Occupation Profile

Technical Apprenticeship in Digital Technology - Cyber Security Pathway at SCQF Level 8

Approved by: Digital Technology Technical Expert Group

Approved date: 08/2021

Purpose:

This occupation profile consists of 11 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: SDS 007

Applying methods and principles in project management

Goal of work situation:
This work situation involves using project management tools to plan, organise and monitor the progress of activities to achieve production quality performance indicators.

Brief outline:
This is about applying methods and principles of project management in line with organisational requirements. This includes ensuring activities are delivered in accordance with the business case and safe systems of work, and involves liaising with and reporting progress to stakeholders, ensuring activities contribute to key milestones and deliverables.

Performance requirements

1. Providing support to prepare business cases for approval of activities
2. Identifying roles, responsibilities and skill sets needed for project activities and resources
3. Planning and scheduling projects in line with agreed objectives, timescales, and organisational requirements
4. Managing activities in line with plans and to achieve milestones
5. Managing change in line with organisational procedures
6. Escalating to relevant personnel where there are deviations from plans
7. Identifying, agreeing, and implementing contingencies to mitigate problems
8. Communicating plan progress in formats to meet the needs of all relevant stakeholders
9. Reporting on progress in line with organisational reporting procedures
10. Collating and evaluating lessons learned to contribute to the continuous improvement of activities

Knowledge and understanding requirements

1. Relevant legislation and codes of practice, safe systems of work, risk and impact assessments for activities
2. The principles and approaches to developing good business cases
3. Different methodologies to plan and deliver activities and how to apply these
4. The tools and processes for identifying and analysing risks and opportunities and how to use them
5. Techniques and tools for monitoring and reviewing risks including when and how to escalate to management
6. Quantitative and qualitative measures of risk analysis and how to apply these
7. The importance of monitoring and controlling project performance including accountability
8. Industry specific tools and software for monitoring performance
9. The importance of establishing an agreed change control process, and the impact and consequences that changes can have on schedule, resources, and budget
10. The type of changes that may affect key performance criteria including time, cost, quality, and business case

11. The importance of contingency plans
12. The importance of evaluating and monitoring the benefits and challenges of activities and how to do this
13. Different ways, formats and frequency of reporting and presenting information on progress to internal and external stakeholders
14. The importance of liaising with internal and external stakeholders and how to do this

Work Situation

URN: SDS 187

Supporting digital business transformation

Goal of work situation:
To identify, evaluate and prioritise the opportunities to apply digital technology to improve operations by transforming business processes.

Brief outline:
This involves evaluating the organisational processes to propose digital technology solutions within businesses to reduce costs, enhance performance and deliver improved services as a result of digital transformation.

Performance requirements

1. Identifying and documenting organisational processes which require digital technology improvement
2. Establishing information requirements of the organisational processes requiring digital technology improvement
3. Evaluating the potential for digital technology solutions to transform the organisational processes that deliver organisational competitiveness
4. Analysing organisational processes to propose potential digital technology solutions
5. Conducting relevant research to inform decision making for digital transformation
6. Conducting health and safety risk assessments of digital transformation scenarios
7. Developing and delivering well-structured digital technology proposals in the form of business reports and presentations which resonate with stakeholders

Knowledge and understanding requirements

1. The meaning and significance of the ‘digital economy’ and ‘digital transformation’
2. How to model business processes
3. How organisations manage and implement technology driven change
4. How to formulate proposals for new digital technology solutions, including estimation of both costs and benefits
5. How digital technologies can be integrated within business processes
6. How digital transformation of business processes is implemented to provide improved productivity and service benefits
7. The legislation, regulations and organisational policies that relate to digital technology and safe use of IT in the workplace
8. The range of professional and unprofessional behaviour in digital technology contexts
9. The principles of business change and how organisations develop in the context of technological change
10. The organisational business objectives and how business strategy is used to achieve these
11. The range of metrics which might be used to evaluate the success of business operations

12. Current issues and ethical aspects in digital transformation implementation
13. The safe use of digital technology equipment in business operations

Work Situation

URN: SDS 012

Developing meta-skills and personal professionalism

Goal of work situation:
To develop meta-skills and personal professionalism through reflective practice, goal setting and active learning to improve own performance in line with organisational requirements.

