# Overview of vulnerabilities

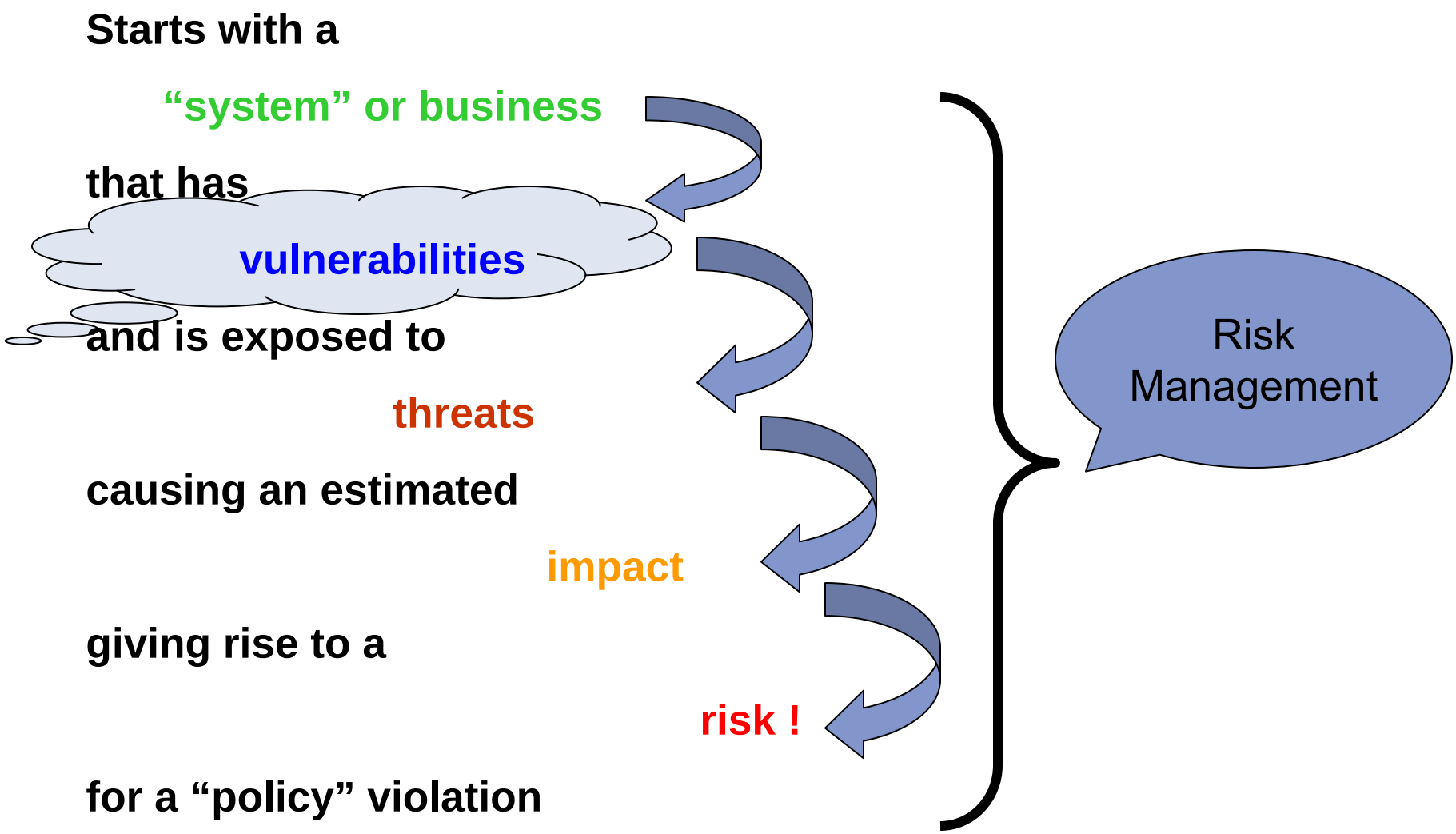
## what should we be worried about?

