The Product (Simple View)

We're building a **Vendor Risk Assessment & Compliance Management Platform**.

Companies use it **before onboarding any external vendor / third-party service** to evaluate:

- Is this vendor safe?
- Will they leak data?
- Will they break compliance laws?
- Will business stop if they fail?

So instead of trusting vendors blindly, the organization fills a structured assessment → system calculates risk → decision: onboard or reject.

What Problem It Soles

Whenever a company integrates something like:

- payment gateway
- cloud hosting
- telemedicine platform
- analytics tool
- outsourcing agency

They are literally giving access to their data, systems, or customers.

One wrong vendor =
data breach + legal fine + reputation damage + operational shutdown.

Right now this process is manual (emails, excel, meetings).
Our product **automates that entire due-diligence workflow**.

How The Product Works (Workflow)

1. User fills a step-by-step intake form
2. Platform analyzes risk factors
3. System calculates risk score
4. Vendor gets classified into tier
5. Decision + compliance actions generated

The form captures things like:

- type of vendor
- data accessed
- system access
- cross-border transfer
- regulations involved
- business impact

All of that feeds the risk engine.

(That structured form is the TRACS Risk Intake Form)

RIF Form & Scoring

What Makes It Smart (Core Logic)

We are not just storing data — we are **doing automated governance**.

The system calculates:

1) Inherent Risk

How dangerous the vendor is by nature

- sensitive data
- high volume
- network access
- geography

2) Control Strength

How safe they claim to be

- ISO certification
- contracts
- security policies

3) Residual Risk

Final risk after controls

Then → assigns a **vendor tier (critical → low)** and tells the company what to do next.

In One Line

A platform that helps organizations **safely trust external partners** using automated risk scoring and compliance validation.

Functional requirement: Entity-Based Multi-Dashboard Architecture with RBAC

1. Objective

Enable clients with multiple entities (e.g., subsidiaries, group companies, or branches across different geographies) to manage compliance and cybersecurity operations through a centralized platform with **segregated entity-level dashboards**, while ensuring **role-based access control (RBAC)** to maintain data confidentiality and operational independence.

2. Key Features

2.1 Entity Management

- Ability to **create, view, edit, and delete entities** within the client's umbrella account.
- Each entity represents a legal or operational unit (e.g., based on geography, function, or division).
- Entity-specific data boundaries to reflect geographic regulations, frameworks (e.g., GDPR, ISO 27001, NIST, DIFC DPL), and assessments.

2.2 Entity-Level Dashboards

- Dedicated dashboard for each entity showing:
    - Compliance status
    - Risk posture
    - Audit logs
    - Notifications and reminders
- Dashboards to support custom widgets based on entity's regulatory needs.

2.3 Global View (Super Admin Access)

- A **Global Compliance Officer / CISO role** can access all entity dashboards.
- Ability to perform cross-entity comparisons, consolidated risk reporting, and generate compliance heatmaps.
- Audit trail and activity log across entities for oversight.

3. Role-Based Access Control (RBAC)

3.1 User Roles (Customizable)

Role	Access Level	Entity Visibility
Global Admin / CISO	Full platform access across all entities	All Entities
Entity Compliance Lead	Full access to own entity	Single Assigned Entity Only
Entity Risk Analyst	Limited access to assessments and risk items	Single Assigned Entity Only
Auditor / Consultant	Read-only access to assigned modules	Per Role & Access Setup
IT / Security Operator	Access to security-specific modules	Entity-specific

3.2 Permissions Granularity

- Visibility into sensitive data (e.g., DSRs, DPIAs) controlled via permission tags.
- Ability to assign entity managers and module leads.

3.3 Custom Role Builder

- Admins can define custom roles and permission sets per entity.
- Enables fine-tuned delegation of compliance responsibilities.

4. Platform Architecture Overview

4.1 Multi-Tenant Architecture with Logical Isolation

- Each client account acts as a *tenant*.
- Entities under a tenant are logically isolated but connected through the parent account.
- Data separation implemented through database-level segmentation (e.g., entity_id scoped queries).

4.2 Hierarchical Access Model

├── Entity A (India - GDPR)

│ ├── Users

│ └── Compliance Frameworks, Risks, Logs

│

├── Entity B (UAE - DIFC)

│ ├── Users

│ └── Assessments, Reports, Alerts

│

└── Global Admin (access to all)

4.3 User Management Layer

- Centralized user directory per client.
- Supports SSO, MFA, and invite-based onboarding.
- User-Entity associations stored in a role-assignment matrix.

5. Data Security and Access Control Logic

- Access enforced through backend middleware that evaluates:
    - User Role
    - Entity Context
    - Resource Permissions
- Audit logs captured for every access/modification, tagged by user, role, and entity.

