Occupation Profile

Modern Apprenticeship in Digital Technology - Cyber Security Pathway SCQF Level 6

Approved by: Digital Technology Technical Expert Group

Approved date: October 2022

Purpose:

This occupation profile consists of 10 work situations routinely carried out in cyber security roles. Collectively these describe all the performance requirements and knowledge and understanding requirements apprentices need to demonstrate competence in the occupation. Each work situation has a unique reference number and is set out as follows:

- Work situation title, goal, brief outline, performance requirements and knowledge and understanding requirements

Contents

Mandatory work situations

Work Situation

URN: SDS0221

Applying problem solving approaches

Goal of work situation:
To select and apply tools and techniques to solve workplace problems in line with organisational procedures.

Brief outline:
This involves individuals identifying and exploring problems, selecting appropriate approaches, planning problem-solving steps, carrying out and assessing problem resolutions. This also includes documenting problems, resolutions and outcomes.

Performance requirements

1. Diagnosing problems to identify the key characteristics, who it affects, the impact and urgency to resolve it
2. Selecting and justifying the most appropriate problem-solving techniques in line with organisational procedures
3. Developing step-by-step plans to solve problems
4. Performing root cause analysis to identify underlying causes of problems and identify solutions
5. Evaluating potential solutions and selecting the most feasible
6. Implementing solutions to resolve problems
7. Assessing effectiveness of problem resolutions to contribute to continuous improvement activities
8. Documenting problems, approaches, steps taken, techniques applied and outcomes of the problem-solving activities to update knowledge bases

Knowledge and understanding requirements

1. What is meant by problem-solving
2. The importance of problem solving within an organisational context
3. How to diagnose problems to understand the main characteristics, impact, stakeholders and importance
4. Industry standard tools and techniques that can be applied to solving problems and how to apply them
5. How to plan problem solving steps
6. Steps involved in root cause analysis and how to apply them
7. How to evaluate solutions to problems and select the most appropriate
8. How to assess the effectiveness of problem-solving techniques and problem solutions
9. Impact on organisations of poor problem solving
10. How to document problems, problem solving approaches and resolutions
11. The importance of maintaining a knowledge base of problems and their resolutions

Work Situation

URN: SDS0224

Producing documentation to support organisational process delivery

Goal of work situations:
To produce and update documentation for colleagues, customers and users to support the delivery of organisational processes.

Brief outline:
This is about individuals assessing documentation requirements, including audience, type of documentation and structure and format required. This also includes creating documents and associated graphics, identifying sources of information to include, maintaining version and revision control and checking documents meet requirements.

Performance requirements

1. Assessing documentation requirements to plan documentation production
2. Selecting structure and format of documentation in line with organisational style guides
3. Identifying sources of information for documentation to meet organisational requirements
4. Producing and updating documentation in line with organisational procedures
5. Applying version and revision control to document production in line with organisational procedures
6. Creating relevant graphics and visualisations within documentation to aid interpretation and illustrate key concepts
7. Reviewing documentation with stakeholders to ensure requirements are met
8. Following procedures for documentation sign off and storage in line with organisational procedures

Knowledge and understanding requirements

1. Who the stakeholders are for documentation
2. Purpose of the documentation being created
3. How to review documentation requirements
4. Steps involved in planning document production
5. Organisational structure and format style guides for standard documents including detailed and summary reports, plans, guidelines, standard operating procedures and project documentation
6. Industry standard conventions of format, structure and layout in documents and how to select and apply them
7. How to identify, locate and utilise information to include in documentation
8. Organisational policies and regulations for data protection and copyright that apply to documentation production
9. Industry standard tools and techniques used for document production and how to apply them
10. How to produce documentation
11. How to apply version and revision control to document production
12. How to create graphics and visualisations in documentation
13. Organisational procedures for testing and quality checking documentation
14. Organisational procedures for document sign off, version control, storage and distribution

Work Situation

URN: SDS0223

Developing meta-skills and personal practice

Goal of work situation:
To develop meta-skills and personal practice through self-evaluation, agreeing objectives, reflecting on practice, and actively learning to improve own performance in line with organisational requirements.

