Amir Neziri

Information Security Management (ISM)

Amir Neziri

- **Information Security Manager and Consultant** for Information Security / IT-Security, Event/Access Management, Application Monitoring & Software Engineering

- Certified ISO/IEC 27001:2013 Lead Auditor

- Academic Careers
  - Master in IT-Security @ Darmstadt University of Technology (TU Darmstadt)

  - Master in Computer Science @ TU Darmstadt

  - Bachelor in Computer Science @ TU Darmstadt

- Contact
  - XING: https://www.xing.com/profile/Amir_Neziri
  - LinkedIn: https://www.linkedin.com/in/amirneziri

Agenda

1

Motivation

2

Information Security Standards

3

Information Security Management Systems (ISMS)

4

ISMS Process

5

ISO/IEC 27001

6

Auditing an ISMS

7

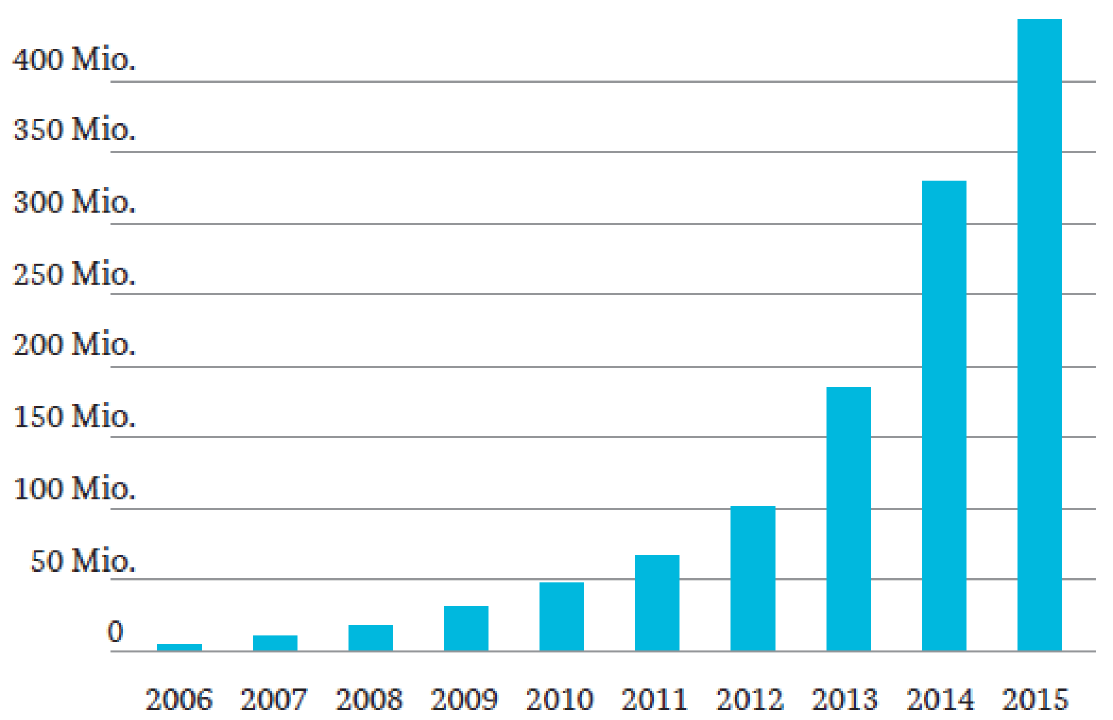
Summary

8

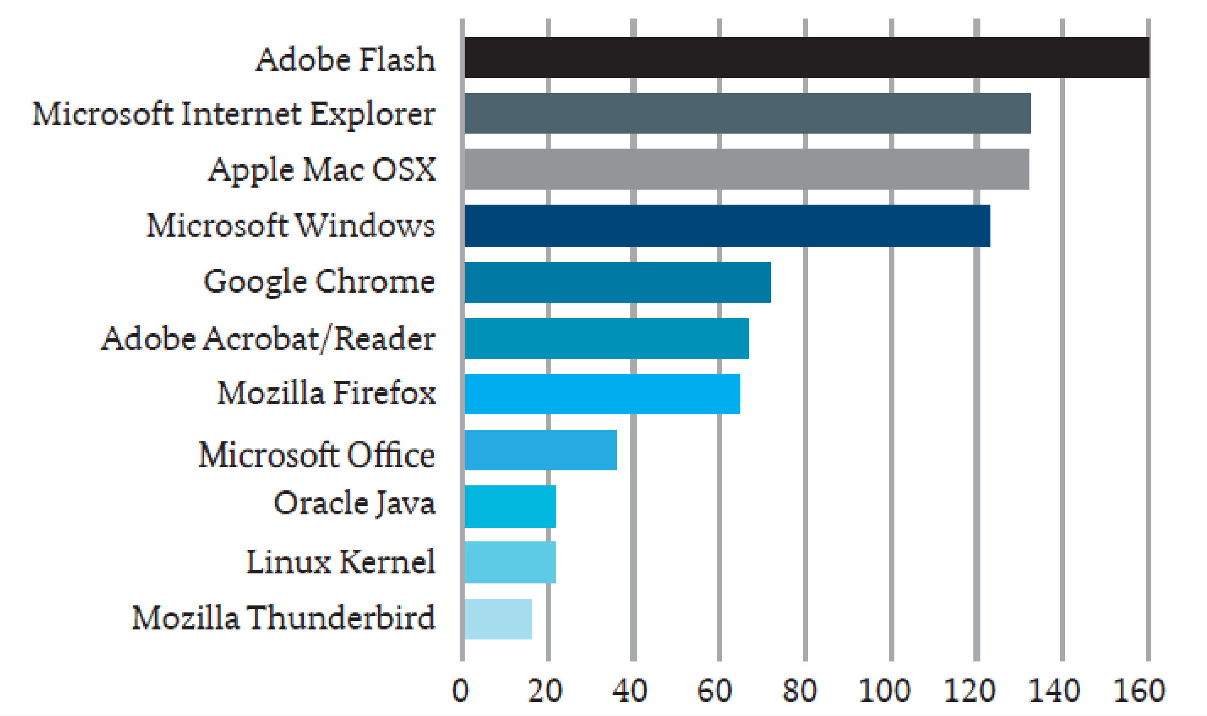
Questions

“Information is knowledge and knowledge is power”

Motivation – Cyber Security Threats (2015)



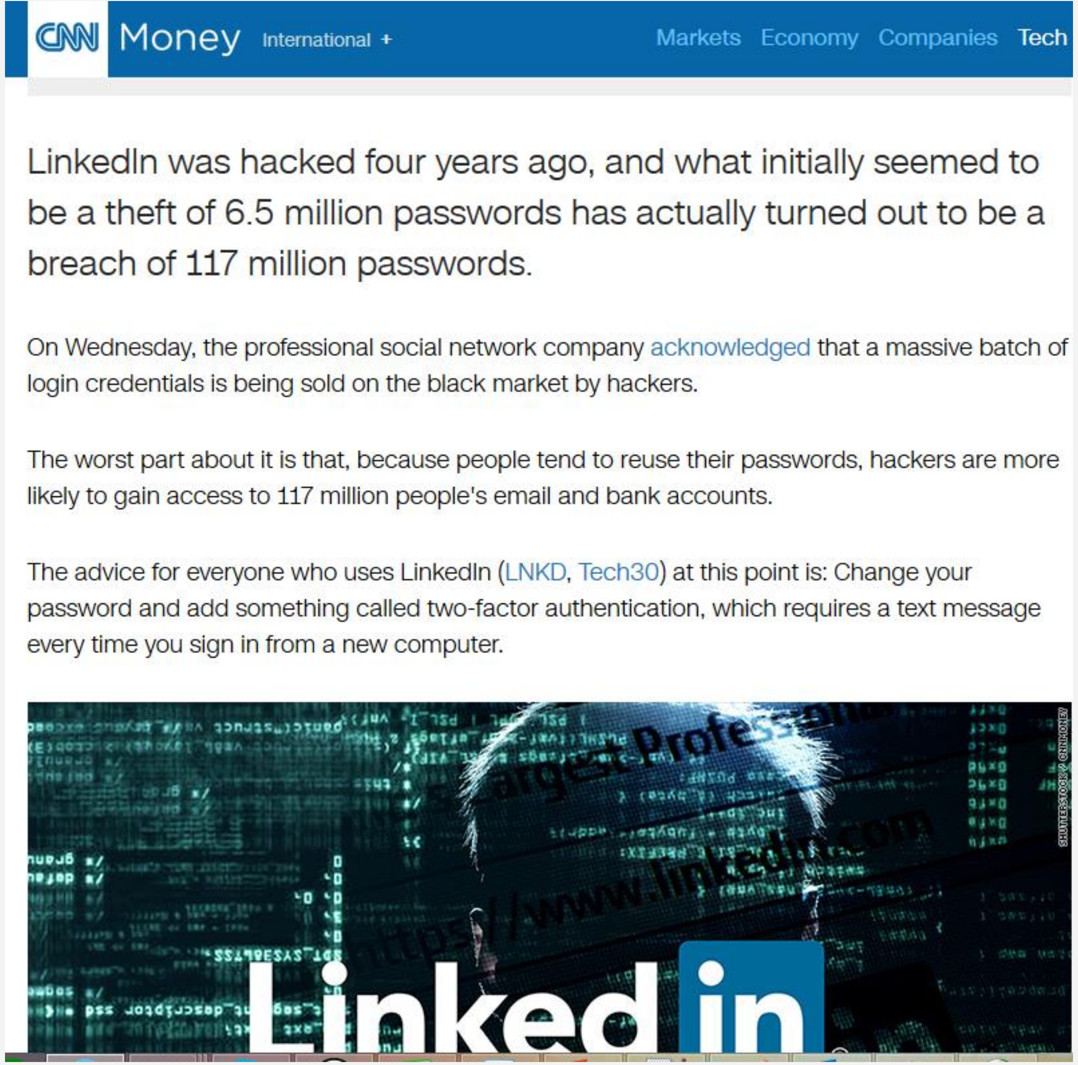
Number of Windows Malwares



Number of Software Vulnerabilities

Source: BSI 2015

Motivation – Breach of Confidentiality & Authenticity



LinkedIn was hacked four years ago, and what initially seemed to be a theft of 6.5 million passwords has actually turned out to be a breach of 117 million passwords.

