

Managing Information Security

Gunnar Boe

Section Manager Campus Network and Systems

UNINETT, Norwegian NREN

EUNIS 2011

Dublin, 16 June 2011

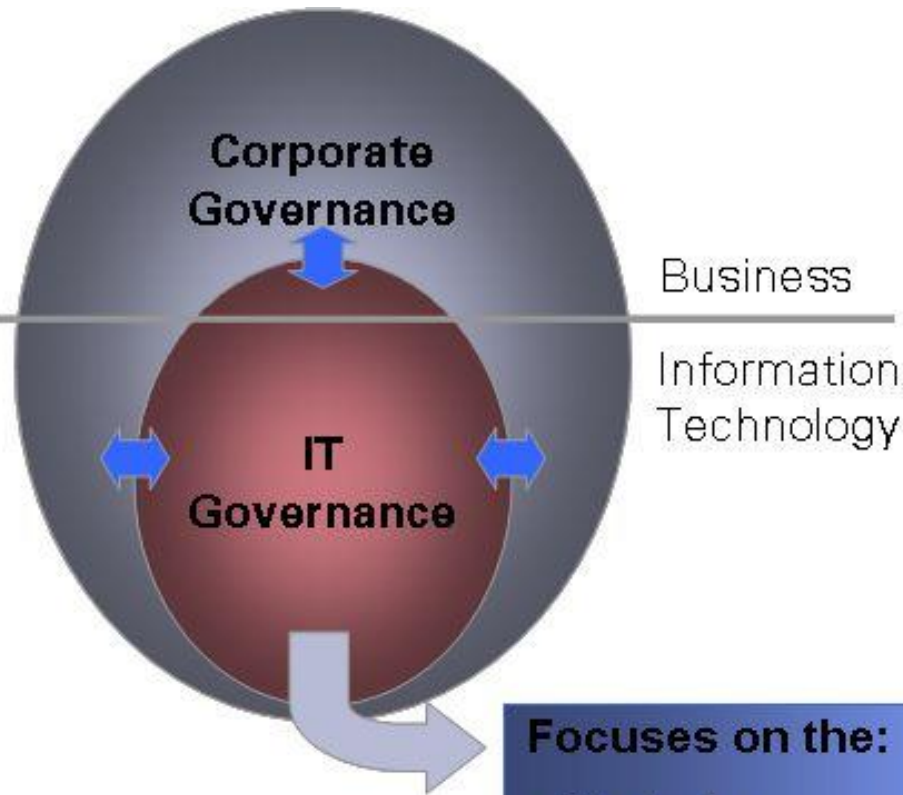
Overview



- 1. Background**
- 2. Information security and its drivers**
- 3. IS Audit**
- 4. General experience of higher education sector**
- 5. Security Policy**
- 6. Further work**

- UNINETT have done a lot of work with Norwegian higher education institutions on technical security for many years
- The IT departments are de facto responsible for Information security, and the solutions have evolved from an exclusively technical point of view
- No clear strategy and no specific goals for information security.
- The lack of involvement and commitment from the upper management has lead to the implementation of arbitrary security measures in many organisations.

- UNINETT has added focus on information security and policy for the Norwegian higher education sector
- UNINETT has prepared a "package" including
 - IS Audit
 - Security Policy, including "basic package"
 - Options:
 - Routines and procedures
 - Risk and Vulnerability Assessments
 - Business Continuity Plans (BCP)



IT Governance is the glue between business processes and involved IT support functions, and in the same time the structure of the IT function itself

- Focuses on the:**
- Strategies,
 - organizational structures,
 - policies, and
 - internal processes

- Necessary within the IT function to:**
- Control risks,
 - achieve regulatory compliance,
 - measure performance, and
 - deliver value

What is Information Security?



- Systematic use of information security management system (ISMS) to protect business information and information systems, physical security and personnel security.
 - Confidentiality (information is only available to those who should have access)
 - Integrity (information is accurate and complete)
 - Availability (information is available within the requirements set)
- Risks - in general
 - Conditions or events may occur and affect the achievement of objectives.
 - Frequency and severity
 - All information systems have vulnerabilities that can be exposed to threats.

