Governance of information security in the HE-sector in Norway

Agnethe Sidselrud and Rolf Sture Normann

UNIT – The Norwegian Directorate for ICT and Joint Services for Higher Education and Research

Governance and Service Delivery

- The organization will help to **realize** the currently applicable **sectoral objectives** for research and higher education.
- The organization is responsible for **national coordination** and has overall management responsibility in the ICT field.
- The organization will implement and **follow up** the strategies and **guidelines set by the Ministry** of Education and Research and follow up **initiatives from the higher education sector** and other relevant actors, e.g. research institute and healthcare sectors.
- The organization will ensure **portfolio management** for the coordination and follow-up of **national development projects** and joint services.

Governance and Service Delivery

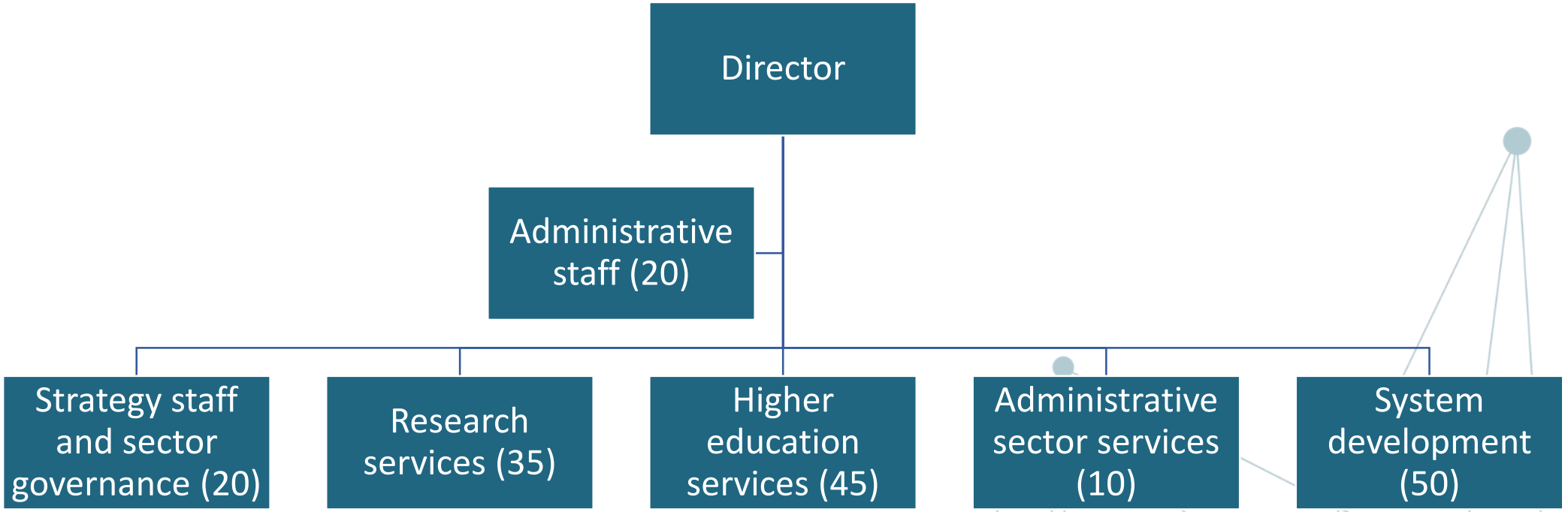
- The organization will **develop and manage a common ICT architecture** for the harmonization and standardization of processes, data and technical interfaces in the higher education sector, and contribute to coordination with other relevant actors

- The organization will **provide shared services** to ensure both the management and execution of education and research, and provide common research information for research in all the research intensive sectors.

