

Riskonami

The giant in AI based Operational Risk Assessment

Welcome to Riskonami

Home Assessments Contact Pricing About pieter.classen@gmail.com User credits available: 1

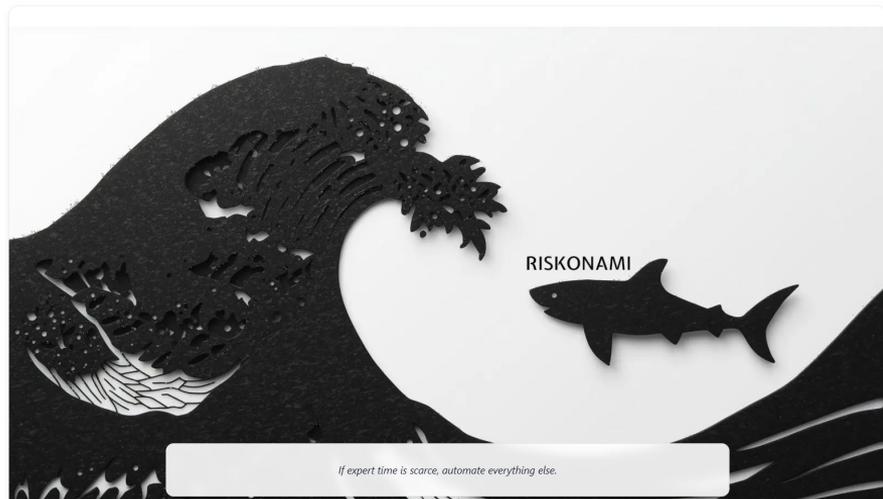
RISKONAMI

GDPR NIS2 ISO 27001 AI ACT CLOUD ACT CSA

When risk hits like a tsunami, speed matters.

Riskonami delivers credible, standards-aligned risk assessments in hours — not weeks — reducing expert involvement from typically ~30 hours per assessment to just ~2-3 hours.

[Request early access](#) - [See how it works](#)



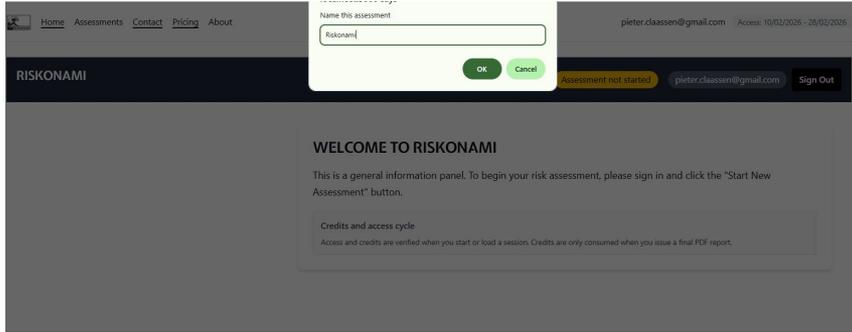
- Riskonami is an AI-powered risk assessment platform that transforms how organizations perform operational security risk assessments.
- It leverages collective security knowledge and threat intelligence to identify risks that humans often overlook.
- Riskonami is built on a PhD-assured model for governance 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

The screenshot displays the user profile for 'pieter.classen@gmail.com'. At the top, there are navigation links: Home, Assessments, Contact, Pricing, and About. The user's email and available credits are shown. The profile section includes a name 'Pieter' and a last name 'Claassen', with a 'Save profile' button. Below this, there are two summary boxes: 'Assessment credits' showing 1 user credit and 0 city credit, and 'Subscription access' showing 'User: None' and a 'History' of dates from 10/02/2026 to 10/02/2026. The main section is 'Assessment sessions', which lists three sessions. The first is 'Riskonami' with a 'Frozen (report issued)' status and a 'Download report' button. The second is 'Untitled assessment' with a 'Phase 10' status. The third is another 'Untitled assessment'. Each session has 'Clone', 'Load', and 'Purge' buttons. The page also includes a 'Refresh' button and a 'Sort by last touched' dropdown menu.

