The Smith Family
Learn today, change tomorrow.

POSITION DESCRIPTION

General Information:	
Position Title:	Supplier Governance and Resilience Analyst
Incumbent:	N/A
Function & Team/Program:	D&T – CSTO – Security Assurance and Compliance
Location(s):	National Office
Manager’s Position Title:	Business Continuity and IT Disaster Recovery Coordinator
Manager’s Name:	Anton Yap
Date Prepared:	17 July 2025
Prepared By:	Anton Yap
Approved By:	Prashant Pandey

Primary Purpose of this Position ***(In one sentence - why does the role exist?)***

To support the BCP and ITDR Coordinator in the execution of Operational Resilience, Third-Party Supplier and Risk Management initiatives and to manage key tasks within these projects and BAU activities.

This position is responsible for supporting the effective management of IT vendor relationships, ensuring compliance with contractual agreements, and enhancing the resilience of critical IT services delivered by third-party suppliers. This role plays a key part in identifying, assessing, mitigating, and monitoring risks associated with IT suppliers, contributing to the overall stability and continuity of the organisation's IT landscape.

Scope:

Direct Reports to this Position	**Indirect Reports**
By Position Title	Total Number
• Nil	• Nil

Financial Dimensions controlled by this Position ***(Include key financial metrics such as revenue growth, income & expense budget, etc)***

Direct control	**Indirect control**
• Nil	• Nil

Other Dimensions of this Position

e.g. Number of programs, site responsibility, geographic spread of team
Projects and Initiatives include:

- Business Continuity Implementation
- Supplier Assurance and Data Deletion
- Ransomware Simulation and Action Plan Completion
- ITDR Planning and Testing
- User Access Review for TSF Critical Applications

Setting Priorities ***(how is work prioritised)***

How often does employee prioritise their own work? Eg. Daily, weekly, monthly, annually, other	Daily, Weekly, Monthly & Quarterly
How often does employee determine the priorities of others? Eg. Daily, weekly, monthly, annually, other	Not Applicable

Key Relationships ***(Who does the role interact with? List the titles of individuals, departments and organisations frequently interacts with)***	
Internal	• CTSO • BCP & ITDR Coordinator • CTSO Organisation • D&T Platform Managers • SmithShield Program Manager • National Risk Manager • Business Unit Contacts (e.g. SADD BU Contacts)
External	• Consultants (if any) • Contractors (if any)

Key Decision Making in this Role: ***(What are the key decisions and recommendations made in this role?)***
Decisions Expected • Planning and execution within project task scope.
Recommendations Expected • Implementation and execution advice and recommendations on project and BAU activities.

Every Team Member at The Smith Family:

- Is expected to uphold The Smith Family Values and Culture;
- Understands and complies with the Child Protection Framework;
- Takes reasonable care for the health and safety of themselves and others;
- Understands and complies with the Workplace, Health and Safety Systems;
- Reports hazards and incidents and participates in risk management as required.

Key Responsibilities / Accountabilities:
Major Area: Business Continuity ***% of Job Total: 20%***
Facilitate meetings with business SMEs to identify critical business processes.
Facilitate business impact analysis workshops and resource dependency analysis discussions.
Develop business continuity plans by documenting information from the different workshops into the BCP template.
Work with critical suppliers to understand and assess their BCDR plans and capabilities.
Identify potential single points of failure within resources needed to run critical processes (e.g. suppliers/ vendors, people, systems) and work to diversify or mitigate risks.
Support the development and testing of supplier/ vendor disruption workarounds, including alternative sourcing strategies and recovery protocols.
Participate in incident response teams related to supplier disruptions.
Major Area: Supplier Assurance ***% of Job Total: 40%***
Conduct comprehensive supplier security assessments, covering operational capability, cybersecurity, and data privacy.
Manage administrative tasks related to supplier assurance such having ownership over the supplier assurance inbox, updating the supplier master list (for identified suppliers not recorded in FOLIO), and the preparation of upload files into FOLIO.

Liaising with supplier contacts to ensure there is documented agreement to protect TSF personal and sensitive information such as having them sign supplier assurance letters.
Monitor and report on vendor performance against Service Level Agreements (SLAs), Key Performance Indicators (KPIs), and contractual obligations in relation to the secure transmission, use, storage and destruction of TSF personal and sensitive information.
Develop, implement, manage and update the partner assurance and supporter assurance master list.
Act as a point of contact for routine supplier queries and issues in relation to the protection of TSF personal and sensitive information, fostering collaborative relationships.
Assist in managing contract lifecycles, including renewals, amendments, and termination processes.
Ensure proper documentation and record-keeping of supplier related documents such as contracts, SLAs, BCP and ITDR test results, security assessments, SOC2 and 3 reports, etc.
Collaborate with legal and procurement teams to ensure contracts include appropriate clauses related to risk, security, compliance, business continuity, and ITDR. Monitor contract expiry and renewal processes to ensure timely reviews and updated risk assessments.
Major Area: Ransomware Simulation ***% of Job Total: 30%***
Manage and update the ransomware simulation action plan tracking sheet.
Execute activities owned by BCP/DR (e.g. documentation) when applicable.
Major Area: IT Disaster Recovery ***% of Job Total: 10%***
Support the ITDR planning and testing processes.
Collate testing results from both D&T and business testers.
Prepare the ITDR test results summary.

Key Challenges in Achieving Goal(s): ***(What are the key challenges faced by this role in meeting goals/objectives)***

- Complexity of the organisation and the documentation and “ownership” of processes.
- Availability and bandwidth of key subject matter experts needed to support initiatives.

Qualifications, Experience and Competencies: ***(What background, knowledge, experience or competencies are required to perform the role at the expected level?)***

	Essential	**Desirable**
Education / Qualifications / Memberships:	• Qualification or certificate in either Business Management, Business Analytics, Process Architecture, Project Management, Information Technology, and Cyber Security	• CBCI certificate from BCI • PMP certification from PMI • CISSP certification from (ISC)2
	Essential	**Desirable**
Experience:	• 3 to 5+ years’ experience in business analytics, process architecture, information technology, cyber security, procurement, risk management, vendor management, or a similar role. • Worked as Project Manager in small to medium process implementation projects. • Worked as Business Analyst in medium to large process or technology projects.	• Worked as a BCM and/ or ITDR professional. • Worked as a Risk or Assurance professional. • Worked as an IAM professional experienced in conducting UAR. • Worked as a Cyber Security professional.

	• Worked as a functional SME in either a BCP, ITDR, implementation, test or certification audit.	
Competencies:	**Essential**	**Desirable**
	• High-level understanding of business continuity concepts and practices • High-level understanding of IT Disaster recovery concepts and practices • Project management planning and organisation skills • Workshop facilitation and probing skills • Excellent analytical and problem-solving skills • Strong attention to detail and accuracy. • Exceptional written and verbal communication skills. • Strong interpersonal, influential and negotiation skills. • Ability to manage multiple priorities in a fast-paced environment. • Proactive and results-oriented mindset.	• High-level understanding of Risk concepts and practices • High-level understanding of cyber security concepts and practices • High-level understanding of Third-Party assurance concepts and practices