DANMARKS STATISTIK

Information security Statistics Denmark

Sanne Nielsen
August 26th 2022

Who am I?

DANMARKS STATISTIK

ESS It Security Framework

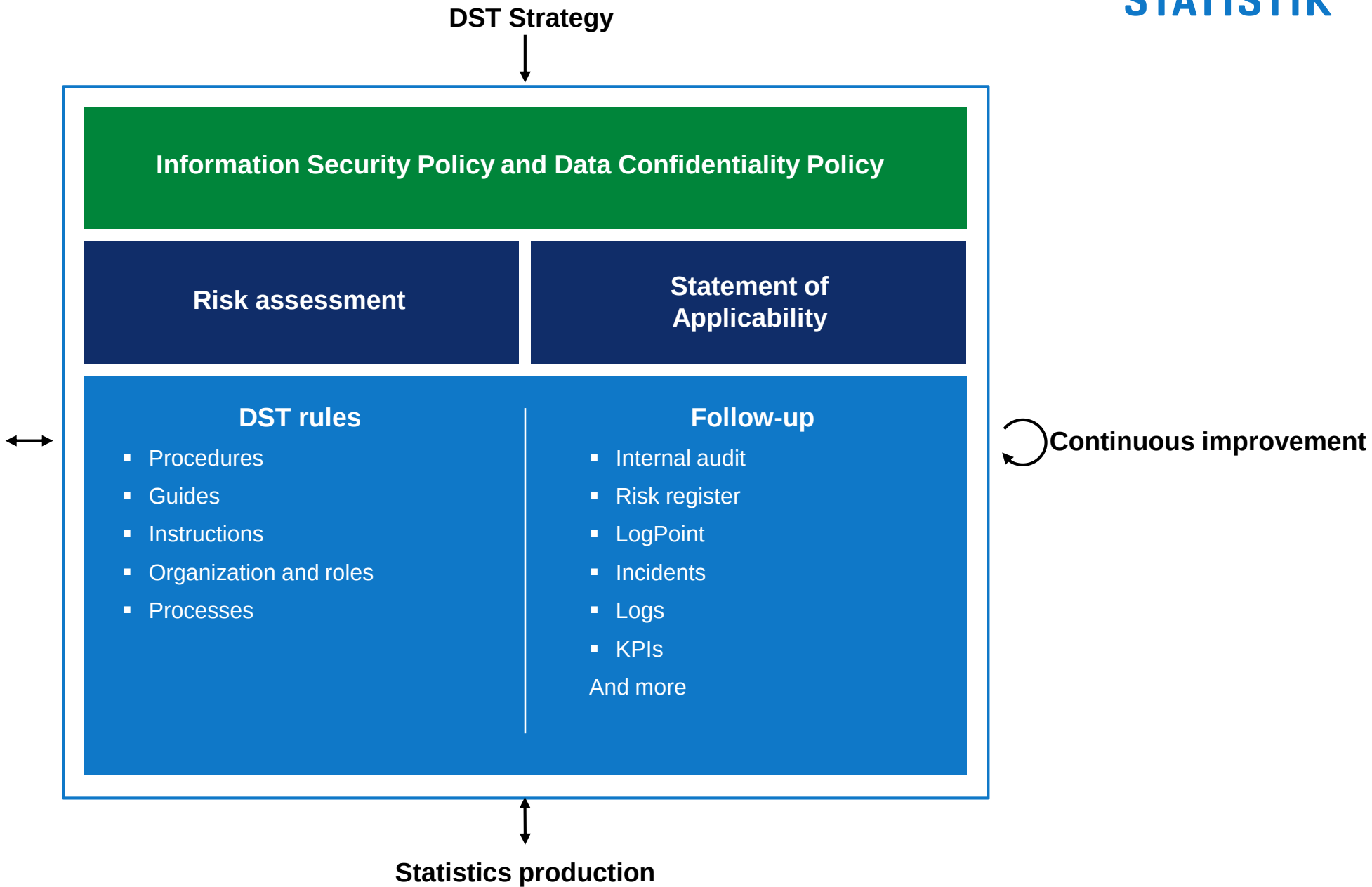
Information Security Management System: Stakeholders and documents

