

Corporate Security

- Practice Session -

Information and Communication Security
WS 2008/2009

Goethe Universität
Frankfurt am Main
26. November 2008



Agenda

1. Introduction to Corporate Security
2. Guidance on Implementing a Security Management Framework
3. Tools and Best Practices
4. Practical Session: Security Policy Development

Corporate Security

Introduction



In executing key business processes, organisations depend on a well-functioning information supply...

- ... that is there when needed
- ... that is reliable
- ... that is available only to those who are authorised to have access to it

➤ The criteria above is not always equally important!

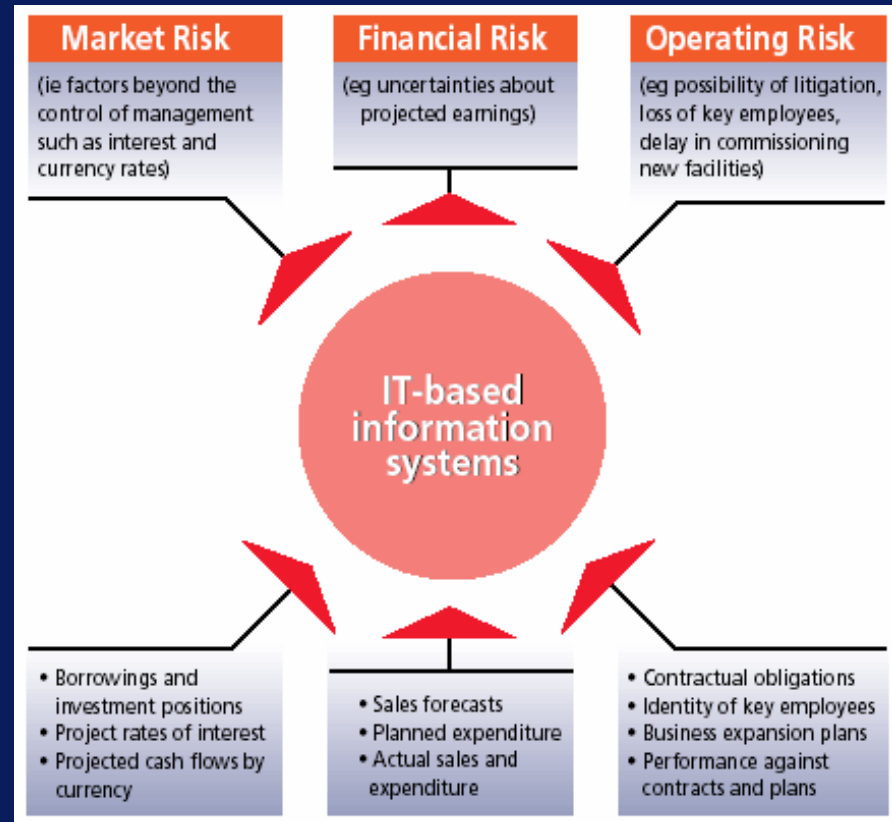


An organisation must therefore organise the collection, storage, handling, processing and provision of data in such a way that these conditions are satisfied.

Corporate information is now almost entirely processed, stored or transmitted by computer systems.

Corporate Security is necessary due to ...

- the potential impact on other forms of risk (see picture)
- increasing dependence on IT-based information systems
- the scale of IT investment
- the ever growing vulnerability of systems
- new IT-based methods of doing business



Source: Information Security Forum

Managing risks associated with IT-based information systems is vital!

“Remember, you are protecting information assets, not computer systems. It is a risk management problem that deals with people, process and technology. You’ve got to integrate all three to protect those assets.”

