ENISA Workshop on Risk Management

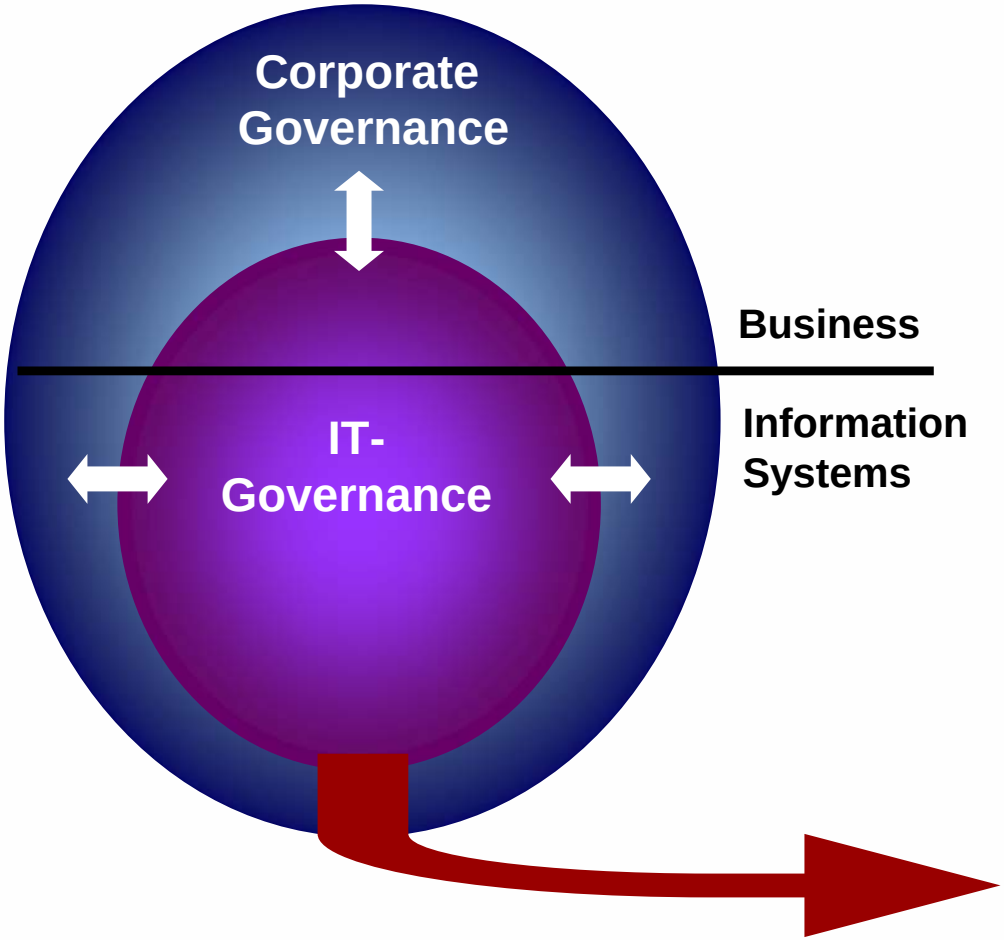
Rome, 13th of October 2006

Risk Management and Corporate Governance: Three Level Compliance Approach

o. Univ. Prof. Dr. Dimitris Karagiannis

University of Vienna
dk@dke.univie.ac.at

IT-Governance



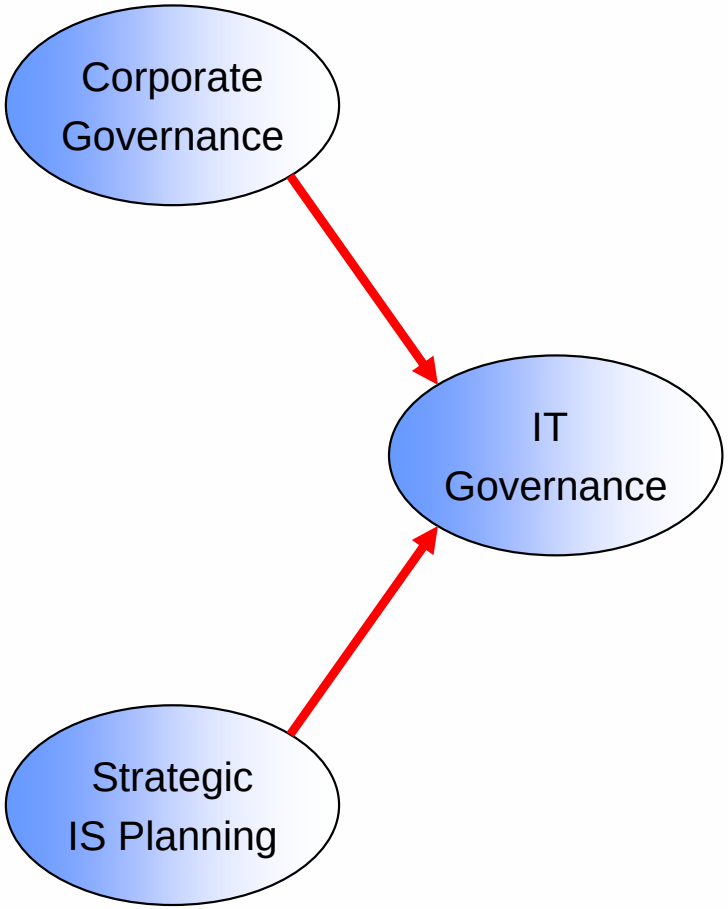
The Management is responsible for IT-Governance. IT-Governance is an integral part of Corporate Governance and consists of management and organizational structures as well as processes. This guarantees that the IT supports and drives business strategies and targets.