Brief outline:
This is about taking responsibility for the development of own meta-skills and personal professionalism. This involves reflecting on and learning from practice; seeking and acting on feedback; agreeing and working towards own goals for continuous professional development (CPD); and managing own wellbeing.

Performance requirements

1. Self-evaluating meta-skills regularly to identify own strengths and improvement needs for development
2. Identifying own strengths and improvement needs for professional development
3. Setting and agreeing SMART objectives for personal development and to achieve business objectives
4. Planning development activities to improve own performance and to achieve business objectives
5. Completing formal and informal activities to support and progress own development
6. Seeking and acting on feedback to improve own performance
7. Critically reflecting on own performance and involvement in activities to support own development and achievement
8. Critically evaluating the development and application of meta-skills in own work to identify future development needs
9. Completing and maintaining records and documents in line with organisational 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 and impact of personal professionalism within the organisation and own role
3. How to use critical reflection and reflective practice to identify gaps in role specific knowledge, skills and meta-skills and the purpose and importance of this
4. How to participate effectively in performance reviews
5. How to set and agree SMART goals – Specific, Measurable, Achievable, Realistic, Time-bound
6. How to prepare development plans, including their content and duration
7. The importance of career and personal goals, including collective organisational learning, when planning own development
8. Sources of up-to-date and appropriate information to support own CPD activities
9. The impact and benefits of CPD including the organisation's key performance indicators (KPIs) and how they are measured and recorded
10. The importance of managing well-being for success in own role and where to get support
11. Appropriate ways to seek and act on feedback to develop own skills and knowledge including the process of 360-degree feedback

12. Different learning models and styles and how to use these for own development

Work Situation

URN: SDS 029

Contributing to cyber security risk assessment and risk management

Goal of work situation:
To contribute to conducting risk assessments on information systems and assets, to inform the implementation of risk management plans that deliver a more resilient organisation.

Brief outline:
This is about individuals contributing to providing risk assessments. This involves establishing the risk management context, identifying and treating the risks faced by the organisation.

Performance requirements

1. Identifying information assets to prepare for risk assessments
2. Planning risk assessments at periodic intervals and when significant change occurs
3. Contributing to risk assessments of information systems using recognised risk assessment methodologies
4. Contributing to risk assessment of governance processes and associated policies and documentation
5. Identifying, categorising, and evaluating security risks to prepare for responses
6. Identifying which risks are within an organisation's risk appetite and which require treatment and mitigation
7. Identifying suitable security controls to mitigate risks
8. Recommending appropriate mitigations to reduce and remove identified risks
9. Implementing information risk management plans
10. Participating in walk-throughs for network infrastructures, applications, and systems, to identify and document key risks

Knowledge and understanding requirements

1. The principles of security risk assessment, risk management and business impact analysis
2. The information assets an organisation seeks to protect
3. The key properties used in information security when considering risk, including confidentiality, integrity, and availability
4. How to perform basic risk assessments
5. Relevant risk assessment methodologies and how to apply them
6. How risk assessments are used to fully understand the number and extent of risks faced by the organisation
7. What risk appetite is and how this varies across different sectors
8. The current risk appetite of the organisation with respect to cyber security
9. What constitutes 'risk' in relation to exploiting vulnerabilities that can impact business operations
10. Approaches to risk treatment and how to apply them

11. Communicating risk assessments and mitigation outcomes to ensure serious risks are flagged to senior management and other relevant stakeholders

11. What controls are taken to treat risks, and the different types of controls that may be required in treating particular risks
12. The ‘cyber security posture’ of the organisation, and how this may contribute to security risks
13. The externally recognised cyber security standards used in cyber security risk assessment
14. The role of the risk owner contrasted with other stakeholders

Work Situation

Contributing to intrusion detection activities

URN: SDS 014

Goal of work situation:
To identify and investigate suspicious activities and take appropriate actions to remediate threats in line with organisational requirements.

Brief outline:
This is about individuals monitoring network and system activity to detect and identify potential intrusion or other anomalous behaviour. This will involve analysing intrusion information to qualify events and initiating appropriate responses, escalating as necessary.