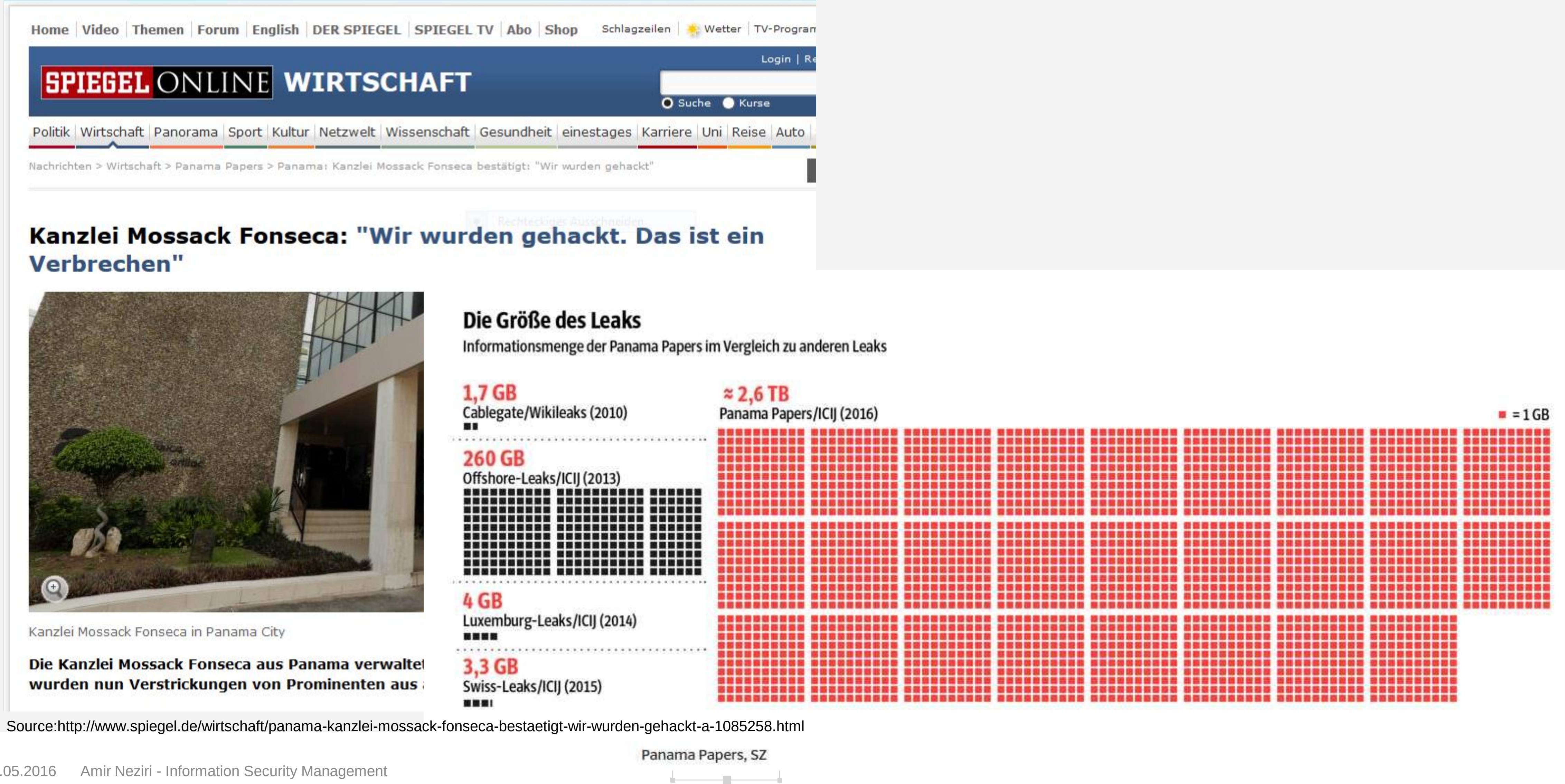
On Wednesday, the professional social network company acknowledged that a massive batch of login credentials is being sold on the black market by hackers.

The worst part about it is that, because people tend to reuse their passwords, hackers are more likely to gain access to 117 million people's email and bank accounts.

The advice for everyone who uses LinkedIn (LNKD, Tech30) at this point is: Change your password and add something called two-factor authentication, which requires a text message every time you sign in from a new computer.

Source: http://money.cnn.com/2016/05/19/technology/linkedin-hack/

Motivation – Breach of Confidentiality



Home | Video | Themen | Forum | English | DER SPIEGEL | SPIEGEL TV | Abo | Shop
Schlagzeilen | Wetter | TV-Program
SPIEGEL ONLINE WIRTSCHAFT
Login | Re
○ Suche ○ Kurse
Politik | Wirtschaft | Panorama | Sport | Kultur | Netzwelt | Wissenschaft | Gesundheit | einestages | Karriere | Uni | Reise | Auto
Nachrichten > Wirtschaft > Panama Papers > Panama: Kanzlei Mossack Fonseca bestätigt: "Wir wurden gehackt"

Kanzlei Mossack Fonseca: "Wir wurden gehackt. Das ist ein Verbrechen"

Kanzlei Mossack Fonseca in Panama City

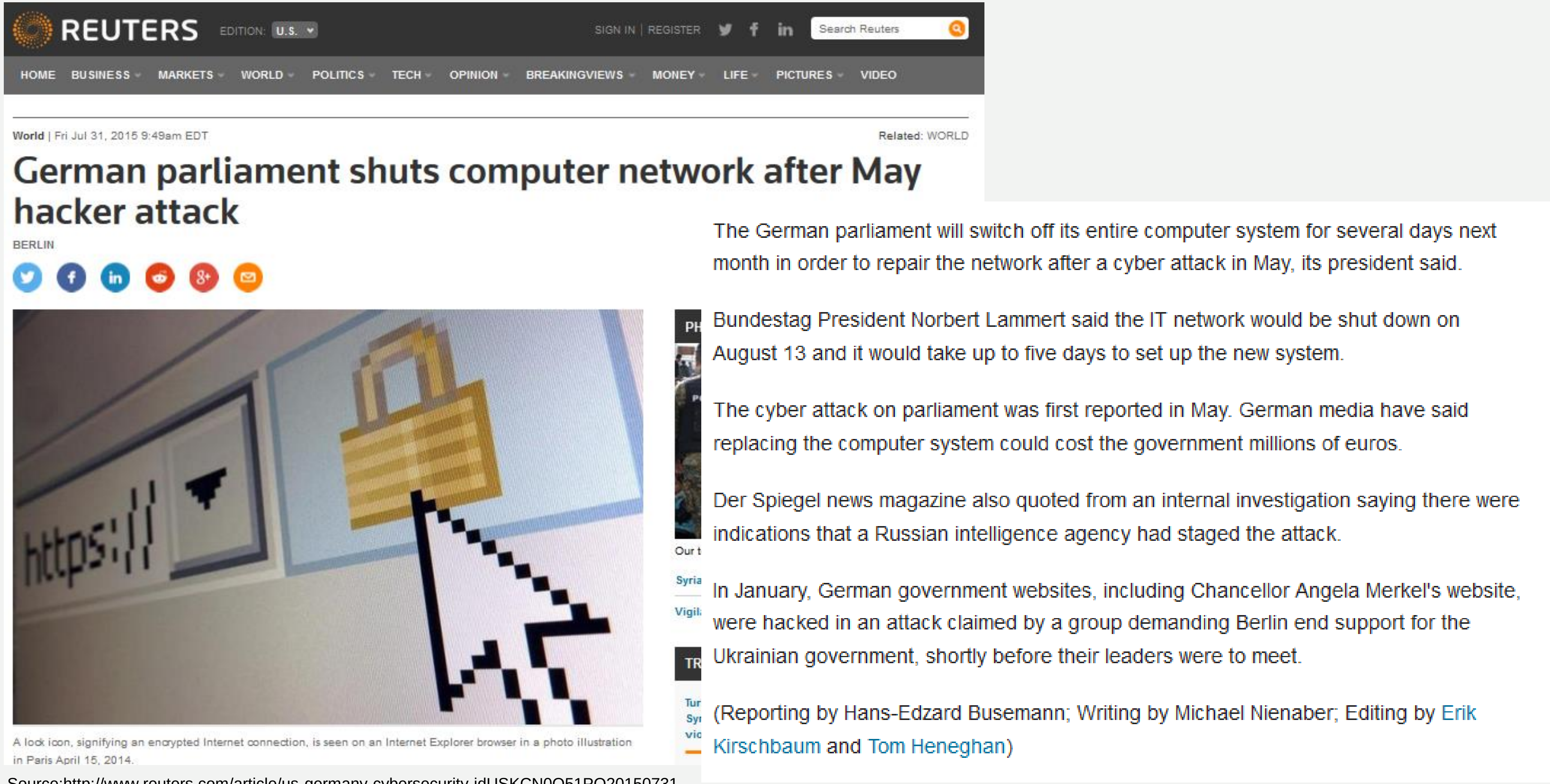
Die Kanzlei Mossack Fonseca aus Panama verwaltet wurden nun Verstrickungen von Prominenten aus

Die Größe des Leaks
Informationsmenge der Panama Papers im Vergleich zu anderen Leaks
1,7 GB
Cablegate/Wikileaks (2010)
260 GB
Offshore-Leaks/ICIJ (2013)
4 GB
Luxemburg-Leaks/ICIJ (2014)
3,3 GB
Swiss-Leaks/ICIJ (2015)
≈ 2,6 TB
Panama Papers/ICIJ (2016)
🟥 = 1 GB

Source:http://www.spiegel.de/wirtschaft/panama-kanzlei-mossack-fonseca-bestaetigt-wir-wurden-gehackt-a-1085258.html

Panama Papers, SZ

Motivation – Breach of Availability & Confidentiality



World | Fri Jul 31, 2015 9:49am EDT

Related: WORLD

German parliament shuts computer network after May hacker attack

BERLIN

A lock icon, signifying an encrypted Internet connection, is seen on an Internet Explorer browser in a photo illustration in Paris April 15, 2014.

The German parliament will switch off its entire computer system for several days next month in order to repair the network after a cyber attack in May, its president said.

Bundestag President Norbert Lammert said the IT network would be shut down on August 13 and it would take up to five days to set up the new system.

The cyber attack on parliament was first reported in May. German media have said replacing the computer system could cost the government millions of euros.

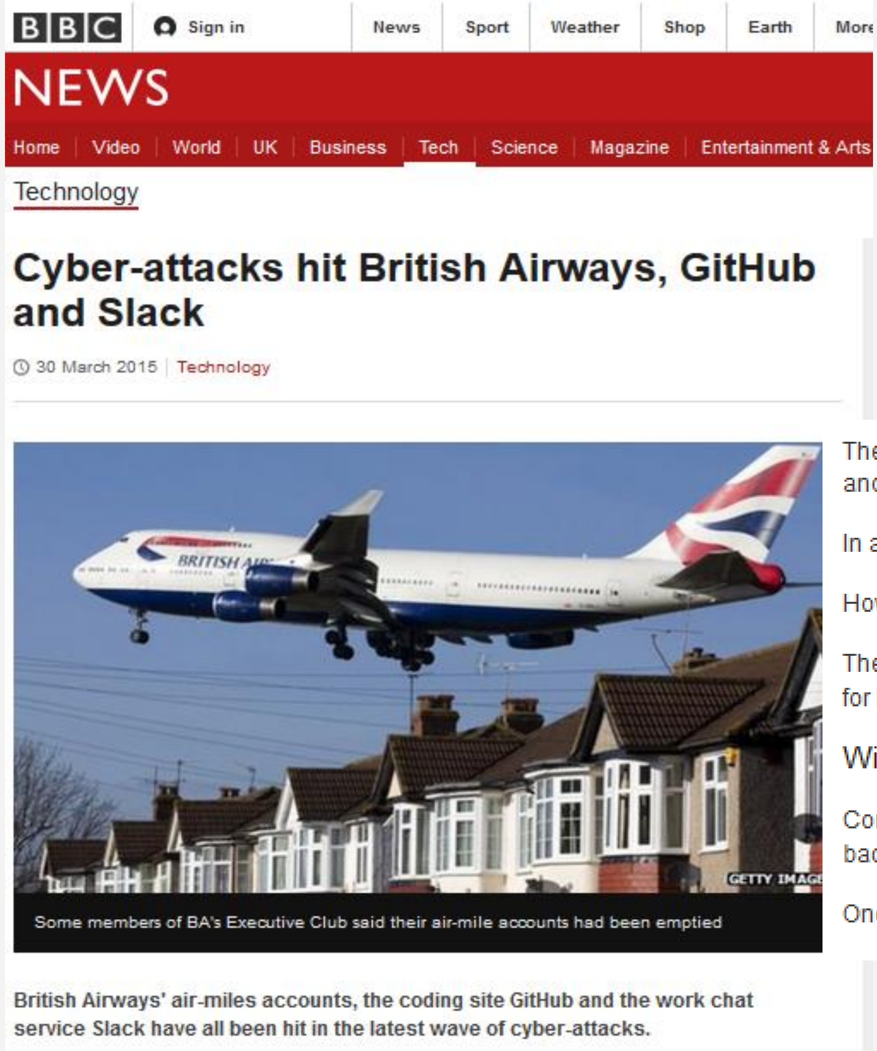
Der Spiegel news magazine also quoted from an internal investigation saying there were indications that a Russian intelligence agency had staged the attack.

