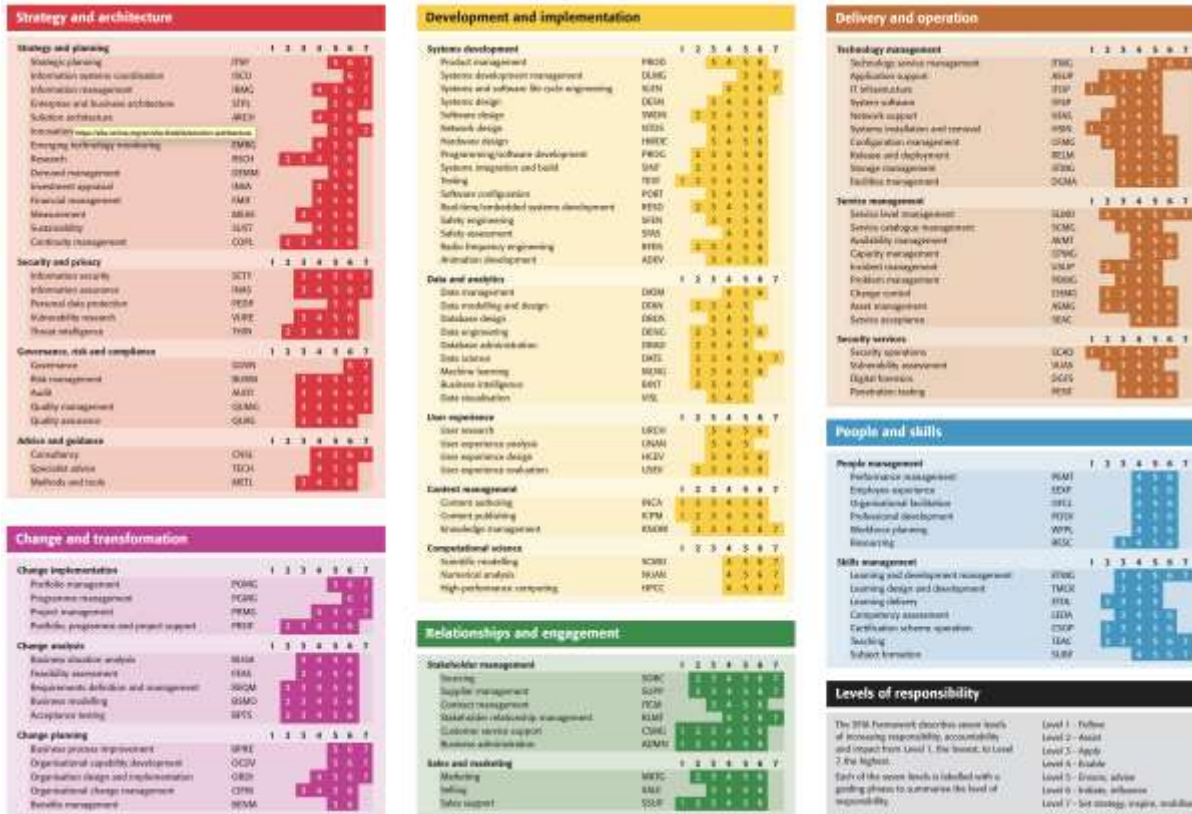
K1 – Contributions to the Community

K2 – Contributions to the IS Profession

K3 – Professional Development

Sections J & K are General Skills

SFIA Framework

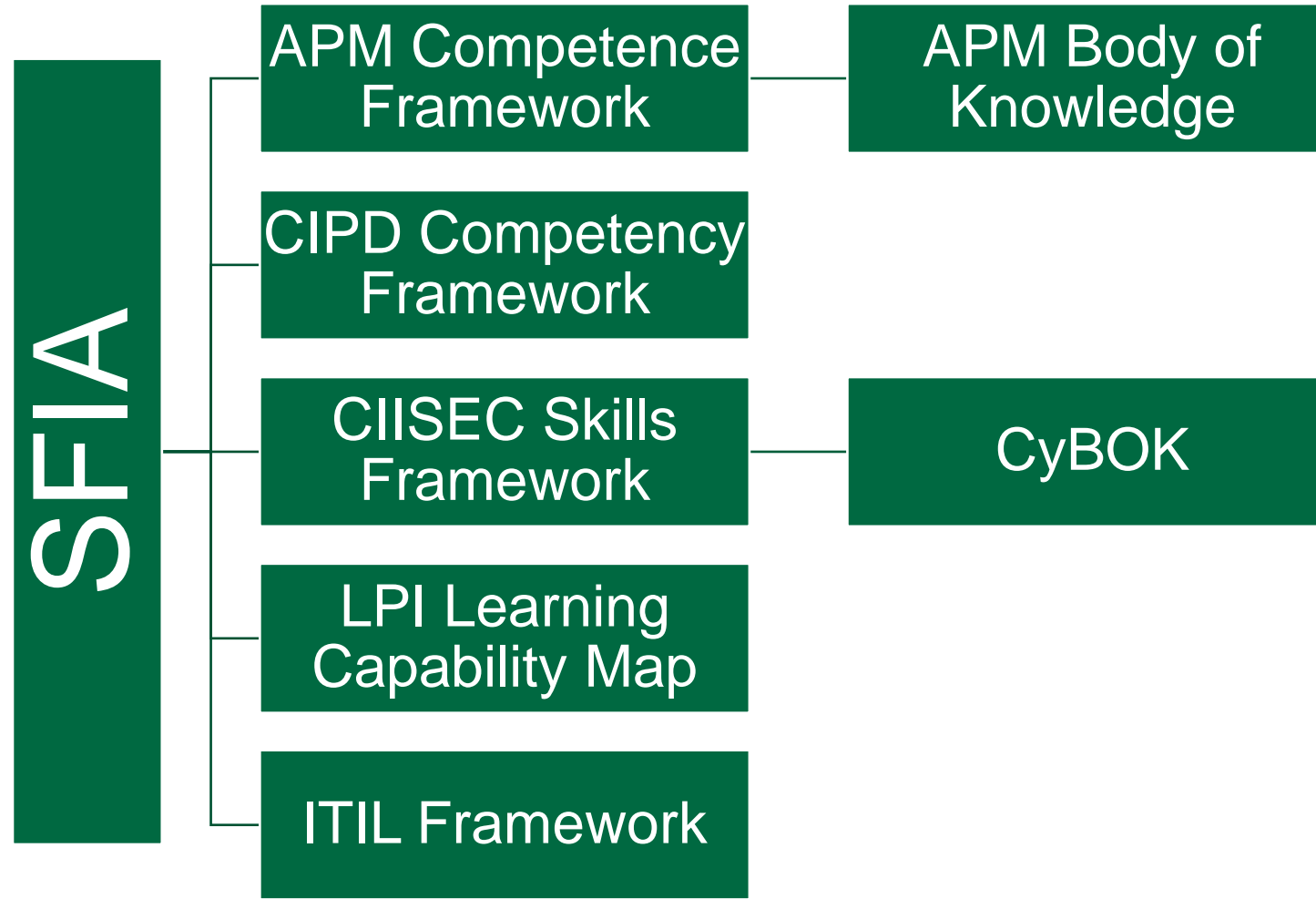


- SFIA is a generalist competency framework that covers most domains relating to the design, development, implementation, management and protection of data and technology.
- Top level categories are:
 - Strategy and architecture
 - Change and transformation
 - Development and implementation
 - Delivery and operation
 - People and skills
 - Relationships and engagement