**Åsmund Skomedal**

**Research Director, Norsk Regnesentral**

**RISKnet Workshop, Oslo, Norway**
**6. May 2009**

# Intro: How to understand Risk



# Intro: What is Risk Management?

- Risk Management
  - Specialty of management
  - Treats risk objectively
  - Should consider not only technical risk, but also psychological, social and cultural contexts

- Management
  - Planning
  - Organising and leading
  - Controlling (!) to achieve organisational objectives efficiently and effectively
  - Revising

# Intro: Types of Risk Management

- Insurance
- Financial
- Political
- Societal
- Credit
- Environmental
- Strategic
- Safety
- Operational

# Objectives of Risk Management

- Survival
- Economy
- Acceptable level of worry and anxiety
- Earnings stability
- Uninterrupted operations
- Continued growth
- Good citizenship or social responsibility
- Satisfaction of externally imposed obligations

# Examples of policy violations

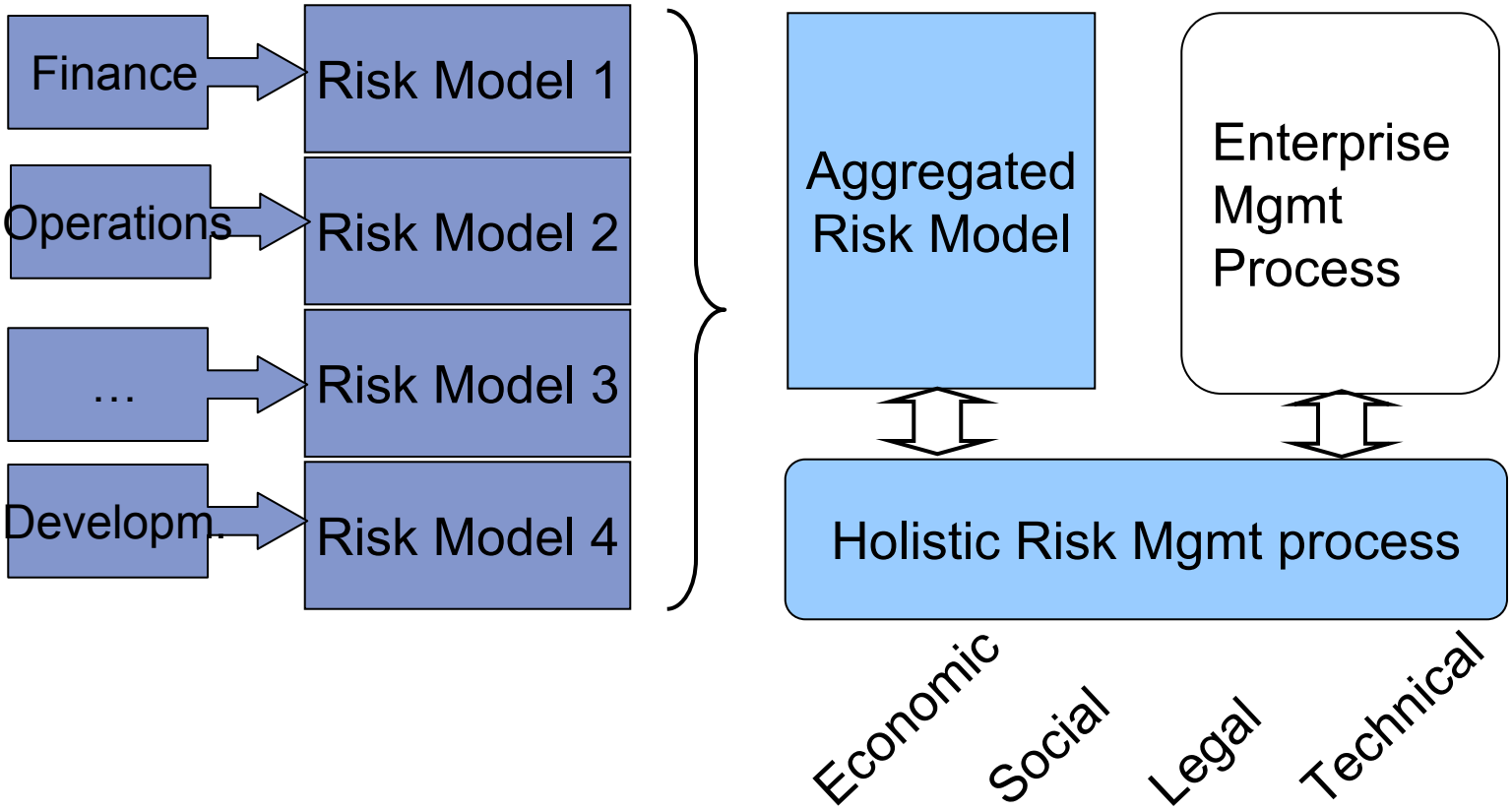
- Survival
- Economy
- Acceptable level of worry and anxiety
- Earnings stability
- Uninterrupted operations
- Continued growth
- Good citizenship or social responsibility
- Satisfaction of externally imposed obligations

