

Technical Description

# Cyber Security

Information and Communication Technology



WorldSkills International, by a resolution of the Competitions Committee and in accordance with the Constitution, the Standing Orders and the Competition Rules, has adopted the following minimum requirements for this skill for the WorldSkills Competition.

The Technical Description consists of the following:

<b>1 INTRODUCTION .....</b>	<b>2</b>
<b>2 THE WORLDSKILLS STANDARDS SPECIFICATION (WSSS) .....</b>	<b>4</b>
<b>3 THE ASSESSMENT STRATEGY AND SPECIFICATION .....</b>	<b>12</b>
<b>4 THE MARKING SCHEME .....</b>	<b>13</b>
<b>5 THE TEST PROJECT .....</b>	<b>16</b>
<b>6 SKILL MANAGEMENT AND COMMUNICATION .....</b>	<b>19</b>
<b>7 SKILL-SPECIFIC SAFETY REQUIREMENTS .....</b>	<b>20</b>
<b>8 MATERIALS AND EQUIPMENT .....</b>	<b>21</b>
<b>9 SKILL-SPECIFIC RULES .....</b>	<b>22</b>
<b>10 VISITOR AND MEDIA ENGAGEMENT .....</b>	<b>24</b>
<b>11 SUSTAINABILITY .....</b>	<b>25</b>

Effective 22 August 2018



Stefan Praschl  
Chair of the Competitions Committee



Michael Fung  
Vice Chair of the Competitions Committee

© WorldSkills International (WSI) reserves all rights in documents developed for or on behalf of WSI, including translation and electronic distribution. This material may be reproduced for non-commercial vocational and educational purposes provided that the WorldSkills logo and copyright notice are left in place.

# 1 INTRODUCTION

## 1.1 NAME AND DESCRIPTION OF THE SKILL COMPETITION

1.1.1 The name of the skill competition is

Cyber Security

1.1.2 Description of the associated work role(s) or occupation(s).

In recent years, we have witnessed an explosive growth of online business transactions, as well as rapid adoption of Internet of Things (IoT) and cloud computing. Coupled with the constant threat of hackers, cyber security professionals are now in great demand globally.

An Information Security Analyst works to protect an organization's computer systems networks, to prevent hackers from accessing and/or stealing sensitive information and data. The job of an Information Security Analyst typically involves installing firewalls and data encryption software to protect confidential information. They also monitor their organization's network for security breaches and investigate a violation when one occurs. Information Security Analysts may also conduct penetration testing, which is when they simulate attacks to look for vulnerabilities in their networks before they can be exploited.

Information Security Analysts are also often involved in designing and executing their organization's disaster recovery plan, which describes the steps and procedures to restore proper function of an organization's IT systems and networks after a disaster or attack. The plan usually includes preventive measures such as regular backing up of and transfer of data to an offsite location.

Information Security Analysts must keep themselves up-to-date to stay one step ahead of potential cyber-attackers. They need to be keep abreast of the latest methods attackers are using to infiltrate computer systems, as well as new security technologies that can help their companies counter these threats.

1.1.3 Number of Competitors per team

Cyber Security is a team skill with two Competitors in each team.

1.1.4 Age limit of Competitors

The Competitors must not be older than 25 years in the year of the Competition.

## 1.2 THE RELEVANCE AND SIGNIFICANCE OF THIS DOCUMENT

This document contains information about the standards required to compete in this skill competition, and the assessment principles, methods and procedures that govern the competition.

Every Expert and Competitor must know and understand this Technical Description.

In the event of any conflict within the different languages of the Technical Descriptions, the English version takes precedence.

## 1.3 ASSOCIATED DOCUMENTS

Since this Technical Description contains only skill-specific information it must be used in association with the following:

- WSI – Competition Rules
- WSI – WorldSkills Standards Specification framework
- WSI – WorldSkills Assessment Strategy
- WSI Online resources as indicated in this document
- WorldSkills Health, Safety, and Environment Policy and Regulations

## 2 THE WORLDSKILLS STANDARDS SPECIFICATION (WSSS)

### 2.1 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](http://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.

