DOMINUS GRAY, LLC

Securing Access to Opportunity

Third-Party Risk Management Program

Built on Secure Controls Framework (SCF)

February 2026

Document ID: DG-TPRM-2026-001

CONFIDENTIAL — DO NOT DISTRIBUTE

SDVOSB | MBE | NaBOVA | VetHUB | SAM.gov Registered

Service-Disabled Veteran-Owned Small Business

Table of Contents

PART 1

TPRM Program Framework

1. Program Overview

Purpose

This Third-Party Risk Management (TPRM) Program establishes the framework, methodology, and assessment tools for evaluating and managing cybersecurity risks introduced through third-party vendors, suppliers, and service providers. The program is built upon the Secure Controls Framework (SCF) Third-Party Management (TPM) control domain to ensure comprehensive coverage of supply chain security requirements.

Scope

This program applies to all third-party entities that:

- Process, store, transmit, or have access to Controlled Unclassified Information (CUI)
- Provide information technology services, cloud hosting, or managed security services
- Have logical or physical access to organizational information systems or networks
- Provide critical business functions where service disruption would impact operations
- Handle sensitive business data, intellectual property, or personally identifiable information (PII)

Regulatory Drivers

Compliance Framework Alignment

This TPRM program satisfies supply chain risk management requirements across multiple regulatory frameworks:

- NIST SP 800-171 Rev 2 — Security Requirements for Protecting CUI (SR Family)
- CMMC 2.0 Level 2 — Supply chain risk management practices
- DFARS 252.204-7012 — Safeguarding Covered Defense Information
- DFARS 252.204-7020 — NIST SP 800-171 DoD Assessment Requirements
- NIST SP 800-161 — Cybersecurity Supply Chain Risk Management Practices
- SCF TPM Domain — Third-Party Management controls (TPM-01 through TPM-11)

Organizations operating within the Defense Industrial Base (DIB) are required to flow down NIST SP 800-171 security requirements to third-party vendors who process, store, or transmit CUI. This program provides the tools and methodology to assess, monitor, and manage third-party compliance with these requirements.

2. Vendor Tiering Model

All vendors are classified into one of three tiers based on the level of access to sensitive data, criticality to operations, and the nature of services provided. The tier classification determines the depth and frequency of security assessments.

TIER 1 — CRITICAL VENDORS

Criteria: Processes or stores CUI • Direct access to CUI systems • Essential to operations • Handles classified or export-controlled data

Assessment: Full comprehensive assessment (all domains) • Annual on-site review • Continuous monitoring • Quarterly risk reporting

Examples: Cloud service providers hosting CUI, managed security service providers (MSSPs), IT infrastructure providers with administrative access, software developers with access to CUI systems

TIER 2 — SIGNIFICANT VENDORS

Criteria: Access to sensitive business data (non-CUI) • Limited system access • Supports but not essential to critical operations • Handles PII or financial data

Assessment: Standard assessment (key domains) • Biannual review • Periodic monitoring • Semi-annual risk reporting

Examples: HR/payroll processors, financial service providers, business application SaaS vendors, professional services firms with data access

TIER 3 — STANDARD VENDORS

Criteria: No access to sensitive data • Commodity or readily replaceable services • No logical or physical access to information systems

Assessment: Abbreviated assessment (self-attestation questionnaire) • Periodic spot checks • Annual vendor inventory update

Examples: Office supply vendors, janitorial services, general consulting without data access, commodity SaaS tools without sensitive data

3. Risk Scoring Methodology

Vendor security maturity is evaluated using a 5-level maturity scale aligned with the Capability Maturity Model Integration (CMMI) and SCF control assessment methodology. Each assessment question is scored against this scale to produce domain scores and a composite vendor risk rating.

Maturity Level Definitions

L0 Not Performed — Score: 0

The control is not implemented. No evidence of any activity related to the control objective. This represents a critical gap requiring immediate remediation for Tier 1 vendors.

L1 Performed Informally — Score: 1

The control is performed on an ad hoc basis without formal documentation or consistent processes. Individuals may implement the control differently. Results are unpredictable and not repeatable.

