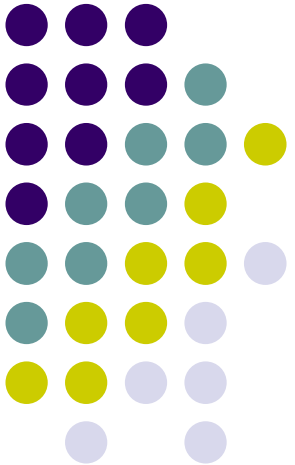
Information Security Management

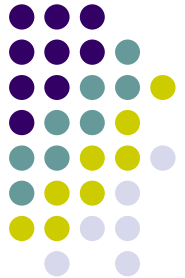
M.Reza Sohizadeh A.

7 May 2009

Reza.Sohizadeh@ii.uib.no



Outline



- Information
- Information Security
- Information Security Management
- Information Security Management System
- ISMS Standard
- ISMS Approach and Traces
- Conclusion

What is Information?

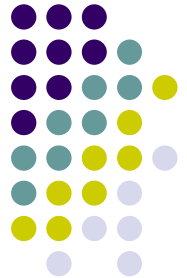
- **Information:** is an asset that, like other important business assets, is essential to an organization's business and consequently needs to be suitably protected. (ISO/ IEC 17799)

- **Asset:** Anything that has value to the organization

Can exist in many forms:

- data stored on computers
- transmitted across networks
- printed out
- written on a paper
- sent by fax
- stored on disks
- held on microfilm
- spoken in conversations over the telephone

Information Security



Preservation of

Confidentiality :

- Ensuring that information is available to only those authorized to have access.

Integrity :

- Safeguarding the accuracy and completeness of information & processing methods.

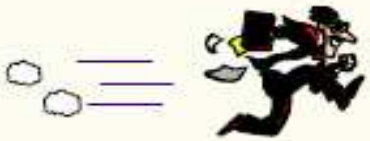
Availability :

- Ensuring that information and vital services are available to authorized users when required.

- Other practices such as authenticity, accountability, non-reputation and reliability can also be involved.

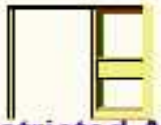
Information Threats

High User knowledge of IT sys.

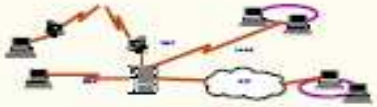


Theft , Sabotage, Misuse, Hacking

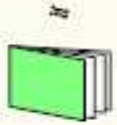
Version Control Problems



Unrestricted Access



Systems / Network Failure



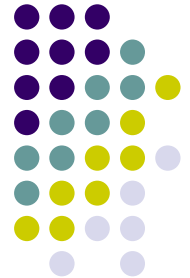
Lack of documentation

Virus

Natural calamities

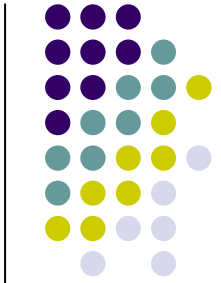
Fire

Information Security



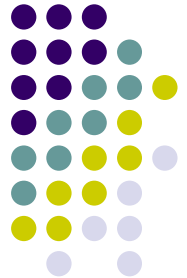
- Information Security is about protecting Information through selection of appropriate Security Controls to:
  - Protects information from a range of threats
  - Ensures business continuity
  - Minimizes financial loss
  - Maximizes return on investments and business opportunities

