INFORMATION AND COMMUNICATION TECHNOLOGY

Cyber Security

WorldSkills Occupational Standards

worldskills

WorldSkills Occupational Standards (WSOS)

General notes on the WSOS

The 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 (www.worldskills.org/WSOS).

The skill competition is intended to reflect international best practice as described by the WSOS, and to the extent that it is able to. The Standard is therefore a guide to the required training and preparation for the skill competition.

In the skill competition the assessment of knowledge and understanding will take place through the assessment of performance. There will only be separate tests of knowledge and understanding where there is an overwhelming reason for these.

The Standard is divided into distinct sections with headings and reference numbers added.

Each section is assigned a percentage of the total marks to indicate its relative importance within the Standards. This is often referred to as the "weighting". The sum of all the percentage marks is 100. The weightings determine the distribution of marks within the Marking Scheme.

Through the Test Project, the Marking Scheme will assess only those skills that are set out in the Standards Specification. They will reflect the Standards as comprehensively as possible within the constraints of the skill competition.

The Marking Scheme will follow the allocation of marks within the Standards to the extent practically possible. A variation of up to five percent is allowed, provided that this does not distort the weightings assigned by the Standards.

WorldSkills Occupational Standards

Section		Relative importance (%)
1	**Work organization and management**	5

The individual needs to know and understand:

- Health and safety legislation, obligations, regulations, and documentation
- The situations when personal protective equipment (PPE) must be used, e.g. for ESD (electrostatic discharge)
- The importance of integrity and security when dealing with user equipment and information
- The importance of safe disposal of waste for re-cycling
- The techniques of planning, scheduling, and prioritizing
- The significance of accuracy, checking, and attention to detail in all working practices
- The importance of methodical working practices

The individual shall be able to:

- Follow health and safety standards, rules, and regulations
- Maintain a safe working environment
- Identify and use the appropriate Personal Protective Equipment for ESD
- Select, use, clean, maintain, and store tools and equipment safely and securely
- Plan the work area to maximize efficiency and maintain the discipline of regular tidying
- Work efficiently and check progress and outcomes regularly
- Keep up-to-date with 'license to practice' requirements and maintain currency
- Undertake thorough and efficient research methods to support knowledge growth
- Proactively try new methods, systems, and embrace change

2	**Communication and interpersonal skills**	10

The individual needs to know and understand:

- The importance of listening as part of effective communication
- The roles and requirements of colleagues and the most effective methods of communication
- The importance of building and maintaining productive working relationships with colleagues and managers
- Techniques for effective teamwork
- Techniques for resolving misunderstandings and conflicting demands
- The process for managing tension and anger to resolve difficult situations
- Requirements for the complete documentation of steps taken in cyber security investigations and the resulting discoveries

Section		Relative importance (%)
	The individual shall be able to: • Use strong listening and questioning skills to deepen understanding of complex situations • Ensure consistently effective verbal and written communications with colleagues • Recognize and adapt to the changing needs of colleagues • Proactively contribute to the development of strong and effective teams • Share knowledge and expertise with colleagues and develop supportive learning cultures • Manage tension/anger and give individuals confidence that their problems can be resolved • Accurately document steps taken and findings in the course of investigations • Ensure policies and procedures for security and operation on information systems are carefully followed	
3	**Secure systems design and creation**	**10**
	The individual needs to know and understand: • IT risk management standards, policies, requirements, and procedures • Cyber defence and vulnerability assessment tools and their capabilities. • Operating Systems • Network systems • Computer programming concepts, including computer languages, programming, testing, debugging, and file types • The cyber security and privacy principles and methods that apply to software development	
	The individual shall be able to: • Apply cyber security and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation) when designing and documenting overall program Test & Evaluation procedures. • Conduct independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by information technology (IT) systems to determine the overall effectiveness of controls • Develop and conduct assessments of systems to evaluate compliance with specifications and requirements • Secure the interoperability of systems or elements of systems incorporating IT • Modify existing computer applications, software, or specialized utility programs • Analyse the security of new or existing computer applications, software, or specialized utility programs, to provide actionable results • Develop and maintain business, systems, and information processes, to support enterprise mission needs	