L2 Planned & Tracked — Score: 2

The control is documented in policy and procedures. Implementation is consistent and tracked. Evidence exists but processes may not be optimized or fully automated.

L3 Well-Defined — Score: 3

The control is formally defined, consistently implemented, and integrated into organizational processes. Regular measurement and reporting. Automation supports consistent execution.

L4 Continuously Optimized — Score: 4

The control is continuously monitored, measured, and improved. Automated detection and response. Metrics drive proactive improvement. Industry-leading practices adopted.

Composite Risk Score Calculation

The composite vendor risk score is calculated by averaging domain scores weighted by the criticality of each domain relative to the vendor's tier classification:

Composite Risk Score Formula

Composite Score = Σ (Domain Score × Domain Weight) / Σ (Domain Weights)

Domain Score = Average maturity level of all questions within the domain (0–4 scale)
Domain Weight = Criticality multiplier based on vendor tier and domain relevance

For Tier 1 vendors: All domains weighted equally (weight = 1.0)
For Tier 2 vendors: Data Protection, Access Control, Incident Response weighted at 1.5x
For Tier 3 vendors: Only Governance, Compliance, and Data Protection domains assessed

Overall Risk Rating

SCORE RANGE	RISK RATING	REQUIRED ACTION

3.5 – 4.0	LOW RISK	Approved. Standard monitoring. Annual reassessment.
2.5 – 3.4	MODERATE RISK	Conditionally approved. Minor remediation required within 90 days.
1.5 – 2.4	ELEVATED RISK	Requires executive approval. Significant remediation within 60 days. Enhanced monitoring.
0.5 – 1.4	HIGH RISK	Not approved for Tier 1/2 services. Material remediation required within 30 days before re-engagement.
0.0 – 0.4	CRITICAL RISK	Immediate disengagement recommended. Vendor lacks fundamental security capabilities.

4. Assessment Lifecycle

The TPRM assessment follows a structured lifecycle to ensure consistent, repeatable evaluation of vendor security posture from initial onboarding through ongoing relationship management.

01 Vendor Onboarding
Initial vendor registration, tier classification based on data access and service criticality, NDA execution, and scoping of assessment requirements.

02 Initial Assessment
Distribution of appropriate questionnaire based on tier. Vendor completes self-assessment. Evidence collection and document review.

03 Risk Scoring
Assessor evaluates vendor responses, validates evidence, assigns maturity levels per control. Calculate domain and composite risk scores.

04 Risk Decision
Risk rating determination. Executive review for elevated/high risk vendors. Approval, conditional approval, or rejection decision.

05 Remediation
For conditionally approved vendors: document required improvements, define timelines, establish milestones. Vendor submits remediation plan.

06 Ongoing Monitoring
Continuous monitoring of vendor risk indicators. Periodic check-ins. Track remediation progress. Threat intelligence feeds for vendor ecosystem.

5. Vendor Inventory Requirements

Organizations shall maintain a comprehensive inventory of all third-party vendors. The following data elements must be tracked and updated for each vendor relationship:

Vendor Identification

- Legal entity name and DBA
- Primary and secondary contacts (name, title, email, phone)
- Physical address and jurisdiction
- DUNS number and SAM.gov UEI (if applicable)
- Contract number and effective dates

Risk Classification

- Assigned vendor tier (1, 2, or 3)
- Data types accessed (CUI, PII, financial, proprietary)
- System access level (admin, user, read-only, none)
- Criticality to operations (essential, important, standard)
- Regulatory applicability (DFARS, ITAR, HIPAA, etc.)

Assessment Status

- Last assessment date and result
- Current risk rating and composite score
- Open remediation items and due dates
- Next scheduled assessment date
- Assigned risk owner and assessor

Compliance & Certifications

- Current certifications (SOC 2, ISO 27001, FedRAMP, etc.)
- Certification expiration dates
- Sub-processor/fourth-party register
- Cyber insurance coverage and expiration
- SPRS score (if CMMC applicable)

PART 2

Vendor Security Assessment Questionnaire

Instructions for Vendors

Please complete all sections of this questionnaire applicable to the services you provide. For each question:

1. Select your Response: Yes (fully implemented), No (not implemented), Partial (partially implemented), or N/A (not applicable)
2. Assign a Maturity Level: L0 (Not Performed) through L4 (Continuously Optimized) — refer to Section 3 for definitions
3. Identify Evidence: List the documents, screenshots, or artifacts that support your response
4. Add Notes: Provide context, planned improvements, or explanations for Partial/No responses

All responses must be supported by verifiable evidence. Dominus Gray reserves the right to validate responses through follow-up interviews, document review, or on-site assessment.