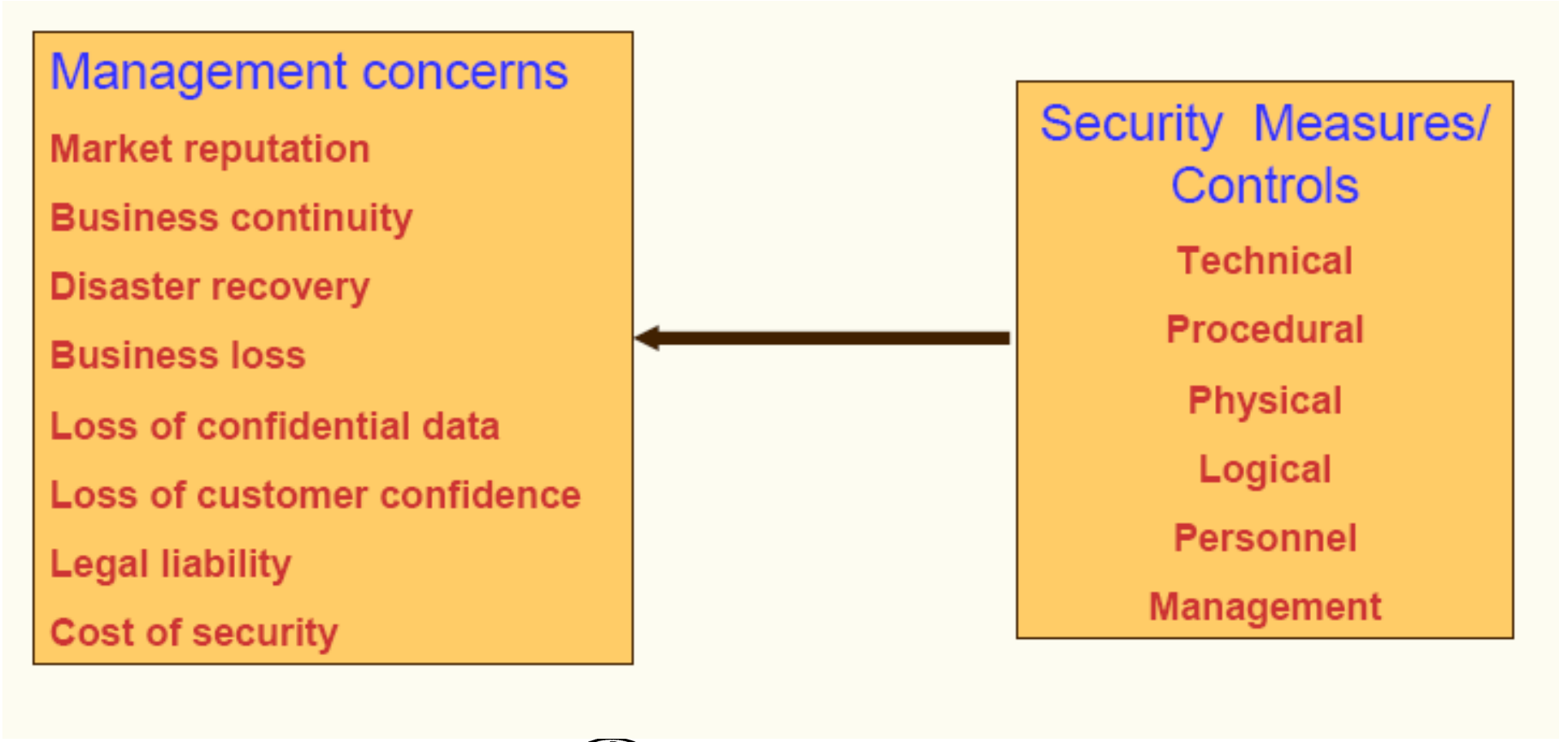
The Challenge is



- Provision and demonstration of secure environment to clients
- Managing security between projects from competing clients
- Preventing loss of product knowledge to external attacks, internal thefts
- Preventing Leak of confidential information to competition
- Meeting Parent company requirements
- Ease of access to large mobile work force
- Providing access to customers where off site development is undertaken with the client.
- Introduction of new technologies and tools
- Managing Legal Compliance
- Managing costs Vs risk

What is needed? (Information Security Management)





Where to start?

Access Control

Confidentiality

Integrity

Availibility

People

?

Privacy

Risk

Authentication

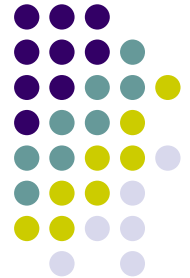
Law, Compliance

Policy

Common Criteria

Cryptography

Why Information Security Management System?



