SCOPE Risk Scoring

Executive Summary

SCOPE (Supply Chain OSINT & Prediction Engine) is a cybersecurity-centric Third Party Risk Management (TPRM) platform designed to evaluate and monitor the cyber posture of vendors. The core of SCOPE is its **multi-dimensional scoring framework**, tailored to reflect real-world risks across cybersecurity hygiene, compliance, geopolitical exposure, and breach reputation. This whitepaper outlines the complete structure, logic, scoring methods, and use cases behind SCOPE's risk evaluation model.

🌐 Risk Level Mapping

All risk scores are expressed on a 0–100 scale and assigned one of four risk levels:

Score	Level	Color
85–100	Low	🟢 Green
70–84	Medium	🟡 Yellow
50–69	High	🟠 Orange
0–49	Critical	🔴 Red

Every subcategory is independently scored and mapped to a risk level. Final risk score is computed as a weighted average across four primary risk domains.

🔒 Cybersecurity Posture (40%)

This category assesses a vendor's exposed digital footprint, technical controls, and readiness to detect/respond to threats.

Subcategory	Weight	Description
Vulnerability Management	5%	Open CVEs, patch cycles, outdated software

Attack Surface (ASM)	5%	Open ports, misconfigured services, exposed assets
Web/Application Security	5%	TLS version, CMS exposure, authentication endpoints
Cloud & Infrastructure Security	5%	S3 buckets, API security, cloud config hygiene
Email Security	5%	SPF, DKIM, DMARC presence
Code Repository Exposure	5%	Hardcoded secrets, public GitHub leaks
Endpoint/Device Hygiene	5%	Use of MDM, AV, device control
IOC & Infra Threat Signals	3%	Blacklisted IPs, C2 infrastructure, threat feed matches
Detection & Response Maturity	2%	SOC readiness, IR plans, logging coverage

---

📜 Compliance & Legal Risk (20%)

This category measures adherence to cyber regulations and frameworks, and the vendor's historical legal security posture.

Subcategory	Weight	Description
Certifications & Standards	6%	ISO 27001, SOC2, NIST CSF, PCI DSS, etc.
Questionnaire Quality	5%	Depth and honesty in SIG/OpenFAIR/NIST documents
Regulatory Violations	5%	Sanctions, fines, or penalties from data protection bodies
Privacy Compliance	2%	GDPR, HIPAA, CCPA alignment
Contractual Security Clauses	2%	Encryption, MFA, audit rights in contracts

---

🌍 Geopolitical & Sector Risk (20%)

Evaluates risk factors based on the vendor's operational region, industry, and infrastructure locality.

Subcategory	Weight	Description
Country Risk	6%	Political instability, sanctions, cyber laws, OFAC lists
Sector Risk Profile	4%	Industry classification (e.g., Finance = High risk)
Company Size & Reach	3%	Global footprint, employee size, asset sprawl
Infrastructure Jurisdiction	3%	Location of hosted systems and legal exposure
Concentration / Monopoly Risk	2%	Critical vendor used across multiple internal systems
Environmental Exposure	2%	Natural disaster risk at HQ or primary DC

📣 Reputation & Exposure History (20%)

Examines breach records, brand risk, and external signals of past compromise.

Subcategory	Weight	Description
Data Breach History	6%	Known breaches, data loss events
Credential / Data Leaks	5%	Leaked email/password, exposed keys
Brand Spoofing & Phishing Kits	3%	Typosquatting, cloned sites, social spoofing
Dark Web & Pastebin Presence	3%	Mentions in threat actor channels, paste dumps
Social/Public Sentiment	3%	Media coverage, defacements, hacktivist attention

---

🔗 Asset Criticality Modifier

Vendors are prioritized based on the declared importance of the services they provide:

Level	Modifier
Critical	1.25x

High	1.10x
Medium	1.00x
Low	0.85x

Applied multiplicatively to the final weighted risk score.

📊 Final Scoring Formula

```
final_score = (
  cyber_score * 0.40 +
  compliance_score * 0.20 +
  geopolitical_score * 0.20 +
  reputation_score * 0.20
) * criticality_modifier
```

Each subcategory is scored 0–100 based on collected data, normalized, and rolled up.

💼 Example: Vendor XYZ

Category	Score	Level
Cybersecurity	66	High
Compliance	82	Medium
Geopolitical	91	Low
Reputation	47	Critical
Final Score	65.9	High

XYZ is marked high-risk due to reputation issues, despite good geopolitical posture.

🤔 Interpretation for Stakeholders

This scoring model allows organizations to:

- Prioritize vendor reviews
- Justify procurement risk decisions
- Show audit-grade documentation of vendor posture
- Monitor risk over time (via score deltas)

The model runs automatically every 3 hours and updates the UI with risk levels, colored badges, and alerts.