CLN - THIRD PARTY RISK AND CONTRACT MANAGEMENT DECISION TREE TOOLKIT

Phase Description			Feasibility	Selection	Onboarding	Vendor Management	Offboarding
			Quickly determine whether engaging a new third party makes sense from a business and risk perspective	Evaluate potential suppliers against requirements and risk appetite, then choose the best fit	Configure the organization and the vendor so they can begin delivering services in a controlled, secure and compliant way	Continuously monitor and manage vendor performance, risk and compliance over the lift of the engagement	Exit the relationship in a controlled manner that preserves data integrity, commercial rights and business continuity
Assurance Level	**Low**	**Risk/Complexity/Maturity:** Minimal. No or very limited access to sensitive data, systems or regulated environments. Often one-off, commoditized or non-strategic buys. **Due-Diligence Profile:** Lightweight – standardized contract terms, basic supplier self-attestation, automated onboarding checklists. **Examples:** Office supplies, catering, minor facilities services in a small or early-stage organization.	• Basic internet search for the company • Basic business ABN search • Check with peers/professional network for feedback • Check website on previous clients • Check for online reviews • Check for red flags via media or regular reports • Check website for security/privacy policy • Check for corporate "blacklist" (if available) eg software • Check for "About us" page • Check for advisory firms' assessment (eg Gartner)	• Vendor submit security questionnaire - single simple/standard questionnaire, pass/fail outcome • Simple questionnaire of what their cyber security capability is	• Use the Chrome extension for securityscorecard.com and assess their rating • Review third party security assessment providers (eg securityscorecard.com) • Verify minimum insurance limits required and any basic compliance certs (eg ISO 27001, PCI DSS notice if they handle cards) • Generic Cyber terms in a contract • Third-Party Inventory Register – key columns: vendor name, risk tier, data access required, contract start/end, next review date • Insurance and Liability Matrix – a simple table capturing each vendor's minimum required cover (eg cyber liability, professional indemnity) and proof of cover expiration	• Organized Meeting, eg annual/three years • Maintain vendor contact logs and change notification procedures • Reviewing security requirements if they change for third-party IT solutions	• Ensure accounts/identities are disabled and credentials revoked • Reclaim physical assets if any • Archive documentation for audit trail/file for record (who, what, when offboarded) • Update third-party inventory register
	Medium	**Risk/Complexity/Maturity:** Moderate. Some internal data exposure, SLAs matter, limited regulatory scope or business-continuity implications. Appropriate for a mid-sized or growing organization. **Due-Diligence Profile:** Mid-depth – vendor questionnaires (security, privacy), financial health checks, moderately tailored contract clauses, periodic performance and risk reviews. **Examples:** Marketing agencies, HR/Payroll platforms, test/dev cloud services in a regulated business.	• Assess whether the vendor is on government panels as they will have performed a feasibility assessment • Check with Procurement to see if vendor has been engaged with previously and if performance/compliance has been assessed • Conduct a cross jurisdictional scan to see if anyone interstate (similar government department or company) has any experience with the vendor • Threat and Risk assessment • Check Office of the Information Commissioner for breaches • Review certifications/ISO 27001 SOA	• Conduct Foreign Interference risk assessment (Home Affairs advice) • Identify contractual clauses • Hosting arrangements and risk • Vendor submit security questionnaire – Questionnaire tailored to organization, Identify risks associated with control gaps and required mitigation actions for Pass, Questions adjusted for risk/info security classification • Privacy threshold assessment • Privacy impact assessment (if needed) • Custom questionnaire – Tiered security risk assessment spreadsheet (prebuilt Excel/Sheets template that automatically flags "Medium/High" risk vendors based on their answers and data-sensitivity profile • Vendor security assessment with result and any additional requirements	• Validate if vendor maintains an acceptable insurance policy, eg cyber liability • Third-Party Incident Response Plan testing (tabletops) • Audit Evidence Validation • Initial Penetration Test – if the vendor will host or un code in your environment, require a pen-test summary report or third-party code review before onboarding • Company Specific Generic Cyber Terms in a Contract • Contractual Security Annex and SLA Schedule –a fill-in-the-blanks annex that spells out minimum SLAs, eg incident notification <= 24 hours, vulnerability