- 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.

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

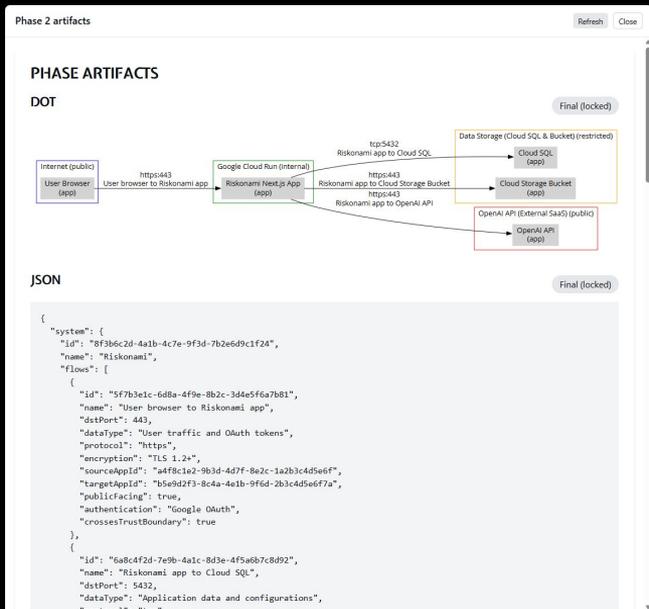
The screenshot displays the Riskonami interface. On the left, the 'ROADMAP' section shows a progress bar for 'Phase 1' (In progress) and a grid of 10 phases. Phase 1, 'Identify assets and CIA impacts', is highlighted as 'Current'. Below the roadmap is a 'Report' section with a 'Status: Not ready' and a 'Revision: 0'. The main area is titled 'IHREAT ANALYSIS' and shows a message: 'Phase complete. Please click Next Phase in the UI to continue.' Below this is a 'RAW DATA (JSON)' section containing a JSON object with the following structure:

```
{
  "CIA": {
    "A": "MEDIUM",
    "C": "HIGH",
    "I": "HIGH"
  },
  "IMPACT": "HIGH",
  "CIAImpact": {
    "Integrity": "HIGH",
    "availability": "MEDIUM",
    "confidentiality": "HIGH"
  },
  "systemName": "Riskonami",
  "description": "Riskonami uses AI to risk assess systems and identify weaknesses",
  "legislation": {
    "CRA": false,
    "LED": false,
    "GDPR": true,
    "NIS2": true,
    "AIAct": false,
    "NISIA": false,
    "AI_ACT": false
  },
  "ownerContact": "pieter@riskonami.com",
  "overallImpact": "HIGH",
  "systemDescription": "Riskonami uses AI to risk assess systems and identify weaknesses",
  "systemOwnerContact": "pieter@riskonami.com",
  "skipDetailedAssessment": false
}
```

- 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.

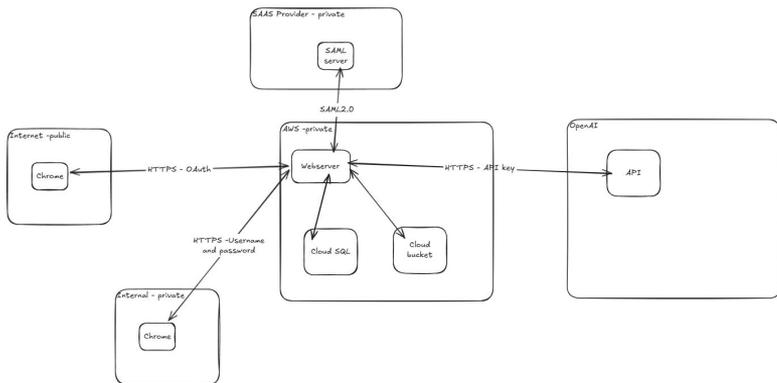
The screenshot shows a 'Confirm draft and end phase' dialog box. It contains a 'Phase requirements: JSON ready.' message. Below this are 'Export session' and 'Import session' buttons. There is an 'Upload files' section with a 'Choose file' button and a 'No file chosen' status. A 'Refresh uploads' button is also present. On the right, there is a text input field with the placeholder 'Type your message to Riskonami...', a 'Send' button, and a 'Start dictation' icon. At the bottom, there is a 'Dictation language' dropdown menu set to 'English (US)'.