In January, German government websites, including Chancellor Angela Merkel's website, were hacked in an attack claimed by a group demanding Berlin end support for the Ukrainian government, shortly before their leaders were to meet.

(Reporting by Hans-Edzard Busemann; Writing by Michael Nienaber; Editing by Erik Kirschbaum and Tom Heneghan)

Source:http://www.reuters.com/article/us-germany-cybersecurity-idUSKCN0Q51PQ20150731

Motivation – Breach of Confidentiality/Authenticity & Integrity

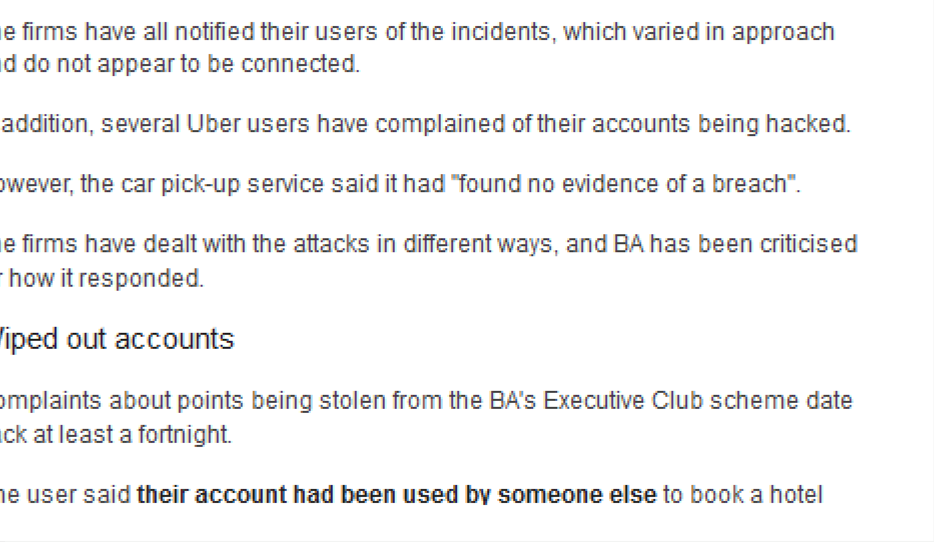


Cyber-attacks hit British Airways, GitHub and Slack

30 March 2015 | Technology

Some members of BA's Executive Club said their air-mile accounts had been emptied

British Airways' air-miles accounts, the coding site GitHub and the work chat service Slack have all been hit in the latest wave of cyber-attacks.



The firms have all notified their users of the incidents, which varied in approach and do not appear to be connected.

In addition, several Uber users have complained of their accounts being hacked.

However, the car pick-up service said it had "found no evidence of a breach".

The firms have dealt with the attacks in different ways, and BA has been criticised for how it responded.

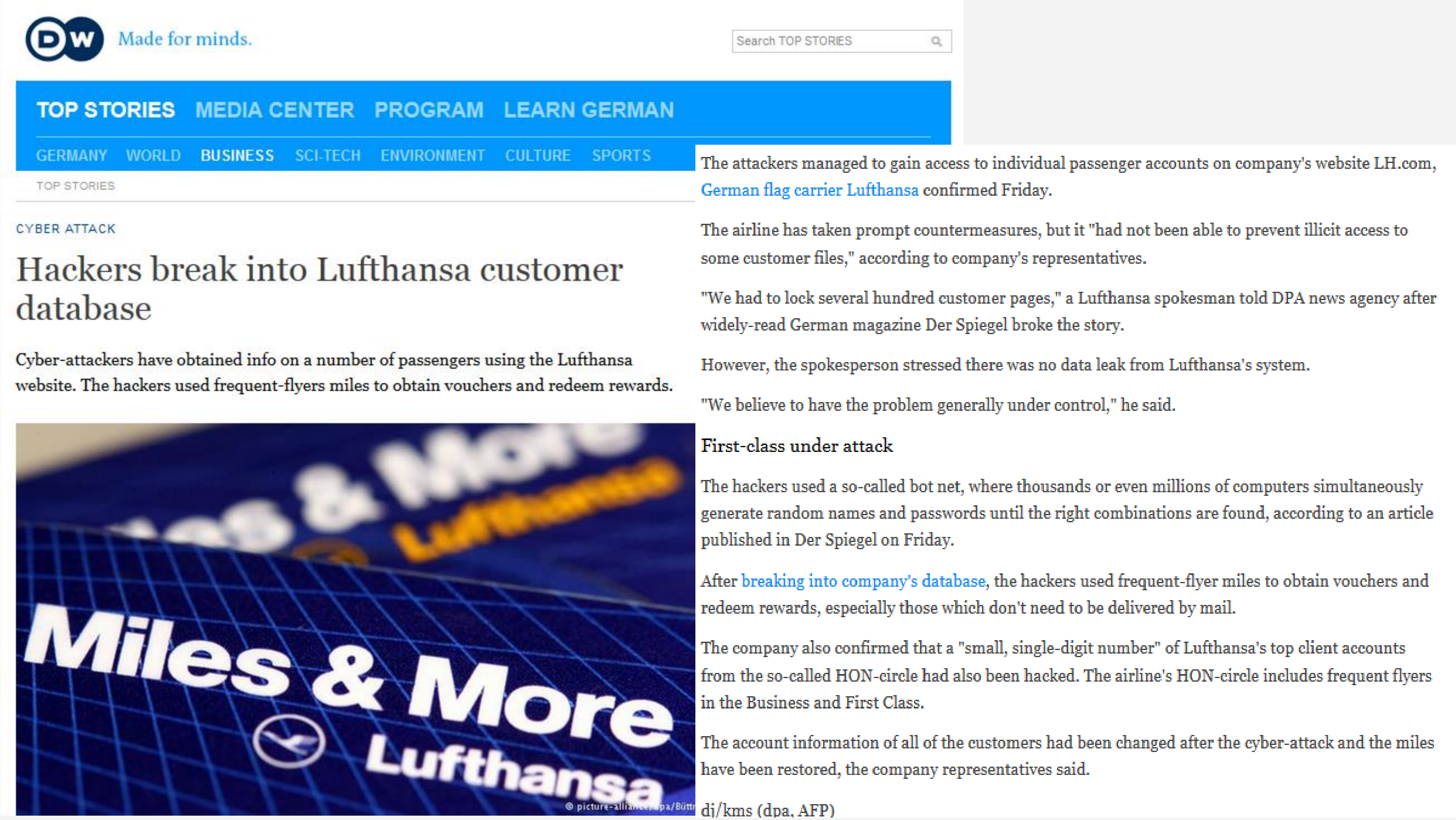
Wiped out accounts

Complaints about points being stolen from the BA's Executive Club scheme date back at least a fortnight.

One user said **their account had been used by someone else** to book a hotel

Source:http://www.bbc.com/news/technology-32115292

Motivation – Breach of Confidentiality



CYBER ATTACK

Hackers break into Lufthansa customer database

Cyber-attackers have obtained info on a number of passengers using the Lufthansa website. The hackers used frequent-flyers miles to obtain vouchers and redeem rewards.

The attackers managed to gain access to individual passenger accounts on company's website LH.com, German flag carrier Lufthansa confirmed Friday.

The airline has taken prompt countermeasures, but it "had not been able to prevent illicit access to some customer files," according to company's representatives.

"We had to lock several hundred customer pages," a Lufthansa spokesman told DPA news agency after widely-read German magazine Der Spiegel broke the story.

However, the spokesperson stressed there was no data leak from Lufthansa's system.

"We believe to have the problem generally under control," he said.

First-class under attack

The hackers used a so-called bot net, where thousands or even millions of computers simultaneously generate random names and passwords until the right combinations are found, according to an article published in Der Spiegel on Friday.

After breaking into company's database, the hackers used frequent-flyer miles to obtain vouchers and redeem rewards, especially those which don't need to be delivered by mail.

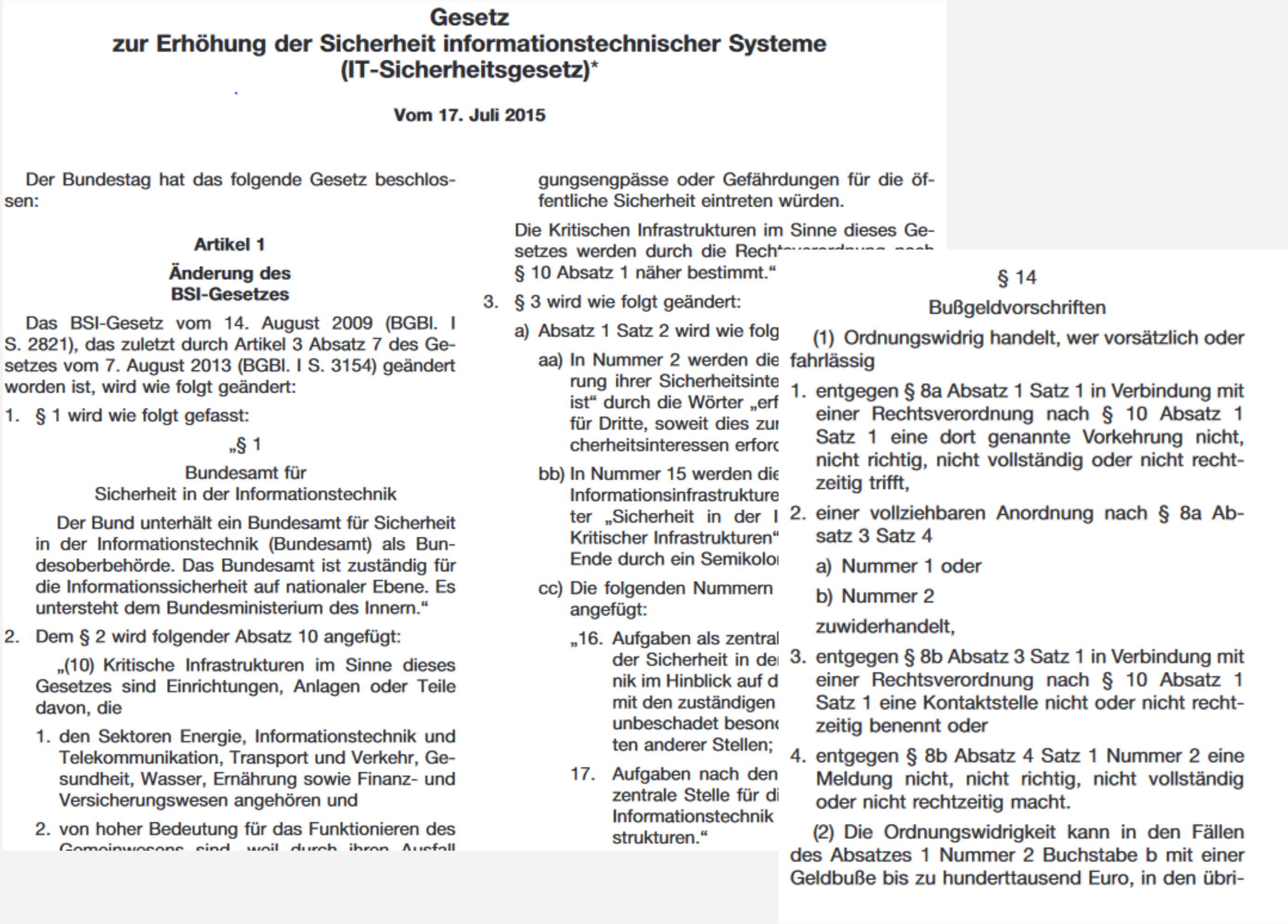
The company also confirmed that a "small, single-digit number" of Lufthansa's top client accounts from the so-called HON-circle had also been hacked. The airline's HON-circle includes frequent flyers in the Business and First Class.

