Information Security Management and ISO 27000 certification: the .SE view

Anne-Marie Eklund Löwinder
Security Manager
.SE
amel@iis.se
@amelsec

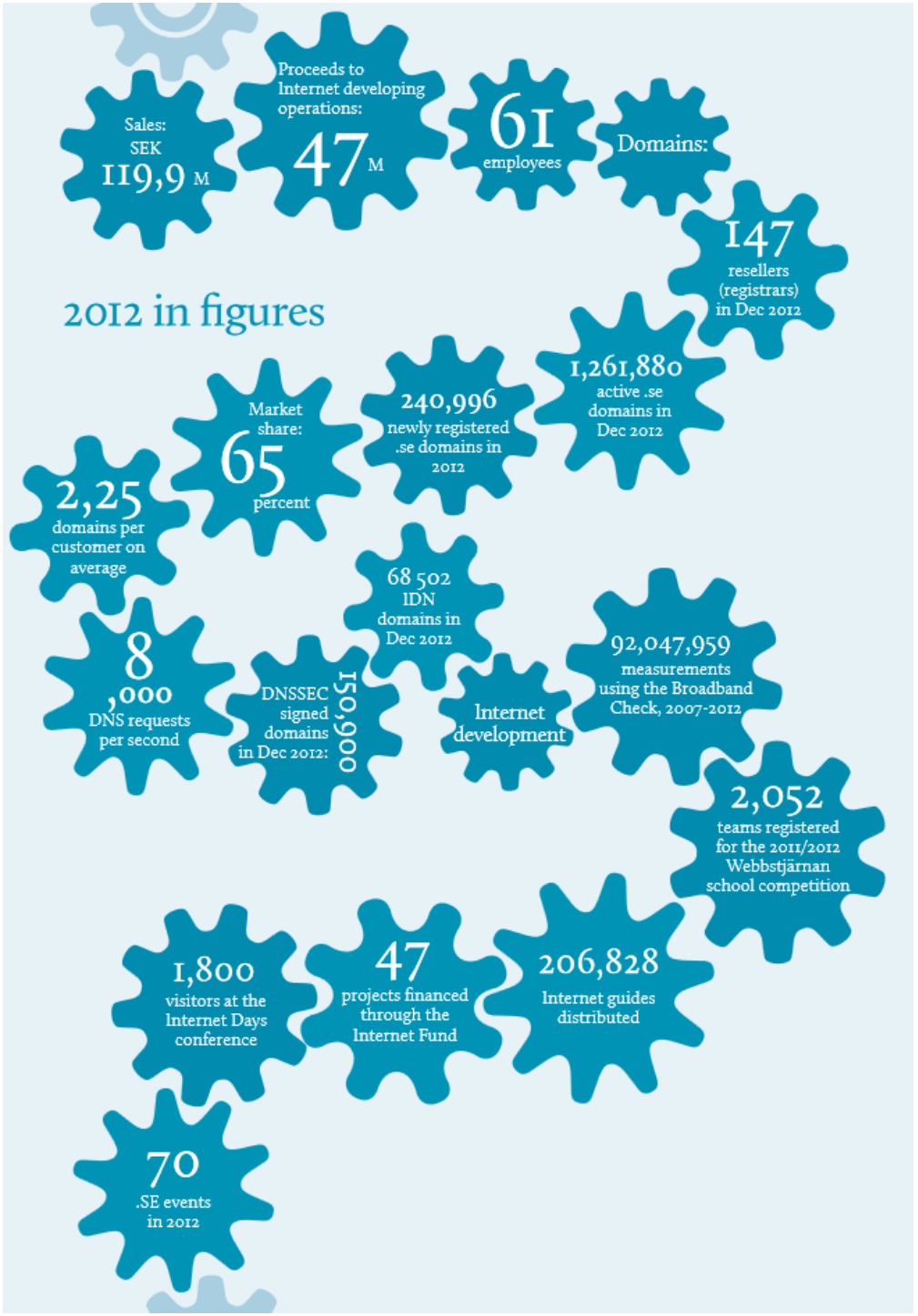
.se

Agenda

- About .SE
- Risk and Information Security Management in a ccTLD.
- ISO 27001, what, how and why?

About .SE

- .SE (The Internet Infrastructure Foundation) is a non-profit organisation.
- A foundation is a legal entity that, in contrast to companies and associations, neither have owners nor members.
- The Foundation is essentially a self-owning financial unit and is governed by its charter of foundation, not by the Swedish Government.