Brief outline:
This is about developing meta-skills and personal practice. This involves reflecting on and learning from practice; acting on feedback; agreeing and working towards own objectives for continuous personal and professional development. Individuals will be supported in their development, usually by their line manager.

Performance requirements

1. Identifying meta-skills and role specific skills regularly used in own work to assess strengths and improvement needs for personal and professional development
2. Discussing and agreeing SMART objectives for personal and professional development and to achieve business objectives
3. Discussing and agreeing appropriate development activities to improve own performance and to achieve business objectives
4. Completing development activities within agreed timescales to support and progress own performance
5. Acting on feedback to improve own performance and development
6. Reflecting on performance, meta-skills and specific skills developed in your role to identify and agree future development needs
7. Completing mandatory training in line with organisational requirements
8. Completing documentation required for personal and professional development in line with organisation policy and procedures

Knowledge and understanding requirements

1. The purpose and importance of meta-skills including their definitions and how they relate to own work
2. The importance of personal and professional development within own organisation and role
3. How to use reflective practice to identify gaps in role specific knowledge, skills and meta-skills
4. How to participate effectively in performance reviews
5. How to discuss and agree SMART objectives – Specific, Measurable, Achievable, Realistic, Time-bound
6. The importance of business and personal objectives in own development
7. Sources of up-to-date and appropriate information to support own development
8. The importance of maintaining well-being in own role and where to get support
9. How to use feedback to develop own skills and knowledge
10. Different learning models and styles and how to use these for own development

Work Situation

URN: SDS0222

Defining requirements to support project delivery

Goal of work situation:
To identify, understand and define stakeholder requirements for own projects to support project delivery.

Brief outline:
This is about individuals assessing requirements for projects they are tasked with delivering, through engaging with stakeholders to understand project goals and outcomes required. This includes defining and documenting requirements, identifying risks, producing estimates, developing plans and providing progress updates.

Performance requirements

1. Scheduling and attending project requirements meetings with stakeholders to gather project requirements
2. Reviewing project requirement specifications, plans and stakeholder feedback to specify own project tasks, deliverables and timescales
3. Undertaking estimation of own tasks and deliverables in line with organisational procedures
4. Producing task breakdown and project schedules to plan own project activities
5. Identifying key risks to own project to develop a risk assessment
6. Producing progress updates of own tasks to inform project monitoring

Knowledge and understanding requirements

1. Who the internal or external stakeholders are for a project
2. How to schedule and conduct stakeholder requirements meetings
3. How to engage with stakeholders and tailor communication styles
4. How to identify project requirements with stakeholders
5. How to interpret project requirement specifications and plans
6. SMART objectives (Specific, Measurable, Achievable, Realistic and Timebound) and how to apply them
7. Understanding the organisation’s approach to managing projects and how this aligns to industry standard approaches
8. Steps involved in producing estimates for own project tasks
9. How to produce task breakdowns and schedules of own tasks and deliverables
10. Steps involved in identifying and assessing risks to own project activities
11. How to track and report own effort and progress on project tasks and outputs delivered
12. How to provide updates on projects and deliverables
13. The importance of developing excellent relationships with colleagues and stakeholders to support own project delivery

Work Situation

URN: SDS0211

Supporting cyber security governance

Goal of work situation:
To support the delivery of cyber security governance and compliance processes in line with organisational requirements.

Note: Individuals receive on-the-job training while working under close supervision as they gain experience, typically working on smaller tasks within larger projects.

Brief outline:
This is about individuals supporting organisational governance and compliance processes. This involves supporting documentation development and standardisation of processes for cyber security governance. This includes supporting implementation of cyber security programmes and accreditations, conducting audits and compliance checks and producing relevant documentation.