remediation <= 30 days, regular security reviews and questionnaires • SOC 2 Type II / ISO 27001 Audit Report Repository – a secure folder or SharePoint library where copies of incoming third- party audit reports are kept, includes metadata (reporting period, scope, issuing firm) • Third-Party Incident Response Plan Summary – extract from the vendor's IR plan showing roles, escalation paths, notification timelines and sample playbooks	• Review SLAs against cyber performance and incident response timelines • Request annual updates to cyber questionnaires or certifications • Conduct joint tabletop exercises for incident preparedness (for critical vendors) • Security design/architecture checks performed prior to implementation • QITC – Good Practice Guide	• Retrieve or verify data deletion/destruction certificates • Remove vendor integrations from production environments • Confirm contract obligations, eg termination terms, have been met • Update vendor register • Offboarding meeting/workshop to ensure compliance/performance feedback/reflections • Formal notice of termination • Completed offboarding checklist • Prevalent Vendor Offboarding due diligence guide
	High	**Risk/Complexity/Maturity**: Significant to Critical. Handling sensitive/regulated data, core business processes or large-scale infrastructure. Typical in large enterprises, government or highly regulated industries. **Due-Diligence Profile**: Rigorous – full security audit or onsite review, proof of third-party certifications (SOC2, ISO 27001, etc), background checks, granular SLAs, continuous monitoring and executive-level governance. **Examples:** Payment processors, production-grade cloud providers, healthcare records management, national-scale IT service providers.	• Use of special website services for organization information/intelligence • Review financial stability via business credit reporting services (eg Equifax, Illion) • Relying on specific vendors • Conduct preliminary threat modelling including potential geopolitical risk factors • Review certifications/ISO 27001 SOA	• Conduct Foreign Interference risk assessment (Home Affairs advice) • Identify contractual clauses • Usage of AI policies	• SOC2 • Perform red team assessments if vendor handles critical assets • "Guideline" providing guidance on generic cyber security clauses/requirements to include with contracts • Include advanced cyber clauses based on sensitivity of data/system exposure • High-risk vendor kick-off workshop – cross-functional workshop (Security, Legal, Procurement, Operations, Business Owner) to align on scope, escalation, data flows, ingress/egress points and governance • As-built security checks performed prior to release • Third-party Continuous Monitoring Plan – documented cadence and tooling for ingesting vendor logs into SIEM, continuous scanning (vuln, container, cloud posture) and threat-intel feeds • Business Impact Analysis (BIA) – describing how a vendor outage or breach would cascade thru the org) • Comprehensive Vendor Due-Diligence Report – a multi-section report including legal entity checks, financial health, past incidents regulatory filings, etc • Vendor Securit Architecture and Data Flow Diagrams – Full technical illustration of how the vendor's systems connect (networks, APIs, data classification, segmentation • Some activities may or may not be required depending on the risk/criticality of the vendor in question	• Vendor Management Plan including Contract Performance KPIs • Automation of third-party assessment process • Include KPIs for contract compliance, security metrics and performance outcomes • Use vendor risk management platforms, eg Archer, ProcessUnity, for continuous monitoring • Commonwealth Government Guidance	• Conduct post-offboarding security review, eg residual access, data remnants • Require attestation of data purging from vendor systems and backups • Formal notice of termination • Completed offboarding checklist • Prevalent Vendor Offboarding due diligence guide
Stakeholder(s) Involved			**Procurement:** Past engagements, financial standing **Security:** Intelligence tools, threat modelling **Legal:** Reputation, public records	**Privacy Office:** Threshold assessment and PIA	**Procurement:** Due diligence and documentation **Security:** Assurance and validation **Legal:** Contract language	**Business Owner:** Relationship oversight **Security:** Risk metrics and compliance **Contract Managers:** SLA enforcement **IT:** Solution development and delivery	**IT Operations:** System Access **Security:** Data handling, risk review **Legal:** Compliance closure

Legend

Key Activity	Artefact	Good Practice Guide

TLP: AMBER

Allies in Cyber Security

Dr Ivano Bongiovanni – General Manager
i.bongiovanni@uq.edu.au

James Chadwick – Principal GRC Specialist
j.chadwick@uq.edu.au

The University of Queensland | St Lucia, Q 4072 Australia

ABN: 63 842 912 684

t +61 7 3365 4417

e membership@auscert.org.au

w auscert.org.au