6. Vendor Information

Company Legal Name:

DBA / Trade Name:

Primary Contact Name & Title:

Contact Email:

Contact Phone:

Company Address:

Services Provided to Organization:

Contract Number / Reference:

Data Types Accessed (CUI / PII / Financial / Proprietary / None):

System Access Level (Administrative / User / Read-Only / None):

Vendor Tier Classification (Tier 1 / Tier 2 / Tier 3):

Assessment Date:

Assessor Name:

7. Domain A: Governance & Risk Management

SCF Control Reference: TPM-03, TPM-04

A1. **Does the organization maintain a formally documented information security program with defined roles, responsibilities, and authority?**

SCF Ref: TPM-03.1

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *Security program charter, organizational chart, RACI matrix*

Notes:

A2. **Are comprehensive risk assessments conducted at least annually that identify threats to information assets and evaluate the likelihood and impact of identified risks?**

SCF Ref: TPM-03.2

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *Risk assessment report, risk register, methodology documentation*

Notes:

A3. **Does the organization hold current compliance certifications relevant to its services (e.g., SOC 2 Type II, ISO 27001, FedRAMP)?**

SCF Ref: TPM-04.1

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *Current certification letters, audit reports, bridge letters*

Notes:

A4. **Is there a dedicated information security function with qualified personnel (CISSP, CISM, or equivalent) responsible for security operations?**

SCF Ref: TPM-03.3

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *Org chart, personnel qualifications, job descriptions*

Notes:

A5. **Are security policies reviewed and updated at least annually, with formal approval by executive management?**

SCF Ref: TPM-03.4

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *Policy documents with revision history, approval records*

Notes:

A6. **Does the organization maintain a current inventory of all information assets, including data flows and system interconnections?**

SCF Ref: TPM-04.2

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *Asset inventory, data flow diagrams, network architecture*

Notes:

A7. **Is there a formal change management process that includes security impact analysis for all system and configuration changes?**

SCF Ref: TPM-04.3

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *Change management policy, CAB records, security review logs*

Notes:

A8. **Does the vendor provide a Software Bill of Materials (SBOM) for delivered software per Executive Order 14028?**

SCF Ref: TPM-04.4

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *SBOM documents (SPDX or CycloneDX format), software composition analysis reports*

Notes:

A9. **Does the vendor comply with NIST Secure Software Development Framework (SSDF) SP 800-218?**

SCF Ref: TPM-04.5

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *SSDF self-attestation, secure development lifecycle documentation, code review procedures*

Notes:

8. Domain B: Access Control

SCF Control Reference: TPM-05, IAC-01

B1. **Does the organization enforce role-based access control (RBAC) with documented access provisioning and de-provisioning procedures?**

SCF Ref: TPM-05.1

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *Access control policy, RBAC matrix, provisioning procedures*

Notes:

B2. **Is multi-factor authentication (MFA) required for all remote access, privileged accounts, and access to systems processing client data?**

SCF Ref: IAC-01.1

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *MFA configuration screenshots, authentication policy*

Notes:

B3. **Are privileged access accounts inventoried, monitored, and subject to enhanced controls including session recording and just-in-time access?**

SCF Ref: TPM-05.2

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *PAM solution documentation, privileged account inventory*

Notes:

B4. **Are user access reviews conducted at least quarterly for privileged accounts and semi-annually for standard accounts?**

SCF Ref: TPM-05.3

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *Access review reports, recertification records*

Notes:

B5. **Does the organization enforce password policies meeting NIST 800-63B requirements (minimum 12 characters, complexity, breach database checking)?**

SCF Ref: IAC-01.2

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *Password policy, technical configuration evidence*

Notes:

B6. **Are remote access connections secured via encrypted VPN or zero-trust network access (ZTNA) with endpoint compliance verification?**

SCF Ref: TPM-05.4

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *VPN/ZTNA configuration, endpoint compliance policy*

Notes:

9. Domain C: Data Protection

SCF Control Reference: TPM-06, DCH-01

C1. **Is all sensitive data encrypted at rest using AES-256 or equivalent FIPS 140-2 validated encryption across all storage systems?**

SCF Ref: TPM-06.1

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *Encryption configuration, key management procedures, FIPS certificates*

Notes:

C2. Is all data encrypted in transit using TLS 1.2 or higher for all internal and external communications?