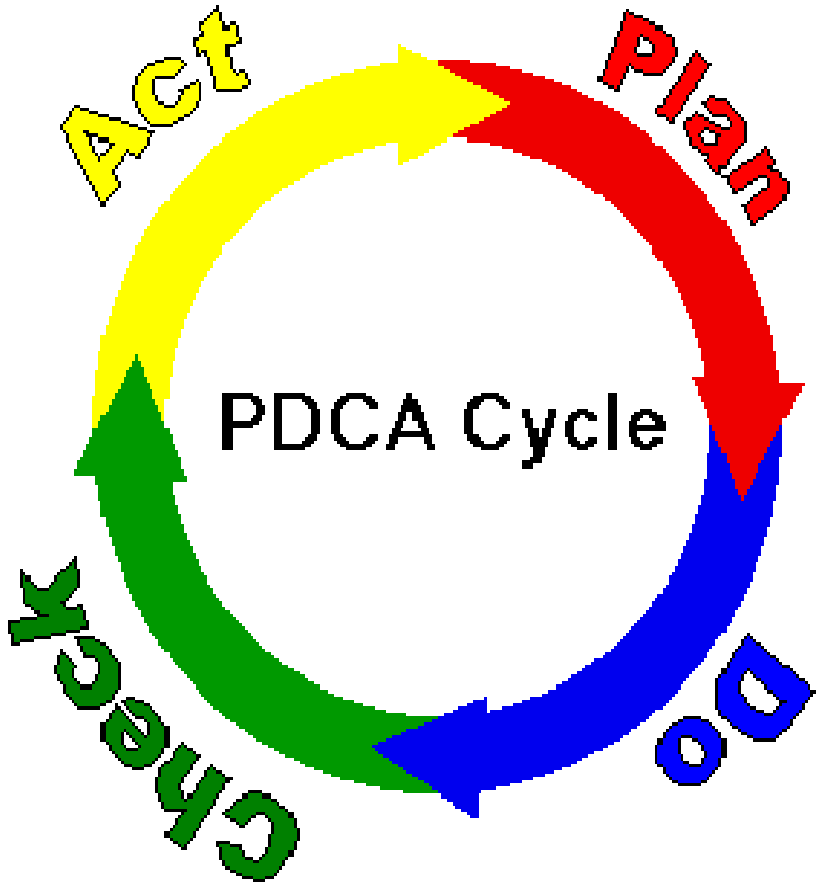
- Information security that can be achieved through technical means is limited.
- Security also depends on people, policies, processes and procedures.
- Resources are not unlimited.
- It is not a once off exercise, but an ongoing activity.
- *All these can be addressed effectively and efficiently only by establishing a proper Information Security Management System (ISMS)*

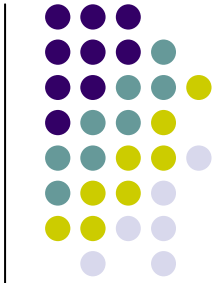
Information Security Management System

With an ISMS we are not intending to make the system '**hacker proof',** but develop a mechanism which can, to a large extent:

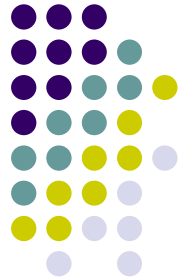
- Anticipate potential problems
- Prepare through proactive measures
- Protect against considerable damage
- Ensure recovery and restoration

Information Security Management System





PLAN	Policy,Organization, Risk Assesmet
DO	Selecting and Implementing Security Controls,Risk Management
CHECK	Check if The implemented controls are working properly and effectively (Metrics)
ACT	If not, what should be done and do it. • Preventive Actions Awareness and training • Corrective Actions

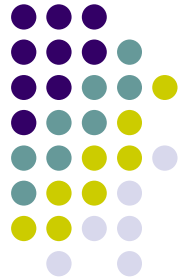


- Don’t you think that a standard approach may help?