DANMARKS STATISTIK

External conditions and stakeholders that may influence ISMS

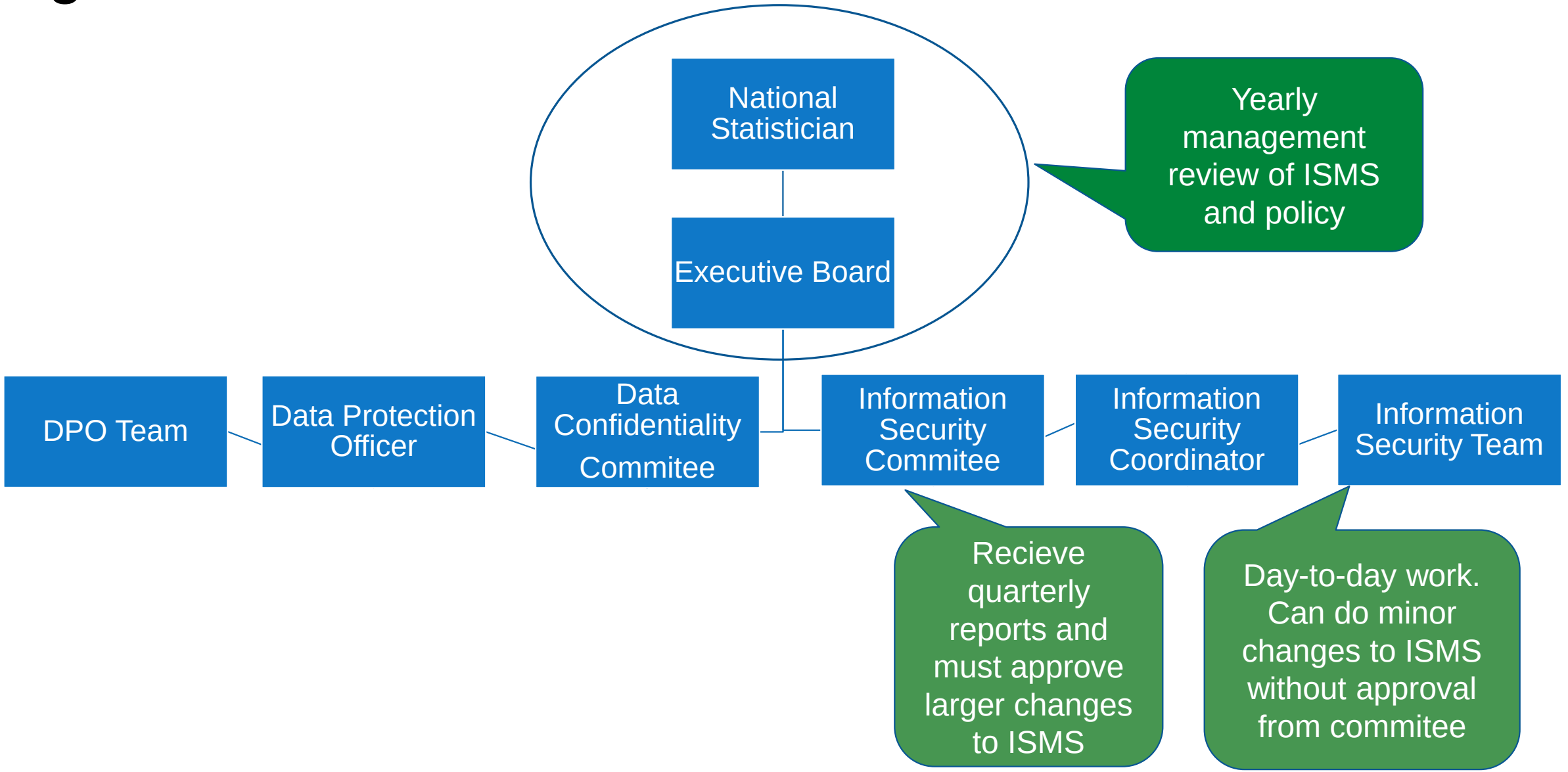
- ISO27001:2013.
- The Ministry's overall information security policy
- Center for Cyber Security
- Eurostat
- GDPR