- Regulatory requirements
- Business requirements
- Actual threats
- Technology

- One-day on-site audit / review
- Start-up meeting with executive/top management (Important!)
- Interviews with key personnel
- Review of the received documentation
- Prepare report

A typical agenda for IS Audit / Security Assessment - 0900-1600



#	Theme	Priority / Discussion	Interview - Person	Time
1	<u>Start-up Meeting.</u>	Review of agenda, Introduction Talk (Info. Sec), Interview	The organization's management	0830- 0930
2	<u>Risk Management</u>	Framework, RVA	Security Manager and Management	0930-10
3	<u>Organization of security</u>	Security Org., Documentation, Security Policy and Standards Roles / responsibilities, IT strategy	Security Manager and Management	
4	<u>Classification and security of data</u>	Responsibility, Classification of info. class model	Security Manager and IT manager	
5	<u>Personnel Security</u>	Security training and attitudes, AUP and conf. agreements, Security Reporting, Job descriptions, Disciplinary sanctions, etc.	Human Relations dept.	1000-1030
6	<u>Physical and environmental security</u>	Physical Sec. zone & access control, Securing assets, Safe disposal, etc.	HSE manager	1030-1100
7	<u>Communications and operations management</u>	Change mgt. Netw. Design, FWs, Variance Reporting, DNS, Proxy, etc.etc.	IT manager / system administrator	1100- 1300 Incl. Lunch
8	<u>Access control</u>	Windows, Linux env. etc	IT manager / system administrator	1300-1400
9	<u>System Development and Maintenance</u>	Version control, change mgt., dev. & staging environment, etc.	IT Operations	1400-1430
10	<u>Continuity Planning</u>	RVA / BIA, BCP Plan, Internal KPIs	Management, IT & HSE mgr.	1430-1530
11	<u>Compliance</u>	Regulatory comp. Policy compliance (ev)	Management, IT & HSE mgr.	1530-1545
12	<u>Final meeting</u>	All - as in the initial meeting. Re-view of findings and further work	All	1545-1600

- The key?

- Management involvement

Three core areas



- ISO 27001/27002:
Strong on security, but does not say how it should work
- Control Objectives for Information and Related Technology (COBIT) by ISACA:
Strong in IT controls and parameters, and security. Provides alignment between business goals/financial goals objectives and planning of policy, procedure and process for IT
- Information Technology Infrastructure Library (ITIL): Strong in IT processes, but limited in security and system development. ITIL is focused on Service Delivery.

§ /Norwegian Personal Data Act - Section 13 Data security

The confidentiality, integrity and accessibility of personal data shall be ensured by means of planned and systematic measures, satisfactory data.

The data system and the security measures shall be documented.

→ Policy

Within EU the following directives regulate many aspects related to information security:

- Directive 95/46/EC (Data Protection Directive)
- Directive 2002/58/EC (the E-Privacy Directive)
- Directive 2006/24/EC Article 5 (The Data Retention Directive)

Benefits of an structured approach



- Provides an essential overview of the risks
- Reduces the risk of adverse events (*Discrepancies*)
- Identify appropriate control measures, which should be:
 - cost-effective
 - easy to manage
 - easy to implement
 - meet the security requirements
 - Helping to secure what is important!

A structured approach to security, based on relevant policies and procedures, helps the institution achieve its goals!

Trends

- Information is more valuable than ever
- Networks are critical infrastructure
- e-mail more and more business critical
- **ID theft**
- **Attacks faster than patches** (zero day)
- **end-users represent a risk**
- targeted attacks
- **organized crime**

The relevant threats are identified through risk assessment

<http://www.sans.org/top20/>

<http://www.gocsi.com/>

<http://www.cert.org/analysis/>

Typical IS audit conclusions



- The technical security of the existing solutions is mostly satisfactory, and provides relevant security against traditional threats.
- A Data Inspectorate audit would have resulted in clear orders that would have to be fulfilled within six months in line with the recommendations in our report.
- Some essential governing documents are missing, e.g.
 - security policy (incl. security objectives and strategy),
 - IT strategy
 - continuity and contingency plans for IT.
- Outsourcing contracts are inadequate with respect to information security, including missing SLA.

i.e – “The terrain can be good - but the map is missing”

- Computers stolen
- Information astray
- ID theft
- Internal information published
- Loss of reputation
- Unavailability of Administrative systems
- Security and risk level is set at a low level in the organizational activities -> leads to "Armoured steel doors In a picked fence"

IS Audit: Overall recommendations



- **Establish Security Policy** based on ISO 27002, and implement it, including a selection of procedures.
- **Establish** the role of **Chief Security Officer** (CSO) and formally anchor the responsibility for information security in senior management .
- **Perform risk assessment** of systems with personal data with respect to confidentiality, integrity and availability.
- Develop an **overview of the Personal Data** that are processed
- Establish a satisfactory **security architecture** based on the concept of security levels
- **Develop BCP** (Business Continuity and Contingency Plans) for ICT infrastructure.

