FSC Guidance Note No. 54

Third-Party Due Diligence and Attestation Questionnaire

17 September 2024

FSC FINANCIAL SERVICES COUNCIL

FSC Guidance Note No. 54

Date of this version:	17 September 2024 No prior versions.
Application of this Guidance Note:	This Guidance Note is designed as a template for use by superannuation funds.
Main Purpose of this Guidance Note:	The purpose of this Guidance Note is to assist in the implementation of quality controls on superannuation fund third-party suppliers relating to cybersecurity and information technology provision and resilience
Disclaimer:	*This document does not constitute any legal, accounting, tax or financial product advice, and does not take into account the objectives, financial situation or needs of any person or the terms of any commercial transaction. Users should obtain their own professional advice tailored to their own circumstances before using this document for their own commercial purposes. The Financial Services Council Ltd (FSC) does not give any warranty with respect to this document and has no responsibility for any loss, damage or liability whatsoever arising from the use of this document. The use of this document is subject to the terms and conditions prescribed by the FSC from time to time in relation to the access, use, transmission or dissemination of this document.*

FSC Guidance Note No. 54

TABLE OF CONTENTS	Paragraph	Page
Scope	1	3
Information Security Governance and Capabilities	Q1	3
Risk Management Process	Q2	3
Compliance with industry Standards	Q3	3
Data Processing & Storage	Q4	4
Data Protection and Privacy	Q5	4
Network and Systems Security	Q6	4
Physical Security and Employee Management	Q7	4
Vulnerability Management	Q8	5
Application Security and Secure Software Development (DevOps)	Q9	5
Logging and Monitoring	Q10	5
Access Control and Identity Management	Q11	5
Security Training and Awareness	Q12	6
Incident Response and Management	Q13	6
Business Continuity and Disaster Recovery Planning	Q14	6
Third-Party Security Management	Q15	6

FSC Guidance Note No. 54

1 Scope

This questionnaire has been designed to assist superannuation funds to implement quality controls on their third-party suppliers relating to cybersecurity and information technology provision and resilience.

This is designed as a template only and is not intended to be a statement of best practice.

Use of this template is completely voluntary.

Superannuation funds should determine the weight given to each individual item as a factor in their decision making. The weight should be completed in the "weight" column.

Description of contracted services:	
Service provider name(s) (list any entities responsible for the provision of the relevant services):	
Address:	
Contact details for respondent: Name of primary contact: Telephone: Email:	
Relevant office locations, and functions performed in each geographical location:	

Security Function	**Weight (%)**	**Evidence Request**	**Justification**
1. Information Security Governance and Capabilities		• Defined Information Security Roles & Functions • Reporting frequency to Senior Management and table of contents of report • Established security framework • Change Management procedure.	Sets the foundation for security practices aligned with business and regulatory needs and industry standards.
2. Risk Management Process		• Risk Management Framework • Risk Appetite Statement • Information Security Policy • Acceptable Use Policy • Sources of threat Intel • Cybersecurity strategy • Relevant insurance including cybersecurity.	Essential for ongoing risk identification, assessment, and prioritisation.
3. Compliance with industry Standards		• Frequency and latest Independent Security Assurance reports/certificates (ISO 27001+SOA +report, SOC 2, ASAE 3402, 3150, PCIDSS, etc)	Independent assurance over the adequacy and operating effectiveness of information security management system.

