AI Native Risk Intelligence Driving Better Risk Management

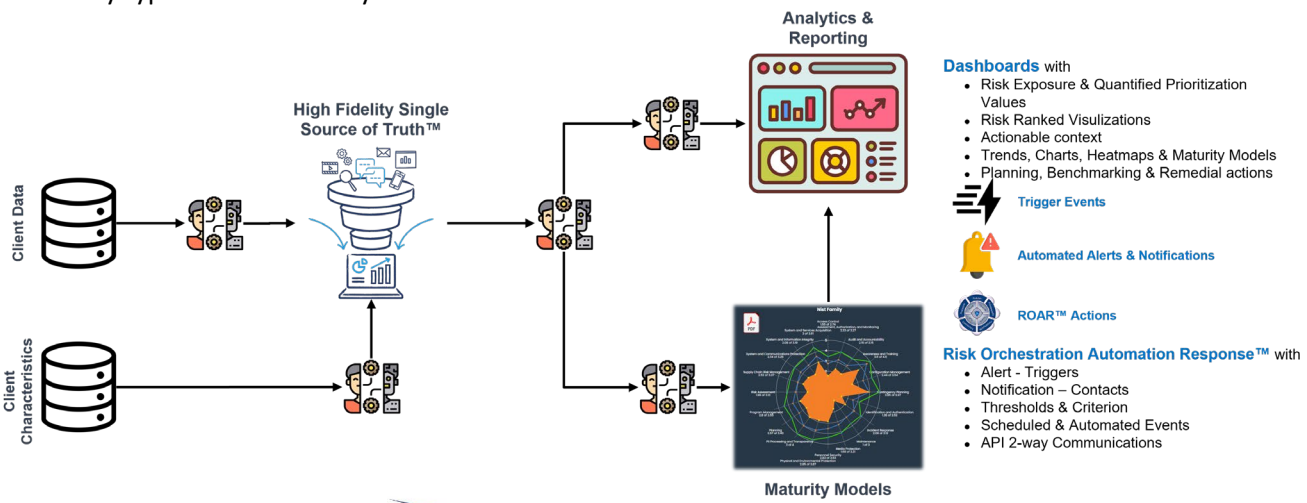
Using our AI Native Integrated Risk Modeling & Decisioning Platform® (IRMD®) solution allows companies to measure, monitor, quantify, and report on many types of risks side-by-side and on-demand. Risks related to cybersecurity, data privacy, regulatory compliance, operational effectiveness, supply chain resilience, and more. Clients refer our **ROAR®** – Risk Orchestration Automation Response® capability as the next generation of GRC Management and our **TOAR®** – Threat Orchestration Automation Response™ as a highly evolved Tactical Threat to Strategic Risk Management solution.

IRMD® creates a timely, contextualized, enterprise-wide view of the organization's unique risk profile. Which eliminates the informational and operational silos common in enterprise risk management and empowers risk managers, executives, and board members to compare one vulnerability to another and understand the biggest threats facing their organizations.

RiskOpsAI™ IRMD® solution is an AI Native, Client risk data driven, risk modeling capability which links business risks to the company's strategic objectives and risk tolerance, for comparisons and quality decisioning about where to allocate resources and how to pivot as new risks emerge and informed by the risk exposure critical context. Enabling quantified Risk decisioning from the strategic business layer designed to protect brand value.

Using the Integrated Risk Model Data Normalizer™ (IRMDN™) with Client telemetry data, a company aggregates and centralizes its risk data in the RiskOpsAI™ High Fidelity Single Source of Truth™ dataset where it is augmented with Client characteristics. The Risk Framework Control Collection™ (RFC2™) then leverages the information in across a variety of Client selected Risk Frameworks, The data is they refined using several microservices, for example, the Risk Control Effectiveness Model™ (RCEM™) assessing the need for cyber insurance or using the Risk Framework Carve-Out™ (RFCO™) leveraging our multi-layered quantification models developing risk exposure values and monetization, ensuring compliance with the myriad cyber, data privacy, or compliance regulations enacted in jurisdictions around the world.