Key figures

- 200 staff
- 2 locations
- 45 services
- 220 institutions
- 3 sectors
- €50 mill budget

UNIT – Organizational structure



Education

Samordna opptak

NVB
Nasjonal vitnemålsdatabase

Vitnemålsportalen
diploma registry

GAUS
Godkjenning av utenlandske studier

RUST
Register for utestengte studenter

Research

CRISTIN
Current Research Information System in Norway

OJS
Open Journal Systems

oria.no

Administration and BI

FILESENDER

Datavarehus

In-house development

URKUND

TimeEdit

canvas

inspera

mediasite

TechSmith Relay

WISEflow

OPENedX

Leganto

Kaltura
open source video

ExLibris
Alma

doi

amesto

tableau

Public 360

SAP

box

basware

UNIT4

Jobbnorge

Frameworks & procurement

Microsoft Azure

safespring

amazon web services

Strategy for digitalization of HE-sector

The strategy states the need for **coordinated leadership of information security and privacy** on the institutional and on the national level as a condition for succeeding in obtaining the sector goals for the high quality in education and research.

Need for better information security and data protection

- Information Security Management System (ISO27001) on the institutional level
- Implementation of the GDPR in the HE-sector during 2017
- Need for better information security and data protection and need for strengthening the governance
- ISO27014:2013 adjusted for the sector level

New national governance model – gains for the HEIs

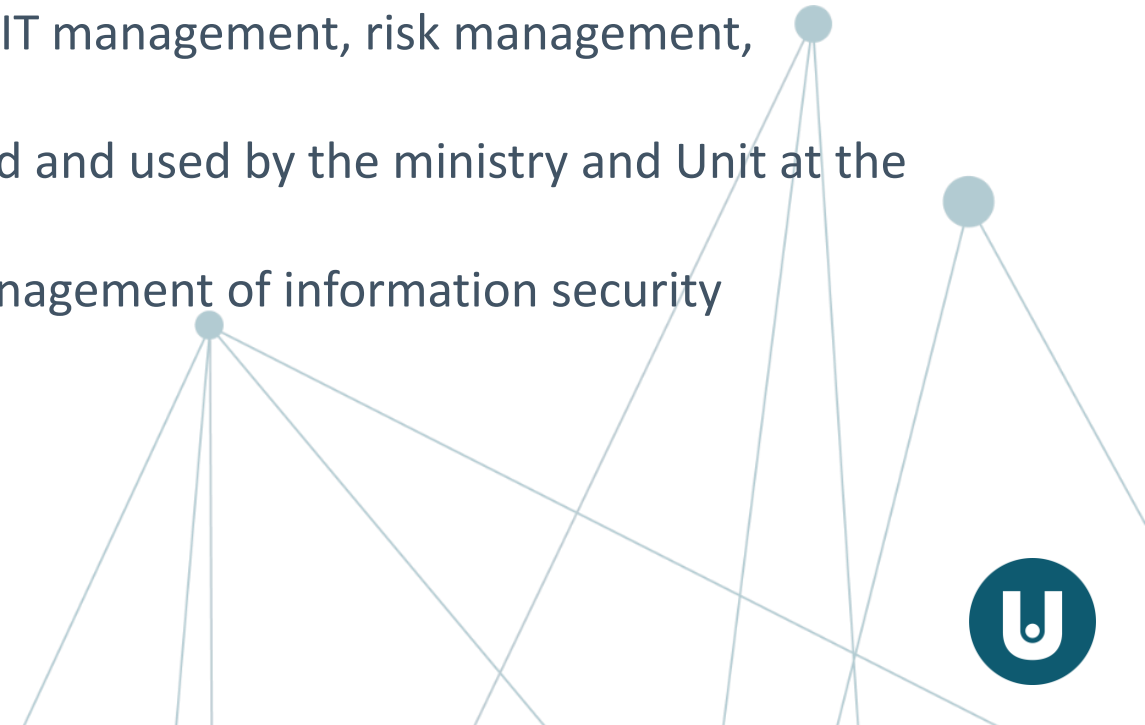
- **More clear direction** for HEIs work with information security in their systems and services through a sub-strategy for information security and privacy.
- **Planned implementation** of the sub-strategy through an action-plan.
- **Closer dialogue and follow-up** between the HEIs and the Ministry.
- **Better and more accurate priorities** made by the Ministry.
- **Customized advice and guidance** for the HE-sector.