And many more…



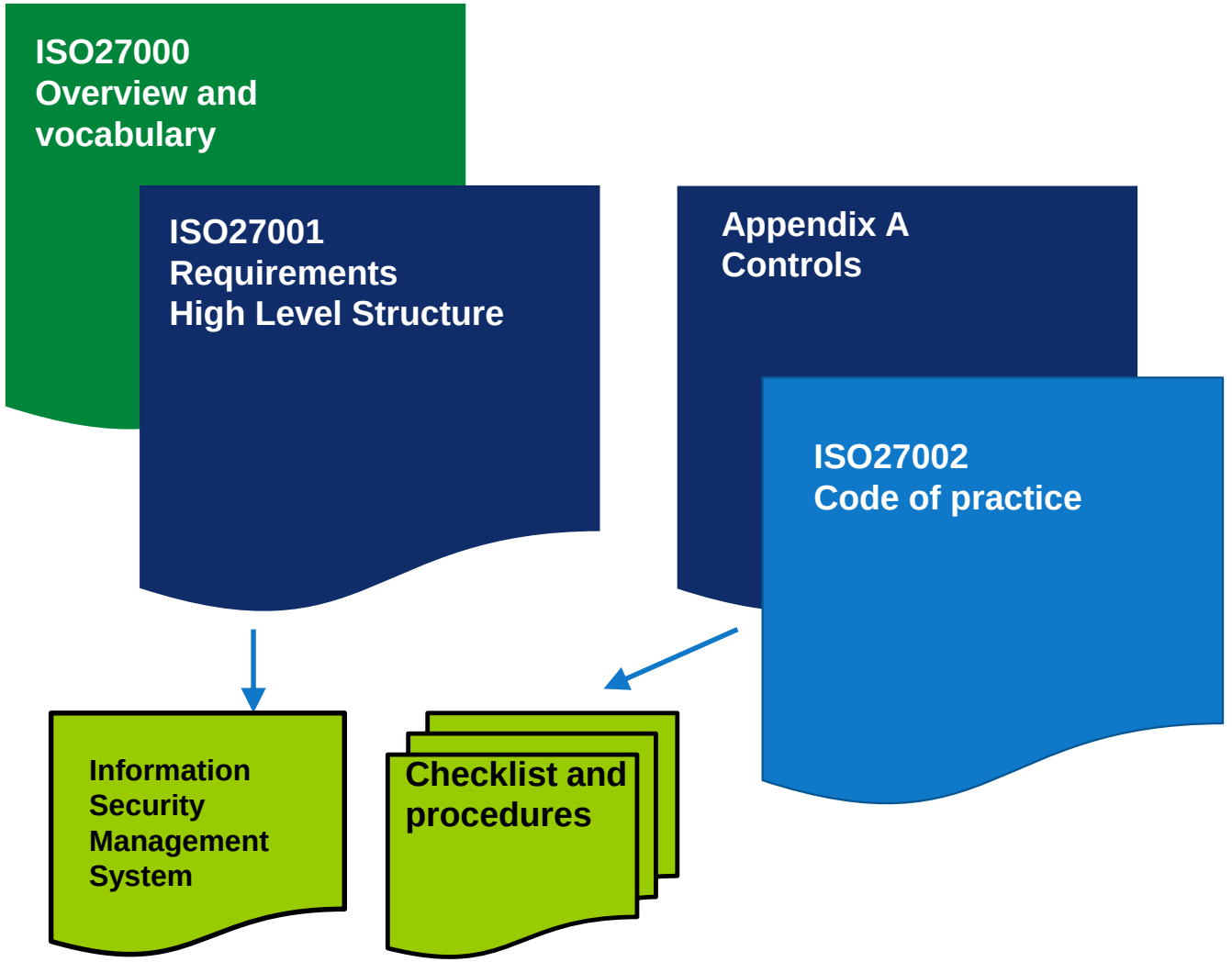
Informations Security Management System: Organization

DANMARKS STATISTIK



ISO27001 structure

DANMARKS STATISTIK



Requirements in ISO27001

DANMARKS STATISTIK

4. Context of the organization
    - 4.1. Understanding the organization and its context
    - 4.2. Understanding the needs and expectations of interested parties
    - 4.3. Determination of the scope of the ISMS
    - 4.4. ISMS

5. Leadership
    - 5.1. Ledership and commitment

6. Planning
    - 6.1 Actions to adress risks and opportunities
    - 6.2 Information security objectives and planning til achive them

7. Support
    - 7.1 Ressources
    - 7.2 Competence
    - 7.3 Awareness
    - 7.4. Communication
    - 7.5 Documented information

8. Operation
    - 8.1 Operational planning and control
    - 8.2 Information security risk assessment
    - 8.3 Information security risk treatment

9. Performance evaluation
    - 9.1. Monitoring, measurement, analysis and evaluation
    - 9.2 Internal audit
    - 9.3. Management review