Performance requirements

1. Performing basic configuration of automated tools, including network monitoring and analysis tools, analytic tools, correlation tools, automation platforms and network analysers
2. Monitoring network and system activity to identify potential intrusion or other anomalous behaviour
3. Observing trends and patterns to identify anomalies
4. Analysing monitoring information, including alerts and advisories supplied by alarms
5. Responding to true threats and initiating appropriate responses, escalating as necessary
6. Performing root cause analysis of intrusion events and making recommendations to reduce false positives and negatives
7. Reporting on intrusion detection activities to appropriate audiences

Knowledge and understanding requirements

1. How to operate effectively within intrusion detection and analysis teams and the importance of this
2. The need for intrusion detection and analysis to maintain information security
3. The function and features of the main network components
4. IT network features and functions including virtual networking the OSI TCP and IP protocols and models
5. The main features of a standard operating network layer
6. The difference between intrusion prevention and intrusion detection
7. The basic principles involved in monitoring network and system activity for anomalous behaviour
8. The role of intrusion detection systems and alarms and how to recognise and respond to alarms and alerts
9. Industry standard automated network monitoring tools including Secure Information and Event Management (SIEM) tools and how to apply them
10. How to configure and tune automated SOC tools including SIEM and network monitoring tools

11. The threat landscape including current and emerging trends
12. How to use intrusion information to make effective decisions on how to respond to intrusion events
13. The mitigations that can be recommended for new intrusions and anomalies
14. The escalation steps, how to escalate intrusion events, who to escalate to and when
15. How to communicate intrusion events and the types of reporting required for different audiences
16. The importance of keeping up to date with latest intrusion trends in industry

Work Situation

URN: SDS 027

Providing incident management and response

Goal of work situation:
To accurately detect and deal with cyber and information security incidents in line with organisational incident management processes.

Brief outline:
This is about individuals acting as first responders to security incidents in line with the organisation's incident management process. This will involve ensuring that incidents are handled appropriately and escalate where required.

Performance requirements

1. Performing basic configuration of automated tools, including network monitoring and analysis tools, analytic tools, correlation tools, automation platforms and network analysers
2. Monitoring network and system activities to identify potential intrusion and other anomalous behaviour
3. Observing trends and patterns to identify anomalies
4. Analysing and monitoring information, including alerts and advisories supplied by alarms
5. Responding to true threats and initiating appropriate responses, escalating as necessary
6. Performing root cause analysis of intrusion events
7. Making recommendations to reduce false positives and negatives
8. Reporting on intrusion detection activities in ways appropriate to different audiences

Knowledge and understanding requirements

1. How to operate effectively within intrusion detection and analysis teams, and the importance of this
2. The need for intrusion detection and analysis to maintain information security
3. The function and features of the main network components
4. IT network features and functions including virtual networking the OSI (Open Systems Interconnection) and TCP/IP (Transmission Control Protocol/Internet Protocol) models
5. The main features of a normal operating network layer
6. The difference between intrusion prevention and intrusion detection
7. The basic principles involved in monitoring network and system activity for anomalous behaviour
8. The role of intrusion detection systems and alarms and how to recognise and respond to alarms and alerts
9. Industry standard automated network monitoring tools including SIEM (Secure Information and Event Management) tools and how to apply them
10. How to configure and tune automated SOC (Security Operations Centre) tools including SIEM and network monitoring tools

11. The threat landscape including current and emerging trends
12. The importance of thorough situational awareness, and the ways this relies on having information and understanding available to make good decisions
13. The mitigations that can be recommended for new intrusions and anomalies
14. The escalation process, including how to escalate intrusion events, who to escalate to and when
15. How to communicate intrusion events and the types of reporting required for different audiences
16. The importance of keeping up to date with latest intrusion trends in industry

Work Situation

URN: SDS 028

Supporting security audit and compliance checking

Goal of work situation:
To provide support to security audit and compliance activities, to help ensure that the organisation complies with internal policies and legal and regulatory requirements.

Brief outline:
This is about individuals verifying that information systems and processes meet security criteria (requirements or policy, standards, and procedures). It also involves ensuring conformance with internal and external requirements.