Governance framework

Based on ISO/IEC 27014:2013

The framework

- Based on ISO/IEC 27014:2013 – Governance of information security
  - Concepts with goals and targets for governing information security and privacy
  - 6 principles
  - 5 processes
  - Compatible with other governance frameworks (IT management, risk management, financial management etc.)
  - Designed for the business level, but now adjusted and used by the ministry and Unit at the sector level
  - Represents the level over the ISO/IEC 27001, management of information security



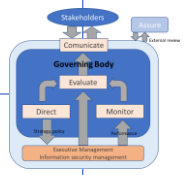
Ministry of HE needs to know the overall status + risk

DET KONGELEGE
KUNNSKAPSDEPARTEMENT

The ministry:
- Direction and demands
- State overview/risk
- Evaluate the state and make corrective actions
- Comunicate

UNIT

Responsible for governance activities in the HE-sector



Local management of information security
ISO 27001

Institusjon n...

Universities and university collages

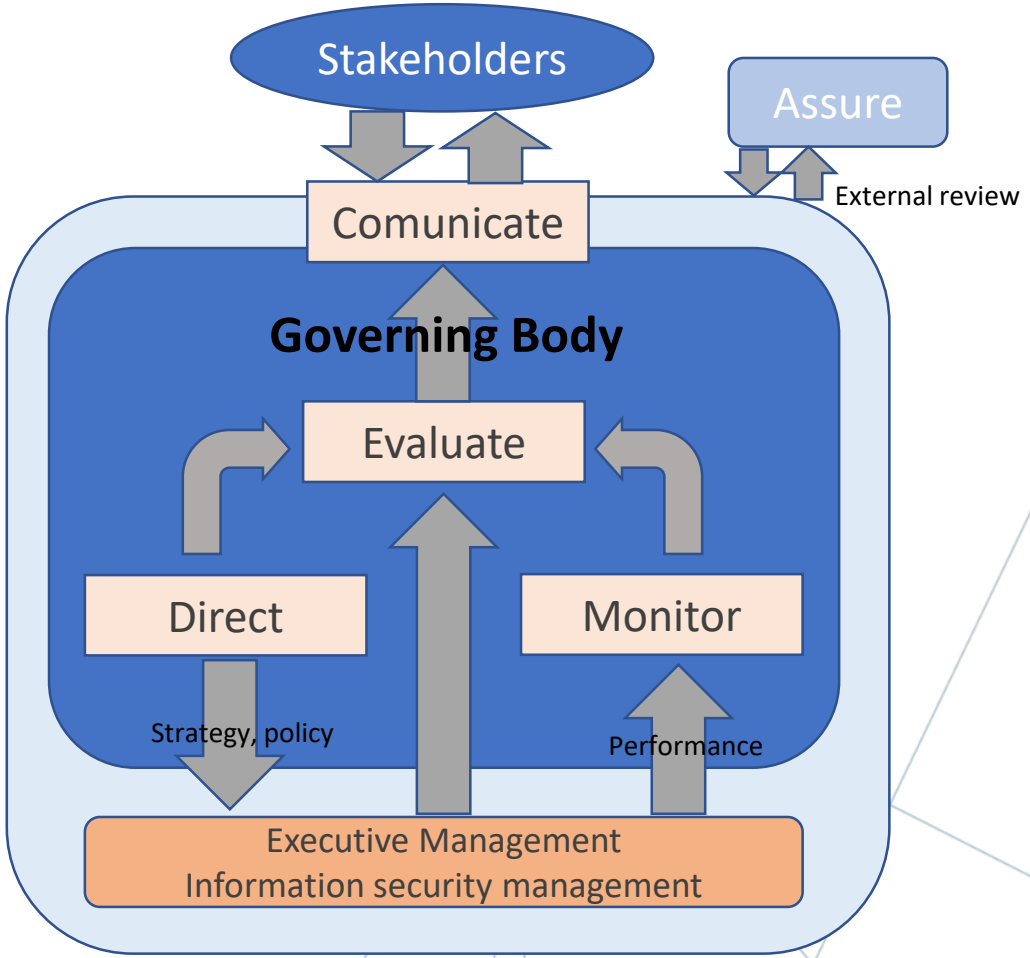
Eget lokalt arbeid på informasjonssikkerhet og personvern

Virksomhet n...

Other organisation under the Ministry

Governance framework (ISO27014:2013)

What are the responsibilities of the Ministry vs Unit's in this model?