Sales:
SEK
119,9 M
Proceeds to Internet developing operations:
47 M
61
employees
Domains:
147
resellers (registrars) in Dec 2012
2012 in figures
1,261,880
active .se domains in Dec 2012
240,996
newly registered .se domains in 2012
Market share:
65
percent
2,25
domains per customer on average
68 502
IDN domains in Dec 2012
8
,000
DNS requests per second
DNSSEC signed domains in Dec 2012:
150900
Internet development
92,047,959
measurements using the Broadband Check, 2007-2012
2,052
teams registered for the 2011/2012 Webbstjärnan school competition
1,800
visitors at the Internet Days conference
47
projects financed through the Internet Fund
206,828
Internet guides distributed
70
.SE events in 2012

As a tld we live on trust:

”We are the trustees for the delegated domain, and have the duty to serve the community”.

(IETF RFC 1591)

.se

Information security

- Everyday security in the information society - a matter of skills and knowledge, not luck!
  - Availability
  - Integrity
  - Confidentiality
  - Traceability

.se

Tasks of a TLD registry

1) Domain name resolution service
   answer to requests for name server information.

2) Registration service
   create, delete, transfer, hold domains and update the information.

3) Directory service
   provide Whois information (domain holder, admin & tech contact, ...)

4) Traditional Business service
   billing, customer support, sometimes dispute resolution.

Cred: Wim Degezelle, CENTR secretariat

.se

TLD Registry

1) Domain name resolution service — KEY FUNCTION
   answer requests for name server information

2) Registration service
   create, delete, transfer, hold domains and update the information

3) Directory service
   provide Whois information (domain holder, admin & tech contact, ...)

4) Traditional Business service
   billing, customer support, sometimes dispute resolution

.se

Security Risks

2)
3)
4)

→ regular “business class” security needs.

1) → the domain resolution service is used by most Internet applications and deserves real special attention.

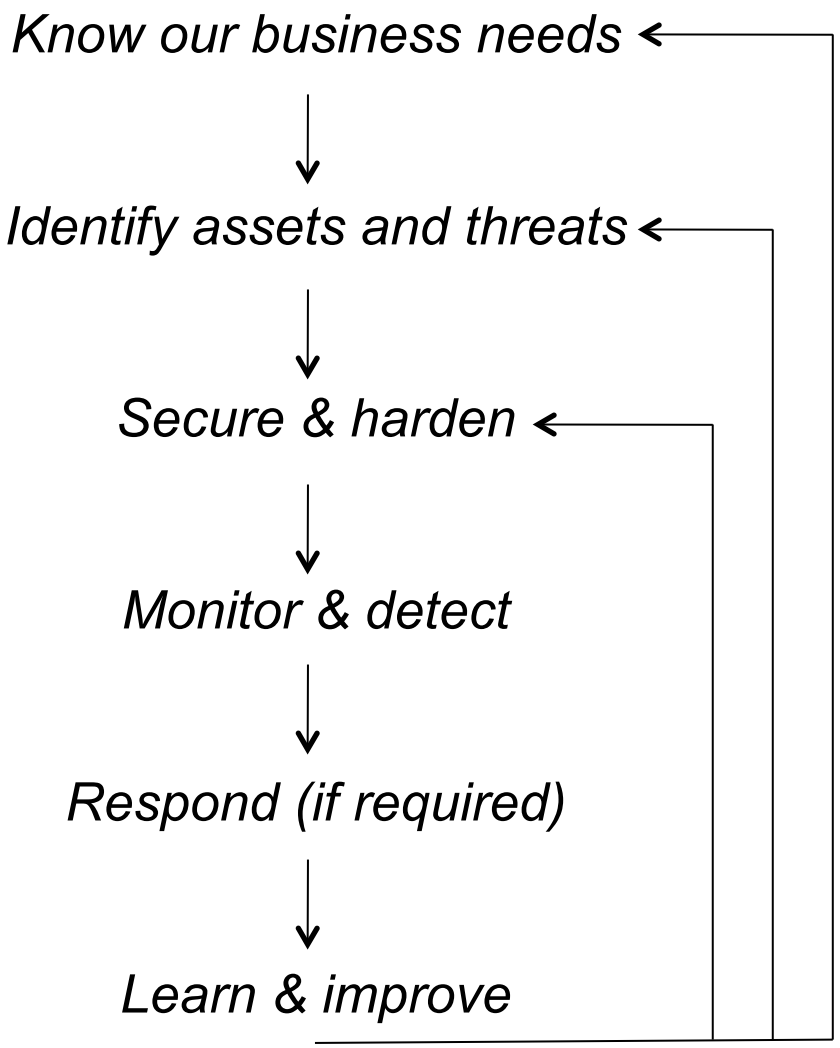
.se

The Internet is too complex to secure. One of the reasons is that it is too complex to understand.