SCF Ref: TPM-06.2

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *TLS configuration, certificate management procedures*

Notes:

C3. Does the organization maintain a formal data classification scheme that identifies CUI, PII, and other sensitive data categories?

SCF Ref: DCH-01.1

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *Data classification policy, labeling procedures, data inventory*

Notes:

C4. Are Data Loss Prevention (DLP) controls implemented to detect and prevent unauthorized exfiltration of sensitive data?

SCF Ref: TPM-06.3

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *DLP policy, tool configuration, incident reports*

Notes:

C5. Are data backups performed in accordance with defined RPO/RTO objectives, with backups encrypted and stored in a separate security domain?

SCF Ref: TPM-06.4

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *Backup policy, backup logs, restoration test results*

Notes:

C6. Does the organization have documented data retention and secure disposal procedures that comply with applicable regulatory requirements?

SCF Ref: DCH-01.2

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *Retention schedule, disposal procedures, certificates of destruction*

Notes:

C7. Are cryptographic key management procedures documented and implemented, including key rotation, escrow, and revocation processes?

SCF Ref: TPM-06.5

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *Key management policy, key rotation logs, HSM documentation*

Notes:

10. Domain D: Incident Response

SCF Control Reference: TPM-07, IRO-01

D1. **Does the organization maintain a formally documented Incident Response Plan (IRP) that is tested at least annually through tabletop or simulation exercises?**

SCF Ref: TPM-07.1

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *IRP document, exercise reports, after-action reviews*

Notes:

D2. **Are client notification procedures documented with defined timelines (e.g., 72-hour notification for data breaches affecting client data)?**

SCF Ref: TPM-07.2

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *Notification procedures, communication templates, escalation matrix*

Notes:

D3. **Does the organization maintain a security incident history log and can it disclose any breaches or security incidents from the past 36 months?**

SCF Ref: IRO-01.1

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *Incident log, breach disclosure reports, remediation evidence*

Notes:

D4. **Does the organization carry cyber liability insurance with coverage adequate for the scope of services and data processed?**

SCF Ref: TPM-07.3

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *Insurance certificate, coverage summary, policy declarations*

Notes:

D5. **Is there a designated incident response team with defined roles, 24/7 contact procedures, and established relationships with law enforcement?**

SCF Ref: IRO-01.2

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *IRT roster, contact procedures, escalation protocols*

Notes:

D6. **Are forensic investigation capabilities available (internal or contracted) to support evidence preservation and root cause analysis?**

SCF Ref: TPM-07.4

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *Forensics retainer agreement, evidence handling procedures*

Notes:

11. Domain E: Business Continuity

SCF Control Reference: TPM-08, BCD-01

E1. **Does the organization maintain a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) that are tested at least annually?**

SCF Ref: TPM-08.1

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *BCP/DRP documents, test reports, after-action improvements*

Notes:

E2. **Are Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) defined, documented, and validated through testing for all critical services?**

SCF Ref: BCD-01.1

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *RPO/RTO documentation, test results, SLA alignment*

Notes:

E3. **Does the organization have geographically separated redundant infrastructure to support continuity of operations during regional events?**

SCF Ref: TPM-08.2

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *Infrastructure architecture, site diversity documentation*

Notes:

E4. **Are BCP/DR tests conducted at least annually, including failover exercises that validate recovery within documented RTO targets?**

SCF Ref: BCD-01.2

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *Test schedules, exercise reports, recovery time measurements*

Notes:

E5. **Does the organization maintain documented procedures for communicating service disruptions to clients, including escalation timelines?**

SCF Ref: TPM-08.3

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *Communication procedures, notification templates, contact lists*