SFIA 8 Security Skills

Category	Subcategory	Skill	Description
Strategy and Architecture	Security and privacy	Information security	Defining and operating a framework of security controls and security management strategies.
		Information assurance	Protecting against and managing risks related to the use, storage and transmission of data and information systems.
		Personal data protection	Implementing and operating a framework of controls and management strategies to promote compliance with personal data legislation.
		Vulnerability research	Conducting applied research to discover, evaluate and mitigate new or unknown security vulnerabilities and weaknesses.
		Threat intelligence	Developing and sharing actionable insights on current and potential security threats to the success or integrity of an organisation.
	Governance, risk and compliance	Governance	Defining and operating a framework for making decisions, managing stakeholder relationships, and identifying legitimate authority.
		Risk management	Planning and implementing organisation-wide processes and procedures for the management of risk to the success or integrity of the enterprise.
		Audit	Delivering independent, risk-based assessments of the effectiveness of processes, the controls, and the compliance environment of an organisation.
Delivery and operation	Security services	Security operations	Delivering management, technical and administrative services to implement security controls and security management strategies.
		Vulnerability assessment	Identifying and classifying security vulnerabilities in networks, systems and applications and mitigating or eliminating their impact.
		Digital forensics	Recovering and investigating material found in digital devices.
		Penetration testing	Testing the effectiveness of security controls by emulating the tools and techniques of likely attackers.

General and Specialist Frameworks and BoKs



EXAMPLE – SFIAPLUS

SFIPlus Online

For each skill at a level:

- Background
- Work Activities
- Knowledge/Skills
- Training
- PDAs (Professional Development Activities)
- Qualifications

The screenshot displays the SFIPlus V7 interface. At the top, there is a navigation bar with 'bcs The Chartered Institute for IT' on the left, 'SFIPlus Tools Help Search' in the center, and the 'SFIA' logo on the right. The main heading is 'SFIPlus V7' and 'Development and Implementation > Systems development'. Below this is the title 'Programming/software development (PROG)' with a 'Back to Matrix' link. A descriptive paragraph follows: 'The planning, designing, creation, amending, verification, testing and documentation of new and amended software components in order to deliver agreed value to stakeholders. The identification, creation and application of agreed software development and security standards and processes. Adopting and adapting software development lifecycle models based on the context of the work and selecting appropriately from predictive (plan-driven) approaches or adaptive/iterative/agile approaches.' Below the description is a 'Level' section with a row of five buttons (7, 3, 4, 5, 4), where the '4' button is highlighted. An 'EXPORT' button is also visible. A horizontal menu below the level section includes 'Background', 'Work Activity', 'Knowledge / Skills', 'Training', 'PDAs', and 'Qualifications', with 'Work Activity' selected. A table with columns 'Title', 'Description', 'Optional', and 'Code' is shown below the menu. The table contains four rows of data:

Title	Description	Optional	Code
Program design	Designs complex programs / scripts and integration software services.		PROG401
Coding	Codes, amends and refactors complex programs / scripts and integration software services in accordance with the design.		PROG402
Testing	Verifies and tests complex programs / scripts and integration software services; corrects errors and re-tests as appropriate.		PROG403
Documentation	Documents all work in accordance with agreed standards.		PROG404

SFIPlus Example – Vulnerability Assessment

Competency Description

- Generic:
 - Identifying and classifying security vulnerabilities in networks, systems and applications and mitigating or eliminating their impact.
- Level 3:
 - Follows standard approaches to performs basic vulnerability assessments for small information systems. Supports creation of catalogues of information and technology assets for vulnerability assessment.

Broken down into work activities (Skills)

- Critical information and technology assets
- Vulnerability identification and analysis
- Vulnerability assessment
- Assessment documentation
- Communication and awareness
- Risk assessment

SFIPlus Example – Vulnerability Assessment

Knowledge Of:

- National/International standards
- Networking and Communications
- Operating Systems
- Operational/Service Architecture
- Access Control Systems
- Own Organisations IT Products and Services
- Third Party IT Products and Services
- Middleware

Knowledge Of (cont.):

- Infrastructure Configuration
- Analytical Tools
- Network Data Security
- Security Software, Tools and Techniques
- Infrastructure/System Security
- Legislation
- Risk Management

SFIPlus Example – Vulnerability Assessment

Behavioural Skills

- Analytical Thinking
- Attention to Detail
- Verbal Expression
- Written Expression
- Teamwork

