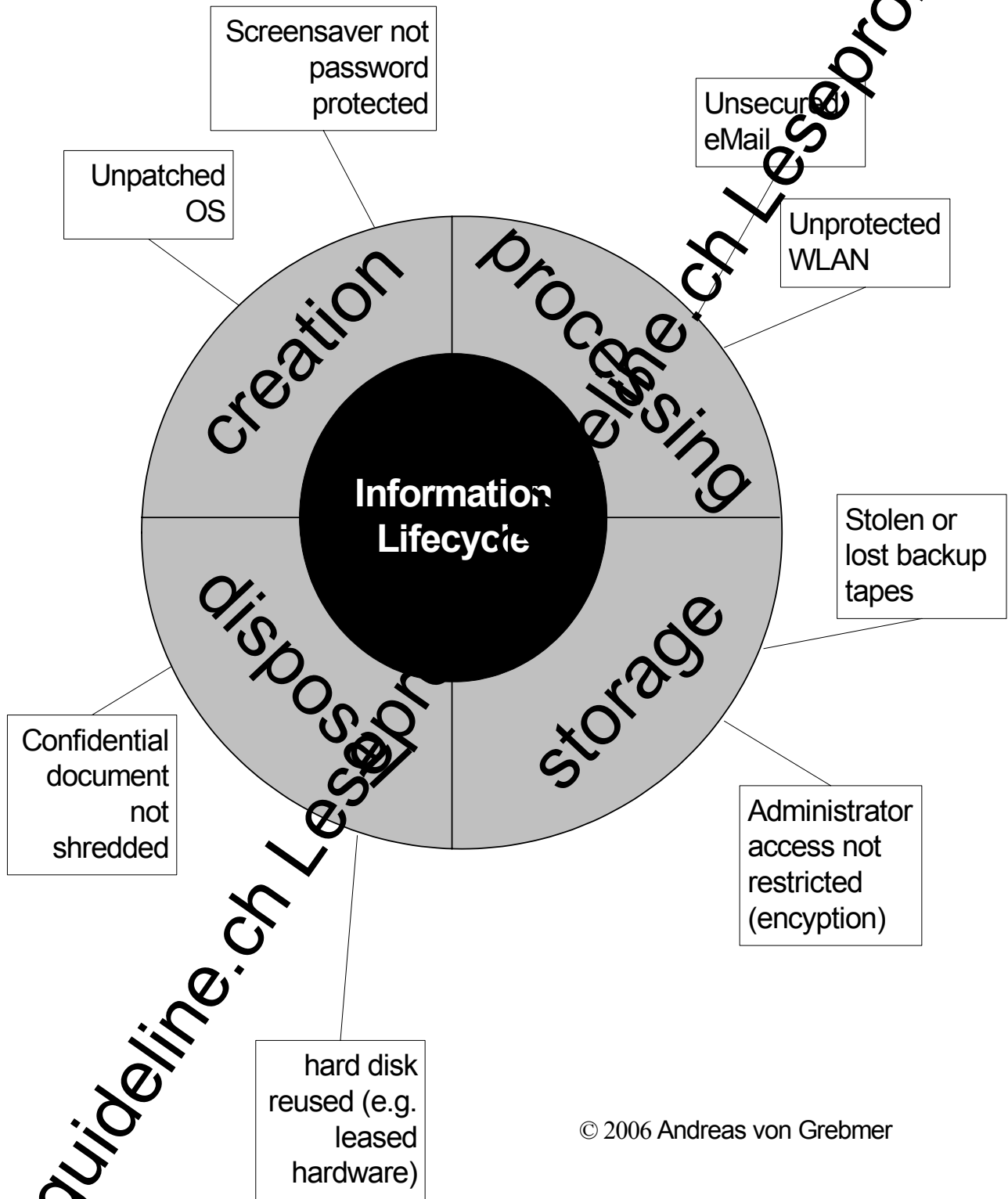


Information and IT Risk Management in a Nutshell

A pragmatic approach to
Information Security

Andreas von Grebmer

Possible threats (risks) during this lifecycle are

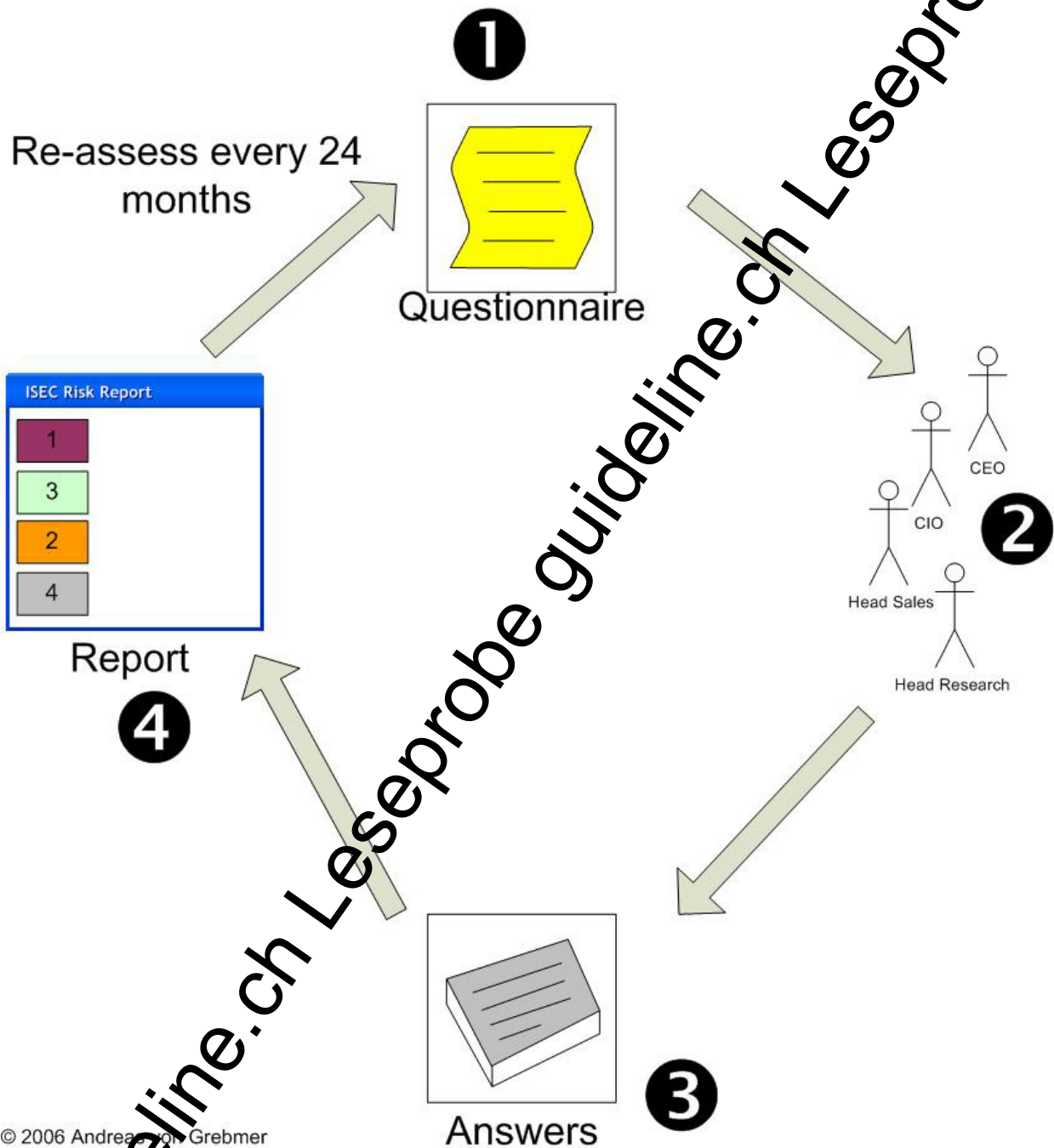


© 2006 Andreas von Grebmer

The importance or criticality of the information for a business or information regulatory

threatening your business both now and in the future. This survey should be redone every 18 to 24 months to monitor changes.

Diagram 12: Management Survey



© 2006 Andreas von Grebmer

1.3.2. Expert Survey

Another source for defining potential risks to your organization is expert surveys. Ask your Information Security officers, coordinators etc. what they see as the major risks. In