Notes:

E6. **Are critical dependencies (sub-processors, infrastructure providers, key personnel) identified and factored into continuity planning?**

SCF Ref: TPM-08.4

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *Dependency analysis, sub-processor register, succession plans*

Notes:

12. Domain F: Human Resources Security

SCF Control Reference: TPM-09, HRS-01

F1. **Are background checks (criminal, employment verification, education) conducted for all personnel with access to client data or systems prior to employment?**

SCF Ref: TPM-09.1

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *Background check policy, screening provider contract, sample records*

Notes:

F2. **Is security awareness training conducted for all employees upon hire and at least annually thereafter, with completion tracking and testing?**

SCF Ref: HRS-01.1

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *Training curriculum, completion records, test results*

Notes:

F3. **Are role-specific security training programs provided for personnel in specialized roles (developers, administrators, incident responders)?**

SCF Ref: TPM-09.2

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *Role-based training matrix, training materials, completion records*

Notes:

F4. **Does the organization have documented termination and transfer procedures that include immediate revocation of access upon separation?**

SCF Ref: HRS-01.2

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *Termination checklist, access revocation procedures, audit logs*

Notes:

F5. **Are confidentiality and non-disclosure agreements required for all employees and contractors prior to accessing sensitive information?**

SCF Ref: TPM-09.3

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *NDA template, signed agreements, contractor acknowledgments*

Notes:

F6. **Does the organization conduct periodic (at least quarterly) phishing simulation exercises with documented results and remedial training?**

SCF Ref: TPM-09.4

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *Phishing simulation reports, click rates, remediation tracking*

Notes:

13. Domain G: Physical & Environmental Security

SCF Control Reference: TPM-10, PES-01

G1. **Are facilities housing systems that process client data secured with multi-layered physical access controls (badge, biometric, mantrap)?**

SCF Ref: TPM-10.1

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *Physical security assessment, access control system documentation*

Notes:

G2. **Are environmental controls (fire suppression, HVAC, water detection, UPS/generator) implemented and monitored for data center and server room areas?**

SCF Ref: PES-01.1

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *Environmental monitoring reports, maintenance records, test logs*

Notes:

G3. **Is visitor access to sensitive areas controlled through sign-in procedures, escort requirements, and badge differentiation?**

SCF Ref: TPM-10.2

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *Visitor management policy, sign-in logs, escort procedures*

Notes:

G4. **Are security cameras and monitoring systems deployed at facility entry points, server rooms, and sensitive processing areas with adequate retention?**

SCF Ref: PES-01.2

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *CCTV coverage map, retention policy, monitoring procedures*

Notes:

G5. **Are physical access logs reviewed regularly and retained for a minimum of 90 days?**

SCF Ref: TPM-10.3

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *Access log review reports, retention configuration, review schedule*

Notes:

14. Domain H: Compliance & Audit

SCF Control Reference: TPM-11, CPL-01

H1. **Does the organization hold current SOC 2 Type II certification, and is the report available for client review under NDA?**

SCF Ref: TPM-11.1

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *SOC 2 Type II report, bridge letter, management assertion*

Notes:

H2. **Does the organization hold ISO 27001 certification for the scope of services provided, and is the certificate current?**

SCF Ref: TPM-11.2

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *ISO 27001 certificate, Statement of Applicability, surveillance audit reports*

Notes:

H3. **If providing cloud services to federal agencies, does the organization hold FedRAMP authorization or equivalent (StateRAMP, TX-RAMP)?**

SCF Ref: CPL-01.1

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *FedRAMP authorization letter, package, continuous monitoring reports*

Notes:

H4. **Are independent security audits or penetration tests conducted at least annually by qualified third-party assessors?**

SCF Ref: TPM-11.3

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *Penetration test report, remediation evidence, assessor qualifications*

Notes:

H5. **Does the organization have a documented regulatory compliance program that tracks applicable requirements (DFARS, ITAR, HIPAA, GDPR, CCPA)?**

SCF Ref: CPL-01.2

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *Compliance matrix, regulatory tracking, gap remediation plans*

Notes:

H6. **Are audit findings tracked to remediation with defined timelines and executive accountability?**