# What is Holistic Risk Management?

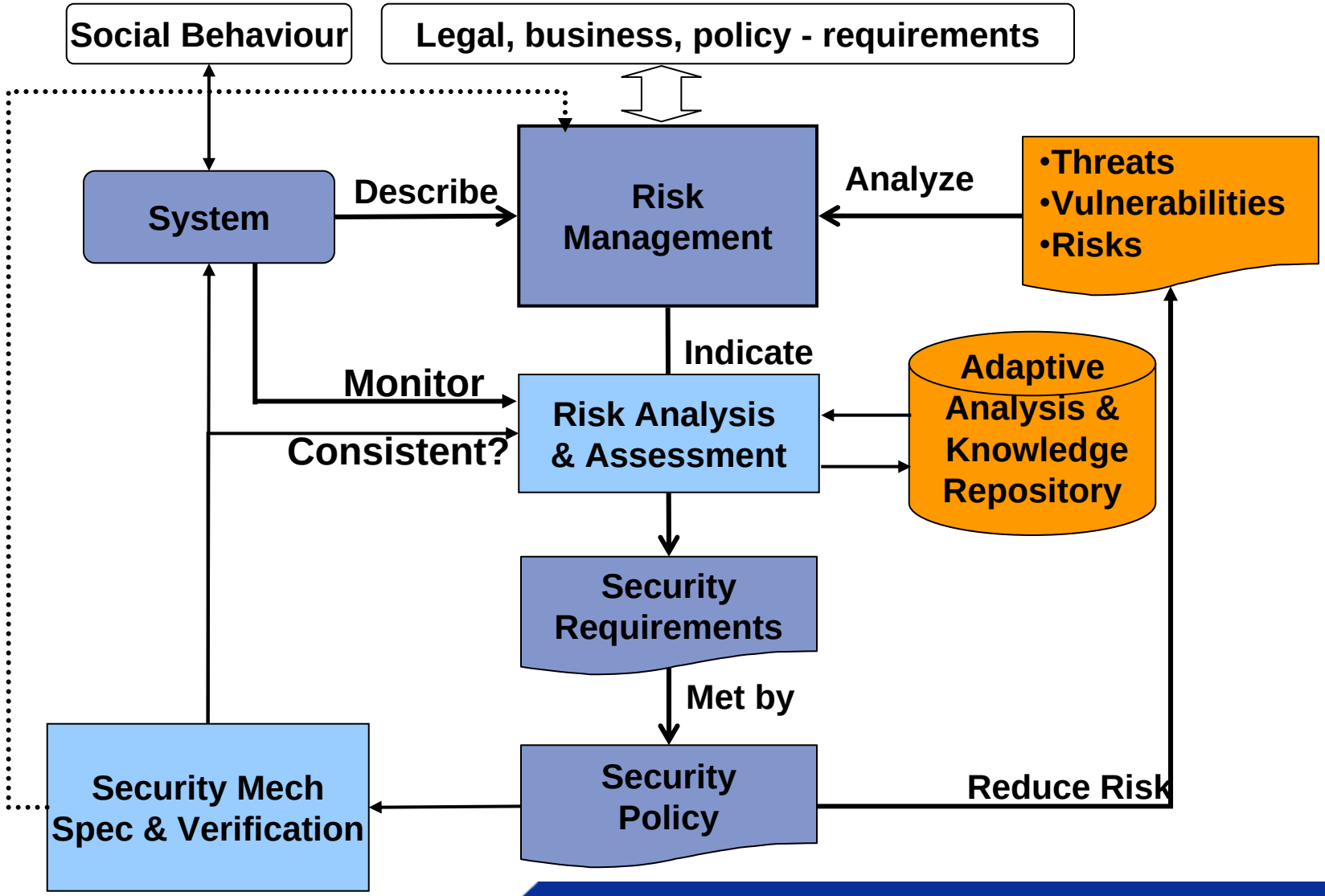
- a reporting system that should comprise:
  - holistic risk ranking and mapping
  - holistic risk aggregation
  - hierarchy of risk treatment options.
- consists of two elements
  - the management of all risks of an enterprise with consideration of all risk interdependences
  - the integration of the risk management into the enterprise management.

