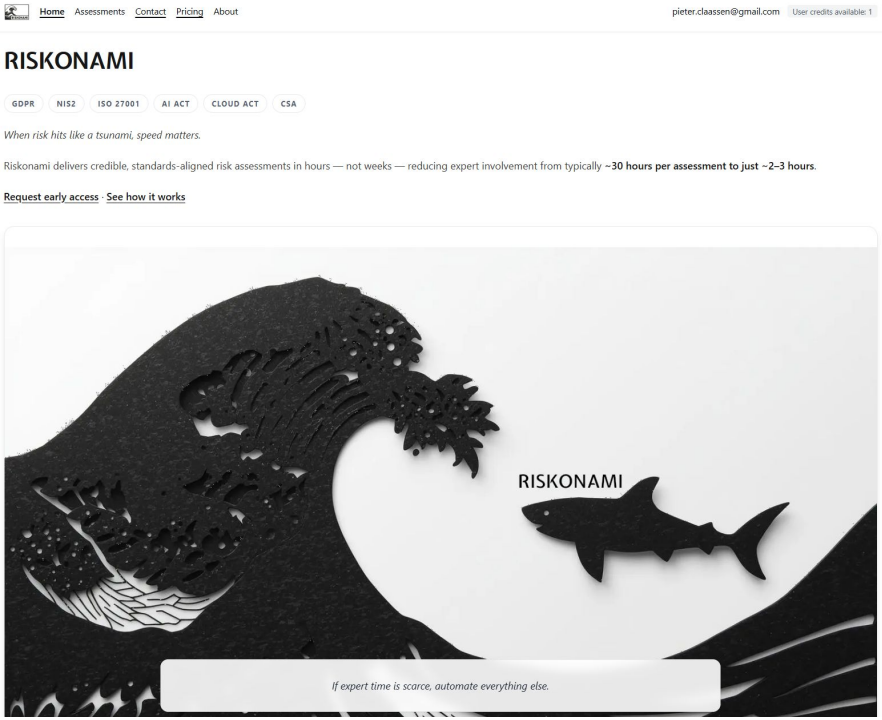
Riskonami

The giant in AI based Operational Risk Assessment

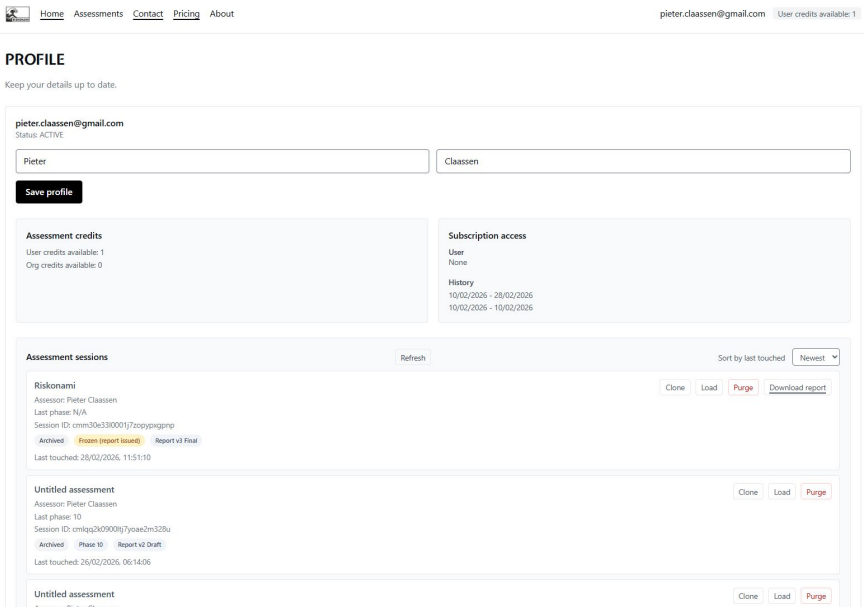
Welcome to Riskonami



https://riskonami.com

- Riskonami is an AI-powered risk assessment platform that transforms how organizations perform operational security risk assessments.
- It leverages collective security knowledge and threat intelligence to identify risks that humans often overlook.
- Riskonami is built on a PhD-assured model for governance and reliability. This ensures managed model drift, high repeatability of outcomes, analytical completeness, and daily assurance validation.
- The platform is designed to measure alignment with ISO 27001 and generate NIS2-compliant reports.
- Most importantly, it dramatically reduces effort.
  - Traditional assessments take around thirty hours.
  - With Riskonami, this is reduced to between one and three hours.
- It is delivered as an enterprise SaaS platform, GDPR compliant, and hosted in Europe.

