



Vendor Intake Form – SCOPE

Overview

The **Vendor Intake Form** is the foundational gateway in SCOPE's cybersecurity risk evaluation workflow. It collects all essential inputs required to construct a dynamic, OSINT-augmented vendor profile, which is then continuously assessed and scored by the risk engine.

This whitepaper outlines every section of the form, what each field contributes to scoring or analysis, and which fields are required vs optional.



Form Sections & Fields




1. Basic Vendor Identification

Field	Type	Required	Notes
Vendor Name	Text	✓ Yes	Display name for dashboards
Country of Operation	Dropdown	✓ Yes	Tied to geopolitical risk
Industry / Sector	Dropdown	✓ Yes	Impacts sector risk scoring
Website / Domain	Text (URL)	✓ Yes	Used for OSINT scanning






2. Business & Operational Context

Field	Type	Required	Notes
Employee Count	Dropdown	✓ Yes	Proxy for vendor scale
Annual Revenue	Numeric	✗ Optional	Enriches financial risk view
Global Footprint	Text	✗ Optional	Used for geopolitical scoring
Data Center / Cloud Region	Multi-select	✗ Optional	Risk by infra locality




3. Asset Dependency & Criticality

Field	Type	Required	Notes
Asset Importance	Dropdown	 Yes	Drives priority multiplier
Function of Vendor	Multi-select	 Yes	E.g., Data Processor, Cloud Provider
# of Internal Dependencies	Numeric	 Optional	Used in concentration risk scoring



4. Security Posture (Self-attested)

Field	Type	Required	Notes
Certifications (ISO, SOC2, etc.)	Multi-select	 Optional	Boosts compliance score
Frameworks Followed (NIST, etc.)	Multi-select	 Optional	Self-declared controls framework
Use of EDR/AV	Checkbox	 Optional	Maps to endpoint hygiene
MDM / BYOD Management Present?	Checkbox	 Optional	Maps to device control score
Incident Response Plan Exists?	Checkbox	 Optional	Used in IR readiness subscore

5. Exposed Infrastructure Details

Field	Type	Required	Notes
Public IP / CIDR (if known)	Text	 Optional	Used for IP-level scan enrichment
Known Subdomains (if available)	Text	 Optional	Supplements subdomain discovery
GitHub Org / Repo (if available)	Text	 Optional	Used for public repo secret detection

6. Compliance Questionnaire Upload (Optional)

Field	Type	Required	Notes
Upload SIG/NIST/OpenFAIR	File Upload	 Optional	Deep compliance analysis
Date of Last Completed Audit	Date Picker	 Optional	Assists in evaluating audit recency

Use of Collected Data

Each field contributes to:

- **Risk Scoring Inputs:** Mapped directly into the scoring engine (see attached scoring whitepaper)
 - **OSINT Automation:** Domains, subdomains, CIDRs used for active/passive recon
 - **Contextual Analysis:** Sector/country impact, asset exposure matrix
 - **Prioritization:** Criticality ranking and alerting logic
-

Summary of Required vs Optional Fields

Section	Required Fields
Basic Info	All
Business Context	Employee Count
Asset Dependency	Asset Importance, Function
Security Posture	None (all optional, boosts score if present)
Infrastructure	None (used for OSINT enrichment)
Compliance Uploads	None



Example Workflow

1. Security or Procurement fills out vendor form
 2. System ingests submitted + inferred OSINT
 3. Risk scoring model is triggered
 4. Score, badge, and alerts populate in dashboard
 5. Risk is recalculated every 3 hours automatically
-



Future Enhancements

- Pre-fill data via domain lookup and AI enrichment
 - Vendor self-assessment portal with guided attestation
 - Real-time field validation based on OSINT signals
 - Integration with GRC or procurement tools (SAP, Coupa)
-



Supporting Documents

- SCOPE Risk Scoring Whitepaper
 - SCOPE Platform Project Whitepaper
-