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

ROADMAP

Phase 3 - In progress Refresh

Phases

1. Identify assets and CIA impacts
JSON: Yes | Doc: No
Get active Preview
2. Build architectural model
JSON: No | Doc: Yes
Get active Preview
3. Assess current controls (Implementation) **Current**
JSON: Yes | Doc: No
Next phase Preview
4. Identify relevant threats
JSON: No | Doc: No
5. Estimate likelihood and impact per threat
JSON: No | Doc: No
6. Compute inherent risk
JSON: No | Doc: No
7. Propose compensating controls
JSON: No | Doc: No
8. Create remediation plan
JSON: No | Doc: No
9. Assess residual risk
JSON: No | Doc: No
10. Generate final report
JSON: No | Doc: No

Report

Status: Not ready

Revisions: 0

Missing phase JSON
Phases: 4, 5, 6, 7, 8, 9, 10

RAW DATA (JSON)

```
{
  "controls": [
    {
      "id": "ISO27002-5.15",
      "title": "Access control",
      "status": "Implemented"
    },
    {
      "id": "ISO27002-5.16",
      "title": "Identity management",
      "status": "Implemented"
    },
    {
      "id": "ISO27002-5.17",
      "title": "Authentication information",
      "status": "Implemented"
    },
    {
      "id": "ISO27002-8.2",
      "title": "Privileged access rights",
      "status": "Implemented"
    },
    {
      "id": "ISO27002-8.3",
      "title": "Information access restriction",
      "status": "Implemented"
    },
    {
      "id": "ISO27002-8.4",
      "title": "Access to source code",
      "status": "Implemented"
    },
    {
      "id": "ISO27002-7.10",
      "title": "Storage media",
      "status": "Implemented"
    },
    {
      "id": "ISO27002-5.23",
      "title": "Information security for use of cloud services",
      "status": "Not-Implemented"
    }
  ]
}
```

- 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.

Confirm draft and end phase

Phase requirements: JSON ready.

Export session Import session

Upload files Choose file No file chosen

Refresh uploads

Type your message to Riskonami...

Send Start dictation

Dictation language: English (US)

Threat enumeration

The screenshot displays the Riskonami web application interface. On the left, a 'ROADMAP' section shows a progress bar for 'Phase 4 - In progress' and a grid of 10 task cards. The 'Current' task is '4. Identify relevant threats'. Below the roadmap, a 'Report' section indicates 'Status: Not ready' and 'Missing phase JSON: Phase: 4, 5, 6, 7, 8, 9, 10'. The main content area shows the results of a threat enumeration for '1. ADVERSARIAL THREATS', specifically 'Authentication & authorisation attacks'. It lists three threat events (ADV001, ADV002, ADV003) with their descriptions and why they are relevant to Riskonami. Below this, there are sections for 'Communications & DoS (denial of service)' and 'Misconfiguration & architecture', each listing relevant threat events. At the bottom, there is a 'Phase requirements: JSON missing' section with a text input field containing 'Can we keep Adversarial and remove the other categories?', a 'Send' button, and a 'Start dictation' button. A 'Dictation language' dropdown is set to 'English (US)'.

