WorldSkills Standards Specification

Cyber Security

Information and Communication Technology

worldskills

 WSC2019_WSSS54

THE WORLDSKILLS STANDARDS SPECIFICATION (WSSS)

GENERAL NOTES ON THE WSSS

The WSSS 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/WSSS).

The skill competition is intended to reflect international best practice as described by the WSSS, and to the extent that it is able to. The Standards Specification 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 Standards Specification 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 Specification. This is often referred to as the "weighting". The sum of all the percentage marks is 100.

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

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

WORLDSKILLS STANDARDS SPECIFICATION

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 team work • Techniques for resolving misunderstandings and conflicting demands • The process for managing tension and anger to resolve difficult situations	
	The individual shall be able to: • Use strong listening and questioning skills to deepen understanding of complex situations • Manage consistently effective verbal and written communications with colleagues • Recognize and adapt to the changing needs of colleagues • Proactively contribute to the development of a strong and effective team • Share knowledge and expertise with colleagues and develop a supportive learning culture • Effectively manage tension/anger and give individuals confidence that their problems can be resolved	
3	**Securely provision**	**15**
	The individual needs to know and understand: • The IT risk management standards, policies, requirements, and procedures. • Cyber defense and vulnerability assessment tools and their capabilities. • Operating Systems. • Computer programming concepts, including computer languages, programming, testing, debugging, and file types. • The cybersecurity and privacy principles and methods that apply to software development.	

	The individual shall be able to: • Apply cybersecurity 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 an information technology (IT) system to determine the overall effectiveness of the controls • Develop, create and maintain new computer applications, software, or specialized utility programs • 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 • Develop information technology (IT) rules and requirements that describe baseline and target architectures • Ensure that the 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 cybersecurity is fully integrated. • Conduct comprehensive technology research 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	Operate and maintain & oversee and govern	15
	The individual needs to know and understand: • Query languages such as SQL (structured query language) and Database Systems. • Data backup and recovery, administration and Data standardization policies. • 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, accelerated cryptographic operations, SSL security, REST/JSON processing). • Network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth). • Systems Administration, network, and operating system hardening techniques. • Organizational information technology (IT) user security policies (e.g., account creation, password rules, access control). • Information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption). • Authentication, authorization, and access control methods. • Cybersecurity, vulnerability and privacy principles. • Selective principles and processes for conducting training and education needs assessment. • Learning Management Systems and their use in managing learning. • Cyber competitions as a way of developing skills by providing hands-on experience in simulated, real-world situations. • Cyber laws and legal considerations and their effect on cyber planning	

	The individual shall be able to: • Develop and administer databases and/or data management systems that allow for the storage, query, protection, and utilization of data. • Manage and administer processes and tools that enable the organization to identify, document, and access intellectual capital and information content. • Address problems; install, configure, troubleshoot, and provide maintenance and training in response to customer requirements or inquiries • Install, configure, test, operate, maintain, and manage networks and their firewalls, including hardware and software that permit the sharing and transmission of all spectrum transmissions of information to support the security of information and information systems. • Install, configure, troubleshoot, and maintain server configurations (hardware and software) to ensure their confidentiality, integrity, and availability. • Manage accounts, firewalls, and patches. • Control access, passwords, and account creation and administration. • Review the organization's current computer systems and procedures in order to design information systems solutions to help the organization operate more securely, efficiently, and effectively. • Bring business and information technology (IT) together by responding to the needs and limitations of both. • Conduct training of personnel within own areas of expertise. • Develop, plan, coordinate, deliver and/or evaluate training courses, methods, and techniques within own areas of expertise. • Assist in the oversight of the cybersecurity program of an information system or network, including managing information security implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, requirements, policy enforcement, emergency planning, security awareness, and other resources. • Assist in the development of policies and plans and/or advocate changes in policy that support organizational cyberspace initiatives or required changes/enhancements. • Supervise, manage, and/or lead work and workers performing cyber and cyber- related and/or cyber operations work.	

5	**Protect and defend**	**15**
	The individual needs to know and understand: • File system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]). • 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 defense-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).	
	The individual shall be able to: • Use defensive measures and information collected from a variety of sources to identify, analyze, 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 defence service provider 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 analyze 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.	

6	Analyze	10
	The individual needs to know and understand: • Cyber threat actors, their equities 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, 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	
	The individual shall be able to: • Identify and assess the capabilities and activities of cybersecurity criminals or foreign intelligence entities • Produce findings to help initialize or support law enforcement and counterintelligence investigations or activities. • Analyze collected information to identify vulnerabilities and potential for exploitation. • Analyze 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 cybersecurity activities. • Identify, preserve, and use system artefacts for analysis	

7	**Collect and operate**	**15**
	The individual needs to know and understand: • Collection strategies, techniques, and tools. • Cyber intelligence/information collection capabilities and repositories. • Information needs and collection requirements are translated, tracked, and prioritized across the extended enterprise. • Required intelligence planning products associated with cyber operational planning. • Cyber operational planning programs, strategies, and resources. • Cyber operations strategies, resources and tools. • Cyber operations concepts, terminology/lexicon (i.e., environment preparation, cyber-attack, cyber defense), principles, capabilities, limitations, and effects.	
	The individual shall be able to: • Execute collection using appropriate strategies and within the priorities established through the collection management process. • Perform in-depth joint targeting and cybersecurity planning processes. • Gather information and develop detailed Operational Plans and Orders supporting requirements. • Assist strategic and operational-level planning across the full range of operations for integrated information and cyberspace operations. • Support activities to gather evidence on criminal or foreign intelligence entities to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or to support other intelligence activities.	
8	**Investigate**	**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. • The judicial process, including the presentation of facts and evidence. • 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 cybersecurity lapses.	
	The individual shall be able to: • Support senior personnel's work with a range of investigative tools and processes to include, but not limited to, interview and interrogation techniques, surveillance, counter surveillance, and surveillance detection. • Collect, process, preserve, analyze, 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 Standards Specifications 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 Standards Specification 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/)
- ESCO: (https://ec.europa.eu/esco/portal/home)
- O*NET OnLine (www.**oneto**nline.org/)