## 2.2 WORLDSKILLS STANDARDS SPECIFICATION

SECTION		RELATIVE IMPORTANCE (%)
<b>1</b>	<b>Work organization and management</b>	<b>5</b>
	<p>The individual needs to know and understand:</p> <ul style="list-style-type: none"> <li>• Health and safety legislation, obligations, regulations, and documentation</li> <li>• The situations when personal protective equipment (PPE) must be used, e.g. for ESD (electrostatic discharge)</li> <li>• The importance of integrity and security when dealing with user equipment and information</li> <li>• The importance of safe disposal of waste for re-cycling</li> <li>• The techniques of planning, scheduling, and prioritizing</li> <li>• The significance of accuracy, checking, and attention to detail in all working practices</li> <li>• The importance of methodical working practices</li> </ul>	
	<p>The individual shall be able to:</p> <ul style="list-style-type: none"> <li>• Follow health and safety standards, rules, and regulations</li> <li>• Maintain a safe working environment</li> <li>• Identify and use the appropriate Personal Protective Equipment for ESD</li> <li>• Select, use, clean, maintain, and store tools and equipment safely and securely</li> <li>• Plan the work area to maximize efficiency and maintain the discipline of regular tidying</li> <li>• Work efficiently and check progress and outcomes regularly</li> <li>• Keep up-to-date with 'license to practice' requirements and maintain currency</li> <li>• Undertake thorough and efficient research methods to support knowledge growth</li> <li>• Proactively try new methods, systems, and embrace change</li> </ul>	
<b>2</b>	<b>Communication and interpersonal skills</b>	<b>10</b>
	<p>The individual needs to know and understand:</p> <ul style="list-style-type: none"> <li>• The importance of listening as part of effective communication</li> <li>• The roles and requirements of colleagues and the most effective methods of communication</li> <li>• The importance of building and maintaining productive working relationships with colleagues and managers</li> <li>• Techniques for effective team work</li> <li>• Techniques for resolving misunderstandings and conflicting demands</li> <li>• The process for managing tension and anger to resolve difficult situations</li> </ul>	

	<p>The individual shall be able to:</p> <ul style="list-style-type: none"> <li>• Use strong listening and questioning skills to deepen understanding of complex situations</li> <li>• Manage consistently effective verbal and written communications with colleagues</li> <li>• Recognize and adapt to the changing needs of colleagues</li> <li>• Proactively contribute to the development of a strong and effective team</li> <li>• Share knowledge and expertise with colleagues and develop a supportive learning culture</li> <li>• Effectively manage tension/anger and give individuals confidence that their problems can be resolved</li> </ul>	
<b>3</b>	<b>Securely provision</b>	<b>15</b>
	<p>The individual needs to know and understand:</p> <ul style="list-style-type: none"> <li>• The IT risk management standards, policies, requirements, and procedures.</li> <li>• Cyber defense and vulnerability assessment tools and their capabilities.</li> <li>• Operating Systems.</li> <li>• Computer programming concepts, including computer languages, programming, testing, debugging, and file types.</li> <li>• The cybersecurity and privacy principles and methods that apply to software development.</li> </ul>	
	<p>The individual shall be able to:</p> <ul style="list-style-type: none"> <li>• Apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation) when designing and documenting overall program Test &amp; Evaluation procedures.</li> <li>• 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</li> <li>• Develop, create and maintain new computer applications, software, or specialized utility programs</li> <li>• Modify existing computer applications, software, or specialized utility programs</li> <li>• Analyse the security of new or existing computer applications, software, or specialized utility programs to provide actionable results</li> <li>• Develop and maintain business, systems, and information processes to support enterprise mission needs</li> <li>• Develop information technology (IT) rules and requirements that describe baseline and target architectures</li> <li>• 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</li> <li>• Conduct software and systems engineering and software systems research to develop new capabilities, ensuring cybersecurity is fully integrated.</li> </ul>	

	<ul style="list-style-type: none"> <li>• Conduct comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems</li> <li>• Consult with stakeholders to evaluate functional requirements and translate functional requirements into technical solutions</li> <li>• Plan, prepare, and execute tests of systems</li> <li>• Analyse, evaluate and report results against specifications and requirements</li> <li>• Design, develop, test, and evaluate information system security throughout the systems development life cycle</li> </ul>	
<b>4</b>	<b>Operate and maintain &amp; oversee and govern</b>	<b>15</b>
	<p>The individual needs to know and understand:</p> <ul style="list-style-type: none"> <li>• Query languages such as SQL (structured query language) and Database Systems.</li> <li>• Data backup and recovery, administration and Data standardization policies.</li> <li>• Network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.</li> <li>• 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).</li> <li>• Network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).</li> <li>• Systems Administration, network, and operating system hardening techniques.</li> <li>• Organizational information technology (IT) user security policies (e.g., account creation, password rules, access control).</li> <li>• Information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).</li> <li>• Authentication, authorization, and access control methods.</li> <li>• Cybersecurity, vulnerability and privacy principles.</li> <li>• Selective principles and processes for conducting training and education needs assessment.</li> <li>• Learning Management Systems and their use in managing learning.</li> <li>• Cyber competitions as a way of developing skills by providing hands-on experience in simulated, real-world situations.</li> <li>• Cyber laws and legal considerations and their effect on cyber planning</li> </ul>	
	<p>The individual shall be able to:</p> <ul style="list-style-type: none"> <li>• Develop and administer databases and/or data management systems that allow for the storage, query, protection, and utilization of data.</li> <li>• Manage and administer processes and tools that enable the organization to identify, document, and access intellectual capital and information content.</li> <li>• Address problems; install, configure, troubleshoot, and provide maintenance and training in response to customer requirements or inquiries</li> <li>• 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.</li> </ul>	