ROADMAP

Phase 4 - In progress

Phases

1. Identify assets and CIA impacts
JSON file (loaded) - DOT file
Set active Preview

2. Build architectural model
JSON file (loaded) - DOT file
Set active Preview

3. Assess current controls implementation
JSON file (loaded) - DOT file
Set active Preview

4. Identify relevant threats **Current**
JSON file - DOT file
Reset phase Preview

5. Estimate likelihood and impact per threat
JSON file - DOT file

6. Compute inherent risk
JSON file - DOT file

7. Propose compensating controls
JSON file - DOT file

8. Create remediation plan
JSON file - DOT file

9. Assess residual risk
JSON file - DOT file

10. Generate final report
JSON file - DOT file

Report
Status: Not ready
Revisions 0

Missing phase JSON
Phase: 4, 5, 6, 7, 8, 9, 10

1. ADVERSARIAL THREATS

Authentication & authorisation attacks

ID	Threat event	Why relevant to Riskonami
ADV001	Session hijacking	Browser ← Cloud Run over the Internet; OAuth sessions and cookies exist.
ADV002	Unauthorised access to authentication credentials	OAuth tokens and any API keys could be stolen or misused.
ADV003	Exploit vulnerable authorisation mechanisms	Role/tenant checks in the app and API could be weak or flawed.

Communications & DoS (denial of service)

ID	Threat event	Why relevant
ADV004	Unauthorised monitoring/modification of communications	Multiple TLS links; misconfig or weak endpoints could expose data in transit.
ADV005	Conduct a denial of service (DoS) attack	Public-facing app/API is reachable from the internet.

Misconfiguration & architecture

ID	Threat event	Why relevant
ADV008	Exploit misconfigured organisational information systems	GCP services/app configs may be mis-set (IAM, storage, database, etc.).
ADV009	Exploit remote access design/config issues (e.g. VPNs)	Relevant if you expose any VPN/remote admin entry points around GCP.
ADV010	Exploit poorly-designed network architecture	Zones and segmentation between app, DB, storage, OpenAI and

Phase requirements: JSON missing

Export session Import session

Upload files No file chosen

Refresh uploads

Can we keep Adversarial and remove the other categories?

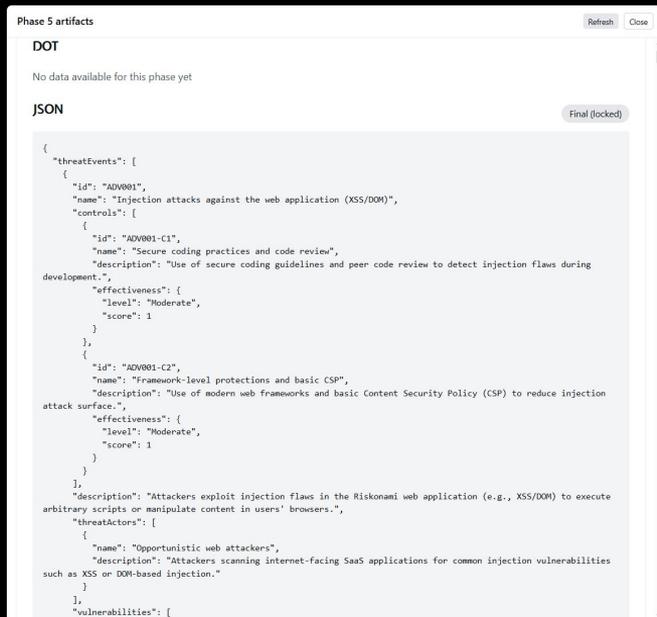
Send

Start dictation

Dictation language English (US)

