

**SKILLS FRAMEWORK FOR SECURITY  
TECHNICAL SKILLS & COMPETENCIES (TSC) REFERENCE DOCUMENT**

<b>TSC Category</b>	Security Risk Management					
<b>TSC</b>	Security Risk Analysis					
<b>TSC Description</b>	Methodological approaches to identify and solve security-related problems					
<b>TSC Proficiency Description</b>	<b>Level 1</b>	<b>Level 2</b>	<b>Level 3</b>	<b>Level 4</b>	<b>Level 5</b>	<b>Level 6</b>
			<b>SEC-SRM-3002-1.1</b>	<b>SEC-SRM-4002-1.1</b>	<b>SEC-SRM-5002-1.1</b>	
			Breakdown straightforward security problems and identify risks	Determine the cause-and-effect relationships between security problems and risks	Assess threat vulnerabilities and risks	
<b>Knowledge</b>			<ul style="list-style-type: none"> <li>• Methods of risk analysis</li> <li>• Types of tell-tale signs and symptoms</li> <li>• Organisational procedures for security operations</li> <li>• Signs of surveillance and intelligence-gathering being conducted, inappropriate demeanours and potential suicide bombers</li> <li>• Types of suspicious activities, inappropriate attires, explosives and incendiary devices used by terrorists</li> <li>• Identification of persons</li> </ul>	<ul style="list-style-type: none"> <li>• Organisational procedures for security operations</li> <li>• Types of security risks</li> <li>• Risk and threat analysis, including risk prioritisation</li> <li>• Relevant security legislation</li> <li>• Contract terms of reference</li> </ul>	<ul style="list-style-type: none"> <li>• Relevant legislations and regulatory frameworks</li> <li>• Threat contexts</li> <li>• Adversary modes of operation</li> <li>• Principles of protective security</li> <li>• Limitations of technology</li> <li>• Types of mitigation measures</li> <li>• Chemical, biological or radiological (CBR) effects</li> <li>• Security-by-design concept</li> <li>• In-place protection procedures</li> <li>• Threat, vulnerability and risk assessment</li> </ul>	
<b>Abilities</b>			<ul style="list-style-type: none"> <li>• Apply basic risk identification techniques</li> <li>• Follow standard operating procedures (SOPs) to identify risks</li> <li>• Study situations and relate to past experience for identification of risks</li> <li>• Discuss situations with security teams to identify risks</li> </ul>	<ul style="list-style-type: none"> <li>• Identify potential risks affecting client security using available organisational, industry and public information sources and assess against likelihood of occurrence</li> <li>• Assess potential risks based on accurate and current understanding of clients' operating environments</li> <li>• Develop structured action plans which identifies key roles and</li> </ul>	<ul style="list-style-type: none"> <li>• Assess and evaluate existing security provisions and ground operations within facilities</li> <li>• Identify and evaluate security threats within facilities and the probability of occurrence</li> <li>• Analyse vulnerabilities as well as operations and activities related to threat scenarios</li> <li>• Assess associated loss or impact on facilities should threats occur</li> </ul>	

**SKILLS FRAMEWORK FOR SECURITY  
TECHNICAL SKILLS & COMPETENCIES (TSC) REFERENCE DOCUMENT**

				<p>responsibilities associated with implementation of security risk management plans</p> <ul style="list-style-type: none"> <li>• Develop contingencies for occurrence of identified risks, and incorporate into plans</li> <li>• Select risk control measures in line with organisational practices, and identify and clarify implications of risk control measures approved by clients</li> <li>• Check risk control measures are documented and supported by suitable agreed organisational guidelines</li> </ul>	<ul style="list-style-type: none"> <li>• Develop overall risk profiles of facilities</li> <li>• Develop measures, which cover manpower, infrastructure, use of technology and reporting systems, to mitigate risks and reduce identified vulnerabilities</li> <li>• Communicate with relevant stakeholders</li> </ul>	
--	--	--	--	--	---	--