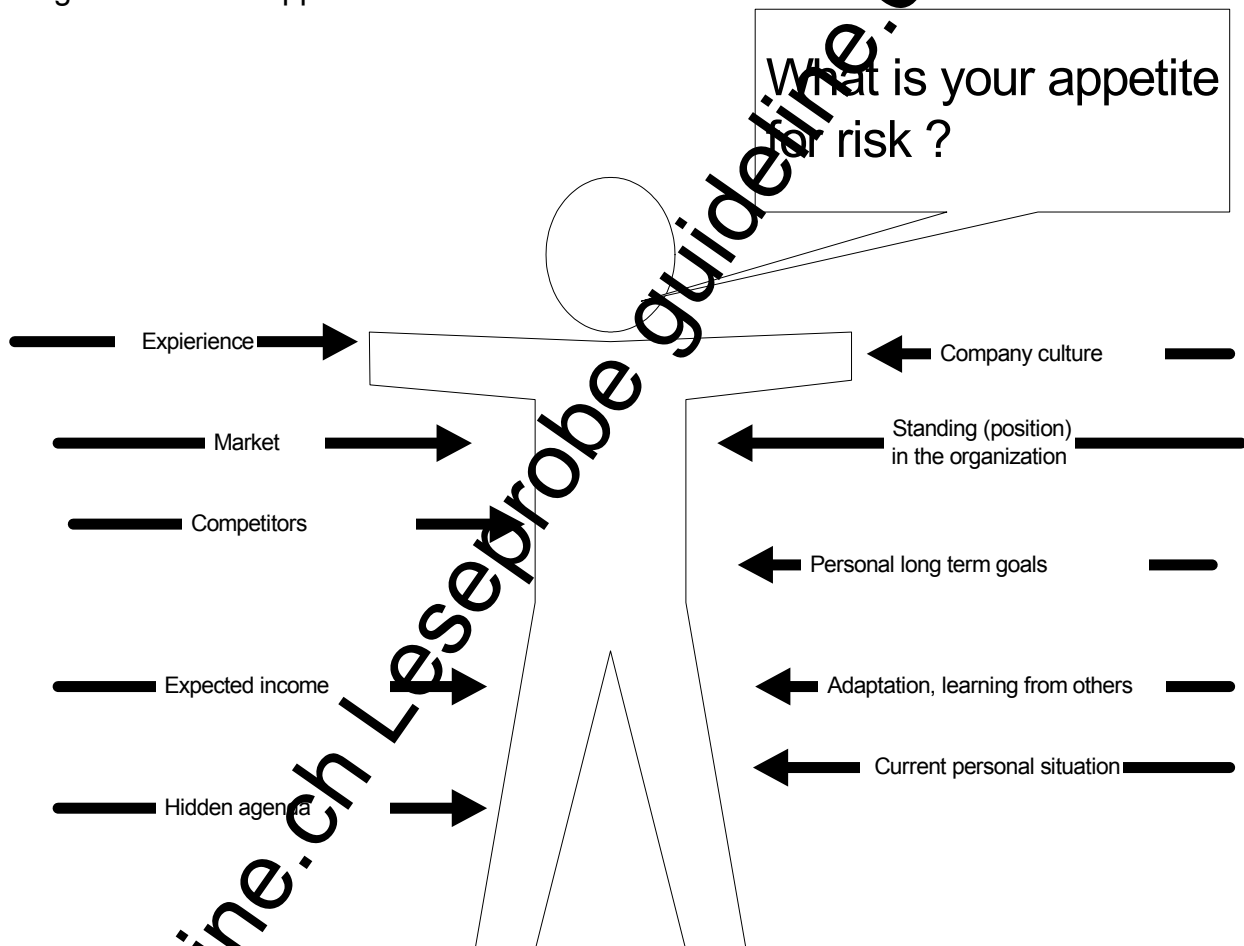
1.6 Risk Appetite and Risk Culture

Risk appetite is the amount of risk that an individual is willing to take (or willing to face). Risk culture describes the amount of risk that an entity is willing to take. Defining the organization's risk appetite/culture is an executive responsibility.

It is important that you know your own risk appetite, because it drives your risk management activities if you are in a position in the company that is responsible for risk management.