Security is:

- 80 % attitudes, knowledge, regulative measures, is controlled through → Policy *PEBKAC*
- 20 % technology, is controlled through → Policy, IT-strategy

“Good IT security starts and ends with individuals, not with firewalls, antivirus or IDS systems. One rotten apple can destroy a whole box in no time, and an apple with the crumbling decay rapidly” (Helge Skrivervik, myMAYDAY.com).



Appropriate security?



What is ISO 27001/27002?



- ISO's standard for information security management system (ISMS)
- ISO 27001 specifies how to design a management system for Security (ISMS)
- ISO 27002 is a Code of practice for information security, and define what an ISMS should include

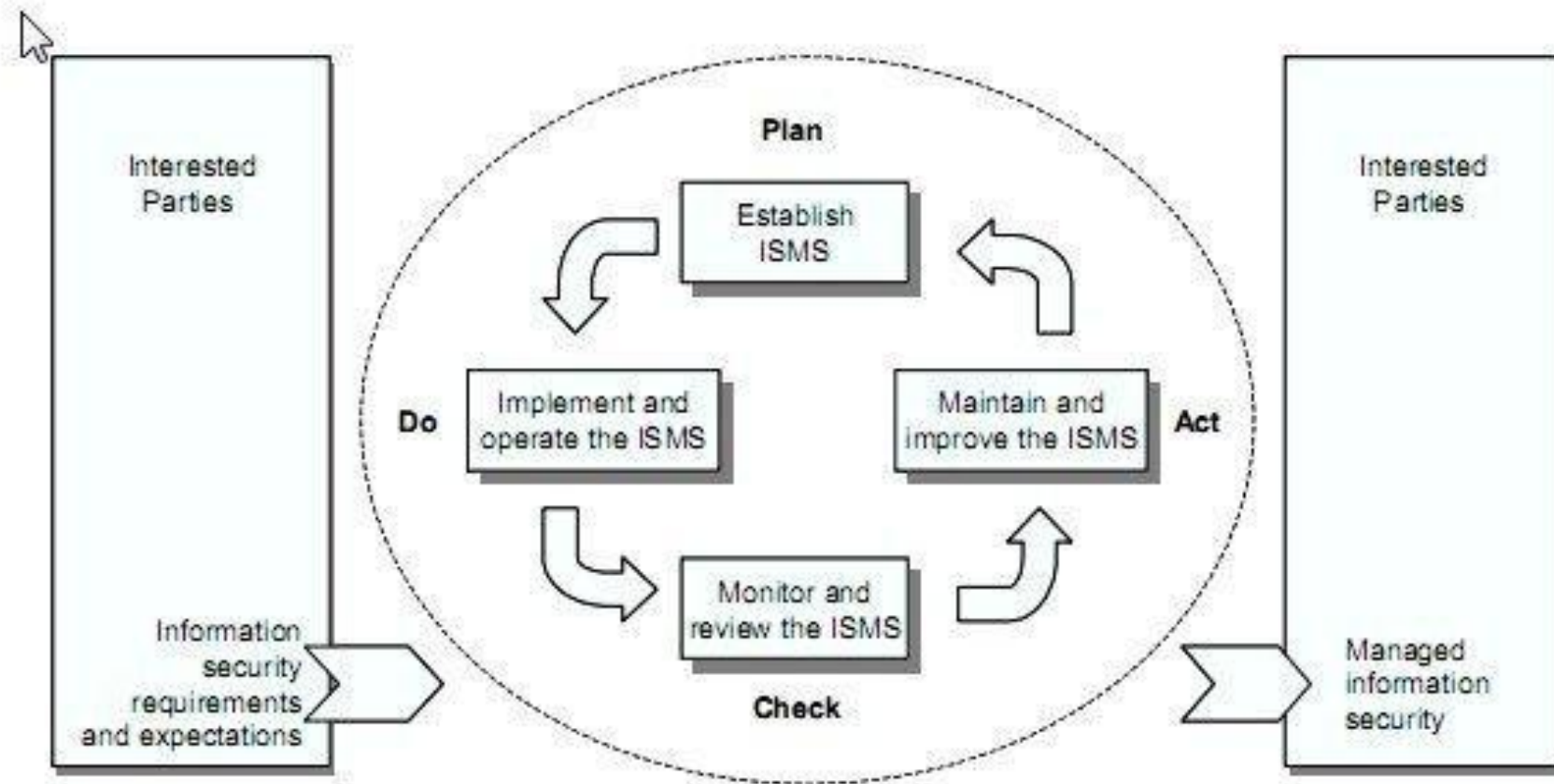


Figure 1 — PDCA model applied to ISMS processes

ISO 27002 in all its cruelty

Some of the contents ...



Contents	Page
FOREWORD	VIII
0 INTRODUCTION	IX
0.1 WHAT IS INFORMATION SECURITY?.....	IX
0.2 WHY INFORMATION SECURITY IS NEEDED?.....	IX
0.3 HOW TO ESTABLISH SECURITY REQUIREMENTS.....	X
0.4 ASSESSING SECURITY RISKS.....	X
0.5 SELECTING CONTROLS.....	X
0.6 INFORMATION SECURITY STARTING POINT.....	X
0.7 CRITICAL SUCCESS FACTORS.....	XI
0.8 DEVELOPING YOUR OWN GUIDELINES.....	XII
1 SCOPE	1
2 TERMS AND DEFINITIONS	1
3 STRUCTURE OF THIS STANDARD	4
3.1 CLAIMS.....	4
3.2 MAIN SECURITY CATEGORIES.....	4
4 RISK ASSESSMENT AND TREATMENT	5
