

VENDOR QUESTIONNAIRE FRAMEWORK

Base Assessment + Industry-Specific Modules

Available at www.tpvrn.net/documents | *The Future of Third-Party Risk Management & Data Privacy*

This framework offers a structured set of due diligence questions organized by security domain. The base questionnaire applies to all vendor relationships that meet the ITC threshold. Industry-specific modules are added as needed based on the vendor's sector, data types, and regulatory environment identified in the ITC.

Response guidance: Vendors must answer every question and provide supporting evidence as required. Unanswered questions or unsupported "Yes" answers will be followed up on before closing the assessment.

PART 1: BASE QUESTIONNAIRE (ALL VENDORS)

VENDOR IDENTIFICATION

Vendor Legal Name	
Primary Security Contact	
Date of Response	
Services in Scope	

DOMAIN 1: INFORMATION SECURITY GOVERNANCE

Domain	Question	Response	Evidence Required
Governance	Does the organization maintain a documented Information Security Policy approved by senior management?	☐ Yes ☐ No ☐ N/A	Policy document
Governance	Is there a designated Chief Information Security Officer (CISO) or equivalent security leadership role?	☐ Yes ☐ No ☐ N/A	Org chart
Governance	Does the organization hold an ISO 27001 certification or SOC 2 Type II report?	☐ Yes ☐ No ☐ N/A	Certificate / Report
Governance	Are information security roles and responsibilities formally documented?	☐ Yes ☐ No ☐ N/A	Role documentation
Governance	Is the security program reviewed and updated at least annually?	☐ Yes ☐ No ☐ N/A	Review records

DOMAIN 2: ACCESS CONTROL

Domain	Question	Response	Evidence Required
Access Control	Is access to systems containing organizational data limited to authorized personnel on a least-privilege basis?	☐ Yes ☐ No ☐ N/A	Access policy
Access Control	Is multi-factor authentication (MFA) required for remote access and privileged accounts?	☐ Yes ☐ No ☐ N/A	MFA configuration
Access Control	Are access rights reviewed and recertified at least annually?	☐ Yes ☐ No ☐ N/A	Review records
Access Control	Is a formal process in place to revoke access for terminated employees?	☐ Yes ☐ No ☐ N/A	Offboarding procedure
Access Control	Are privileged access activities logged and monitored?	☐ Yes ☐ No ☐ N/A	Log samples

DOMAIN 3: DATA SECURITY

Domain	Question	Response	Evidence Required
Data Security	Is data classified according to a formal data classification policy?	☐ Yes ☐ No ☐ N/A	Classification policy
Data Security	Is organizational data encrypted at rest using AES-256 or equivalent?	☐ Yes ☐ No ☐ N/A	Encryption specification
Data Security	Is organizational data encrypted in transit using TLS 1.2 or higher?	☐ Yes ☐ No ☐ N/A	Transport configuration
Data Security	Is a data inventory and mapping process maintained for all data types handled on behalf of the organization?	☐ Yes ☐ No ☐ N/A	Data inventory
Data Security	Is a documented data retention and secure disposal policy in place?	☐ Yes ☐ No ☐ N/A	Retention policy, disposal records
Data Security	Is organizational data stored in dedicated environments segregated from other clients?	☐ Yes ☐ No ☐ N/A	Architecture documentation

DOMAIN 4: VULNERABILITY AND PATCH MANAGEMENT

Domain	Question	Response	Evidence Required
Vulnerability Mgmt	Are vulnerability scans conducted at least quarterly for systems handling organizational data?	☐ Yes ☐ No ☐ N/A	Scan reports
Vulnerability Mgmt	Is penetration testing conducted at least annually by a qualified third party?	☐ Yes ☐ No ☐ N/A	Pentest summary / attestation
Vulnerability Mgmt	Are critical patches applied within 30 days of release? High-risk within 90 days?	☐ Yes ☐ No ☐ N/A	Patch management policy
Vulnerability Mgmt	Is a formal vulnerability management program with defined SLAs in place?	☐ Yes ☐ No ☐ N/A	Program documentation

