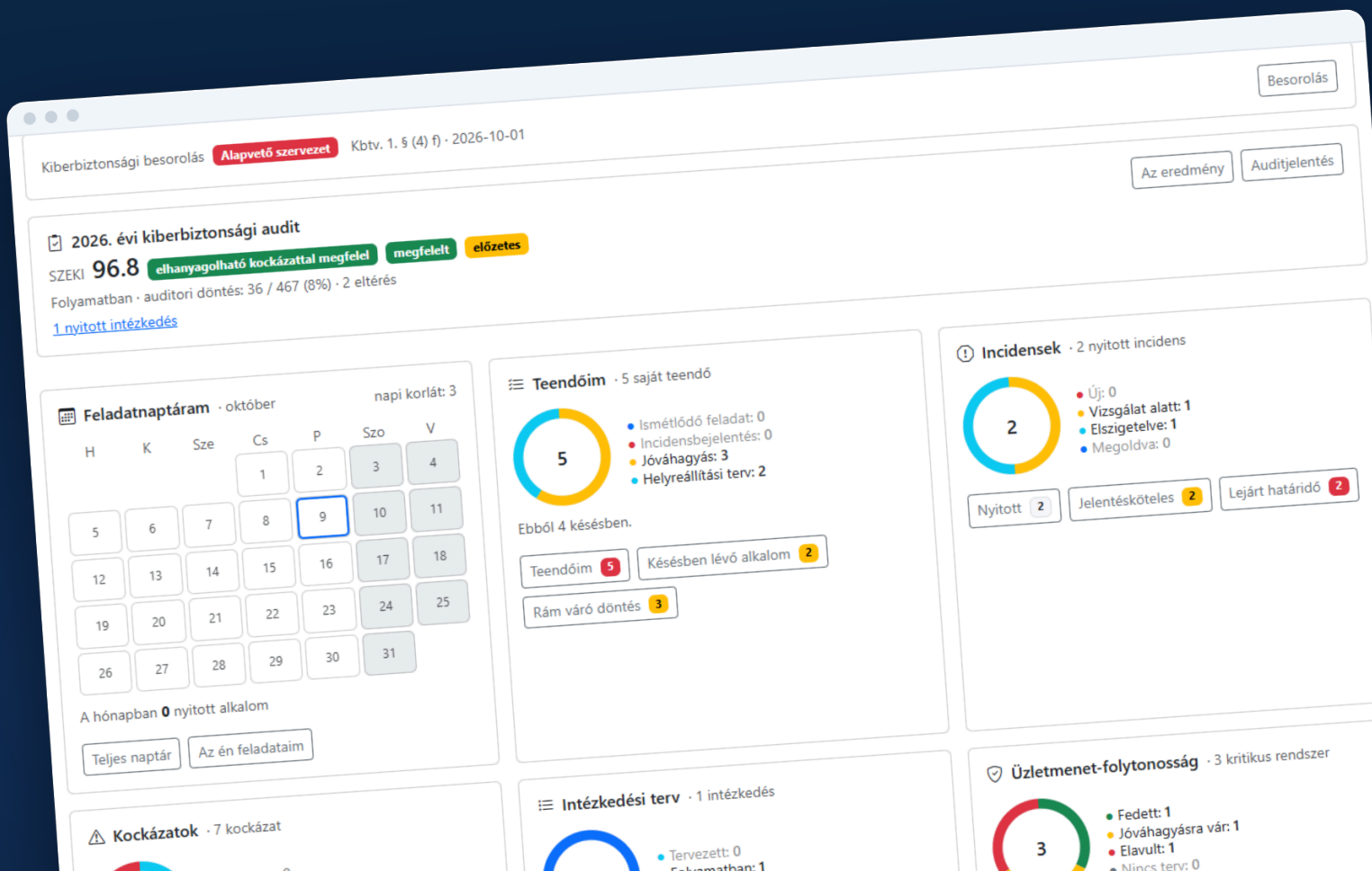
NISNavigator

Product overview
2026

NIS2 compliance that works – and can be proven.