Section		Relative importance (%)
	• Develop information technology (IT) rules and requirements that describe baseline and target architectures • Ensure that stakeholder security requirements necessary to protect the organization's mission and business processes are adequately addressed in all aspects of enterprise architecture, including reference models, segment and solution architectures, and the resulting systems supporting those missions and business processes • Conduct software and systems engineering and software systems research to develop new capabilities, ensuring cyber security is fully integrated. • Conduct research (including penetration testing) to evaluate potential vulnerabilities in cyberspace systems • Consult with stakeholders to evaluate functional requirements and translate functional requirements into technical solutions • Plan, prepare, and execute tests of systems • Analyse, evaluate and report results against specifications and requirements • Design, develop, test, and evaluate information system security throughout the systems development life cycle	
4	**Secure systems operation and maintenance**	**15**
	The individual needs to know and understand: • Query languages such as SQL (structured query language) and Database Systems. • Network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services. • Firewall concepts and functions (e.g., Single point of authentication/audit/policy enforcement, message scanning for malicious content, data anonymization for PCI and PII compliance, data loss protection scanning, SSL security and REST/JSON processing). • Network security architecture concepts including topology, protocols, components, and principles. • Systems Administration, network, and operating system hardening techniques. • Organizational information technology (IT) user security policies (e.g., account creation, password rules, and access control). • Information technology (IT) security principles and methods. • Authentication, authorization, and access control methods. • Cyber security vulnerability and privacy principles	

Section		Relative importance (%)
	The individual shall be able to: • Install, configure, test, operate, maintain, and manage network infrastructure • manage software that permits the sharing and transmission of all data • Install, configure, troubleshoot, and maintain server configurations (hardware and software) to ensure their confidentiality, integrity, and availability • Manage accounts in relation to access control, passwords, account creation, and administration Analyse organizations' computer systems and update information systems solutions to help them operate more securely, efficiently, and effectively. • Develop methods to monitor and measure risk, compliance, and assurance efforts. • Conduct audits of information technology (IT) programs, infrastructure network to provide ongoing optimization, cyber security and problem-solving support	
5	**Secure systems protection and defence**	**15**
	The individual needs to know and understand: • File system implementations • System files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files • Network security architecture concepts including topology, protocols, components, and principles (e.g., application of defence-in-depth) • Industry-standard and organizationally accepted analysis principles, methods, and tools to identify vulnerabilities • Threat investigations, reporting, investigative tools, and laws/regulations • Incident categories, response, and handling methodologies • Cyber defence and vulnerability assessment tools and their capabilities • Countermeasure design for identified security risks • Authentication, authorization, and access approaches (e.g. role-based access control, mandatory access control and discretionary access control)	

Section		Relative importance (%)
	The individual shall be able to: • Use defensive measures and information collected from a variety of sources to identify, analyse, and report events that occur or might occur within the network to protect information, information systems, and networks from threats • Test, implement, deploy, maintain, review, and administer the infrastructure hardware and software that are required to effectively manage the computer network and resources • Monitor network to actively remediate unauthorized activities • Respond to crises or urgent situations within own areas of expertise to mitigate immediate and potential threats • Use mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security Investigate and analyse all relevant response activities • Conduct assessments of threats and vulnerabilities • Determine deviations from acceptable configurations, enterprise, or local policy • Assess the level of risk and develop and/or recommend appropriate mitigation countermeasures in operational and non-operational situations • Follow documented enterprise procedures for incident preparedness and response	
6	**Operations and Management**	20
	The individual needs to know and understand: • Cyber threat actors and their methods • Methods and techniques used to detect various exploitation activities • Cyber intelligence/information collection capabilities and repositories • Cyber threats and vulnerabilities • Basics of network security (e.g., encryption, firewalls, authentication, honey pots, perimeter protection) • Vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins) • Which system files (e.g., log files, registry files, and configuration files) contain relevant information and where to find those system files • Structure, approach, and strategy of exploitation tools (e.g., sniffers, keyloggers) and techniques (e.g., gaining backdoor access, collecting/exfiltrating data, conducting vulnerability analysis of other systems in the network) • Internal tactics to anticipate and/or emulate threat capabilities and actions • Internal and external partner cyber operations capabilities and tools • Target development (i.e., concepts, roles, responsibilities, products, etc.) • System Artefacts and forensic use cases • Emerging exploitation or threats as they apply to installed systems and software • Importance of preparedness for recovery in cases of natural disaster	