Performance requirements

1. Supporting the implementation and operation of the organisational cyber security policies, procedures, processes, and controls ensuring compliance with those requirements
2. Contributing to security audits under supervision
3. Verifying that information systems and processes meet specified security criteria (requirements or policy, standards, and procedures)
4. Carrying out security compliance checks in accordance with an appropriate methodology
5. Reporting the findings from information security audit and compliance checking activities
6. Contributing to the review and communication of the audit results to stakeholders
7. Assisting with planning activities to remediate any issues resulting from any particular information security audit

Knowledge and understanding requirements

1. The concepts and benefits of security management systems, governance, national and international standards
2. The basic principles of information security governance and how it applies within an organisation
3. The governance roles, policies, standards, and guidelines for cyber security and how they work together to deliver identified security outcomes
4. The overall process of an audit and the requirements for, and basic principles involved in conducting security audits of information systems
5. How to collect and analyse audit information
6. The need to consider Cloud environments when undertaking security audits and compliance checks
7. The benefits of compliance monitoring and the common compliance monitoring standards
8. The importance of demonstrating adherence to the legal, regulatory, compliance and standards environment within which the business operates
9. The difference between ‘trusted’ and ‘trustworthy’ and the role of assurance in cyber security
10. The potential impacts that occur where information governance alignment has not been observed

Optional Work Situations

A minimum of one optional work situation must be achieved.

Work Situation

Delivering threat intelligence

URN: SDS 017

Goal of work situation:
To identify, analyse and aggregate threat information to provide trusted actionable intelligence to inform strategic decision-making in line with organisational requirements.

Brief outline:
This is about individuals assessing and validating information from identified sources on current and potential security threats to the organisation. This will involve analysing significant trends and identifying potential threat agents and their capabilities, to highlight security issues relevant to the organisation and maintain 'situational awareness'.

Performance requirements

1. Identifying external sources of threat intelligence and advice including using third party and open sources
2. Contributing to threat intelligence gathering tasks through validating and consulting external sources of threat data
3. Discovering, identifying, and analysing new threats and attack techniques, to produce prioritised threat lists
4. Monitoring and detecting potential security threats in IT systems and escalating them in accordance with organisational procedures
5. Correlating threat information from a variety of sources, which are presented in a range of formats, to validate threats
6. Prioritising threats to an organisation and their methods of attack
7. Identifying and categorising threats in preparation for mitigation responses
8. Developing recommendations for mitigations against validated threats
9. Producing threat intelligence reports appropriate to the audience

Knowledge and understanding requirements

1. The concepts of threats, vulnerabilities, and assurance
2. The threats, vulnerabilities, impacts and mitigations in information systems and the enterprise environment
3. The principles of threat intelligence, modelling and assessment
4. The principles and methodologies for conducting threat intelligence gathering and analysis
5. The trusted sources of threat intelligence, including third party and open source
6. How to undertake threat identification using network reconnaissance techniques
7. Threat data collection and acquisition techniques and how to apply them
8. How to undertake routine threat intelligence tasks and threat assessments
9. How to identify and develop mitigations against threats
10. Ways in which threat modelling can be used to developing attack trees

and perform impact assessments

11. How threat intelligence informs threat modelling activities
12. Commercial and open-source threat intelligence and modelling tools and how to apply them
13. How do develop threat intelligence reports for different audiences

Work Situation

URN: SDS 015

Contributing to scoping and implementing security testing

Goal of work situation:
To test the security of systems to identify vulnerabilities or potential exploits of critical systems and sensitive data through conducting vulnerability assessments and penetration testing in line with organisational requirements.

Brief outline:
This is about individuals contributing to the scoping and conduct of vulnerability assessments and penetration testing for potential; exploits against networks and infrastructures, web applications, mobile devices, and control systems. This also involves contributing to the review and interpretation of testing reports.

Performance requirements

1. Contributing to the scoping of vulnerability assessments and tests for public domain vulnerabilities to assess the potential for exploitation
2. Testing network infrastructure domains, including end user devices, with static and dynamic routes, to given requirements
3. Performing penetration exploits as part of simulated attack exercises
4. Providing evidence that the system meets design requirements
5. Discovering vulnerabilities in a system through a mix of research and practical exploration
6. Identifying common vulnerabilities in an organisations network infrastructure, applications, and systems
7. Conducting impact assessments to determine the prioritisation of vulnerabilities identified
8. Reporting potential issues in line with procedures and making recommendations on remediations and mitigation options

