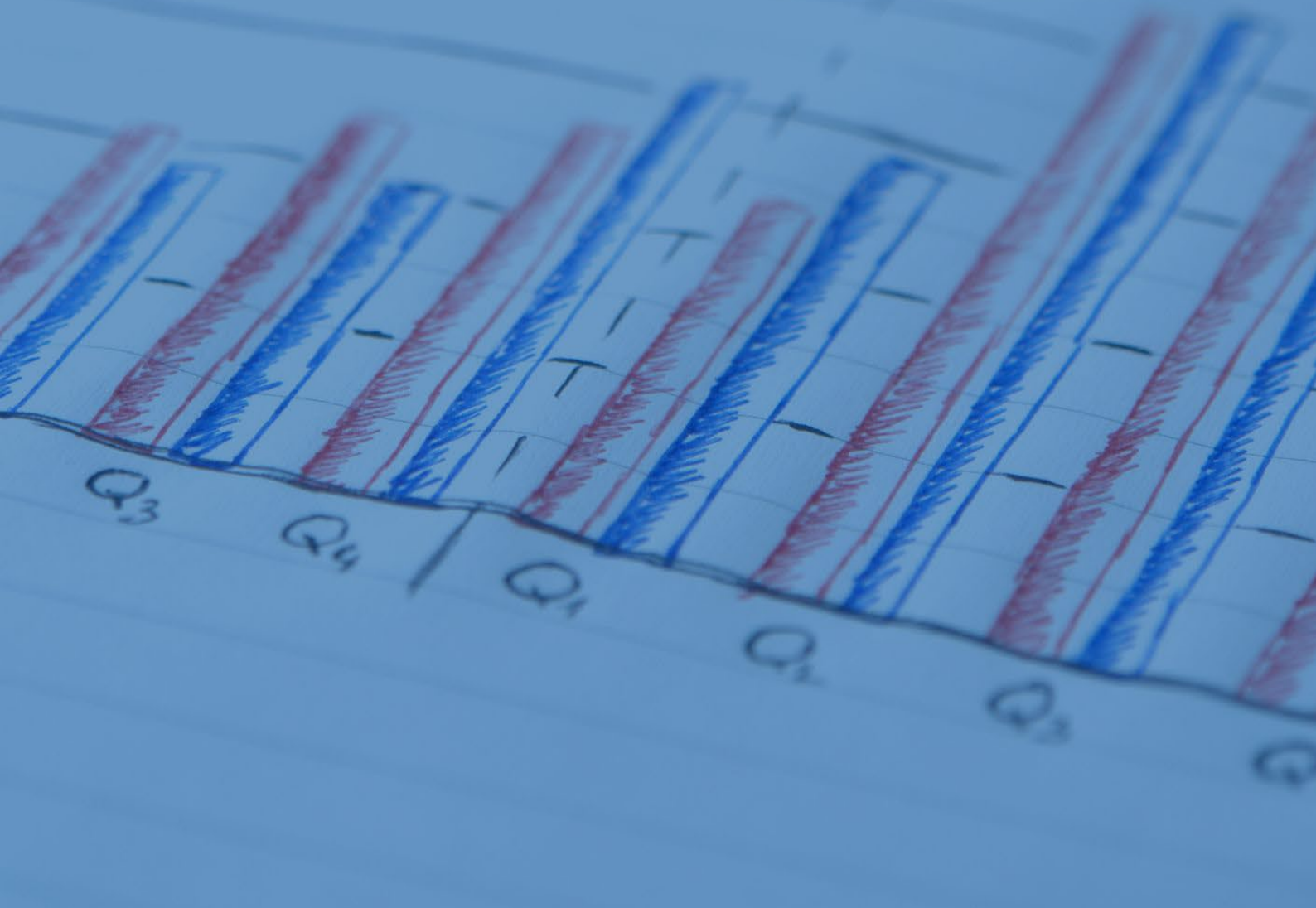
Apprenticeships Are Us

SYSTEM AND ORGANISATION CONTROL REPORT REVIEW POLICY AND CHECKLIST



PURPOSE

The purpose of this policy and checklist is to ensure Apprenticeships Are Us Ltd (ARU) conducts an annual, structured review of System and Organisation Control (SOC) reports for all key third-party service providers and vendors who manage financial data, personal information, or IT systems critical to ARU's operations.

This process is designed to:

- Validate the adequacy and effectiveness of third-party internal controls over data security, privacy, and financial integrity.
- Identify potential deficiencies or exceptions that could impact ARU's compliance or service delivery.
- Demonstrate due diligence in accordance with governance, audit, and regulatory standards.

