

The GRC solution for security and compliance

Highly configurable GRC framework — a centralized platform for managing processes, risks, controls and compliance with the NIS2 directive, ISO standards and other regulatory frameworks.

REGULATION

→

RISK

→

CONTROLS

→

PROVABLE COMPLIANCE

Compliance can no longer be proven from spreadsheets

TODAY

- Disconnected Excel records and manually maintained lists
- Evidence scattered across folders and email threads
- Manual tracking of measures, deadlines and document reviews
- Unclear who is responsible for what
- Management has no view of the actual state

WITH GRC-CSUITE

- ✓ Centralized registers of assets, processes, risks and suppliers
- ✓ Documents with versioning and access control
- ✓ Corrective actions with an owner, a deadline and a status
- ✓ Automatic reminders for contracts and mandatory reviews
- ✓ Dashboards and an audit trail as proof of implementation

From disconnected data to a single system for managing compliance, security and risk.

Six modules form one management system

GRC-CSuite system structure

OVERSIGHT LEVEL



SELF-ASSESSMENT

Compliance measurement against ZSIS guidelines, KPI dashboards and decision support

OPERATIONAL LEVEL



ASSETS

A central register of resources with a Service Catalogue and business impact analysis



PROCESSES

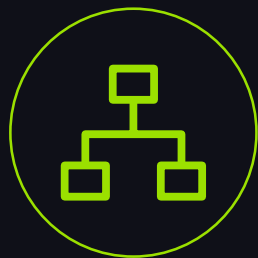
Business and IT processes with responsibilities, workflows and data flows

ANALYTICAL LEVEL



RISKS

The full risk lifecycle: likelihood, impact, exposure, measures and statuses



SUPPLIERS

Supply chain security — a key NIS2 requirement — with SLAs and contracts

INTEGRATION LAYER



DOCUMENTATION

A central repository of policies, reports and compliance evidence, linked to every module

A configurable framework — modules, measure levels, assessment methodologies and permissions adapt to the organization's scope and needs.

GRC-CSuite — platform capabilities

COMPLIANCE

Regulatory Compliance

NIS2 / ZKS Self-Assessment

Controls Management

Regulatory Reporting

RISK

Risk Management

Supplier / Third-Party Risk

CAPA / Corrective Actions

Business Impact Analysis

OPERATIONS

Asset Management

Process Management

Contract & SLA Management

Workflow & Responsibilities

EVIDENCE & OVERSIGHT

Policy & Document Management

Evidence & Audit Trail

Dashboards & KPI

Configuration & Access Control

One platform for managing compliance, risk, suppliers, assets, processes and evidence — from regulatory requirement to management reporting.