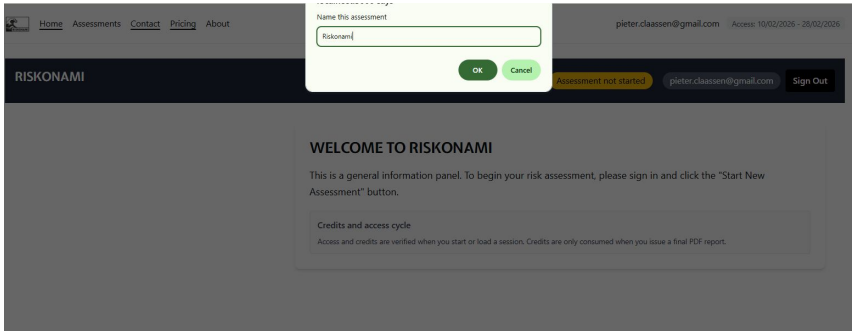
Multi user/multi assessment



- ➔ Riskonami allows you to manage multiple assessments simultaneously.
- ➔ You can save and load assessments from your profile, share them with colleagues, and download them at any stage.
- ➔ Once reports are issued, they can be re-downloaded at any time.
- ➔ The platform is built for collaboration and full lifecycle management.

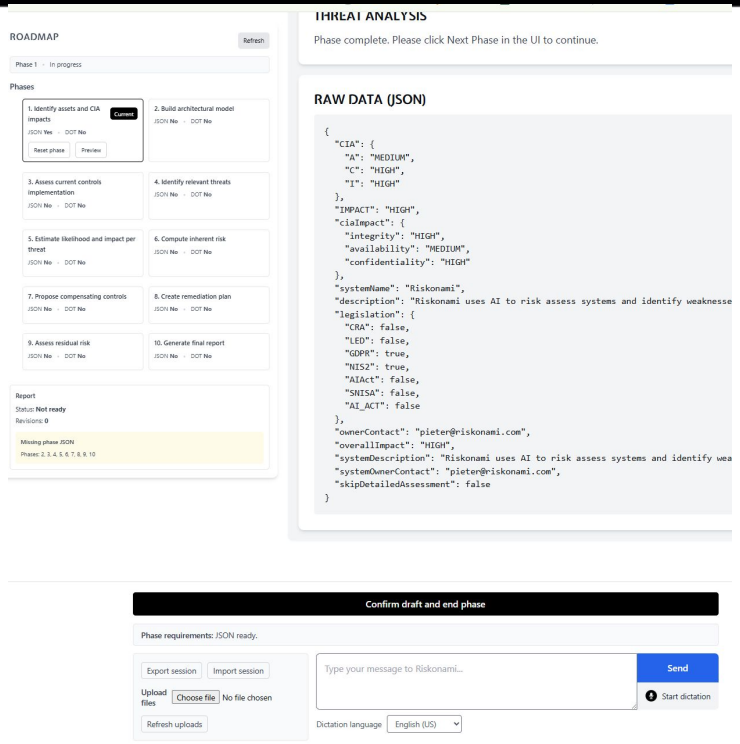
https://riskonami.com

Start the assessment



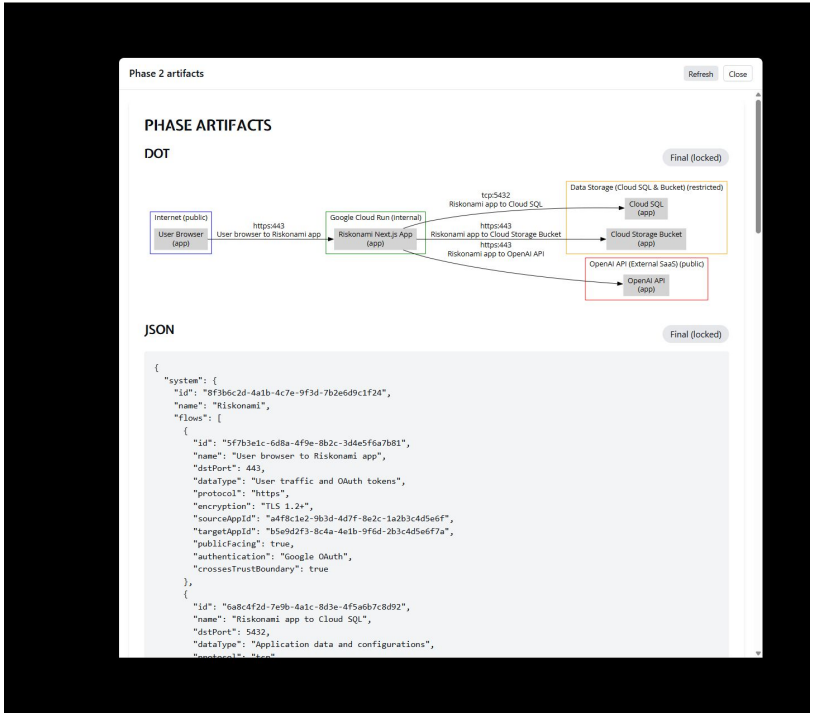
- ➔ To begin, you create a new assessment and assign it a name.
- ➔ From there, Riskonami guides you through a structured, AI-driven workflow that standardizes the entire assessment process.

Impact assessment