The account information of all of the customers had been changed after the cyber-attack and the miles have been restored, the company representatives said.

dj/kms (dpa, AFP)

Source:http://www.dw.com/en/hackers-break-into-lufthansa-customer-database/a-18374698

Motivation – German Act „IT-Sicherheitsgesetz“



Gesetz
zur Erhöhung der Sicherheit informationstechnischer Systeme
(IT-Sicherheitsgesetz)*

Vom 17. Juli 2015

Der Bundestag hat das folgende Gesetz beschlossen:

Artikel 1

Änderung des BSI-Gesetzes

Das BSI-Gesetz vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 3 Absatz 7 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154) geändert worden ist, wird wie folgt geändert:

1. § 1 wird wie folgt gefasst:

„§ 1

Bundesamt für
Sicherheit in der Informationstechnik

Der Bund unterhält ein Bundesamt für Sicherheit in der Informationstechnik (Bundesamt) als Bundesoberbehörde. Das Bundesamt ist zuständig für die Informationssicherheit auf nationaler Ebene. Es untersteht dem Bundesministerium des Innern.“

2. Dem § 2 wird folgender Absatz 10 angefügt:

„(10) Kritische Infrastrukturen im Sinne dieses Gesetzes sind Einrichtungen, Anlagen oder Teile davon, die

1. den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und

2. von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall

gungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.

Die Kritischen Infrastrukturen im Sinne dieses Gesetzes werden durch die Recht
§ 10 Absatz 1 näher bestimmt.“

3. § 3 wird wie folgt geändert:

a) Absatz 1 Satz 2 wird wie folg

aa) In Nummer 2 werden die
rung ihrer Sicherheitsinte
ist“ durch die Wörter „erf
für Dritte, soweit dies zur
cherheitsinteressen erforc

bb) In Nummer 15 werden die
Informationsinfrastrukture
ter „Sicherheit in der I
Kritischer Infrastrukturen“
Ende durch ein Semikolo

cc) Die folgenden Nummern
angefügt:

„16. Aufgaben als zentral
der Sicherheit in de
nik im Hinblick auf d
mit den zuständigen
unbeschadet besonc
ten anderer Stellen;

17. Aufgaben nach den
zentrale Stelle für di
Informationstechnik
strukturen.“

§ 14

Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 8a Absatz 1 Satz 1 in Verbindung mit einer Rechtsverordnung nach § 10 Absatz 1 Satz 1 eine dort genannte Vorkehrung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig trifft,

2. einer vollziehbaren Anordnung nach § 8a Absatz 3 Satz 4
   a) Nummer 1 oder
   b) Nummer 2

   zuwiderhandelt,

3. entgegen § 8b Absatz 3 Satz 1 in Verbindung mit einer Rechtsverordnung nach § 10 Absatz 1 Satz 1 eine Kontaktstelle nicht oder nicht rechtzeitig benennt oder

4. entgegen § 8b Absatz 4 Satz 1 Nummer 2 eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht.

(2) Die Ordnungswidrigkeit kann in den Fällen des Absatzes 1 Nummer 2 Buchstabe b mit einer Geldbuße bis zu hunderttausend Euro, in den übri-

Information Security

We have to protect information of any kind and origin.

How?

Information Security Standards (1)

- ISO 27001 - "Information Technology – Security Techniques – Information Security Management Systems Requirements Specification„
  - the first international standard for management of information security that also allows certification
  - provides general recommendations among the introduction, operation, and improvement of a documented information security management system that also takes the risks into account

- ISO 27002 - "Information technology – Code of practice for information security management“
  - defines a framework for information security management
  - establish a functioning security management system and anchor it in the organization

- ISO 27005 - "Information security risk management„
  - contains general recommendations for risk management for information security
  - It supports implementation of the requirements from ISO/IEC 27001

Source: BSI-Standard-100-1

Information Security Standards (3)

- ISO 27006 - "Information technology - Security techniques - Requirements for the accreditation of bodies providing certification of information security management systems"
  - specifies requirements for the accrediting of certification bodies for ISMS and also handles
  - specific details of the ISMS certification process.

- ISO 17799 - "Information Technology – Code of Practice for Information Security Management“
  - necessary steps for developing a fully-functioning IT security management and for integrating this securely in the organization
  - recommendations relate to the management level

- ISO 13335 - "Management of Information and Communications Technology Security" (formerly "Guidelines on the Management of IT Security")
  - is a general guide for initiating and implementing the IT security management process.
  - Concepts and models for information and communications technology security management
  - Techniques for information security risk management
  - Management guidance on network security

Source: BSI-Standard-100-1

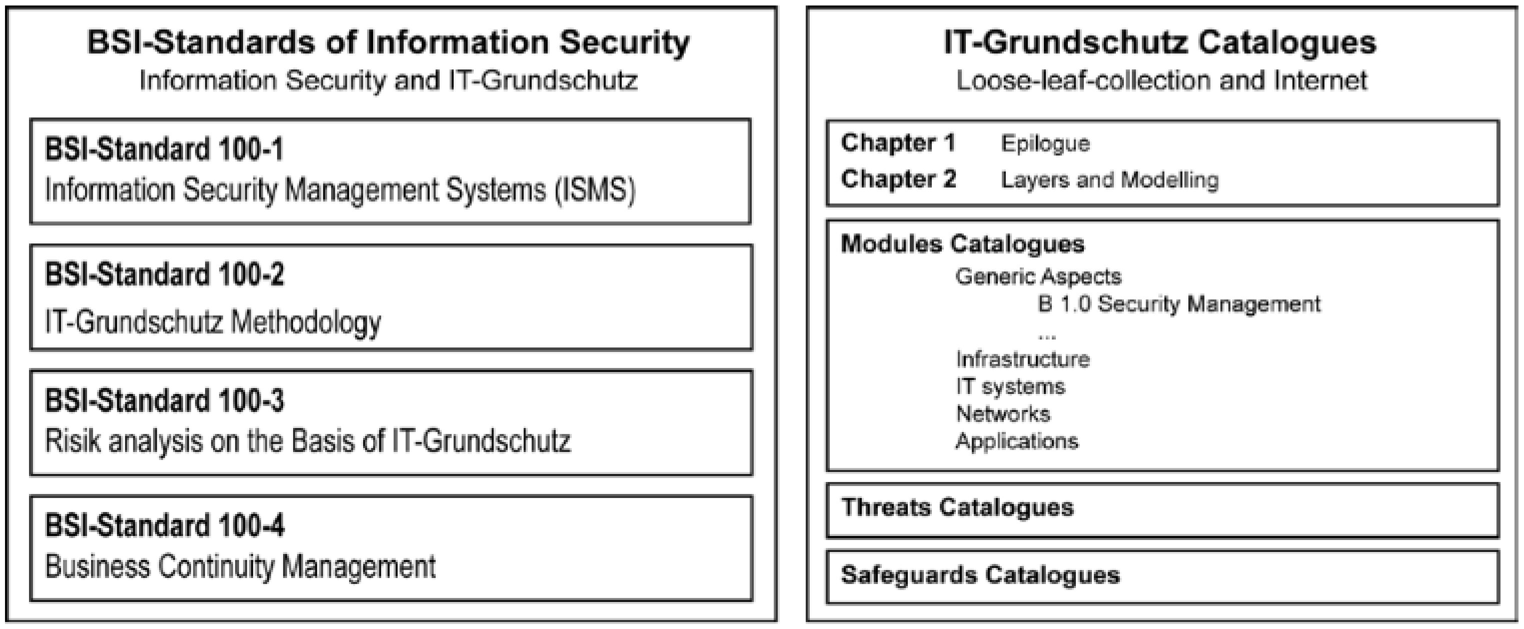
Information Security Standards (4)

- COBIT (Control Objectives for Information and related Technology)
  - describes a method for controlling the risks arising from the use of IT to support business-related processes
  - documents are issued by the IT Governance Institute (ITGI)
  - authors ideas are based on the existing standards for security management such as ISO 27002

- ITIL (IT Infrastructure Library)
  - is a collection of several books on the subject of IT service management
  - developed by the United Kingdom’s Office of Government Commerce (OGC)
  - Goal: optimize and improve the quality and cost-effectiveness of IT services

Source: BSI-Standard-100-1

Information Security Standards (5)



BSI-Standards of Information Security
Information Security and IT-Grundschutz

BSI-Standard 100-1
Information Security Management Systems (ISMS)

BSI-Standard 100-2
IT-Grundschutz Methodology

BSI-Standard 100-3
Risik analysis on the Basis of IT-Grundschutz

BSI-Standard 100-4
Business Continuity Management

IT-Grundschutz Catalogues
Loose-leaf-collection and Internet

Chapter 1 Epilogue
Chapter 2 Layers and Modelling

Modules Catalogues
Generic Aspects
B 1.0 Security Management
...
Infrastructure
IT systems
Networks
Applications

Threats Catalogues

Safeguards Catalogues

Figure 1: Overview of BSI publications on Information Security management

Source: BSI-Standard-100-1

Information Security Standards (6)

- BSI-Standard 100-1 Information security management systems (ISMS)
  - defines the general requirements of an ISMS
  - Is fully compatible with the ISO 27001
- BSI-Standard-100-2 IT-Grundschutz Methodology
  - explains in a step-by-step fashion how an management system for information security can be developed and operated in practice
- BSI-Standard-100-3 Risk analysis on the basis of IT-Grundschutz
  - a methodology for risk analysis on the basis of IT-Grundschutz

- BSI-Standard-100-4-Emergency Management
  - explains a method for establishing and maintaining an agency-wide or company-wide emergency management system.
- IT-Grundschutz Catalogues
  - have a modular structure and contain modules for typical processes, applications and IT components
  - recommending information security measures for each subject,
  - they describe the most important threats from which an institution should protect itself against

Information Security Management System (ISMS)

- Definition 1: “An ISMS is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process.” [Source: ISO 27001]

- Definition 2: “The ISMS specifies the instruments and methods that the management should use to clearly manage (plan, adopt, implement, supervise and improve) the tasks and activities aimed at achieving information security. “