- 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



The screenshot shows a web interface titled "Phase 5 artifacts" with a "Refresh" and "Close" button. Below the title, it says "DOT" and "No data available for this phase yet". Underneath, there is a "JSON" section with a "Final (locked)" button. The JSON content is as follows:

```
{
  "threatEvents": [
    {
      "id": "ADV001",
      "name": "Injection attacks against the web application (XSS/DOJ)",
      "controls": [
        {
          "id": "ADV001-C1",
          "name": "Secure coding practices and code review",
          "description": "Use of secure coding guidelines and peer code review to detect injection flaws during development.",
          "effectiveness": {
            "level": "Moderate",
            "score": 1
          }
        },
        {
          "id": "ADV001-C2",
          "name": "Framework-level protections and basic CSP",
          "description": "Use of modern web frameworks and basic Content Security Policy (CSP) to reduce injection attack surface.",
          "effectiveness": {
            "level": "Moderate",
            "score": 1
          }
        }
      ],
      "description": "Attackers exploit injection flaws in the Riskonami web application (e.g., XSS/DOJ) to execute arbitrary scripts or manipulate content in users' browsers.",
      "threatactors": [
        {
          "name": "Opportunistic web attackers",
          "description": "Attackers scanning internet-facing SaaS applications for common injection vulnerabilities such as XSS or DOM-based injection."
        }
      ],
      "vulnerabilities": [

```

- 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

```
Phase 6 artifacts Refresh Close
JSON Final (locked)
{
  "threats": [
    {
      "id": "ADV002",
      "name": "Credential stuffing and brute-force attacks",
      "impacts": [
        {
          "impactType": "Confidentiality",
          "calculatedRisk": {
            "riskLevel": "Critical",
            "riskScore": 15
          },
          "impactEstimation": {
            "level": "High",
            "score": 3
          },
          "likelihoodEstimation": {
            "level": "Almost Certain",
            "score": 5
          }
        },
        {
          "impactType": "Availability",
          "calculatedRisk": {
            "riskLevel": "Medium",
            "riskScore": 8
          },
          "impactEstimation": {
            "level": "Medium",
            "score": 2
          },
          "likelihoodEstimation": {
            "level": "Likely",
            "score": 4
          }
        }
      ]
    }
  ]
}
```

- 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



```
Phase 7 artifacts Refresh Close
{
  "name": "Change management for website components",
  "controlId": "IS027002-8.32",
  "description": "Changes to the production website (code, configuration, integrations) are reviewed and approved before deployment, at least informally, to reduce the chance of introducing exploitable weaknesses.",
  "effectiveness": {
    "level": "Low",
    "score": 2
  }
},
{
  "treatmentDecision": "Mitigate",
  "recommendedControls": [
    {
      "name": "Strengthened third-party due diligence and security clauses",
      "description": "Formalize vendor due diligence and expand security clauses in contracts or agreements with hosting and development providers, including specific security controls, breach notification timelines, and right to audit or obtain assurance reports.",
      "exampleProducts": [
        {
          "url": "https://example.com/vendor-security-template",
          "rating": 4.5,
          "vendor": "Internal/Template",
          "productName": "Standardized Vendor Security Requirements Template"
        }
      ],
      "estimatedEffectiveness": {
        "level": "High",
        "score": 4
      }
    },
    {
      "name": "Enforced MFA and least-privilege for third-party access",
      "description": "Require multi-factor authentication and least-privilege access for all third parties who can administer or deploy changes to the website, using role-based access and periodic review of access rights.",
      "exampleProducts": [
        {
          "url": "https://www.okta.com",
          "rating": 4.6,
          "vendor": "Okta",
          "productName": "Okta Identity Cloud"
        }
      ],
      "estimatedEffectiveness": {
        "level": "High",
        "score": 4
      }
    }
  ]
}
```