Knowledge and understanding requirements

1. The main security concepts including security, identity, confidentiality, integrity, availability, threat, vulnerability, risk
2. The purpose of security testing, and how it contributes to assurance of information systems and data
3. The different types of security testing and the difference between vulnerability assessments and penetration tests
4. The principles of penetration testing and the common types of penetration tests for infrastructure and application testing domains
5. Security testing objectives, approaches and methodologies
6. The types and purposes of security testing tools
7. How to select security testing tools
8. How to conduct network infrastructure testing for security issues and vulnerabilities
9. How to test applications for security issues and vulnerabilities
10. Why security testing cannot guarantee security

11. The common vulnerabilities in network infrastructures, applications, and systems
12. The impact of vulnerabilities and how they are ranked and prioritised
13. How vulnerabilities are mitigated and how to propose appropriate responses to current and new vulnerabilities relevant to network infrastructure and business environments

Work Situation

Maintaining security operations

URN: SDS 023

Goal of work situation:

To implement security controls in response to threat and vulnerability analysis to maintain security within the organisations level of risk appetite.

Brief outline:
This is about individuals contributing to the scoping and conduct of vulnerability assessments and penetration testing for potential; exploits against networks and infrastructures, web applications, mobile devices, and control systems. This also involves contributing to the review and interpretation of testing reports.

Performance requirements

1. Identifying and reviewing cyber security business requirements
2. Implementing organisational processes for maintaining the security of information including security operating procedures, security policies and standards in respect of system and network management
3. Assessing and responding to new technical, physical, personnel and procedural vulnerabilities
4. Analysing security control needs to mitigate identified vulnerabilities
5. Identifying and implementing security controls in line with organisational policies and procedures
6. Maintaining security controls in line with organisational policies and procedures
7. Monitoring security tools, including threat and vulnerability databases, to analyse and react to new risks across organisational network infrastructure, applications, and systems
8. Maintaining patch management, firewall and anti-malware update plans
9. Liaising with system owners to ensure the timely roll out of patches in line with plans

Knowledge and understanding requirements

1. The need for secure management of information systems and the types of incidents which could occur if this is not done
2. The main processes for managing the security of information systems
3. The need for information systems and services to be operated securely and the main policies and practices involved in achieving this
4. How group policy is used to manage the working environment of user and system accounts, including how these work
5. How to select and implement controls to meet cyber security requirements
6. The main Operating System (OS) security functions and associated features
7. The range of anti-virus and anti-malware protections and how to apply and maintain them
8. The role of cyber security culture in maintaining cyber security resilience
9. The legal and regulatory requirements including General Data Protection Regulation (GDPR), International Safety Management (ISM)

10. Conducting impact analysis of proposed patches, firewall and anti-malware updates and maintain up-to-date road maps
11. Planning, developing, and delivering security awareness training to end users
12. Implementing endpoint protection policies, including open USB ports
13. Implementing business continuity management, data backup and recovery in line with organisational policies and procedures

and cyber security frameworks and the importance of following these
10. How to integrate cyber security controls within existing network infrastructures and business systems
11. The potential risk from insider threats
12. The implications of hidden mistakes
13. What types of threats are derived from malicious intent and can occur due to inadvertent mistakes
14. The sources of patch update intelligence and how to use these
15. The patch management, vulnerability management, and risk assessment processes and how to use them
16. The potential risks from supply chains
17. The risks associated with poor endpoint protection and open USB ports
18. How to perform backup and recovery tests

Work Situation

URN: SDS 025

Performing digital forensic analysis

Goal of work situation:
To secure the scene, investigate and capture evidence maintaining evidential weight and analyse the evidence to identify breaches of policy, regulation, or law in line with legislative and organisational requirements.

Brief outline:
This is about individuals undertaking forensic tasks as a first responder. This involves maintaining the chain of custody, and using specialist tools to recover, preserve and analyse data to provide a full investigation capability.

