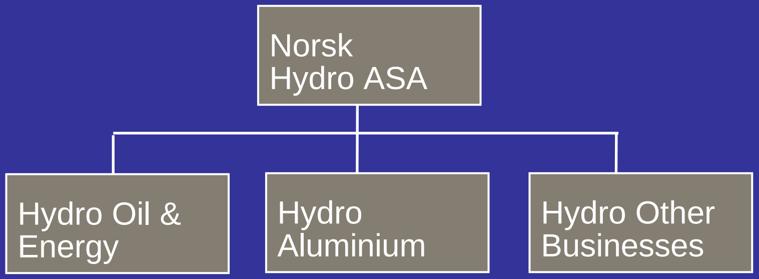
HYDRO

IS-sikkerhet med basis i gammel og ny ISO standard - ISO 17799.

SINTEF 22.09.2005

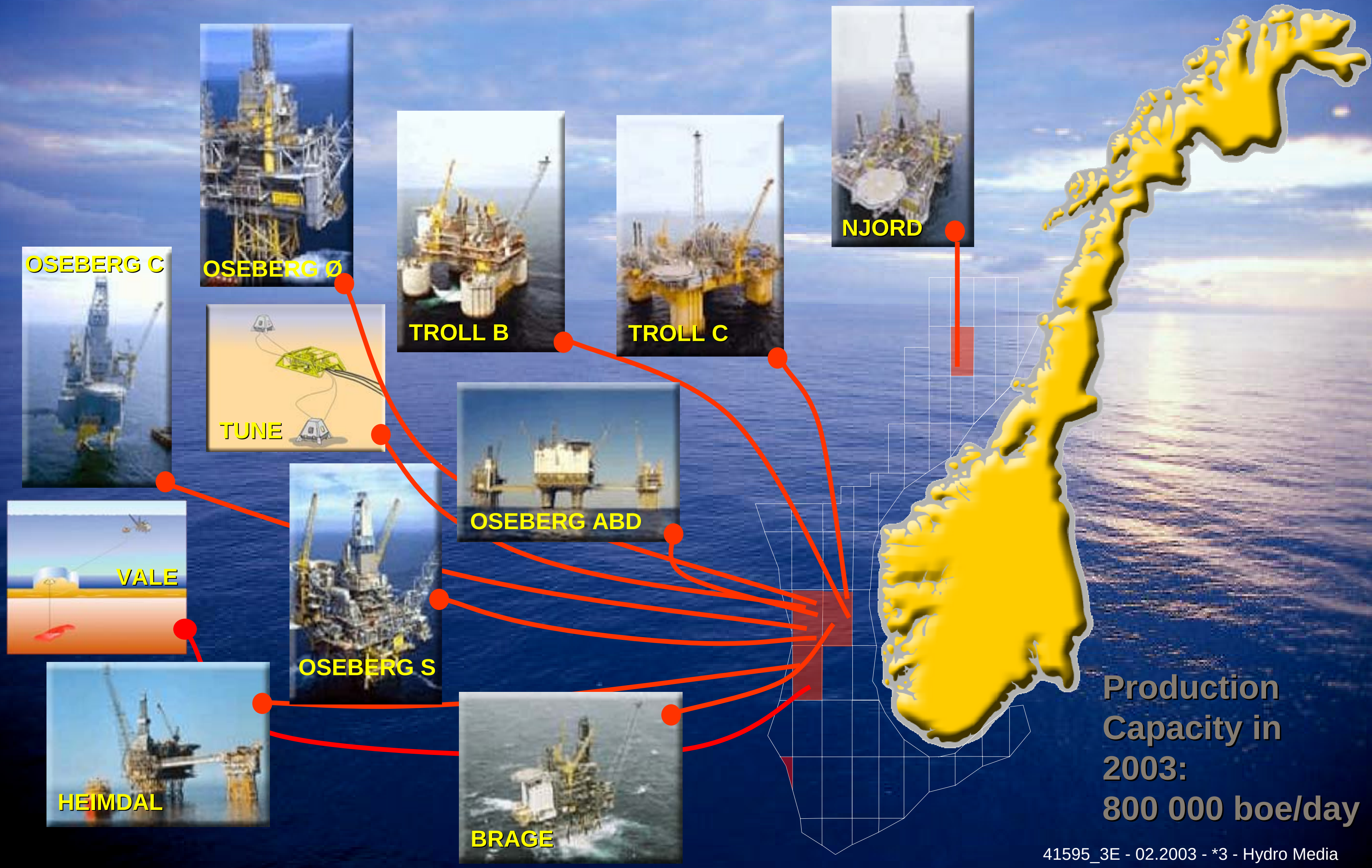
Norsk Hydro



- **Fortune 500, Energy and Aluminum**
  - ✓ Aluminum: Ranked as the third largest in the world
  - ✓ Leading in production of Oil and Gas in the North Sea
  - ✓ Leading in developing Renewable energy
- **36 000 employees**
- **40 countries**
- **100 years aniversary in 2005**