FSC Guidance Note No. 54

Security Function	Weight (%)	Evidence Request	Justification
4.Data Processing & Storage		• Listing of all locations/geographic regions where customer/business data will be stored and/or processed including redundancy and/or backup • Listing of all third- and fourth-party suppliers that handles, processes and/or store customer data, their purpose, locations/geographic regions.	Confirms data jurisdiction.
5. Data Protection and Privacy		• Privacy Policy • Data handling and classification policy and procedure • Data Privacy Policy • Information Security Policy • Crypto Policy and Key Management process • Evidence of information asset register • Threats and vulnerabilities listed and evidence that these are regularly reviewed and processes updated according to current threat analysis • SSL Lab report for public certificates. Screenshot of back-end configuration of TLS (e.g. load balancer) • Screenshot showing encryption enabled, confirmation of method of encryption applied and algorithm used on data stores (end-user devices, databases, file servers, cloud storage, virtual disks and backup systems) • Evidence of secure data destruction.	Central to regulatory compliance and securing sensitive information.
6. Network and Systems Security		• Network diagram • Architectural diagram • System hardening standards • Evidence of IPS and IDS • Evidence of AV on endpoints • Screenshot or report from application whitelisting tool • List of any end-of-life and/or end of support systems in use • Evidence of SOC or monitoring procedure • Logging standard or policy • Frequency and latest independent Pentest attestation letter of internal network and status of remediation of any critical or high findings.	Prevents unauthorised access and ensures the confidentiality and integrity and availability of data.
7. Physical Security and Employee Management		• Secure Access Protocols • Vetting and or background checking procedure for staff	

FSC Guidance Note No. 54

Security Function	Weight (%)	Evidence Request	Justification
		• Confidentiality and non-disclosure policies and procedures for staff and third parties including disciplinary procedures and recourse.	
8. Vulnerability Management		• Vulnerability management process (including patching timeframes) • Percentage of systems hosting critical CDEs full authenticated scanned within last 30 days • Number of high severity (e.g. Qualys 4/5) vulnerabilities per server over 30 day • Percentage of APIs and Applications penetration tested in the last year • Number of open high penetration testing findings.	Measures the number and remediation progress of software bugs identified through tools and manual checks
9. Application Security and Secure Software Development (DevOps)		• Secure coding standards • Secure coding principles • Training program for Developers • Evidence of separation of dev, test, and prod environments • Evidence of SAST, DAST tools • Evidence of WAF • Frequency and latest independent Pentest attestation letter of application and status of remediation of any critical or high findings.	Ensures the secure development of systems.
10. Logging and Monitoring		• Percentage or number of systems being monitored for both availability and security alerts • Percentage of systems reporting into the monitoring platform for 100% of last month console (coverage) • Number of high severity events that have not been reported to us within the SLA • Percentage of high severity alert compared to low severity (how good is the triage process) • Number of qualified security breaches • Number of security playbooks defined and tested • Material control weakness and incident notification processes.	Measures the identification of anomalous activity and the speed required to determine whether it is benign or dangerous.
11. Access Control and Identity Management		• Access Control Policy • Password Management Standard • Access provisioning and deprovisioning process • Evidence of Support of MFA • Evidence of Support of SSO	Prevents unauthorised access to systems and data.

FSC Guidance Note No. 54

Security Function	Weight (%)	Evidence Request	Justification
		• Frequency of access reviews for standard and privileged users. • Number of systems not integrated into enterprise directory/ID management • average number of individual accounts per user (proliferation of accounts) • Percentage privileged accounts compared to regular accounts • Percentage of dormant accounts (not used for more than 30 days) • Percentage externally facing systems with MFA.	
12. Security Training and Awareness		• Security training topics covered and frequency • Training results • Phishing simulation statistics • Security clauses covered in employment contracts, including survival clauses.	Mitigates human-related security risks through education and awareness.
13. Incident Response and Management		• Incident management process • Evidence of Playbooks • Test results of playbooks • Defined incident notification timeframe • Defined notification timeframe for material control weaknesses • Include key contact details for the vendor in the case of an incident • Report of last incident response simulation exercise conducted in the last 12 months.	Ability to minimise impact, respond and recover from security incidents through preparedness and swift action.
13. Business Continuity and Disaster Recovery Planning		• Defined RTO • Defined RPO • DR/BCP Test Frequency • Latest DR/BCP Test results and any improvement actions • Latest Backup restore results	Ensures operational resilience and recovery capabilities.
14. Third-Party Security Management		• Supplier relationship policy and process • Evidence of third-party assessments and ongoing monitoring • Security clauses covered in supplier contracts.	Ensures security is maintained throughout the supply chain.

FSC
FINANCIAL
SERVICES
COUNCIL

fsc.org.au