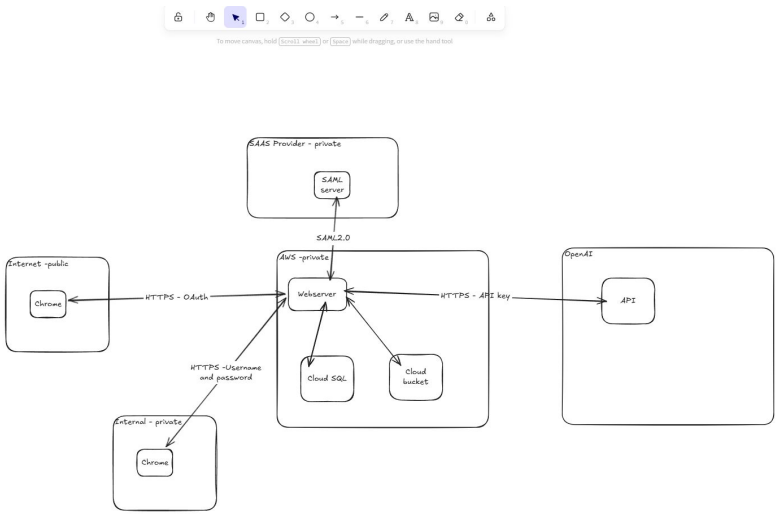
- ➔ In Phase One, Riskonami determines how critical your application is to your organization.
- ➔ This is done by evaluating confidentiality, integrity, and availability.
- ➔ It also considers applicable legislation and regulatory exposure.
- ➔ This establishes the system's impact profile and forms the foundation for the rest of the analysis.

System analysis



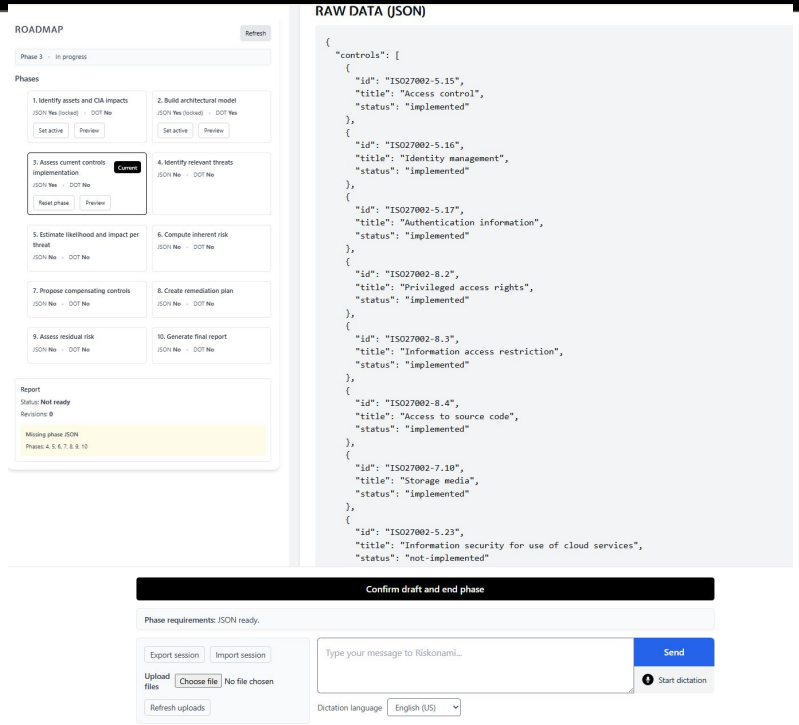
- ➔ In Phase Two, Riskonami builds your system model interactively.
- ➔ It identifies trust zones, maps applications, and analyzes flows between zones.
- ➔ The AI continuously questions you until the system is fully described.
- ➔ This structured model drives all downstream threat and control analysis.