Bruce Schneier, 2001

.se

Methodology for security



.se

Like all public networked systems, the system of public domain name servers is threatened by a variety of purposeful attacks, both malicious and mischievous, by individuals or groups that aim to disable or divert their operations. The operators of the DNS are responding to these threats, but not all the desirable steps to ensure security have yet been implemented.

Signposts in Cyberspace

ISBN 0-309-09640-5 (2005)

.se

Conclusions

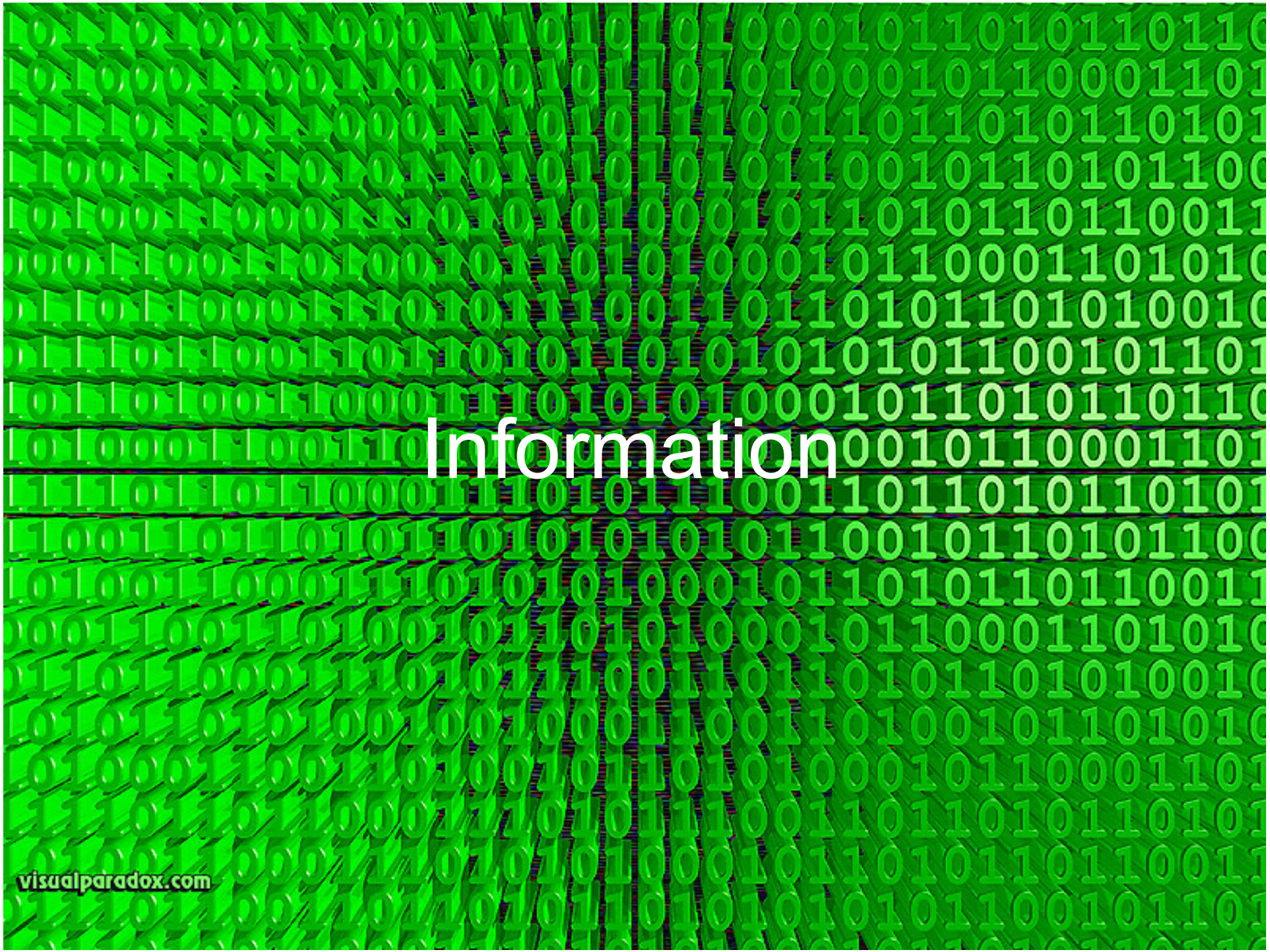
- ccTLD registries are relatively small infrastructure providers, but their infrastructure is used by most Internet users.