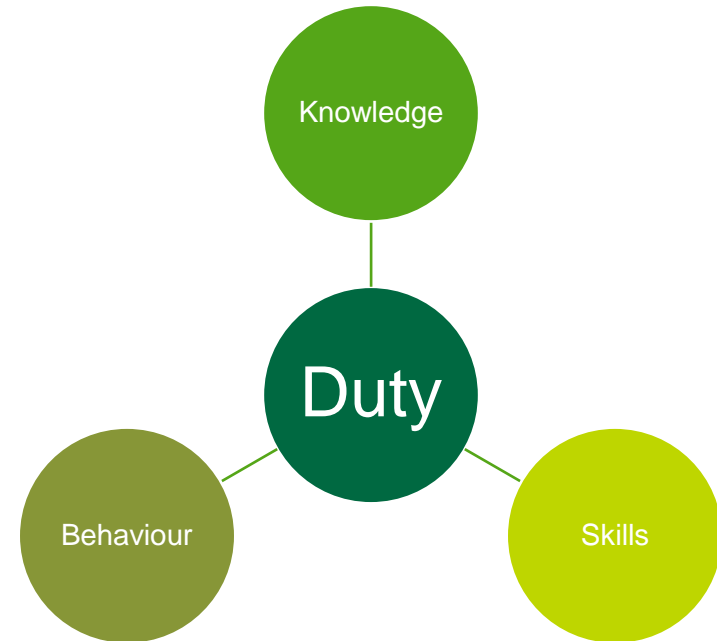
Behavioural Skills

- Time Management Techniques
- Report Writing Techniques

EXAMPLE – OCCUPATIONAL STANDARDS

Duties: Knowledge, Skills and Behaviours (KSBs)

- For each duty, it is necessary to identify the knowledge, skills and behaviours that a competent person in the occupation would be expected to have / demonstrate
- As well as **helping to shape and inform the training plan** for apprentices, they will also **contribute to the end point assessment** planning process



Knowledge, Skills & Behaviours

- **knowledge** is the information, technical knowledge, and ‘know-how’ that the individual needs to have and to understand in order to successfully carry out the duties that make up the occupation
- **skills** are the practical application of knowledge needed to successfully undertake the duties that make up the occupation. They have to be learnt through on and/or off-the-job training or experience. Start with a verb.
- **behaviours** are mind-sets, attitudes or approaches required for competence

Occupational Standards

Occupational standards typically have:

- 15 to 20 knowledge statements
- 15 to 20 skill statements
- Five to six behaviour statements.
- It is not necessary for knowledge statements to always have a corresponding skill or behaviour statement. Knowledge may underpin several skills and behaviours.
- You need to identify (map) the KSBs required to undertake each duty. Each KSB is likely to be needed for more than one duty. Only map the most relevant KSBs to each duty. You need to ensure that each KSB is mapped to at least one duty.

Best Practice

Describe them in terms of someone who is fully competent in the occupation

- Only include KSBs at their highest level
- The readability of an apprenticeship standard should be appropriate to the skill level
- The language used should be gender-neutral
- List according to assessment for example health and safety could be two statements both in knowledge assessed through a test and in skills assessed through observation
- Future proof statements
- Be as specific as possible

Apprenticeships – Cyber Security Technician

Role:

- Provide first line cyber security support.

Duties: (extract)

- **Duty 1** Apply procedures and controls to maintain security and control of an organisation.
- **Duty 2** Contribute to the production and development of security culture across an organisation including assisting with the promotion of cyber security awareness programmes, monitoring the effectiveness of cyber security awareness programmes, promoting an effective cyber security culture
- **Duty 3** Process cyber security helpdesk requests ensuring confidentiality, integrity and availability of digital information, meeting relevant legal and regulatory requirements for example access control requests.
- **Duty 4** Conduct the installation and maintenance of technical security controls in accordance with relevant procedures and standards.
- **Duty 5** Monitor, identify, report and escalate information security incidents and events in accordance with relevant procedures and standards.