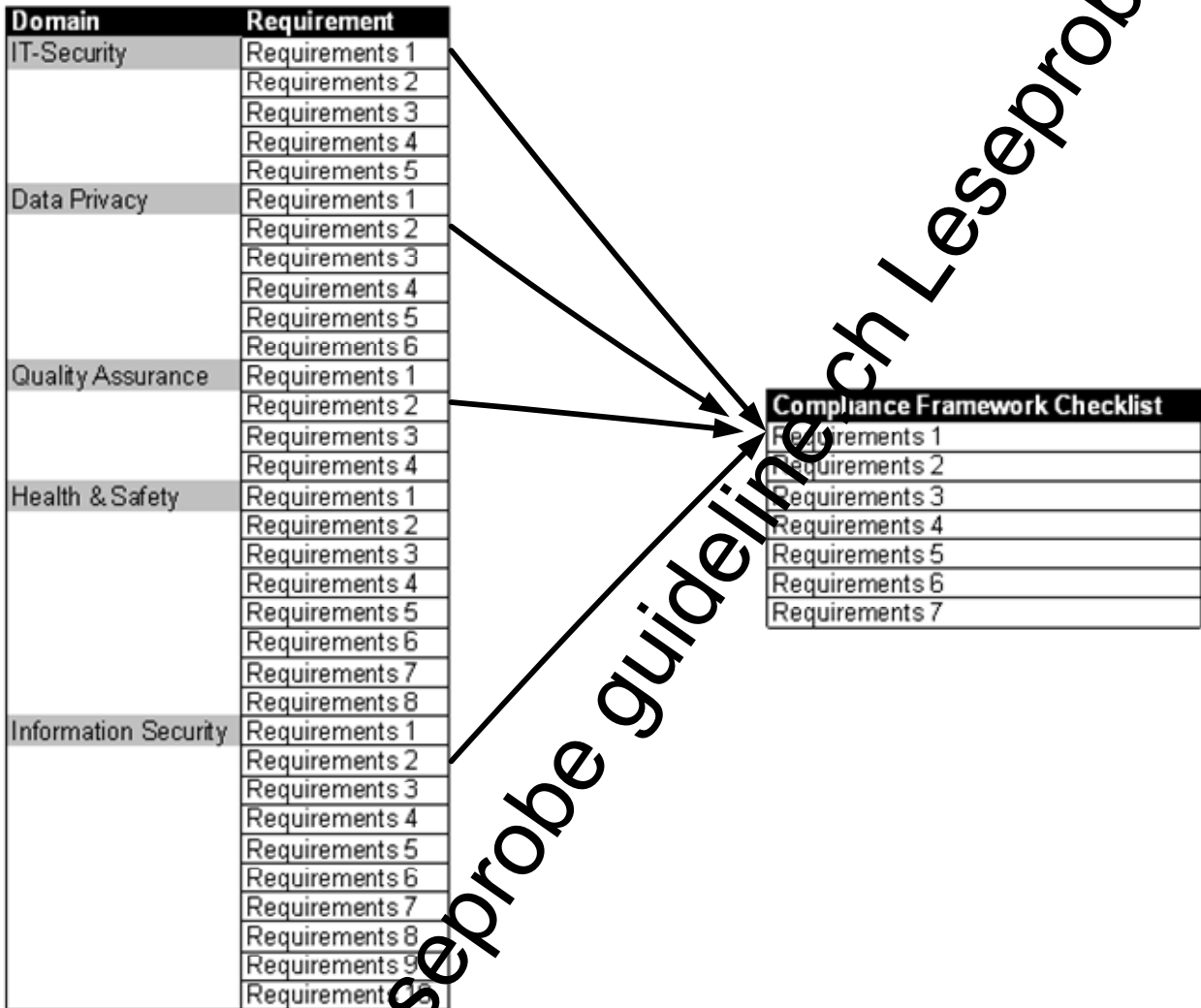
What sets your risk appetite? What influences your risk appetite? This diagram shall illustrate what factors influence this (maybe there are more factors).

Diagram 15: Risk Appetite



© 2006 Andreas von Grebmer

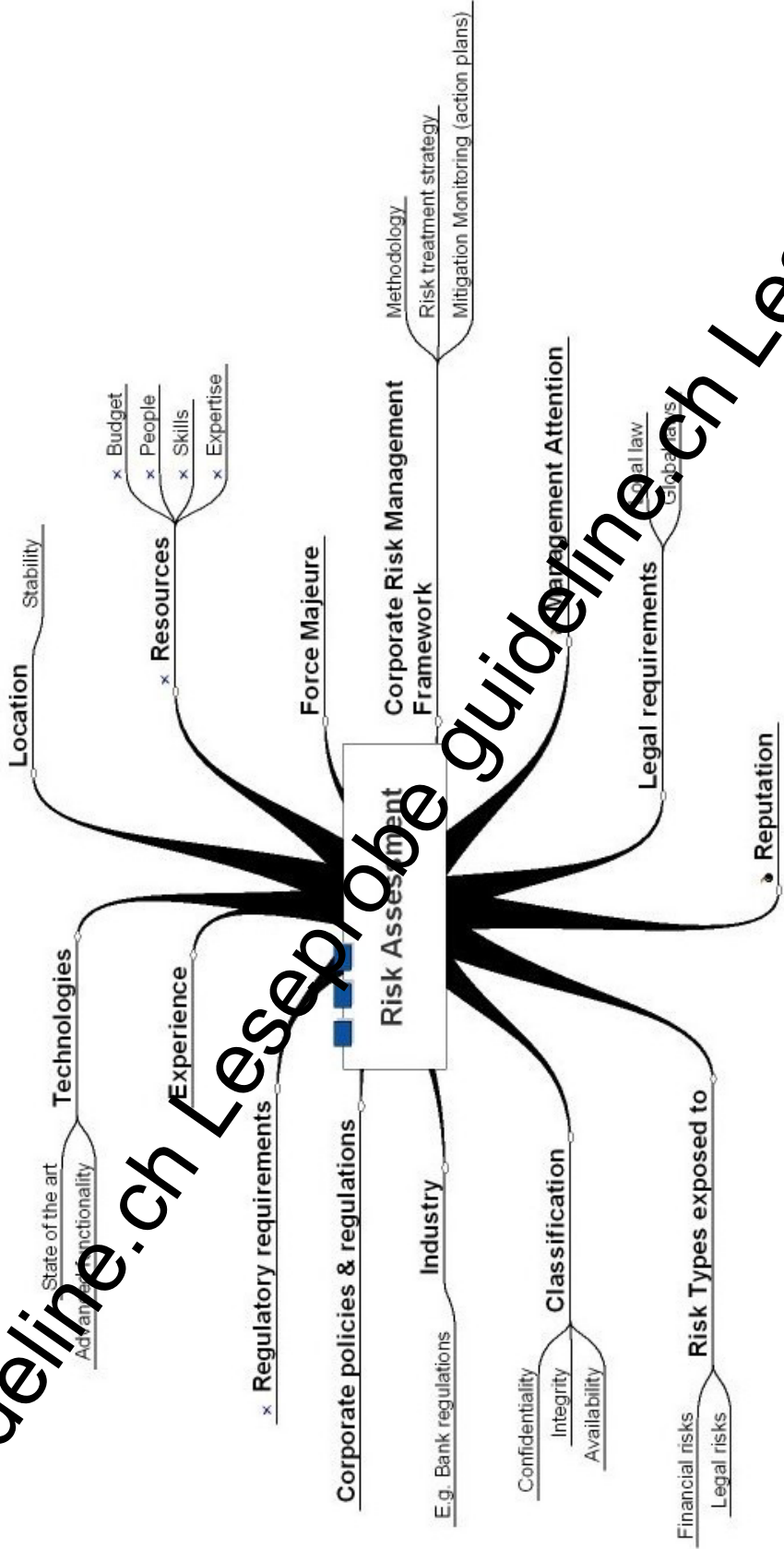
Diagram 20: Consolidating compliance requirements