	<ul style="list-style-type: none"> <li>• Install, configure, troubleshoot, and maintain server configurations (hardware and software) to ensure their confidentiality, integrity, and availability.</li> <li>• Manage accounts, firewalls, and patches.</li> <li>• Control access, passwords, and account creation and administration.</li> <li>• 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.</li> <li>• Bring business and information technology (IT) together by responding to the needs and limitations of both.</li> <li>• Conduct training of personnel within own areas of expertise.</li> <li>• Develop, plan, coordinate, deliver and/or evaluate training courses, methods, and techniques within own areas of expertise.</li> <li>• 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.</li> <li>• Assist in the development of policies and plans and/or advocate changes in policy that support organizational cyberspace initiatives or required changes/enhancements.</li> <li>• Supervise, manage, and/or lead work and workers performing cyber and cyber- related and/or cyber operations work.</li> </ul>	
<b>5</b>	<b>Protect and defend</b>	<b>15</b>
	<p>The individual needs to know and understand:</p> <ul style="list-style-type: none"> <li>• File system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]).</li> <li>• System files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files.</li> <li>• Network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).</li> <li>• Industry-standard and organizationally accepted analysis principles, methods and tools to identify vulnerabilities.</li> <li>• Threat investigations, reporting, investigative tools and laws/regulations.</li> <li>• Incident categories, response and handling methodologies.</li> <li>• Cyber defence and vulnerability assessment tools and their capabilities.</li> <li>• Countermeasure design for identified security risks.</li> <li>• Authentication, authorization and access approaches (e.g. role-based access control, mandatory access control and discretionary access control).</li> </ul>	
	<p>The individual shall be able to:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Test, implement, deploy, maintain, review, and administer the infrastructure hardware and software that are required to effectively</li> </ul>	

	<p>manage the computer network defence service provider network and resources.</p> <ul style="list-style-type: none"> <li>• Monitor network to actively remediate unauthorized activities.</li> <li>• Respond to crises or urgent situations within own areas of expertise to mitigate immediate and potential threats.</li> <li>• Use mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security.</li> <li>• Investigate and analyze all relevant response activities.</li> <li>• Conduct assessments of threats and vulnerabilities</li> <li>• Determine deviations from acceptable configurations, enterprise or local policy</li> <li>• Assess the level of risk and develop and/or recommend appropriate mitigation countermeasures in operational and non-operational situations.</li> </ul>	
<b>6</b>	<b>Analyze</b>	<b>10</b>
	<p>The individual needs to know and understand:</p> <ul style="list-style-type: none"> <li>• Cyber threat actors, their equities and their methods.</li> <li>• Methods and techniques used to detect various exploitation activities.</li> <li>• Cyber intelligence/information collection capabilities and repositories.</li> <li>• Cyber threats and vulnerabilities.</li> <li>• Basics of network security (e.g., encryption, firewalls, authentication, honey pots, perimeter protection).</li> <li>• Vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).</li> <li>• Which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files.</li> <li>• 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).</li> <li>• Internal tactics to anticipate and/or emulate threat capabilities and actions.</li> <li>• Internal and external partner cyber operations capabilities and tools.</li> <li>• Target development (i.e., concepts, roles, responsibilities, products, etc.)</li> <li>• System Artefacts and forensic use cases</li> </ul>	
	<p>The individual shall be able to:</p> <ul style="list-style-type: none"> <li>• Identify and assess the capabilities and activities of cybersecurity criminals or foreign intelligence entities</li> <li>• Produce findings to help initialize or support law enforcement and counterintelligence investigations or activities.</li> <li>• Analyze collected information to identify vulnerabilities and potential for exploitation.</li> <li>• Analyze threat information from multiple sources, disciplines, and agencies across the Intelligence Community.</li> <li>• Synthesize and place intelligence information in context; draw insights about the possible implications.</li> <li>• Apply current knowledge of one or more regions, countries, non-state entities, and/or technologies.</li> </ul>	

