VENDOR RISK ASSESSMENT CHECKLIST

VENDOR'S NAME	**ABC Company**	PHONE	
PERSON OF CONTACT	**Andrew Smith**	ADDRESS	
EMAIL	andrew@abccompany.com	DATE OF ASSESSMENT	

CATEGORY	CONTROL/REQUIREMENT	RESPONSE	EVIDENCE	ANALYST VALIDATION	RISK LEVEL	ADDITIONAL NOTES
GOVERNANCE & COMPLIANCE	Does the vendor comply with relevant regulations (e.g., GDPR, HIPAA, PCI-DSS)?	Partial	Copy of compliance certificates, attestation letters, or regulatory audit reports provided.	Verified authenticity of certificates; confirmed scope covers vendor's operations.	MEDIUM	
	Does the vendor have documented security policies and procedures?	Yes	Latest version of Information Security Policy & SOPs uploaded to secure portal.	Reviewed policy version & effective date; found incomplete sections—follow-up requested.	LOW	
	Has the vendor assigned a security officer or responsible person for cybersecurity?	Partial	Organizational chart showing named CISO; job description provided.	Confirmed individual employed and responsible; LinkedIn & HR confirmation received.	MEDIUM	
DATA SECURITY	Is sensitive data encrypted at rest and in transit?	Yes	Screenshots/config docs of encryption settings; TLS certificates; encryption policy.	Checked sample data flow; confirmed AES-256 at rest & TLS1.2+ in transit.	LOW	
	Does the vendor conduct regular vulnerability scan?	Yes	Latest quarterly vulnerability scan report (redacted).	Confirmed scan date ≤90 days old; risk items tracked; no critical unaddressed findings.	LOW	
	Are regular backups performed and tested?	Yes	Backup schedule & last restore test report provided.	Verified successful restore test logs; random spot check done.	LOW	
ACCESS MANAGEMENT	Is there a process for role-based access control (least privilege)?	Partial	Access matrix / RBAC policy document.	Reviewed sample user roles vs privileges; minor over-provisioning noted.	MEDIUM	
	Does the vendor use multi-factor authentication (MFA) for critical systems?	Yes	Screenshot of MFA settings on admin console; MFA policy doc.	Verified by test login with vendor-provided demo account.	LOW	
	Are user accounts reviewed regularly to remove inactive/terminated users?	Yes	Last quarterly user access review report.	Checked random sample of terminated users; accounts disabled timely.	LOW	
BUSINESS CONTINUITY	Does the vendor have a tested disaster recovery and business continuity plan?	Partial	Copy of BCP/DRP with test results and lessons learned report.	Confirmed last test date & participants; improvement actions tracked.	MEDIUM	
	Has the Disaster Recovery Plan (DRP) been tested in the past 12 months?	No	Vendor provided outdated DRP test report (last test 3 years ago).	Verified date <12 months; test objectives achieved.	HIGH	
	Does the vendor have an incident response process for handling breaches?	Yes	Incident Response Plan + escalation flowchart.	Verified last test date in report is >12 months old.	LOW	
THIRD-PARTY MANAGEMENT	Does the vendor conduct risk assessments of its own third parties (subcontractors)?	Yes	Third-party risk policy + sample vendor risk assessment report.	Confirmed process covers critical vendors; saw evidence of follow-up	LOW	
	Are vendors required to sign security/privacy agreements before onboarding?	No	Vendor contracts provided — only standard commercial terms, no DPA/NDA sections.	Cross-checked contract templates against privacy clause checklist — missing required clauses.	HIGH	
	Is there a process to monitor third-party performance and compliance on an ongoing basis?	Yes	SLA monitoring dashboard screenshots or audit schedule.	Checked metrics updated monthly; alerts in place for non-compliance.	LOW	