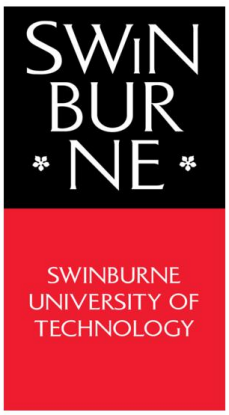
School of Business Law & Entrepreneurship



INF20031

Cybersecurity for business
Semester 1, 2025

Student Name: Abir Hasan Shuvo

Student ID: 105086966

This document includes**: CLA#2**

Submission Deadline: 04 April at 23:59

Task A

RBA Risk Appetite Statement Strengths

The risk appetite statement from the Reserve Bank of Australia (RBA) is a strong, articulate statement of enterprise risk management. This may be its three greatest strengths:

- **Strategic Alignment:** The risk appetite is directly tied to the Bank's operational, financial and policy objectives. This alignment helps make risk-taking intentional and closely aligned with the institution's long-range strategic goals.

- **Differentiated Risk Tolerance**: Verbose statements in its approach across risk types diffuse a "one-size-fits-all" model. But low tolerance for compliance and reputational risk, higher tolerance for operational experimentation. This nuanced perspective demonstrates maturity and realism in risk governance.

- Strong emphasis on accountability and governance the policy sets out roles and responsibilities at both board and senior management levels, embedding strong oversight over all processes. This helps build a risk-conscious culture and enables consistent decision-making in line with the organisation's values.

Task B

Improving the University of Melbourne Cybersecurity Mission

The University of Melbourne's present cybersecurity mission achieves the right balance between innovation and responsibility. Nevertheless, it can be improved significantly by more clearly linking cybersecurity to both strategic value creation and risk boundaries.

Improved Mission Statement:

"The University of Melbourne, as a place of teaching and research excellence, understands that cybersecurity is the foundation of the academic mission and communal trust. Our cybersecurity mission: Build world-class education, research, and digital transformation while ensuring data protection, system resilience, and user safety. We have a moderate appetite for technological innovation, supporting risk-taking that is consistent with our values and freedom to pursue academic inquiry, and maintaining a low appetite for anything that would endanger personal data, critical infrastructure, and intellectual property. "This mission is executed through strong governance, shared responsibility, and constant risk assessment to keep our information systems secure, evolving and ethically sound."

This addition concretely defines purpose, links cybersecurity to organisational values and specifies a risk posture — all of which is in keeping with the high-level strategic direction encouraged in Task A.

Task C

Cybersecurity Mission Statement for Zenith Logistics

“Logistics respects the responsibility of protecting its systems, customer information, and supply chain technologies and will do so with a layered and dynamic cybersecurity program. Our cybersecurity efforts form the backbone of the company’s operational excellence and growth to ensure confidentiality, integrity, and availability of information assets across all logistics functions. Our risk-based approach reflects default low tolerance to risks creating impact to critical systems, customer trust and regulatory compliance, while an accepted controlled level of operational and technological risk support agility and innovation. Our mission is achieved through proactive risk assessment, incident response preparedness, continual training for our staff, and compliance with internationally implemented security frameworks. Zenith views cybersecurity as not only an IT function, but also a fundamental component of our business resilience and stakeholder confidence.”