John Lindquist,
CEO EWA Information and
Infrastructure Technologies

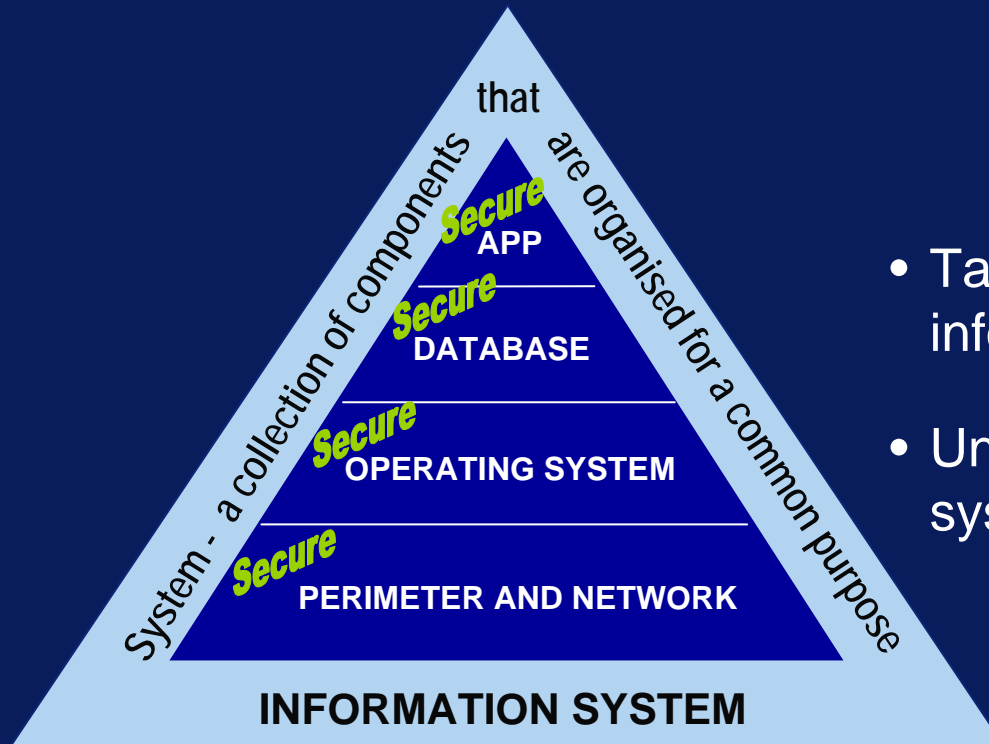




Corporate Security

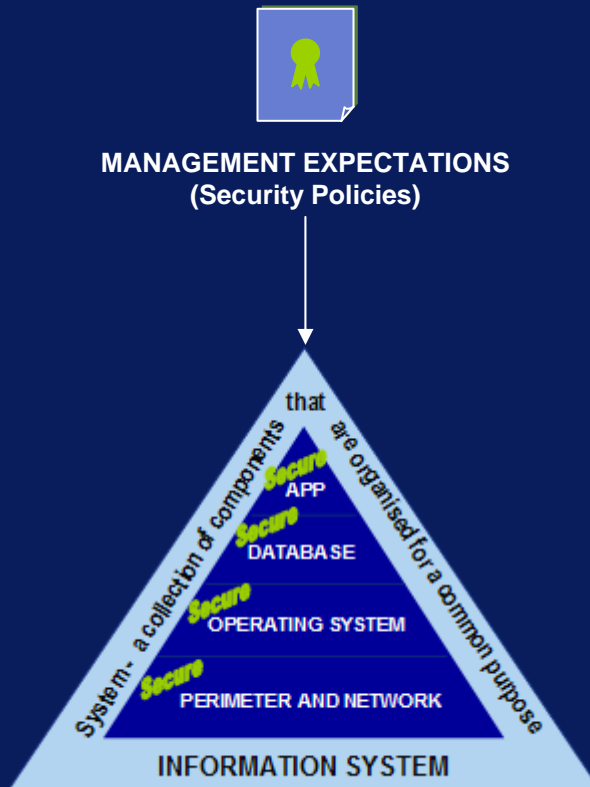
Guidance on
Implementing
a Security Management
Framework

Step 1: Target security efforts



- Take a business view of an information system
- Understand the value of that system to the business

