<table>
<thead>
<tr>
<th>TSC Category</th>
<th>Operations and User Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>TSC</td>
<td>Threat and Vulnerability Management</td>
</tr>
<tr>
<td>TSC Description</td>
<td>Manage cyber threats and system vulnerabilities to minimise cyber risks</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>EPW-OUS-2021-1.1</td>
<td>EPW-OUS-3021-1.1</td>
<td>EPW-OUS-4021-1.1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recognise cyber threats and system vulnerabilities and recommend methods to eliminate them</td>
<td>Analyse cyber threats and system vulnerabilities and review mitigation measures</td>
<td>Develop organisational frameworks on cyber threat and system vulnerabilities</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Knowledge**

- Ethics related to cybersecurity
- Different types of system threats
- Different types of system vulnerabilities
- Threat assessment techniques
- System risk areas
- Relevant cybersecurity codes and standards
- Ethics and regulations related to cybersecurity
- Cyber threat investigation techniques
- Root cause analysis techniques
- Cyber threat and system vulnerability audit techniques
- Vulnerability assessment techniques
- System vulnerability ratings
- Threat analysis systems
- Laws and regulations related to cybersecurity
- Stakeholder communication channels
- Best practices and industry trends for cybersecurity and threat vulnerabilities management
- Key Performance Indicators (KPIs) for system integrity to withstand cyber threats
- Levels of system risks
- Technology upgrades in the market

**Abilities**

- Identify levels of system threats detected
- Highlight areas of potential system vulnerability
- Recommend measures to close gaps for system vulnerabilities
- Audit cyber threats and system vulnerabilities
- Investigate system breaches
- Perform analysis on system integrity to measure the ability of the system to withstand cyber threats
- Analyse areas for potential system vulnerabilities and risks
- Develop organisational cyber threat and system vulnerability frameworks
- Determine communication plans with relevant stakeholders on system breaches
- Determine KPIs and security levels for system integrity
<table>
<thead>
<tr>
<th>Range of Application</th>
<th>Range of application includes, but is not limited to:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Gas Systems Operations</td>
</tr>
<tr>
<td></td>
<td>• Transmission and Distribution</td>
</tr>
</tbody>
</table>

- Review mitigation measures to reduce system vulnerabilities
- Analyse potential impact of loss due to detected threats
- Devise strategies to mitigate systemic risks to overall cybersecurity systems
- Determine appropriate responses to levels of threats and potential impact of loss
- Recommend upgrades and patches to address unacceptable system risks