  - ISO/IEC 27001:2005, NIST SP 800x

ISO27001/ISO17799/BS7799: History

ISO 2700x Family



27000 Fundamentals & Vocabulary

27005:2008

Risk Management

27001:2005 ISMS

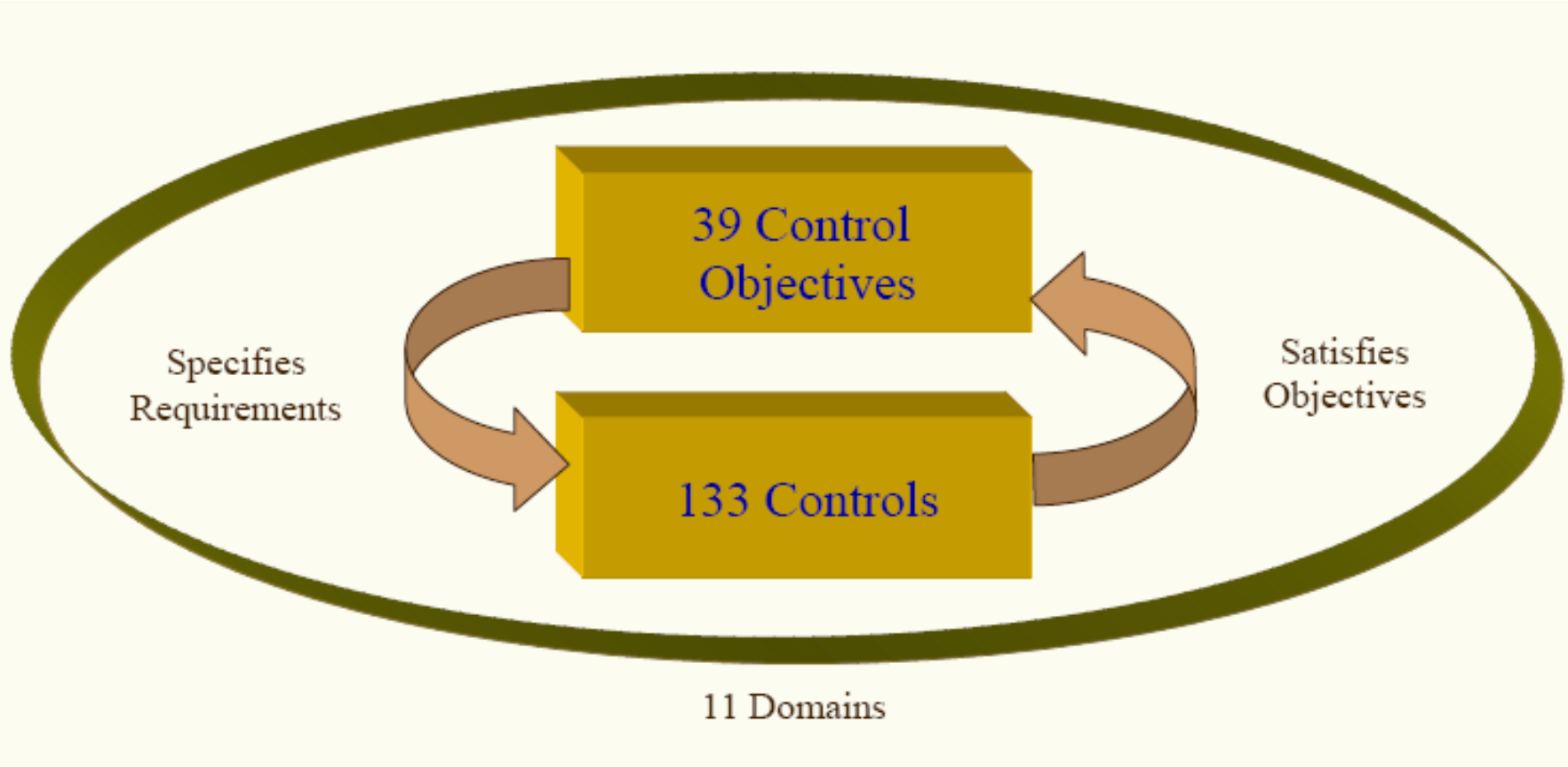
27002 Code of Practice for ISM

27003 Implementation Guidance

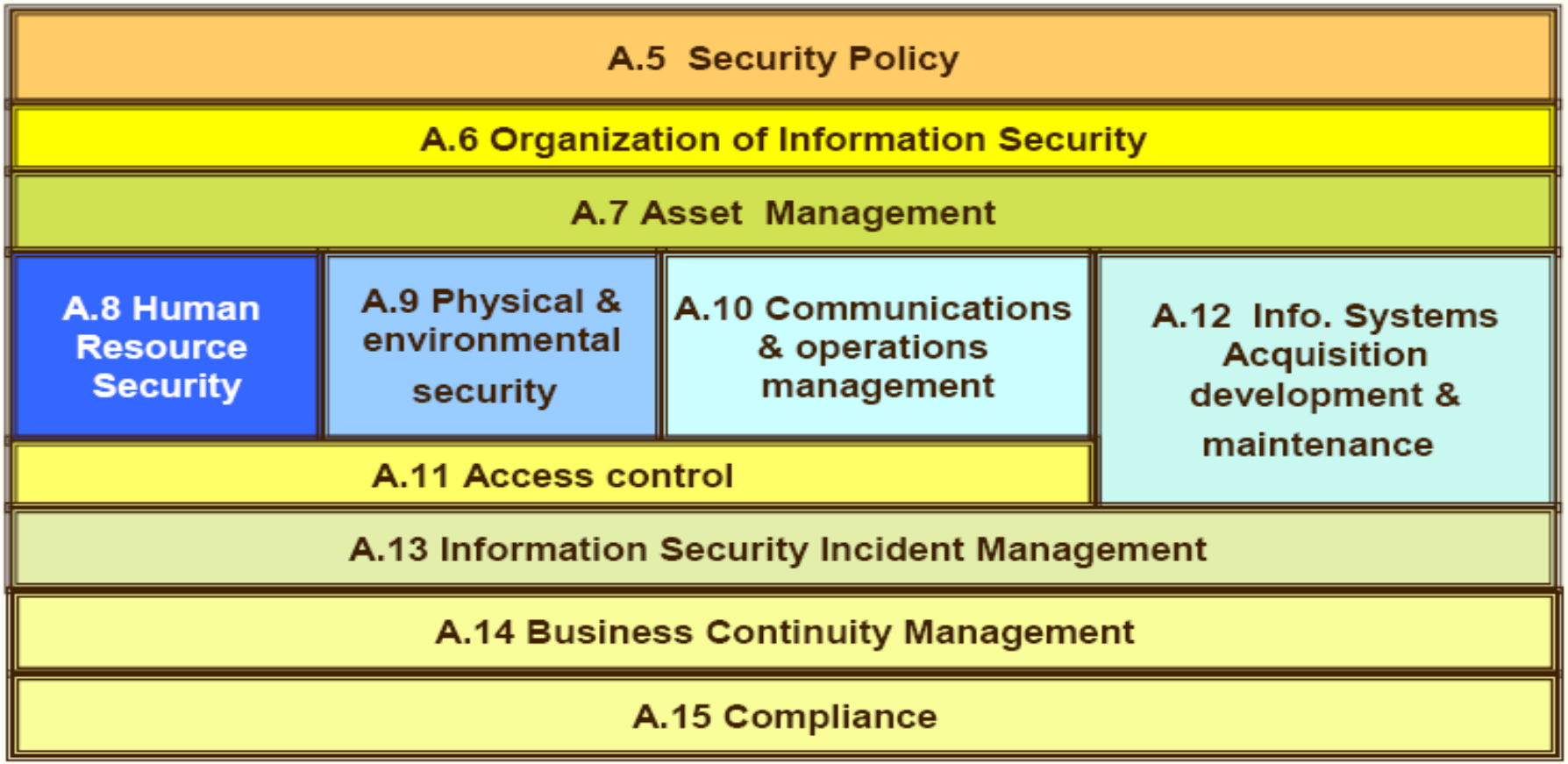
27004 Metrics & Measurement

27006 Guidelines on ISMS accreditation

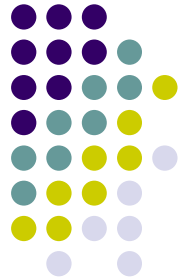
Overview of ISO/IEC27001:2005



ISO/IEC 27001:2005 Domains

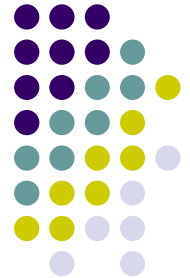


CONFIRMED / SCHEDULED



- ISO27000 - Information technology: Information security management systems, Overview and vocabulary
  ISO27007 - Guidelines for Information Security Management Systems Auditing
  ISO27008 - Guidelines for ISM auditing with respect to security controls (approved April 2008)
  ISO27011 - Information technology: Information security management guidelines for telecommunications
  ISO27799 - Health Informatics: Information security management in health using ISO/IEC 17799