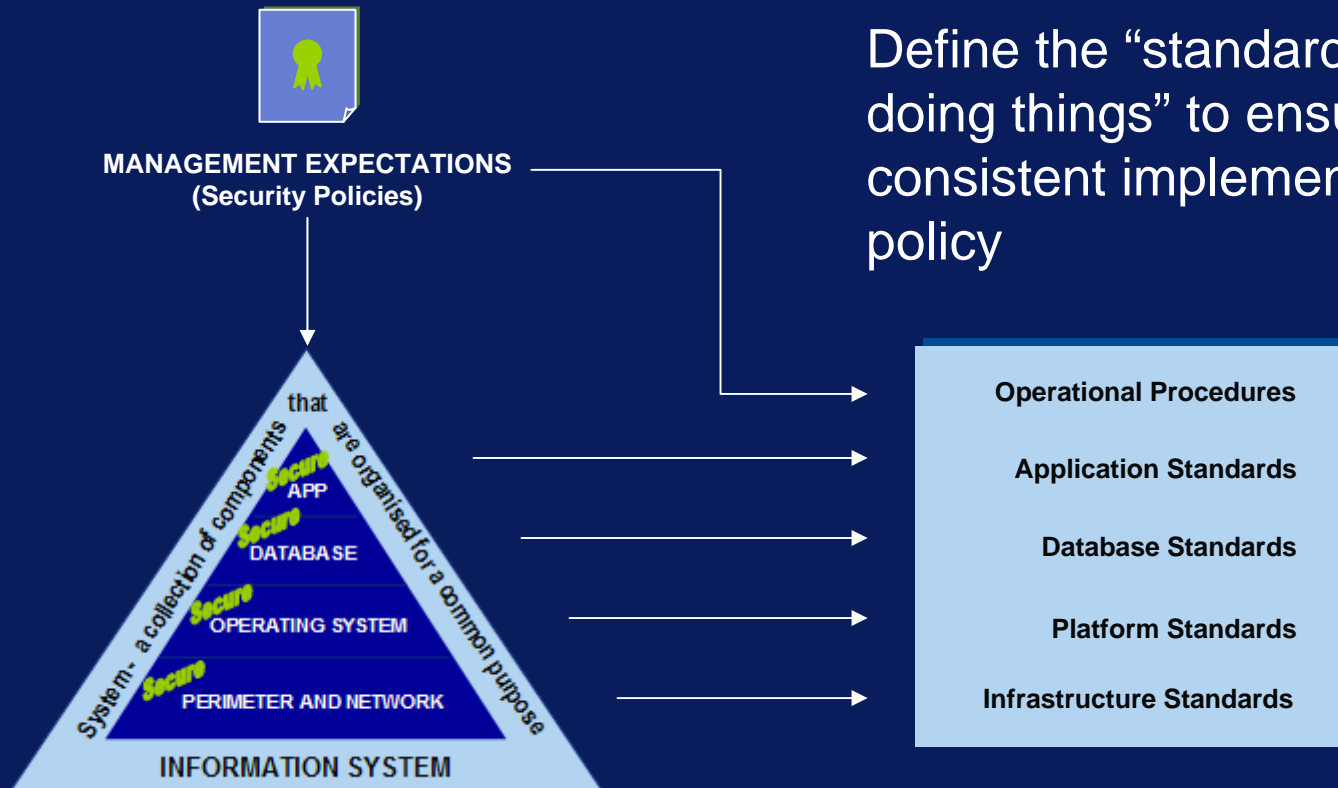
Step 2: Document security objectives



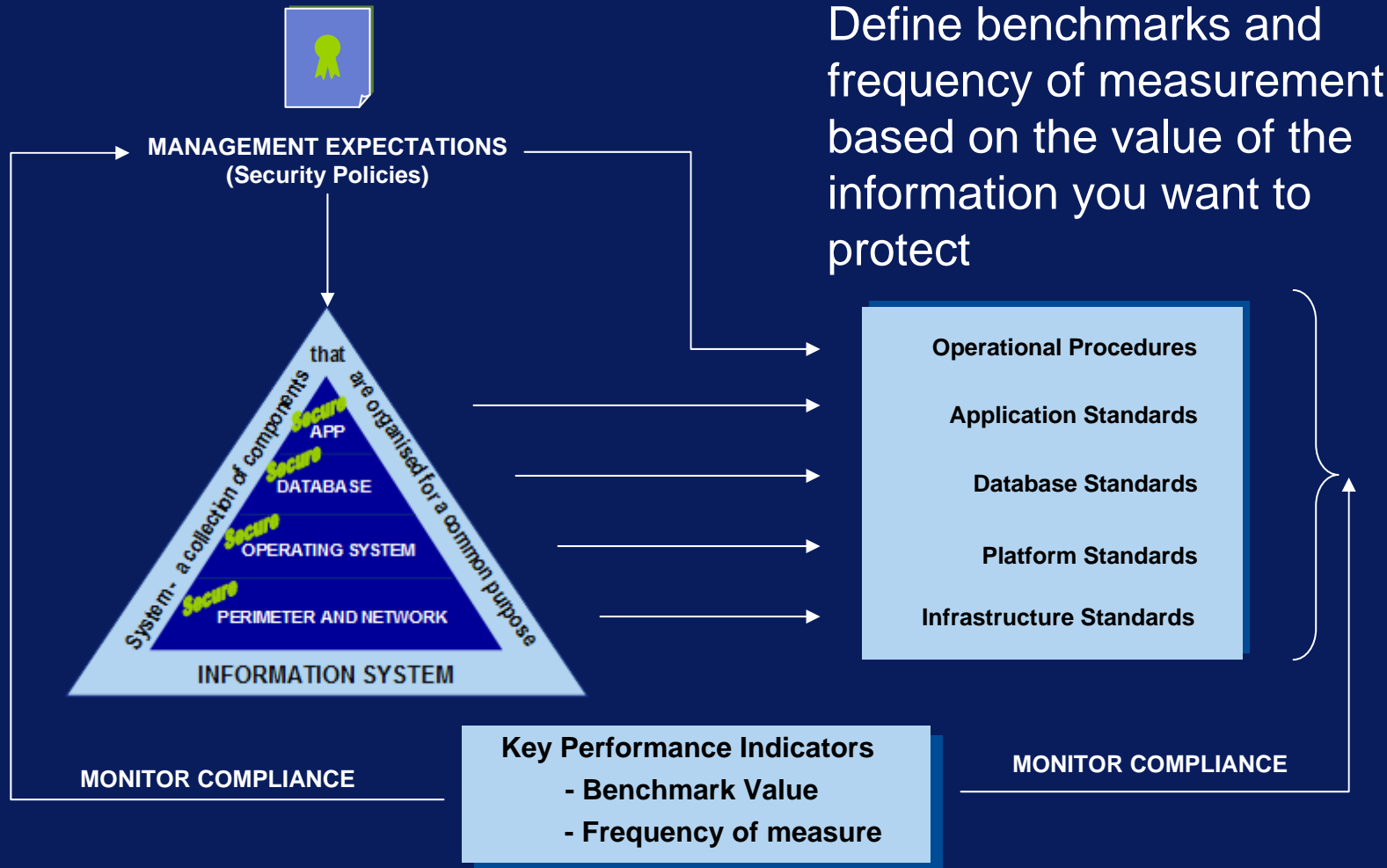
Apply Management Expectations for security to information systems. Consider:

- target company's risk appetite
- legal or legislative requirements
- principles of due care
- best practices
- previous incidents
- auditor recommendations