One system for the full compliance cycle of the Hungarian Cybersecurity Act: from scoping through risk management and incident deadlines to the result of the official audit. Every step carries a date, an owner and a traceable audit trail.

Act LXIX of 2024 (Kbtv.) | MK Decree 7/2024 | SZTFH Decree 1/2025 | (EU) 2022/2555 – NIS2



THE CHALLENGE

NIS2 is not a one-off project, but a cycle that repeats every year

Organisations within the scope of the Cybersecurity Act must implement risk-proportionate measures, notify the authority of significant incidents within hours, and every two years an independent audit checks whether all of this actually works in practice. Accountability rests with senior management.

19
chapters in the requirements catalogue the organisation must comply with

24 hours
to send the early warning about a significant incident

2 years
between mandatory cybersecurity audits for essential and important entities

> **An auditor does not ask whether you have a policy, but whether it works: who approved it, when it was reviewed, when it was tested, and what the result was.**

THE NISNAVIGATOR ANSWER

The complete compliance cycle in one system

The modules build on each other, so the system does not just store data – it guides you: risks are tied to known assets, plans to known services. Evidence is not extra work, but a by-product of everyday work.

01
Scoping
Does the Act apply to us – as an essential or an important entity?

02
Inventory
Services, assets, suppliers and certificates in one place.

03
Risk analysis
Assessment, treatment plan, MITRE ATT&CK attack vectors.

04
Policies and approval
Versioned document store, management decisions under the four-eyes principle.

05
Recurring tasks
Reviews, training, backup restore tests – scheduled and reminded by the system.

06
Business continuity
Recovery plans, tests, coverage and KPIs.

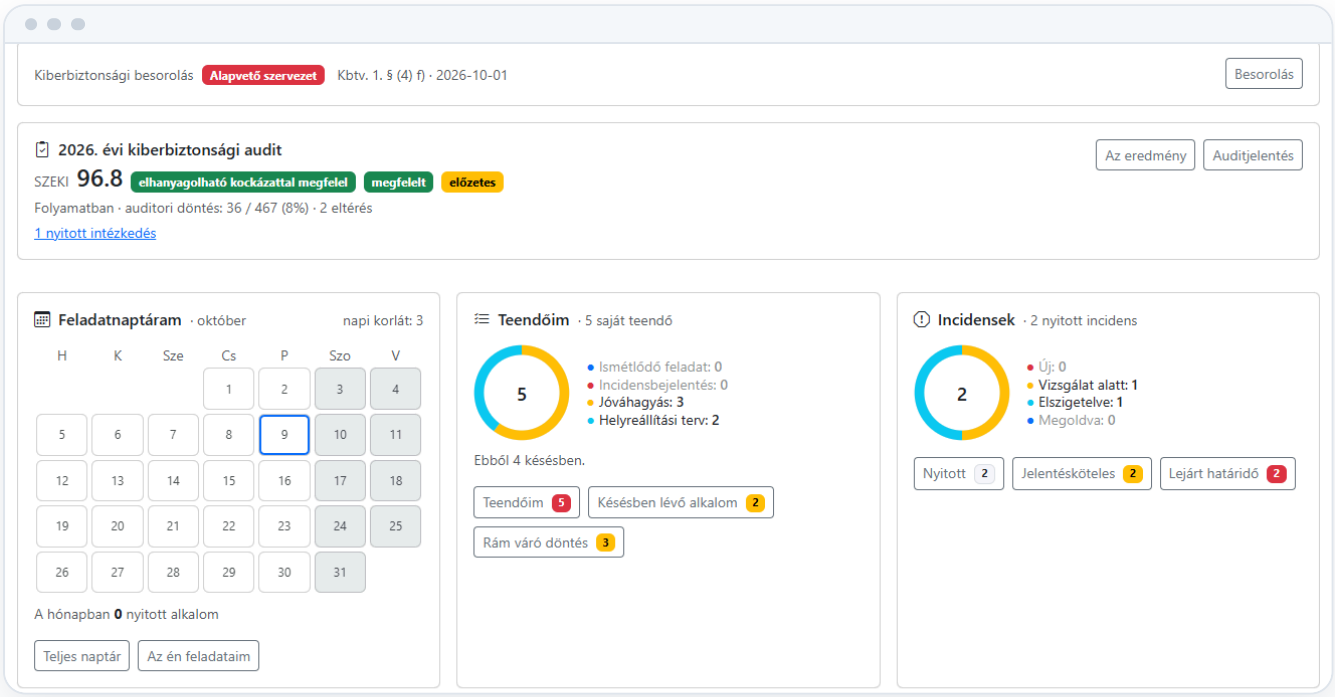
07
Incident handling
24-hour, 72-hour and one-month deadlines in real time.