UNCONFIRMED / NOT YET SCHEDULED



ISO27010 ISM Guidelines for Sector-Sector Working and Communications

ISO27031 ICT Readiness for Business Continuity

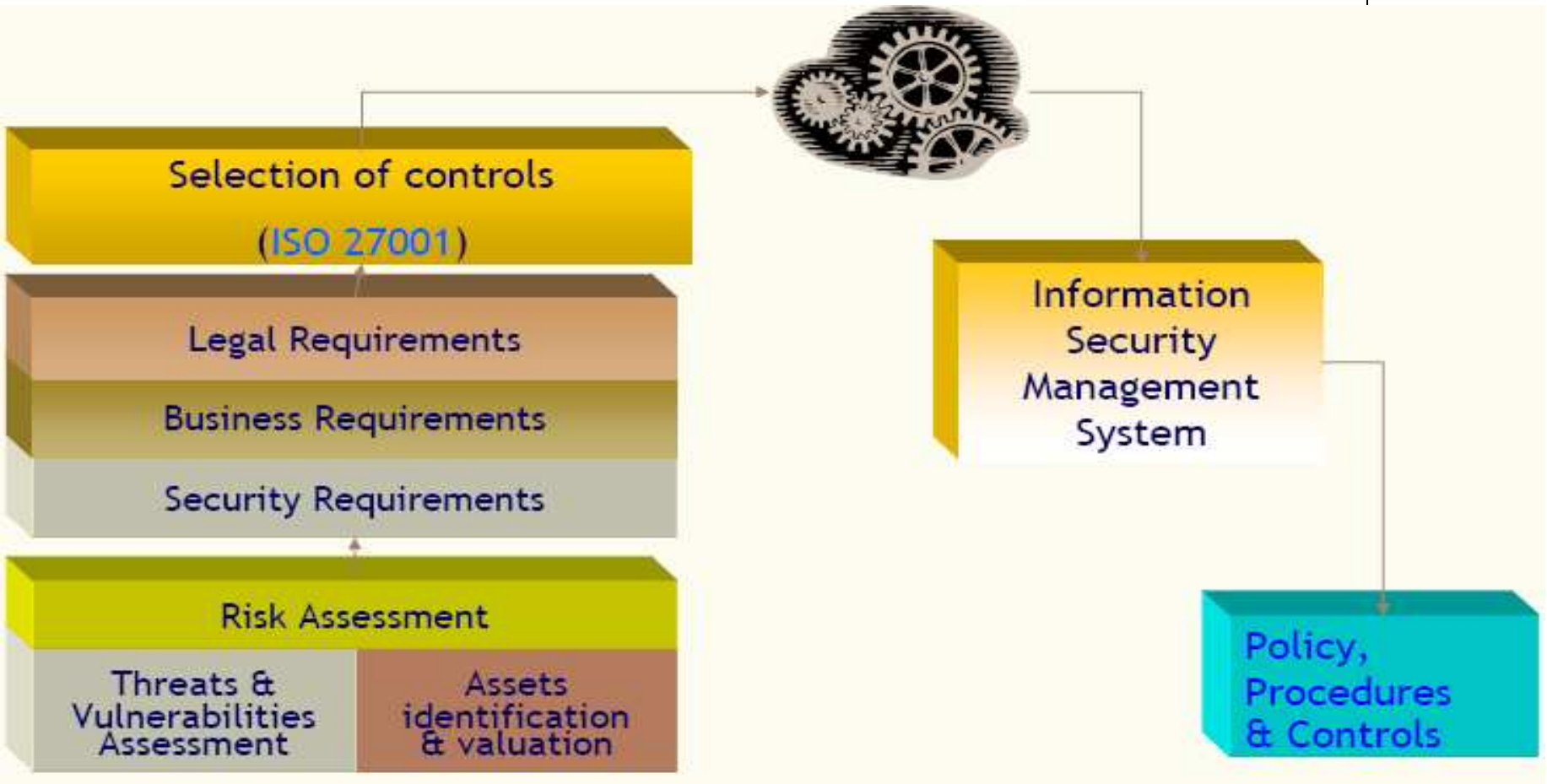
ISO27032 Cyber Security

ISO27033 Network Security / Intrusion Detection (to replace ISO 18028)

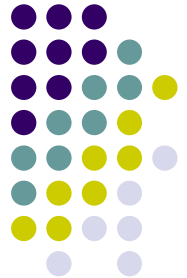
ISO27034 Guidelines for application security

ISO27051 Telecommunications (ITU-T)

How the system works?

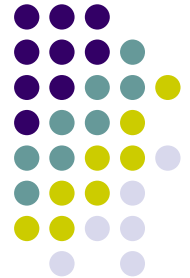


Risk Assesment



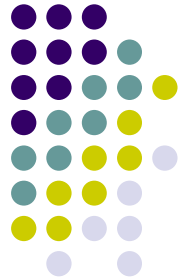
- Risk analysis refers to the processes used to evaluate those probabilities and consequences, and also to the study of how to incorporate the resulting estimates into the decision-making process.
- The risk assessment process also serves as a decision-making tool, in that its outcomes are used to provide guidance on the areas of highest risk, and to devise policies and plans to ensure that systems are appropriately protected.

