

INFORMATION TECHNOLOGY CHECKLIST (ITC)

Third-Party Risk Management | Vendor Intake Assessment Tool

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

The Information Technology Checklist (ITC) is the initial step in the vendor intake process. It must be completed by the requesting business unit, in collaboration with TPRM, information technology, and legal teams, before any risk tier is assigned, any questionnaire is chosen, or any due diligence activity starts.

Any "Yes" answer in Section 3 (Information Scope Assessment) requires the mandatory completion of an IT Data Security Addendum before the vendor relationship can proceed.

SECTION 1: REQUESTOR INFORMATION

Date of Request	
Requestor Name	
Business Unit / Department	
Project / Initiative Name	
Requestor Email	
Supervisor / Approver	

SECTION 2: VENDOR AND ENGAGEMENT INFORMATION

Vendor / Supplier Name	
Vendor Website	
Primary Vendor Contact	
Vendor Contact Email	
Description of Services	

2A. Agreement Type (select one)

☐	Master Service Agreement (MSA)
☐	One-Time / Single Engagement Contract
☐	Statement of Work (SOW) under existing MSA
☐	Other (describe): _____

2B. Service Category (select all that apply)

☐	Infrastructure as a Service (IaaS)	☐	Software as a Service (SaaS)
☐	Platform as a Service (PaaS)	☐	Business Process as a Service (BPaaS)
☐	Unified Communications as a Service (UCaaS)	☐	Desktop as a Service (DaaS)
☐	Consulting / Professional Services	☐	Information Provisioning
☐	AI-Enabled Processing / Analytics	☐	Other: _____

SECTION 3: INFORMATION SCOPE ASSESSMENT

Complete this section carefully. Any "Yes" answer triggers the IT Data Security Addendum requirement.

3A. Will the vendor access, process, store, or transmit organizational information that is non-public or regulated?

☐ Yes	TRIGGERS IT Data Security Addendum. Complete Section 3B and proceed to full due diligence.
☐ No	Proceed to Section 4. Reduced due diligence path may apply.

3B. Data Types Involved (select all that apply)

	Data Type		Data Type
☐	Consumer Data	☐	Credit Card Data (PCI DSS)
☐	Employee Data	☐	EU Personal Data (GDPR)
☐	Financial Data	☐	HIPAA-Protected Health Information (PHI)
☐	Intellectual Property	☐	Personally Identifiable Information (PII)
☐	Trade Secrets / Proprietary Information	☐	Design / Manufacturing Data
☐	Marketing Materials / Customer Lists	☐	Other: _____

3C. Data Handling (select all that apply)

☐	Process organizational data	☐	Store or host organizational data
☐	Transmit organizational data	☐	Access organizational systems or networks

3D. Data Classification

Based on the data types identified above, classify the highest sensitivity level of information involved:

	Classification	Description
☐	RESTRICTED	Highest protection required. Exposure risk includes identity theft, regulatory penalties, and significant reputational damage. Includes PHI, PII, financial account data, trade secrets.
☐	CONFIDENTIAL	Non-public business information. Includes customer data, financial

	Classification	Description
		records, strategies, and proprietary processes not rising to Restricted level.
[]	PROPRIETARY	Business information not publicly available but carrying commercial or competitive value. Lower exposure risk than Confidential.

SECTION 4: AI AND EMERGING TECHNOLOGY FLAGS

Complete this section if the vendor provides AI-enabled services. "Yes" answers trigger AI-specific assessment track.

Question	Answer	Notes / Details
Does the vendor use artificial intelligence or machine learning in service delivery?	[] Yes [] No	
Will organizational data be used to train or fine-tune AI models?	[] Yes [] No	
Does the vendor use AI for profiling, scoring, or automated decision-making?	[] Yes [] No	
Is the vendor subject to the EU AI Act or similar AI regulation?	[] Yes [] No	
Has the vendor provided documentation of AI governance practices?	[] Yes [] No	

SECTION 5: OUTCOME AND ROUTING

	Outcome	Action Required
[]	Full Due Diligence	Section 3 = Yes AND data classification = Restricted or Confidential. Full questionnaire, evidence review, IT Data Security Addendum, and DPA required.
[]	Reduced Due Diligence	Section 3 = Yes AND data classification = Proprietary. Short-form questionnaire, standard contract provisions.
[]	Expedited / Low Risk	Section 3 = No. Lightweight review, standard commercial terms. Document rationale.