	<ul style="list-style-type: none"> <li>• Apply language, cultural, and technical expertise to support information collection, analysis, and other cybersecurity activities.</li> <li>• Identify, preserve, and use system artefacts for analysis</li> </ul>	
<b>7</b>	<b>Collect and operate</b>	<b>15</b>
	<p>The individual needs to know and understand:</p> <ul style="list-style-type: none"> <li>• Collection strategies, techniques, and tools.</li> <li>• Cyber intelligence/information collection capabilities and repositories.</li> <li>• Information needs and collection requirements are translated, tracked, and prioritized across the extended enterprise.</li> <li>• Required intelligence planning products associated with cyber operational planning.</li> <li>• Cyber operational planning programs, strategies, and resources.</li> <li>• Cyber operations strategies, resources and tools.</li> <li>• Cyber operations concepts, terminology/lexicon (i.e., environment preparation, cyber-attack, cyber defense), principles, capabilities, limitations, and effects.</li> </ul>	
	<p>The individual shall be able to:</p> <ul style="list-style-type: none"> <li>• Execute collection using appropriate strategies and within the priorities established through the collection management process.</li> <li>• Perform in-depth joint targeting and cybersecurity planning processes.</li> <li>• Gather information and develop detailed Operational Plans and Orders supporting requirements.</li> <li>• Assist strategic and operational-level planning across the full range of operations for integrated information and cyberspace operations.</li> <li>• 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.</li> </ul>	
<b>8</b>	<b>Investigate</b>	<b>15</b>
	<p>The individual needs to know and understand:</p> <ul style="list-style-type: none"> <li>• Threat investigations, reporting, investigative tools and laws/regulations.</li> <li>• Malware analysis concepts and methodologies.</li> <li>• Processes for collecting, packaging, transporting, and storing electronic evidence while maintaining chain of custody.</li> <li>• The judicial process, including the presentation of facts and evidence.</li> <li>• Types and collection of persistent data.</li> <li>• Concepts and practices of processing digital forensic data.</li> <li>• Types of digital forensics data and how to recognize them.</li> <li>• Forensic implications of operating system structure and operations.</li> <li>• Specific operational impacts of cybersecurity lapses.</li> </ul>	
	<p>The individual shall be able to:</p> <ul style="list-style-type: none"> <li>• 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.</li> </ul>	

	<ul style="list-style-type: none"><li>• Collect, process, preserve, analyze, and present computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations.</li></ul>	
	<b>Total</b>	<b>100</b>

## 3 THE ASSESSMENT STRATEGY AND SPECIFICATION

### 3.1 GENERAL GUIDANCE

Assessment is governed by the WorldSkills Assessment Strategy. The Strategy establishes the principles and techniques to which WorldSkills assessment and marking must conform.

Expert assessment practice lies at the heart of the WorldSkills Competition. For this reason it is the subject of continuing professional development and scrutiny. The growth of expertise in assessment will inform the future use and direction of the main assessment instruments used by the WorldSkills Competition: the Marking Scheme, Test Project, and Competition Information System (CIS).

Assessment at the WorldSkills Competition falls into two broad types: measurement and judgement. For both types of assessment the use of explicit benchmarks against which to assess each Aspect is essential to guarantee quality.

The Marking Scheme must follow the weightings within the Standards Specification. The Test Project is the assessment vehicle for the skill competition, and also follows the Standards Specification. The CIS enables the timely and accurate recording of marks, and has expanding supportive capacity.

The Marking Scheme, in outline, will lead the process of Test Project design. After this, the Marking Scheme and Test Project will be designed and developed through an iterative process, to ensure that both together optimize their relationship with the Standards Specification and the Assessment Strategy. They will be agreed by the Experts and submitted to WSI for approval together, in order to demonstrate their quality and conformity with the Standards Specification.

Prior to submission for approval to WSI, the Marking Scheme and Test Project will liaise with the WSI Skill Advisors in order to benefit from the capabilities of the CIS.

## 4 THE MARKING SCHEME

### 4.1 GENERAL GUIDANCE

This section describes the role and place of the Marking Scheme, how the Experts will assess Competitors' work as demonstrated through the Test Project, and the procedures and requirements for marking.

The Marking Scheme is the pivotal instrument of the WorldSkills Competition, in that it ties assessment to the standards that represent the skill. It is designed to allocate marks for each assessed aspect of performance in accordance with the weightings in the Standards Specification.

By reflecting the weightings in the Standards Specification, the Marking Scheme establishes the parameters for the design of the Test Project. Depending on the nature of the skill and its assessment needs, it may initially be appropriate to develop the Marking Scheme in more detail as a guide for Test Project design. Alternatively, initial Test Project design can be based on the outline Marking Scheme. From this point onwards the Marking Scheme and Test Project should be developed together.

Section 2.1 above indicates the extent to which the Marking Scheme and Test Project may diverge from the weightings given in the Standards Specification, if there is no practicable alternative.

The Marking Scheme and Test Project may be developed by one person, or several, or by all Experts. The detailed and final Marking Scheme and Test Project must be approved by the whole Expert Jury prior to submission for independent quality assurance. The exception to this process is for those skill competitions which use an independent designer for the development of the Marking Scheme and Test Project. Please see the Rules for further details.

Experts and independent designers are required to submit their Marking Schemes and Test Projects for comment and provisional approval well in advance of completion, in order to avoid disappointment or setbacks at a late stage. They are also advised to work with the CIS Team at this intermediate stage, in order to take full advantage of the possibilities of the CIS.