- 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

```
Phase 8 artifacts Refresh Close
{
  "risks": [
    {
      "id": "risk-1-third-party-breach",
      "description": "If a third-party service or plugin we use on our website is compromised, attackers could access or leak customer data handled through that integration. This risk exists even if our own core systems are not directly breached.",
      "residualRisk": {
        "level": "Low",
        "score": 2
      },
      "existingControls": [
        {
          "name": "Vendor and plugin review",
          "controlId": "ctl-1-vendor-mgmt",
          "description": "CTD reviews and approves key third-party plugins and website integrations, preferring reputable vendors, standard OAuth-based sign-in, and minimizing the amount of customer data shared.",
          "effectiveness": {
            "level": "Moderate",
            "score": 3
          }
        }
      ],
      "treatmentDecision": "Mitigate",
      "recommendedControls": [
        {
          "name": "Formal third-party risk and data-sharing review",
          "description": "Introduce a lightweight, documented review checklist for any new website plugin or third-party integration that could access customer data, covering data types shared, least-privilege configuration, incident commitments, and removal procedures.",
          "exampleProducts": [
            {
              "url": "https://example.com/internal/vendor-checklist",
              "rating": 4.5,
              "vendor": "Internal",
              "productName": "Vendor security and DPIA checklist (internal template)"
            }
          ],
          "estimatedEffectiveness": {
            "level": "High",
            "score": 4
          }
        }
      ],
      "treatmentRecommendation": {
        "action": "Mitigate",

```

- 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.

The screenshot displays the Riskonami web interface. At the top, the header includes the logo 'RISKONAMI', a 'Phase: 9' indicator, the user email 'pieter.daassen@gmail.com', and a 'Sign Out' button. The main content area is divided into two columns. The left column, titled 'ROADMAP', shows a progress bar for 'Phase 9 - In progress' and a grid of 10 task cards. Each card represents a step in the process, such as '1. Identify assets and CIA impacts' and '8. Assess residual risk', with 'Set active' and 'Preview' buttons. The '8. Assess residual risk' card is highlighted with a 'Complete' status. Below the roadmap is a 'Report' section showing 'Status: Not ready' and 'Revisions: 0'. The right column, titled 'THREAT ANALYSIS', contains text explaining the current phase: 'We're now in phase 9: Assess residual risk. I've preloaded the prior-phase JSON, which gives you your in-scope threats, likelihoods, impact ratings, and current risk treatment plan; we'll use that to update the "risktreatment.json" with final residual risk levels. I'll ask one question at a time, and we'll save the JSON only after you review a concise preview and confirm.' It lists three high-risk areas: ADV005 (Data exfiltration or tampering via legitimate access), ADV008 (Inappropriate disclosure of sensitive data to third-party AI services), and ACC001 / ADV002 (Account takeover / credential stuffing). A 'First focused question:' section asks about maintaining the same target residual risk level as the baseline register (Low) after planned controls. A 'Progress:' section notes that prior phases are loaded and high-risk areas are identified, with calibration of target residual risk levels for the highest-impact threats in progress.

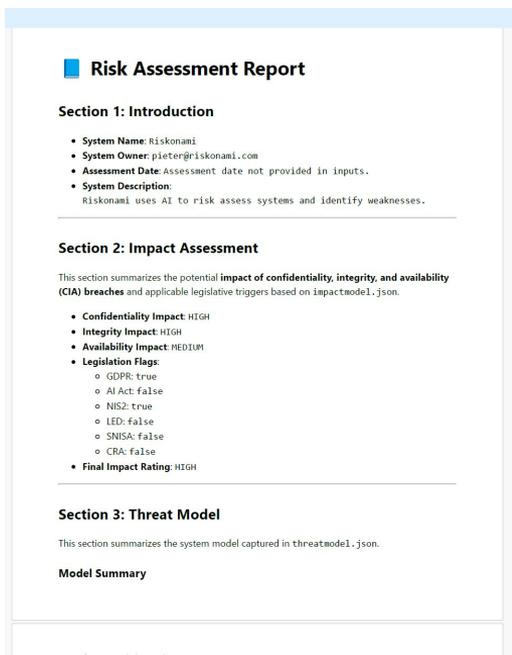
This screenshot shows a section of the Riskonami interface. It features a 'Phase requirements: JSON missing.' notification. Below this are buttons for 'Export session' and 'Import session'. An 'Upload Files' section includes a 'Choose file' button, a 'No file chosen' status, and a 'Refresh uploads' button. To the right, there is a text input field with the placeholder 'Type your message to Riskonami...', a 'Send' button, and a 'Start dictation' button with a microphone icon. A 'Dictation language' dropdown menu is set to 'English (US)'.