System analysis



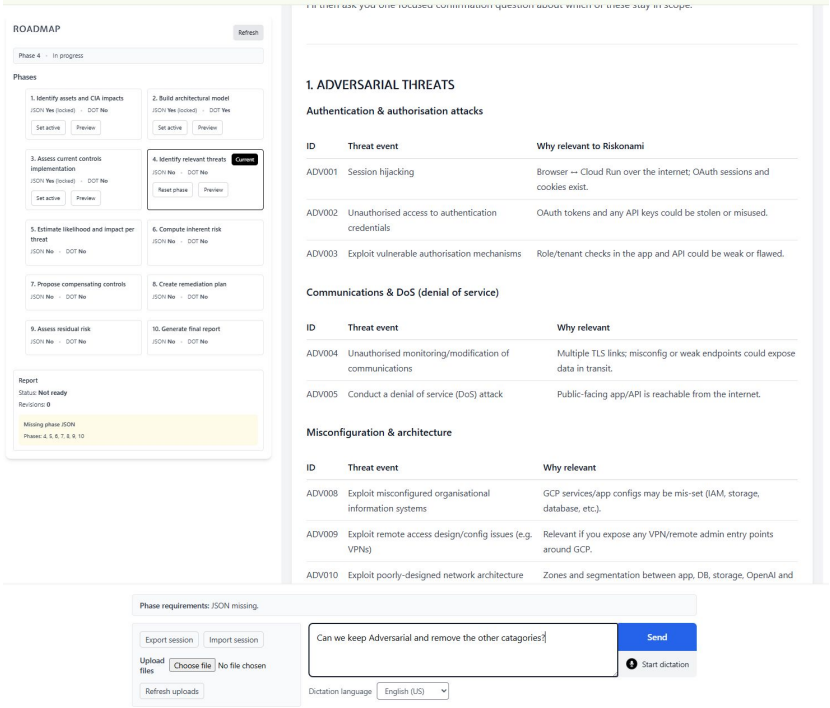
- ➔ If you already have architecture or flow diagrams, you can upload them directly.
- ➔ Riskonami analyzes the diagrams, documents and images. It extracts system structure, and generates a candidate threat model.
- ➔ This accelerates the modeling process while preserving accuracy and completeness.

Control Identification



- In Phase Three, Riskonami identifies the relevant ISO 27001 controls for your system.
- It assesses which controls are currently implemented and determines their level of maturity.
- Through interactive questioning, it validates implementation status to ensure accuracy.