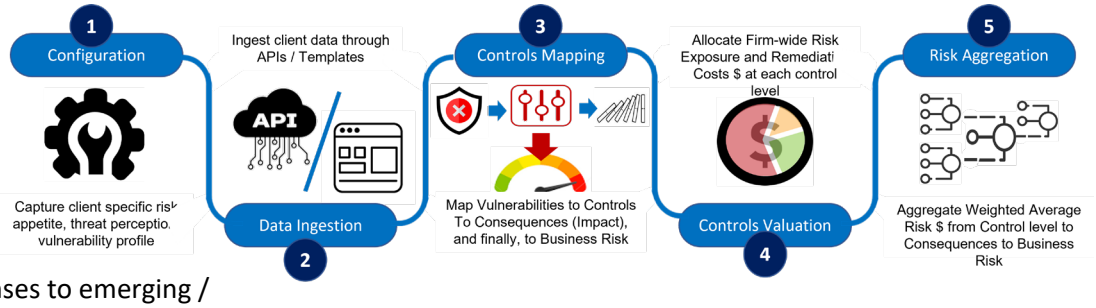
Lastly, Risk Orchestration Automation Response® (ROAR®) automates manual actions. Programmatically acting upon threat-risks related to cybersecurity, data privacy, regulatory compliance, operational effectiveness, supply chain or operational resilience, and more. Automating the ability to measure, monitor, qualify / quantify (monetize) and report on many types of risks side-by-side on-demand.



RiskOpsAI™
We Believe Risk Can Be Managed™

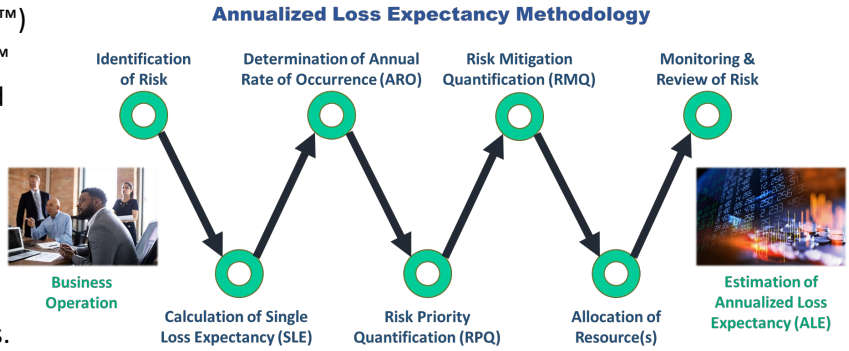
A Customized, Personalized Perspective

Using our 5-step process to set up a unique platform experience typically within 2 to 3 weeks, each Client feeds its IRMD® platform, using API's, uploads CSV files, or manually inputs data via our assessment interface, with up-to-date internal data and information reflecting its specific circumstances currently available. Our unique 'Bottom-up to Top-down' modeling approach supports risk data mapping to business Goals & Objectives precisely conveys the organization's risk profile and benchmarks to inform priority decision making and operational responses to emerging / evolving risks. Providing a level of risk agility not previously found.



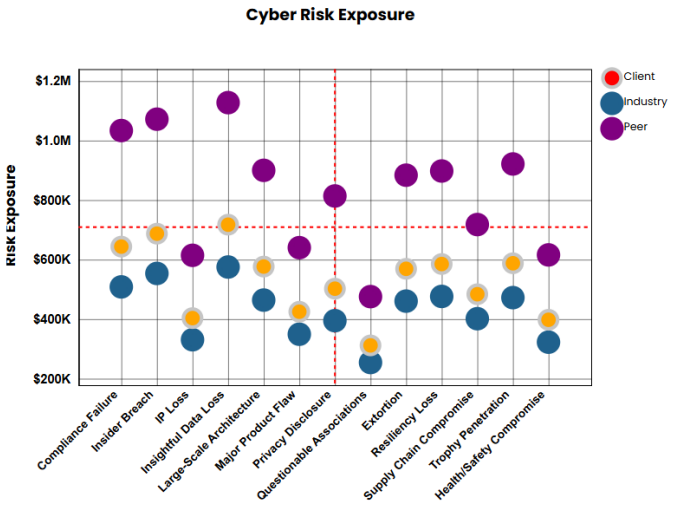
Financial Impact is Quantified

The IRMD® goes far beyond traditional risk scoring methodology to calculate and predict the risk exposure financial impact, remediation cost, and annual loss expectancy of each data record of risk across the enterprise. Using The RiskOpsAI™ Risk Common Key Control Set™ (RCKCS™) measuring within the Risk Common Control Model™ (RCCM®) using AI Native methods for qualifying and validating risk, the Integrated Risk Modeling Risk Quantification™ (IRMRQ™) microservice model then quantifies risk exposure in three layers so that decision-makers can immediately compare the severity of one risk challenge to another, set priorities, and create data-driven remediation plans.