In all cases a draft Marking Scheme must be entered into the CIS at least eight weeks prior to the Competition using the CIS standard spreadsheet or other agreed methods.

### 4.2 ASSESSMENT CRITERIA

The main headings of the Marking Scheme are the Assessment Criteria. These headings are derived in conjunction with the Test Project. In some skill competitions the Assessment Criteria may be similar to the section headings in the Standards Specification; in others they may be totally different. There will normally be between five and nine Assessment Criteria. Whether or not the headings match, the Marking Scheme as a whole must reflect the weightings in the Standards Specification.

Assessment Criteria are created by the person(s) developing the Marking Scheme, who are free to define criteria that they consider most suited to the assessment and marking of the Test Project. Each Assessment Criterion is defined by a letter (A-I). It is advisable not to specify either the Assessment Criteria, or the allocation of marks, or the assessment methods, within this Technical Description.

The Mark Summary Form generated by the CIS will comprise a list of the Assessment Criteria.

The marks allocated to each Criterion will be calculated by the CIS. These will be the cumulative sum of marks given to each Aspect within that Assessment Criterion.

## 4.3 SUB CRITERIA

Each Assessment Criterion is divided into one or more Sub Criteria. Each Sub Criterion becomes the heading for a WorldSkills marking form. Each marking form (Sub Criterion) contains Aspects to be assessed and marked by measurement or judgement, or both measurement and judgement.

Each marking form (Sub Criterion) specified both the day on which it will be marked, and the identity of the marking team.

## 4.4 ASPECTS

Each Aspect defines, in detail, a single item to be assessed and marked together with the marks, or instructions for how the marks are to be awarded. Aspects are assessed either by measurement or judgement.

The marking form lists, in detail, every Aspect to be marked together with the mark allocated to it .

The sum of the marks allocated to each Aspect must fall within the range of marks specified for that section of the skill in the Standards Specification. This will be displayed in the Mark Allocation Table of the CIS, in the following format, when the Marking Scheme is reviewed from C-8 weeks. (Section 4.1)

	CRITERIA								TOTAL MARKS PER SECTION	WSS MARKS PER SECTION	VARIANCE	
	A	B	C	D	E	F	G	H				
STANDARDS SPECIFICATION SECTION	1	5.00							5.00	5.00	0.00	
	2		2.00					7.50		10.00	0.50	
	3								11.00	10.00	1.00	
	4			5.00					5.00	5.00	0.00	
	5				10.00	10.00	10.00			30.00	30.00	0.00
	6		8.00	5.00				2.50	9.00	24.50	25.00	0.50
	7			10.00				5.00		15.00	15.00	0.00
TOTAL MARKS	5.00	10.00	10.00	10.00	10.00	10.00	15.00	20.00	100.00	100.00	2.00	

## 4.5 ASSESSMENT AND MARKING

There is to be one marking team for each Sub Criterion, whether it is assessed and marked by judgement, measurement, or both. The same marking team must assess and mark all competitors, in all circumstances. The marking teams must be organized to ensure that there is no compatriot marking in any circumstances. (See 4.6.)

## 4.6 ASSESSMENT AND MARKING USING JUDGEMENT

Judgement uses a scale of 0-3. To apply the scale with rigour and consistency, judgement must be conducted using:

- benchmarks (criteria) for detailed guidance for each Aspect (in words, images, artefacts or separate guidance notes)
- the 0-3 scale to indicate:
  - 0: performance below industry standard
  - 1: performance meets industry standard
  - 2: performance meets and, in specific respects, exceeds industry standard
  - 3: performance wholly exceeds industry standard and is judged as excellent

Three Experts will judge each Aspect, with a fourth to coordinate the marking and acting as a judge to prevent compatriot marking.

## 4.7 ASSESSMENT AND MARKING USING MEASUREMENT

Three Experts will be used to assess each aspect. Unless otherwise stated only the maximum mark or zero will be awarded. Where they are used, the benchmarks for awarding partial marks will be clearly defined within the Aspect.

## 4.8 THE USE OF MEASUREMENT AND JUDGEMENT

Decisions regarding the selection of criteria and assessment methods will be made during the design of the competition through the Marking Scheme and Test Project.

## 4.9 COMPLETION OF SKILL ASSESSMENT SPECIFICATION

As this is a new skill the skill assessment specification will be agreed by the Experts.

## 4.10 SKILL ASSESSMENT PROCEDURES

All Experts should be assigned to a module team. The Competitor's work may not be altered in any way to facilitate marking unless included in the marking scheme.

The Experts attending the Competition will be divided into smaller marking groups within their module team to mark each specific section of the marking criteria. Progressive marking for all sections of the Competition. Each module/task/section will be completed on the assigned day so that progressive marking can take place.