1.8 System Risk Assessment

Imagine the following day-to-day situation: the implementation of a single IT system, a business process or just a new procedure. This often occurs in a dedicated project. You focus on the system and its direct and (if necessary) indirect interfaces. Indirect interfaces are interfaces that feed direct interfaces to your system. Indirect interfaces are generally not well controlled and present risks of corrupt or inaccurate data. The implementation bears two kinds of risks. First technological risks e.g. a standard application server usually implies a high number of security risks that could have an impact on your infrastructure. Secondly there are business risks if the new system is not performing correctly or reliably. These kinds of risks are compiled in a System Risk Assessment.

Diagram 27: Risk Assessment Influences Mind Map with dependency examples

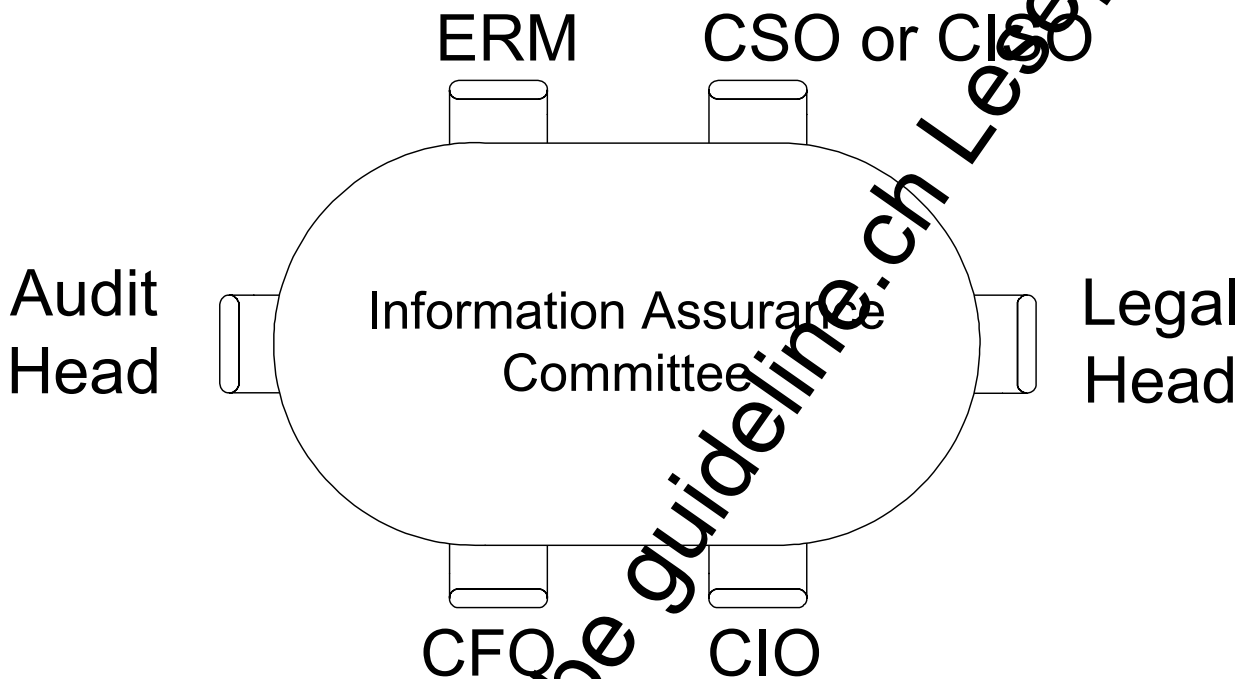


Same symbols show where possible relations are.