4.1 ASSESSING SECURITY RISKS.....	5
4.2 TREATING SECURITY RISKS.....	5
5 SECURITY POLICY	7
5.1 INFORMATION SECURITY POLICY.....	7
5.1.1 Information security policy document.....	7
5.1.2 Review of the information security policy.....	8
6 ORGANIZING INFORMATION SECURITY	9
6.1 INTERNAL ORGANIZATION.....	9
6.1.1 Management commitment to information security.....	9
6.1.2 Information security co-ordination.....	10
6.1.3 Allocation of information security responsibilities.....	10
6.1.4 Authorization process for information processing facilities.....	11
6.1.5 Confidentiality agreements.....	11
6.1.6 Contact with authorities.....	12
6.1.7 Contact with special interest groups.....	12
6.1.8 Independent review of information security.....	13
6.2 EXTERNAL PARTIES.....	14
6.2.1 Identification of risks related to external parties.....	14
6.2.2 Addressing security when dealing with customers.....	15
6.2.3 Addressing security in third party agreements.....	16
7 ASSET MANAGEMENT	19
7.1 RESPONSIBILITY FOR ASSETS.....	19
7.1.1 Inventory of assets.....	19
7.1.2 Ownership of assets.....	20
7.1.3 Acceptable use of assets.....	20
7.2 INFORMATION CLASSIFICATION.....	21
7.2.1 Classification guidelines.....	21
7.2.2 Information labeling and handling.....	21
8 HUMAN RESOURCES SECURITY	23
8.1 PRIOR TO EMPLOYMENT.....	23
8.1.1 Roles and responsibilities.....	23

ISO/IEC FDIS 17789:2005(E)