Performance requirements

1. Assessing the need for forensic activities
2. Engaging with relevant organisational processes to ensure forensic activities are appropriately deployed
3. Securing scenes and capturing evidence in accordance with legal guidelines and organisational policies to minimise disruption to business and maintain evidential weight
4. Applying forensic techniques to identify sources of evidence on different devices (including fixed and mobile)
5. Using open source and commercial digital forensic tools to acquire digital evidence
6. Using open source and commercial digital forensic tools to analyse digital evidence and identify breaches of policy, regulation, or law, including the presence of malware
7. Documenting and presenting evidence in line with organisational requirements
8. Acting as an expert witness, where required, to corroborate that the items of digital evidence collected at the crime scene are the same evidence that is being presented in a court of law

Knowledge and understanding requirements

1. The principles of digital forensics and the importance of ensuring evidence is not contaminated
2. The capability of forensics to support investigations
3. What is meant by chain of custody in preserving the probative value of evidence
4. The importance of following the organisation's Forensics Readiness Plan
5. Possible sources of digital forensic information
6. The processes, procedures, techniques, and tools used to recover and preserve digital evidence and conduct digital forensic analysis
7. The main stages of a digital forensics process including:
    a. identifying the material to be investigated
    b. seizing the media in a forensically secure manner
    c. acquiring a forensic image of the media for examination
    d. analysing the forensic image of original media ensuring this is not modified during analysis
8. The purpose of Forensics Readiness Plans
9. The architectures of digital systems and devices including hardware,

software, networked and cloud environments, fixed endpoint, and mobile devices

10. The volatile nature of data
11. Hard disk file structures including FAT32 (File Allocation Table 32) file system and NFS (Network File System) and SSD (Solid State Drive) access
12. The ways hashing is used to verify that data is not modified, tampered with, or corrupted
13. Relevant legislation and guidance, including the Data Protection Act (DPA) and Regulation of Investigatory Powers Act (RIPA)

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 methods and principles of project management	✓	✓	✓		✓			✓		✓		
Supporting digital business transformation	✓		✓		✓			✓				
Developing meta-skills and personal professionalism	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Contributing to cyber security risk assessment and risk management		✓	✓		✓			✓				
Contributing to intrusion detection activities	✓	✓	✓		✓			✓				✓
Contributing to scoping and implementing security testing	✓	✓	✓		✓	✓		✓		✓		
Delivering threat intelligence	✓		✓	✓	✓	✓	✓	✓	✓	✓		✓
Maintaining security operations	✓				✓	✓			✓		✓	
Performing digital forensic analysis		✓	✓		✓				✓	✓		
Providing incident management and response	✓				✓			✓				✓
Supporting security audit and compliance checking		✓						✓		✓		

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 methods and principles of project management	• Project management suite • Engineering and Manufacturing suite 4 • Engineering Leadership and Manufacture suite 4 • Industrial Design Suite	• Maintain IT project-based documentation TECIS30131 • Initiate an IT project TECIS30141 • Develop an IT project management plan TECIS30142	• Monitor and control the delivery of an IT project TECIS30143 • Close and review an IT project TECIS30144 • Manage risks in an IT project TECIS30145
Supporting digital business transformation	• Carry out business process design and improvement assignments ESKITP2024.03	• Assist in the design, implementation and maintenance of change management plans and assignments ESKITP2034.03	• Use safe and secure practices when working with digital systems ESKITU040
Developing meta-skills and personal professionalism	• Business and Administration suite • Management and Leadership suite		
Contributing to cyber security risk assessment and risk management	• Contribute to risk assessment and management activities TECIS60231 • Carry out risk assessment and management activities TECIS60241		
Contributing to intrusion detection activities	• Assisting with monitoring network activity for anomalous behaviour TECIS610301 • Carry out intrusion detection and analysis TECIS610401		
Contributing to scoping and implementing security testing	• Contribute to identifying threats and attacks for security testing TECIS60431 • Carry out security testing activities TECIS60441		
Delivering threat intelligence	• Contribute to routine threat intelligence tasks TECIS609301 • Carry out threat intelligence assessments TECIS609401		
Maintaining security operations	• Contribute to operational security management activities TECIS60531 • Carry out operational security management activities TECIS60541 • Contribute to identity and access management activities TECIS60533		
Performing digital forensic analysis	• Contribute to digital forensic examinations TECIS60633 • Carry out digital forensic examinations TECIS60643		
Providing incident management and response	• Contribute to incident investigation and management activities TECIS60632 • Carry out incident investigation and management activities TECIS60642		
Supporting security audit and compliance checking	• Contribute to audit, compliance and assurance activitiesTECIS60731 • Carry out audit, compliance and assurance activities TECIS60741		