Performance requirements

1. Supporting development of governance and compliance documentation in line with organisational requirements
2. Supporting implementation of processes to support cyber security governance
3. Supporting attainment of organisational cyber security accreditations to validate cyber security management system maturity
4. Supporting delivery of security audits and compliance checks in line with organisational procedures
5. Documenting and reporting status and outcomes of cyber security compliance to stakeholders in line with organisational procedures

Knowledge and understanding requirements

1. Main principles of information security governance
2. The role of information security management systems in supporting security governance
3. Roles and responsibilities of individuals, at all levels, who are responsible for making cyber security decisions
4. Main processes involved in information security governance and how to implement them
5. How to develop and update cyber security governance and compliance documentation
6. Regulatory and organisational policies and standards relating to information and cyber security governance and compliance
7. Industry standard organisational cyber security accreditation standards and the requirements to achieve them
8. How to conduct cyber security audits and compliance checks
9. How to document and produce status reports for cyber security governance and compliance

Work Situation

URN: SDS0212

Contributing to the implementation of cyber security controls

Goal of work situation:
To contribute to implementing, testing and maintaining cyber security controls in line with organisational requirements.

Note: Individuals receive on-the-job training while working under close supervision as they gain experience, typically working on smaller tasks within larger projects.

Brief outline:
This is about individuals contributing to implementing organisational technical and administrative controls used to treat cyber security risk. This includes applying and maintaining controls, administering access controls and testing ongoing performance of security controls to ensure they meet the specified levels of risk treatment.

Performance requirements

1. Contributing to implementing, maintaining and tuning technical security controls to protect organisational infrastructure including:
    - Anti-malware and endpoint protection
    - Firewall network protection
    - Patch management
2. Administering user access controls in line with organisational policies and procedures
3. Contributing to operating system and application hardening to mitigate security vulnerabilities in line with organisational procedures
4. Contributing to cyber security controls testing exercises to ensure controls perform to organisational standards

Knowledge and understanding requirements

1. The role of cyber security controls to protect information assets and systems
2. Organisation cyber security risk management policy and procedures
3. Basic networking concepts and security principles used to support applications, services and data storage for on-premises and cloud
4. Industry standard network protocols, including HTTPS (Hypertext Transfer Protocol Secure) and TLS (Transport Layer Security) protocols
5. Different cloud environments (public, private, hybrid) and cloud control frameworks
6. Main types of controls (preventative, directive, detective and corrective) used to manage information security risk
7. Differences between technical and procedural cyber security controls
8. How to implement, maintain and tune industry standard technical controls including firewalls, anti-malware and patch management
9. Main concepts of access control management including single sign on, federated access and multifactor authentication techniques
10. Principles of least privilege and ‘need to know’ access to information systems

11. How to administer user access controls
12. Steps involved in system hardening and how to apply them
13. How to test cyber security controls across relevant infrastructure

Work Situation

URN: SDS0213

Contributing to cyber security risk assessment and management

Goal of work situation:
To contribute to the identification, assessment and management of risks to organisational assets to prioritise risk reduction activities.

Note: Individuals receive on-the-job training while working under close supervision as they gain experience, typically working on smaller tasks within larger projects.

Brief outline:
This is about individuals contributing to analysing and managing risks to the organisation including undertaking risk assessments with supervision and contributing to risk identification, analysis, evaluation, monitoring and treatment. This also involves maintaining risk registers, contributing to risk reviews and documenting risk status.

Performance requirements

1. Updating the Digital Asset Management (DAM) system to maintain digital assets in line with organisational requirements
2. Contributing to the identification and assessment of cyber security risks within organisational systems to inform risk treatment action planning
3. Contributing to monitoring and tracking risk mediation plans in line with organisational procedures
4. Updating the organisation's risk register to document and track risks in line with organisational procedures
5. Attending risk review meetings to update on risk status and risk management planning
6. Reporting and communicating identified risks and their status to colleagues and stakeholders

Knowledge and understanding requirements

1. Differences between physical assets and information assets
2. What is meant by Confidentiality, Integrity and Availability (CIA) for an organisation’s information assets
3. Threat landscapes and the different threats and threat actors relevant to an organisation
4. How to identify and record organisational assets in a digital asset management system (DAM)
5. Organisational risk assessment and management policies and procedures and how to apply them
6. How to conduct risk assessments
7. Steps involved in monitoring and tracking risks and how to apply them
8. What is meant by a ‘risk register’ and how to document and maintain them
9. The role of risk review meetings and how to inform them on risk status
10. Main legislation and regulations that apply to cyber security risk assessment and management
11. How to work with key risk indicators used to assess and measure potential risks
12. Organisational risk appetite
13. How to report on risk assessments

Work Situation

URN: SDS0214

Contributing to cyber security awareness programmes

Goal of work situation:
To contribute to informing and deploying the organisation's cyber security awareness programmes to maintain employee knowledge of cyber security issues and preventative measures across the organisation.

