Risk Assessment Framework

This page explains **how Unicis identifies, assesses, and manages security and service risks** to protect your compliance data and ensure reliable platform availability.

risk-management, iso31000, iso27005, iso20000, iso27001, security

Why We Assess Risks

As a compliance software provider, Unicis faces risks that could impact:

- **Your data security** — Unauthorized access, breaches, data loss
- **Platform availability** — Outages, slow performance, service disruptions
- **Regulatory compliance** — Security incidents, failed audits, regulatory violations
- **Business continuity** — Infrastructure failures, natural disasters, vendor issues

By systematically assessing and managing these risks, we reduce the likelihood of problems and improve our ability to recover quickly if they occur.

Our Risk Management Approach

We use **ISO 31000** (international risk management standard) combined with **ISO 27005** (information security risk) to:

1. Identify Risks

We ask: “What could go wrong?”

Examples:

- A critical system vulnerability is discovered
- A server fails and backups don't work
- A contractor with access leaves and their access isn't revoked
- A deployment bug makes customer data temporarily unavailable
- A ransomware attack encrypts our databases

2. Assess Risks

For each risk, we evaluate:

- **Impact** — How serious would it be? (1 = negligible, 5 = catastrophic data loss)
- **Likelihood** — How often might it happen? (1 = almost never, 5 = multiple times per year)
- **Risk Score** — Impact × Likelihood tells us which risks need attention most urgently

Example:

- Risk: “Unpatched critical vulnerability exploited”
- Impact: 5 (customer data breach)

- Likelihood: 2 (rare, because we patch quickly)
- Score: 10 (medium-high risk)

3. Treat Risks

For each risk, we choose a strategy:

Strategy	Example
—	—
Mitigate	Deploy a Web Application Firewall (WAF) to reduce likelihood of exploitation
Accept	Accept risk of rare data center outage (handled by AWS redundancy)
Transfer	Use AWS disaster recovery (AWS handles infrastructure risks)
Avoid	Don't deploy on Fridays (reduces chance of deployment bugs causing weekend issues)

4. Monitor & Improve

We track:

- **Patch deployment time** — How quickly we fix vulnerabilities
- **Incident response time** — How quickly we detect and respond to security incidents
- **Uptime %** — Platform availability month-over-month
- **Access control violations** — Any unauthorized access attempts

Results are reviewed in monthly leadership meetings and shown on our Scorecard.

Risk Categories We Manage

Risk Category	Examples	How We Address It	Related Document
—	—	—	—
Security Risks	Data breach, malware, unauthorized access, unpatched vulnerability	Encryption, access control, patch management, monitoring	ISO 27001
Availability Risks	Platform outage, slow performance, deployment failures	Infrastructure redundancy, testing, change management	ISO 20000-1
Compliance Risks	Failed audit, regulatory violation, GDPR incident notification	Security controls, incident response, compliance procedures	NIS2, CRA
Operational Risks	Human error, misconfiguration, contractor misuse	Training, access control, audit procedures	Accountability Chart
Vendor Risks	Vendor breach, loss of service, vendor data mishandling	Vendor assessment, contracts, monitoring	Trusted Subprocessors

Risk Governance

Role	Responsibility	Related Document
—	—	—
CEO (Predrag)	Approve risk appetite; allocate budget for risk mitigation; review critical risks quarterly	Accountability Chart
CTO (Peter)	Identify technical risks; implement controls; track patch deployment and incident response	ISO 27001 Implementation

Operations (Alexander)	Identify operational risks; manage access control; support incident response	ISO 20000-1 Implementation
All Employees	Report risks or suspicious activity when discovered	Security Policy

Our Risk Appetite

Critical risks (major impact): → Must be mitigated immediately; escalated to CEO

High risks (significant impact): → Must be mitigated within 30 days

Medium risks: → Mitigated within 90 days as resources allow

Low risks: → Accepted or monitored; no immediate action

How This Protects You

Our systematic risk approach means:

```
 **Threats are identified early** – Before they cause problems
 **Security controls are focused** – On the risks that matter most
 **Incident response is planned** – We know what to do if an incident occurs
 **Compliance is maintained** – We meet GDPR, NIS2, CRA, DORA requirements
 **Continuous improvement** – We get better based on results and lessons learned
 **Transparency** – We report incident response time and uptime to you regularly
via [[pub:company:scorecard|Scorecard]]
```

Regulatory Alignment

Our risk management framework supports compliance with:

- ISO 27001:2022 — Risk assessment per ISO 27005
- ISO 20000-1:2018 — Risk management for service delivery
- NIS2 Directive — Article 21 cybersecurity measures
- CRA Regulation — Risk management and incident response
- GDPR — Article 32 (risk assessment and mitigation)

See Also

- ISO 27001:2022 — Information Security Management System
- ISO 20000-1:2018 — Service Management System
- Information Security Policy — Our security commitment
- Service Strategy — Service commitments and SLAs
- Service Performance Scorecard — Real-time risk monitoring
- Accountability Chart — Risk management roles

Questions?

Questions about how we manage risks?

→ Email us: **security@unicis.tech**

Navigation

← Trust Center | Information Security Policy →

Last reviewed: October 2026 — next review: Q4 2026

risk-management, framework, iso31000, iso27005, security

From:
https://handbook.unicis.tech/ - **Unicis Handbook**

Permanent link:
https://handbook.unicis.tech/pub/trust_center/risk_framework?rev=1784641116

Last update: **21.07.2026 13:38**