Thereby risk management is not only aligned to the **risk** view, but also includes the **success potentials**.

# Multidisciplinary Approach



# A Risk Management process



# Information Security Management System (ISMS)

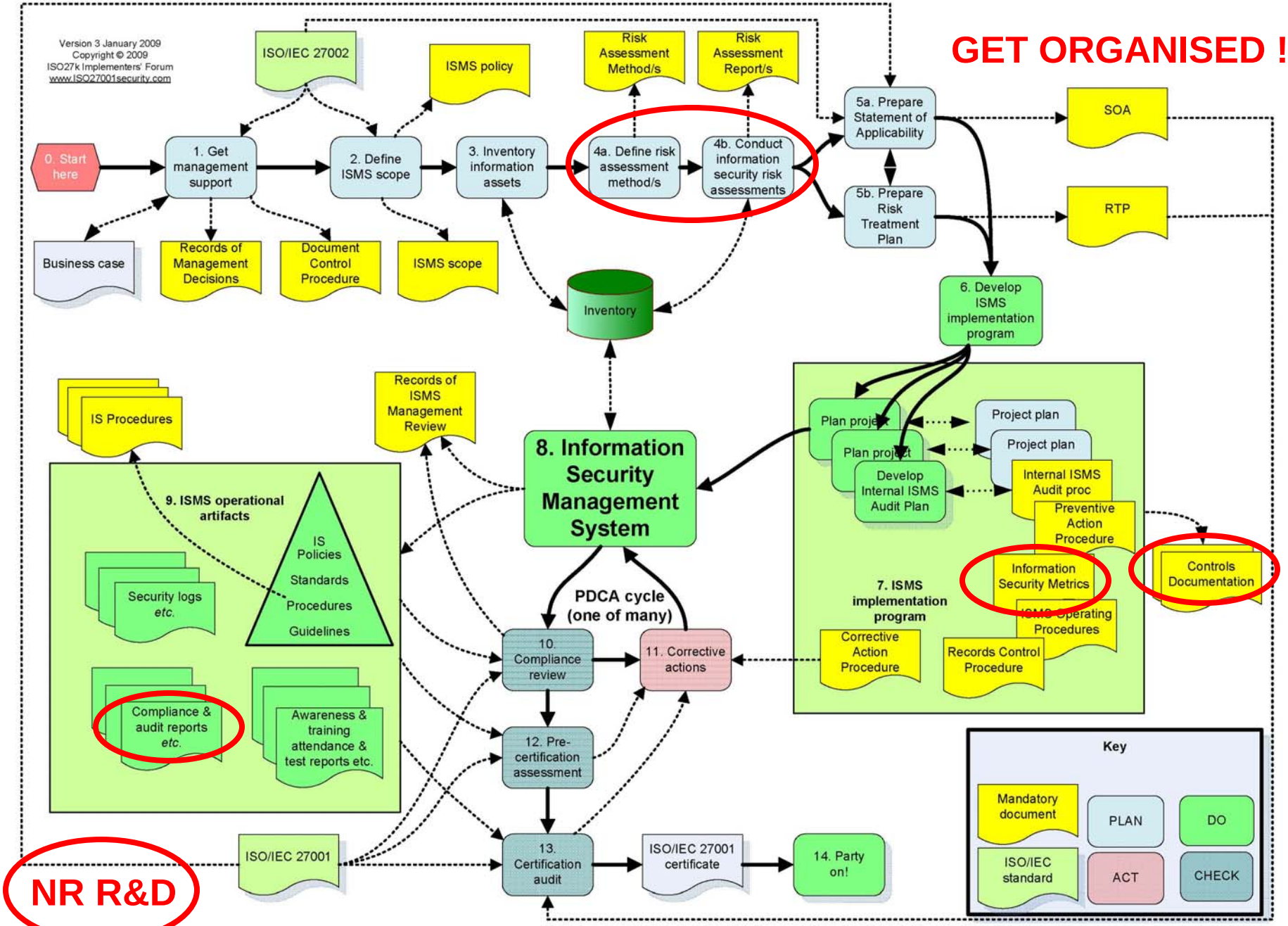
## Drivers

- compliance
- criticality
- complexity
- criminals
- customer confidence
- certification
- …

# ISMS highlights (of topics)

Process: Plan – Do – Check – Act, topics are:

- (legal) and contractual regulation
- (security) policy, organisation
- information classification, assets and human resources
- **controls**
  - physical security
  - ICT systems security
    - purchase, development & test, operations
    - networks, storage, exchange, access (network, OS, app)
  - e-commerce, public information
- monitoring and security incidents, continuity management
- audit and certification
- Standardisation (ISO 27000 series) is a platform for certification


Version 3 January 2009
Copyright © 2009
ISO27k Implementers' Forum
www.ISO27001security.com
GET ORGANISED !
ISO/IEC 27002
ISMS policy
Risk Assessment Method/s
Risk Assessment Report/s
0. Start here
1. Get management support
2. Define ISMS scope
3. Inventory information assets
4a. Define risk assessment method/s
4b. Conduct information security risk assessments
5a. Prepare Statement of Applicability
5b. Prepare Risk Treatment Plan
SOA
RTP
Business case
Records of Management Decisions
Document Control Procedure
ISMS scope
Inventory
6. Develop ISMS implementation program
IS Procedures
Records of ISMS Management Review
8. Information Security Management System
9. ISMS operational artifacts
IS Policies
Standards
Procedures
Guidelines
Security logs etc.