Marking scheme:

- Each Competitor is provided with the Mark Summary Form
- A full "how-to-marking scheme" will only be seen by the Experts. (Reason: The full marking scheme would give the answers to the Competitor.)



## 5 THE TEST PROJECT

### 5.1 GENERAL NOTES

Sections 3 and 4 govern the development of the Test Project. These notes are supplementary.

Whether it is a single entity, or a series of stand-alone or connected modules, the Test Project will enable the assessment of the skills in each section of the WSSS.

The purpose of the Test Project is to provide full, balanced and authentic opportunities for assessment and marking across the Standards Specification, in conjunction with the Marking Scheme. The relationship between the Test Project, Marking Scheme and Standards Specification will be a key indicator of quality, as will be its relationship with actual work performance.

The Test Project will not cover areas outside the Standards Specification, or affect the balance of marks within the Standards Specification other than in the circumstances indicated by Section 2.

The Test Project will enable knowledge and understanding to be assessed solely through their applications within practical work.

The Test Project will not assess knowledge of WorldSkills rules and regulations.

This Technical Description will note any issues that affect the Test Project's capacity to support the full range of assessment relative to the Standards Specification. Section 2.1 refers.

### 5.2 FORMAT/STRUCTURE OF THE TEST PROJECT

The Test Project will require the Competitors to set up, install, configure, and harden computers, servers, firewall, networking equipment and associated software to meet the typical tasks of a network and systems security technician/consultant.

The Test Project will be divided into three distinct areas to be carried out over a spread of four (4) days of the competition:

- Infrastructure Setup and Security Hardening;
- Cybersecurity Incident Response, Digital Forensic Investigations and Application Security;
- Capture-The-Flag (CTF) Challenge.

### 5.3 TEST PROJECT DESIGN REQUIREMENTS

Each Test Project module must be:

- At a level that a Competitor can comfortably complete;
- The highest level of difficulty in the competition included modules, must be less than or equal to the knowledge, skillsets, and abilities defined in the seven (7) cyber security functions stated in the WorldSkills Standards Specification.
- Designed using a standard cover sheet for each section on the WorldSkills International template available on the website;
- Self-explanatory requiring minimal translation (Competitor instructions containing a minimum of text);
- Each module should have a detailed physical topology image followed by a detailed logical topology image;
- Be accompanied by a marking scheme that will be finalized at the Competition in accordance with the Technical Description;
- All operating systems and other software used in the Competition are to be in English language versions.

## 5.4 TEST PROJECT DEVELOPMENT

The Test Project MUST be submitted using the templates provided by WorldSkills International ([www.worldskills.org/expertcentre](http://www.worldskills.org/expertcentre)). Use the Word template for text documents and DWG template for drawings.

### 5.4.1 Who develops the Test Project or modules

The SMT (Skill Management Team) selects the module teams and the Test Projects are then developed by each module team. Test Projects may ONLY be submitted by module development teams, no individual submissions. Experts should submit their ideas and work with the module development team.

The Capture-The-Flag (CTF) Challenge on day 3 and 4 will be developed by an Independent Test Project Designer.

### 5.4.2 How and where is the Test Project or modules developed

All module teams must send their Test Projects to the Skill Competition Manager three months before the Competition. It is the responsibility of all Experts as a member of a module team, to access and be an active part in the development of their own modules Test Project and in case of voting, cast their votes on the forum. The active work on the module teams Test Projects will and must be done in the closed forum that they are specifically assigned to.

Note: The module team leader should be an Expert with previous experience from at least one WorldSkills competition (whenever possible) and be nominated by the Chief Expert after consultation with the Deputy Chief Expert.

It is the module team leader's responsibility to ensure that each module conforms to the Technical Description, complete with proof of testing and a Marking Scheme.

### 5.4.3 When is the Test Project developed

The Test Project is developed according to the following timeline:

TIME	ACTIVITY
C-12 months	SMT contacts the WSS-team and registered Experts to invite them for the upcoming work with the skill management process.
C-9 months	SMT contacts the registered Experts to invite them to be part of the Module team that they prefer. After this the SMT choose and asks experienced Experts to be one of the Module Team Leaders.
C-6 months	SMT allocates Experts to the Module teams and under lead by the Module Team Leader they start designing the outlines and collection of activities suitable for the Test Projects for their Module.
C-3 months	Proposed Test Projects are developed. Each Module team including the Independent Test Project Designer send their Test Project to the Skill Competition Manager who check the quality and consistency and send them to Director of Skills Competition.
C-1 month	Module teams submit the corresponding marking scheme for their Test Projects.

## 5.5 TEST PROJECT VALIDATION

The Test Project modules developed by the module teams will be validated by the Skill Competition Manager and the Chief Expert.

The module designed by the Independent Designer will be validated by the Skill Competition Manager.