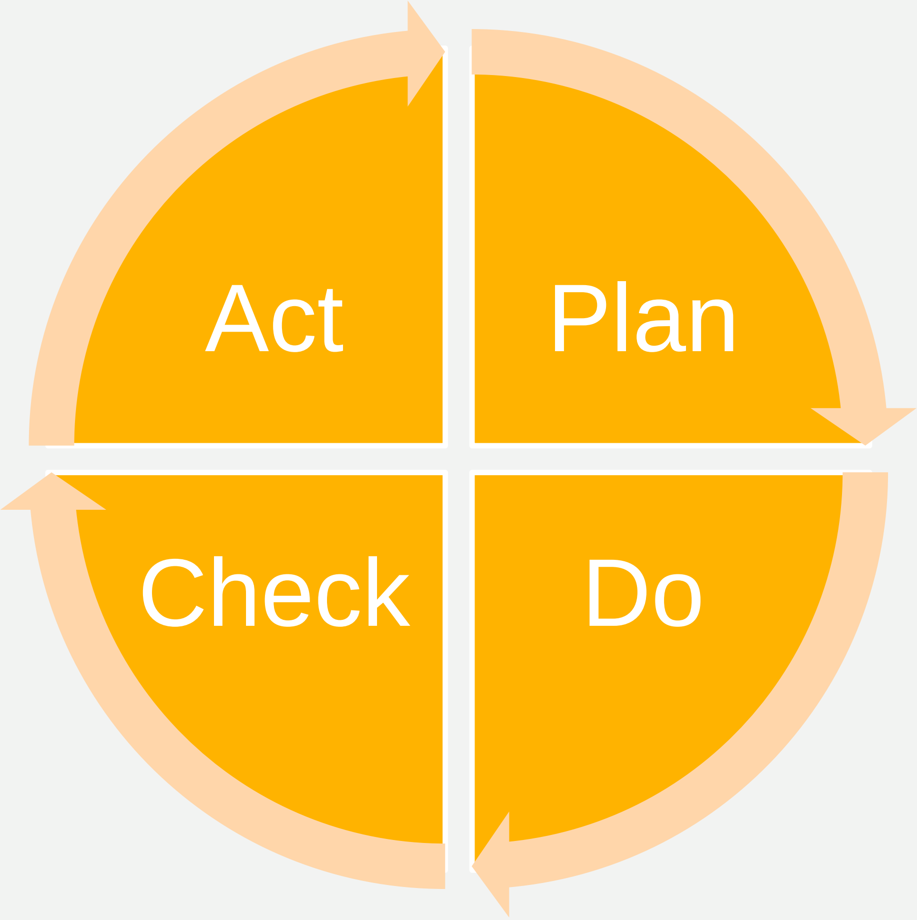
- Aims of an ISMS
  - establish an effective appropriate level of information security
  - Complying with laws (e.g. “IT-Sicherheitsgesetz” in, BDSG in Germany) , legal provisions, ordinances and contractual obligations (e.g. Company Policies)

- Most used protection objectives in an ISMS
  - Confidentiality
  - Integrity
  - Availability (and Authenticity)

- ISMS Process: PDCA (Plan, Do, Check and Act)

ISMS Process – Plan, Do, Check and Act (PDCA)

- Plan
  - Define the ISMS guidelines, objectives, processes and procedures
- Do
  - Implement and execute the ISMS guidelines, objectives, processes and procedures
- Check
  - Asses the ISMS at the guidelines, objectives and check results
- Act
  - Take corrective actions based on the check results



ISO/IEC 27001 – Information Security Management

- The ISO 27000 family of standards helps organizations keep information assets secure
- Using the ISO 27000 family of standards will help organizations to manage the security of assets such as financial information, intellectual property, employee details or entrusted information entrusted
- ISO/IEC 27001 is the best-known standard in the family providing requirements for an information security management system (ISMS)
- Certification to ISO/IEC 27001 is possible but not obligatory. For some industries, certification is a legal or contractual requirement
- ISO/IEC 27001:2013 was published on 25th September 2013
  - requirements for establishing, implementing, maintaining and continually improving an information security management system

Source: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

ISO/IEC 27001 – 27001:2013 Structure

1. Scope of the standard
2. How the document is referenced
3. Reuse of the terms and definitions in ISO/IEC 27000
4. Organizational context and stakeholders
5. Information security leadership and high-level support for policy
6. Planning an information security management system; risk assessment; risk treatment
7. Supporting an information security management system
8. Making an information security management system operational
9. Reviewing the system's performance
10. Corrective action

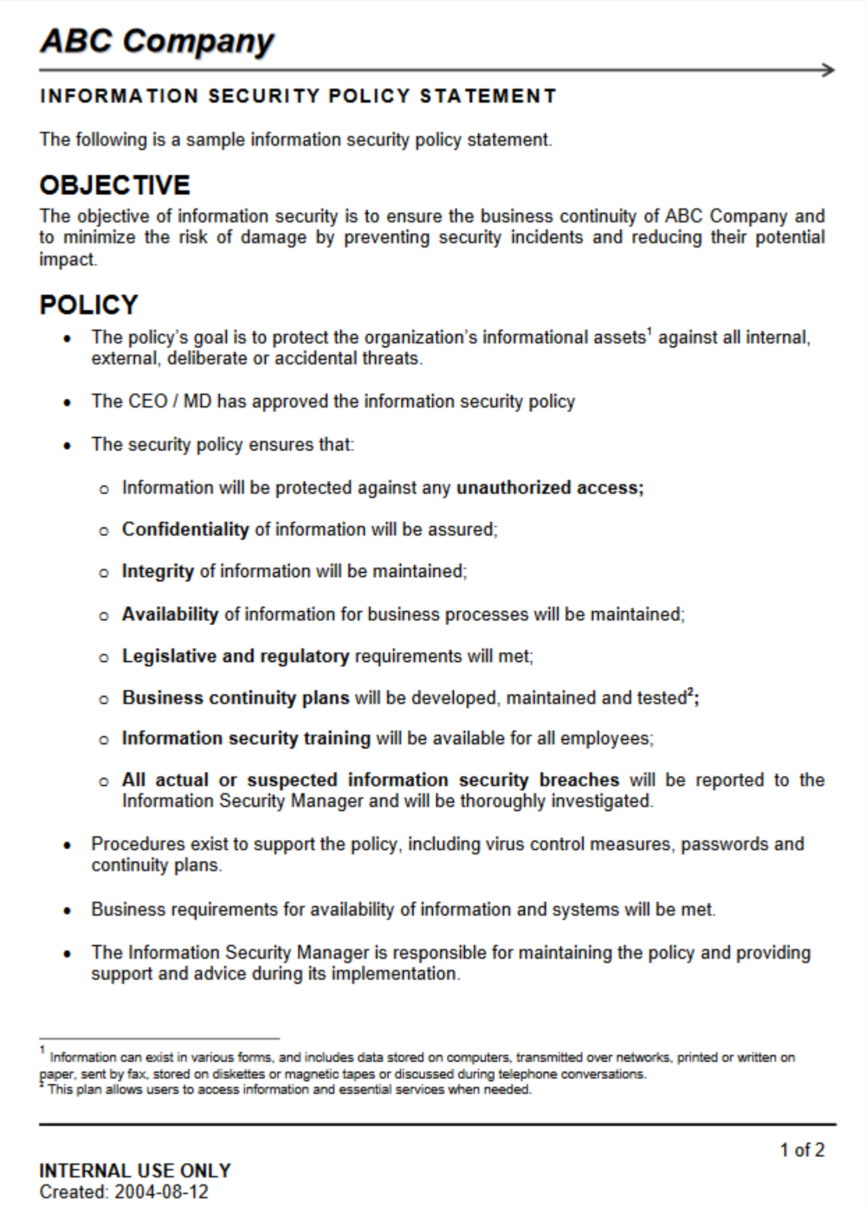
- Annex A: List of controls and their objectives.

ISO/IEC 27001 – Minimum Documentation Requirements (1)

Section	ISO 27001:2013 Mandatory Documents
4.3	The scope of the ISMS
5.2	Information security policy
6.1.2	Information security risk assessment process
6.1.3	Information security risk treatment process
6.1.3 d)	The Statement of Applicability
6.2	Information security objectives
7.2 d)	Evidence of competence
7.5.1 b)	Documented information determined by the organisation as being necessary for the effectiveness of the ISMS
8.1	Operational planning and control
8.2	Results of the information security risk assessment
8.3	Results of the information security risk treatment
9.1	Evidence of the monitoring and measurement of results
9.2	A documented internal audit process
9.2 g)	Evidence of the audit programmes and the audit results

ISO/IEC 27001 – Minimum Documentation Requirements (2)

Sections	ISO 27001:2013 Mandatory Documents
9.3	Evidence of the results of management reviews
10.1 f)	Evidence of the nature of the non-conformities and any subsequent actions taken
10.1 g)	Evidence of the results of any corrective actions taken
Annex A)	*



ABC Company

INFORMATION SECURITY POLICY STATEMENT

The following is a sample information security policy statement.

OBJECTIVE

The objective of information security is to ensure the business continuity of ABC Company and to minimize the risk of damage by preventing security incidents and reducing their potential impact.

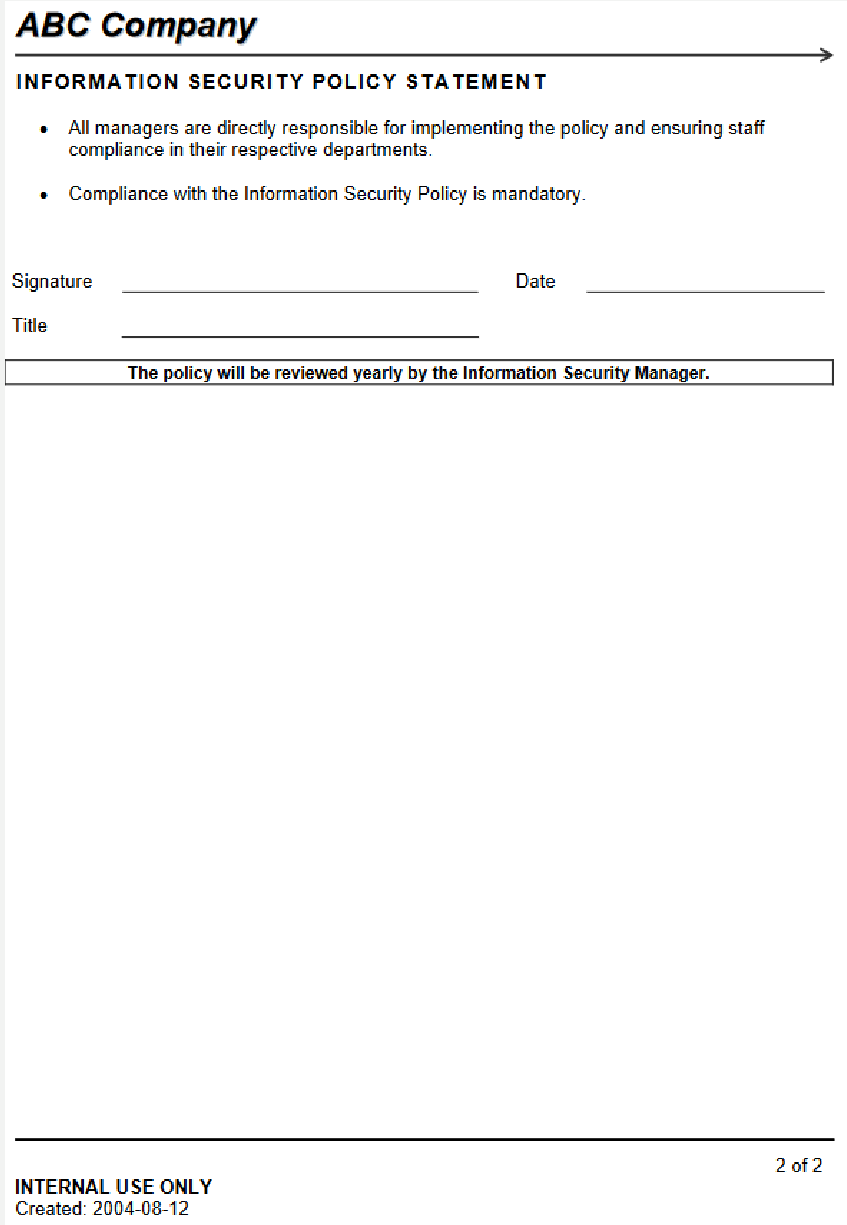
POLICY

- The policy's goal is to protect the organization's informational assets[1] against all internal, external, deliberate or accidental threats.
- The CEO / MD has approved the information security policy
- The security policy ensures that:
  - Information will be protected against any **unauthorized access;**
  - **Confidentiality** of information will be assured;
  - **Integrity** of information will be maintained;
  - **Availability** of information for business processes will be maintained;
  - **Legislative and regulatory** requirements will met;
  - **Business continuity plans** will be developed, maintained and tested[2]**;**
  - **Information security training** will be available for all employees;
  - **All actual or suspected information security breaches** will be reported to the Information Security Manager and will be thoroughly investigated.
- Procedures exist to support the policy, including virus control measures, passwords and continuity plans.
- Business requirements for availability of information and systems will be met.
- The Information Security Manager is responsible for maintaining the policy and providing support and advice during its implementation.