- Current practice of high level security and resilience are in place to ensure the DNS function.

- Active channels and platforms are available for good practice sharing and for secure and fast information sharing and threats.

.se

Crowd in Sweden. Photo: Robert Ekegren/Scanpix


Information
visualparadox.com

Source: 4seasonsomdinc.com/

Premises

What made me feel safe(r)?

- Developed & deployed a robust security policy – agreed upon by the board and management team.
- Risk analysis – learn what you have to deal with.
- Baseline security – “this and nothing less”.
- Critical systems security plan – added security depending on the systems role and information.
- Identity and access management process.
- Disaster recovery – plan and exercise.
- Communication and training.

.se

What made me feel safe(r)?

- Full scale testing environment for all changes, through the entire chain.
- Scrutinise and update organisation, responsibilities and routines.
- Perform risk analysis and exercise incident handling.
- Clearly define responsibilities for different roles.
- Redundant competence and staffing at system operations.
- Automatic controls and locks.
- Crisis management drilled to know what to do by repetitious practice.
- Release manager with the mandate to decide on GO or NOT GO.
- Accurate time planning of new releases.
- Monitoring, monitoring, monitoring.

.se

Why organizations should go through an ISO 27000 certification

- Provable quality of information security.
- Continuous information security improvement cycle.
- Working processes are structured.
- Image building.

.se

ISO 27001 vs ISO 27002

- 27001 -> What you should do.
- 27002 -> How you can implement controls.

Do’s

- Get FULL support of CEO & management team.
- Have a good reason for certification.
- Work together with your colleagues.
- Build your OWN ISMS, suitable for you!
- KISS.
- Practical ISMS.
- Choose the right auditor.

Dont’s

- Don’t do it on your own.
- Don’t loose yourself in the Risk analysis swamp.
- Don’t set up to many KPI’s.

