WE ARE RECORDING

PUT QUESTIONS INTO CHAT

WE WILL BE STARTING AT 7PM
“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

Welcome to our group!

If you're interested in any aspect of IT learning, it would be great to have 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, please get in touch at specialists@bcs.org.uk.

Kevin Simons, Chair

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

https://www.youtube.com/c/BCSMemberGroups/playlists
Follow us on Social Media

• 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
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 STREATERT
IT Skills Frameworks

How do they all fit together?

- What IT skills frameworks do you know of?

Join at slido.com #2609 511
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

Plan and organise

Acquire

Deploy

Develop

Assess

Analyse

Reward
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

<table>
<thead>
<tr>
<th>Knowledge</th>
<th>Cognitive Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowledge 1</td>
<td>Cognitive level description</td>
</tr>
<tr>
<td>Knowledge 2</td>
<td>Cognitive level description</td>
</tr>
<tr>
<td>...</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Skill</th>
<th>Knowledge</th>
<th>Performance Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skill 1</td>
<td>List of knowledge required to demonstration skill 1</td>
<td>Performance level description</td>
</tr>
<tr>
<td>Skill 2</td>
<td>List of knowledge required to demonstration skill 1</td>
<td>Performance level description</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: BS ISO/IEC-24773-1:2019
# Competency and Proficiency

<table>
<thead>
<tr>
<th>Competency</th>
<th>Knowledge</th>
<th>Skill</th>
<th>Proficiency level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Competency 1</td>
<td>List of knowledge required to demonstrate competency 1</td>
<td>List of skills required to demonstrate competency 1</td>
<td>Proficiency level description</td>
</tr>
<tr>
<td>Competency 2</td>
<td>List of knowledge required to demonstrate competency 2</td>
<td>List of skills required to demonstrate competency 2</td>
<td>Proficiency level description</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Role 1</th>
<th>Competency 1 required to fulfil role 1</th>
<th>Performance level required to fulfil role 1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Competency 2 required to fulfil role 1</td>
<td>Performance level required to fulfil role 1</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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
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.

Source: CyBOK https://www.cyb.org/knowledgebase/
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.

Source: CIIsec https://www.ciisec.org/
## CII Sec Skills Framework – Skills A to F

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

<table>
<thead>
<tr>
<th>SECTION</th>
<th>Security Discipline – Data Protection, Privacy and Identity Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>G1</td>
<td>Data Protection</td>
</tr>
<tr>
<td>G2</td>
<td>Privacy</td>
</tr>
<tr>
<td>G3</td>
<td>Identity and Access Management (IAM/IdM)</td>
</tr>
<tr>
<td>SECTION</td>
<td>Security Discipline – Business Resilience</td>
</tr>
<tr>
<td>H1</td>
<td>Business Continuity and Disaster Recovery Planning</td>
</tr>
<tr>
<td>H2</td>
<td>Business Continuity and Disaster Recovery Management</td>
</tr>
<tr>
<td>H3</td>
<td>Cyber Resilience</td>
</tr>
<tr>
<td>SECTION</td>
<td>Security Discipline – Information Security Research</td>
</tr>
<tr>
<td>I1</td>
<td>Research</td>
</tr>
<tr>
<td>I2</td>
<td>Applied Research</td>
</tr>
</tbody>
</table>

**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

Source: SFIA Foundation https://sfia-online.org/
## SFIA 8 Security Skills

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

SFIA

- APM Competence Framework
- CIPD Competency Framework
- CIISC Skills Framework
- LPI Learning Capability Map
- ITIL Framework

APM Body of Knowledge

CyBOK

bcs.org
EXAMPLE – SFIAPLUS
SFIAplus Online

For each skill at a level:

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

For each skill at a level:

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

Duties
What are the core day-to-day responsibilities of your role?

Knowledge
What do you need to know about to be able to fulfil your role?

Skills
What do you need to be able to demonstrate to show that you can apply the knowledge proficiently?

Behaviours
What generic behaviours should you be demonstrating whilst performing your role?
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.
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.

### 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.

### Behaviour - let me see you exhibit
- Effective communication.
- Safe physical manual handling
- Team Working
- Practical exhibit handling.

<table>
<thead>
<tr>
<th>Knowledge, Skills, and Behaviours – Development Template</th>
</tr>
</thead>
<tbody>
<tr>
<td>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</td>
</tr>
</tbody>
</table>

---

The content for lectures/seminars

The content for labs/exercises

What needs to be observed
KEY TAKEAWAYS
The Skills Management Cycle

1. Plan and organise
2. Acquire
3. Deploy
4. Develop
5. Analyse
6. Assess
7. Reward
The Integrated Skills Model

Role

Duties

Knowledge

Technical Knowledge
(Knowledge of a tool/technique)

Skills

Technical Skills
(Ability to use tool/technique in a controlled environment)

Behaviours
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