Compliance & audit reports etc.
Awareness & training attendance & test reports etc.
PDCA cycle (one of many)
10. Compliance review
11. Corrective actions
12. Pre-certification assessment
13. Certification audit
ISO/IEC 27001
ISO/IEC 27001 certificate
14. Party on!
Plan project
Project plan
Develop Internal ISMS Audit Plan
Internal ISMS Audit proc
Preventive Action Procedure
Information Security Metrics
Controls Documentation
7. ISMS implementation program
ISMS Operating Procedures
Corrective Action Procedure
Records Control Procedure
Key
Mandatory document
ISO/IEC standard
PLAN
DO
ACT
CHECK
NR R&D

# Risk Mgmt, ISMS and QA relationship

| Risk Management | ISMS | Quality Assurance |
| --- | --- | --- |
| ► Legal | ► Legal Compliance | ► Requirements |
| ► Social | ► Security Risk Assessment & management | ► Quality Management |
| ► Financial | | |
| ► Development | ► Policy and organisation | ► Organisation |
| ► Operational | ► Human resources | ► Human resources |
| | ► Classification and assets | ► Business processes |
| | ► Security Controls | ► QA routines |
| | ► Monitor policy compliance | ► Monitor performance |
| | ► Corrective Actions | ► Revise system |

ISMS

# ICT Security & Privacy Vulnerabilities

E.g. for “Home Computer” protection (from cert.org)

- Task 1 - Install and Use Anti-Virus Programs
- Task 2 - Keep Your System Patched
- Task 3 - Use Care When Reading Email with Attachments
- Task 4 - Install and Use a Firewall Program
- Task 5 - Make Backups of Important Files and Folders
- Task 6 - Use Strong Passwords
- Task 7 - Use Care When Downloading and Installing Programs
- Task 8 - Install and Use a Hardware Firewall

Corresponding Vulnerab.