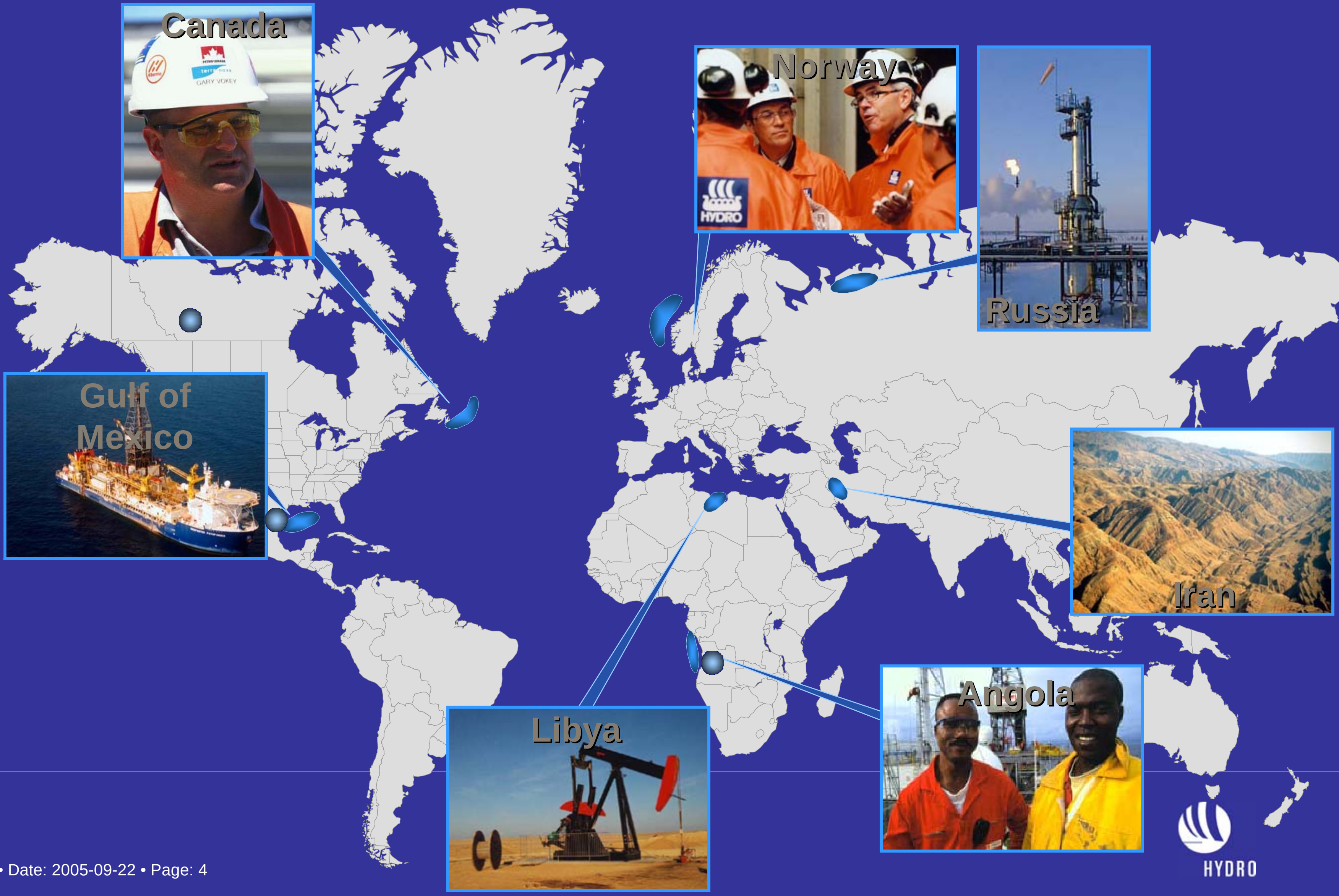
www.hydro.com

Second largest operator NCS, 2003



Production Capacity in 2003:
800 000 boe/day

Taking our Norwegian expertise abroad

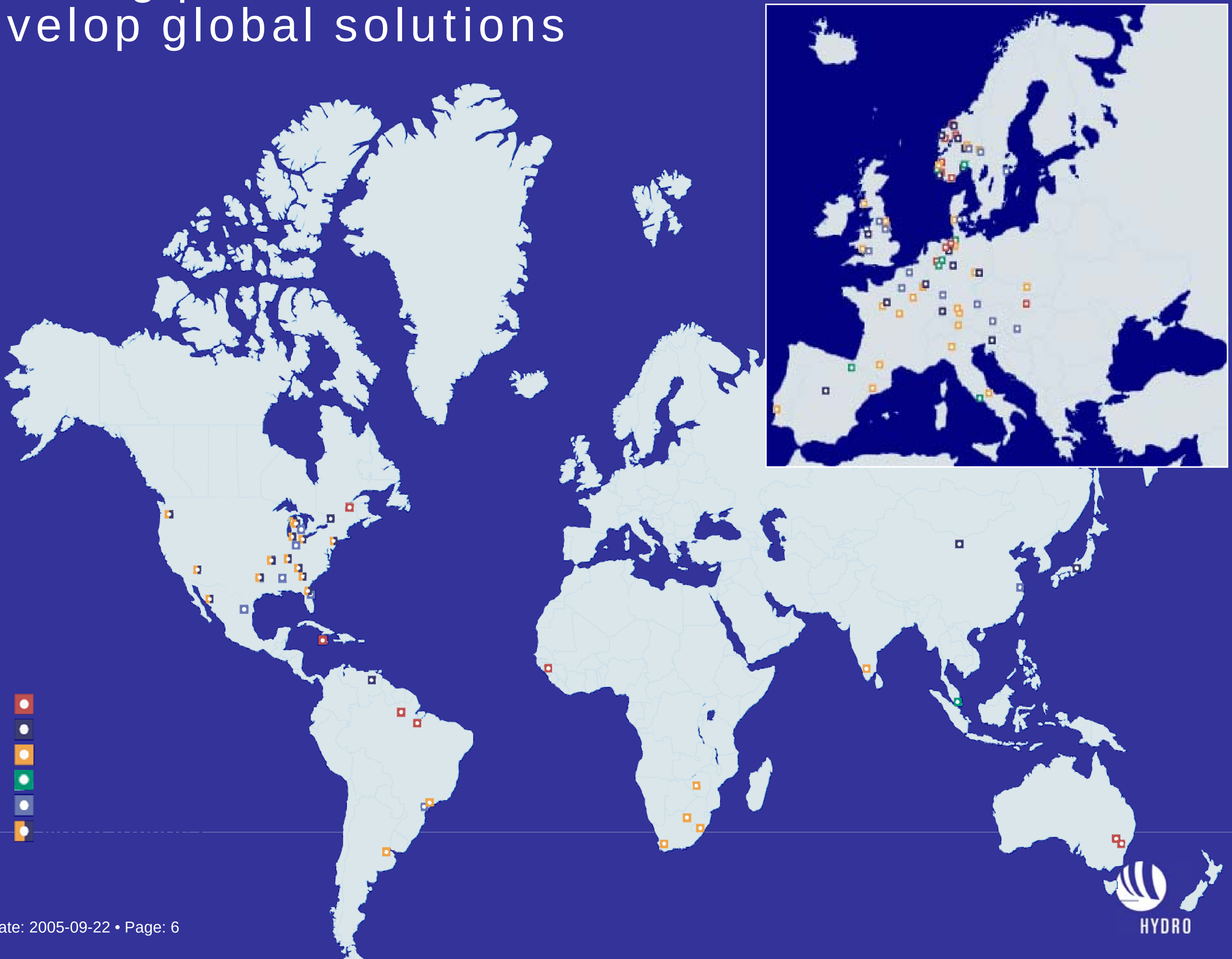


Hydro Aluminium puts the properties of aluminium into advanced application areas

- **Properties of aluminium:**
  - Strong and light
  - Highly corrosion resistant
  - Good conductivity
  - Good reflective qualities
  - Easy to form and process
  - Impermeable and odourless
  - Non-flammable
  - Good recyclability
  - Good energy absorption qualities