Apprenticeships – Cyber Security Technician

Knowledge: (extract)

- **K1:** Principles of organisational information security governance and the components of an organisation's cyber security technical infrastructure including hardware, operating systems, networks, software and cloud
- **K2:** Cyber security policies and standards based on an Information Security Management System (ISMS)
- **K3:** Types of physical, procedural and technical controls
- **K4:** Awareness of how current legislation relates to or impacts upon the occupation including Data Protection Act, Regulation of Investigatory Powers Act, Human Rights Act, Computer Misuse Act, Freedom of Information Act, Official Secrets Act, Payment Card Industry Data Security Standard (PCI-DSS), Wireless and Telegraphy Act, professional body codes of conduct, ethical use of information assets
- **K5:** Cyber security awareness and components of an effective security culture, different organisational structures and cultures, the importance of maintaining privacy and confidentiality of an organisation's information and the impact of a poor security culture
- **K6:** Principles of cyber security compliance and compliance monitoring techniques

Skills: (extract)

- **S1:** Follow information security procedures
- **S2:** Maintain information security controls
- **S3:** Develop information security training and awareness resources
- **S4:** Monitor the effectiveness of information security training and awareness
- **S5:** Handle and assess the validity of security requests from a range of internal and external stakeholders
- **S6:** Follow technical procedures to install and maintain technical security controls
- **S7:** Monitor and report information security events
- **S8:** Recognise when and how to escalate information security events in accordance with relevant procedures and standards
- **S9:** Review and modify access rights to digital information systems, services, devices or data
- **S10:** Maintain an inventory of digital information systems, services, devices and data storage

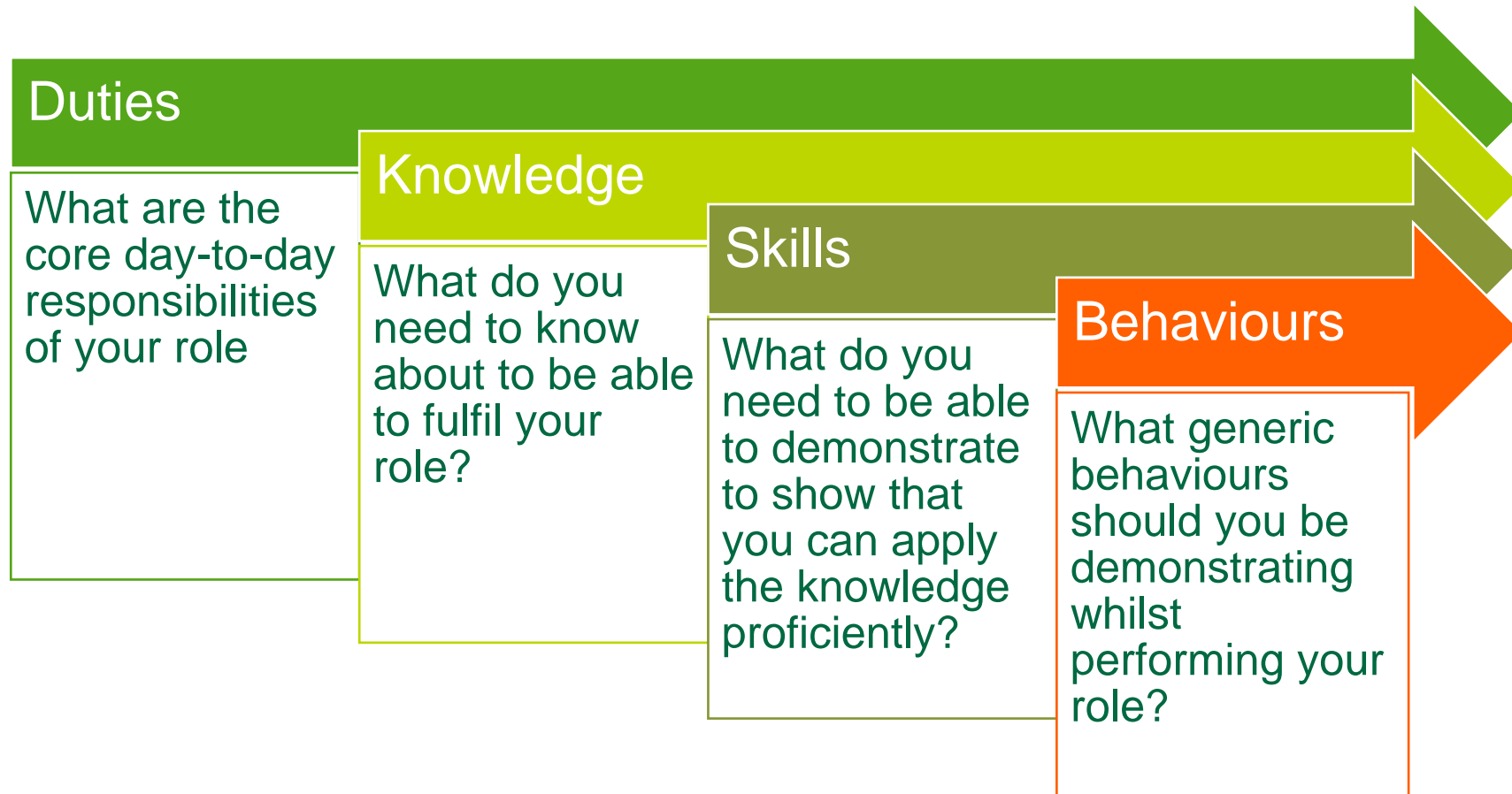
Apprenticeships – Cyber Security Technician