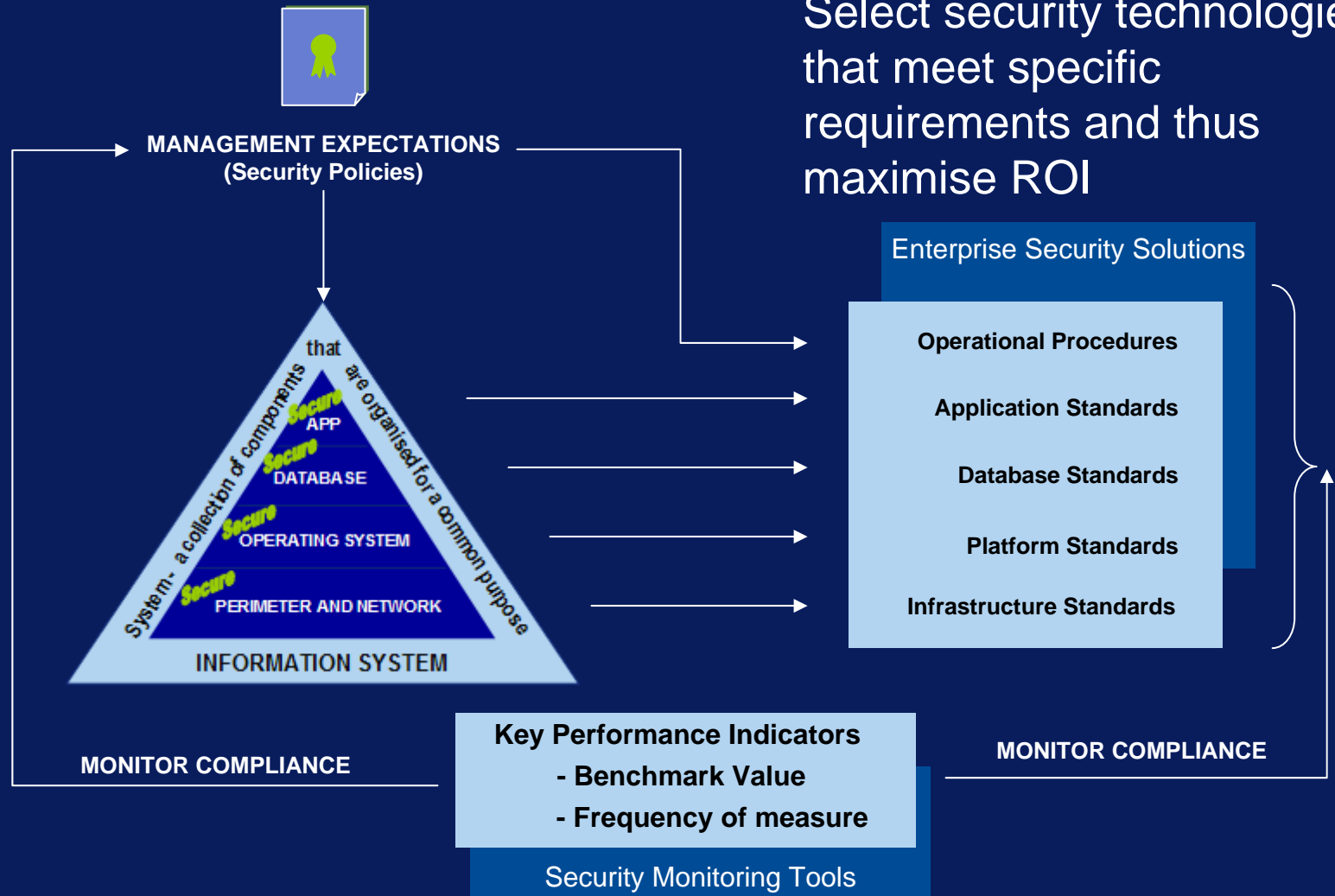
Step 3: Define policy-derived security controls



Step 4: Monitor and measure compliance



Step 5: Choose enabling technologies



Corporate Security

Tools and
Best Practices



Tools and Best Practices

Policy Implementation

The following supporting elements are derived from a security policy:

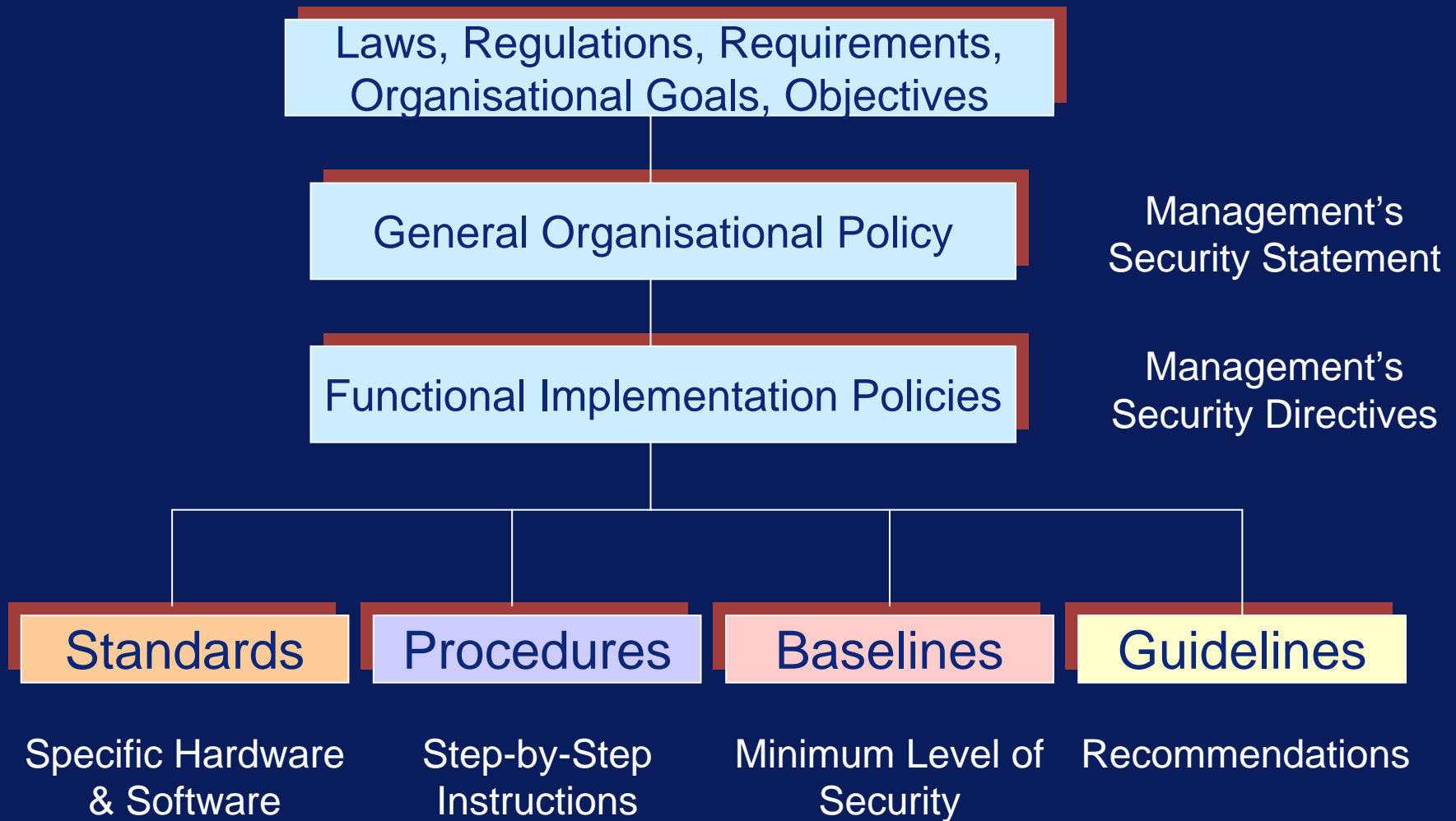
- **Standards**
- **Procedures**
- **Baselines**
- **Guidelines**

and will enforce the security policy principles on every business process and system.