It must be demonstrated that the Test Project/modules can be completed within the material, equipment and knowledge constraints, and that the hardware and software list is correct and is provided for use. The Test Project, infrastructure setup and base configurations must be analysed for ambiguity and confusion. Unnecessary resources of any kind must not be made available to Competitors as it may induce the Competitor to make errors.

## 5.6 TEST PROJECT SELECTION

The Test Project modules are selected by the Experts by vote on the forum.

The Capture the Flag (CTF) module is developed by an Independent Test Project Designer

## 5.7 TEST PROJECT CIRCULATION

The Test Project is circulated via the website as follows:

The Test Project modules are circulated 3 months prior to the Competition on the website.

The module designed by the Independent Test Project Designer is not circulated.

## 5.8 TEST PROJECT COORDINATION (PREPARATION FOR COMPETITION)

Coordination of the Test Project will be undertaken by:

- The Skill Management Team;
- The Chief Expert assigns Experts to each module team. Each module team is responsible for one Test Project module;

Each module team will be allocated a team of Experts. The module team leader will work closely with the Skill Management Team to allow for the completion of the module. The Team Leader will be responsible for the completion of each module in line with this document and ensure the modules are true and correct.

## 5.9 TEST PROJECT CHANGE AT THE COMPETITION

The circulated Test Project modules are subject to 30% change at the Competition. The Experts in the Test Project Development team will make the 30% change at the competition

## 5.10 MATERIAL OR MANUFACTURER SPECIFICATIONS

Specific material and/or manufacturer specifications required to allow the Competitor to complete the Test Project will be supplied by the Competition Organizer and are available from [www.worldskills.org/infrastructure](http://www.worldskills.org/infrastructure) located in the Expert Centre.

## 6 SKILL MANAGEMENT AND COMMUNICATION

### 6.1 DISCUSSION FORUM

Prior to the Competition, all discussion, communication, collaboration, and decision making regarding the skill competition must take place on the skill specific Discussion Forum (<http://forums.worldskills.org>). Skill related decisions and communication are only valid if they take place on the forum. The Chief Expert (or an Expert nominated by the Chief Expert) will be the moderator for this Forum. Refer to Competition Rules for the timeline of communication and competition development requirements.

### 6.2 COMPETITOR INFORMATION

All information for registered Competitors is available from the Competitor Centre ([www.worldskills.org/competitorcentre](http://www.worldskills.org/competitorcentre)).

This information includes:

- Competition Rules
- Technical Descriptions
- Mark Summary Form (where applicable)
- Test Projects (where applicable)
- Infrastructure List
- WorldSkills Health, Safety, and Environment Policy and Regulations
- Other Competition-related information

### 6.3 TEST PROJECTS [AND MARKING SCHEMES]

Circulated Test Projects will be available from [www.worldskills.org/testprojects](http://www.worldskills.org/testprojects) and the Competitor Centre ([www.worldskills.org/competitorcentre](http://www.worldskills.org/competitorcentre)).

### 6.4 DAY-TO-DAY MANAGEMENT

The day-to-day management of the skill during the Competition is defined in the Skill Management Plan that is created by the Skill Management Team led by the Skill Competition Manager. The Skill Management Team comprises the Skill Competition Manager, Chief Expert and Deputy Chief Expert. The Skill Management Plan is progressively developed in the six months prior to the Competition and finalized at the Competition by agreement of the Experts. The Skill Management Plan can be viewed in the Expert Centre ([www.worldskills.org/expertcentre](http://www.worldskills.org/expertcentre)).

## 7 SKILL-SPECIFIC SAFETY REQUIREMENTS

Refer to WorldSkills Health, Safety, and Environment Policy and Regulations for Host country or region regulations.

## 8 MATERIALS AND EQUIPMENT

### 8.1 INFRASTRUCTURE LIST

The Infrastructure List details all equipment, materials and facilities provided by the Competition Organizer.

The Infrastructure List is available at [www.worldskills.org/infrastructure](http://www.worldskills.org/infrastructure).

The Infrastructure List specifies the items and quantities requested by the Experts for the next Competition. The Competition Organizer will progressively update the Infrastructure List specifying the actual quantity, type, brand, and model of the items. Items supplied by the Competition Organizer are shown in a separate column.

At each Competition, the Experts must review and update the Infrastructure List in preparation for the next Competition. Experts must advise the Director of Skills Competitions of any increases in space and/or equipment.

At each Competition, the Technical Observer must audit the Infrastructure List that was used at that Competition.

The Infrastructure List does not include items that Competitors and/or Experts are required to bring and items that Competitors are not allowed to bring – they are specified below.

### 8.2 COMPETITORS TOOLBOX

Competitors are not required to bring a toolbox.

### 8.3 MATERIALS, EQUIPMENT, AND TOOLS SUPPLIED BY COMPETITORS IN THEIR TOOLBOX

Competitors are not required to bring any tools to the Competition.