8.1.2 Screening.....	2
8.1.3 Terms and conditions of employment.....	2
8.2 DURING EMPLOYMENT	2
8.2.1 Management responsibilities.....	2
8.2.2 Information security awareness, education, and training.....	2
8.2.3 Disciplinary process.....	2
8.3 TERMINATION OR CHANGE OF EMPLOYMENT	2
8.3.1 Termination responsibilities.....	2
8.3.2 Return of assets.....	2
8.3.3 Removal of access rights.....	2
9 PHYSICAL AND ENVIRONMENTAL SECURITY	3
9.1 SECURE AREAS.....	3
9.1.1 Physical security perimeter.....	3
9.1.2 Physical entry controls.....	3
9.1.3 Securing offices, rooms, and facilities.....	3
9.1.4 Protecting against external and environmental threats.....	3
9.1.5 Working in secure areas.....	3
9.1.6 Public access, delivery, and loading areas.....	3
9.2 EQUIPMENT SECURITY.....	3
9.2.1 Equipment siting and protection.....	3
9.2.2 Supporting utilities.....	3
9.2.3 Cabling security.....	3
9.2.4 Equipment maintenance.....	3
9.2.5 Security of equipment off-premises.....	3
9.2.6 Secure disposal or re-use of equipment.....	3
9.2.7 Removal of property.....	3
10 COMMUNICATIONS AND OPERATIONS MANAGEMENT	3
10.1 OPERATIONAL PROCEDURES AND RESPONSIBILITIES.....	3
10.1.1 Documented operating procedures.....	3
10.1.2 Change management.....	3
10.1.3 Segregation of duties.....	3
10.1.4 Separation of development, test, and operational facilities.....	3
10.2 THIRD PARTY SERVICE DELIVERY MANAGEMENT.....	3
10.2.1 Service delivery.....	3
10.2.2 Monitoring and review of third party services.....	4
10.2.3 Managing changes to third party services.....	4
10.3 SYSTEM PLANNING AND ACCEPTANCE.....	4
10.3.1 Capacity management.....	4
10.3.2 System acceptance.....	4
10.4 PROTECTION AGAINST MALICIOUS AND MOBILE CODE.....	4
10.4.1 Controls against malicious code.....	4
10.4.2 Controls against mobile code.....	4
10.5 BACK-UP.....	4
10.5.1 Informative back-up.....	4
10.6 NETWORK SECURITY MANAGEMENT.....	4
10.6.1 Network controls.....	4
10.6.2 Security of network services.....	4
10.7 MEDIA HANDLING.....	4
10.7.1 Management of removable media.....	4
10.7.2 Disposal of media.....	4
10.7.3 Information handling procedures.....	4
10.7.4 Security of system documentation.....	4
10.8 EXCHANGE OF INFORMATION.....	4
10.8.1 Information exchange policies and procedures.....	4
10.8.2 Exchange agreements.....	5
10.8.3 Physical media in transit.....	5
10.8.4 Electronic messaging.....	5
10.8.5 Business information systems.....	5

ISO/IEC FDIS 17789:2005(E)

10.9 ELECTRONIC COMMERCE SERVICES.....	53
10.9.1 Electronic commerce.....	53
10.9.2 On-Line Transactions.....	54
10.9.3 Publicly available information.....	55
10.10 MONITORING.....	55
10.10.1 Audit logging.....	55
10.10.2 Monitoring system use.....	56
10.10.3 Protection of log information.....	57
10.10.4 Administrator and operator logs.....	58
10.10.5 Fault logging.....	58
10.10.6 Clock synchronization.....	58
11 ACCESS CONTROL	60
11.1 BUSINESS REQUIREMENT FOR ACCESS CONTROL.....	60
11.1.1 Access control policy.....	60
11.2 USER ACCESS MANAGEMENT.....	61
11.2.1 User registration.....	61
11.2.2 Privilege management.....	62
11.2.3 User password management.....	62
11.2.4 Review of user access rights.....	63
11.3 USER RESPONSIBILITIES.....	63
11.3.1 Password use.....	64
11.3.2 Unattended user equipment.....	64
11.3.3 Clear desk and clear screen policy.....	65
11.4 NETWORK ACCESS CONTROL.....	65
11.4.1 Policy on use of network services.....	66
11.4.2 User authentication for external connections.....	66
11.4.3 Equipment identification in networks.....	67
11.4.4 Remote diagnostic and configuration port protection.....	67
11.4.5 Segregation in networks.....	68
11.4.6 Network connection control.....	68
11.4.7 Network routing control.....	69
11.5 OPERATING SYSTEM ACCESS CONTROL.....	69
11.5.1 Secure log-on procedures.....	69
11.5.2 User identification and authentication.....	70
11.5.3 Password management system.....	71
11.5.4 Use of system utilities.....	72
11.5.5 Session time-out.....	72
11.5.6 Limitation of connection time.....	72
11.6 APPLICATION AND INFORMATION ACCESS CONTROL.....	73
11.6.1 Information access restriction.....	73
11.6.2 Sensitive system isolation.....	74
11.7 MOBILE COMPUTING AND TELEWORKING.....	74
11.7.1 Mobile computing and communications.....	74
11.7.2 Teleworking.....	75
12 INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE	77
12.1 SECURITY REQUIREMENTS OF INFORMATION SYSTEMS.....	77
12.1.1 Security requirements analysis and specification.....	77
12.2 CORRECT PROCESSING IN APPLICATIONS.....	78
12.2.1 Input data validation.....	78
12.2.2 Control of internal processing.....	78
12.2.3 Message integrity.....	79
12.2.4 Output data validation.....	79
12.3 CRYPTOGRAPHIC CONTROLS.....	80
12.3.1 Policy on the use of cryptographic controls.....	80
12.3.2 Key management.....	81
12.4 SECURITY OF SYSTEM FILES.....	83
12.4.1 Control of operational software.....	83
12.4.2 Protection of system test data.....	84