08
Evidence and audit
Compliance table, audit following the SZTFH methodology, audit report.

OVERVIEW AND DAILY WORK

One screen shows where your organisation stands

The home page gives every module its own card: the chart shows how many items there are of each kind, and the buttons open exactly the filtered list a number comes from. Overdue deadlines, outdated plans, decisions awaiting approval – nothing stays hidden.

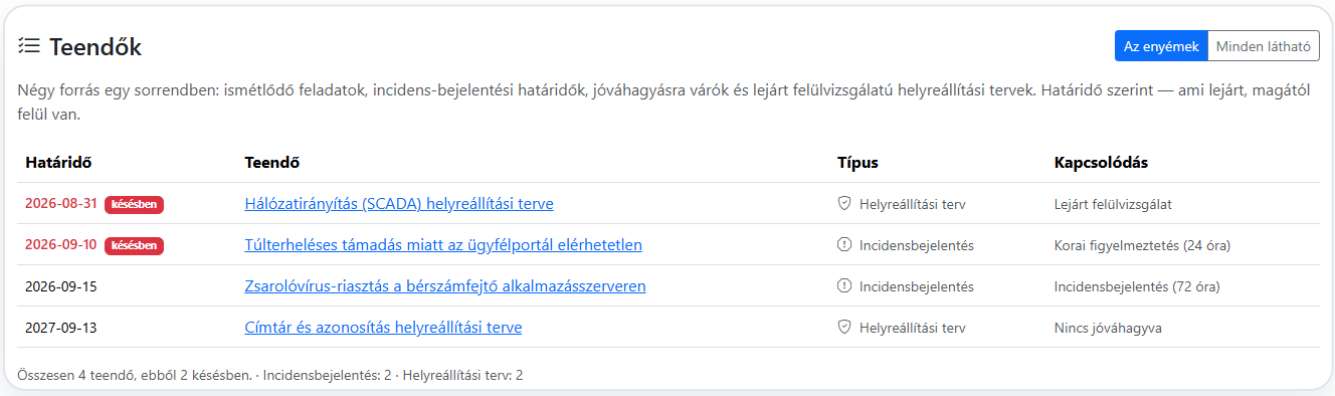


The overview page: scoping result, current audit index, task calendar, to-dos and incidents at a glance – followed by cards for risks, action plan, continuity, certificates, assets and suppliers.

To-dos: a single list, ordered by deadline

Recurring tasks, incident notification deadlines, decisions awaiting approval and plans due for review are merged into one list. Anything overdue automatically moves to the top.