SCF Ref: TPM-11.4

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *Finding tracker, remediation evidence, management reports*

Notes:

H7. **Does the organization support client audit rights, including on-site assessments with reasonable notice?**

SCF Ref: CPL-01.3

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *Contract audit clause, prior client audit reports*

Notes:

H8. **If providing cloud services for CUI, does the vendor hold FedRAMP Moderate authorization or demonstrate documented equivalency? Verify at marketplace.fedramp.gov.**

SCF Ref: CPL-01.4

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *FedRAMP authorization letter, FedRAMP Marketplace listing, equivalency documentation*

Notes:

H9. Does the vendor handle ITAR or EAR controlled data? If yes, document export control compliance measures.

SCF Ref: CPL-01.5

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *Export control compliance program, ITAR/EAR registration, technology control plan*

Notes: _____

H10. Has the vendor adopted or planned adoption of Zero Trust Architecture principles per NIST SP 800-207?

SCF Ref: CPL-01.6

Response: ☐ Yes ☐ No ☐ Partial ☐ N/A **Maturity Level:** ☐ L0 ☐ L1 ☐ L2 ☐ L3 ☐ L4

Evidence Required: *Zero Trust architecture roadmap, ZTA implementation plan, NIST SP 800-207 alignment assessment*

Notes: _____

15. Risk Summary Scorecard

Complete this section after scoring all assessment domains. Calculate domain averages and the composite vendor risk score to determine the overall risk rating.

ASSESSMENT DOMAIN	QUESTI	AVG	WEIGH	WEIGHTED	RATING
B. Access Control	6	__ / 4.0	1.0	_____	
C. Data Protection	7	__ / 4.0	1.0	_____	
D. Incident Response	6	__ / 4.0	1.0	_____	
E. Business Continuity	6	__ / 4.0	1.0	_____	
F. Human Resources Security	6	__ / 4.0	1.0	_____	
G. Physical & Environmental	5	__ / 4.0	1.0	_____	
H. Compliance & Audit	10	__ / 4.0	1.0	_____	
COMPOSITE VENDOR RISK SCORE				**_____ / 4.0**	

Overall Risk Rating (circle one)

- LOW RISK (3.5–4.0)
- MODERATE RISK (2.5–3.4)
- ELEVATED RISK (1.5–2.4)
- HIGH RISK (0.5–1.4)
- CRITICAL RISK (0.0–0.4)

Assessment Decision

- APPROVED — Vendor meets minimum security requirements for assigned tier.
- CONDITIONALLY APPROVED — Vendor approved subject to remediation of identified deficiencies.

☐ NOT APPROVED — Vendor does not meet minimum security requirements. Remediation required before re-assessment.

☐ DEFERRED — Additional information or assessment required before a decision can be made.

Assessor Name & Signature: _____

Assessment Date: _____

Risk Owner Name & Signature: _____

Approval Date: _____

16. Remediation Requirements

Document all required vendor improvements identified during the assessment. Each remediation item should include a clear description, priority, responsible party, and target completion date.

#	DOMAIN	FINDING / GAP	PRIORI	OWNER	DUE	STATUS
2						
3						
4						
5						
6						
7						
8						
9						
10						

Remediation Priority Definitions

CRITICAL — Must be resolved within 30 days. Risk is unacceptable and may require immediate disengagement if not addressed.
HIGH — Must be resolved within 60 days. Significant risk requiring management attention and dedicated resources.
MEDIUM — Must be resolved within 90 days. Moderate risk that should be addressed in the normal course of business.
LOW — Must be resolved within 180 days. Minor risk or improvement opportunity.

- **Remediation Tracking**

The vendor shall provide written remediation plans within 14 business days of receiving assessment results. Remediation plans must include specific actions, responsible parties, milestones, and target completion dates. Progress updates are required at intervals determined by the assigned priority level.

Appendix A: Evidence Request List

The following documents and artifacts should be requested from vendors as part of the assessment process. Not all items are required for every vendor — tailor the request based on vendor tier and applicable domains.