TPRM Reviewer Sign-Off

Reviewed By	
Date of Review	
Assigned Risk Tier	
IT Data Security Addendum Required?	

Additional Notes	
-------------------------	--

ITC SUPPLEMENTAL MODULE: HEALTHCARE / HIPAA

This module is triggered when: (1) the vendor is a healthcare organization, business associate, or subcontractor; or (2) the Information Scope Assessment identifies HIPAA-protected health information (PHI).

HC-1: HIPAA Business Associate Status

Question	Answer	Notes
Is a HIPAA Business Associate Agreement (BAA) required?	☐ Yes ☐ No	
Has the vendor signed a BAA with other covered entities?	☐ Yes ☐ No	
Will the vendor create, receive, maintain, or transmit PHI on behalf of the organization?	☐ Yes ☐ No	
Does the vendor use subcontractors who may access PHI?	☐ Yes ☐ No	If Yes, BAA flow-down required

HC-2: PHI Safeguards

Question	Answer	Notes
Does vendor encrypt PHI at rest and in transit?	☐ Yes ☐ No	AES-256 or equivalent
Does the vendor maintain a HIPAA breach notification procedure?	☐ Yes ☐ No	60-day notification requirement
Does vendor conduct HIPAA Security Rule risk analysis?	☐ Yes ☐ No	
Are minimum necessary access controls implemented?	☐ Yes ☐ No	
Does vendor have documented workforce HIPAA training?	☐ Yes ☐ No	

ITC SUPPLEMENTAL MODULE: FINANCIAL SERVICES / PCI DSS + DORA

This module is triggered when: (1) the vendor is a financial services entity or payment processor; or (2) the Information Scope Assessment identifies credit card data, financial account data, or EU financial services context.

FS-1: PCI DSS Scope

Question	Answer	Notes
Will the vendor store, process, or transmit cardholder data?	☐ Yes ☐ No	Triggers PCI DSS scope
Is the vendor PCI DSS compliant? What level?	☐ Yes ☐ No	
Does vendor hold a current Attestation of Compliance (AoC)?	☐ Yes ☐ No	Request copy
Does the vendor use tokenization or point-to-point encryption (P2PE)?	☐ Yes ☐ No	

FS-2: DORA (EU Digital Operational Resilience Act)

Applicable when the organization or vendor is subject to DORA (EU financial entities from January 17, 2025).

Question	Answer	Notes
Is this vendor an ICT third-party service provider under DORA?	☐ Yes ☐ No	
Does the vendor qualify as Critical ICT Third-Party Provider?	☐ Yes ☐ No	ESMA/EBA/EIOPA designation
Is a DORA-compliant contractual arrangement in place or planned?	☐ Yes ☐ No	
Has the vendor provided a register of ICT subcontractors?	☐ Yes ☐ No	
Does vendor support digital operational resilience testing?	☐ Yes ☐ No	TLPT requirements

ITC SUPPLEMENTAL MODULE: GOVERNMENT / CMMC + CUI

This module is triggered when: (1) the vendor supports a federal government contract or subcontract; or (2) the Information Scope Assessment identifies Controlled Unclassified Information (CUI), Federal Contract Information (FCI), or defense-related data.

GOV-1: CUI and FCI Handling

Question	Answer	Notes
Will the vendor handle Controlled Unclassified Information (CUI)?	☐ Yes ☐ No	Triggers NIST 800-171
Will the vendor handle Federal Contract Information (FCI)?	☐ Yes ☐ No	Triggers FAR 52.204-21
Does the vendor hold a current CMMC certification?	☐ Yes ☐ No	Specify level: 1 / 2 / 3
Has vendor completed a System Security Plan (SSP) per NIST 800-171?	☐ Yes ☐ No	

GOV-2: CMMC Requirements

Question	Answer	Notes
CMMC Level required per contract: __ 1 __ 2 __ 3	☐ Yes ☐ No	
Has vendor been assessed by a C3PAO (Certified Third-Party Assessor Organization)?	☐ Yes ☐ No	Level 2 / 3
Does vendor have a Plan of Action & Milestones (POA&M) for any open findings?	☐ Yes ☐ No	
Does vendor restrict CUI to U.S.-person access where required?	☐ Yes ☐ No	ITAR / EAR applicability
Does vendor flow CMMC requirements down to its subcontractors?	☐ Yes ☐ No	