Tools and Best Practices

Policy Hierarchy



Tools and Best Practices

Types of Guidance

- **Standards**
 - specific anti-virus software
 - specific firewall system
- **Procedures**
 - user registration
 - incident response
- **Baselines**
 - server build specifications
 - IDS configurations
- **Guidelines**
 - product evaluation criteria
 - government recommendations

Standards form the base upon which an overall framework is being built ...

- **ISO/IEC 17799:2000 The Code of Practice for Information Security Management** at the core of the information security framework (see slide 26);
- **The ISF Standard of Good Practice** which addresses information security from a business perspective and focuses on the arrangements made by leading organisations to keep the business risks associated with critical information systems under control (www.securityforum.org);
- **COBIT** or “Control Objectives for Information and Related Technology” – a generally applicable and accepted framework for good IT security and control practices (www.isaca.org);
- **ITIL** (the IT Infrastructure Library), and in particular, Security Management, which focuses on the process of implementing security requirements identified in the IT Service Level Agreement, rather than considering business issues of security policy (www.itil.co.uk);
- **Common Criteria/ISO 15408** – which deals with functional and assurance requirements of specific IT equipment (www.iso15408.net);
- **GASSP** or “Generally Accepted System Security Principles”, which is a collection of security best practices (<http://www.infosectoday.com/Articles/gassp.pdf>);
- **GMITS/ISO 13335** – a five-part “Guidelines for the Management of IT Security” which provides a conceptual framework for managing IT security.

...enabling corporations to quickly implement an enterprise-wide Information Security Management Program.

Corporate Security

Practical Session

Security Policy Development



Practical Example
Electronic Communications – Acceptable Use Policy

Security Policy Development

Risks associated with electronic communication

- Unauthorised access to vital company or personal information
- Potential loss or corruption of business information or denial of service
- Loss of productivity and spiraling costs through the excessive use of telephone, e-mail and Internet resources for non-business purposes
- Potential contractual liabilities by unintentionally committing the company to obligations that have not been authorised (e.g. software license obligations when downloading trial software; e-mail, etc.)
- Potential exposure to legal liability or serious reputational damage through the distribution of offensive and/or defamatory material attributed to the company

Security Policy Development

Policy Objectives

- Mitigate against legal liability by setting boundaries for appropriate employee conduct when using electronic communications facilities
- Safeguard Electronic Communications facilities from abuse, damage or disruption
- Ensure that employees understand that the electronic communications facilities provided to them are primarily for business use
- Comply with all relevant regulatory and legislative requirements

Security Policy Development

Type of Use

- Internal communication to colleagues, co-workers or management via fax, e-mail, FTP or through the Intranet web site
- Public communication with another organization via fax, e-mail, FTP or to their Internet web site
- Public communication with any third party (irrespective of whether this is for business purposes or not) via fax, e-mail, FTP or to their Internet web site
- Communications with any third party via Internet Newsgroups or bulletin boards
- Voice communications via company telephone services

Security Policy Development

Roles & Responsibilities

- All **Users** are responsible for complying with related policies and standards for security.
- The **Information Security Steering Group** is responsible for the formulation of company policy and standards for security, ensure that risks are identified and managed, resolve disputes and endorse any proposed non-compliance with this and related policies.
- The **Information Security Manager** is responsible for the provision of specialist support and advice to the Information Security Steering Group, plan and coordinate information security related activities in the organisation and undertake independent monitoring of security status in accordance with this and related policies.
- **Information Owners** are responsible for determining the security requirements of their systems, authorising access and defining access privileges in accordance with sound risk management principles and the directives of the Information Security Steering Group.
- **Security Administrators** must ensure that security controls are implemented in accordance with Information Owner directives.
- **Internal Audit** is responsible for monitoring compliance with policies.