10. Improvement
    - 10.1 Continual improvement
    - 10.2 Nonconformity and corrective action

Chapters in Annex A (ISO27001:2013) Controls

DANMARKS STATISTIK

5. Information Security Policies
6. Organisation of Information Security
7. Human Resources Security
8. Asset Management
9. Access Control
10. Cryptography
11. Physical and Environmental Security
12. Operational Security
13. Communications Security
14. System Acquisition, Development and Maintenance
15. Supplier Relationships
16. Information Security Incident Management
17. Information Security Aspects of Business Continuity Management
18. Compliance

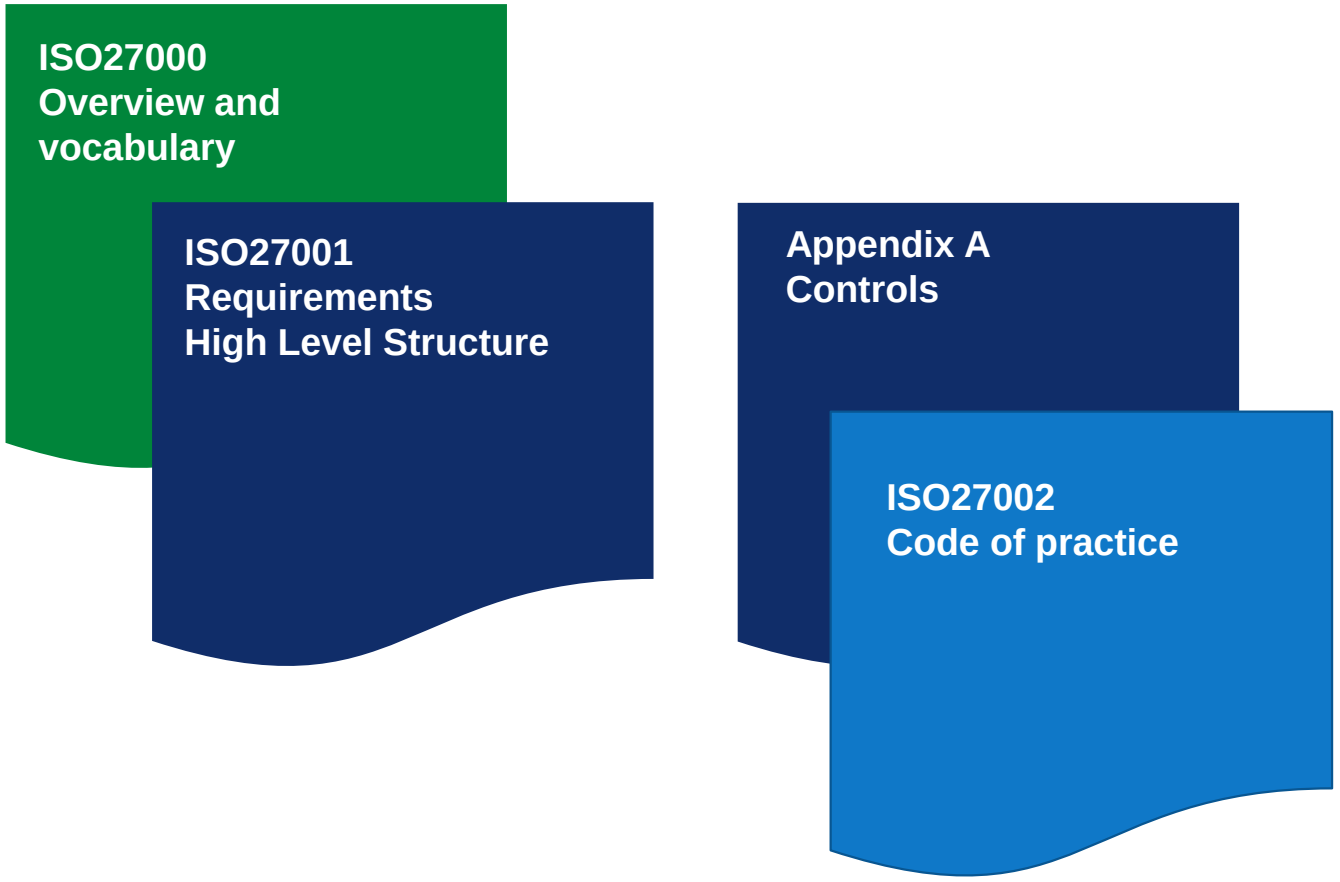
New ISO27001:2022 and ISO27002:2022

DANMARKS STATISTIK

Almost no changes to ISO27001 requirements

Annex A and 27002 has been completely restructured

- Before 114 controls; now 93 controls
- 11 new controls
- New structure: from 14 to 4 chapters



New controls in 27001/27002

DANMARKS STATISTIK

2021 chapter	Control name
5.7	Threat intelligence
5.23	Information security for use of cloud services
5.30	ICT readiness for business continuity
7.4	Physical security monitoring
8.9	Configuration management
8.10	Information deletion
8.11	Data masking
8.12	Data leakage prevention
8.16	Monitoring activities
8.22	Web filtering
8.28	Secure coding

CIA triad: the three pillars of informations security

DANMARKS STATISTIK

You need to know your data is protected from unauthorized access.