DOMAIN 5: INCIDENT RESPONSE AND NOTIFICATION

Domain	Question	Response	Evidence Required
Incident Response	Does the organization maintain a documented Incident Response Plan?	☐ Yes ☐ No ☐ N/A	IRP document
Incident Response	Is the IRP tested at least annually through tabletop or full exercise?	☐ Yes ☐ No ☐ N/A	Exercise records
Incident Response	Will the organization notify the contracting party within 72 hours of a confirmed security incident affecting organizational data?	☐ Yes ☐ No ☐ N/A	Notification policy
Incident Response	Are security incident logs retained for a minimum of 12 months?	☐ Yes ☐ No ☐ N/A	Retention policy
Incident Response	Has the organization experienced a security incident in the past 24 months? If yes, please describe the nature and remediation.	☐ Yes ☐ No ☐ N/A	Incident summary

DOMAIN 6: BUSINESS CONTINUITY AND DISASTER RECOVERY

Domain	Question	Response	Evidence Required
BCM / DR	Does the organization maintain a documented Business Continuity Plan (BCP)?	☐ Yes ☐ No ☐ N/A	BCP document or attestation
BCM / DR	Is the BCP tested at least annually?	☐ Yes ☐ No ☐ N/A	Test records
BCM / DR	What are the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for services provided to the organization?	☐ Yes ☐ No ☐ N/A	RTO/RPO documentation
BCM / DR	Are backups of organizational data maintained and tested regularly?	☐ Yes ☐ No ☐ N/A	Backup/restore test records

DOMAIN 7: THIRD-PARTY AND SUPPLY CHAIN RISK

Domain	Question	Response	Evidence Required
Supply Chain	Does the organization maintain a current inventory of subprocessors and sub-vendors with access to organizational data?	☐ Yes ☐ No ☐ N/A	Subprocessor list
Supply Chain	Are subprocessors subject to equivalent security requirements through contractual flow-down?	☐ Yes ☐ No ☐ N/A	Contract terms / attestation
Supply Chain	Is prior approval or advance notification required before engaging new subprocessors?	☐ Yes ☐ No ☐ N/A	Subprocessor policy
Supply Chain	Is a software bill of materials (SBOM) maintained for software products provided?	☐ Yes ☐ No ☐ N/A	SBOM

PART 2: HEALTHCARE MODULE (HIPAA)

Include when: Vendor handles PHI or operates as a HIPAA Business Associate.

Domain	Question	Response	Evidence Required
HIPAA	Has the organization executed a HIPAA Business Associate Agreement (BAA) with covered entities?	☐ Yes ☐ No ☐ N/A	BAA template
HIPAA	Has the organization completed a HIPAA Security Rule risk analysis within the past 12 months?	☐ Yes ☐ No ☐ N/A	Risk analysis summary
HIPAA	Does the organization maintain a documented PHI breach notification procedure meeting the 60-day notification requirement?	☐ Yes ☐ No ☐ N/A	Breach notification policy
HIPAA	Are workforce members trained on HIPAA requirements at least annually?	☐ Yes ☐ No ☐ N/A	Training records
HIPAA	Is PHI accessible only to workforce members who need it for their job functions (minimum necessary standard)?	☐ Yes ☐ No ☐ N/A	Access control documentation
HIPAA	Are audit logs maintained for all access to PHI systems?	☐ Yes ☐ No ☐ N/A	Log samples
HIPAA	Does the organization have documented procedures for honoring individual rights requests (access, amendment, accounting of disclosures)?	☐ Yes ☐ No ☐ N/A	Procedures documentation

PART 3: FINANCIAL SERVICES MODULE (PCI DSS + DORA)

Include when: Vendor processes cardholder data or is subject to DORA as an ICT third-party service provider.