Monitor

This process gives an overview of the status and enables the governing body to assess the achievement of strategic objectives.

- **The Ministry:**
  - Evaluate Unit's reports
  - Evaluate information from other actors (ministries, etc.)
  - Do own assessments based on other open threat reports

- **Unit:**
  - Systematically read and evaluate national risk- and threat reports
  - Review the institutions and organisations governed/owned by the Ministry
  - Evaluate information about incidents, threat and vulnerabilities from Uninett CERT
  - Yearly risk and condition report
  - Report to the Ministry if any major changes in the threat landscape

Evaluate

This process considers the current and forecast achievement of security objectives based on current processes and planned changes, and determines where any adjustments are required.

- **The Ministry:**
  - Ensure that the Ministry's plans and initiativ supports information security and privacy concerns
  - Respond to the results of the monitor process (report from Unit)
  - Prioritize and establish effective initiatives

- **Unit:**
  - Ensure that information security and privacy supports the sector goals (digitization strategy)
  - Evaluate how the sector complies with national regulations and requirements from authorities
  - Suggest new effective initiatives/projects to the Ministry

Direct

By this process the governing body gives direction about information security objectives and strategy that need to be implemented.

- **The Ministry:**
  - Approve strategy and policy
  - Assess need
  - Give governing directions

- **Unit:**
  - Develop and implement strategy and policy
  - On behalf of the ministry have a leading role of the implementation
  - Promote a positive security culture
  - Investigate more when needed

Communicate

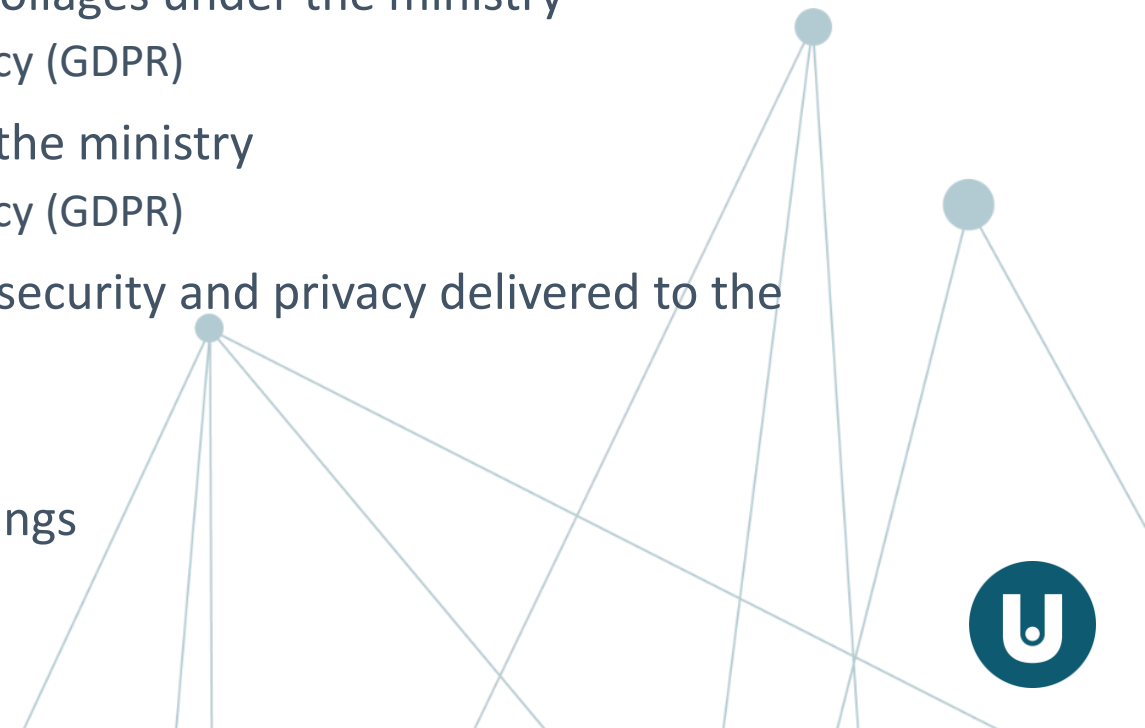
By this process the governing body and stakeholders exchange information about information security