### 8.4 MATERIALS, EQUIPMENT, AND TOOLS SUPPLIED BY EXPERTS

Experts do not supply any equipment.

### 8.5 MATERIALS AND EQUIPMENT PROHIBITED IN THE SKILL AREA

Competitors are prohibited from bringing any materials and equipment to the Competition.

### 8.6 PROPOSED WORKSHOP AND WORKSTATION LAYOUTS

Workshop layouts are available at [www.worldskills.org/sitelayout](http://www.worldskills.org/sitelayout).

## 9 SKILL-SPECIFIC RULES

Skill-specific rules cannot contradict or take priority over the Competition Rules. They do provide specific details and clarity in areas that may vary from skill competition to skill competition. This includes but is not limited to personal IT equipment, data storage devices, internet access, procedures and work flow, and documentation management and distribution.

TOPIC/TASK	SKILL-SPECIFIC RULE
Use of technology – USB, memory sticks	<ul style="list-style-type: none"> <li>• Experts – Experts are allowed to bring USB/memory sticks into the Expert Meeting Room. USB/memory sticks will be allowed to be taken outside of the meeting room at the end of each day. Competitors – Competitors are not allowed to bring USB/memory into the workshop.</li> </ul>
Use of technology – personal laptops	<ul style="list-style-type: none"> <li>• Experts – Experts are allowed to bring laptops into the Expert Meeting Room. Laptops will be allowed to be taken outside of the meeting room at the end of each day.</li> <li>• Competitors – No laptops are allowed in the workshop.</li> </ul>
Use of technology – personal cameras	<ul style="list-style-type: none"> <li>• Experts – Experts are allowed to bring cameras into the Expert Meeting Room. Cameras will be allowed to be taken outside of the meeting room at the end of each day.</li> <li>• Competitors – No cameras are allowed in the workshop until the completion of competition on day four.</li> </ul>
Use of technology – mobile devices	<ul style="list-style-type: none"> <li>• Experts – No electronic devices are to be brought to any Competitors workstations under any circumstances unless with the approval of either the Chief or Deputy Chief Experts.</li> <li>• Competitors – Electronic devices (Including mobile phones) must stay in Competitor bags (switched off or on silent) within the lockers provided. No electronic devices are to be brought to Competitors workstations under any circumstances unless with the approval of either the Chief or Deputy Chief Experts.</li> </ul>
Source file/notes	<ul style="list-style-type: none"> <li>• Competitors – No notes may be brought into the workshop under any circumstances. All notes made at the Competitor workstation must remain on the Competitors desk at all times. No notes may be taken outside of the workshop.</li> </ul>
Equipment failure	<ul style="list-style-type: none"> <li>• Competitors – In the occurrence of equipment failure Competitors must notify Experts immediately by raising their hand. Experts will take note of the time that the Competitor is not able to make use of their equipment. Any time lost due to equipment failure will be provided to the Competitor at the end of the standard Module time.</li> <li>• No additional time will be granted for work not saved prior to the equipment failure.</li> </ul>

TOPIC/TASK	SKILL-SPECIFIC RULE
Final Test Projects	<ul style="list-style-type: none"> <li>Competitors - Final Test Projects for all Competitors will be backed up and made available to all Competitors at the conclusion of the competition.</li> </ul>
Music	<ul style="list-style-type: none"> <li>Competitors - Competitors will be allowed to supply on Familiarization Day a memory stick containing a maximum of 20 un-edited songs. In addition to the memory stick, Competitors may also supply a maximum of three original music CDs. All music will be collated and shared amongst all Competitors.</li> </ul>
Familiarization Day	<ul style="list-style-type: none"> <li>Competitors - During Familiarization Day Competitors cannot use the available time to work on or solve any tasks related to the Competition. Prior to completing Familiarization all Competitors need to clean their respective computers removing all the files created/used to test the software. This includes the removal of all databases which have been created.</li> </ul>
Breaks	<ul style="list-style-type: none"> <li>Competitors - No extra time will be given to Competitors who stop work during competition time to go to the bathroom or for those who break for a food and/or drink. When time is completed all Competitors must stop all work on their computer immediately.</li> </ul>



## 10 VISITOR AND MEDIA ENGAGEMENT

Following is a list of possible ways to maximize visitor and media engagement:

- Two mirrored monitors displayed for the public to view Competitors screens;
- Display screens showing a presentation on what competitors are currently working on;
- Enhanced understanding of Competitor activity;
- Career opportunities.

## 11 SUSTAINABILITY

This skill competition will focus on the sustainable practices below:

- Recycling – No printing for Competitor workstations;
- No printing of Test Projects. Test Projects will be provided within media files;
- Use of completed Test Projects after Competition;
- Limit the amount of software to be installed on Competitor workstations;
- Open source software.

## 12 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.onetonline.org/](http://www.onetonline.org/))