#	DOCUMENT / ARTIFACT	RECEI	TI
1	Information Security Policy (current version)		1,
2	Risk Assessment Report (most recent)		1,
3	SOC 2 Type II Report or Bridge Letter		1,
4	ISO 27001 Certificate and Statement of Applicability		1,
5	Penetration Test Report (most recent, executive summary acceptable)		1,
6	Business Continuity Plan and DR Plan (table of contents + key sections)		1,
7	Incident Response Plan (table of contents + notification procedures)		1,
8	Data Flow Diagram for client data		1,
9	Network Architecture Diagram (sanitized)		1,
10	Encryption Standards Documentation		1,
11	Access Control Policy and RBAC Matrix		1,
12	Background Check Policy		1,
13	Security Awareness Training Program Documentation		1,
14	Vulnerability Management Program Documentation		1,
15	Patch Management Policy and Compliance Reports		1,
16	Cyber Liability Insurance Certificate of Coverage		1,
17	Sub-processor / Fourth-Party List		1,
18	Data Processing Agreement (DPA) Template		1
19	Data Retention and Disposal Policy		1
20	Change Management Policy		1
21	Physical Security Assessment or Certification		1
22	Regulatory Compliance Matrix		1

Evidence Handling

All vendor evidence shall be classified as CONFIDENTIAL and stored in the organization's secure document repository. Evidence shall be retained for the duration of the vendor relationship plus three (3) years. Access to vendor assessment files shall be limited to authorized TPRM personnel.

Appendix B: Contract Security Requirements

The following security clauses should be incorporated into vendor agreements and contracts. Clauses may be adapted based on vendor tier, services provided, and applicable regulatory requirements.

1. Data Protection & Handling

Vendor shall implement and maintain administrative, technical, and physical safeguards to protect Client data in accordance with NIST SP 800-171 and applicable regulations. Vendor shall not process, store, or transmit Client data outside the continental United States without prior written consent.

2. Incident Notification

Vendor shall notify Client within seventy-two (72) hours of discovering any Security Incident affecting Client data. Notification shall include: nature of the incident, data affected, containment actions taken, and designated point of contact for ongoing communications.

3. Audit & Assessment Rights

Client reserves the right to conduct security assessments of Vendor operations upon thirty (30) days written notice, not to exceed once annually under normal circumstances. Vendor shall cooperate fully and provide access to relevant personnel, systems, and documentation.

4. Sub-processor Management

Vendor shall not engage sub-processors that access Client data without prior written approval. Vendor shall maintain a current register of approved sub-processors and ensure equivalent security obligations through written agreements.

5. Data Return & Destruction

Upon contract termination, Vendor shall return all Client data within thirty (30) days and provide a certified certificate of destruction for all copies within sixty (60) days. Destruction shall meet NIST SP 800-88 standards.

6. Compliance Certification

Vendor shall maintain compliance with all applicable regulatory requirements throughout the contract term and provide evidence of current certifications upon request. Any lapse in certification shall be reported within five (5) business days.

7. Insurance Requirements

Vendor shall maintain cyber liability insurance with minimum coverage of $5,000,000 per occurrence and $10,000,000 aggregate. Vendor shall provide a certificate of insurance upon request and notify Client of any material changes to coverage.

8. Security SLAs

Vendor shall remediate Critical vulnerabilities within 48 hours, High within 7 days, Medium within 30 days, and Low within 90 days of identification. Vendor shall provide monthly vulnerability management reports.

9. Flow-Down Requirements

In the event Vendor processes Controlled Unclassified Information (CUI), Vendor shall comply with DFARS 252.204-7012, NIST SP 800-171, and applicable CMMC requirements. All flow-down requirements shall apply to sub-processors.

10. Right to Terminate

Client may terminate the agreement with thirty (30) days notice if Vendor fails to remediate identified security deficiencies within agreed timelines, experiences a material data breach, or fails to maintain required certifications.

11. CMMC Certification Requirement

Vendor must maintain CMMC certification at the level required for the data they will access. For CUI: CMMC Level 2 minimum. Verification via SPRS required prior to contract award and annually thereafter.

Legal Review Required

These contract security clauses are provided as templates and must be reviewed by qualified legal counsel before inclusion in vendor agreements. Requirements may need to be tailored based on specific regulatory obligations, industry standards, and the nature of the vendor relationship.