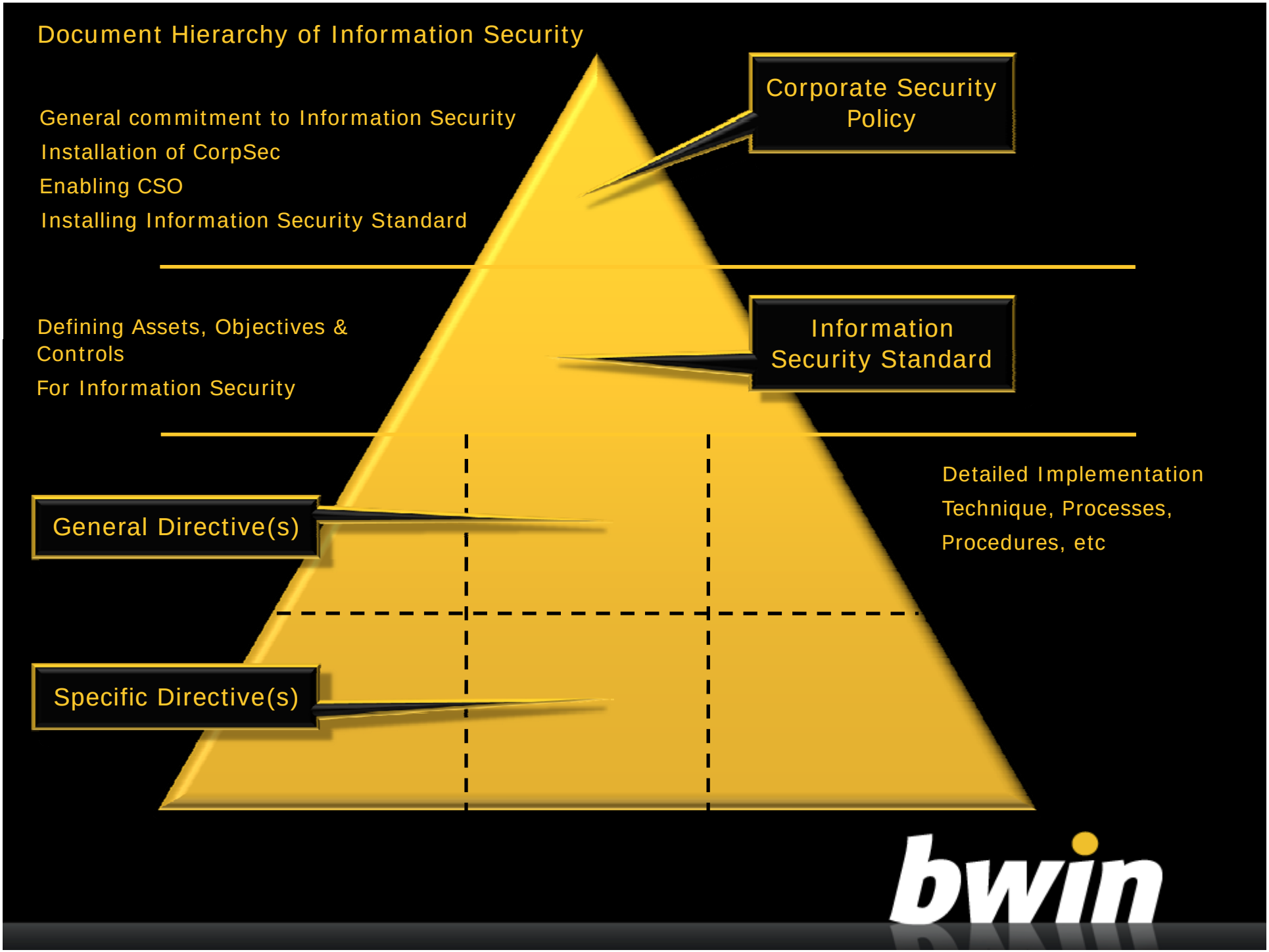
Document Hierarchy of Information Security
General commitment to Information Security
Installation of CorpSec
Enabling CSO
Installing Information Security Standard
Corporate Security Policy
Defining Assets, Objectives & Controls
For Information Security
Information Security Standard
Detailed Implementation
Technique, Processes, Procedures, etc
General Directive(s)
Specific Directive(s)
bwin

bwin

ISMS Structure Overview

- ISMS = Information Security Management System.
- It consists of 3 types of documents, structured in 3 tiers.
- Tier 1: Information Security Policy, general statement about information security, enabling security organisation, requires information security standard.
- Tier 2: Information Security Standard, defining objectives and controls for information security, giving guidance for implementation. Consists of 15 chapters, one for each main realm of information security.
- Tier 3: Information Security Directives, giving more detailed implementation guidance for certain areas.

Information Security Policy

- High level document
- Only abstract goals for information security
- Defines security organisation and it’s duties
- Defines the “corner pillars”
- “Orders” a security standard document based on ISO 27002
- Defines security as a innate part of bwin’s business

Information Security Standard

- Based on ISO 27002
- Adapted to the special needs of bwin
- 15 chapters
  - Introduction
  - Scope
  - Terms and definitions
  - Structure of this standard
  - Risk assessment and treatment
  - Security policy
  - Organisation of information security
  - Asset management
  - Human resources security
  - Physical and environmental security
  - Communications and operations management
  - Access control
  - Information systems acquisition, development and maintenance
  - Information security incident management
  - Business continuity management
  - Compliance
- Defining objectives and controls for information security based on international regulations and best practices
- Leaving the decision to management not to implement and take the risk

Security Directives

- Information Classification & Handling
  Defines templates and procedures for classification if information in the 3 dimensions, confidentiality, integrity and availability
- Risk Management
  Defines how Risk management has to be done at bwin
- Directive on Worldwide Security Organization
  Internal organisation of CorpSec
- Asset Management
  Defining assets, responsibility for assets, documentation, …
- HR Directive
  Describing what HR has to consider when hiring personal and external resources
- Physical & Environmental Directive
  Directive to handle premises of bwin, physical security, entry control, doors, windows, …
- Access Control Directive
  Security directive for IT operations, defining operations management, logging, administration rules, …
- System Acquisition / Development & Maintenance Directive
  Security rules for architecture, software development and procurement of systems and software
- Security Incident Management Directive
  How to log and report security events
- Business Continuity Directive
  Rules to define and run required availability in IT and to handle critical services on failure
- Audit Directive
  How to deal with internal and external auditors, provide correct data and evidence
- Users Directiveto Information Security
  Rules for the users of bwin's IT infrastructure
- Privacy Protection Directive

bwin

Principles for Security Directives

- Derived from Information Security Standard or a more abstract Directive
- Dedicated the a special task, region or audience
- Only needed if Standard is not adequate or specific enough
- Examples:
  - General HR Security Directive
    - HR Security Directive for Austria/Sveden/…
  - General Security Directive for Data Centres
    - Security Directive for Data Centre A
    - Security Directive for Data Centres in USA
  - Security Directive for Webserver
    - Security Directive for IIS/Apache/…

ToDos

1. CEOs sign and publish Corporate Security Policy
2. Workshops with Business Responsibles about their chapters (C-lvl, Head-Ofs) (Oliver Eckel)
3. Release of accorded Information Security Standard by CSO
4. Workshop with Business Experts about detailed Directives (MK+CG)
5. Gap Analysis
6. Budget and time estimation
7. Implementation considering priority


bwin