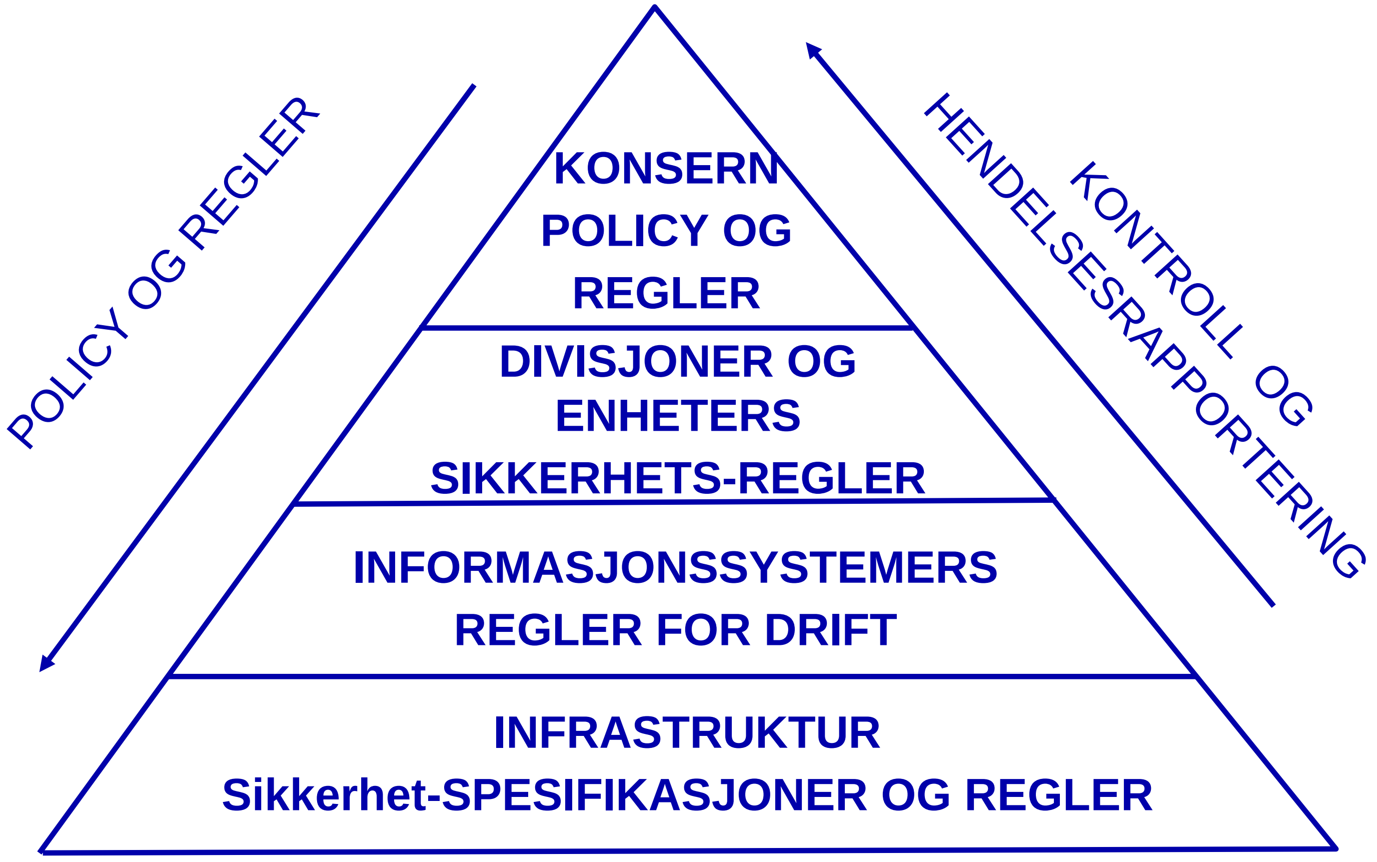
- **This makes aluminium ideal for the building, automotive and packaging industries, where Hydro Aluminium holds leading positions**

A strong position to develop global solutions



STYRINGS- OG KONTROLLSTRUKTUR

INFORMASJONS SIKKERHET



POLICY OG REGLER

KONTROLL OG HENDELSESRAPPORTERING

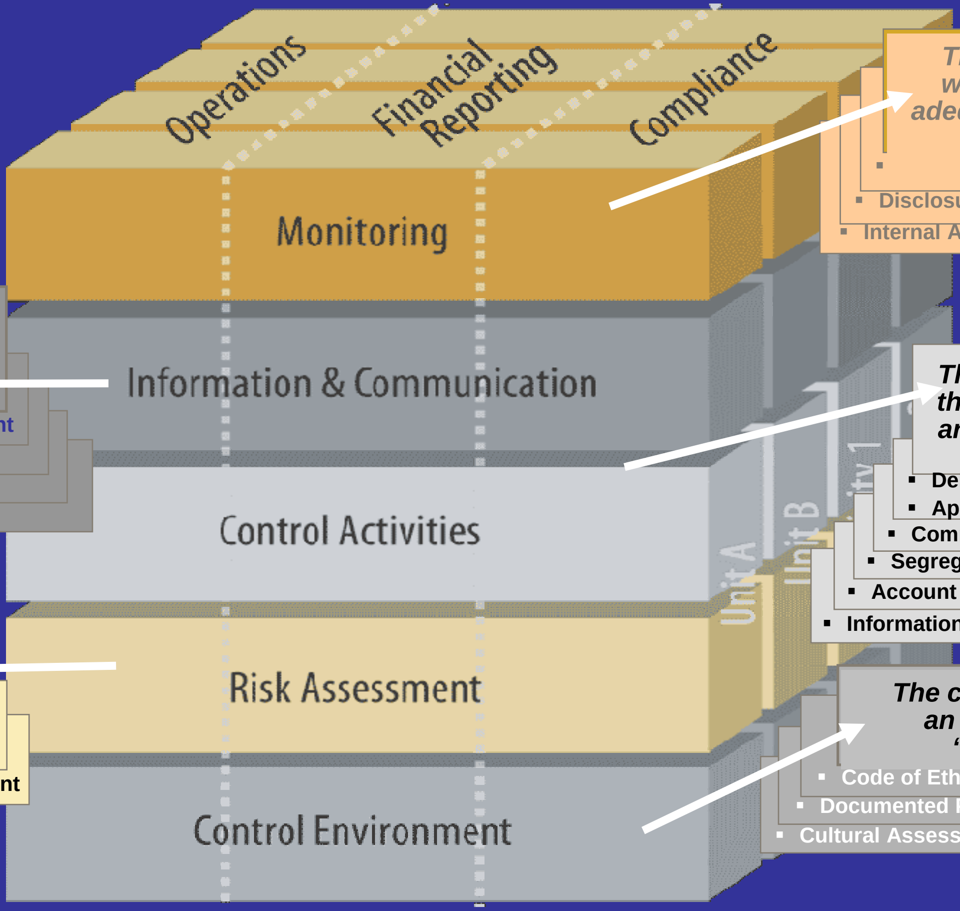
KONSERN POLICY OG REGLER

DIVISJONER OG ENHETERS SIKKERHETS-REGLER

INFORMASJONSSYSTEMERS REGLER FOR DRIFT

INFRASTRUKTUR
Sikkerhet-SPESIFIKASJONER OG REGLER

COSO* model:



The process to determine whether internal control is adequately designed, executed effective and adaptive

- Disclosure Committee
- Internal Audits

The process which ensures that relevant information is identified and communicated in a timely manner

- Messages from Senior Management
- Policies and Procedures
- Training
- Code of Ethics

The policies and procedures that help ensure that actions are identified to manage risk are executed and timely

- Delegation of Authority
- Approvals
- Common Processes and Systems
- Segregation of Duties
- Account Reconciliations
- Information Technology Controls

The evaluation of internal and external factors that impact an organization's performance

- Business Risk Management
- Process Risk Management
- Internal Audit Risk Assessment

The control conscience of an organization. The "tone at the top"