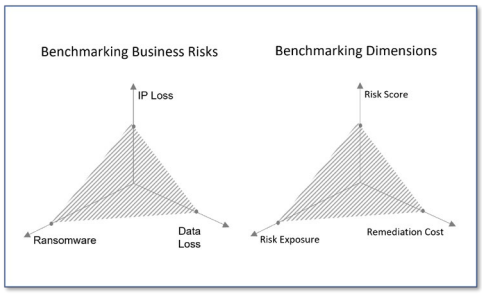
Industry-Specific Risk Benchmarking

Traditional benchmarks available today, unfortunately, typically provide only high-level guidance due to the generic framework applied. On the other hand, within the IRMD® data can be adjusted to take account of industry type, company size, risk appetite, data assets, and other factors. This provides a company-specific industry benchmark to assess a company's specific threat exposure and overall risk management program performance.



Best-in-class “outside-in” risk benchmarking maps three coordinates:

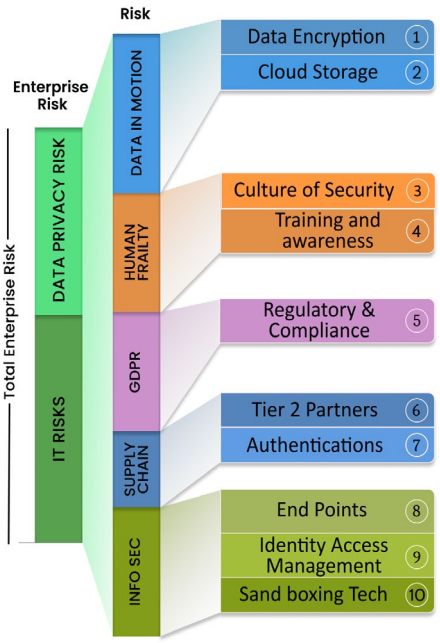
1. The enterprise’s own risk profile and risk values based on its unique data.
2. Broad industry average risk values.
3. A narrower band of benchmark data reflecting the enterprise’s specific peer group.

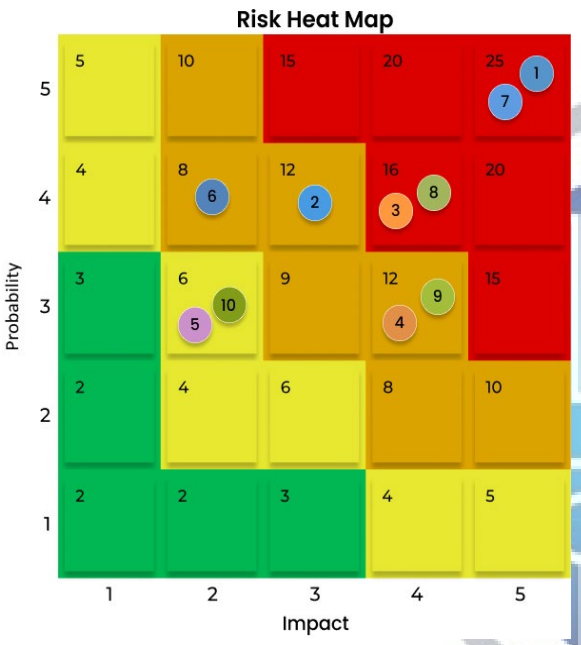


Visualized within virtually any risk / compliance framework, or risk model available or even those clients customized for specific use cases.

Persona based Dashboard Reporting for Executive, Management, and Operational Teams

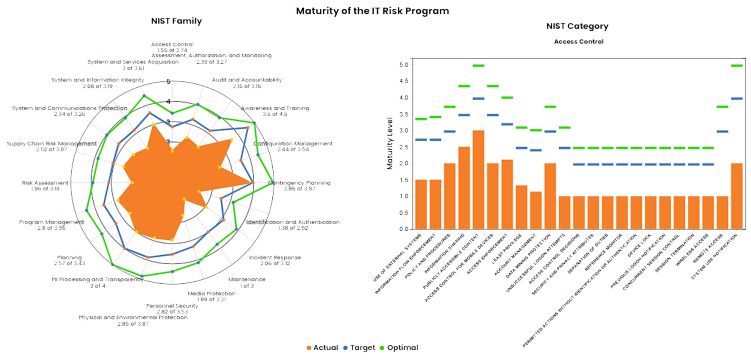
The RiskOpsAI™ IRMD® collects and analyzes a Client organizations risk data, translates it into business intelligence, and presents it visually in intuitive dashboards — customizable for each level of the organization. This enables C-Suite, functional leadership, and operations to drill into the information that they need to do their jobs and to communicate with each other more effectively as decisions are made.





