



UNIVERSITY OF TARTU

Implementation of ISO 27001 at the University of Tartu

Becoming the first ISO/IEC 27001:2022 certified university in Estonia

Elin Nurges, Information Security Adviser, University of Tartu

NORDUnet Conference 2026

Elin Nurges

Role

Information Security Adviser at the University of Tartu. Implementation of ISO management systems and internal audits: ISO/IEC 27001, ISO/IEC 27005, ISO 31000, ISO 9001, ISO 22301. Implementation of the Estonian information security standard and external audits.

Background

MBA in Management of Information Technology

Certification and membership

- ISO/IEC 27001 Senior Lead Auditor
- ISO/IEC 27005 Senior Lead Risk Manager
- ISACA Estonia, Information Systems Audit and Control Association
- Estonian Data Protection Association

How certification is offered today



UNIVERSITY OF TARTU

What the offers promise

Speed

Certification is described in weeks rather than months. In the template model, the customer is expected to adapt and complete the supplied documents in one to five business days.

Price

A documentation kit with policies, records and a pre-filled Statement of Applicability costs 1000-5000 euros, not 10 000- 100 000 euros

Automation

Compliance platforms collect evidence from cloud services automatically, run control tests continuously and keep the Statement of Applicability current without manual work.

What the tools give, and what they cannot

What the tools give

- A complete document baseline in days, with the structure of the standard made visible
- A checklist of the 93 Annex A controls that nobody has to reconstruct from the text
- Automated evidence collection and reminders, which lowers the cost of staying certified
- Continuous testing of technical controls where the environment is cloud-based and uniform
- A realistic route for small organisations that could not afford a consultant

What they cannot give

- A template describes a generic organisation. The scope, the risks and the owners still have to be ours
- A risk assessment cannot be pre-filled. Someone has to accept residual risk in their own name
- Evidence of operation takes calendar time: an audit cycle, a management review, records of use
- Every additional document is one more thing to keep current for three years
- The tools assume one organisation with one way of working. A university has many

The Organisation

What exactly were we certifying?



UNIVERSITY OF TARTU

The University of Tartu

Founded in 1632. Estonia's national university and its largest research institution.

Four faculties and 32 institutes, together with colleges, museums, the library, the Estonian Biobank and an observatory.

About 15 000 + students, 1,400 of them international from 90 countries. About 4,700 employees, a fifth of them international, 58 percent academic staff.

Tartu, Tallinn, Pärnu, Narva and Viljandi: more than 70 buildings in five cities.

A central IT department and three specialised IT units: the high performance computing centre, the Estonian Biobank and the library.

Every one of these units has its own history of how information is handled.

The IT landscape, in round numbers

70+

buildings in five cities

100+

information systems and
applications

30,000+

user accounts

10,000+

helpdesk requests a year

Why certify at all

Research partnerships. An increasing number of international projects make information security conformity a precondition for participation.

Legal requirements. Estonian cybersecurity regulation recognises a valid ISO/IEC 27001 certificate, which changes what the university has to demonstrate and to whom.

Research and study data. Protecting it is a long-term objective in its own right, not a by-product of compliance.

Credibility. A certificate is a short answer to a question partners were already asking in long form.

The trigger. The Cybersecurity Act has applied to universities since August 2022. The earlier Estonian standard ISKE, from 2007, was only indicative for universities. Its successor E-ITS came into force in 2024, with ISO/IEC 27001 accepted as an alternative. We chose the international standard, and we chose to certify.

A university is not the organisation the standard imagines

The standard assumes	A university has
A single management hierarchy	Distributed governance: faculties, institutes and colleges with real autonomy
Information that defaults to closed	Open research, open data and publication as a core mission
Employees who follow process	Academic freedom, and researchers who choose their own tools
A known, managed system landscape	Decades of departmental systems, grant-funded infrastructure and instruments
Stable staff	Students, visiting researchers, doctoral candidates and project staff arriving and leaving constantly

