Cyber Security

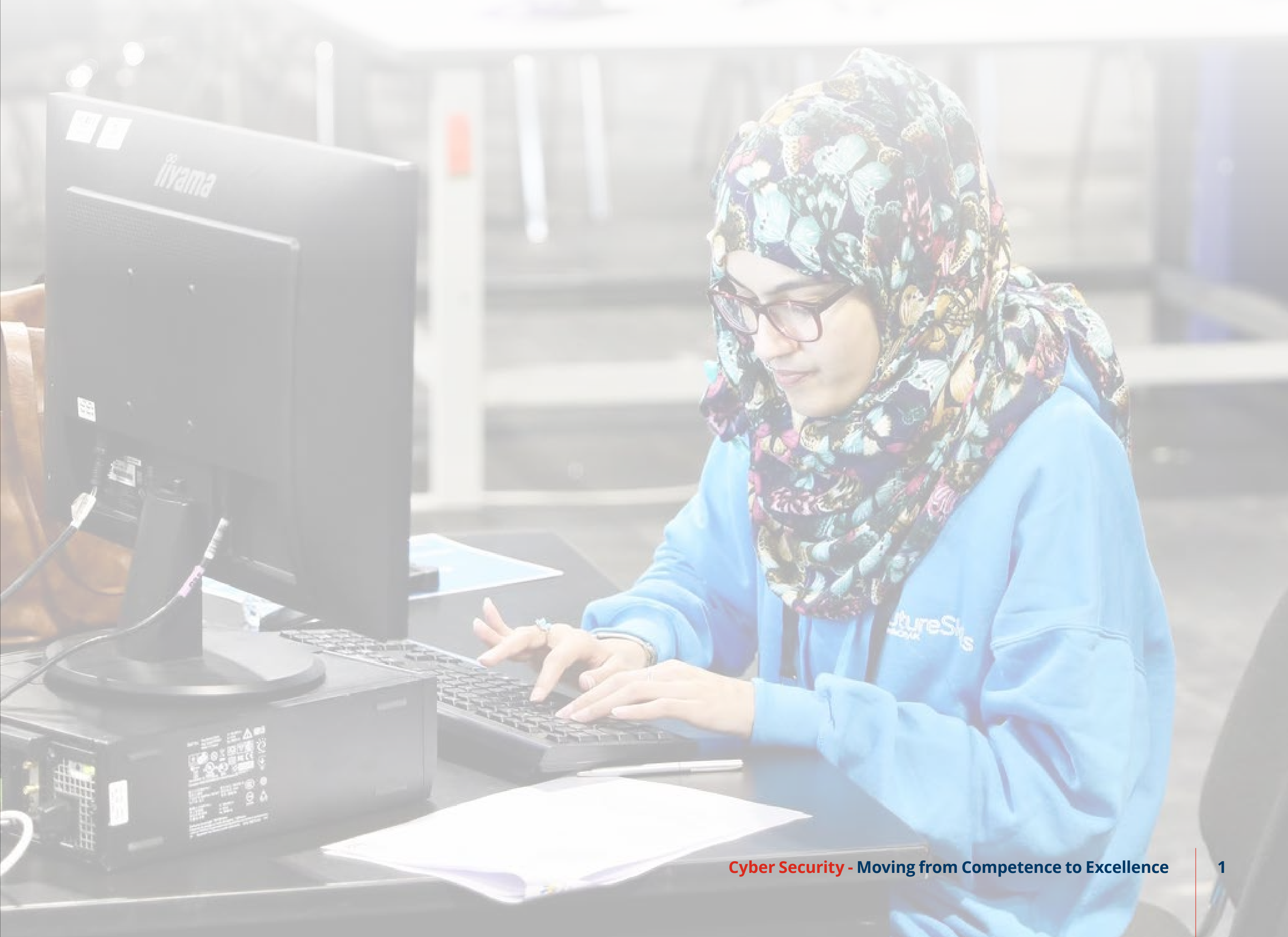
Section one

Moving from Competence to Excellence

A closer look at two key aspects of the Cyber Security World Occupational Standard.

Aspect:	Total number of Marks (%)
A: Secure systems operation and maintenance	15
B: Investigation and Digital Forensics	15

The WorldSkills Occupational Standard (WSOS) specifies the knowledge, understanding, and specific skills that underpin international best practice in technical and vocational performance. It should reflect a shared global understanding of what the associated work role(s) or occupation(s) represent for industry and business.



