Application of the IT Baseline Protection Manual

Dr. Angelika Plate
BSI
Tel.: +49 228 9582 321
Fax: +49 228 9582 405
E-mail: plate@bsi.de

Background

- Risk Analysis
  - accurate results
  - sufficient security
  - effective safeguards...

  BUT
  - time and resource consuming
  - difficult to do
  - effort not always appropriate

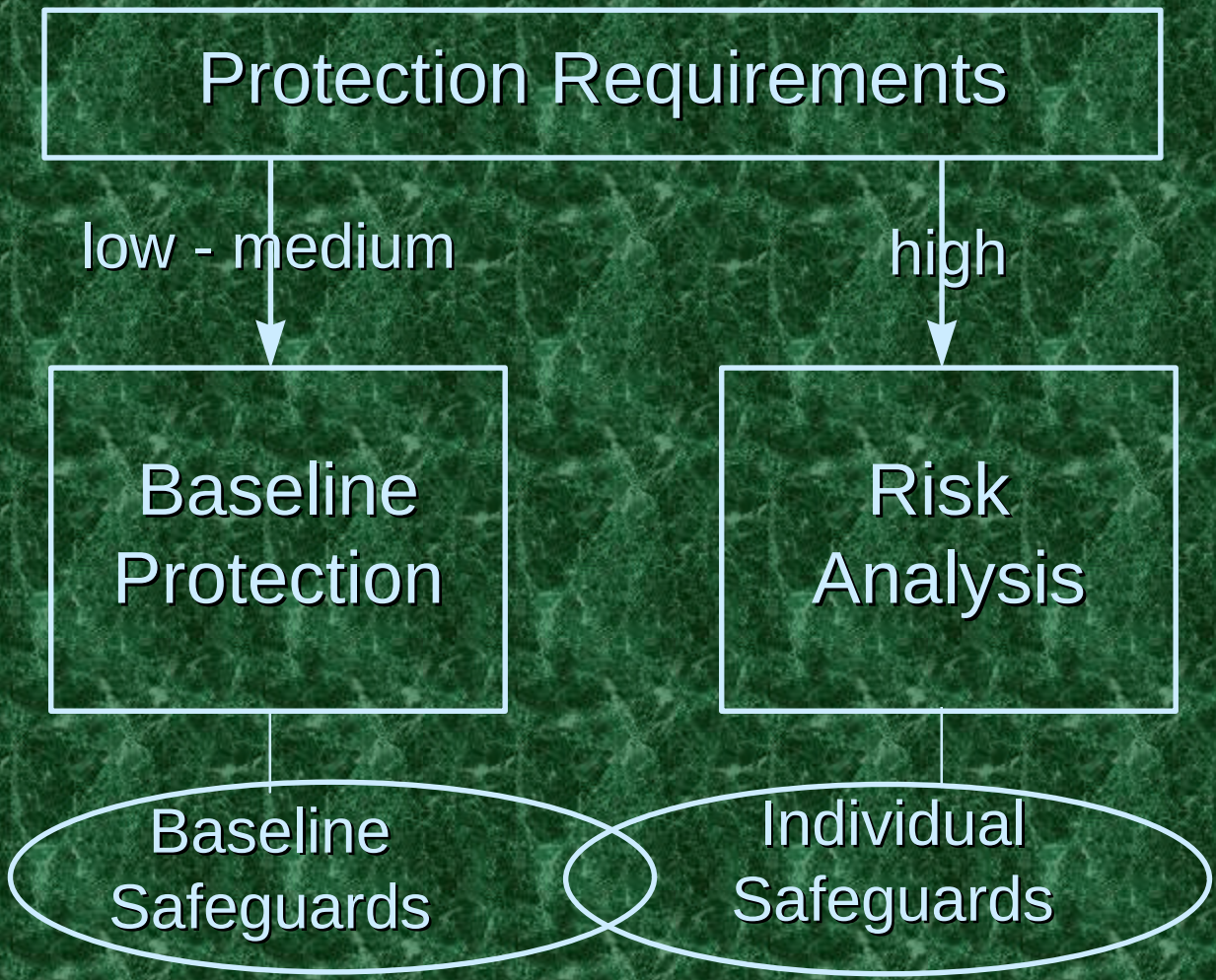
Baseline Protection

- recommending safeguards for typical IT systems
- easy safeguard selection

BUT

- maybe not always appropriate
- only for low to medium security requirements
-

Combined Approach



Protection Requirements

- low to medium, e.g. less than $10,000
- high, e.g. less than $100,000
- very high, e.g. more than $100,000

The limits have to be determined by the organization!

IT Baseline Protection Manual

- Generic Components
- Infrastructure
- Non-Networked Systems
- Local Area Networks
- Data Transfer Systems
- Telecommunications
- Other IT Components

Other Baseline Activities

- NIST Computer Security Handbook
- Code of Practice for Information Security Management
- Information Security Guidelines
- Baseline Security Standards, Features and Mechanisms
- GMITS, Part 4: Selection of Safeguards

Using the IT Baseline Protection Manual

Step 1: Mapping the IT System

The Manual has a ‘modular’ structure:

- Chapter 3: generic components
- Chapter 4: infrastructure
- Chapters 5 seq.: IT-specific modules

Using the IT Baseline Protection Manual

Step 2: Reading the modules

Each module contains:

- general description
- assumed threats
- suggested safeguards

Using the IT Baseline Protection Manual

Step 3: Reading the descriptions

Detailed descriptions are given in

- threat catalogues
- safeguard catalogues
  - responsibilities
  - description
  - implementation

Using the IT Baseline Protection Manual

Step 4: Inventory of existing safeguards

Step 5: Comparison of existing and recommended safeguards

All recommended safeguards should be implemented to achieve baseline protection!

Future Developments

- in 1997 (already included):

  Windows NT, Windows 95, and Novell 3.x
- in 1998 (planned):

  databases, X.400, fax-server, SAP R/3, Novell 4.0, heterogeneous networks

A tool to support the application of the manual is available!