Security put in system



1	INFORMATION SECURITY POLICY	4
1.1	SECURITY GOALS	4
1.2	SECURITY STRATEGY	
2	ROLES AND AREAS OF RESPONSIBILITY	
2.1	ROLES AND RESPONSIBILITIES	
3	PRINCIPLES FOR INFORMATION SECURITY AT <X> UNIVERSITI	
3.1	RISK MANAGEMENT	
3.2	INFORMATION SECURITY POLICY	
3.3	SECURITY ORGANIZATION	
3.4	CLASSIFICATION AND CONTROL OF ASSETS	
3.5	INFORMATION SECURITY IN CONNECTION WITH USERS	
3.6	INFORMATION SECURITY REGARDING PHYSICAL CONDITIONS	
3.7	IT COMMUNICATIONS AND OPERATIONS MANAGEMENT	
3.8	ACCESS CONTROL	
3.9	INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTEN.	
3.10	INFORMATION SECURITY INCIDENT MANAGEMENT	
3.11	CONTINUITY PLANNING	
3.12	COMPLIANCE	
4	GOVERNING DOCUMENTS FOR SECURITY WORK	
4.1	PURPOSE OF GOVERNING DOCUMENTS	
4.2	DOCUMENT STRUCTURE	
5	DEFINITIONS	
6	REFERENCES	
6.1	INTERNAL REFERENCES	
6.2	EXTERNAL REFERENCES	21

■ Inspectorate often get questions about how the company I can adapt to the Data Inspectorate's requirements for information security. Among other ,it is Asked about the relationship with ISO standards. The regulation is based on ISO standards . Chapter 2 of the Personal Data Regulations (The Information Security chapter) is based on and *have the same systematics as the ISO standard 17799*. The standard is more exhaustive and is another useful tool for enterprises. The standard series consist of two parts. The first part is translated into Norwegian. The standard can be obtained by contacting Pronorm.