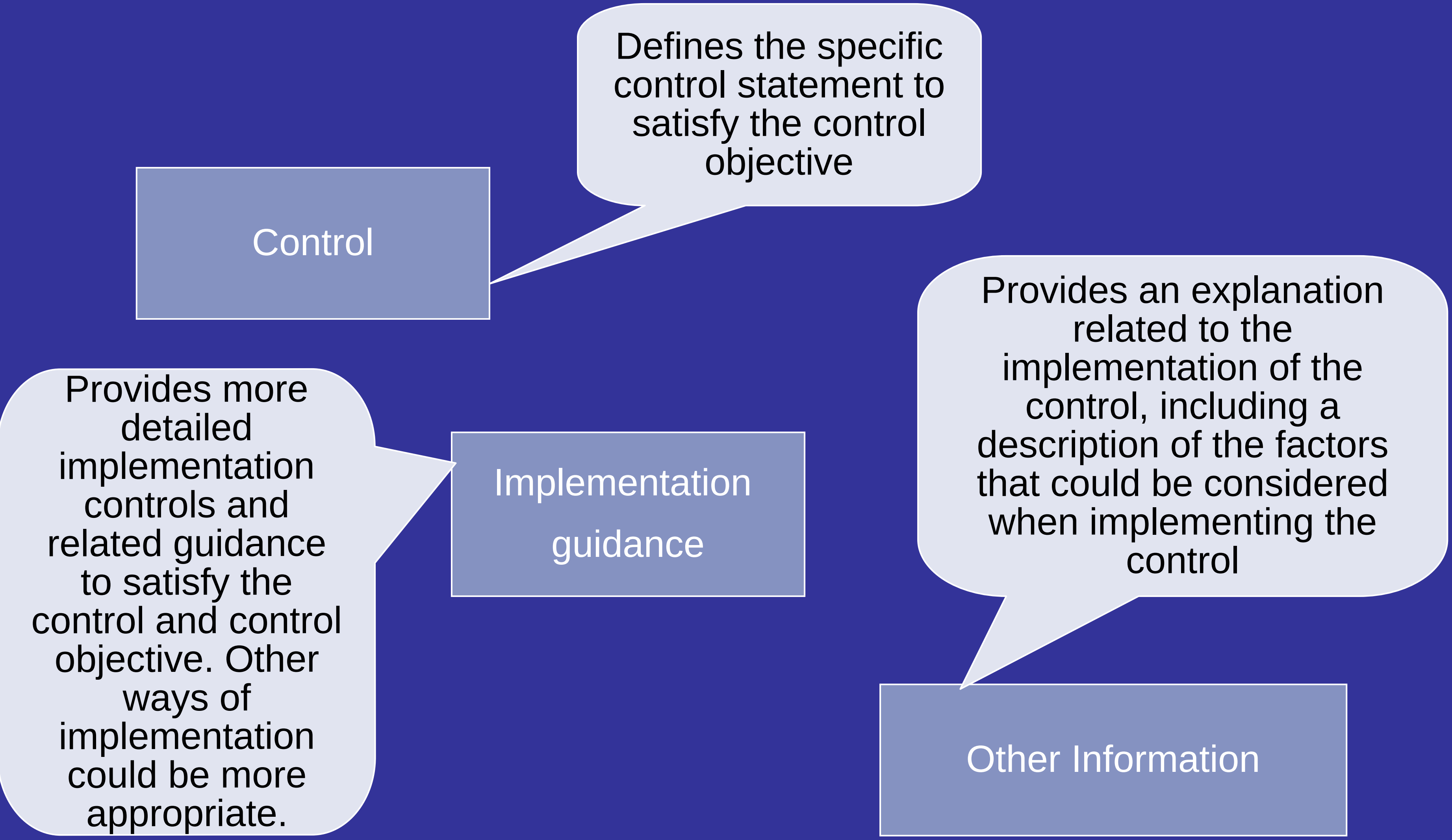
- Code of Ethics
- Documented Policies and Procedures
- Cultural Assessment

© 1992 by the American Institute of Certified Public Accountants, Inc. Reprinted with permission.

Corporate Sikkerhet Requirements Control areas:

- ✓**Based on ISO-17 799**
- ✓**Policy (K18.1)**
- ✓**CD11-1:**
  - **Organisation and responsibility**
  - **Information classification**
  - **Computer hardware Security**
  - **User identification and authorization**
  - **Securing information systems**
  - **Securing telecommunication and computer networks**
  - **Verification of information Security level**
  - **Securing against interruptions**
  - **Reporting nonconformity's**
  - **Review**

ISO 17799: 2005 Control Structure



Control

Defines the specific control statement to satisfy the control objective

Implementation guidance

Provides more detailed implementation controls and related guidance to satisfy the control and control objective. Other ways of implementation could be more appropriate.

Other Information

Provides an explanation related to the implementation of the control, including a description of the factors that could be considered when implementing the control

3.1 Clauses

Each clause contains a number of main security categories. The eleven clauses (accompanied with the number of main security categories included within each clause) are:

a) Security Policy (1);

b) Organizing Information Security (2);

c) Asset Management (2);

d) Human Resources Security (3);

e) Physical and Environmental Security (2);

f) Communications and Operations Management (10);

g) Access Control (7);

h) Information Systems Acquisition, Development and Maintenance (6);

i) Information Security Incident Management (2);

j) Business Continuity Management (1);

k) Compliance (3).

39 main security

categories

Each main security category contains:

a) a control objective stating what is to be achieved; and

b) one or more controls that can be applied to achieve the control objective.

5.1 Information security policy

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

Management should set a clear policy direction in line with business objectives and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization.

ISO 1 7799 : 2005

10.5 Back-up

Objective: To maintain the integrity and availability of information and information processing facilities.

Routine procedures should be established to implement the agreed back-up policy and strategy (see also 14.1) for taking back-up copies of data and rehearsing their timely restoration.

10.5.1 Information back-up

Control

Back-up copies of information and software should be taken and tested regularly in accordance with the agreed backup policy.

ISO 1 7799 : 2005 Continued:

Implementation guidance

Adequate back-up facilities should be provided to ensure that all essential information and software can be recovered following a disaster or media failure.