Threat enumeration

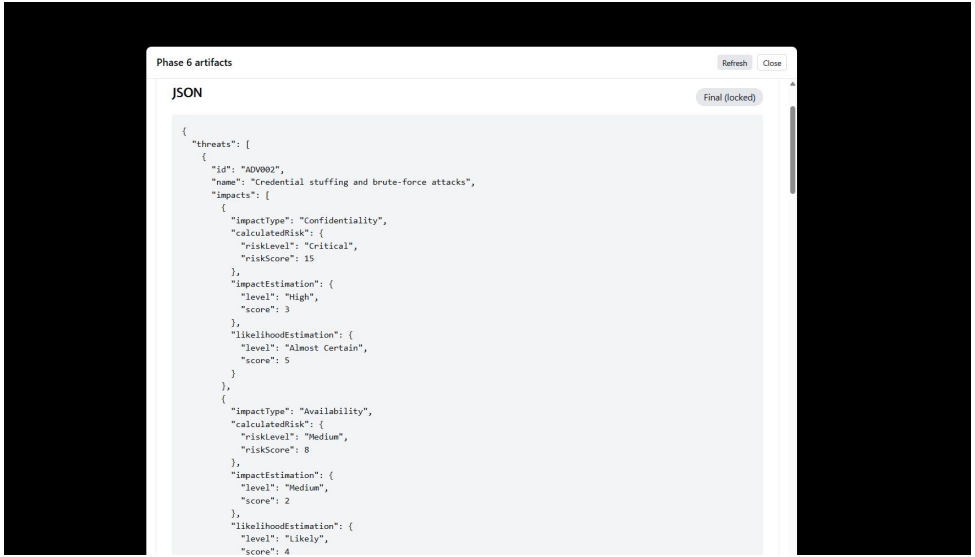


- ➔ In Phase Four, Riskonami enumerates threats using a structured taxonomy.
- ➔ Threats are classified as adversarial, environmental, or accidental using IRAM2 TEC and TCL.
- ➔ The system proposes relevant threats for your specific model, and you confirm their applicability.

Likelihood Estimation

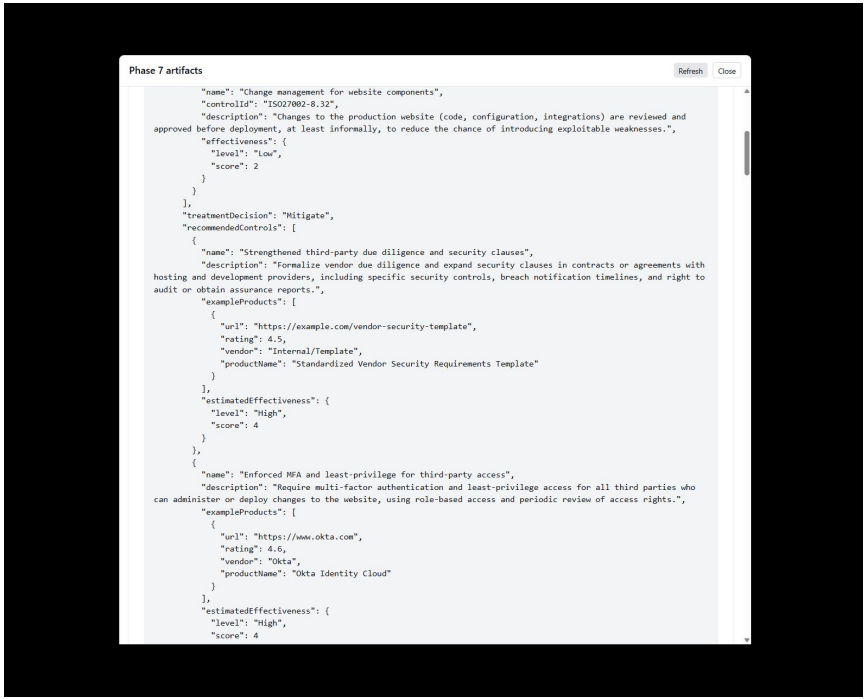
- ➔ In Phase Five, Riskonami estimates the likelihood of each threat.
- ➔ This is based on industry data, observed attack patterns, threat actor capability and motivation, targeting likelihood, and historical evidence.
- ➔ You can confirm or adjust these values to ensure the results are realistic and defensible.

Inherent Risk Calculation



- ➔ In Phase Six, Riskonami combines threats, likelihood estimates, and existing controls to calculate the inherent risk posture of your system.
- ➔ This reflects your organization’s exposure before remediation.