Building the ISMS

Scope, risk, controls and the people who had to care



UNIVERSITY OF TARTU

Defining the scope

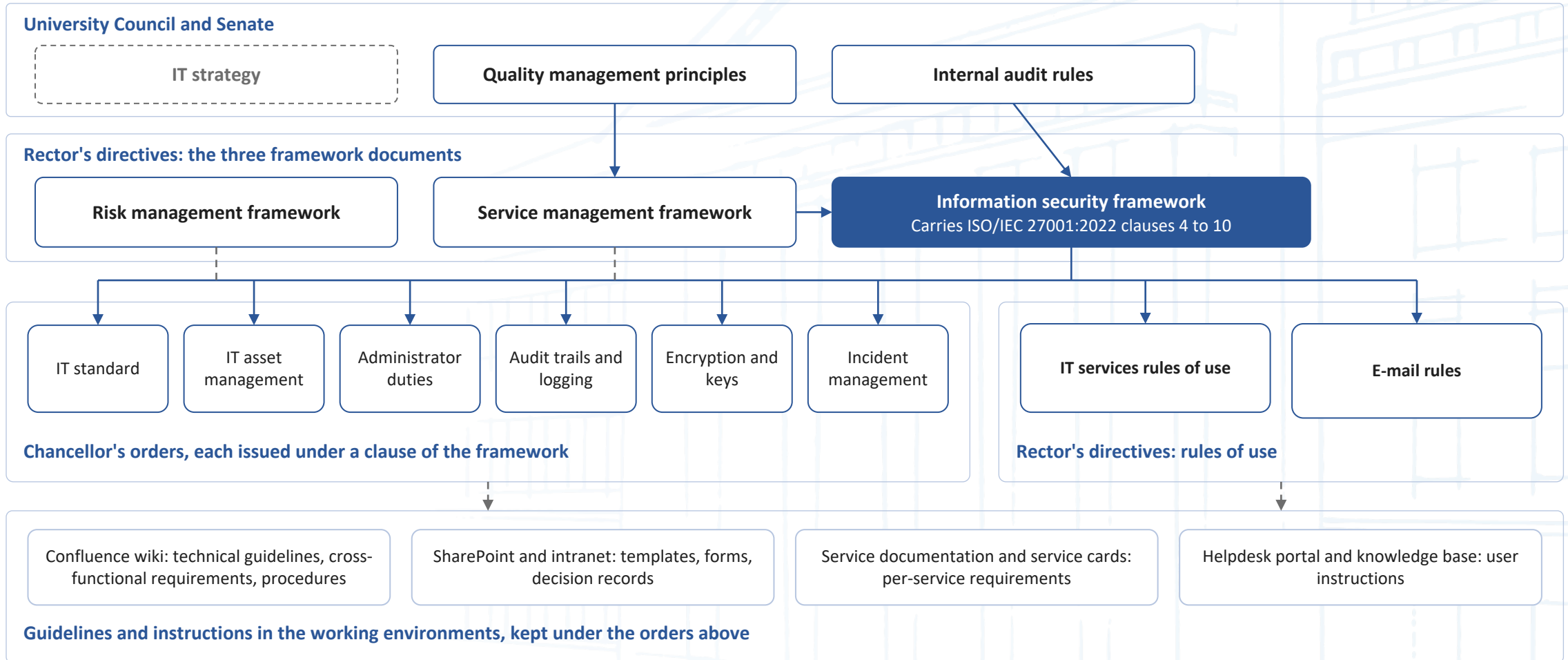
Scope is the first decision and the one that shapes every later step. In a decentralised university it is also the hardest.

The certified scope: the information security management system covers the university's teaching, research and development activities, as well as the supporting administrative activities, in accordance with the information security principles and the related legislation and guidelines.

Not applied to the independent research work of doctoral students that is not carried out using the university's resources. Where the university provides no system, no data and no infrastructure, it cannot own the controls.

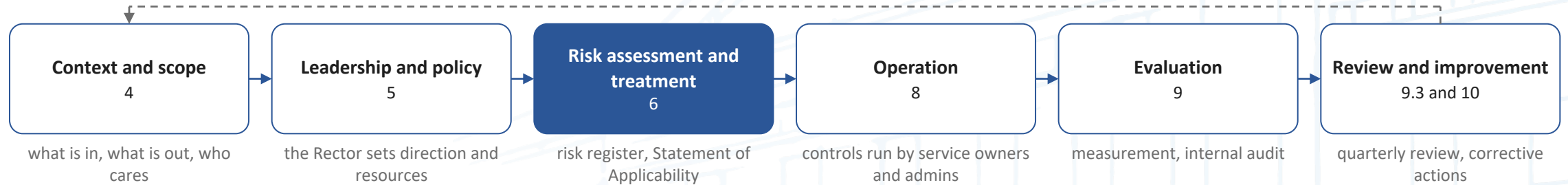
The certification audits were run in two stages: the scientific computing centre in spring 2025, the remaining structural units in autumn and winter 2025.

