## TSC Category
Strategy and Architecture

## TSC
Cyber Risk Management

## TSC Description
Develop cyber risk assessment and treatment techniques that can effectively pre-empt and identify significant security loopholes and weaknesses, demonstration of the business risks associated with these loopholes and provision of risk treatment and prioritisation strategies to effectively address the cyber-related risks, threats and vulnerabilities identified to ensure appropriate levels of protection, confidentiality, integrity and privacy in alignment with the security framework.

<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>ICT-SNA-6007-1.1</td>
<td>ICT-SNA-5007-1.1</td>
<td>ICT-SNA-6007-1.1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Develop cyber risk assessment techniques and roll-out endorsed measures to address identified cyber security risks, threats and vulnerabilities.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assess and direct enhancements to cyber risk assessment techniques, and develop strategies to address cyber security loopholes.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Evaluate the readiness and robustness of the organisation’s cyber security defences, and authorise cyber risk assessment activities.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Knowledge

- Cyber risk assessment techniques
- Security risks, threats and vulnerabilities
- Possible treatments of security risks, threats and vulnerabilities
- Required levels of confidentiality, integrity, privacy and personal data protection as well as privacy technologies
- Design of cyber risk assessment techniques
- Projection of cyber security risks, threats and vulnerabilities
- Key requirements and objectives of various cyber risk assessments
- Pros and cons of various treatment approaches
- Business risks and implications from cyber security loopholes
- Key business implications of cyber risk assessment and testing policies
- Evolving security landscape and emerging cyber security threats
- Measures of organisational readiness against threats
- Assessment of potential business risks from security loopholes

©SkillsFuture Singapore and Infocomm Media Development Authority
Effective Date: November 2017, Version 1.1
| Abilities | • Develop cyber risk assessment techniques to identify security loopholes and weaknesses in the business  
| • Design cyber risk assessments by consolidating insights from the business and various functions  
| • Identify cyber security risks, threats and vulnerabilities, and their impact on the organisation  
| • Identify possible treatments for cyber risks, threats and vulnerabilities identified  
| • Implement endorsed treatment and measures to address security gaps  
| • Guide the development of cyber risk assessment techniques  
| • Pre-empt risks, vulnerabilities and threats across organisation policies, processes and defences  
| • Evaluate effectiveness of current cyber risk assessment techniques  
| • Direct improvements or modifications to vulnerability assessment techniques in view of emerging security risks and threats  
| • Lead the implementation of cyber risk assessment activities throughout organisation, ensuring alignment with organisation’s policies and principles  
| • Analyse cybersecurity loopholes identified and project business risk and impact to the organisation  
| • Evaluate options and decide on suitable treatment of cyber risks, threats and vulnerabilities  
| • Develop strategies to address loopholes and ensure appropriate levels of protection, confidentiality, integrity and personal data protection  
| • Establish organisation’s position and strategy for assessing and managing cyber risk  
| • Determine security testing policies and authorise the management of all testing activities within the organisation  
| • Articulate implications of potential cyber threats on requirements of organisational readiness and assessment techniques  
| • Weigh potential business risks associated with cyber security risks, threats and vulnerabilities surfaced  
| • Assess overall strength of the organisation’s existing defences in light of evolving internal and external security landscape  
| • Endorse strategies to effectively address the security risks, threats and vulnerabilities identified and evaluate potential costs to the organisation to implement the strategies  
| Range of Application |