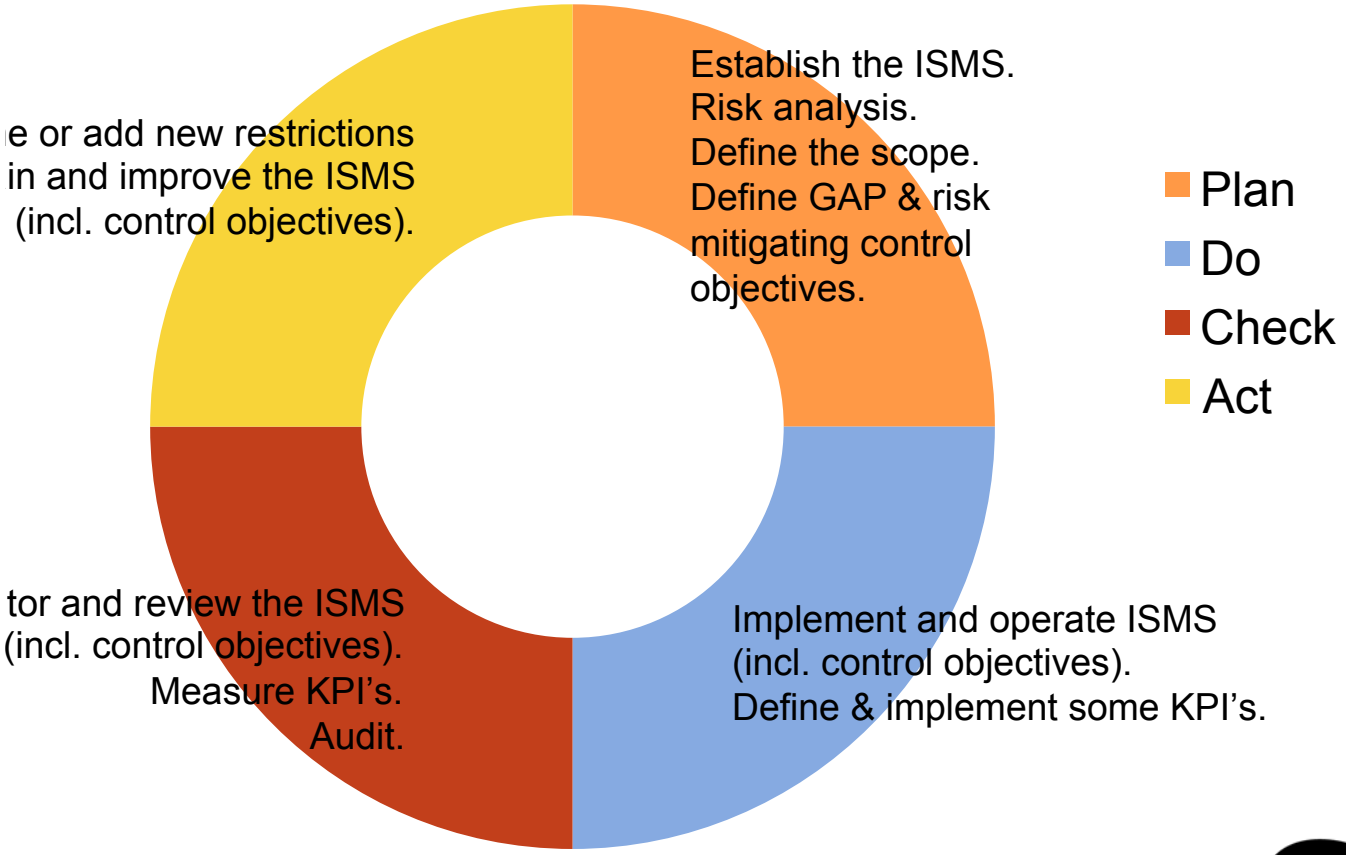
.se

ISO 27001 fundamentals

- ISO 27001 - Model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS).
- Strategic decision.
- ISMS scaled in accordance with organisational needs (small organization -> small ISMS).
- PDCA cycle.
- Risk based approach.
- Requirements (Chapter 1-8) and Annex A, (B, C)

.se

The ISO 27001 PDCA cycle



.se

Documentation requirements

- ISMS documentation includes:
  - Document Control - identified, reviewed, approved, versions, revisions, distribution.
  - Control of records - records shall be established and maintained to provide evidence of conformity to requirements and the effective operation of the ISMS.

Documents

- Scope.
- Statement of applicability (aka SOA ☺).
- ISMS manual and related documents.

.SE's scope

The Management System is applicable to:

Administration and technical operation of the national domain name registry for the Swedish top level domain .se.

Statement Of Applicability version 1.0, dated 2012-09-05.

Five management responsibilities

- Management commitment:
  - What Management should do - At least 4 meetings a year (minutes), let MT decide, establish, control.
  - Resource management .
  - Provision of resources .
  - Training, awareness and skills .

Internal ISMS audits

- Planned intervals.
- Goal: to determine whether controls are effective, maintained, etc.
- Audit criteria, scope, frequency.
- Audit process.

ISO/IEC 27001 Chapter 6 – Internal ISMS audits

- The organization shall conduct internal ISMS audits at **planned intervals to determine whether the control objectives, controls, processes and procedures of its ISMS:**
  - conform to the requirements of this International Standard and relevant legislation or regulations;
  - conform to the identified information security requirements;
  - are **effectively implemented and maintained; and**
  - perform as expected.

.se

Management review

- Planned intervals -> ISO subscribes at least once a year.
- Input:
  - Audit, feedback, vulnerabilities, changes, KPI's, etc.
- Output:
  - Improvement of the effectiveness of the ISMS & Controls.
  - Update of the risk assessment and risk treatment plan.
  - Modification of procedures and controls that effect information security.
  - Resource needs.

ISMS improvement

- Continuous improvements.
- Corrective action - Incident Management.
- Preventive action - Problem Management.
- Non conformities = security breach/incident, audit shortcomings.

Certification audit cycle

- The certification is valid for **three years, but it is required that an annual surveillance audit is performed which verifies that the ISO 27001 standard requirements for information security is still observed.**

Intertek

Certificate

Translation from a Swedish Original

The following organization's Information Security Management System has been assessed by Intertek Certification AB and found to comply with the requirements of:

SS-ISO/IEC 27001:2006

The conditions and extent of this certificate are stated in the decision report

Certificate Number
120652

Initial Certification Date
7 February 2013

Certificate Issue Date
7 February 2013

Certificate Expiry Date
6 February 2016

Stiftelsen för Internetinfrastruktur

Stockholm (Sweden)

SWEDAC ACKREDITERING
1639
ISO/IEC 17021
ISO/IEC 27006

The Management System is applicable to:

Administration and technical operation of the national domain name registry for the Swedish top level domain.se

Statement Of Applicability version 1.0, dated 2012-09-05.

Magnus Molin, CEO
Intertek Certification AB
P.O Box 1103, SE 164 22 Kista, Sweden

.se

ISO 27001:2005 CERTIFICATION TM

.se

Thank you!
Questions and answers.