Copyright 2006 Andreas von Grebmer

players in your organization. This could for example be accomplished by building an information assurance committee that oversees all activities for information protection.

Diagram 33: Information assurance committee



The information assurance committee should meet at least twice a year and take necessary decisions to set a clear strategy and bundle or assign resources for information assurance.

Possible agenda for an information assurance committee:

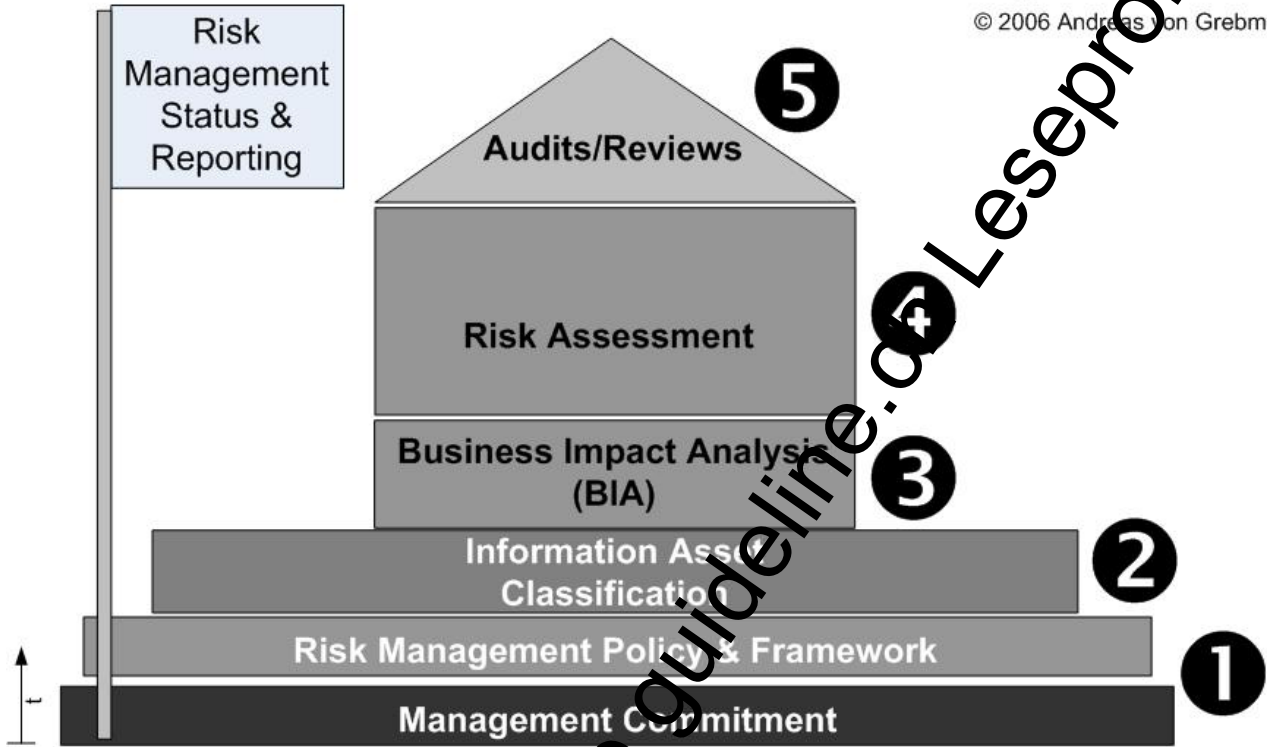
- Incidents and Incident response, audit observations
- Remaining information risks
- Strategic information security projects/security architecture
- Necessary actions
- Information security budget
- Third party risks
- New policies and regulations

With these contributions you have the capability to build your “House of risk management”, being your enterprise information risk management framework:

Diagram 34: House of information risk management






"The house of information risk management"

© 2006 Andreas von Grebmer







Step 1 For your risk management framework you need, first of all, a policy founded and supported by the top management. This ensures the appropriate level of importance and buy-in from the business. The responsibility lies with the management.






Involved roles:

 Senior management	 Enterprise or chief risk manager	 Business owner, Process owner, Information owner	 Information Security	 Audit
--	---	---	---	--

Step 2 The next step is an inventory and adequate classification of all information assets. This is the basis of every risk assessment. Without the notion of the value of an asset it is not possible to determine the business impact on an asset.

			
Business owner Process owner Information owner	Service provider	Subject matter expert	Information Security

Step 3 The Business Impact Analysis provides you with the critical assets for which you perform a risk assessment.

				
Enterprise or chief risk manager	Business owner Process owner Information owner	Service provider	Subject matter expert	Information Security

Step 4 The risk assessment analyses the measures implemented ensuring availability, integrity and confidentiality of an asset. The outcome of risk assessments are action plans containing security measures to be implemented to protect information assets.