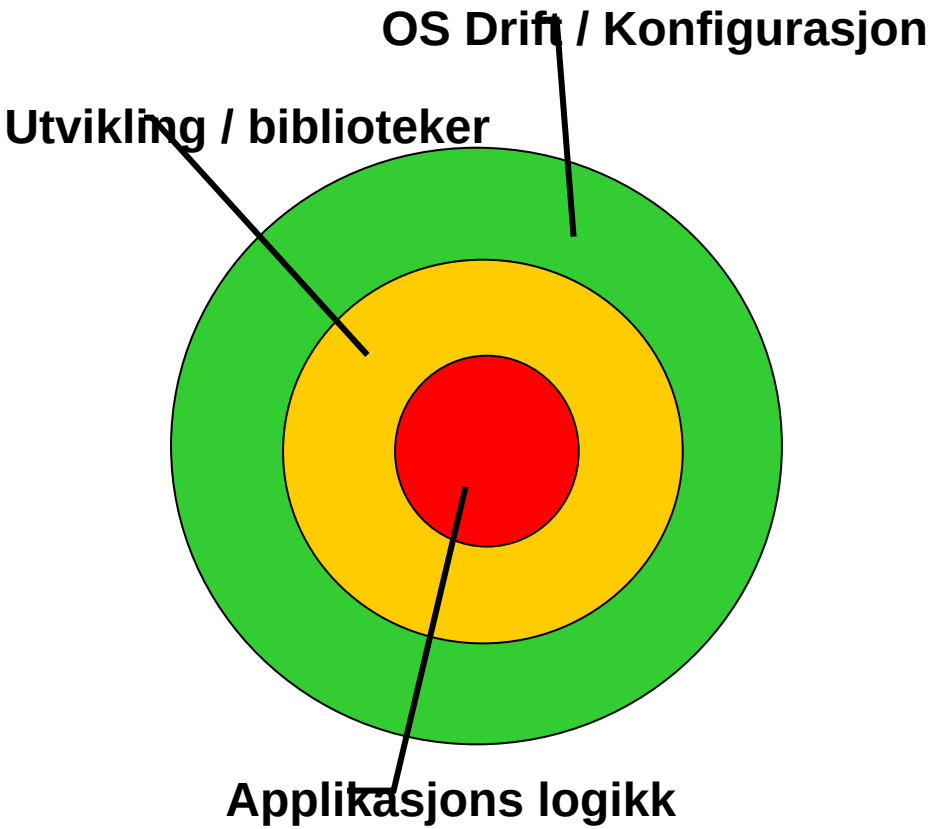
- Errors in SW
- System Mgmt complexity
- Social engineering
- IP faults
- HW errors
- Weak passwords
- Trojan SW
- Network driver errors

# ICT Security & Privacy Vulnerabilities (2)

The OWASP Top 10 Web Application Security Risks for 2010 are:

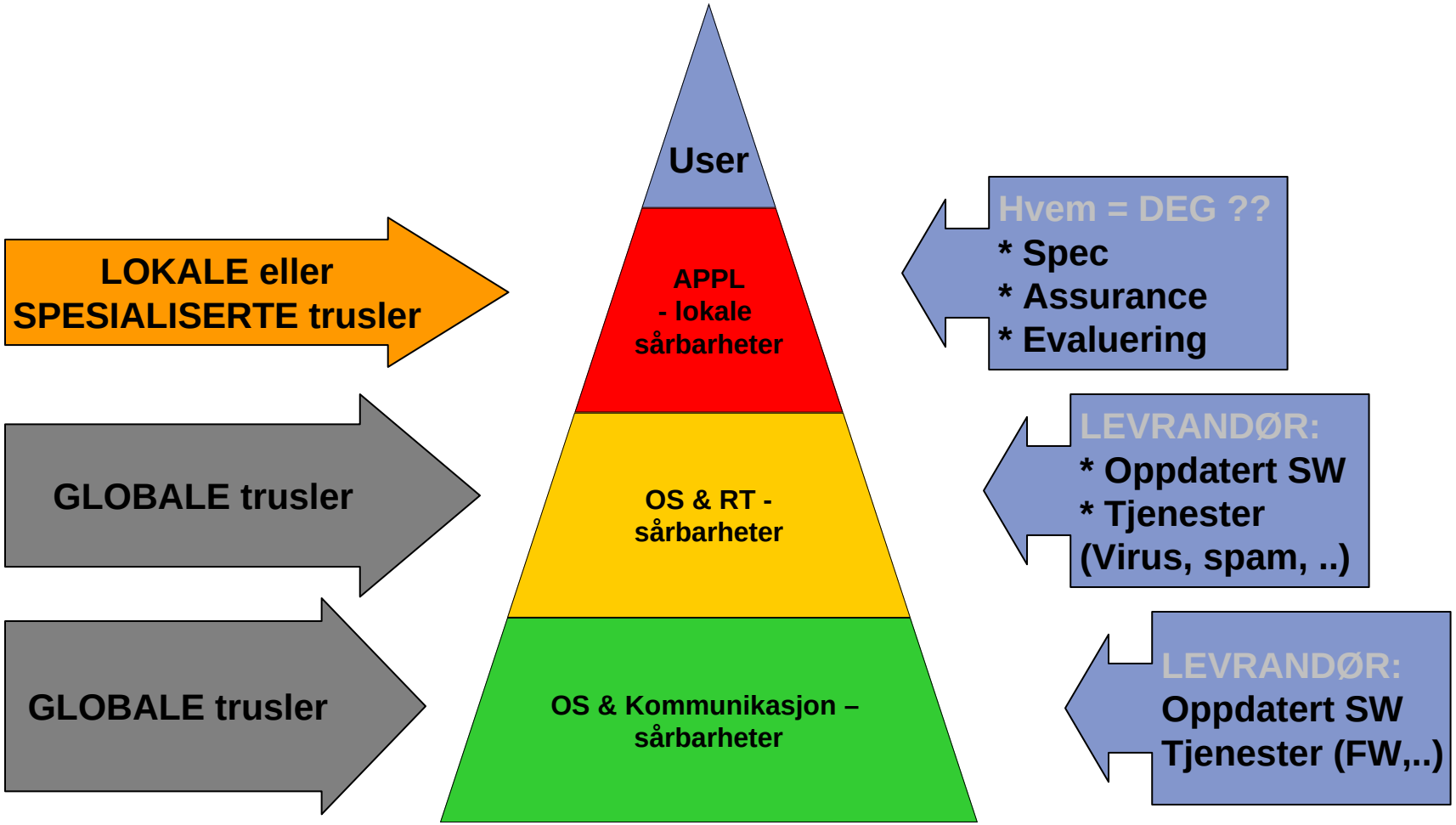
- A1: Injection
- A2: Cross-Site Scripting (XSS)
- A3: Broken Authentication and Session Management
- A4: Insecure Direct Object References
- A5: Cross-Site Request Forgery (CSRF)
- A6: Security Misconfiguration
- A7: Insecure Cryptographic Storage
- A8: Failure to Restrict URL Access
- A9: Insufficient Transport Layer Protection
- A10: Unvalidated Redirects and Forwards

# What is changing in IS security?




| Komponent | Sikkerhet / Kvalitet |
|---|---|
| OS | OK ? |
| Utvikling | Variabel |
| Applikasjon | Dårlig ? |

# What is changing ? (2)



# What else is changing?

- Regulation
- Organisations
- Systems (purchase, develop, outsource, ….)

… so handling changes is what we should worry about (?)

… and if so, then security **monitoring** and **adaptive** solutions becomes **important !**

- Questions ?

- Thank you for your attention

e-mail: asmund.skomedal@nr.no