Report Generation and Issuance

The screenshot displays the Riskonami report generation interface. On the left is a 'ROADMAP' section with 10 phases, each with 'Set active' and 'Preview' buttons. The main area shows a 'Comment (optional)' field, an 'HTML Preview' section with a list of GDPR and NIS2 compliance items, and a 'Section 3: Threat Model' section. This section includes a summary of the system model, a 'Model Summary' with bullet points for System, Trust Zones, and Flows, and a 'Threat Model Diagram' showing a network of components like 'Internet (public)', 'Google Cloud Run (Internal)', and 'Riskonami app to Cloud SQL'. Below this is 'Section 4: Likelihood Assessment' with a 'Likelihood Table' and a 'Download session JSON' button.

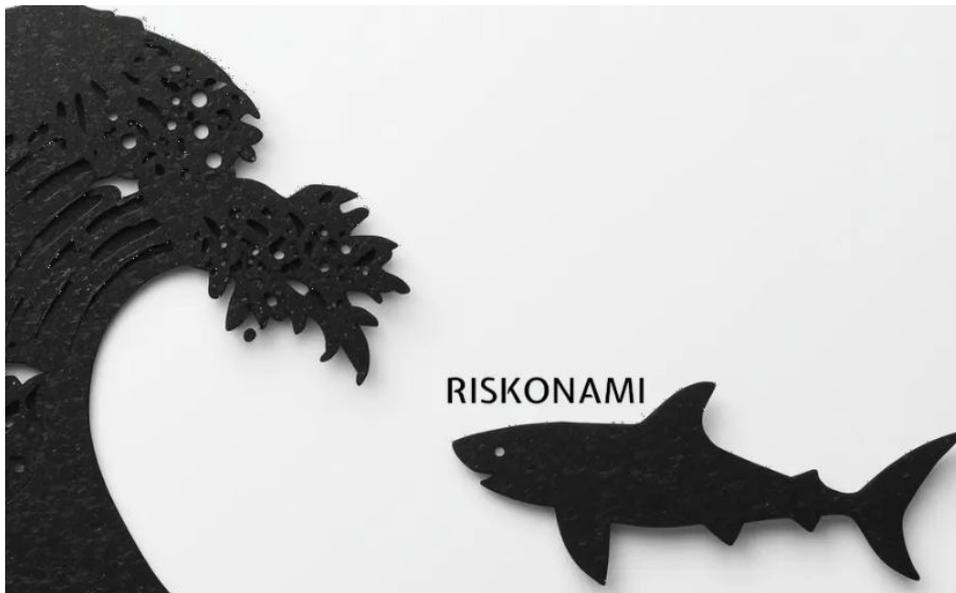
- Riskonami generates a full report that can be previewed in HTML.
- The report is authored in Markdown and includes all diagrams and system models.
- Before issuance, it is fully editable.
- Once issued, the assessment is locked to ensure integrity.
- You may clone the assessment to begin a new cycle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

Final PDF Report



- 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

Riskonami

The giant in AI based Operational Risk Assessment



Welcome to Riskonami

AI powered platform with combination of processes and powerful predictive models.

Riskonami is complete solution to overcome the complexities and its own benefits.

Multi user/multi assessment



Start the assessment



Impact assessment



System analysis



System analysis



Control Identification



Threat enumeration



Threat enumeration



Likelihood Estimation



Inherent Risk Calculation



Risk Treatment and Compensating Controls



Remediation Planning



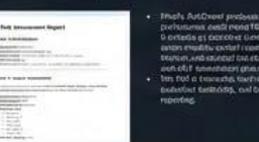
Residual Risk Assessment



Report Generation and Issuance



Final PDF Report



Conclusion



Conclusion