The following items for information back up should be considered:

a) the necessary level of back-up information should be defined;

b) accurate and complete records of the back-up copies and documented restoration

procedures should be produced;

c) the extent (e.g. full or differential backup) and frequency of backups should reflect the

business requirements of the organization, the security requirements of the information

involved, and the criticality of the information to the continued operation of the organization;

d) the back-ups should be stored in a remote location, at a sufficient distance to escape any

damage from a disaster at the main site;

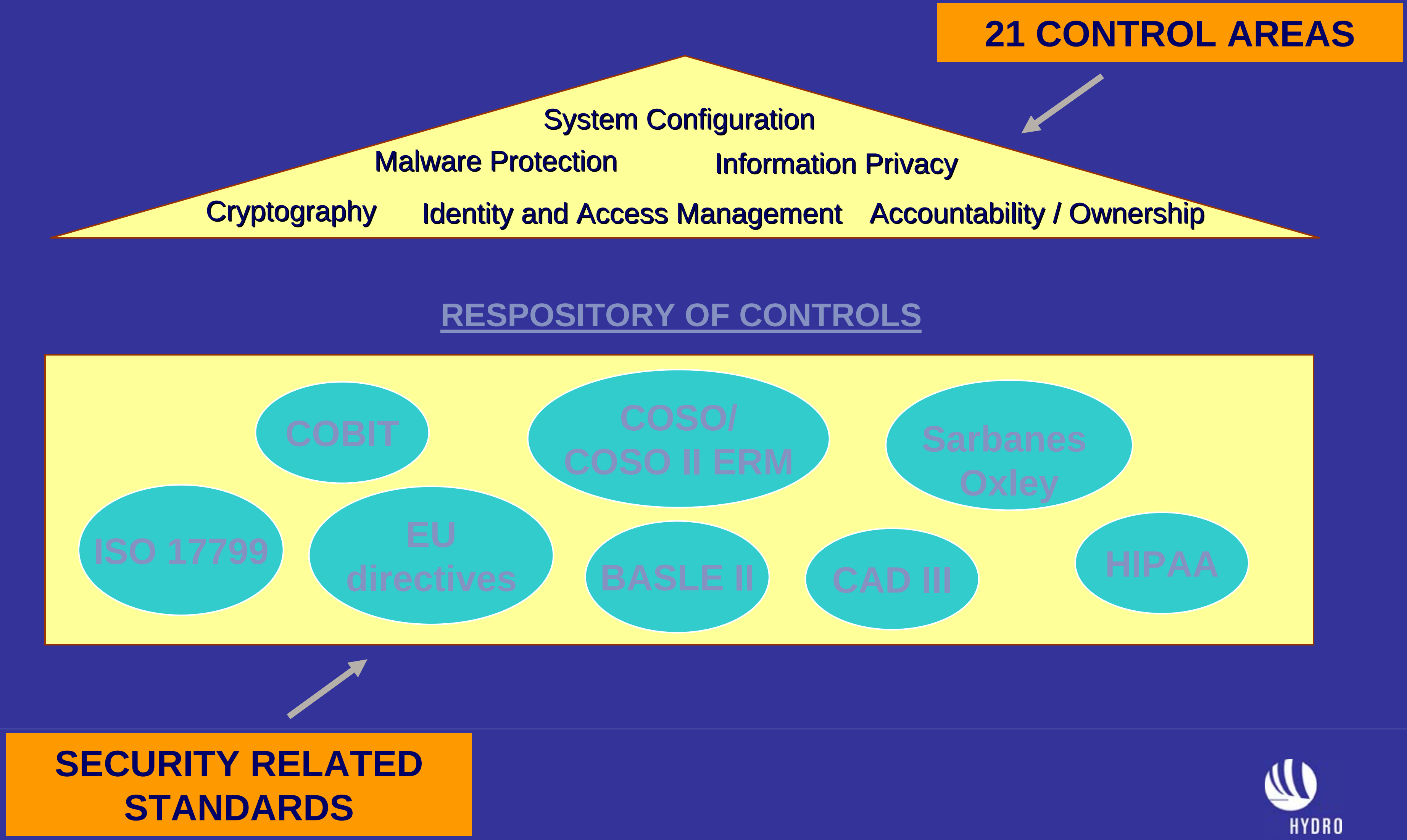
e) back-up information should be given an appropriate level of physical and environmental

protection (see clause 9) consistent with the standards applied at the main site; the

controls applied to media at the main site should be extended to cover the back-up site;

f) back-up media should be regularly tested to ensure that they can be relied upon for

ISF's META Standard schematic



The key 21 high-level control areas

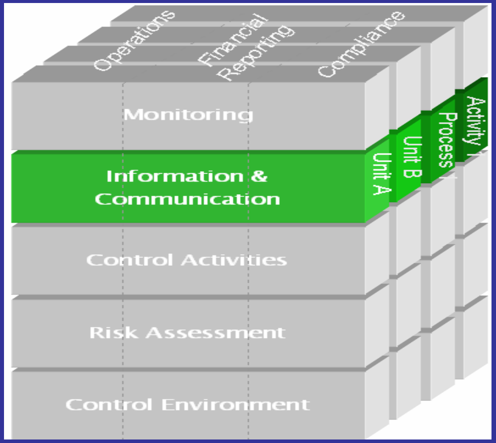
1. Information Security Governance
2. Information Security Policy
3. Security Education / Awareness
4. Accountability / Ownership
5. Information Risk Analysis
6. Asset Management
7. Identity and Access Management
8. Application Security
9. Physical and Environmental Security
10. System Configuration
11. System Monitoring
12. Network Security
13. Electronic Communication
14. Cryptography
15. Information Privacy
16. Malware Protection
17. System Development
18. Change Management
19. Incident Management
20. Third Party Management
21. Business Continuity

SOX IS/IT “how to” guide;
COBIT/Deloitte RACK

The **COSO** model has been developed into SOX COBIT ‘de facto standard’ by IT-Governance Institute.

The SOX **COBIT** version is covered by Deloitte’s own audit RACK (with near 100% coverage)

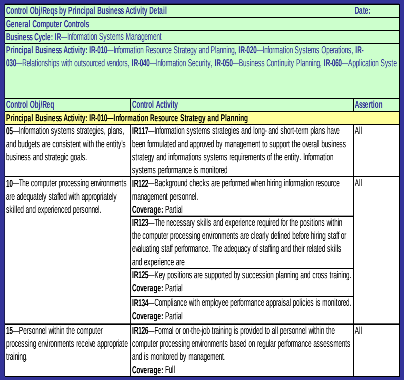
This **RACK** has been slightly modified (expanded and ‘cleaned) and then ‘scaled down’ to a “Light” version (only the Control Objectives)



COSO model

The **Full RACK** is to be used for the major Applications/systems (C2K, Hyperion, SAP etc)
whereas the **Light RACK** is to be used for Applications/systems of less significance
(minor ERP systems, local hosting etc)

Deloitte “Full RACK”



Control Obj/Reqs by Principal Business Activity Detail		Date:
General Computer Controls		
Business Cycle: IR—Information Systems Management		
Principal Business Activity: IR-010—Information Resource Strategy and Planning, IR-020—Information Systems Operations, IR-030—Relationships with outsourced vendors, IR-040—Information Security, IR-050—Business Continuity Planning, IR-060—Application Syste		
Control Obj/Req	Control Activity	Assertion
Principal Business Activity: IR-010—Information Resource Strategy and Planning		
05—Information systems strategies, plans, and budgets are consistent with the entity's business and strategic goals.	**IR117**—Information systems strategies and long- and short-term plans have been formulated and approved by management to support the overall business strategy and informations systems requirements of the entity. Information systems performance is monitored	All
10—The computer processing environments are adequately staffed with appropriately skilled and experienced personnel.	**IR122**—Background checks are performed when hiring information resource management personnel. **Coverage:** Partial	All
	IR123—The necessary skills and experience required for the positions within the computer processing environments are clearly defined before hiring staff or evaluating staff performance. The adequacy of staffing and their related skills and experience are	
	IR125—Key positions are supported by succession planning and cross training. **Coverage:** Partial	
	IR134—Compliance with employee performance appraisal policies is monitored. **Coverage:** Partial	
15—Personnel within the computer processing environments receive appropriate training.	**IR126**—Formal or on-the-job training is provided to all personnel within the computer processing environments based on regular performance assessments and is monitored by management. **Coverage:** Full	All