Risk Assesment

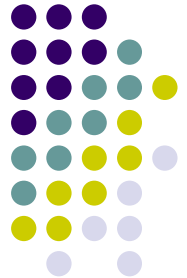


- a) What can go wrong?
- b) What is the likelihood of it going wrong?
- c) What consequences would arise?

Risk Management

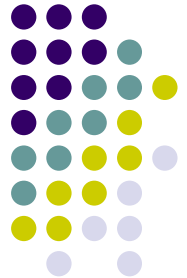


- Often, this is followed by risk evaluation, risk acceptance and avoidance, and risk management, according to the following questions:
- a) What can be done?
- b) What options are available, and what are their associated trade-offs in terms of cost, benefits, and risks?
- c) What impact do current management decisions have on future options?
- d) What are the priorities?



- **Is this system just for business purpose?**

CIIP in Norway

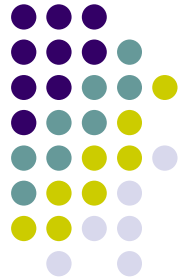


- In 1998, the State Secretary Committee for ICT formed a subcommittee with a mandate to report on the status of ICT vulnerability efforts in Norway.

- Furthermore, the importance of CIIP is also stressed by the Defense Review and the Defense Policy Commission 2000.

- In the aftermath of attacks in the US on 11 September 2001, the government considered it necessary to increase national safety and security, particularly within civil defense, in the Police Security Service, and in emergency planning within the health sector

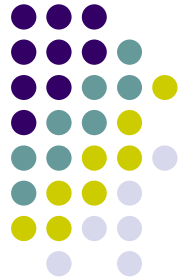
CIIP in Norway



- The Norwegian government published a national strategy for securing ICT systems in Norway in June 2003.

- The strategy involved all aspects of ICT security, ranging from security for individuals, businesses, and the daily activities of the government to the security of IT-dependent critical infrastructure.

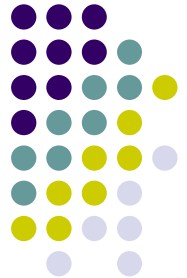
CIIP in Norway



- As a result of the recommendations of the strategy, the NorCERT, NorSIS, and KIS organizations were established.

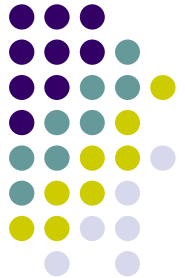
- In 2007, this was supplanted by the National Guidelines to Strengthen Information Security, 2007–2010.

CIIP in Norway



- Directorate for Civil Protection and Emergency Planning (DSB). 4(Risk Assesment), A.14(BCP)
- National Security Authority (NSM) A.13(IRP)
  - SERTIT
  - NorCERT
- The National Information Security Co-ordination Council (KIS) 5(Management Resp.),6(Audit) ,7(Review)
- Norwegian Post and Telecommunications Authority (NPT)—A.10,A.11,A.12
- Norwegian Center for Information Security (NorSIS)A.8(Awarenesss and Training)

Security Operation Center Outputs/ISMS



- Security monitoring for risk management **(ISO/IEC 27005)**
- Security posture risk analysis **(ISO/IEC 27005)**
- Secure role-based portal access **(A.11 ISO 27001)**
- Real-time monitoring and status of incidents and tickets

(A.10.10 ISO 27001)

- Security policy reports **(A.5 ISO 27001)**
- Real-time assessment per incident as well as weekly and monthly reports **(A.13 ISO 27001)**
- Security incident reports **(A.13 ISO 27001)**
- Information required to prepare a compliance audit

(A.15.3 ISO 27001)

- Evidence of security policy compliance

(A.15.2 ISO 27001)

- Trends of security incidents and events

(A.13.2 ISO 27001)

Conclusion

Access Control(A.11)

Confidentiality(A.12) Integrity(A.12)

Availibility(A.12) People(A.8)

Privacy(A.15) Risk(4)

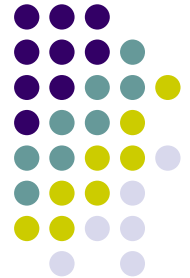
Authentication(A.11)

Law, Compliance(A.15)

Policy(A.5)

Common Criteria (complementery Standard)

Cryptography(A.12.3)



Question?