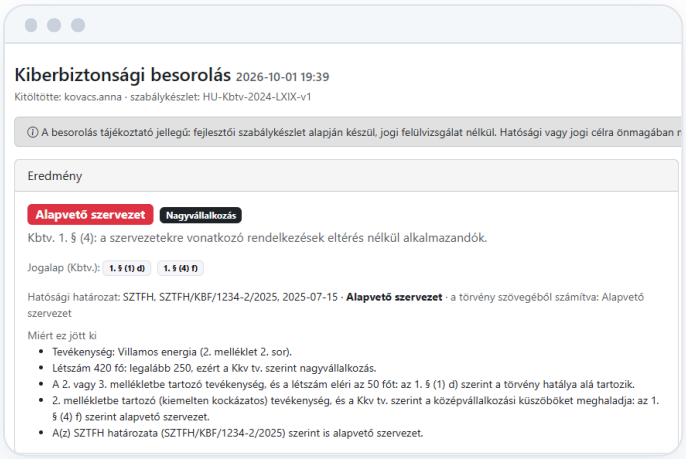
- Daily e-mail digest of your own to-dos
- Everyone sees their own area of responsibility



SCOPING AND COMPLIANCE

Find out in minutes what the law expects of you

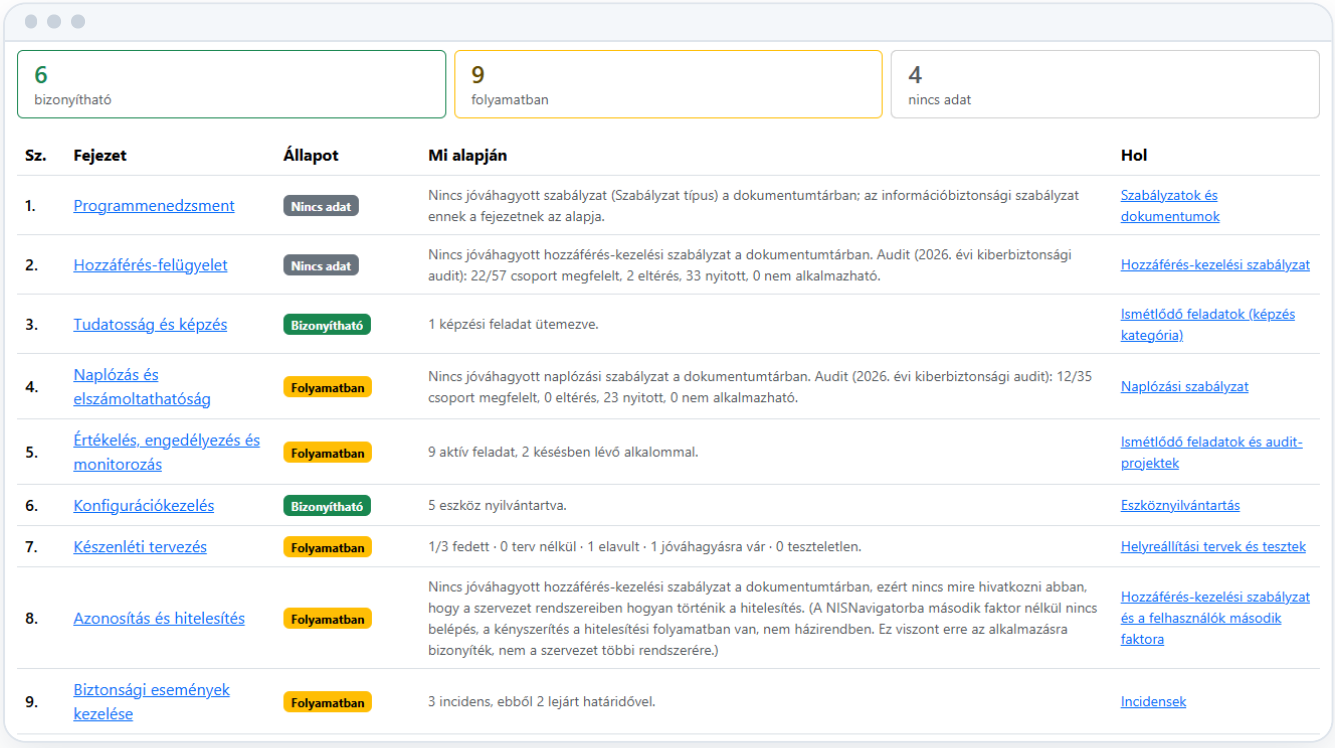
A four-step questionnaire with fixed statutory thresholds determines whether the organisation falls under the Cybersecurity Act and, if so, whether as an essential or an important entity and under which provision. Alongside the result, the system explains why it came out that way and what it means in practice.