6. Compliance Mapping and Localization

- Frameworks and templates auto-configured based on entity's region.
- Localization support for regulations (e.g., ISO 27701 for UAE, GDPR for EU entities).
- Crosswalk tools to map and reuse controls across entities.

7. UX & Navigation

- Entity Selector in the top navigation bar for quick switching.
- Landing page for Global Admin to show an overview of all entity statuses.
- Alerts and tasks filtered by entity context.

8. Future Enhancements (Backlog)

- **Cross-entity workflow automation** (e.g., assign a single control across all).
- **AI-powered compliance gap identification per entity**.
- **Entity comparison benchmarking dashboard**.
- **Customizable notification routing based on entity risk levels**.

TRACS Risk Intake Form (RIF)

Section 1: Third Party Information

Field Label	Field Type	Mandatory	Notes/Options
Third Party Legal Name	Text	Yes	—
Country of Operations	Dropdown	Yes	Predefined country list
Website URL	URL	No	Optional for verification
SPOC Contact Name	Text	Yes	Single Point of Contact
SPOC Email	Email	Yes	—
SPOC Phone Number	Phone	Yes	International format recommended
Type of Third Party	Multi-select Dropdown	Yes	Industry-specific list (see categories below)
Nature of the Third Party	Radio Buttons	Yes	- Established / Reputed- New / Niche- Other (text input)
Data Hosting Arrangement	Multi-select	Yes	- On-Prem- Cloud - IaaS- Cloud - PaaS- Cloud - SaaS

Dropdown Options for "Type of Third Party": (Categorized, collapsible UI)

- Cybersecurity / IT Services
- Banking / Fintech
- Healthcare / Healthtech
- Retail / E-commerce

- Manufacturing / IoT / Industrial
- Telecom / Cloud / SaaS
- Professional Services / BPO
- Government / Regulated Sector
- General Services
- Other (text input)

Enable the respective heading sub-options upon the respective selection

Cybersecurity / IT Services

- Managed Security Service Provider (MSSP)
- IT Services / ITES
- Penetration Testing / VAPT Firm
- Security Product Vendor (SIEM, DLP, etc.)
- Threat Intelligence Provider
- SOC-as-a-Service Vendor
- Cloud Security Service Provider

Banking / Fintech

- Core Banking Software Vendor
- Digital Lending Platform
- KYC/AML Solution Provider
- Payment Gateway / Processor
- Credit Scoring / Risk Rating Agency
- Regulatory Reporting Vendor
- Financial API Aggregator

Healthcare / Healthtech

- Electronic Health Record (EHR) Vendor
- Revenue Cycle Management (RCM) Partner

- Telemedicine Platform
- Medical Billing & Coding Vendor
- HIPAA-Compliant Cloud Provider
- Claims Processing Vendor
- Health Information Exchange (HIE)

Retail / E-commerce

- POS System Provider
- Loyalty Program Vendor
- Digital Marketing Agency
- Customer Analytics Service
- Fulfillment / Logistics Partner
- Payment Processing Vendor

Manufacturing / IoT / Industrial

- SCADA / ICS Vendor
- IoT Device Manufacturer
- Industrial Automation Provider
- Robotics Vendor
- Predictive Maintenance Service
- Product Lifecycle Management (PLM) Vendor

Telecom / Cloud / SaaS

- Cloud Hosting Provider (AWS, Azure, GCP)
- Telco Infrastructure Provider
- SaaS Collaboration Tool (Zoom, Slack, etc.)
- CDN Provider
- Data Center Operator
- Email Security Vendor

Professional Services / BPO

- Business Process Outsourcing (BPO) Vendor
- Legal / Contractual Advisory Firm
- Compliance Consulting Partner
- HR / Payroll Processing Vendor
- Background Verification Agency
- Audit & Assurance Firm

Government / Regulated Sector

- Regulatory Reporting / Audit Partner
- Digital Identity & e-KYC Provider
- Government-Sourced Vendor
- Public Cloud with Sovereignty Clause

General Services (Cross-Industry)

- Managed Services Provider (MSP)
- Professional Services
- Legal Advisory Services
- Logistics / Courier Services
- Training / Awareness Program Vendor
- Insurance Provider
- Staffing / Recruitment Agency
- Facility Management / AMC Vendor
- Software Development Partner

Other: ___

Section 2: Nature of Engagement

Field Label	Field Type	Mandatory	Notes

Description of Services	Text area	Yes	Brief service description
Expected Start Date	Date Picker	Yes	—
Contract Value (Approx.)	Number	No	Currency + value format
Contract Type	Radio Buttons	Yes	POC / POV / Pilot / Full Contract / Renewal
Contract Duration	Radio Buttons	Yes	<6 months / 6–12 months / >12 months
Renewal of Existing Third Party	Yes/No	Yes	If Yes, show "Third Party ID" field
Third Party ID	Text	Conditional	Visible only if above is Yes
Fourth Party Involved?	Yes/No	Yes	If Yes, show "Fourth Party Name & Nature" field
Fourth Party Legal Name & Nature of Services	Textarea	Conditional	Visible only if above is Yes