- **The Ministry:**
  - Report to external stakeholders
  - Evaluate results from external reviews
  - Be sure to know all the regulation and requirements from the stakeholders

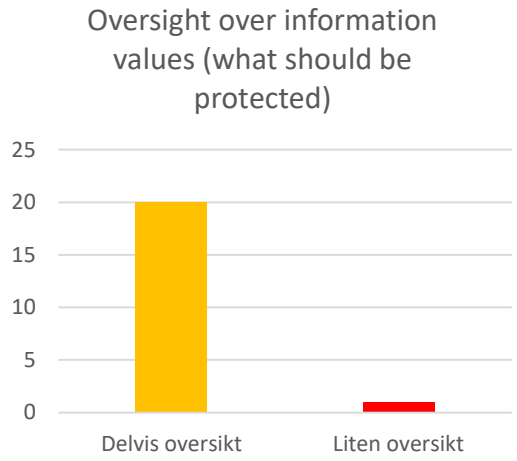
- **Unit:**
  - Provide an open report
  - Evaluate external reviews
  - Best practice documents and guidance
  - Be advisor for the Ministry
  - Ad-hoc reports when needed

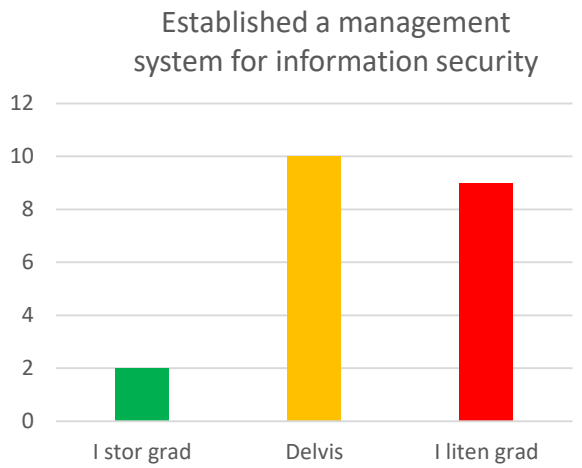
Implementation in 2019

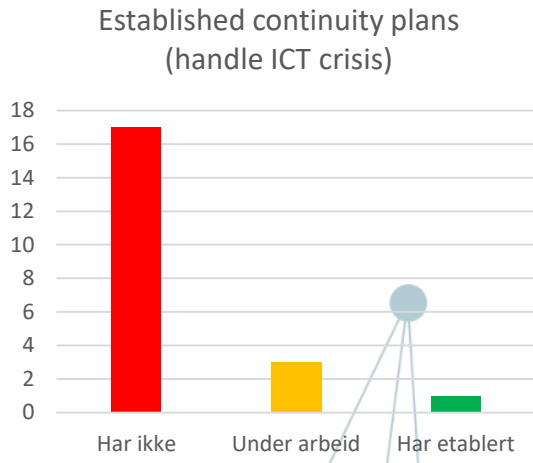
- Unit and the ministry adjust the standard to fit the HE-sector
- A letter to the institutions from our Minister of Education
- Developed a procedure for the processes «monitor» and «evaluate»
- Survey interview with 21 universities and university collages under the ministry
  - 24 questions regarding information security and privacy (GDPR)
- Survey interview with the other organisations under the ministry
  - 13 questions regarding information security and privacy (GDPR)
- Risk and condition report of the state of information security and privacy delivered to the Ministry
- Open Risk and condition report
- Develop a strategy and action plan based on the findings
- Develop a sector-wide information security policy

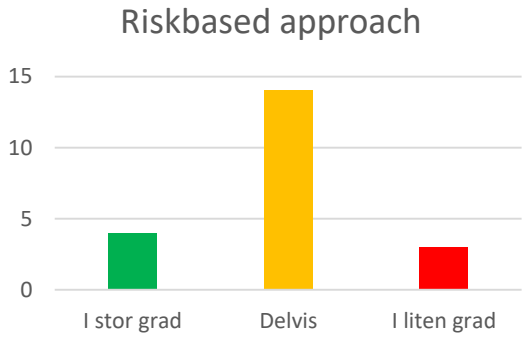


Some findings…









www.unit.no