<table>
<thead>
<tr>
<th>TSC Category</th>
<th>Security Risk Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>TSC</td>
<td>Security Risk Analysis</td>
</tr>
<tr>
<td>TSC Description</td>
<td>Methodological approaches to identify and solve security-related problems</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TSC Proficiency Description</th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
<th>Level 5</th>
<th>Level 6</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SEC-SRM-3002-1.1</td>
<td>SEC-SRM-4002-1.1</td>
<td>SEC-SRM-5002-1.1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Breakdown straightforward security problems and identify risks</td>
<td>Determine the cause-and-effect relationships between security problems and risks</td>
<td>Assess threat vulnerabilities and risks</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Knowledge**

- Methods of risk analysis
- Types of tell-tale signs and symptoms
- Organisational procedures for security operations
- Signs of surveillance and intelligence-gathering being conducted, inappropriate demeanours and potential suicide bombers
- Types of suspicious activities, inappropriate attires, explosives and incendiary devices used by terrorists
- Identification of persons
- Organisational procedures for security operations
- Types of security risks
- Risk and threat analysis, including risk prioritisation
- Relevant security legislation
- Contract terms of reference
- Relevant legislations and regulatory frameworks
- Threat contexts
- Adversary modes of operation
- Principles of protective security
- Limitations of technology
- Types of mitigation measures
- Chemical, biological or radiological (CBR) effects
- Security-by-design concept
- In-place protection procedures
- Threat, vulnerability and risk assessment

**Abilities**

- Apply basic risk identification techniques
- Follow standard operating procedures (SOPs) to identify risks
- Study situations and relate to past experience for identification of risks
- Discuss situations with security teams to identify risks
- Identify potential risks affecting client security using available organisational, industry and public information sources and assess against likelihood of occurrence
- Assess potential risks based on accurate and current understanding of clients' operating environments
- Develop structured action plans which identifies key roles and
- Assess and evaluate existing security provisions and ground operations within facilities
- Identify and evaluate security threats within facilities and the probability of occurrence
- Analyse vulnerabilities as well as operations and activities related to threat scenarios
- Assess associated loss or impact on facilities should threats occur
| Responsibilities associated with implementation of security risk management plans | • Develop contingencies for occurrence of identified risks, and incorporate into plans  
• Select risk control measures in line with organisational practices, and identify and clarify implications of risk control measures approved by clients  
• Check risk control measures are documented and supported by suitable agreed organisational guidelines |
| --- | --- |
| Develop overall risk profiles of facilities | • Develop measures, which cover manpower, infrastructure, use of technology and reporting systems, to mitigate risks and reduce identified vulnerabilities  
• Communicate with relevant stakeholders |