## TSC Category
Infocomm Technology

## TSC
Information and Communication Technology Disaster Recovery Management

## TSC Description
Develop, evaluate and refine policies and processes to guide recovery of critical Information Technology infrastructure and systems following a crisis or disaster

<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>FSS-ICT-2002-1.1</td>
<td>FSS-ICT-3002-1.1</td>
<td>FSS-ICT-4002-1.1</td>
<td>FSS-ICT-5002-1.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Follow operational procedures and contingency plans to ensure adequate risk safeguards to Information Technology (IT) infrastructure and systems</td>
<td>Assist to develop disaster recovery plans by recommending refinements to the developed plans</td>
<td>Evaluate key risk indicators and their implications on disaster recovery plan to monitor the efficiency and effectiveness of responses for similar incidents or disruptions</td>
<td>Drive policies and procedures to guide recovery of critical Information Technology (IT) infrastructure and systems and lead communication with relevant stakeholders during disruptive events</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Knowledge
- IT infrastructure
- Key risk indicators of disruptive events
- Disaster recovery management practice principles
- Components of disaster recovery plans
- Formal exercise and plan testing documentation requirements
- Business continuity testing on infrastructure and critical business applications
- Internal and external threats that may impact organisation Information Technology (IT) infrastructure and systems
- Test results components and how they fit into the overall testing plans
- Relevant regulatory requirements and leading practices of Information Technology (IT) disaster recovery plans within the industry
- Scope of disaster recovery testing
- Crisis response and recovery activities
- Types of disaster recovery plan audits
- Objectives of disaster recovery plan audits
- Business continuity management leading practices within the industry
- Business impact of IT disruptive events on the organisation

### Abilities
- Adhere to operational procedures to ensure adequate risk safeguards and contingency plans are in place
- Document formal exercise and testing for management reviews for the refinement of the disaster recovery management plans
- Support identification of threats to the IT infrastructure and systems and provide inputs to team members
- Participate in disaster recovery testing for IT
- Identify internal and external threats to the IT infrastructure and systems
- Apply facilitation techniques to support development of business continuity strategies
- Interpret business continuity strategies to assist in the development of IT disaster recovery plans
- Recommend refinements to business continuity strategies, business continuity plans and IT disaster recovery plans in
- Review IT infrastructure and systems to ensure adequate risk safeguards and contingency plans are in place
- Monitor the efficiency and effectiveness of responses to significant incidents or disruptions
- Review the IT disaster recovery plans and processes
- Utilise key risk indicators of disruptive events to inform and activate crisis response and recovery activities
- Develop policies and processes to guide recovery of critical IT infrastructure and systems following a crisis or disaster
- Assess potential impact of business risks and threats on IT systems
- Conduct periodic exercising of crisis response and recovery activities and periodic auditing of disaster recovery plans in consultation with relevant stakeholders

©SkillsFuture Singapore
Effective Date: August 2020, Version 1.1
<table>
<thead>
<tr>
<th>Skill</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infrastructure management</td>
<td>Maintain infrastructure on a regular basis in accordance with disaster recovery testing plans</td>
</tr>
<tr>
<td>Crisis communication</td>
<td>Consult with relevant stakeholders to ensure alignment with disaster recovery plans</td>
</tr>
<tr>
<td>Crisis assessment</td>
<td>Prioritise the resources available in the organisation to support disaster recovery plans</td>
</tr>
<tr>
<td>Risk management</td>
<td>Interpret crisis assessment documentation to contribute to disaster recovery plans</td>
</tr>
<tr>
<td>Risk minimisation</td>
<td>Evaluate risk minimisation alternatives against specifications and cost constraints</td>
</tr>
<tr>
<td>Event management</td>
<td>Direct review of crisis response, recovery activities and stand-down procedures to make improvements for future activation during crisis situations</td>
</tr>
<tr>
<td>Communication management</td>
<td>Manage communication of disruptive events to relevant stakeholders to ensure alignment with disaster recovery plans</td>
</tr>
</tbody>
</table>