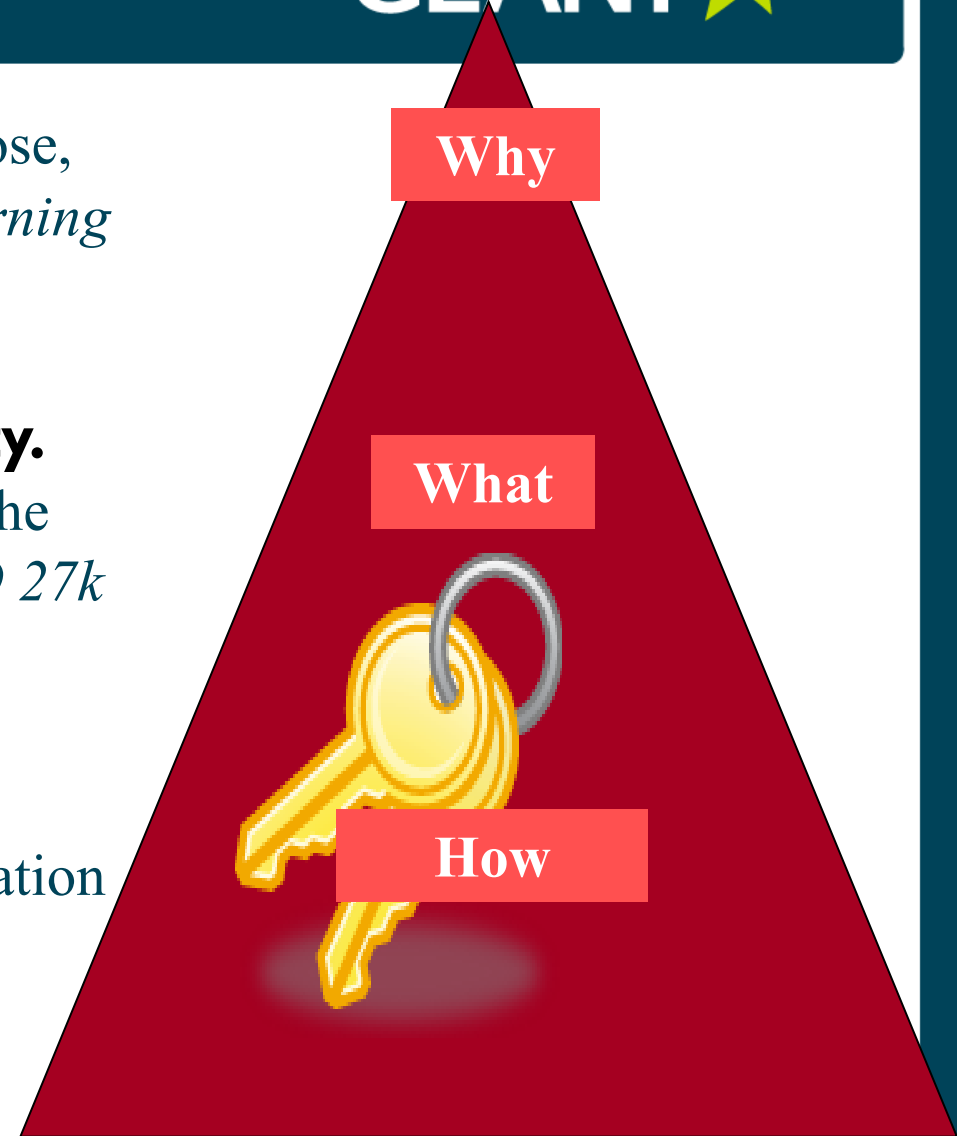
nal data

Security with a system – document structure

1) Security Policy defines the goals, purpose, responsibility and overall requirements. *Governing document*

2) Guidelines for information security. Defines what should be done to comply with the established policy. *Governing document – ISO 27k structure*

3) Standards and procedures Contain detailed guidelines for the implementation of security. *Accomplishing and controlling documents*



A security policy must

- *be possible to implement and enforce*
- *be concise and easy to understand*
- *balance protection with productivity*
- express why it is established
- describe what it covers
- define the responsibilities and contact points
- *specify how the violations will be handled*

Roadmap - implementing policy



Process for implementation of security policy

1. Draft of policy before workshop → version 0.7
 2. Policy workshop → version 0.8

 1. Internal treatment in the management → version 0.9
 2. Approval of the Board → version 1.0
 3. Policy comes into force; publishing, information, training
 4. Revision Process for 6-12 months
- CSO is the process responsible, IT director is secretary

Achieved results



Our achievements in the sector include

Phase I:

- 85% of the institutions covered with IS Audit
- 60% of the institutions have implemented IS Policy

Phase II

Assisting the institutions with

- Risk assessments
- Business Impact Assessments
- Developing BCP

Remember:

Security is not difficult, but challenging. It is not a project but a process. And it never ends, but is continuously evolving. (Helge Skrivervik
– myMAYDAY.com)

- ... a risk-controlled approach ...



At last



- <http://www.isaca.org>
- <http://www.iso.org>
- <http://www.datatilsynet.no>

kenneth.hostland@uninett.no



THANK YOU
FOR YOUR ATTENTION!



Questions?



GEANT3 NA3 Task 4: Campus Best Practice

- http://www.geant.net/About_GEANT/Campus_Best_Practice/Pages/home.aspx
- <http://http://www.terena.org/activities/campus-bp/>
- gn3campus@uninett.no

- Look out for more BPDs coming along...
- Subscribe to announcements
 - campus-bp-announcements@terena.org