SOX COBIT

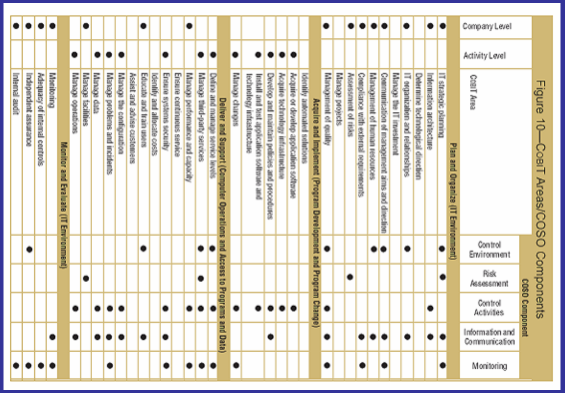
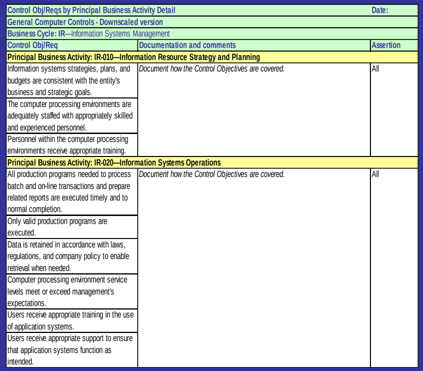


Figure 10—COBIT Areas/COSO Components

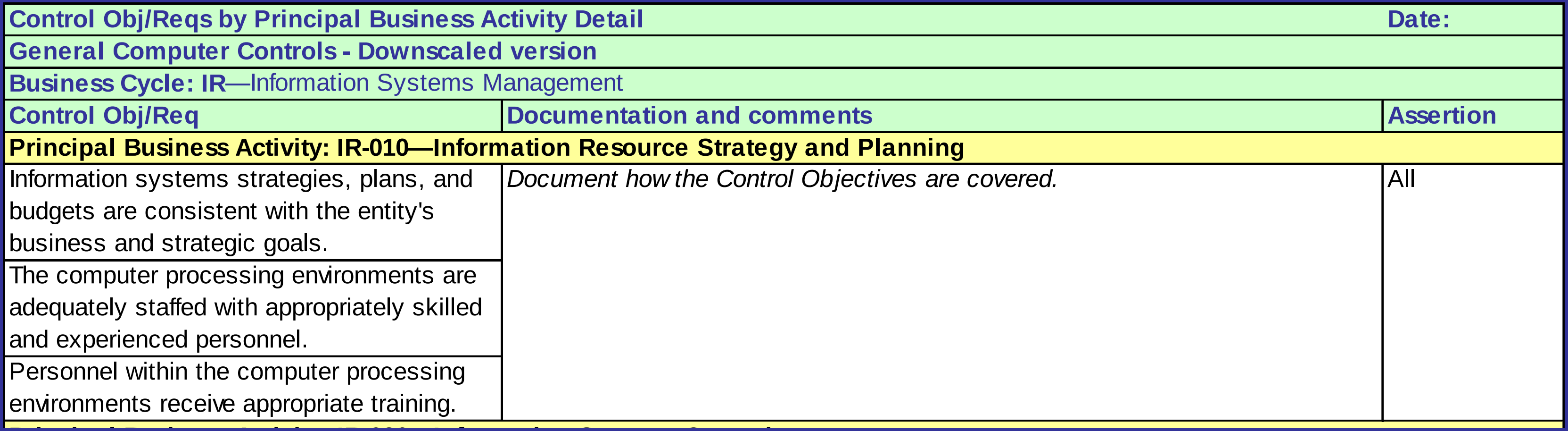
			COSO Component				
Company Level	Activity Level	COBIT Area	Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring
		Plan and Organize (IT Environment)					
●		IT strategic planning	●	●		●	●
●		Information architecture			●	●	
		Determine technological direction					
●		IT organization and relationships	●			●	
		Manage the IT investment					
●		Communication of management aims and direction	●			●	●
●		Management of human resources	●			●	
●		Compliance with external requirements				●	●
●		Assessment of risks		●			
		Manage projects					
●		Management of quality	●		●	●	●
		Acquire and Implement (Program Development and Program Change)					
		Identify automated solutions					
	●	Acquire or develop application software			●		
	●	Acquire technology infrastructure			●		
	●	Develop and maintain policies and procedures			●	●	
	●	Install and test application software and technology infrastructure			●		
	●	Manage changes			●		●
		Deliver and Support (Computer Operations and Access to Programs and Data)					
	●	Define and manage service levels	●		●		●
	●	Manage third-party services	●	●	●		●
●		Manage performance and capacity			●		●
		Ensure continuous service					
	●	Ensure systems security			●	●	●
		Identify and allocate costs					
●		Educate and train users	●			●	
		Assist and advise customers					
	●	Manage the configuration			●	●	
	●	Manage problems and incidents			●	●	●
	●	Manage data			●	●	
●		Manage facilities		●			
	●	Manage operations			●	●	
		Monitor and Evaluate (IT Environment)					
●		Monitoring				●	●
●		Adequacy of internal controls					●
●		Independent assurance	●				●
●		Internal audit					●

Deloitte “Light RACK”



Control Obj/Reqs by Principal Business Activity Detail		Date:
General Computer Controls - Downscaled version		
Business Cycle: IR—Information Systems Management		
Control Obj/Req	Documentation and comments	Assertion
Principal Business Activity: IR-010—Information Resource Strategy and Planning		
Information systems strategies, plans, and budgets are consistent with the entity's business and strategic goals.	*Document how the Control Objectives are covered.*	All
The computer processing environments are adequately staffed with appropriately skilled and experienced personnel.		
Personnel within the computer processing environments receive appropriate training.		
Principal Business Activity: IR-020—Information Systems Operations		
All production programs needed to process batch and on-line transactions and prepare related reports are executed timely and to normal completion.	*Document how the Control Objectives are covered.*	All
Only valid production programs are executed.		
Data is retained in accordance with laws, regulations, and company policy to enable retrieval when needed.		
Computer processing environment service levels meet or exceed management's expectations.		
Users receive appropriate training in the use of application systems.		
Users receive appropriate support to ensure that application systems function as intended.		

