

Security in a Business Setting: ISO 27001

Tom Chothia
Computer Security Lecture 22

This Lecture

- An overview of security at the business level.
- The ISO27001 Security Standard.
- Developing an Information Security Management Systems (ISMS).

When is a New Security Measure Good?

When it saves more than it costs:

$$\sum \Delta Costs < \sum \Delta Benefits$$

Benefits can be very hard to calculate, however we know a security measure is bad when:

$$\sum \Delta Costs > Total Losses$$

Information Security

- Not just interested in the security of computers.
 - e.g. print out of secret information could be left in trash
 - Someone could lie to staff members, who then enter that data into your systems.
- Often called Information Security, or **Information Assurance**.

An Ongoing Process

- An ISMS must be continually monitored.
 - Reports of new faults, IDS monitoring, Patch policy.
- If a organisation's activities shift, the ISMS will need an update.
- Maybe the first ISMS missed something. It needs to be regularly reviewed.

ISO 27001

- ISO 27001 is the international standard on how to do a ISMS.
- It provides a guide for what companies need to do.
- It can be audited, so a organisation can prove to others that it has an ISMS.

ISO 27002

ISO 27002 gives best practice for security.

Last revised in 2005.

It is not complete, but it is useful to help get ISO 27001 certified.

Getting ISOs

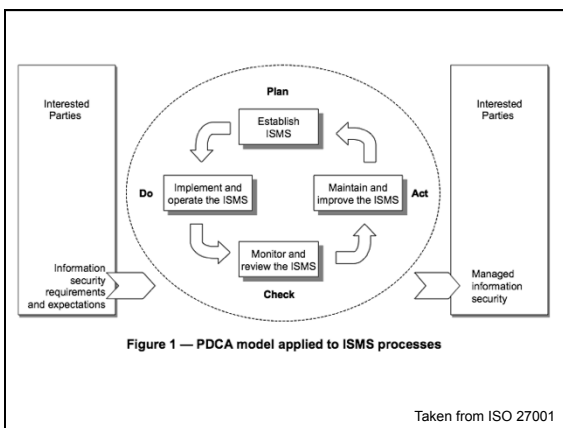
You have to pay for copies of ISO.
... but you can get them for free via the University.

Go to the Library webpage:

www.elibrary.bham.ac.uk -> Log in -> Find Resources -> Find by Type -> Standards and Patents then GO -> British Standards Online -> Search for ISO 27001

Important Parts of ISO 27001

- Understanding an organization's information security requirements.
- Build and run controls to manage an organization's information security.
- Monitoring and reviewing the ISMS.
- Continual improvement of ISMS.



Some Terms

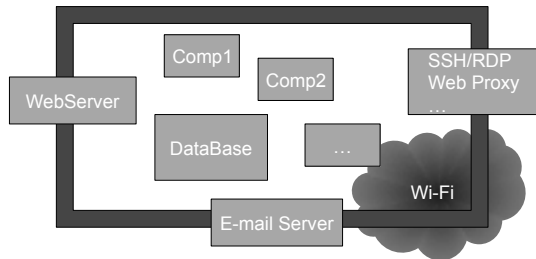
- Asset
- Threat
 - Something bad that might happen to an asset
- Vulnerability
 - Means by which the threat can happen
- Information Security Event.
- Information Security Incident.

Establish the ISMS

Define the organisation, e.g.

- What it does.
- The Scope of ISMS,
 - what's in it and what's not.
- **Assets**

A Typical Business Network



For Example

- An organisation that sells widgets.
- Does the ISMS include the
 - widgets manufacturer?
 - the payment system?
- Some Assets:
 - The telephone system.
 - E-mail system.
 - Purchase history ... and many more.

Define an ISMS policy

- How are risks and threats going to be measured, and what are the objectives?
 - e.g. UK gov. system (linked on website).
- Align with other company standards
 - e.g. ISO 9000 for general management
- What Laws apply?