This Executive Persona view example is reflected in the Risk Heat Map and the aligned expansion detail is an example of the ability to illustrate the top ten business threats approaching the material breach level required within new US / EU regulations. Showcasing the areas impacted and the ability to expand out the organization’s remediation efforts in one simple visualization.

Or Management Persona showing various risk management teams how well their risk areas are meeting compliance, maturity and their resilience to prevent reputational or operational harm.

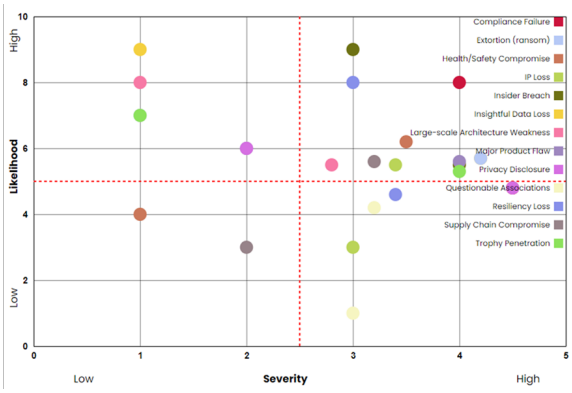


This Maturity visualization is traditionally derived from a formal risk assessment, in the IRMD® it can show the risk exposures of any part of the organization at a click of a button. Bringing AI Native capability to all the operational teams referencing from the same definition of risk exposure to the organization.

Risk Scenario Planning

Native Artificial Intelligence and Machine Learning makes the RiskOpsAI™ solution a reliable, predictive process that enables enterprises to compare threats — looking at best and worst-case scenarios — and decide where to invest in risk mitigation.

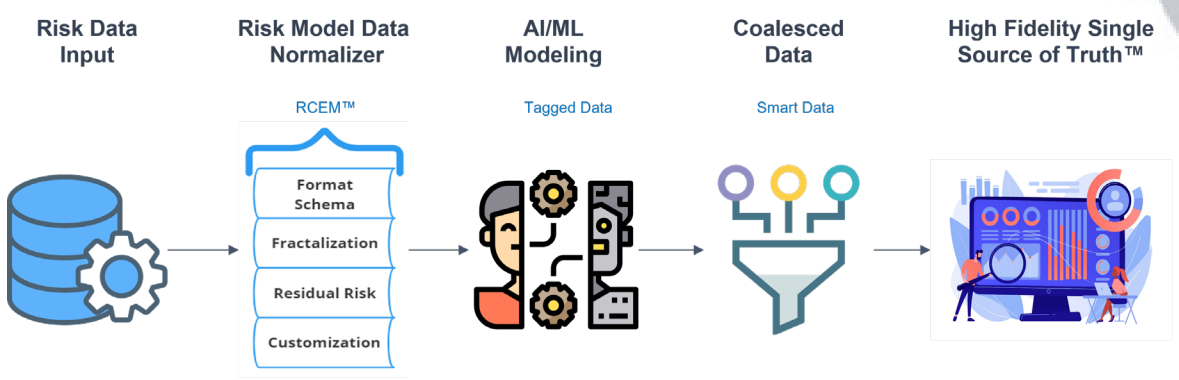
#	Business Risks	Likelihood	Risk Exposure	Remediation Cost	Remediation Cost in %
1	Business continuity	3.1	5493638	1098654	63%
2	Climate/Environment	2.9	4592599	918459	35%
3	Competition	2.8	4660146	931967	79%
4	Cyber attack	3.9	9068017	1813482	58%
5	Geo-political	2.7	4690629	938061	84%
6	Supply chain	3	4480633	896068	42%
7	Third party vendors	2.9	6182454	1236408	69%
8	Financial	3.7	7529523	1505805	18%
9	M&A	3	4664447	932826	90%
10	Operational	4.3	7519963	1503893	57%
11	People/talent	2.8	4828169	965573	79%
12	Product quality	3.5	6436427	1287198	32%
13	Intellectual Property	2.5	4984078	996746	66%
14	Legal	3.3	3701086	740167	87%
15	Regulatory Compliance	4.3	6681750	1336258	52%



Rapid Platform Customization and Deployment

When you buy a business suit, you start with the same product as the next person and then make any necessary alterations. The length of the sleeves, the hem, perhaps the waistline. A bit of tailoring to make it bespoke and ensure it's a perfect fit for you. You don't wear it home off the rack and you don't design a new suit from scratch. It's 90% ready, and you and the tailor do the rest to make it yours.