Behaviours:

- **B1:** Manage own time to meet deadlines and manage stakeholder expectations
- **B2:** Work independently and take responsibility for own actions within the occupation
- **B3:** Use own initiative
- **B4:** A structured approach to the prioritisation of tasks
- **B5:** Treat colleagues and external stakeholders fairly and with respect without bias or discrimination
- **B6:** Act in accordance with occupation specific laws, regulations and professional standards and not accept instruction that is incompatible with any of these
- **B7:** Review own development needs in order to keep up to date with evolution in technologies, trends and innovation using a range of sources

TRY IT!

Build your own profile



Digital Forensics Role - Duties

LIST THE CORE RESPONSIBILITIES OF THE ROLE:

- **Maintain evidence management. Handle exhibits and evidential material in line with agreed protocols to ensure the integrity, continuity, and security of digital evidence for the purpose of investigative processing and court proceedings.**
- Ensure the appropriate capture and preservation of digital forensic material utilising appropriate forensic technology for digital examinations (specific tool training may be required).
- Make appropriate decisions on the processing of digital evidence in support of investigations whilst complying with legislation.
- To work within a quality-controlled environment aligning to standard operating policies and procedures.
- Apply an understanding of other physical forensic evidence whilst conducting digital investigative decisions to ensure the preservation of all evidence.
- Adapt the use of specialist technical equipment within a laboratory, at a crime scene or other appropriate location to conduct forensic examination's. Ensuring handling, transport, storage, and environmental factors are all considered.
- Undertake equipment testing, fault finding and maintenance according to agreed schedules and in line with quality standards and investigative needs to ensure appropriate health and safety considerations, the use of PPE and awareness of potential biohazards are all considered as part of the examination process.
- Technical problem solving. Applying scientific methodology and rational to address technical problems, analyse and retrieve data. Understanding and embedding known equipment limitations and investigative decision making into any problem solving.
- Produce evidential contemporaneous notes, reports (including Streamlined Forensic reporting), and continuity statements attending court, tribunals and hearings as required in support of the investigative process.
- Support a peer review process to ensure evidential quality and individual competency.
- Inform a digital forensic strategy providing advice on technical capabilities and contributing to investigative meetings.
- Following risk assessments; local, national and on digital forensics and crime scenes activities from multiple agencies to ensure the integrity of digital evidence.
- Liaison with colleagues from a variety of disciplines both external and internal to the organisation exercising responsibility for work within defined parameters.

Knowledge, Skills, and Behaviours – Development Template

Maintain evidence management. Handle exhibits and evidential material in line with agreed protocols to ensure the integrity, continuity and security of digital evidence for the purpose of investigative processing and court proceedings

Knowledge- explain to me

- Know agreed submission process and acceptance criteria's.
- Understanding of Data Protection Act
- Know/understand vulnerability of data on Digital devices and best practice for preservation.

