Approach to Network & Information Security (NIS2) Directive

ENISA's understanding of the expansive nature of threats predicted through 2030, ENISA has updated their NIS Directive to a broader level of coverage under the recently published NIS2 Directive.

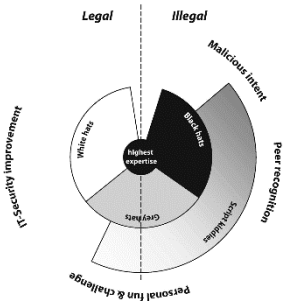
The RiskOpsAI™ fulfillment of Gartner's emerging CTEM (Continuous Threat Exposure Management) category offers an AI driven continuous and predictive approach to NIS2's wholistic risk governance / management, through supporting of effective risk AI foresight decision-making, driving business protections.

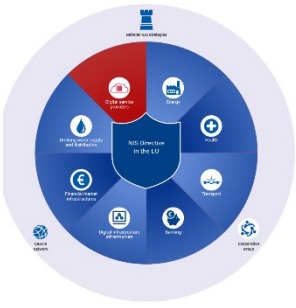
- Organizations carry significant risk in today's rapidly changing operational technology landscape, where predicting and minimizing the impact of multiple digital service providers risks (including cyber, data privacy, compliance and ESG) can be challenging.
- The current tactical approach to digital service providers risk management (reactive, siloed, periodic and piecemeal) fails to connect the impact of risk to an organization's business goals and objectives.
- Aggregating third party risk data from multiple vendors and suppliers to create a single source of truth is a risk management imperative when seeking to eliminate blind spots and reduce exposure.

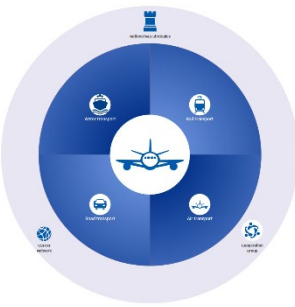
Digital Service Providers Risk Management

NIS2 broadens the scope of covered to include a governance centric approach and with the addition of IOT/OT (ICS) driven under the IEC 62443 controls brings digital business and supplier into a common risk management structure. The RiskOpsAI platform provides detailed drill down analytics (by risk framework, provider, function) where each digital service providers risk exposure is visualized and reported for informed decision-making.

- Highly and wholistic focus on Digital Service Provider risk across various services.
- Transparency of exposure by Digital Service Provider enables direct governance actions.







A Comprehensive View of Digital Service Provider Risk

The NIS2 scope is covered by two annexes. The Directive applies to both public and private entities referred to in Annex I or II.

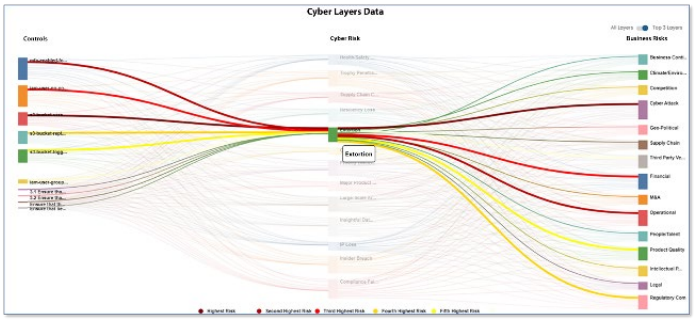
- Annex I scope includes the sectors of high criticality, which can be either an Essential or an Important entity depending on the total annual revenue and size of the organization (Energy, Transportation, Health, Potable Water, FinTech Infrastructure, Banking, & Digital Infrastructure).
- Annex II provides the other critical sectors set out by the EU, which will only fall into the Important Entity category (Postal, Food, Waste Management, Manufacturing, Manufacturing of Chemicals, & Digital Providers).

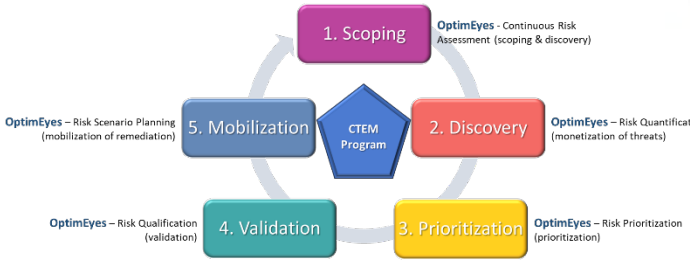
AI Driven Digital Providers Risk Analytics & Visibilities

The RiskOpsAI™ driven CTEM platform generates dashboards that are highly configurable for multiple personas and use cases. Furthermore, each dashboard is highly customizable for multiple purposes and roles to generate a wide range of Digital Providers analytics.

Comprehensive and customizable visual illustrations offer direct threat correlation to Digital Providers to quickly identify where the risks are original and their impact to business operations. This provides direct Continuous Threat Exposure Management (CTEM).

Governing decision, through meaningful dashboard insights minimize negative events, enables support for resources and support business goals.





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***