Risk Treatment and Compensating Controls

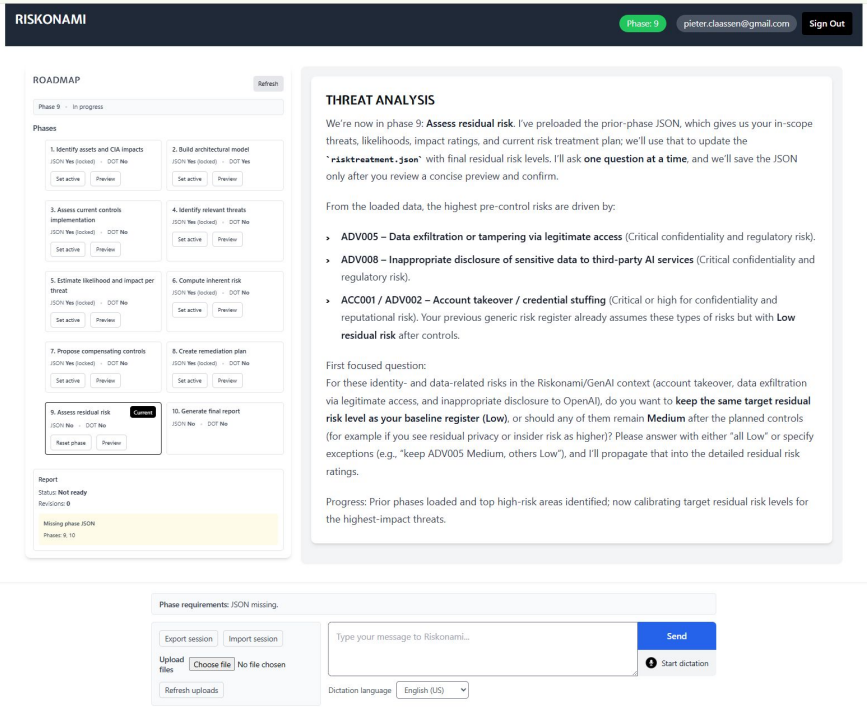


- ➔ In Phase Seven, Riskonami recommends compensating controls and provides practical, real-world mitigation examples.
- ➔ You then decide how each risk will be treated — whether it will be accepted, mitigated, or transferred.

Remediation Planning

- ➔ In Phase Eight, Riskonami generates a practical remediation plan.
- ➔ This includes clearly defined actions, assigned task owners, agreed deadlines, and prioritization.
- ➔ The output becomes operational and trackable.

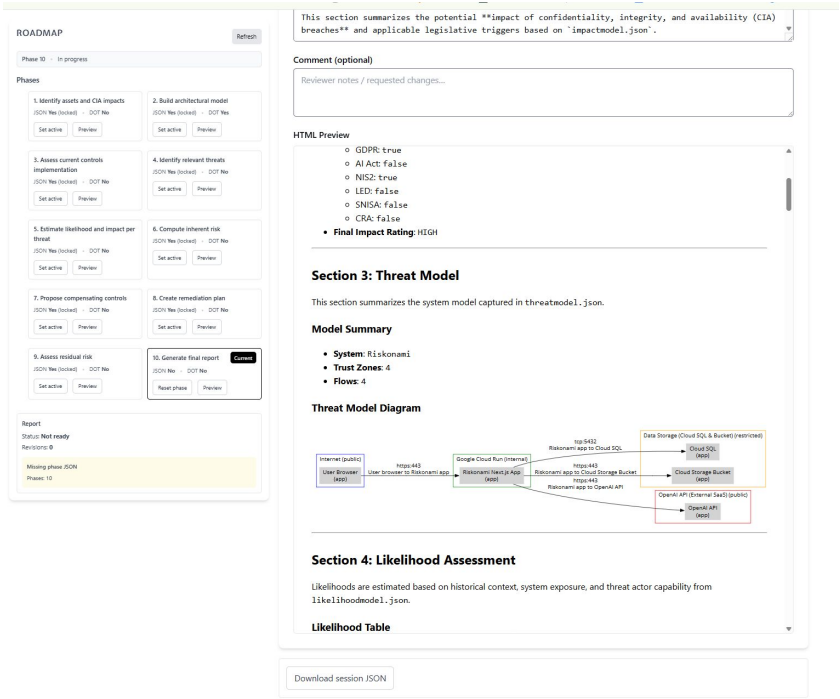
Residual Risk Assessment



- In Phase Nine, once planned controls are applied, Riskonami recalculates residual risk.
- This quantifies the remaining exposure.
- If risk remains, it can be formally accepted and documented in alignment with NIS2 requirements.