---

Section 3: Data & System Access

Field Label	**Field Type**	**Mandatory**	**Notes**
Types of Data to be Accessed/Processed	Multi-select Checkboxes	Yes	- Personal- Financial- Sensitive Personal/Health- IP- **None (if None, skip next fields)**
Data Classification	Multi-select Checkboxes	Conditional	Only visible if data is not "None"- Confidential / Internal / Private / Public / None
Types of Personal Data Involved	Multi-select	Conditional	Customer / Employee / Company Data
General Volume of Data Accessed or Processed	Dropdown	Conditional	- None- <1,000- 1k–10k- 10k–100k- 100k–1M- >1M- Unknown
Volume of Personal Data Records (PII)	Dropdown	Conditional	- None- <10- 10–100- 100–500- >500- Unknown
Client System Access Required?	Yes/No	Yes	If Yes, show system access type field

Type of System Access	Text Input	Conditional	e.g., API, Remote, VDI, etc.

Section 4: Risk Considerations

Field Label	Field Type	Mandatory	Notes
Cross-border Data Transfer Involved?	Yes/No	Yes	If Yes, show "List Countries" field
List Countries (Cross-border)	Text Input	Conditional	—
Data Hosting/Processing Country	Text Input	Conditional	—
Known Risks (Operational, Reputational, Breaches)	Yes/No	Yes	If Yes, show Describe field
Describe Known Risks	Textarea	Conditional	—
Would a sudden and unexpected loss of this vendor cause a material disruption to your organization?	Yes/No	Yes	If Yes, show Describe field
Would that loss impact your organization's customers?	Yes/No	Yes	If Yes, show Describe field
How difficult will it be to replace this service with an alternative?	Radio Buttons	Yes	Easy / Difficult
Expected Annual Volume of Business-Critical Records	Dropdown	Yes	- <10,000- 10,000–50,000- >50,000
Access to IT Network/Infrastructure?	Yes/No	Yes	If Yes, show Describe field
Is service performed domestically?	Yes/No	Yes	If No, show Describe field
Describe International Service	Text area	Conditional	—

Section 5: Compliance & Security

Field Label	Field Type	Mandatory	Notes

Frameworks/Regulations Applicable to This Engagement	Multi-select Checkboxes	Yes	- GDPR / HIPAA / ISO 27001 / SOC 2 / PCI DSS / NIS 2 / Other / None
Vendor Compliant/Certified with Any Frameworks?	Multi-select Checkboxes	Optional	Ask for supporting documents below

---

Section 6: Reputational & Sanctions Screening (Conditional Display Rule)

If any of the following conditions are met:

- **Country of operations is high-risk (**If country is in a **high-risk or sanctioned list** (e.g., Iran, North Korea, Syria, Russia, Belarus, etc.), then **trigger reputational check**
- **Data sensitivity = Sensitive / Financial / Health AND Volume >100,000**
- **System access or IT network access = Yes**
- **Fourth party involved**
- **Business impact = Yes**
  → Display section: "Reputational Risk & Sanctions Screening")

Field Label	Field Type	Mandatory	Description / Options
Is the third party located in or affiliated with a sanctioned or high-risk country?	Yes/No	Yes	Show country if Yes (Conditional text input)
Is the third party listed on any international sanctions lists (e.g., OFAC, EU, UN, FATF)?	Yes/No	Yes	Tooltip: "Based on initial screening or due diligence tools"
Is the third party involved in any litigation, regulatory action, or adverse media that could harm your organization's reputation?	Yes/No	Yes	If Yes, describe and attach evidence

Section 7: Supporting Documentation & Assessment Opt-Out

Field Label	Field Type	Mandatory	Notes

Upload Supporting Documents	File Upload	Optional	Proposal, Certifications, Risk Reports, etc.
Additional Comments or Context	Textarea	Optional	—
Expected timeline to complete the assessment	Date	Yes	Date select
Due Dilligence exception form	Checkbox (Single select)	Yes	If user opts Yes, route to exception form.