Section		Relative importance (%)
	The individual shall be able to: • Identify and assess the capabilities and activities of cyber security criminals or foreign intelligence entities • Produce findings to help initialize or support law enforcement and counterintelligence investigations or activities • Analyse collected information to identify vulnerabilities and potential for exploitation • Analyse threat information from multiple sources, disciplines, and agencies across the Intelligence Community • Synthesize and place intelligence information in context, draw insights about the possible implications • Apply current knowledge of one or more regions, countries, non-state entities, and/or technologies • Apply language, cultural, and technical expertise to support information collection, analysis, and other cyber security activities • Identify, preserve, and use system artefacts for analysis • Execute successful data and systems recovery in case of loss	
7	**Intelligence collection and analysis**	**10**
	The individual needs to know and understand: • Identify and assess the capabilities and activities of cyber security criminals or foreign intelligence entities • Produce findings to help initialize or support law enforcement and counterintelligence investigations or activities • Analyse collected information to identify vulnerabilities and potential for exploitation • Analyse threat information from multiple sources, disciplines, and agencies across the Intelligence Community • Synthesize and place intelligence information in context, draw insights about the possible implications • Apply current knowledge of one or more regions, countries, non-state entities, and/or technologies • Apply language, cultural, and technical expertise to support information collection, analysis, and other cyber security activities • Identify, preserve, and use system artefacts for analysis • Execute successful data and systems recovery in case of loss	

Section		Relative importance (%)
	The individual shall be able to: • Identify and assess the capabilities and activities of cyber security criminals or foreign intelligence entities • Produce findings to help initialize or support law enforcement and counterintelligence investigations or activities • Analyse collected information to identify vulnerabilities and potential for exploitation • Analyse threat information from multiple sources, disciplines, and agencies across the Intelligence Community • Synthesize and place intelligence information in context, draw insights about the possible implications • Apply current knowledge of one or more regions, countries, non-state entities, and/or technologies • Apply language, cultural, and technical expertise to support information collection, analysis, and other cyber security activities • Identify, preserve, and use system artefacts for analysis Execute successful data and systems recovery in case of loss	
8	**Investigation and Digital Forensics**	**15**
	The individual needs to know and understand: • Threat investigations, reporting, investigative tools and laws/regulations • Malware analysis concepts and methodologies • Processes for collecting, packaging, transporting, and storing electronic evidence while maintaining chain of custody • Types and collection of persistent data • Concepts and practices of processing digital forensic data • Types of digital forensics data and how to recognize them • Forensic implications of operating system structure and operations • Specific operational impacts of cyber security lapses	
	The individual shall be able to: • The individual shall be able to: • Collect, process, preserve, analyse, and present computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations	
	Total	**100**

References for industry consultation

WorldSkills is committed to ensuring that the WorldSkills Occupational Standards fully reflect the dynamism of internationally recognized best practice in industry and business. To do this WorldSkills approaches a number of organizations across the world that can offer feedback on the draft Description of the Associated Role and WorldSkills Occupational Standards on a two-yearly cycle.

In parallel to this, WSI consults three international occupational classifications and databases:

- ISCO-08: (http://www.ilo.org/public/english/bureau/stat/isco/isco08/) ILO 3512
- ESCO: (https://ec.europa.eu/esco/portal/home)
- O*NET Online (www.**onet**online.org/)

Your WSOS appears most closely to relate to an information *Security Analyst:*
https://www.onetonline.org/link/summary/15-1122.00

or an ICT Security Technician:
http://data.europa.eu/esco/occupation/a44a1dc5-be08-4840-8bd5-770c4ac1ca6d

Adjacent occupations can also be explored through these links.

The following table indicates which organizations were approached and provided valuable feedback for the Description of the Associated Role and WorldSkills Occupational Standards in place for WorldSkills Shanghai 2021.

Organization	Contact name
Keysight Technologies (Global)	Mateen Anis Padela, Senior Solutions Architect