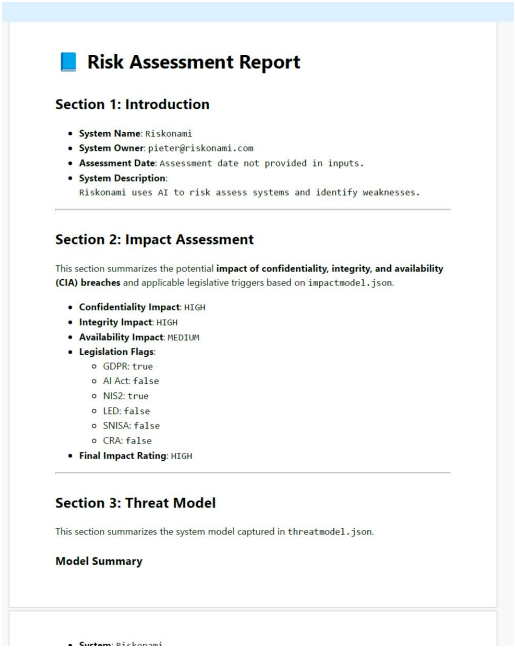
https://riskonami.com

Report Generation and Issuance



- ➔ Riskonami generates a full report that can be previewed in HTML.
- ➔ The report is authored in Markdown and includes all diagrams and system models.
- ➔ Before issuance, it is fully editable.
- ➔ Once issued, the assessment is locked to ensure integrity.
- ➔ You may clone the assessment to begin a new cycle or regenerate reports as required.

Final PDF Report



📘 **Risk Assessment Report**

Section 1: Introduction

- **System Name**: Riskonami
- **System Owner**: pieter@riskonami.com
- **Assessment Date**: Assessment date not provided in inputs.
- **System Description**:
  Riskonami uses AI to risk assess systems and identify weaknesses.

Section 2: Impact Assessment

This section summarizes the potential **impact of confidentiality, integrity, and availability (CIA) breaches** and applicable legislative triggers based on impactmodel.json.

- **Confidentiality Impact**: HIGH
- **Integrity Impact**: HIGH
- **Availability Impact**: MEDIUM
- **Legislation Flags**:
  - GDPR: true
  - AI Act: false
  - NIS2: true
  - LED: false
  - SNISA: false
  - CRA: false
- **Final Impact Rating**: HIGH

Section 3: Threat Model

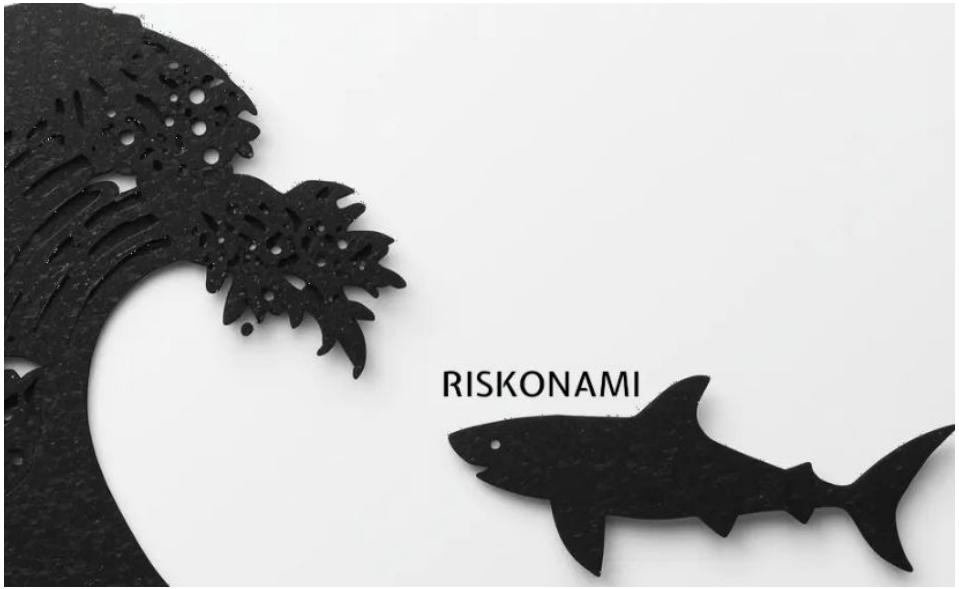
This section summarizes the system model captured in threatmodel.json.