Note: Individuals receive on-the-job training while working under close supervision as they gain experience, typically working on smaller tasks within larger projects.

Brief outline:
This is about individuals contributing to researching cyber security notices to maintain organisational awareness of new threats. It includes contributing to the development of cyber security awareness programmes and advisory notifications. It also includes producing guides and dashboards for cyber security awareness.

Performance requirements

1. Contributing to identifying organisational cyber security awareness programme needs to inform research planning activities
2. Researching trusted external sources of cyber security threats, including breaches, malware and phishing to inform cyber security awareness programmes
3. Contributing to documenting research outcomes to update the organisation's cyber security knowledge base
4. Contributing to producing awareness guides and advisory notifications in line with organisational procedures
5. Contributing to producing dashboards and status reports on the effectiveness of cyber security awareness programmes

Knowledge and understanding requirements

1. The importance of maintaining organisational awareness of cyber security threats that might impact employees
2. The purpose of cyber security awareness in maintaining an organisation's cyber security culture
3. The role of cyber security notifications in updating employees of new threats and how to respond to them
4. How to identify cyber security awareness programme needs and perform gap analysis against current provision
5. How to perform cyber security research of external threat notices to inform organisational awareness programmes and advisory notification development
6. How employee awareness contributes to cyber security risk mitigation
7. Various sources of cyber security threat notices and how to access them
8. How to maintain current awareness of breaches, malware and phishing attacks
9. How to develop organisational awareness programmes

10. How to plan and deliver advisory cyber security awareness and guidance
11. How to produce dashboards and reports to update status of cyber security advisory and awareness activities

Optional work situations

A minimum of one optional work situation must be achieved

Work Situation

URN: SDS0215

Contributing to network vulnerability analysis

Goal of work situation:
To contribute to conducting network vulnerability assessments to identify vulnerabilities in organisational networks.

Note: Individuals receive on-the-job training while working under close supervision as they gain experience, typically working on smaller tasks within larger projects.

Brief outline:
This is about individuals contributing to identifying and assessing vulnerabilities identified through scanning organisational networks. This also involves mitigating vulnerabilities through contributing to system patching and remedial activities and producing vulnerability assessment reports.

Performance requirements

1. Contributing to scoping and planning vulnerability assessments in line with organisational procedures
2. Contributing to conducting vulnerability assessments to identify vulnerabilities in on-premises and cloud network environments in line with assessment plans
3. Contributing to analysing and interpreting vulnerability assessment results to identify vulnerabilities
4. Contributing to implementing automated tools to improve efficiency of vulnerability assessments
5. Contributing to network system patching informed via vulnerability assessments in line with organisational procedures
6. Contributing to vulnerability assessment reports in line with organisational reporting processes

Knowledge and understanding requirements

1. That vulnerabilities in systems can compromise the confidentiality, integrity, or availability of information
2. Differences between vulnerability assessments and penetration tests
3. That a network vulnerability assessment is the review and analysis of an organisation’s network infrastructure to find cyber security vulnerabilities and network security loopholes
4. Steps involved in scoping and planning vulnerability assessments and how to apply them
5. Industry standard architectures and key features of on-premises and cloud network infrastructure
6. How to conduct vulnerability assessments for on-premises and cloud network infrastructure using industry standard tools
7. How to assess vulnerabilities through analysing and interpreting vulnerability assessment results
8. Common network vulnerabilities and how to mitigate them
9. Industry standard tools used to automate vulnerability assessments and how to implement them
10. Steps involved in applying network system patching to mitigate vulnerabilities and how to apply them

11. That vulnerability assessments seek to identify known vulnerabilities, such as system misconfiguration, outdated software, and a lack of patching and new vulnerabilities
12. How to prepare vulnerability assessment reports

Work Situation

URN: SDS0216

Supporting cyber security incident response and management

Goal of work situation:
To support incident response activities for cyber security incidents to ensure they are managed in line with organisational procedures.