- **Reasoned result** – based on activity, headcount and turnover, with references to the legal provisions
- **Concrete obligations** – registration, audit and supervisory fee, with deadlines
- **PDF report** for management and for your documentation
- **System-level security classification** – based on 16 criteria, with management approval

Compliance table: the first thing an auditor asks for

It compares all 19 chapters of the requirements catalogue in MK Decree 7/2024 with your records and tells you, chapter by chapter, whether there is something to show – **Provable** **In progress** **No data** – and exactly on what basis. The foundation of the monthly management report.



RISK MANAGEMENT

From risk to management decision, in a single chain

Under the Act, every measure must be proportionate to risk. NISNavigator keeps the chain together: what could happen, how serious it is, what we do about it, what remains afterwards, and who approved it.



A risk record: inherent and residual score, treatment strategy, owner, deadline and the full approval trail.

Risk matrix

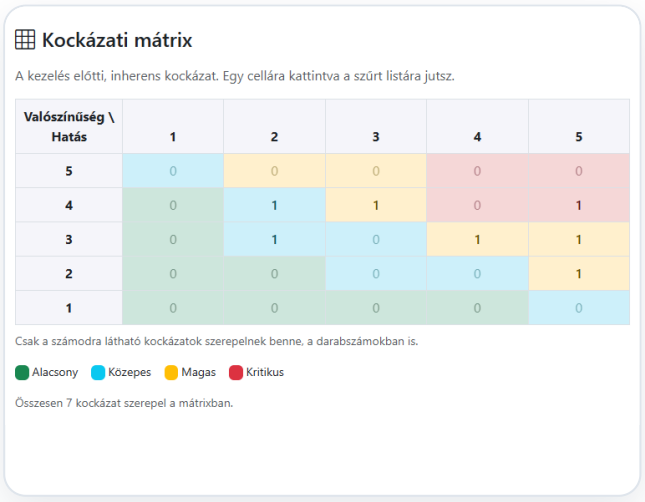
Inherent and residual views; click a cell to open the filtered list.

MITRE ATT&CK attack vectors

Asset-level threat analysis based on the international technique catalogue – the technical foundation of risk assessment.

Four-eyes approval

Risks, policy versions and recovery plans all go through the same approval workflow; nobody can approve their own submission.



INCIDENT HANDLING

When it matters, every hour counts

For significant incidents, the law measures compliance in hours. NISNavigator counts the deadlines from the moment of awareness, sends e-mail reminders, and records verifiably what happened, when, and on whose decision.

24 hours
Early warning

72 hours
Incident notification

1 month
Final report



The incident record with countdowns, reference numbers, status tracking and a chronological timeline.

BUSINESS CONTINUITY

The plan is the intent, the test is the evidence

Recovery plans with RTO and RPO targets, documented recovery tests, and a view that records nothing but shows the gaps: which critical service has no valid plan behind it.