[1] Information can exist in various forms, and includes data stored on computers, transmitted over networks, printed or written on paper, sent by fax, stored on diskettes or magnetic tapes or discussed during telephone conversations.
[2] This plan allows users to access information and essential services when needed.

1 of 2

INTERNAL USE ONLY
Created: 2004-08-12



ABC Company

INFORMATION SECURITY POLICY STATEMENT

- All managers are directly responsible for implementing the policy and ensuring staff compliance in their respective departments.
- Compliance with the Information Security Policy is mandatory.

Signature ____________________ Date ______________

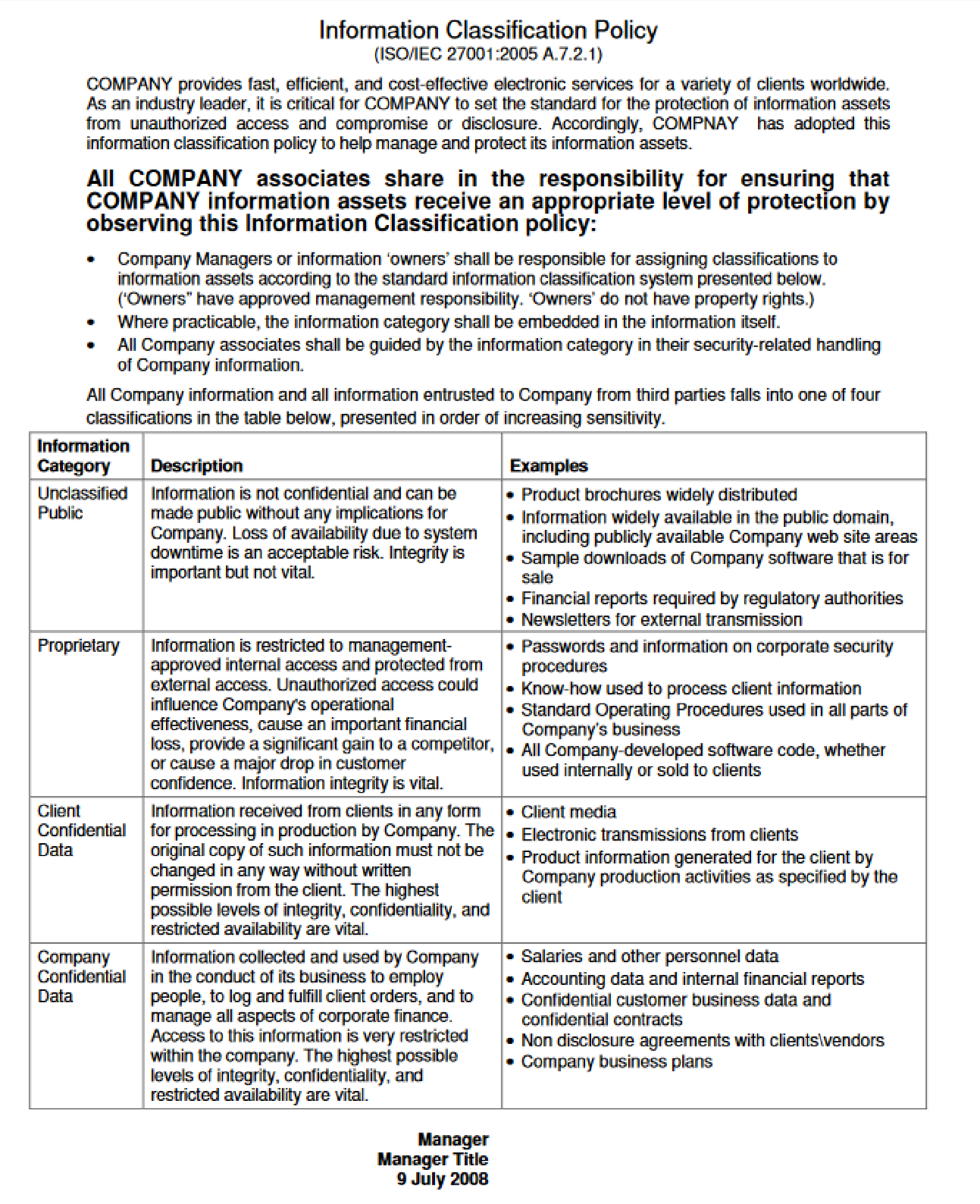
Title ____________________

The policy will be reviewed yearly by the Information Security Manager.

2 of 2

INTERNAL USE ONLY
Created: 2004-08-12

Source: http://security.stackexchange.com/questions/58810/iso-27001-procedures-templates-for-isms-at-small-companies



Information Classification Policy

(ISO/IEC 27001:2005 A.7.2.1)

COMPANY provides fast, efficient, and cost-effective electronic services for a variety of clients worldwide. As an industry leader, it is critical for COMPANY to set the standard for the protection of information assets from unauthorized access and compromise or disclosure. Accordingly, COMPNAY has adopted this information classification policy to help manage and protect its information assets.

All COMPANY associates share in the responsibility for ensuring that COMPANY information assets receive an appropriate level of protection by observing this Information Classification policy:

- Company Managers or information 'owners' shall be responsible for assigning classifications to information assets according to the standard information classification system presented below. ('Owners" have approved management responsibility. 'Owners' do not have property rights.)
- Where practicable, the information category shall be embedded in the information itself.
- All Company associates shall be guided by the information category in their security-related handling of Company information.

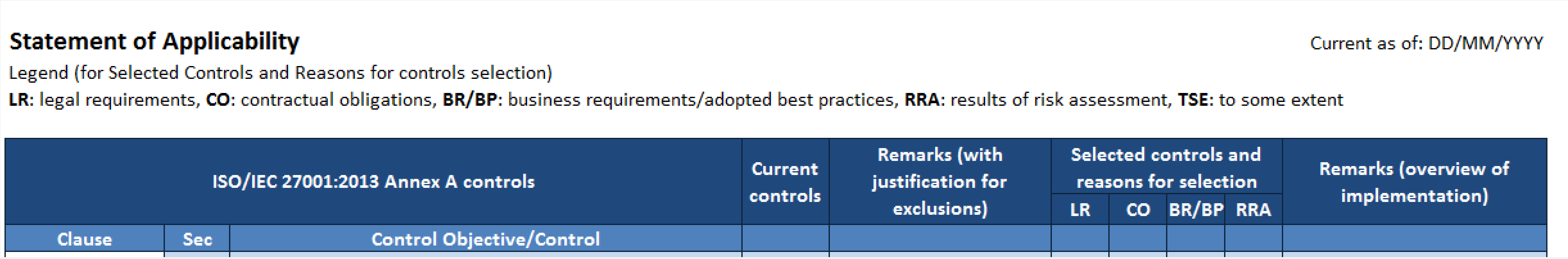
All Company information and all information entrusted to Company from third parties falls into one of four classifications in the table below, presented in order of increasing sensitivity.

Information Category	Description	Examples
Unclassified Public	Information is not confidential and can be made public without any implications for Company. Loss of availability due to system downtime is an acceptable risk. Integrity is important but not vital.	• Product brochures widely distributed • Information widely available in the public domain, including publicly available Company web site areas • Sample downloads of Company software that is for sale • Financial reports required by regulatory authorities • Newsletters for external transmission
Proprietary	Information is restricted to management-approved internal access and protected from external access. Unauthorized access could influence Company's operational effectiveness, cause an important financial loss, provide a significant gain to a competitor, or cause a major drop in customer confidence. Information integrity is vital.	• Passwords and information on corporate security procedures • Know-how used to process client information • Standard Operating Procedures used in all parts of Company's business • All Company-developed software code, whether used internally or sold to clients
Client Confidential Data	Information received from clients in any form for processing in production by Company. The original copy of such information must not be changed in any way without written permission from the client. The highest possible levels of integrity, confidentiality, and restricted availability are vital.	• Client media • Electronic transmissions from clients • Product information generated for the client by Company production activities as specified by the client
Company Confidential Data	Information collected and used by Company in the conduct of its business to employ people, to log and fulfill client orders, and to manage all aspects of corporate finance. Access to this information is very restricted within the company. The highest possible levels of integrity, confidentiality, and restricted availability are vital.	• Salaries and other personnel data • Accounting data and internal financial reports • Confidential customer business data and confidential contracts • Non disclosure agreements with clients\vendors • Company business plans

Manager
Manager Title
9 July 2008

Source: http://www.iso27001security.com/ISO27k_Model_policy_on_information_classification.pdf

ISO/IEC 27001 – Statement of Applicability (Example)