Model Summary

- **System**: Riskonami

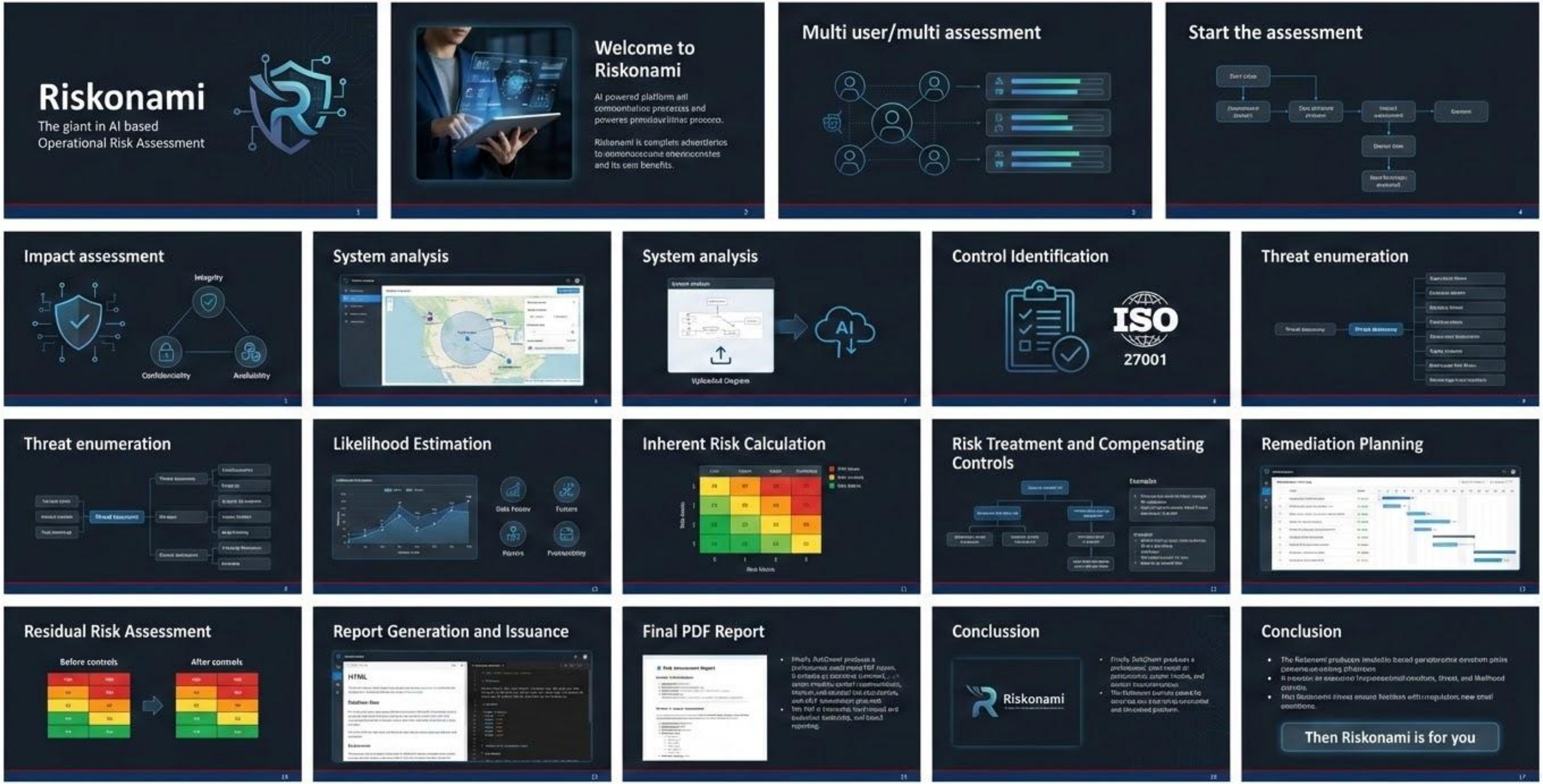
- ➔ Finally, Riskonami produces a professional, audit-ready PDF report.
- ➔ It includes an executive summary, system models, control implementation status, threat and likelihood analysis, inherent and residual risk calculations, and a full remediation plan with ownership and timelines.
- ➔ The PDF is immutable once issued and suitable for auditors, regulators, executive leadership, and board reporting.

Conclusion



- ➔ If you are worried about actual risk
- ➔ If you need GDPR, NIS2 and ISO risk assessments done
- ➔ If you are focused on risk and not compliance
- ➔ If you want enchanted analysis faster at a reduce cost

Then Riskonami is for you



https://riskonami.com