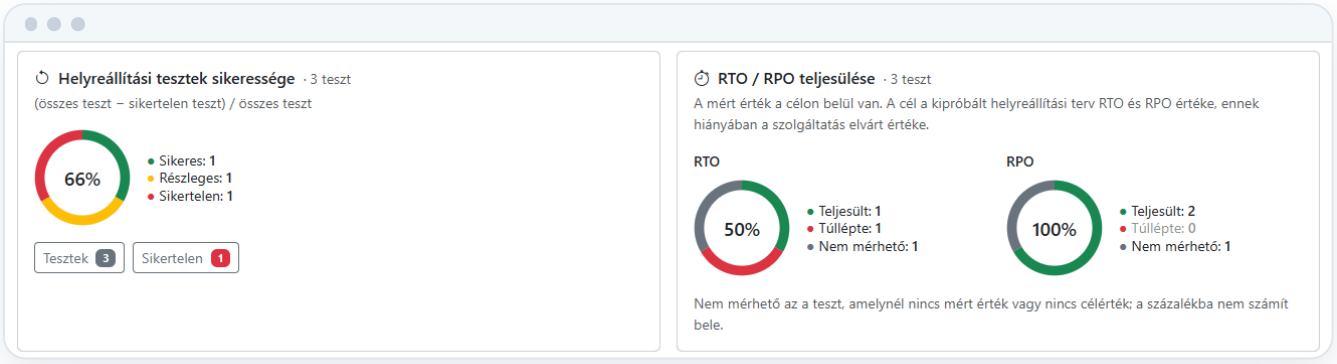


The coverage view: problem rows always first, overdue reviews and RTO gaps in red. The system also derives KPIs from the test results – see the next page.

MEASURABLE CONTINUITY

Two numbers that show whether recovery works

Twenty test records will not tell you whether the organisation is doing better or worse than a year ago. The KPI page answers this with two indicators over a selectable period (3, 6, 12 months or all time), always with the same formula – so the trend is readable too.



The KPI page: the number of tests always appears next to the percentage, and the underlying tests are one click away.

KPI 1

Recovery test success rate

```
(all tests − failed) / all tests
```

Every restore test and DR exercise counts. A partial result is not a failure: the organisation was able to recover – whether fast enough is measured by the second indicator.

KPI 2

RTO and RPO achievement

```
measured value ≤ target → achieved
```

Calculated separately because they point to different problems: an exceeded RTO means a slow process, an exceeded RPO means infrequent backups. Targets come from the approved plan or the service's expected values; unmeasurable tests are shown but do not distort the percentage.

Proven starting targets

≥ 90%
Success rate
With 8–12 tests a year, one failure is acceptable; a second one triggers an investigation.

≥ 80%
RTO achievement
Recovery time depends on many factors; persistent overruns signal an unrealistic target.

100%
RPO achievement
Backup frequency is a configuration matter – no tolerance here.