Documentation

Like ISO 9000, ISO 27001 is all about documentation.



Laws: The Data Protection Act

A 1998 UK Law, includes:

- Organisations can only use data for the purpose it was collected.
- Data cannot be disclosed without consent.
- Anyone can access data about themselves.
- Organisations holding data must have "adequate" security.

A "deliberate or negligent" breach of personal data means a fine up to £500k

Other Laws:

Many countries have a data protection act:

- Greece: Law 2472/1997
- Germany: Federal Data Protection Act

...

Other Laws include:

- Freedom of Information Act (UK)
- Freedom of Information Act (USA)
- Sarbanes–Oxley Act (USA)

Identify the risks

- Identify the assets within the scope of the ISMS & their owners.
- Identify the threats to each of those assets.
- Identify the vulnerabilities that might be exploited.
- Identify the impact of loss of each asset
 - Is it confidentiality, integrity and/or availability.

Example: Purchase history

Assign this asset to sales IT manager.

Threat	Lost	Corrupted	Out of date	Stolen
CIA	Availability	Integrity	Integrity	Confidentiality

Vulnerabilities:

- Bugs in records system, SQL injection attacks, unauthorized remote access to system, malicious/incompetent staff, fire flood etc.

Risk Assessment

- Assess the business impact for each loss.
 - Scale 0-10, 1-6, cash equivalent loss.
- Assess the likelihood of each kind of security failure.
- Estimate the risk.
 - Impact x likelihood, expected cash loss a year.
- Decide which risks are acceptable, and which require treatment.

Impact:

Impact out of 10:

	Lost	Corrupted	Out of date	Stolen
Single record	2	3	1	5
Less than %50	4	5	2	6
%50-%100	5	6	4	6

Very hard to know when this is correct, important to continually review this.

Likelihood

On a scale of 1 to 10 how likely are the Vulnerabilities. E.g. For data corruption:

Bugs	SQL	Hackers	Insider	Fire	Flood
2	3	4	5	4	1

Other good measures include:

- Probability
- Events per year

Based on history and good guess work.

Risk

- Risk depends on the likelihood and the impact.
- This depends on the risk assessment methodology.
- For levels of 1 to 10 we can say that:

$$\text{Risk} = \text{Impact} \times \text{Likelihood}$$
- Other good option is expected cost per year.

Risks

For a large amount of customer data:

	Out of date	Lost	Corrupted	Stolen
Flood	-	5	-	-
Bugs	16	10	12	-
SQL injection	12	15	18	18
Hackers	10	16	16	24
Fire	-	20	-	-
Insiders	20	25	30	30

Treating the Risk:

- Avoid it:
 - take steps to stop it happening
- Mitigate it:
 - take steps to make the impact less serious
- Transfer it:
 - Make someone else responsible.
- Accept it:
 - Decide to live with it.

For example

- Loss of data:
 - Avoid by not collecting data
- Stolen data:
 - Mitigate this by encrypting stored data
- Data destroyed by fire:
 - Transfer it using fire insurance.
- Main and backup disks fail at same time
 - Accept, probably of this = 0.0000001%

Final Steps:

- Specify the controls: i.e., mitigation and avoidance techniques.
- Obtain Management approval.
 - of accepted risks and overall ISMS
- Prepare a statement of applicability, i.e. overview of ISMS.

Assurance

ISOs give **some** assurance to other organisations, that your organisation is secure



Exercise 4

- For Exercise 4 you need to carry out a ISO 27001 style risk assessment.
- Pick a company of your choice,
 - Identify the assets
 - Calculate the risks
 - Say how and why to mitigate, avoid, transfer or accept.
- Use what you have learn on this module.

Revision

- Read the set papers.
- Watch videos/look at lecture slides.
- Come and see me during my office hour next term.

This Lecture

- An overview of security at the business level.
- The ISO27001 Security Standard
- Developing an Information Security Management System (ISMS).