PCI DSS Questions

Domain	Question	Response	Evidence Required
PCI DSS	What PCI DSS level applies and has compliance been validated by a QSA?	☐ Yes ☐ No ☐ N/A	AoC / ROC
PCI DSS	Is cardholder data encrypted end-to-end, including in transit and at rest?	☐ Yes ☐ No ☐ N/A	Encryption specification
PCI DSS	Are cardholder data environments segmented from other networks?	☐ Yes ☐ No ☐ N/A	Network architecture diagram
PCI DSS	Is a Web Application Firewall (WAF) deployed for all web-facing cardholder data systems?	☐ Yes ☐ No ☐ N/A	WAF configuration
PCI DSS	Are vulnerability scans of cardholder data environments conducted quarterly by an ASV?	☐ Yes ☐ No ☐ N/A	ASV scan reports

DORA Questions

Domain	Question	Response	Evidence Required
DORA	Has the organization reviewed its DORA obligations as an ICT third-party service provider?	☐ Yes ☐ No ☐ N/A	DORA readiness assessment
DORA	Is the organization prepared to support DORA-required contractual provisions including audit rights and exit strategies?	☐ Yes ☐ No ☐ N/A	Contract template
DORA	Does the organization maintain a register of all ICT sub-service providers (sub-outsourcing) with access to financial entity data?	☐ Yes ☐ No ☐ N/A	Sub-outsourcing register
DORA	Is the organization prepared to participate in threat-led penetration testing (TLPT) as required by DORA?	☐ Yes ☐ No ☐ N/A	TLPT readiness

PART 4: GOVERNMENT MODULE (CMMC + CUI)

Include when: Vendor handles CUI, FCI, or supports federal contracts requiring CMMC certification.

Domain	Question	Response	Evidence Required
CMMC / CUI	What CMMC Level does the organization hold or is pursuing? Has a C3PAO assessment been completed?	☐ Yes ☐ No ☐ N/A	CMMC certificate / assessment
CMMC / CUI	Has the organization completed a System Security Plan (SSP) per NIST SP 800-171?	☐ Yes ☐ No ☐ N/A	SSP
CMMC / CUI	Does the organization have an open Plan of Action and Milestones (POA&M)?	☐ Yes ☐ No ☐ N/A	POA&M
CMMC / CUI	Is CUI clearly identified, labeled, and handled according to the CUI Registry requirements?	☐ Yes ☐ No ☐ N/A	CUI handling policy
CMMC / CUI	Are CUI handling requirements flowed down to subcontractors?	☐ Yes ☐ No ☐ N/A	Subcontract clauses
CMMC / CUI	Is access to CUI restricted to U.S. persons where required?	☐ Yes ☐ No ☐ N/A	Access control documentation

PART 5: AI GOVERNANCE MODULE

Include when: Vendor provides AI-enabled services, uses AI in service delivery, or will process organizational data through AI systems.

Domain	Question	Response	Evidence Required
AI Governance	Does the organization maintain a documented AI governance policy?	☐ Yes ☐ No ☐ N/A	AI governance policy
AI Governance	Will organizational data be used to train or fine-tune AI models?	☐ Yes ☐ No ☐ N/A	Data use terms
AI Governance	Are AI systems subject to pre-deployment testing including accuracy, bias, and fairness assessments?	☐ Yes ☐ No ☐ N/A	Testing documentation
AI Governance	Is model performance monitored in production for drift, degradation, and fairness?	☐ Yes ☐ No ☐ N/A	Monitoring procedures
AI Governance	Does the organization provide model cards or equivalent documentation for AI systems used in service delivery?	☐ Yes ☐ No ☐ N/A	Model card / documentation
AI Governance	Are there contractual prohibitions on using organizational data to train AI models without explicit consent?	☐ Yes ☐ No ☐ N/A	Contract terms
AI Governance	Does the vendor support the organization's right to human review of AI-driven decisions affecting the organization?	☐ Yes ☐ No ☐ N/A	Human review procedures

ASSESSOR SIGN-OFF

Assessment Completed By	
Assessment Date	
Overall Assessment Outcome	☐ Approved ☐ Conditional Approval ☐ Rejected ☐ Escalated
Open Issues / Remediation Required	