The regulatory framework, in one picture



What the standard requires, and how it links

Management system core, clauses 4 to 10 of the standard

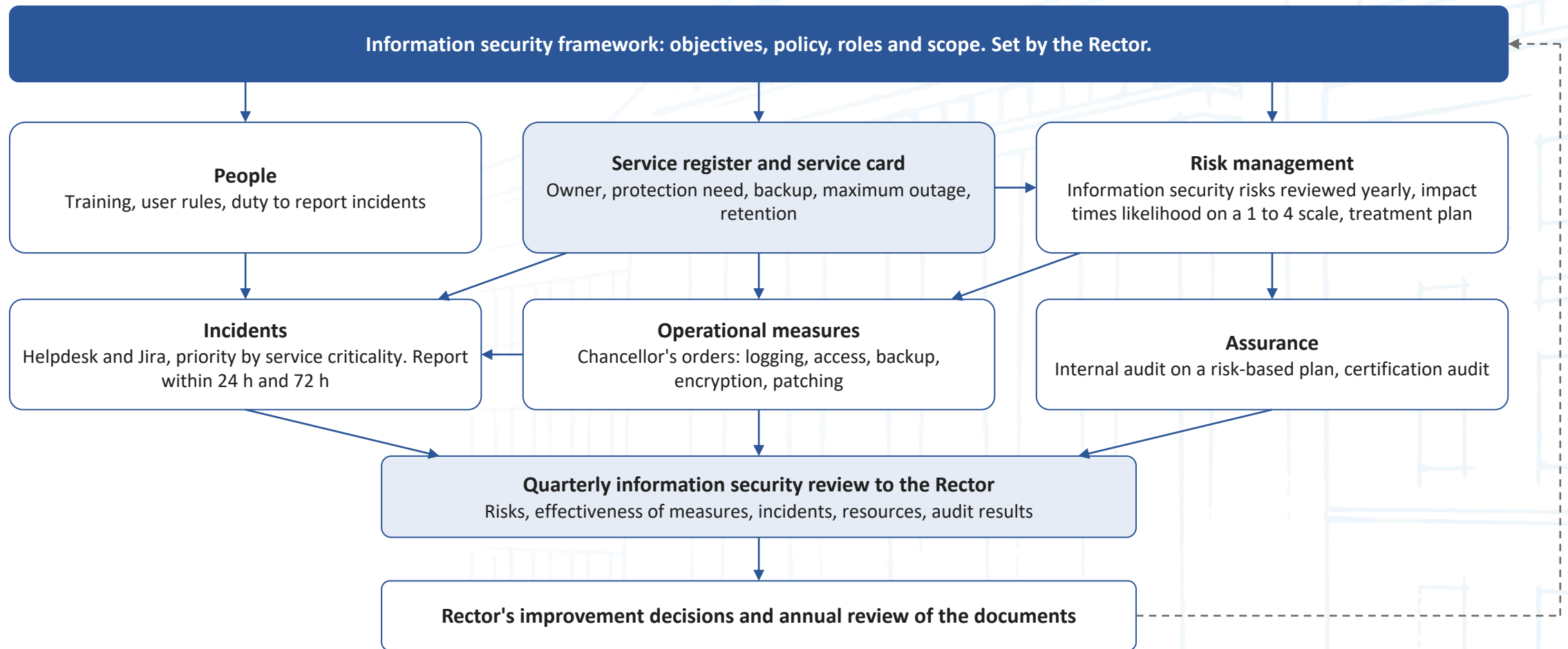


Support, clause 7: resources, competence, awareness, communication, documented information

Operational processes, Annex A



How the pieces depend on each other



Getting faculties and support units to engage

An ISMS that lives only in the IT department is an ISMS that fails its first surveillance audit. Three groups have to carry it, each with a different job.

Top management

Funds the work and makes recorded decisions at the management review. At Tartu: the Rector decides, the Chancellor approves the quarterly review.