You have to be able to trust your data

You need to be able to access your data.

Security Objectives at DST

DANMARKS STATISTIK

1. that confidential information, including all unpublished statistical data, is **protected from unauthorized access**.
   - **Facilitate confidential processing, transmission and storage of data**, e.g. by using de-identification/pseudonymisation and encryption of data to the widest extent possible.
   - Prevent **loss and leakage** of data
   - Support compliance with the General Data Protection Regulation (**GDPR**), also as a data processor for others
   - Prevent **identification of individuals** and sole proprietorships, e.g. through deidentification and statistical disclosure limitation

2. that all information, statistical data as well as non-statistical data, is **correct and complete** and that IT systems are functioning correctly
   - Prevent **fraud** by means of automated and manual control measures
   - And building on this, obtain **correct functioning of the IT systems** with a minimum risk of tampering with data and systems. I.e. means for this purpose must be available and applied according to specific needs

3. that all information, both statistical data and non-statistical data, and IT services are **available**
   - Provide **operational security** and minimum risk of **critical failures, eg.** as a result of cyber terrorism and attacks on infrastructure

Data Confidentiality Policy

DANMARKS STATISTIK

The overall principles for the data confidentiality policy are:

- To protect the identity of the persons, businesses and institutions for which Statistics Denmark has data.
- To ensure that data in Statistics Denmark is solely applied for statistical or scientific surveys.

External users may apply individual data via one of Statistics Denmark's four service schemes:

1. The researcher scheme
2. The ministry scheme
3. The law model scheme
4. Data warehouses

Awareness concept

Campaigns

based on e.g. incidents, organizational needs or external demands.

Target groups and subject varies.