SOX IS/IT "how to" guide;
Use of COBIT/Deloitte RACK Light version



Control Obj/Reqs by Principal Business Activity Detail		**Date:**
General Computer Controls - Downscaled version		
Business Cycle: IR—Information Systems Management		
Control Obj/Req	**Documentation and comments**	**Assertion**
Principal Business Activity: IR-010—Information Resource Strategy and Planning		
Information systems strategies, plans, and budgets are consistent with the entity's business and strategic goals.	*Document how the Control Objectives are covered.*	All
The computer processing environments are adequately staffed with appropriately skilled and experienced personnel.		
Personnel within the computer processing environments receive appropriate training.		

Control Objectives

- These are the same as for the 'Full' version, but the requirement of the Control Activities are less ->
- Concentrate on
  - IR020 Operations
  - IR040 Security
  - IR060 Application implementation
  - IR070 Databases
  - IR080 Network
  - IR090 Software support

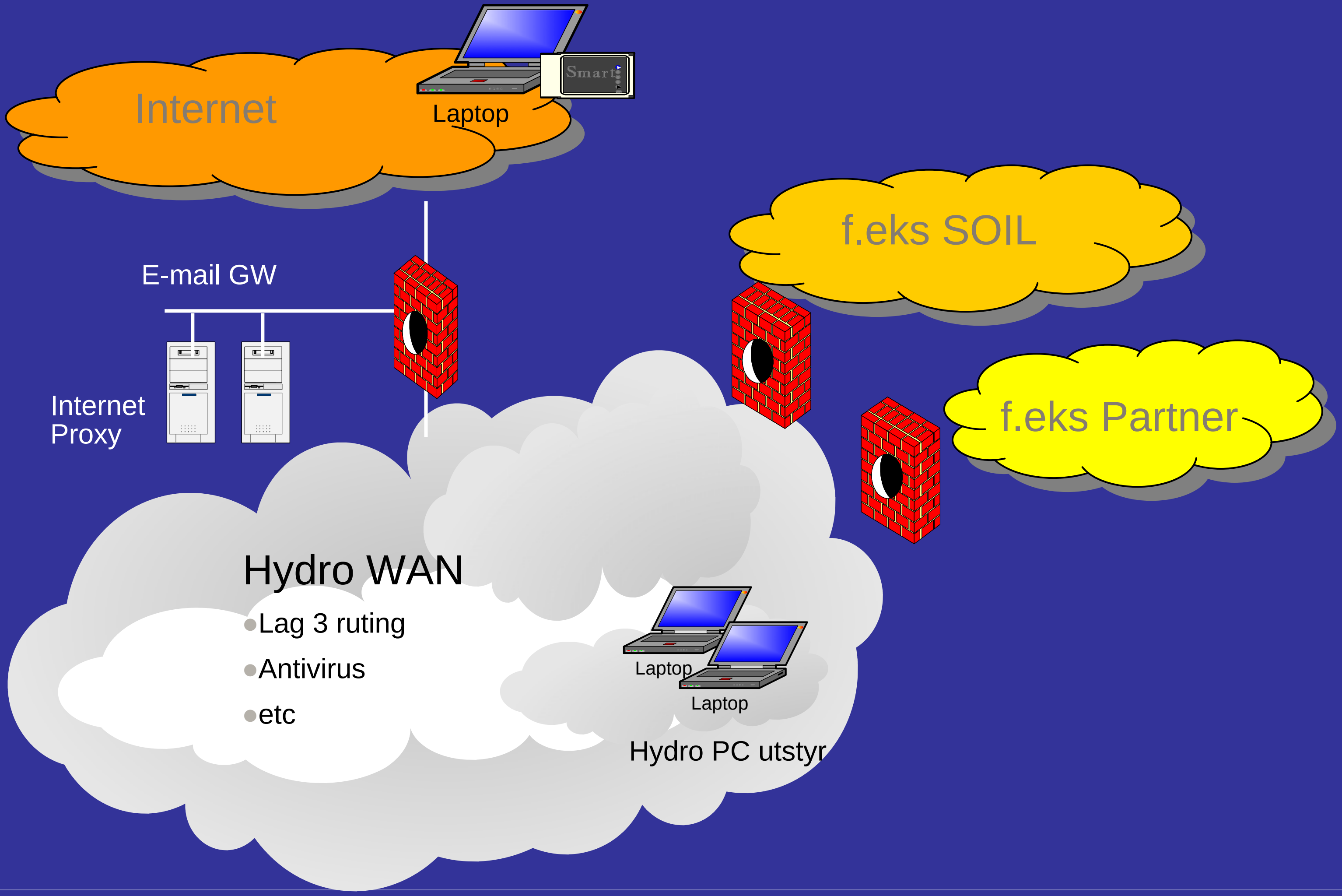
Control Activity

- **The Control Activity will be checked against NHC CD011-1 Information Security as minimum base standard**
- Be particular aware of new addition
  IR998 End User Computing (= spreadsheets)
  IR999 Emergency change
- Feel free to use your own Control Activities, mark these clearly in the report (spreadsheet)
- Every Control Activity should be testable and a description of the test entered into RiskNavigator

Assertion

- These are referring to the coverage of the Control (see Control description)

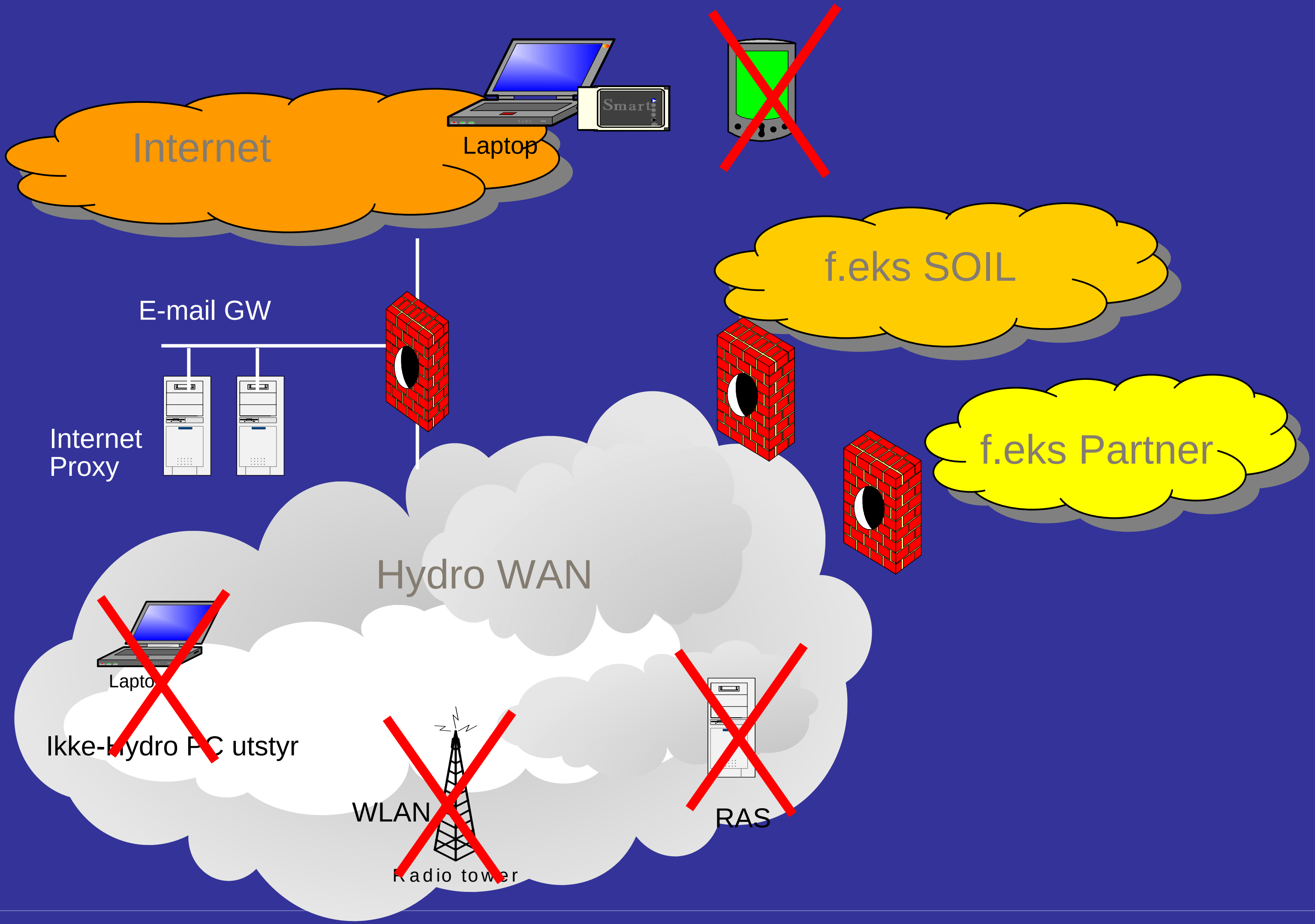
2. Eksempler på hva som fungerer av IT/IS sikkerhet