Process and service owners

Operate the controls every day. Their routine is what produces the evidence: service cards, access reviews, backup tests, incident records.

Internal audit

Independent it audits.

How much documentation is actually required?

Documented information required by ISO/IEC 27001:2022

Scope of the ISMS (4.3)	Operational planning and control (8.1)
Information security policy (5.2)	Results of risk assessment (8.2)
Risk assessment process (6.1.2)	Results of risk treatment (8.3)
Risk treatment process (6.1.3)	Monitoring and measurement results (9.1)
Statement of Applicability (6.1.3 d)	Internal audit programme and results (9.2)
Information security objectives (6.2)	Results of management review (9.3)
Evidence of competence (7.2)	Nonconformities and corrective actions (10.2)

Roughly fifteen items. Our own internal framework runs to sixteen acts, most of them short. The toolkits offer more than a hundred templates. Every extra document is one more thing somebody has to keep up to date every year..

Where the evidence actually lives

Main projects in ISMS management

68,000+ tickets

Helpdesk: incidents, changes, access requests, orders

Risk register: 3,100+ risks with owners and treatment

Information security team plan: the yearly objectives

ISO 27001 implementation: findings and corrective actions

Identity and access management: the development project

Central logging: sources, retention, alerts

Incident reports: what happened, why, what changed

Helpdesk team plan: procedures of the first line

Jira Assets: five main object schemes

36,000+ objects

CMDB: devices, servers, network, people, services, contracts	30,000+
--	---------

Personal data processing register	4,700+
-----------------------------------	--------

Risk background data: threats, vulnerabilities, consequences	700+
--	------

Service catalogue: support and outsourced services	280+
--	------

ISO 27001 controls: ISMS+ all 93 Annex A controls as objects	116
--	-----

Where the standard meets academic life



UNIVERSITY OF TARTU

Distributed governance and a single management system

The standard expects top management to direct the ISMS. A university expects faculties to govern themselves.

In practice this means the ISMS has to work through existing governance with some modifications.

- ISMS management
- Risk management
- Service management
- Crisis management
- IT service management
- Incident management
- Asset management
-

Certification and after

The audits, the calendar, and what continues



UNIVERSITY OF TARTU

The certification audit

Certification body: BM Certification Estonia OU, an independent accredited body.

Spring 2025: audits at the university's scientific computing centre.

Autumn and winter 2025: audits across the remaining structural units.

January 2026: certificate issued. The first Estonian university to hold ISO/IEC 27001:2022.

"The university implements an information security management system in accordance with the information security principles and the related legislation and guidelines (jointly referred to as the documents of the information security management system). The system covers the university's teaching, research and development activities, as well as the supporting administrative activities. The information security management system is not applied to the independent research work of doctoral students that is not carried out using the university's resources."

What it actually took

One to five business days, or a couple of weeks, was the promise from the vendors.

Three years was the reality, from start to the certificate.

The certificate is not the finish line

The certificate is valid for three years, with surveillance audits in years one and two and recertification in year three. Between audits the system has to keep running: risk reviews, internal audits, management reviews, corrective actions verified as effective.

What we are working on now

- Closing the minor observations from the audit. An auditor always finds something.
- Joiners, movers and leavers. A multi-year access management project to remove internal and external rights on time and to manage groups centrally, including the case where a leaver stays on as a student.
- Engaging IT specialists across the university, not only the central department, in security awareness and in the work itself.
- Keeping the reviews going: services and service cards, the personal data processing register, the existing risks and the risk method itself.
- A stronger presence in the rectorate, so that information security is discussed where decisions are made.
- A training concept that is specific to the university rather than generic.

What are my recommendations

1 Do it once, and properly

Allow two to three years if you can. That means starting now, not in three years 😊 .

2 Spend the first year on the foundations

Describe the services, identify the partners, run a first risk assessment. The IT-specific processes can be planned from there, because by then you know what you have.

3 Build incident and change management early

If they need to be created or improved, do it at the start. It takes time to mature, and auditors read history, not designs.

4 Do not send people spreadsheets

One lead with one assistant runs the interviews, enters the data in a structured form and keeps the quality up from the first interview to the last.



ut.ee



elin.nurges@ut.ee



linkedin.com/in/elin-nurges

Thank you

Elin Nurges

Information Security Adviser, University of Tartu