A: Secure systems operation and maintenance

What does competence look like in this area?

The cybersecurity field requires a combination of technical expertise, operational efficiency, best practices and effective communication to ensure secure system operation and maintenance.

Technical Competence: The competitor possesses a deep understanding of operating systems, network architecture, security tools, configuration and hardening skills and is proficient in patch management and ensuring systems are up-to-date with the latest security updates.

Operational Efficiency: The competitor is proficient in monitoring unusual activity, analysing logs, identifying compromise indicators, detecting and responding to incidents, using forensic techniques, implementing robust backup solutions and executing disaster recovery plans.

Adherence to Best Practices and Compliance: The competitor is proficient in implementing security frameworks, risk management, and documentation, ensuring systems comply with organisational policies and regulatory requirements, conducting thorough risk assessments and generating actionable reports for stakeholders.

Soft Skills: Actively addresses security incidents, innovates, and adapts to emerging threats, continuously improving through professional development and a proactive approach to learning and applying new measures.

What does excellence look like in this area?

Excellence in cybersecurity involves mastering advanced skills, implementing cutting-edge technologies and demonstrating leadership in secure system operation and maintenance.

Advanced Technical Mastery: The competitor possesses extensive knowledge of operating systems and network configurations, is proficient in deploying and managing advanced security tools, is skilled in using SIEM tools for real-time monitoring and threat detection and masters automated configuration management tools.

Superior Operational Capabilities: The competitor utilises advanced monitoring tools and threat intelligence platforms to identify and mitigate threats, integrates them into security operations, leads expert incident response and forensic investigations, designs reliable backup solutions, and implements advanced disaster recovery plans.

Leadership in Best Practices and Compliance: The competitor contributes to industry security standards development, ensures compliance with regulations, and prepares for future changes. They conduct comprehensive risk assessments, develop strategic mitigation plans, and maintain detailed documentation of security policies and procedures.

Advanced Soft Skills and Continuous Improvement: The competitor applies innovative solutions to complex security challenges, continuously assesses and refines these methods and is committed to lifelong learning through advanced certifications and active participation in the cybersecurity community.

B: Investigation and Digital Forensics

What does competence look like in this area

Competence in investigation and digital forensics requires technical skills, methodical procedures, and a deep understanding of legal and ethical considerations.

Technical Competence: The competitor possesses proficiency in forensic tools, data acquisition techniques, file systems, network forensics, malware analysis and network traffic analysis. They are proficient in analysing file systems, recovering deleted files, tracing network-based attacks and using tools like Wireshark, tcpdump, and NetworkMiner for packet analysis.

Methodical Procedures: The competitor possesses expertise in evidence handling, incident response and documentation, as well as a strong understanding of legal requirements and incident response frameworks. They are proficient in maintaining a chain of custody, providing forensic support and writing comprehensive reports.

Legal and Ethical Considerations: Legal frameworks, jurisdictional issues and ethical conduct are crucial in digital forensics, ensuring objectivity and impartiality in analysis and reporting.

Communication and Collaboration: Effective communication, team collaboration and expert testimony are essential skills for presenting complex technical findings to non-technical stakeholders and collaborating with multidisciplinary teams.

What does excellence look like in this area?

To demonstrate excellence in investigation and digital forensics, mastering fundamental skills, demonstrating advanced capabilities, demonstrating leadership and continuously innovating are required.

Advanced technical expertise: The competitor possesses proficiency in various forensic tools, advanced data acquisition techniques, and a deep understanding of complex systems. They can handle advanced scenarios like cloud and IoT forensics. They also have advanced skills in malware analysis and custom tool development.

Methodological Excellence: The competitor demonstrates rigorous evidence handling protocols, employs advanced evidence integrity techniques, leads incident response efforts, and produces comprehensive forensic reports. They are adept at coordinating and executing investigations, refining response plans and tailoring reports to different audiences.

Legal and ethical leadership: Expert knowledge of legal frameworks, credible court testimony and upholding ethical conduct are key qualities of a digital forensics professional who guides junior analysts in ethical practices.

Communication and influence: Exceptional communication skills, including articulating complex technical concepts, providing expert analysis and leading cross-functional teams in forensic investigations, are crucial for effective decision-making and policy development.