The content for lectures/seminars

Skill – show me

- Safe handling and storage of digital exhibits
- Safe handling and storage of Personal and sensitive data
- Compliance with set submission and examination criteria.
- Use effective methods to protect and preserved data.

The content for labs/exercises

Behaviour- let me see you exhibit

- Effective communication.
- Safe physical manual handling
- Team Working
- Practical exhibit handling.

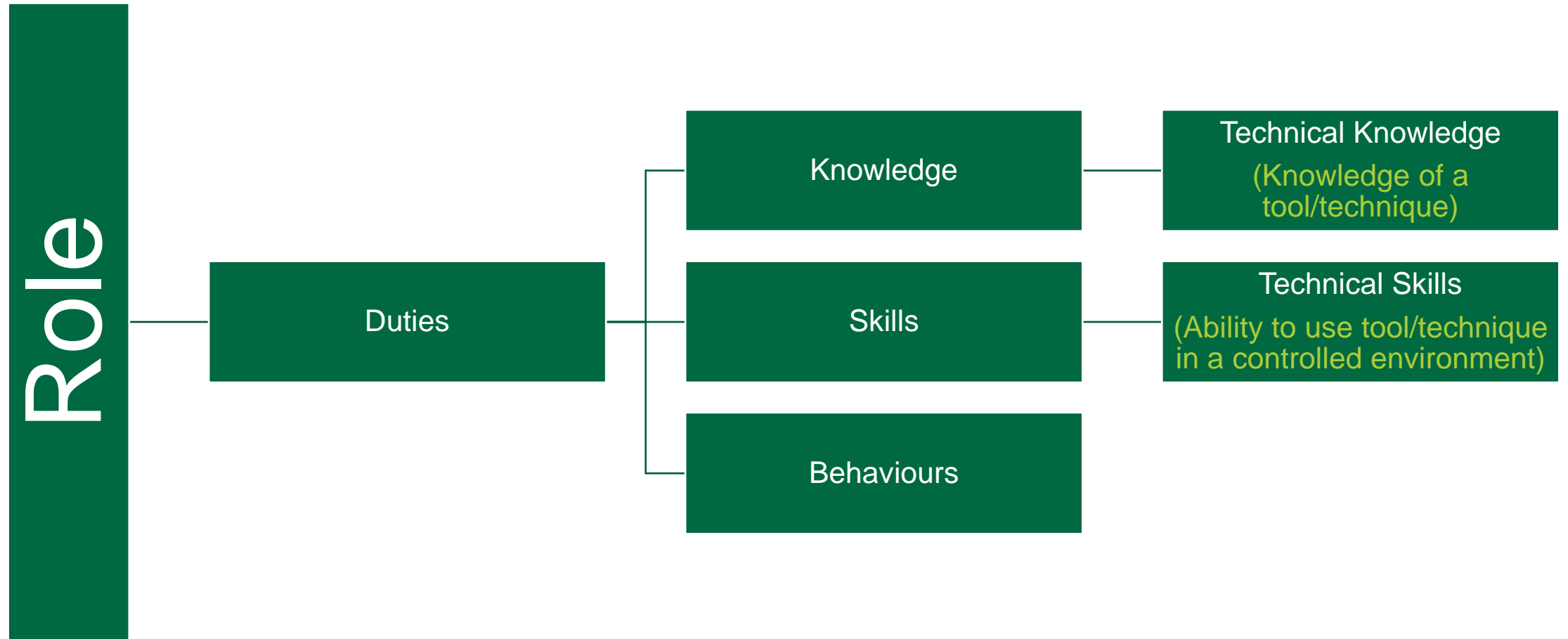
What needs to be observed

KEY TAKEAWAYS

The Skills Management Cycle



The Integrated Skills Model



Key Takeaways



When you are looking at skills management issues, recognise when it is best to use knowledge, skills, duties or competence frameworks – they perform different roles



With appropriate use, the skills management cycle will help improve communication and understanding for all involved – managers, HR and individuals



By using a mix of generalist, specialist and technical skills frameworks organisations can achieve a consistent and integrated skills and people management approach.

QUESTIONS

THANK YOU