Statement of Applicability

Current as of: DD/MM/YYYY

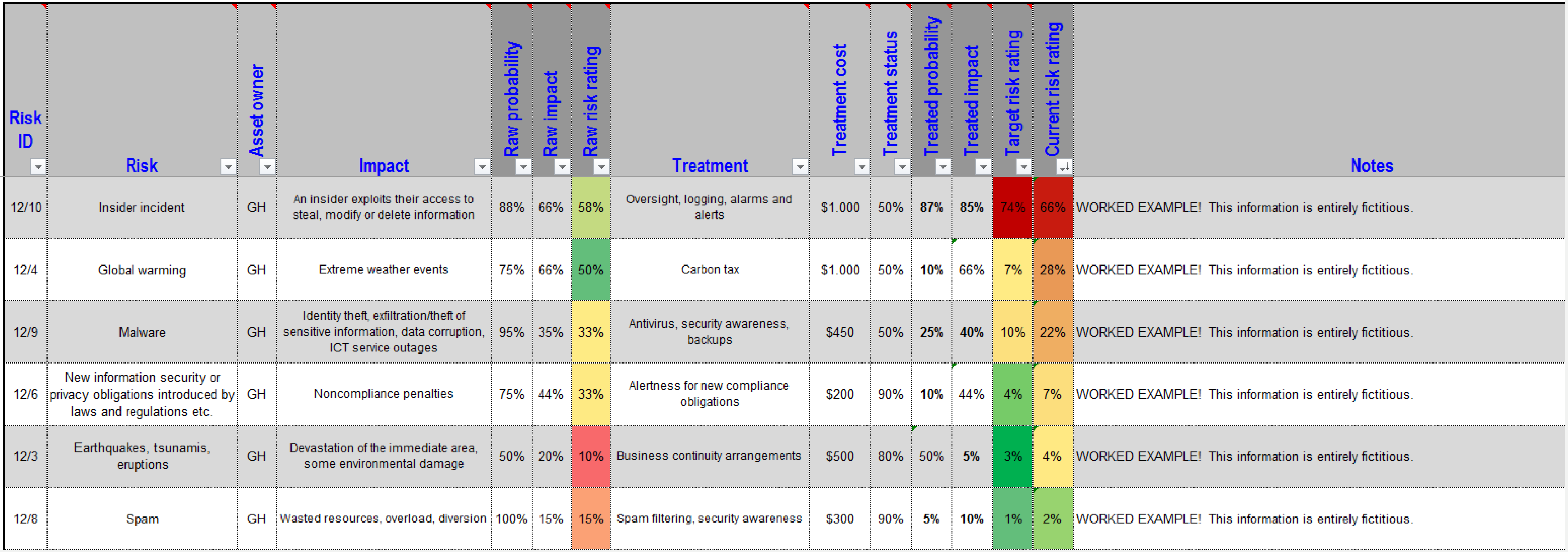
Legend (for Selected Controls and Reasons for controls selection)

LR: legal requirements, **CO**: contractual obligations, **BR/BP**: business requirements/adopted best practices, **RRA**: results of risk assessment, **TSE**: to some extent

ISO/IEC 27001:2013 Annex A controls			Current controls	Remarks (with justification for exclusions)	Selected controls and reasons for selection				Remarks (overview of implementation)
					LR	CO	BR/BP	RRA	
Clause	Sec	Control Objective/Control							

Source: http://www.iso27001security.com/ISO27k_SOA_2013_in_3_languages.xlsx

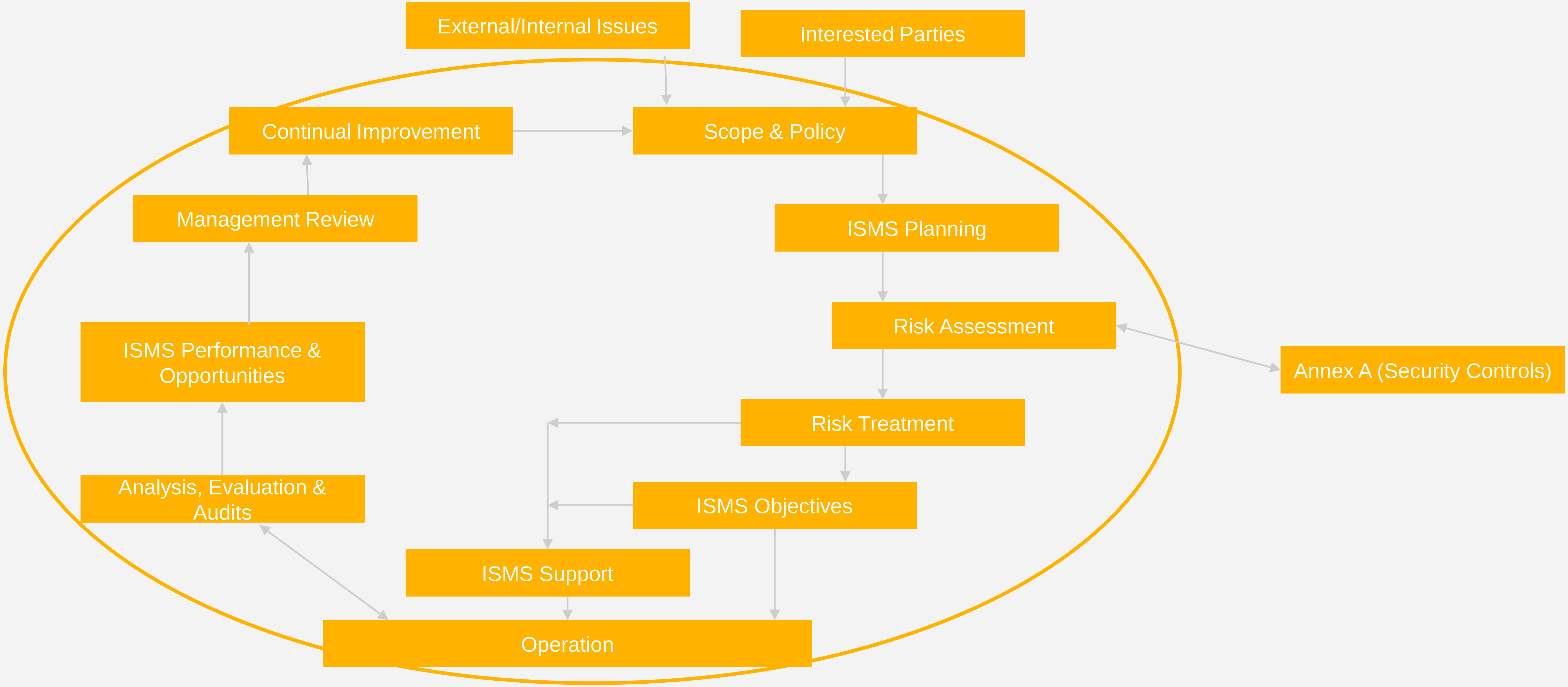
ISO/IEC 27001 – Risk Register (Example)



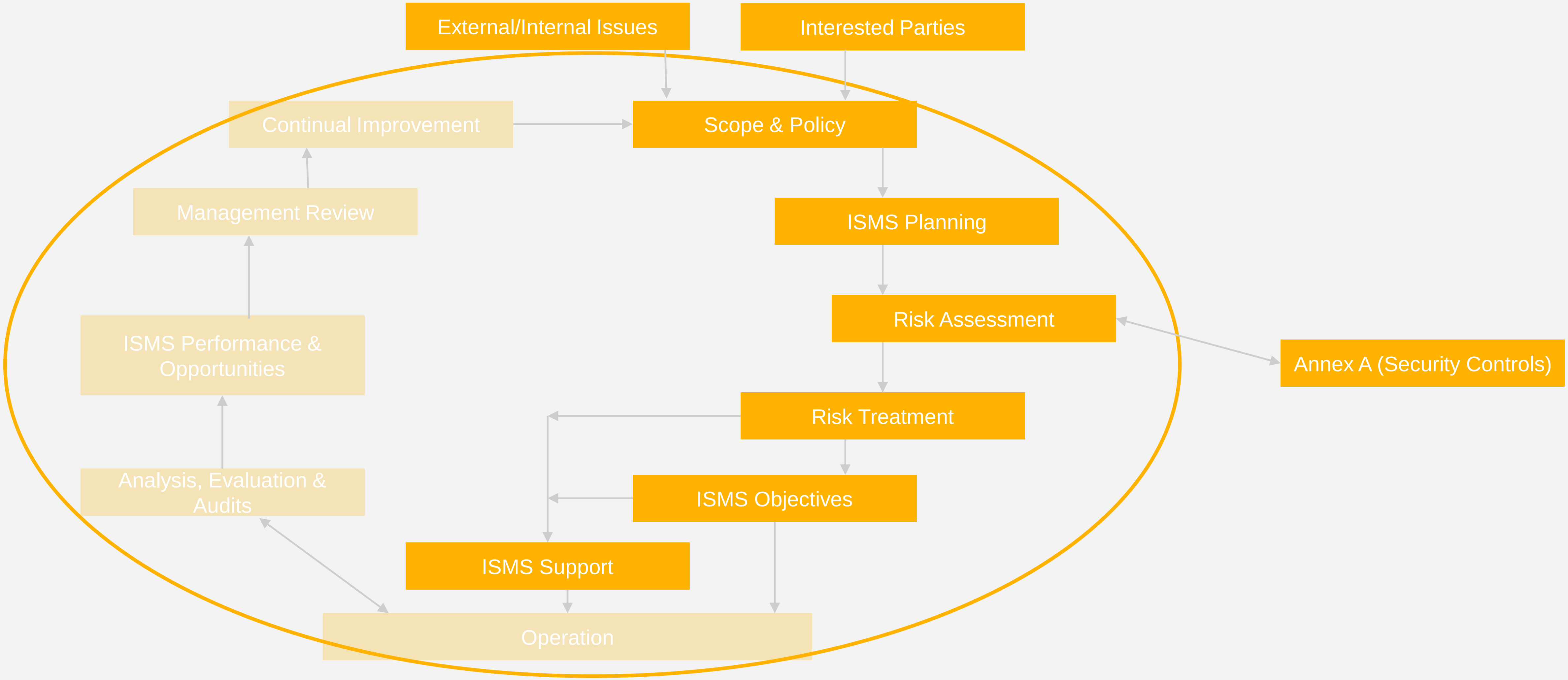
Risk ID	Risk	Asset owner	Impact	Raw probability	Raw impact	Raw risk rating	Treatment	Treatment cost	Treatment status	Treated probability	Treated impact	Target risk rating	Current risk rating	Notes
12/10	Insider incident	GH	An insider exploits their access to steal, modify or delete information	88%	66%	58%	Oversight, logging, alarms and alerts	$1.000	50%	**87%**	**85%**	74%	66%	WORKED EXAMPLE! This information is entirely fictitious.
12/4	Global warming	GH	Extreme weather events	75%	66%	50%	Carbon tax	$1.000	50%	**10%**	66%	7%	28%	WORKED EXAMPLE! This information is entirely fictitious.
12/9	Malware	GH	Identity theft, exfiltration/theft of sensitive information, data corruption, ICT service outages	95%	35%	33%	Antivirus, security awareness, backups	$450	50%	**25%**	**40%**	10%	22%	WORKED EXAMPLE! This information is entirely fictitious.
12/6	New information security or privacy obligations introduced by laws and regulations etc.	GH	Noncompliance penalties	75%	44%	33%	Alertness for new compliance obligations	$200	90%	**10%**	44%	4%	7%	WORKED EXAMPLE! This information is entirely fictitious.
12/3	Earthquakes, tsunamis, eruptions	GH	Devastation of the immediate area, some environmental damage	50%	20%	10%	Business continuity arrangements	$500	80%	50%	**5%**	3%	4%	WORKED EXAMPLE! This information is entirely fictitious.
12/8	Spam	GH	Wasted resources, overload, diversion	100%	15%	15%	Spam filtering, security awareness	$300	90%	**5%**	**10%**	1%	2%	WORKED EXAMPLE! This information is entirely fictitious.