Every non-conformity automatically gets a measure, an owner and a deadline

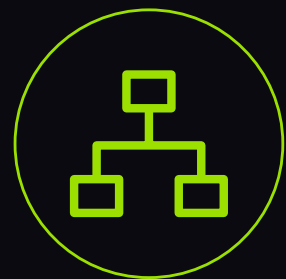


SELF-ASSESSMENT → CAPA



RISK

Identification → Likelihood & impact → Exposure → Measures, deadlines, statuses

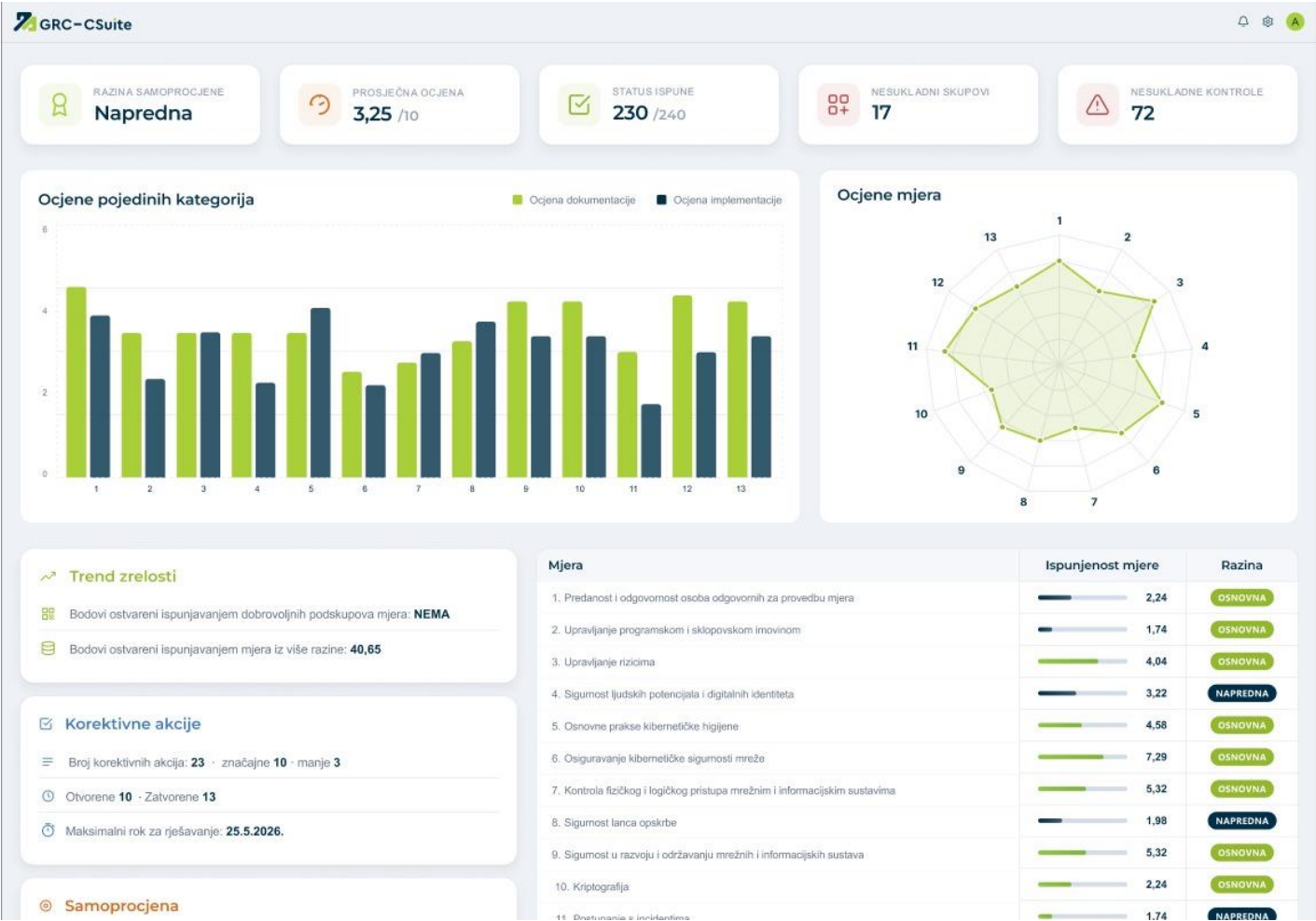


SUPPLIER

Register entry → Services & SLA → Linked risks → Contracts & evidence

From identifying an issue to implementation and proof — in one connected process, with an audit trail.

Management sees results, risks and deadlines on one screen



Self-Assessment — compliance overview

Heat maps — inherent, planned and actual residual risk



Measure status

■ Implemented 22 ■ In progress 26 ■ Risk accepted 30 ■ Not implemented 22

The four canonical register states — share of measures by implementation status (100 total).

Risk management — heat maps and measure status

Are we compliant?

Where are the biggest gaps?

Who owns what, and what is late?

What needs a Board decision?

Why GRC-CSuite



GOVERNANCE AND ACCOUNTABILITY

Defensible oversight and accountability, backed by consistent, audit-ready reporting.



RISK AND COMPLIANCE

Connect risks, controls and evidence to operational decisions, incidents and reporting — not just regulatory checklists.



THIRD-PARTY AND SUPPLY CHAIN RISK

Continuous monitoring of suppliers, evidence and dependencies across the entire value chain.



FRAMEWORK MAPPING ACROSS STANDARDS

Apply the same controls and evidence across NIS2, DORA, ISO 27001 and future regulations — without rebuilding.

An operational GRC system in four steps

01 **ASSESS**

Baseline self-assessment,
gap identification and
regulatory scope

02 **CONFIGURE**

Setting up modules,
registers, roles and
responsibilities

03 **OPERATIONALIZE**

Records, user training and
day-to-day work in the
system

04 **IMPROVE**

Maturity trend tracking,
corrective actions and
continuous compliance

Proposed implementation model — adapts to the organization's scope and maturity.

Technology + cyber security expertise

GRC-CSuite is built by the Cyber Security team

Contact us

grc.cyber-security.hr



VIDEO GUIDE · 1/4

Sign-in, navigation and shared elements

Where compliance meets resilience



VIDEO GUIDE · 2/4

Self-assessment

Assessing cyber resilience according to ZSIS guidelines



VIDEO GUIDE · 3/4

Risk assessment

Identifying, analysing and tracking risks



VIDEO GUIDE · 4/4

Documentation

Versioning, standards and access control

Thank you!