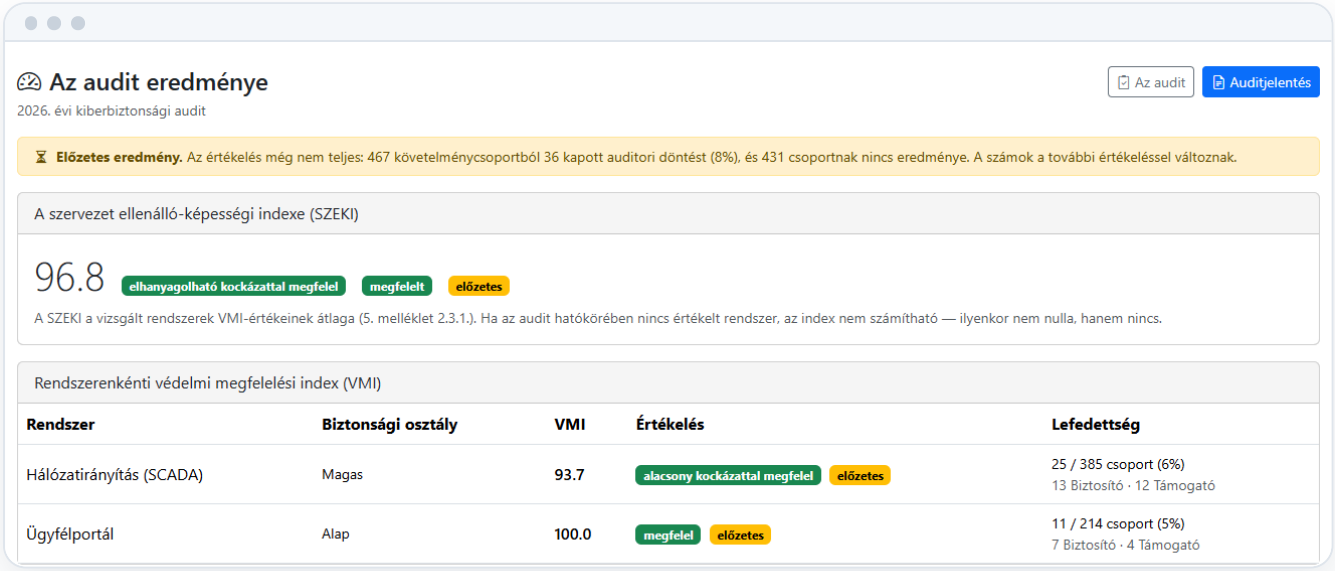
Recommended quarterly KPI review

1. **Schedule** – As a recurring task, after the restore tests.
2. **Compare** – 12-month view against the previous quarter.
3. **Root cause** – Off target: read the lessons of the tests behind it.
4. **Act** – Fix the plan, set a realistic target, back up more often.
5. **Report** – To management, attached as evidence.

CYBERSECURITY AUDIT

Audit-ready – following the SZTFH methodology

The audit project links the classified systems to the requirements catalogue and guides you through each requirement group: does it apply, is it met, and if not, how serious is the gap. The organisation's self-assessment and the auditor's findings run in two separate lanes and never overwrite each other.



Automatically calculated protection compliance index (VMI) per system and organisational resilience index (SZEKI).

Audit preparation

Organisational questionnaire and fee calculation from data already recorded – ready for requesting quotes.

Deviations

Every deliberate deviation in writing, justified and approved by management – in a register you can hand over.

Action plan

From gap to fix: owner, deadline, milestones and evidenced closure.

And more to support everyday work

Recurring tasks and calendar

A rule written once becomes scheduled occurrences, reminders and retained evidence.

Versioned document store

Encrypted storage, each version with its own approval; you always know what was in force.

Suppliers and supply chain

Who we depend on, what they committed to, when we last assessed them – with document requests.

Certificates

Multi-stage e-mail warnings before expiry – no more unexpected outages.

Storage media destruction

Media tracked from removal to destruction confirmed with photos.

Requirements catalogue

The complete statutory catalogue, searchable and filterable – even outside an audit.

BUILT-IN SECURITY

Your most sensitive data in safe hands

The system holds your organisation's security map – so it was built to meet the catalogue's requirements itself.

Mandatory two-factor login
Password plus authenticator app, with recovery codes.

Need-to-know visibility
Everyone sees only their own records and those assigned to them – enforced at database level.

Sealed audit log
Every action numbered in sequence; the integrity check reveals any direct tampering.

Encryption and protected login
Encrypted confidential fields and files, IP blocking against password guessing, encrypted migration package.

FAST ROLLOUT

Working compliance in 90 days

A proven sequence for an organisation of 300–500 people – the user manual guides you step by step.

Weeks 1–2	**Foundations** – users, e-mail, first login
Weeks 2–4	**Scoping** and services with RTO/RPO
Weeks 3–6	**Assets** – recorded by the asset owners
Weeks 5–9	**Risks** and attack vectors
Weeks 7–11	**Policies** approved
Weeks 9–13	**Rhythm and continuity** – tasks, plans, first test
Week 13	**Management review** with PDF report

A role for everyone

Administrator
Admin

Users, settings, licence, audit log and assignments.

Compliance manager
ComplianceManager

Scopes, manages risks, documents and plans, approves, classifies incidents.

Asset owner
AssetOwner

Records their own systems, schedules and completes tasks.

Auditor
Auditor

Sees everything, changes nothing – only for the duration of the audit.

Try it risk-free

NISNavigator runs with full functionality even without a licence – enough to pilot it in a smaller organisation or a single department. The licence only lifts the quantity limits; every feature is available from day one.

5	5	5
assets	services	users

The screenshots show the application's Hungarian user interface with a fictitious organisation (Zöldmező Energia Zrt.); all names and data are invented. Scoping results are indicative and do not replace legal review. The incident module does not submit notifications to the authority, but it tracks and documents the deadlines.