Impact-Based Classification

Based on selected checkboxes and inputs, classify Third party into:

Impact Type	**Trigger Conditions in RIF**	**Explanation**
Regulatory	If any of the following are selected:- Data to be accessed: ☐ Personal ☐ Financial ☐ Health- Data classification: ☐ Confidential / Private- Cross-border transfers: ☐ Yes- Frameworks: ☐ GDPR ☐ HIPAA	Involves compliance with laws/regulations (e.g., GDPR, HIPAA, RBI norms) due to handling sensitive or cross-border data. Requires DPO/legal team involvement.
Financial	If:- Contract value > ₹25 lakhs- ☐ Recurring billing model- ☐ Direct financial systems/API integration (e.g., payment gateway, core banking)	Indicates significant cost exposure or integration with financial systems. Needs finance/legal due diligence (e.g., indemnity, SLA clauses).
Operational	If:- Third party is involved in core product delivery (e.g., hosting, platform module, user-facing tool)- Client system access: ☐ Yes (e.g., API, remote admin)- Data hosting: ☐ Cloud SaaS / IaaS	Impacts uptime, system security, user experience. Requires IT/security review. May be part of business continuity plan.
Reputational	If:- Known Risk/Breach: ☐ Yes- Public-facing services (e.g., customer support, website hosting)- High profile partner (brand association)- Fourth party: ☐ Yes (especially if consumer-facing)	Could impact public trust or brand value due to prior incident or public exposure. Needs comms/legal oversight.

Risk scoring approach:

Example: *SecureHealth Inc.*

1. Third Party Information

Field	Value
Third Party Legal Name	SecureHealth Inc.
Country of Operations	USA
Website URL	www.securehealth.com
SPOC Name / Contact	Jane Doe / jane.doe@securehealth.com / +1-202-555-0101
Type of Third Party	Healthcare / Healthtech → Telemedicine Platform
Nature of Third Party	Established
Data Hosting	Cloud - SaaS

---

2. Nature of Engagement

Field	Value
Description of Services	HIPAA-compliant video consultation platform
Start Date	July 1, 2025
Contract Value	$200,000
Contract Type	Full Contract
Duration	>12 months
Renewal?	No
Fourth Party	No

---

3. Data & System Access

Field	Value
Data Involved	✅ Sensitive Health

Data Classification	✅ Confidential
Type of Data	✅ Customer
Volume of Data	✅ >1 Million
Volume of PII	✅ Above 500
System Access	✅ Yes – API, Remote
Network Access	✅ Yes

---

4. Risk Considerations

Field	**Value**
Cross-border	✅ Yes (USA ↔ UAE)
Known Incidents	❌ None
Business Disruption	✅ Yes
Customer Impact	✅ Yes
Ease of Replacement	❌ Difficult
IT Network Access	✅ Yes
Domestic Delivery	❌ No (Outsourced support from India)

---

5. Compliance & Security

Field	**Value**
Frameworks Relevant	✅ HIPAA, ✅ GDPR, ✅ ISO 27001
Certifications	✅ ISO 27001 Cert, ✅ HIPAA Report Uploaded

📊 **NIST-Aligned Risk Scoring (1–3 Scale)**

Step 1: Inherent Risk Scoring

Risk Factor	Justification	Score
Data Sensitivity	Sensitive health data (PHI)	3 (High)
Data Volume	>1 million records/year	3 (High)
System Access	API + Remote access	3 (High)
Geography	UAE is not GDPR adequate	2 (Moderate)
Business Criticality	Disruption impacts care delivery	3 (High)
Prior Incidents	No known history	1 (Low)

Inherent Risk Score = (3 + 3 + 3 + 2 + 3 + 1) / 6 = 2.5 (High)

Step 2: Control Effectiveness Scoring

Control Domain	Input	Score
Technical Controls	ISO 27001 certified	3
Process Controls	HIPAA policies and procedures shared	2
Contractual Controls	DPA + SLA included	3
Supply Chain Risk	Mixed geography, moderate risk	2
Audit History	Clean certifications	3

Control Effectiveness Score = (3 + 2 + 3 + 2 + 3) / 5 = 2.6 (Strong)

Step 3: Residual Risk Calculation

Residual Risk = Inherent Risk ÷ Control Effectiveness = 2.5 ÷ 2.6 = ~0.96

Metric	Value	Risk Level
Inherent Risk Score	2.5	**High**
Control Effectiveness	2.6	**Strong**
Residual Risk Score	0.96	**Low**

✅ **Final Risk Decision Output (for TRACS UI)**

- **Residual Risk Level:** Low (Proceed with onboarding)
- **Risk Tier:** Tier 1 Critical Vendor → **Annual Review Required**
- **Recommended Actions:**
    - Maintain SLAs and DPA enforcement
    - Monitor any changes in processing volumes or cross-border arrangements

Final Vendor Tier Matrix

Final Tier	Description	Inherent Risk	Residual Risk	Business Impact
Tier 1 – Critical	Key to operations, sensitive data, high exposure	High (≥2.1)	Medium or High	High dependency
Tier 2 – High	Processes sensitive/internal data, some customer/system access	Medium–High (1.6–2.5)	Medium	Medium dependency
Tier 3 – Medium	Limited access or non-critical services	Medium (1.5–2.0)	Low	Low–Moderate
Tier 4 – Low	No data/system access, replaceable vendors	Low (≤1.5)	Low	No impact