

Accountability Chart

[eos](#), [accountability-chart](#), [organization](#), [leadership](#)

The **Accountability Chart** maps each organizational seat to its responsibilities and who fills it. It's maintained in the Unicis internal system and reviewed quarterly.

[→ View Full Accountability Chart \(Internal\)](#)

SMS & ISMS Role Assignments (October 2026)

As Unicis pursues [ISO 20000-1:2018](#) (Service Management System) and [ISO 27001:2022](#) (Information Security Management System) certification, the following role assignments are effective:

Seat	SMS Role (ISO 20000-1)	ISMS Role (ISO 27001)	Responsibility
CEO (Predrag)	SMS Sponsor / Service Strategy Owner	ISMS Sponsor / Information Security Policy Approval	Oversees both systems; approves policies and budgets; reviews metrics quarterly
CTO (Peter)	Service Delivery Owner, Incident Response Lead	Information Security Implementation, Technical Controls Lead	Technical lead for service reliability and security; manages incidents, vulnerabilities, deployments
Operations (Alexander)	Support Manager, Change Management Owner	Access Control Manager, Incident Escalation Lead	Operational responsibilities for service delivery; manages user provisioning and support escalation
Marketing (Ksenija)	Communications & Stakeholder Updates Lead	Security Awareness & Training Lead	Supports communications around service updates and security awareness training

What These Roles Mean

SMS (Service Management System) Roles

Per [ISO 20000-1:2018](#), the SMS requires:

- **SMS Sponsor** (Predrag) — Owns the SMS as a whole; ensures it delivers value and gets resources
- **Service Delivery Owner** (Peter) — Accountable for incident response, problem management, capacity planning, deployment success
- **Support Manager** (Alexander) — Owns customer support interactions; escalates critical issues; manages response SLAs
- **Communications** (Ksenija) — Communicates service updates and SLA performance to stakeholders

Related Metrics: [Scorecard #6](#), [#11](#), [#12](#), [#14](#) (uptime, incident response, patches, deployments)

ISMS (Information Security Management System) Roles

Per [ISO 27001:2022](#), the ISMS requires:

- **ISMS Sponsor** (Predrag) — Owns information security direction; approves policies; allocates security budget
- **Information Security Implementation** (Peter) — Implements technical security controls; manages vulnerabilities; leads incident investigation
- **Access Control Manager** (Alexander) — Manages user access requests, approvals, and deprovisioning; tracks access control compliance
- **Security Awareness Lead** (Ksenija) — Delivers security training and awareness to team

Related Metrics: [Scorecard #9](#), [#12](#), [#13](#) (security alerts, patch deployment, access provisioning)

How These Roles Support Commitments

Commitment	Owner	How It's Measured
—	—	—
99% Platform Uptime	Peter (Service Delivery)	Scorecard #6 — Real-time uptime %
2-hour P1 Response	Peter + Alexander (Incident Response)	Scorecard #11 — Avg response time
8-hour P2 Response	Alexander (Support Manager)	Scorecard — Avg response time
7-day Patch Deployment	Peter (Security Implementation)	Scorecard #12 — Days to deploy
1-day Access Provisioning	Alexander (Access Control)	Scorecard #13 — Days to provision
99% Deployment Success	Peter (Service Delivery)	Scorecard #14 — Success %

See [Service Performance Scorecard](#) for real-time performance.

Related Documentation

Standards & Certifications:

- [ISO 20000-1:2018 Overview](#) — Service Management System
- [ISO 27001:2022 Overview](#) — Information Security Management System
- [Information Security Policy](#) — Security commitment details
- [Service Strategy & Commitments](#) — Service delivery commitments

Performance & Governance:

- [Scorecard](#) — Real-time role metrics and targets
- [Quarterly Planning & Reviews](#) — How roles review performance
- [Risk Assessment Framework](#) — How roles manage risks

Policies & Procedures:

- [Document Control Procedure](#) — How policies are approved and maintained
 - [IT Security Policy](#) — Detailed security procedures
-

Quarterly Accountability Review

Each quarter (Q1/Q2/Q3/Q4), role owners review:

- Their assigned metrics on [Scorecard](#)
- Performance against [Service Strategy](#) commitments
- Changes needed for [ISO 20000-1](#) or [ISO 27001](#) compliance
- Updates to the [Full Accountability Chart](#) (internal)

Results are discussed in [Quarterly Planning Sessions](#).

[← Trust Center](#) | [Scorecard](#) [→](#)

Last reviewed: October 2026 — next review: Q4 2026 (SMS/ISMS roles added)

[eos](#), [accountability-chart](#), [iso20000](#), [iso27001](#), [organization](#)

From:

<https://handbook.unicis.tech/> - **Unicis Handbook**

Permanent link:

https://handbook.unicis.tech/pub/company/accountability_chart/start?rev=1784641227

Last update: **21.07.2026 13:40**