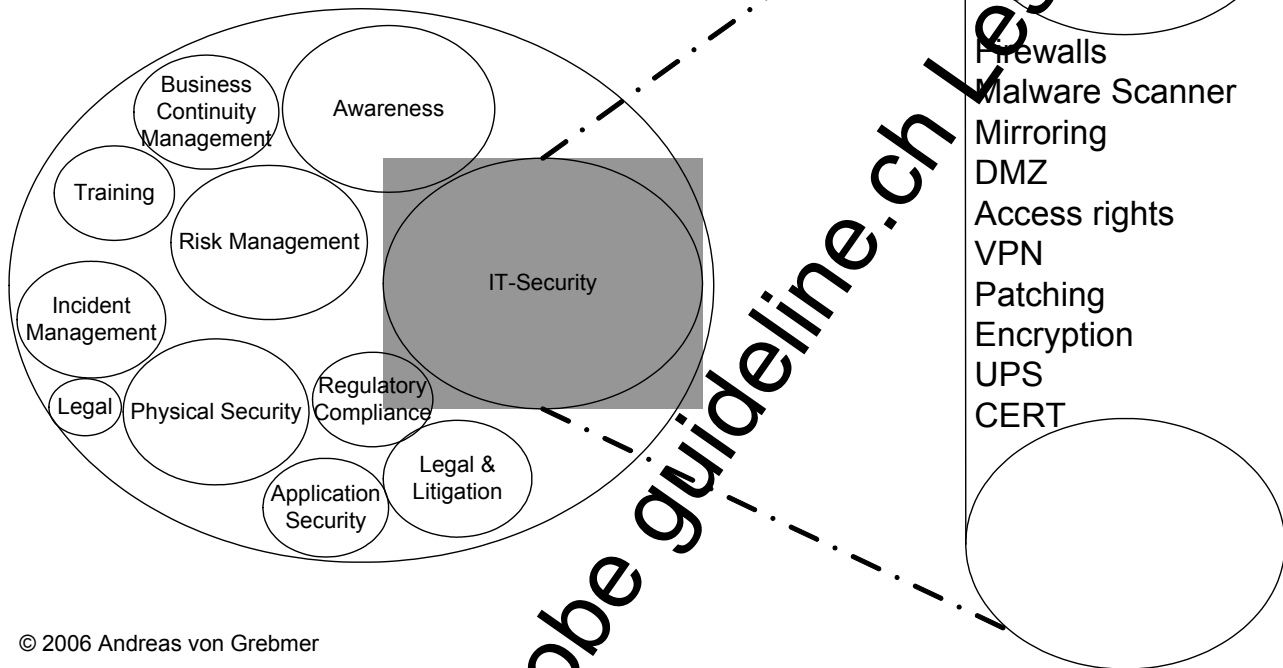
				
Business owner Process owner Information owner	Service provider	Subject matter expert	IT Security	Information Security

Diagram 45: Topics of Information and IT Security

Information Security

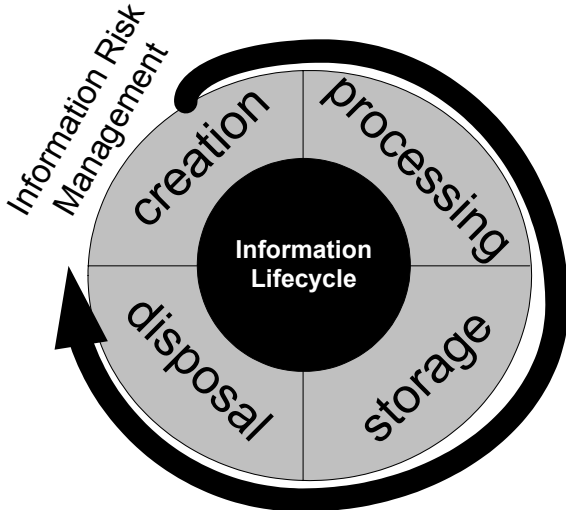


© 2006 Andreas von Grebmer

Information Security covers but is not limited to these following topics:

Topic	Content
Awareness	The level of maturity that your employees have in respect to Information Security. Besides training, management attention to Information Security is the main driver towards a sustainable awareness level amongst your employees.
Physical Security	An Information Security zone concept for facilities, buildings and premises is defined and established. An Information Security zone concept to categories of rooms and their contents helps to get an overview and the right level of security.
Training	Information Security training modules for various target groups such as Building Manager, HR Specialists, IT Help Desk Staff etc. are available. Information Security specialists get training from external institutes.
Business Continuity Management	Business Continuity Planning (BCP) and Disaster Recovery (DRP) are in place and tested. Management is aware and

- Information creation
- Information processing (incl. transmission)
- Information storage
- Information disposal



© Andreas von Grebmer

The classification (CIA) drives the measures taken to protect the information during its lifecycle. The disposal phase is as important as the others, because the information might still be of great interest for others (confidentiality).