LEGISLATIVE AND STANDARDS ALIGNMENT

The SOC review process supports ARU's obligations under:

- **Privacy Act 1988 (Cth)** – Australian Privacy Principles (APP 11: Security of Personal Information)
- **Cyber Security Act 2018 (Cth)**
- **ISO/IEC 27001:2022** – Information Security Management Systems (Annex A: Controls 5.18, 5.21, and 5.23)
- **ACSC Essential Eight** – Vendor risk management, application hardening, and access control
- **National Standards for Group Training Organisations (2017)**

SCOPE

This policy applies to all third-party service providers engaged by ARU who manage or host:

- Financial systems (e.g., MYOB, Workforce One)
- Cloud storage and infrastructure (Microsoft 365 / Azure)
- Data analytics and reporting (Power BI)
- Governance and compliance systems (BoardEffect)

The SOC review must be completed annually by the Operations Manager and tabled at the Continuous Improvement Committee (CIC) meeting, with a summary provided to the ARU Board of Directors.

DEFINITIONS

Term	Definition
SOC Report	An independent auditor's report issued under the AICPA framework assessing the effectiveness of a service provider's internal controls.
SOC 1 Report	Focuses on controls relevant to **financial reporting** (e.g., MYOB, Workforce One).
SOC 2 Report	Focuses on controls related to **security, availability, processing integrity, confidentiality, and privacy** (e.g., Microsoft 365, Azure).
Type I Report	Evaluates whether controls are suitably designed at a specific point in time.
Type II Report	Tests whether controls operated effectively over a defined period (usually 6–12 months).
RTO (Recovery Time Objective)	Maximum acceptable downtime before business operations must be restored.
RPO (Recovery Point Objective)	Maximum acceptable data loss measured in time.

VENDOR AND REPORT DETAILS

Field	Information to Record
Vendor Name	e.g., MYOB / Microsoft Azure / Workforce One
Service Provided	Payroll, Data Hosting, CRM, etc.
SOC Report Type	SOC 1 Type I / SOC 1 Type II / SOC 2 Type I / SOC 2 Type II
Reporting Period	___ to ___
Report Issued By	(Name of Independent Auditor)
Date Received by ARU	___

EXECUTIVE SUMMARY – AUDITOR'S OPINION

☐ Unqualified – No exceptions ☐ Qualified – Exceptions noted ☐ Adverse – Significant deficiencies

Summary of Findings / Exceptions (if any):

Reviewer's Assessment:

☐ All controls effective ☐ Minor improvement areas ☐ Significant risk identified

DETAILED REVIEW QUESTIONS

Category	Key Question	Y/N/N-A	Comments / Actions Required
Scope & Applicability	Does the SOC report cover all systems ARU relies upon?		
Control Effectiveness	Were any control failures reported that could affect ARU's data or financial records?		
Access Management	Does the vendor restrict user/admin access based on least-privilege principles?		
Change Management	Are changes to the vendor's systems tested, approved, and documented?		
Data Security & Encryption	Is data encrypted in transit and at rest?		
Incident Response & Notification	Does the vendor have an incident-response plan and notify clients of breaches?		
Back-ups / DR Capability	Are backups tested and DR objectives met (RTO/RPO)?		
Sub-service Organisations	Are subcontractors relied upon, and are they included in the SOC scope?		
Independent Auditor Credentials	Was the report issued by a licensed CPA/Chartered Accountant firm?		
Remediation Evidence	Have prior-year exceptions been remediated?		

RISK RATING AND FOLLOW-UP ACTIONS

Overall Risk Level	**☐ Low ☐ Medium ☐ High**
Required Actions (if any):	
Responsible Officer:	
Due Date for Completion:	

SIGN-OFF

Name / Position	Signature	Date
Finance Manager		
General Manager		
Managing Director		

REPORTING AND RECORD KEEPING

- Completed checklists and all supporting SOC documentation are to be stored securely in SharePoint.
- All exceptions, remediation actions, and risk ratings are to be logged in the Risk Register and discussed at the next CIC meeting.
- The Compliance Officer is responsible for monitoring progress of any required corrective actions.
- The ARU Board will be notified of any High Risk or Adverse SOC findings immediately.

ENFORCEMENT

Failure to complete or maintain annual SOC reviews may result in:

- Non-compliance findings under the *National Standards for GTOs (2017)*.
- Audit qualifications or management letter findings.
- Disciplinary or corrective action for staff responsible for vendor oversight.

DOCUMENT CONTROL

Version	Authorised by	Authorisation Date	Change Summary
1.0	ARU Board of Directors	01/07/2025	Initial release – aligned with Vendor Performance Review Framework