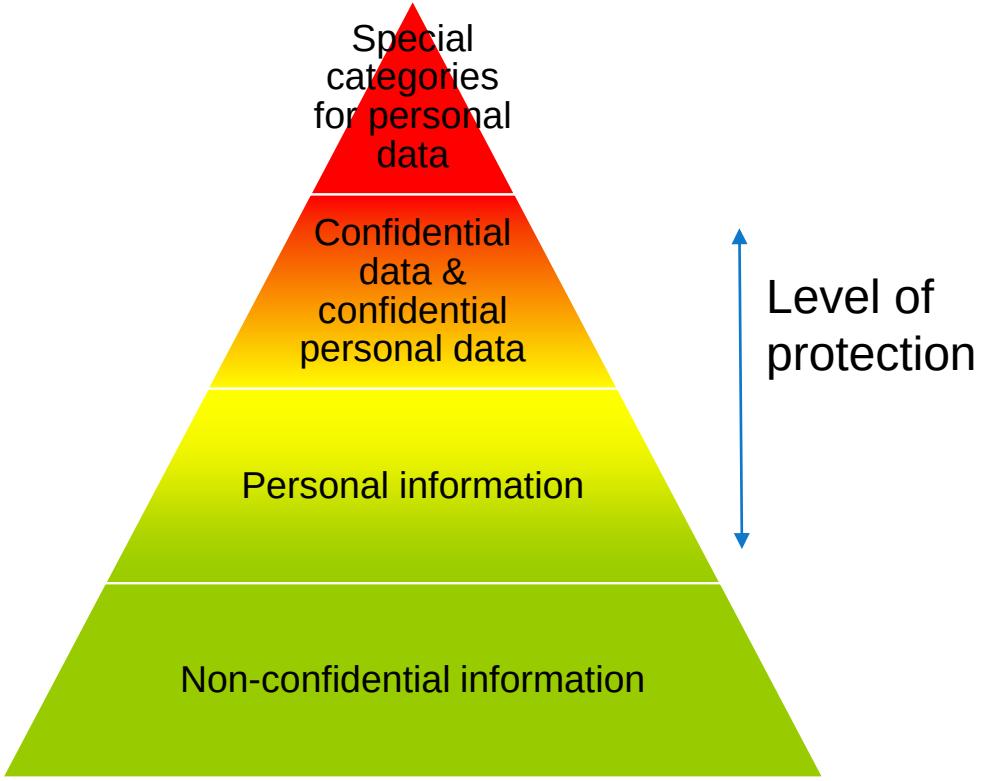
Data Classifications

DANMARKS STATISTIK

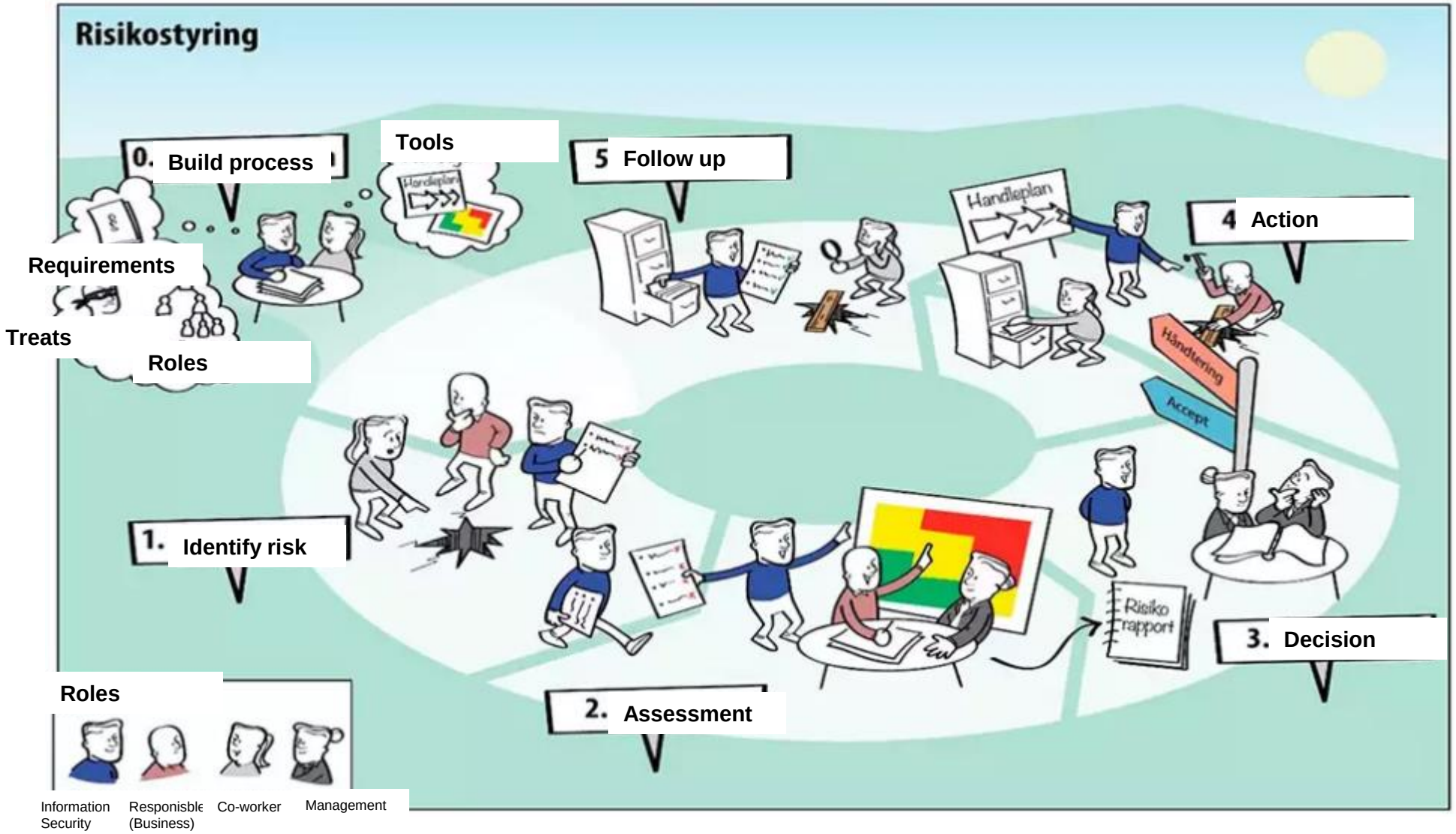
Statistical data

All data is confidential!

Non-statistical data



Risk management



Risk assessment and management

DANMARKS STATISTIK