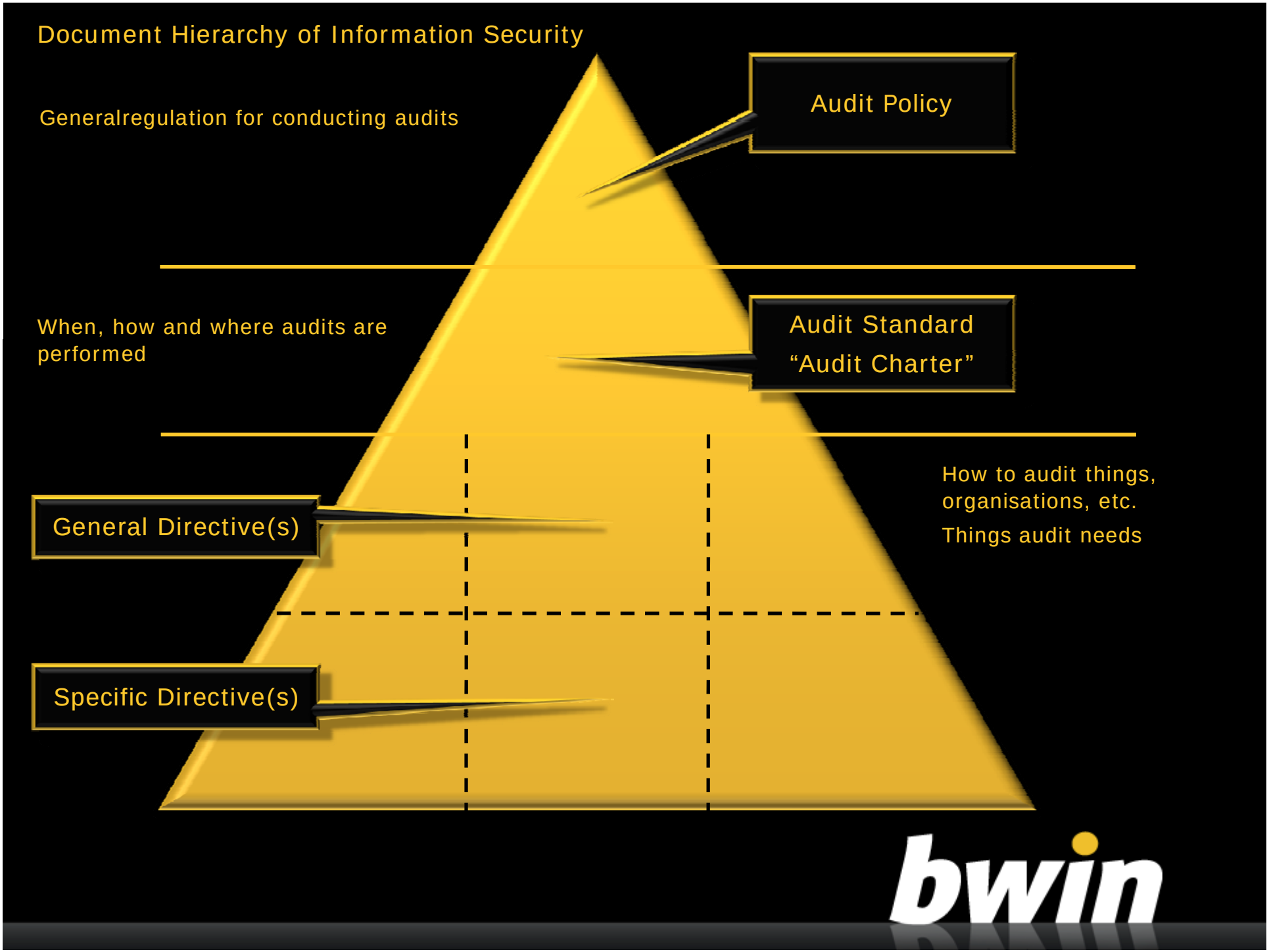
AuditDirectiveImplenetation

Sebastian Strobl, Pierre Kwaku, Christoph Gruber
CC: Oliver van Assche, Oliver Eckel
29.09.2010


Document Hierarchy of Information Security
Generalregulation for conducting audits
Audit Policy
When, how and where audits are performed
Audit Standard
“Audit Charter”
How to audit things, organisations, etc.
Things audit needs
General Directive(s)
Specific Directive(s)
bwin

bwin

Principles for Audit Directives

- Derived from Audit Standard or a more abstract Directive
- Dedicated the a special task, region or audience
- Only needed if Standard is not adequate or specific enough

Requirements for Audit Documents

- Internal “Code of Conduct for Audit Department”
  - How the things are done
  - Quality Assurance
  - …
- Requirements for Others
  - What data has to be provided
  - Quality of data (integrity, …)
  - …
- Cooperation with external auditors
  - Corporate Audit has to be single point of contact to external auditors
  - …

bwin

Code Of Conduct

- Information systems audit controls
- Protection of information systems audit tools
- Other internal regulations, beside IT

bwin

Directive to Others

- Starts with ISS ch. 6 (Security Coordinators), one contact in each department
- Implementation of audit rights into contracts with internal and external staff
- ISS 9.1.2 physical entry controls
- ISS 10.1.1 documented operating procedures
- ISS 10.1.2 change management
- ISS 10.2.2 monitoring and review of third party services
- ISS 10.6.2 security of network services
- ISS 10.7 media management
- ISS 10.10 audit logging
- ISS 11.7.2 teleworking
- ISS 12.3.2 keymanagement
- ISS 12.4.2 protection of system test data
- ISS 12.4.3 access control to program source code
- ISS 12.5.1 change control procedures
- ISS 12.5.5 outsourced software development
- ISS 13.2 management of information security incidents and improvements
- ISS 15.1 compliance with legal requirements
- ISS 15.2 Compliance with security policies and standards, and technical compliance

Cooperation with external Auditors

- Corporate Audit Department has to be the single point of contact for external auditors
- Exceptions?

  Tax audit?
- Law enforcement
- ...

Thank You