Service Strategy & Commitments

This page explains **what we deliver, who we serve, and the commitments we make** as an ISO 20000-1:2018 certified IT service provider.

service-strategy, iso20000, scope, service-delivery

Our Service Value Proposition

Unicis delivers cloud-native GRC (Governance, Risk, Compliance) software to help **EU SMEs navigate complex regulatory frameworks** — NIS2, GDPR, DORA, CRA, ISO 27001.

What we provide:

- Platform for compliance control mapping and management
- Pre-built control libraries for major EU compliance frameworks
- Risk assessment and remediation tracking
- Compliance evidence documentation

What you get:

- Reduce time/cost of compliance program setup (weeks → days)
- Stay compliant with changing regulations
- Demonstrate due diligence to auditors and regulators
- Centralize compliance data in one system

Service Scope (What We Manage)

In Scope (Unicis Responsibility):

- □ SaaS Platform (platform.unicis.tech) — application, APIs, user interfaces
- □ Self-hosted Infrastructure — servers, databases, security monitoring, backups
- □ Deployments & Updates — code review, testing, production releases
- □ Customer Support — technical assistance, onboarding, feature guidance
- □ Security & Incident Response — vulnerability management, incident handling
- □ Uptime & Performance — monitoring, alerting, optimization

Out of Scope (Your Responsibility or Vendor Responsibility):

- □ Your data classification or privacy decisions — that's your choice
- □ Your compliance obligations — we provide tools; you define your scope
- □ Third-party platforms (Mautic, Dolibarr, Nextcloud, etc.) — vendors manage their security
- □ Your internal access control — you decide who in your org uses Unicis

Our Service Commitments

As an ISO 20000-1 provider, Unicis commits to these measurable targets:

Service Level Indicator	Target	How We Track It	Link
Platform Availability	≥ 99% uptime per month	Status Page / Grafana monitoring	Scorecard #6
Critical Incident Response (P1)	≤ 2 hours to respond	Incident response log	Scorecard #11
High Priority Response (P2)	≤ 8 hours to respond	Incident response log	Scorecard
Deployment Success Rate	≥ 99% (no production bugs)	GitHub Actions, incident log	Scorecard #14
Security Patch Deployment	≤ 7 days for critical vulnerabilities	Vulnerability tracking	Scorecard #12
Mean Time to Recovery (MTTR)	≤ 4 hours for critical incidents	Incident recovery log	ISO 20000-1

Real-time performance is visible on our Scorecard.

How We Operate

Our service delivery follows **ITIL best practices** (ISO 20000-1 requirement):

Service Design

We design the platform to be:

- Reliable (redundancy, failover)
- Secure (encryption, access control)
- Scalable (handles growth)
- Maintainable (clear code, documentation)

For details, see ISO 20000-1 Overview.

Service Transition

Before every update:

- Code review (multiple eyes)
- Automated testing (catches bugs)
- Staging environment (test before live)
- Gradual rollout (catch issues early)
- Rollback capability (revert if needed)

Service Delivery

After every deployment:

- Monitoring (uptime, performance, security)
- Support available (for customer questions)
- Incident response (rapid for critical issues)
- Backups and disaster recovery
- Access control (who can do what)

For details, see ISO 27001 Overview (security) and Information Security Policy.

Continuous Improvement

We improve based on:

- Metrics (uptime %, response time, deployment success) — tracked in Scorecard
- Customer feedback
- Incident investigations (what went wrong? how to prevent?)
- Security audits (annual third-party review per ISO 27001)

Service Customers

Primary Target:

- EU SMEs (10–100 employees)
- Operating in regulated industries
- Navigating NIS2, CRA, GDPR, DORA, ISO 27001
- Seeking professional compliance software (not DIY spreadsheets)

Secondary:

- Large enterprises with specific compliance workflows
- EU Project participants
- Consultants/advisors building compliance for clients

Support & Escalation

How to reach us:

Issue Type	Contact	Response Time
—	—	—
Critical Incident (P1)	Support Portal or emergency email	2 hours
Urgent (P2)	Support Portal	8 hours
General Question	Support Portal or Community Discord	24 hours
Sales / Account	sales@unicis.tech	24 hours
Security Question	security@unicis.tech	2 hours

Infrastructure & Service Dependencies

Unicis Platform Hosting:

- **Primary Infrastructure** — Scaleway VPS in Amsterdam (EU only)
- **AI Endpoint & DNS** — OVH (AI processing and domain management)
- Additional EU regions available on request

Self-Hosted Services (On Scaleway):

- Mautic — Email marketing and lead nurture (deprecated soon)
- Dolibarr — ERP/CRM system for accounts and subscriptions
- Nextcloud — Document storage and collaboration

- OpenProject — Project management and budget tracking
- Moodle — Training and learning management
- FreeScout — Support ticket management
- Jitsi — Video conferencing for 15+ participants
- LimeSurvey — Surveys, polls, feedback collection
- Element/Matrix — Internal team communication
- n8n — Workflow automation and integrations
- Matomo — Analytics and usage metrics
- Fider — Feedback and feature roadmap

Code Repository:

- **GitLab EU** — Proprietary code repository and CI/CD pipeline (EU-based)

Third-Party Cloud Services:

- Wise — Payment processing and transfers
- Discord — Community and partner communication

Data Location:

- Primary services hosted in **Amsterdam, EU (Scaleway)**
- All customer data remains in EU jurisdiction
- Compliant with GDPR, NIS2, and CRA data residency requirements
- Code stored in EU-based GitLab

All vendors are assessed for security and reliability. See Trusted Subprocessors for vendor details and contracts. For detailed infrastructure information, see Infrastructure & Tech Stack.

Risk Management

We systematically identify and manage risks to your data and platform availability. See Risk Assessment Framework for details on our approach.

Approved Service Changes

Service commitments can only be changed by CEO approval. Changes are announced via:

- Email to all active customers
- Announcement in Community Discord
- Updated on this page (with date and change details)

Last significant change: **N/A (first version, October 2026)**

Standards & Certifications

- ISO 20000-1:2018 — IT Service Management (certification in progress)
- ISO 27001:2022 — Information Security Management (certification in progress)
- NIS2 Directive — EU cybersecurity requirements
- CRA Scope — EU cyber resilience requirements

- GDPR — EU data protection

Related

- ISO 20000-1:2018 Certification — Service Management System
- ISO 27001:2022 Certification — Information Security Management
- Service Performance Scorecard — Real-time metrics
- Information Security Policy — Security commitment
- Risk Assessment Framework — How we manage risks
- Trusted Subprocessors — Vendor details
- Infrastructure & Tech Stack — Where your data lives
- Accountability Chart — Leadership roles
- Quarterly Planning & Reviews — How we review performance

Questions?

Questions about our service commitments?

→ Email us: **support@unicis.tech**

Navigation

← Trust Center | Scorecard →

Last reviewed: October 2026 — next review: Q4 2026

service-strategy, iso20000, scope, service-delivery, commitments

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

Permanent link:
https://handbook.unicis.tech/pub/company/service_strategy

Last update: **21.07.2026 14:00**