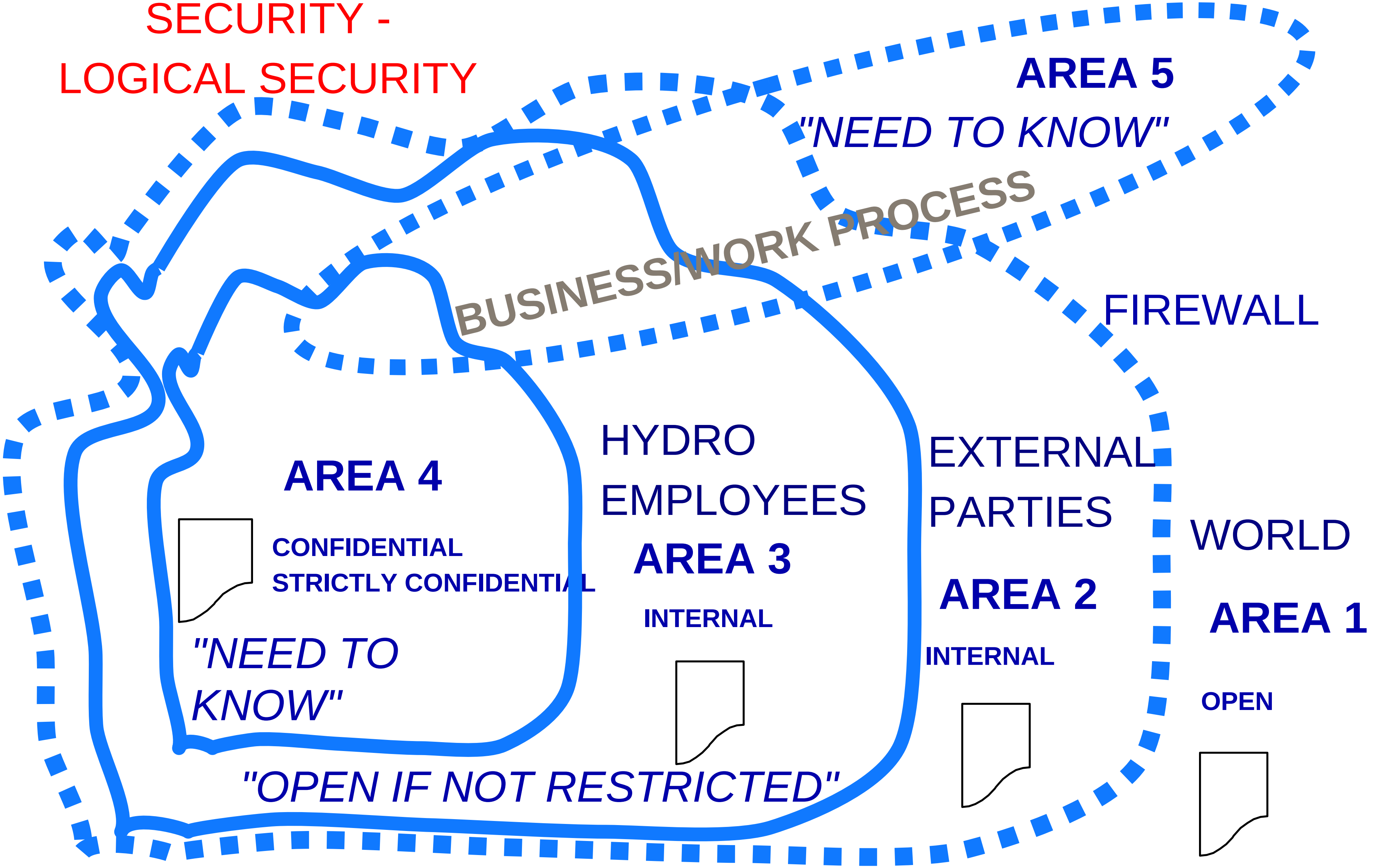
Hydro WAN

- Lag 3 ruting
- Antivirus
- etc

2. Eksempler på hva som utfordrer IT/IS sikkerhet



INFORMATION SECURITY - LOGICAL SECURITY



AREA 5

"NEED TO KNOW"

BUSINESS/WORK PROCESS

FIREWALL

AREA 4

CONFIDENTIAL

STRICTLY CONFIDENTIAL

"NEED TO KNOW"

HYDRO EMPLOYEES

AREA 3

INTERNAL

EXTERNAL PARTIES

AREA 2

INTERNAL

WORLD

AREA 1

OPEN

"OPEN IF NOT RESTRICTED"

HYDRO'S INTERNAL NETWORK

Analyse / Konklusjon

Hva fungerer ?

- **Rolledeling**
    - ✓ hvem som har styring, hvem som produserer IT/IS
- **Skille på hvem som utøver sikkerhetsfunksjoner – regelsetting og drift**

Hva er utfordringene ?

- **Organisatoriske:**
    - Balansen mellom hva som skal være sentralt ”styrt og produsert” og hva som kan være lokalt ”styrt og produsert”
    - Samordne prosesser på tvers av forretningsområdene
- **Menneskelige:**
    - Holdninger, kunnskap og prosesser
      pga kjente barrierer som språk, kultur, avstand osv.
- **Tekniske:**
    - Ikke proprietære systemer
    - Overganger til Offentlige nett
    - Identity/ Access Management