Note: Individuals receive on-the-job training while working under close supervision as they gain experience, typically working on smaller tasks within larger projects.

Brief outline:
This is about individuals supporting information security incident investigation, analysis and management. This involves verifying severity of cyber security incidents and following escalation and resolution procedures. This also includes documenting incidents and their resolution and updating the organisation's knowledge base.

Performance requirements

1. Supporting response to cyber security alerts in line with organisational procedures
2. Supporting analysis of system log files and alerts to identify cyber security incidents
3. Supporting verification of the presence of a cyber security incident and its severity to determine whether to resolve or escalate it
4. Investigating low severity incidents to resolve them in line with playbooks and organisational procedures
5. Documenting cyber security incident information and resolution activities to update the incident management system
6. Updating the knowledge base to inform future incident response activities

Knowledge and understanding requirements

1. Basic principles of incident management and response and how to apply them
2. Organisational information security processes and policies relating to incident response, management and documentation
3. Benefits of effective incident management to the organisation’s cyber resilience
4. Steps involved in cyber security incident response and how to follow them
5. Industry standard tools for incident detection and how to apply them
6. How to analyse system log files to detect potential incidents
7. How to verify existence and severity of cyber security breaches and incidents
8. Common low level cyber security issues that can arise in networked environments and how to respond to them
9. Escalation procedures for cyber security incidents and how to apply them
10. How to provide information security incident documentation and reports

11. How to update organisational knowledge bases with incident details and mitigations

The relationship between meta-skills and work situations

	Meta skills alignment											
Work situation	Adapting	Collaborating	Communicating	Creativity	Critical thinking	Curiosity	Feeling	Focussing	Initiative	Integrity	Leading	Sense making
Applying problem solving approaches	✓		✓	✓	✓	✓	✓		✓	✓		✓
Producing documentation to support organisational process delivery	✓	✓	✓	✓		✓	✓	✓	✓	✓		✓
Developing meta-skills and personal practice	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Defining requirements to support project delivery	✓	✓	✓		✓	✓	✓	✓		✓		✓
Supporting cyber security governance	✓	✓	✓	✓	✓	✓		✓	✓	✓		✓
Contributing to the implementation of cyber security controls	✓	✓	✓	✓	✓	✓		✓	✓	✓		✓
Contributing to cyber security risk assessment and management	✓	✓	✓	✓	✓	✓		✓	✓	✓		✓
Contributing to cyber security awareness programmes	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
Contributing to network vulnerability analysis	✓	✓	✓	✓	✓	✓		✓	✓	✓		✓
Supporting cyber security incident response and management	✓	✓	✓	✓	✓	✓		✓	✓	✓		✓

The table above indicates where there are opportunities to develop and evidence meta-skills in each work situation within the occupation profile. Please note, this information is for guidance, and indicates where meta-skills are explicit rather than an exhaustive list. There may be opportunities for individuals to develop and evidence other meta-skills when carrying out their role.

The relationship between National Occupational Standards and work situations

The table below indicates where there are links between National Occupational Standards and each work situation within the occupation profile

Work situation	National Occupational Standards Alignment
Applying problem solving approaches	ESKITP7034 Problem Management TECHDUPS1 Recognise and resolve routine digital technology problems
Producing documentation to support organisational process delivery	ECHDUWP1 Create and edit digital documents
Developing meta-skills and personal practice	CFABAA626 Plan how to manage and improve own performance in a business environment
Defining requirements to support project delivery	TECDT20341 Undertake system requirements elicitation and definition TECDT20351 Manage system requirements engineering
Supporting cyber security governance	TECIS60731 Contribute to information security audit, compliance and assurance activities
Contributing to the implementation of cyber security controls	TECIS60531Contribute to operational information security management activities
Contributing to cyber security risk assessment and management	TECIS60231 Contribute to information security risk assessment and management activities
Contributing to cyber security awareness programmes	TECIS600202 Protect against cyber security threats
Contributing to network vulnerability analysis	TECDT61131 Assist in implementing vulnerability assessment processes
Supporting cyber security incident response and management	TECIS60632 Contribute to information security incident investigation and management activities