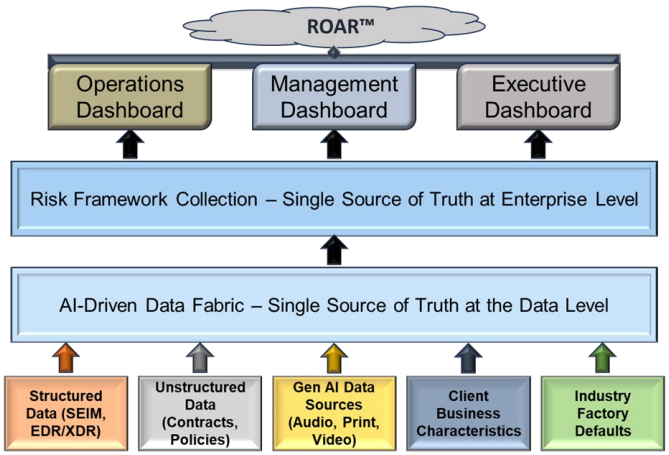
That's the RiskOpsAI™ IRMD® approach to enterprise risk modeling. It starts with a template and default settings that reflect best practices, experience, and common preferences. Then it adjusts to reflect your company's industry, unique set of risks, the weight it gives to specific vulnerabilities, and its objectives, business priorities, and risk appetite. This initial customization enriches the platform, establishes the training of the AI/ML models with your data and your unique characteristics enabling the generation of risk quantification and exposure analytics that are accurate and specific for your organization.



We believe in a Crawl – Walk – Run mindset to ensure no major process break, or any heavy lifting is required to stand up our IRMD® platform. A couple of 1-hour workshops and some sample data and that's enough needed to establish an AI Native IRMD® model with your data to tell your data's story.

Conclusion

The RiskOpsAI™ Integrated Risk Modeling & Decisioning Platform® is defined as a set of best practices and processes supported by a risk-aware culture and enabling advance AI technologies. This platform can be established in as little as 2 weeks with a model that improves decision making and performance through an integrated view of how well an organization manages its unique set of risks. Under this definition, Integrated Risk Modeling & Decision Making has certain attributes: strategy, assessment, response, communication & reporting, monitoring, and technology.



IRMD® platform enhances, supports, and informs of the risks confronting from small to large to mega sized companies. Enabling them to continue to expand, mature, change, accelerate, and grow more in tune with their risk profile and posture. Ransomware attacks, regulatory demands, technological disruption, disparate state and national data privacy laws, geopolitical tensions threatening vulnerable supply chains — these are just a few of the challenges organizations face day after day.

As common-to-advance risks emerge and evolve, companies often lack the information and context needed to assess their risk situation effectively, compare one threat against another, gauge the implications, set priorities, and make informed decisions. They need their organization-wide risk profile presented clearly, in real-time, to enable informed, consistent decision-making – at the board, managerial, and operational levels.

AI Native *Continuous* Risk Exposure Management

Continuous Cyber Risk Compliance

- *Continuous* AI-Driven Risk Compliance Validation
- AI-Driven Multi-layer Risk Exposure Quantification
- Control Effectiveness Cyber Program based Maturity Modeling

Thirdparty Threat Exposure Management

- *Continuous* AI-Driven Vendor Risk Exposure Quantification
- Automated Stack ranked vendors by Risk Exposure
- AI-Driven Vendor Lifecycle Risk Assessment automation using ROAR™

Continuous Control-Tool Rationalization

- *Continuous* AI-Driven Control Effectiveness Data Coverage
- Tool–Control Coverage gaps & redundancy identification
- Rationalized performance / risk key indices Optimization driven Decision-making

About OptimEyes AI® d.b.a. RiskOpsAI™ (Risk Operations Using AI™)

San Diego-based OptimEyes AI® doing business as RiskOpsAI™ known as the Integrated Risk Modeling & Decisioning® Company, is a pioneer of AI-driven, IRMR methodologies. Built by cyber, risk, and compliance veterans, our software-as-a-service (SaaS) platform helps Fortune 2000 organizations discover, measure, prioritize, predict, and optimize cybersecurity, data privacy, and enterprise risks. For more information, contact us at info@optimeyes.ai, and visit https://optimeyes.ai, and follow us on:

**** For a No Obligation Risk Assessment evaluation, please contact: sales@optimeyes.ai***