Source: http://www.iso27001security.com/ISO27k_Risk_Register_v2.xlsm

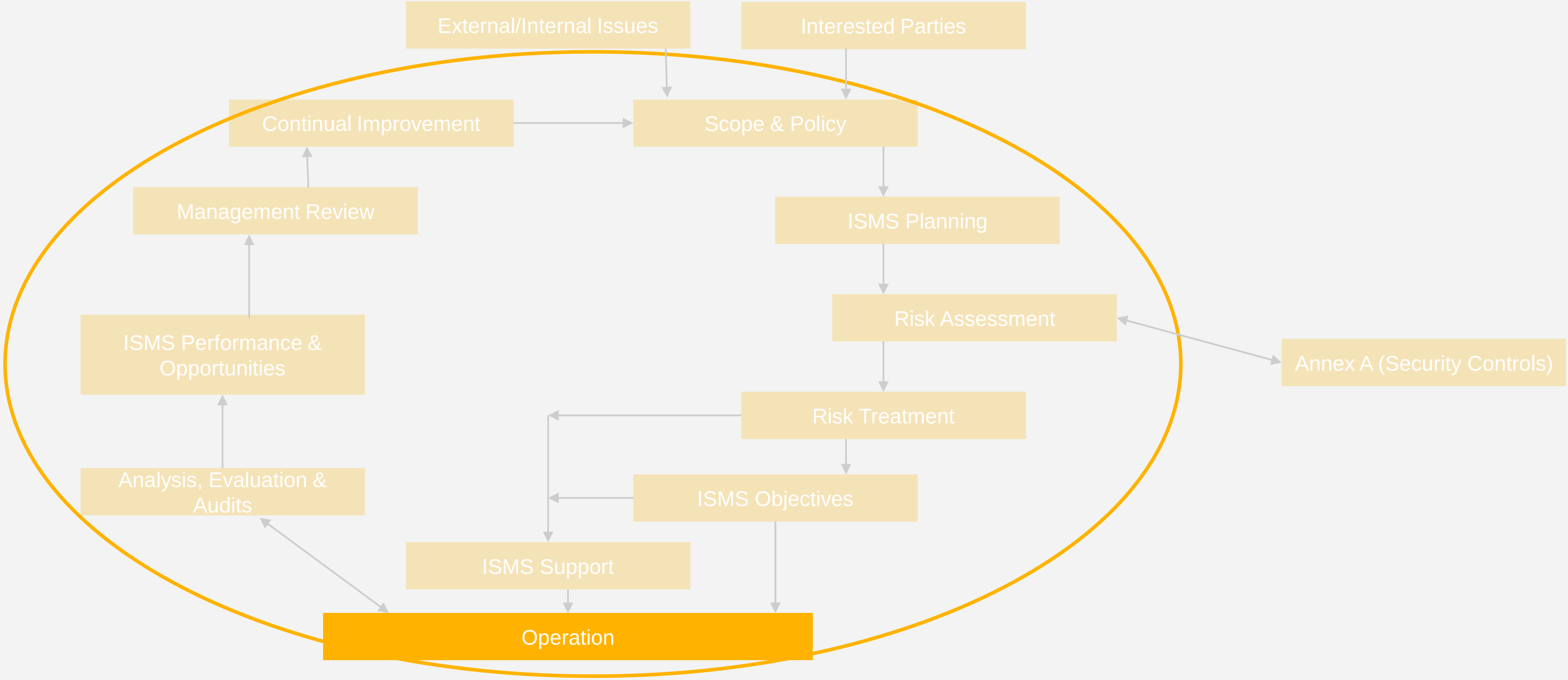
ISO/IEC 27001 – ISMS (ISO 27001:2013) Implementing



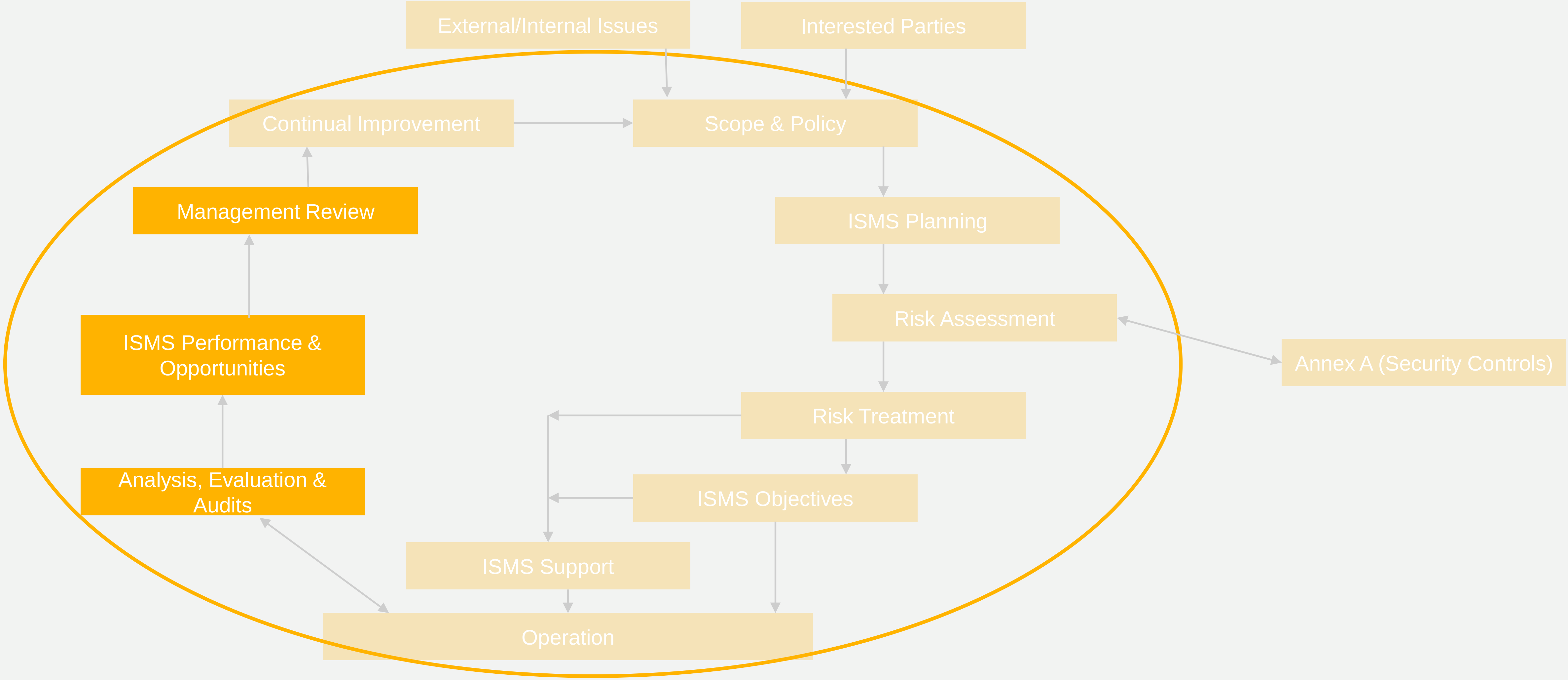
ISO/IEC 27001 – ISMS - Plan



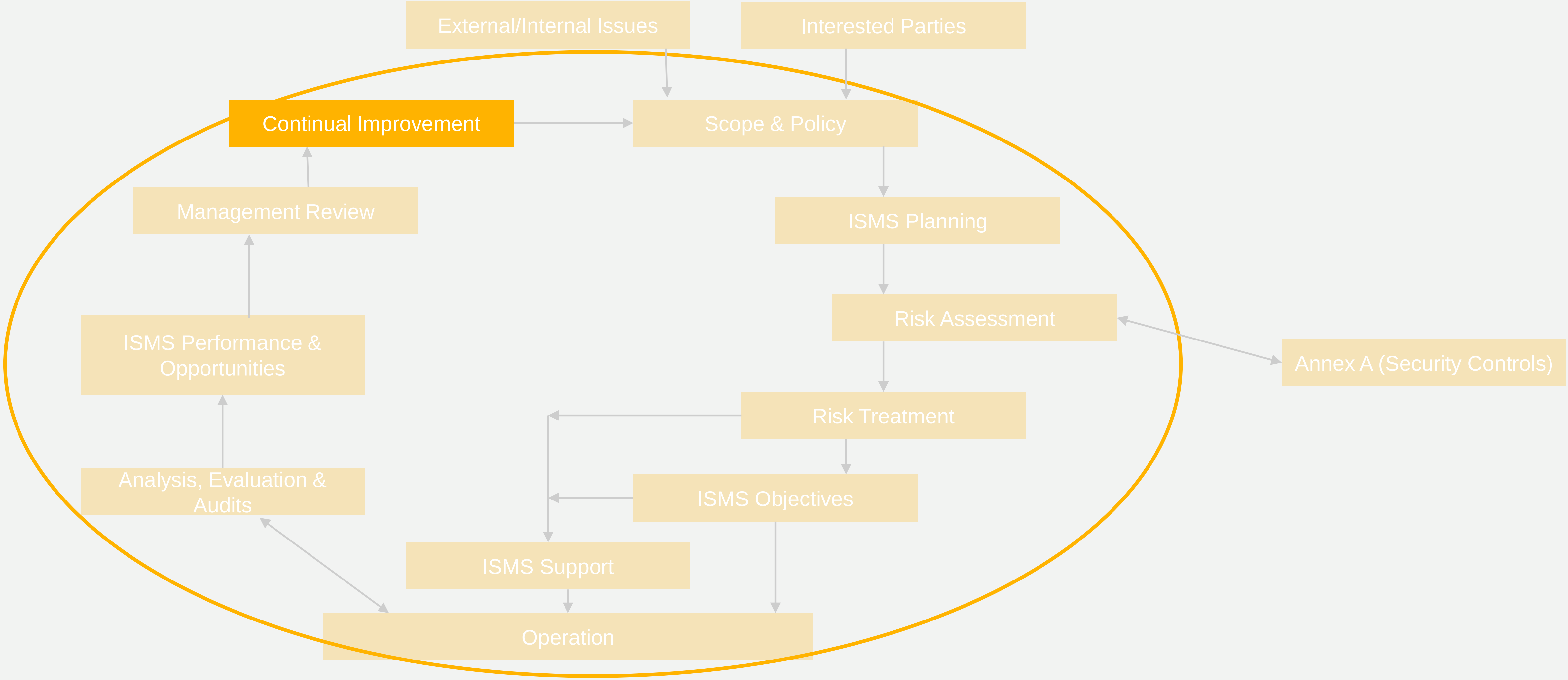
ISO/IEC 27001 – ISMS - Do



ISO/IEC 27001 – ISMS - Check



ISO/IEC 27001 – ISMS - Act



Auditing an ISMS

- ISO 19011 provides guidance on auditing management systems

- Aspects of an Audit
  - Scope: e.g. HR-, Development-, Sales-Departments, geographic locations etc.
  - Criteria: e.g. ISO2700x, Company Internal Regulations/Policies etc.
  - Objectives: Certifications, Compliance with internal regulations, Improvements in Processes

- Types of Audits
  - First party – Intern
  - Second Party – Customer or Provider
  - Third Party – Certification or Independent

- Audit Evidences
  - Documented Information
  - Observations
  - Interview

Summary

- ISMS is approach for providing security of company sensitive information
- Need for an ISMS because of critical IT-Security Situation and Compliance (see e.g. German Act “IT-Sicherheitsgesetz”)
- The most important ISMS Objectives: Confidentiality, Integrity and Availability (CIA)

- Information Security Standards: ISO 2700x Series, ISO 13335, ISO 17799, COBIT, ITIL
- ISMS Process (Plan, Do, Check and Act)

Questions?

Thank you very much for your Attention!

„Nichts in dieser Welt ist sicher, außer dem Tod und den Steuern.“

(Benjamin Franklin)

References

- http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
- https://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/it-sicherheitsgesetz.pdf?__blob=publicationFile
- https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-1_e_pdf.pdf;jsessionid=A7649BB8D1210C17DDEEEF9722F4B57D.2_cid368?__blob=publicationFile&v=1
- https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2015.pdf?__blob=publicationFile&v=2
- http://www.iso.org/iso/catalogue_detail?csnumber=50675
- http://www.iso27001security.com/html/toolkit.html