Security Policy Development

Policy Decisions (Examples)

- All users with access to *any electronic communications facilities* must be uniquely identified and authenticated in line with the objectives stipulated in the company's Logon Policy.
- Misrepresenting, obscuring, suppressing, or replacing a user's identity (pretending to be someone else) on an electronic communications system is strictly *forbidden*.
- Users may *not* view, store or distribute any material that is sexually explicit, pornographic, racist, sexist, or derogatory of race, origin, sex, sexual orientation, age, disability, religion or political beliefs.
- ...

Security Policy Development Example

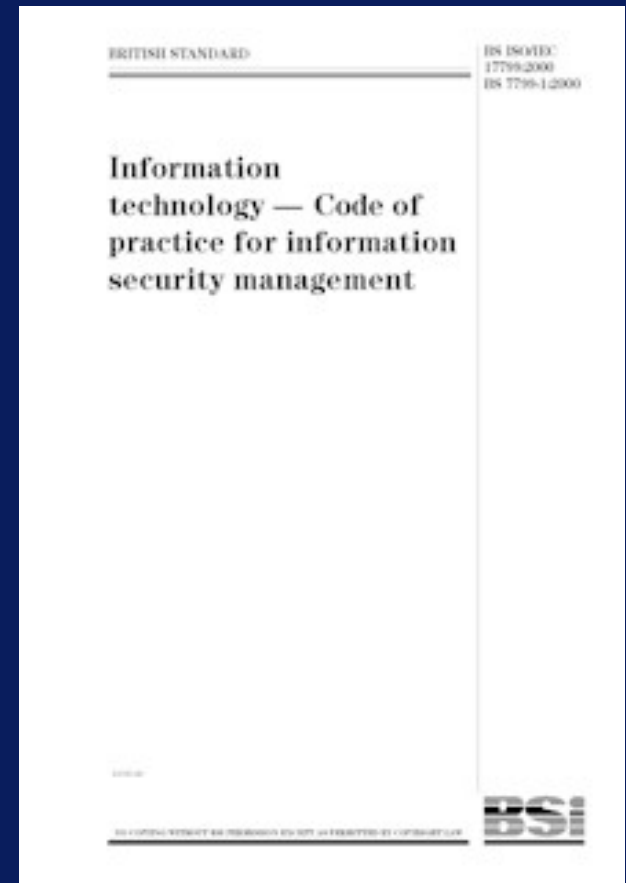


**ELECTRONIC COMMUNICATIONS
ACCEPTABLE USE POLICY**

Security Policy Development

Supporting Material

- **ISO/IEC 17799:2000 (Information technology - Code of practice for information security management)**, renamed to ISO/IEC 27002, contains 36 control objectives and suggests hundreds of specific controls, organised into 10 main sections. Supporting text under each control objective contains advice on how to satisfy the objective, and mentions a number of best practice information security controls. It can serve as a basis for developing security policies and should be used in this exercise
- For the standard 'specification' of an Information Security Management System also refer to ISO 27001.
- Find the content of ISO/IEC 17799 (27002) at http://iso-17799.safemode.org/index.php?page=ISO_17799 or <http://www.17799central.com/>



Contact Details

Deloitte.

Stefan Weiss

Senior Manager
Security & Privacy Services

Franklinstrasse 50
60486 Frankfurt am Main
Tel.: + 49 69 75695 6355
Fax: + 49 69 75695 116355
Mobile + 49 172 3590 674
email: stefanweiss@deloitte.de
www.deloitte.com/de/security



Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, its member firms, and their respective subsidiaries and affiliates. As a Swiss Verein (association), neither Deloitte Touche Tohmatsu nor any of its member firms have any liability for each other's acts or omissions. Each of the member firms is a separate and independent legal entity operating under the names "Deloitte", "Deloitte & Touche", "Deloitte Touche Tohmatsu", or other related names. Services are provided by the member firms or their subsidiaries or affiliates and not by the Deloitte Touche Tohmatsu Verein.
Copyright © 2008 by Deloitte & Touche GmbH Wirtschaftsprüfungsgesellschaft. All rights reserved.

Member of
Deloitte Touche Tohmatsu