See Information Owner
 See Information Custodian
 See CIA

Information Owner

→ Information Management

The person or organization owning the information. A delimitation exists in respect of the process owner: a process owner owns a business process which uses information, but this information must not necessarily be owned by the process owner, so the process owner must work with the relevant information owner or information custodian. The Information owner is responsible for the classification of the information. Classification can not be delegated to the information custodian or information user.

See Information Custodian.
 See Information Classification
 See CIA

Information Risk

→ Information Management

All business related risks associated with valuable information (assets).

Information Security

→ Definition, ISO/IEC 17799:2000

→ Definition, ISO/IEC 27001:2005

Preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability,

non-repudiation and reliability can also be involved.

ISO Definition: "Information is an asset which, like other important business assets, has value to an organization and consequently needs to be suitably protected. Information security protects information from a wide range of threats in order to ensure business continuity, minimize business damage and maximize return on investments and business opportunities. Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Whatever forms the information takes, or means by which it is shared or stored, it should always be appropriately protected. Information security is characterized here as the preservation of

- a) Confidentiality: ensuring that information is accessible only to those authorized to have access;
- b) Integrity: safeguarding the accuracy and completeness of information and processing methods;
- c) Availability: ensuring that authorized users have access to information and associated assets when required.

Information security is achieved by implementing a suitable set of controls, which could be policies, practices, procedures, organizational structures and software functions. These controls need to be established to ensure that the specific security objectives of the organization are met."

Information Security Awareness

→ Information management

In your enterprise you have to build up information security awareness to a degree that is necessary to run your business. The more you have unique products and processes the more effort you have to spend to obtain a consistent high level of awareness of ALL your employees. A typical approach is to establish an initial awareness training that all employees have to pass with follow up training raising special topics. The training records should be tracked and the management must support the campaign. The program must transmit the main corner stones of your information security program to your employees, e.g.

- Classification of information
- How to treat which classification level
- How to report an incident
- Basic regulations like disposal of information, e-mail and internet rules
- The responsibilities they have in their role
- When and how to encrypt information

A key target of the ISEC awareness program must be the development of a common language in your company e.g. the definition what is "strictly

confidential” and how to handle information assets that carry this kind of information.

Information Security Event

→ Definition, ISO/IEC TR 18044:2004

An identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.

Information Security Forum

→ Organizations

The Information Security Forum is the world's leading independent authority on information security. <http://www.securityforum.org>.

Information Security Incident

→ Definition, ISO/IEC TR 18044:2004

A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

Information Security Management System (ISMS)

→ Organizations

The Information Security Management System is the framework set up to steer and monitor the information security within an organization, e.g. reporting lines, KPIs, score card etc. It is part of the overall management system, based on a system risk approach, to establish, implement, operate, monitor, review, maintain and improve information security. It includes organizational structure, policies, planning, responsibilities, practices, procedures, processes and resources.

Information Security Standards

→ Information Management

- BS7799
- ISO17799
- ISO27001

Information Systems Audit and Control Association (ISACA)

→ Organizations

Founded in 1967. See www.isaca.org.

Infrastructure

→ Definition

Infrastructure in the context of this book means all tangible things (except humans) that are needed to create, transmit, store or dispose of information. Examples: Input terminal, LAN, router, printer, fax etc.

Integrity

→ Definition, ISO/IEC 13335-1:2004

The property of safeguarding the accuracy and

completeness of information (-assets, software and procedures).

International Standard Organization

→ Organizations

ISO is a network of the national standards institutes of 157 countries, on the basis of one member per country, with a Central Secretariat in Geneva, Switzerland, that coordinates the system. www.iso.org.

ISACA, see Information Systems Audit and Control Association

ISEC, see Information Security

ISF, see Information Security Forum

ISO, see Information Standard Organization

ISO/IEC17149

→ Information Security Standards

“Information technology — Code of practice for information security management”, First edition 2005-12-01. Provides implementation guidance that can be used when designing controls for ISO27001. IEC stands for International Electro technical Commission.

ISO26300

→ Security Standards

Open-Document-Format (ODF), vendor independent document for long term storage of documents. Does not contain meta-data descriptions.

ISO27001

→ Information Security Standards

First edition 2005-10-15. ISO standard for „Information technology – Security techniques – Information security management system – Requirements“. Describes control objectives and controls for an ISMS on a high level. Also lists correspondence between ISO27001, ISO 9001:2000, ISO14001:2004. IEC stands for International Electro technical Commission.

ISO27002

→ Information Security Standards

ISMS Implementation Guidance, outlining controls and mechanisms. Successor of ISO17799

ISO27003

→ Information Security Standards

ISMS Implementation Guidance and help. Expected 2008/2009.

ISO27004

→ Information Security Standards

ISMS Metrics and Measures. Emerging standard.