THIRD-PARTY RISK REVIEW

ITSM VENDOR GOVERNANCE

CHECKLIST

guides.matstrange.net

PURPOSE

Ensure every vendor renewal and new contract passes a consistent set of control checks before sign-off. Prevent critical security, resiliency, compliance, and communication gaps from being missed under time pressure. Provide a single audit-ready record of vendor risk posture tied to ITSM requirements.

How to use this checklist: Complete one row per vendor. Assign an owner for each control area. Record the evidence reviewed, assign a risk level (Critical / High / Medium / Low), and document the recommended remediation where gaps exist. Escalate Critical and High findings before contract execution or renewal.

SECURITY CONTROLS

Review all security controls relevant to data handling, access management, and incident response.

CONTROL AREA	EVIDENCE REQUIRED	OWNER	RISK LEVEL	RECOMMENDED REMEDIATION
Data encryption at rest	Vendor encryption policy, certificate or audit extract	Security Lead		
Data encryption in transit	TLS configuration documentation or third-party scan report	Security Lead		
Access control and least privilege	IAM policy documentation, role matrix	Security Lead		
Privileged access management	PAM tool evidence, audit logs sample	Security Lead		
Vulnerability management programme	Patch cadence policy, last scan report	Security Lead		
Penetration testing	Most recent pen test report (within 12 months)	Security Lead		
Security incident response plan	Documented IRP with defined SLAs for notification	Security Lead		
Multi-factor authentication enforcement	MFA policy scope document	Security Lead		
Employee security awareness training	Training completion records or policy	Security Lead		
Third-party sub-processor controls	Sub-processor list and applicable contractual clauses	Security Lead		

RESILIENCY CLAIMS

Validate that vendor resiliency commitments are evidenced and tested, not just stated.

CONTROL AREA	EVIDENCE REQUIRED	OWNER	RISK LEVEL	RECOMMENDED REMEDIATION
Recovery Time Objective (RTO)	Documented RTO with supporting DR test results	Service Owner		
Recovery Point Objective (RPO)	Documented RPO with backup schedule and test evidence	Service Owner		
Business continuity plan	Current BCP document, last review date	Service Owner		
Disaster recovery test results	DR test report within last 12 months	Service Owner		
Redundancy and failover architecture	Infrastructure diagram showing redundancy	Service Owner		
SLA uptime commitments	Signed SLA extract with uptime percentage	Service Owner		
Historical uptime performance	12-month uptime report or status page history	Service Owner		
Incident history and post-incident reviews	PIR summaries for all P1/P2 incidents in past 12 months	Service Owner		
Capacity planning evidence	Capacity review documentation	Service Owner		

COMPLIANCE CERTIFICATIONS

Confirm that all applicable certifications are current, scoped correctly, and cover the services being procured.

CONTROL AREA	EVIDENCE REQUIRED	OWNER	RISK LEVEL	RECOMMENDED REMEDIATION
ISO 27001 certification	Current certificate with scope statement	Compliance Lead		
SOC 2 Type II report	Most recent SOC 2 Type II report (within 12 months)	Compliance Lead		
Cyber Essentials / Plus (UK)	Valid certificate	Compliance Lead		
GDPR / UK GDPR compliance	Data Processing Agreement (DPA) signed	Compliance Lead		
PCI DSS (if applicable)	AOC or SAQ; confirm scope includes relevant services	Compliance Lead		
DORA readiness (if applicable)	ICT risk management documentation	Compliance Lead		
Right to audit clause	Confirmed in contract	Compliance Lead		
Certification renewal calendar	Confirmed expiry dates for all active certs	Compliance Lead		
Data residency confirmation	Written confirmation of data storage locations	Compliance Lead		

COMMUNICATION PLANS

Verify that the vendor has defined, tested, and contractually committed communication processes for incidents and changes.

CONTROL AREA	EVIDENCE REQUIRED	OWNER	RISK LEVEL	RECOMMENDED REMEDIATION
Incident notification SLA	Contract clause or SLA defining notification timescales	Service Owner		
Named escalation contacts	Escalation matrix with named contacts and numbers	Service Owner		
Major incident communication process	Documented major incident comms procedure	Service Owner		
Planned maintenance notification window	Agreed notice period in contract or SLA	Service Owner		
Change advisory process	Defined change communication process	Change Manager		
Status page or service notification feed	URL or feed reference confirmed	Service Owner		
Post-incident report commitment	SLA for PIR delivery after major incidents	Service Owner		
Executive escalation path	Named executive sponsor or account director	Relationship Owner		

RISK LEVEL KEY

LEVEL	DEFINITION
Critical	Immediate contractual or regulatory exposure; do not proceed without resolution
High	Significant gap requiring remediation plan with agreed deadline before sign-off
Medium	Acceptable short-term; remediation required within agreed timeframe
Low	Minor gap; monitor and review at next scheduled assessment

SIGN-OFF BLOCK

Reviewer name: _____ Vendor name: _____ Contract / renewal date: _____ Review date: _____ Overall risk rating: _____ Approved to proceed: Yes / No / Conditional Conditions (if applicable): _____ Approver signature: _____

CONDITIONAL APPROVAL PATH

If Conditional is selected, the following must be completed before execution or renewal:

ACTION	OWNER	DUE DATE
Remediation item 1		
Remediation item 2		
Sign-off re-evaluation		

Conditional approvals expire on: _____ Escalation if remediation not complete: _____