IT-Governance Institute

Facts

- The importance of IT governance can be appreciated in light of the Gartner Group's finding that large organizations spend over 50% of their capital investment on IT
- Enron Case: increased focus on corporate accountability.
- Companies with better than average IT governance earn at least a 20% higher return on asstes than organizations with weaker governance.
- At least 50 countries have corporate-governance regulatory frameworks in place.

Background



Corporate Governance	***Strategic IS Planning***	***IT Governance***
Strategic direction	Aligning investment in IS with business goals	Strategic alignment
	Exploiting IT for competitive advantage	Delivering business value through IT; exploiting opportunities and maximizing benefits
Performance management	Directing efficient and effective management of IS resources	Performance management; IT resources used responsibly
Risk management		Risk management; Appropriate IT risks management
Policies and procedures	Developing technology policies and architectures	
Control accountability		

IT-Governance: Compliance

Compliance can be classified in three levels:

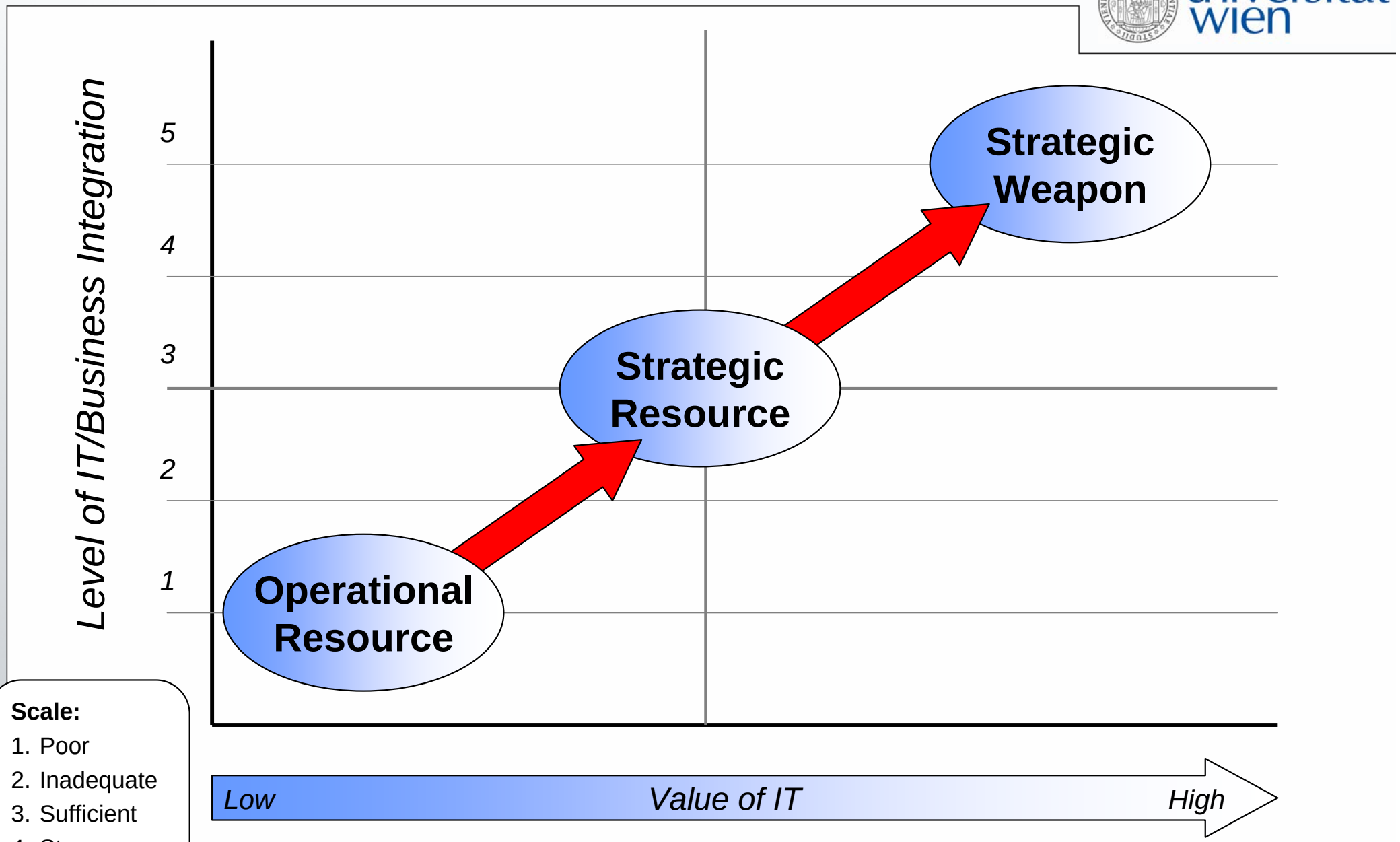
- “Technology Compliance”

- “Business Compliance”

- “Regulations Compliance”

Sarbanes-Oxley

Business-IT Alignment



Scale:

1. Poor
2. Inadequate
3. Sufficient
4. Strong
5. Extraordinary

IT Governance Tools Classification

Process Type/ Organizational Entity	*Procedure*	*Activity*	*Business Unit*	*Business System*
Core business processes	ITIL/BS15000	• CMM/CMMI • IT Audit • IT Due Diligence	Six Sigma	IT Service CMM
Decision making processes	SAS70	COBIT		• IT Governance Review • IT Governance Assessment • IT Governance Checklist • IT Governance Assessment Process Mode
Support processes	• ISO1799/ BS7799 • SysTrust	• ASL • PRINCE2		SOX

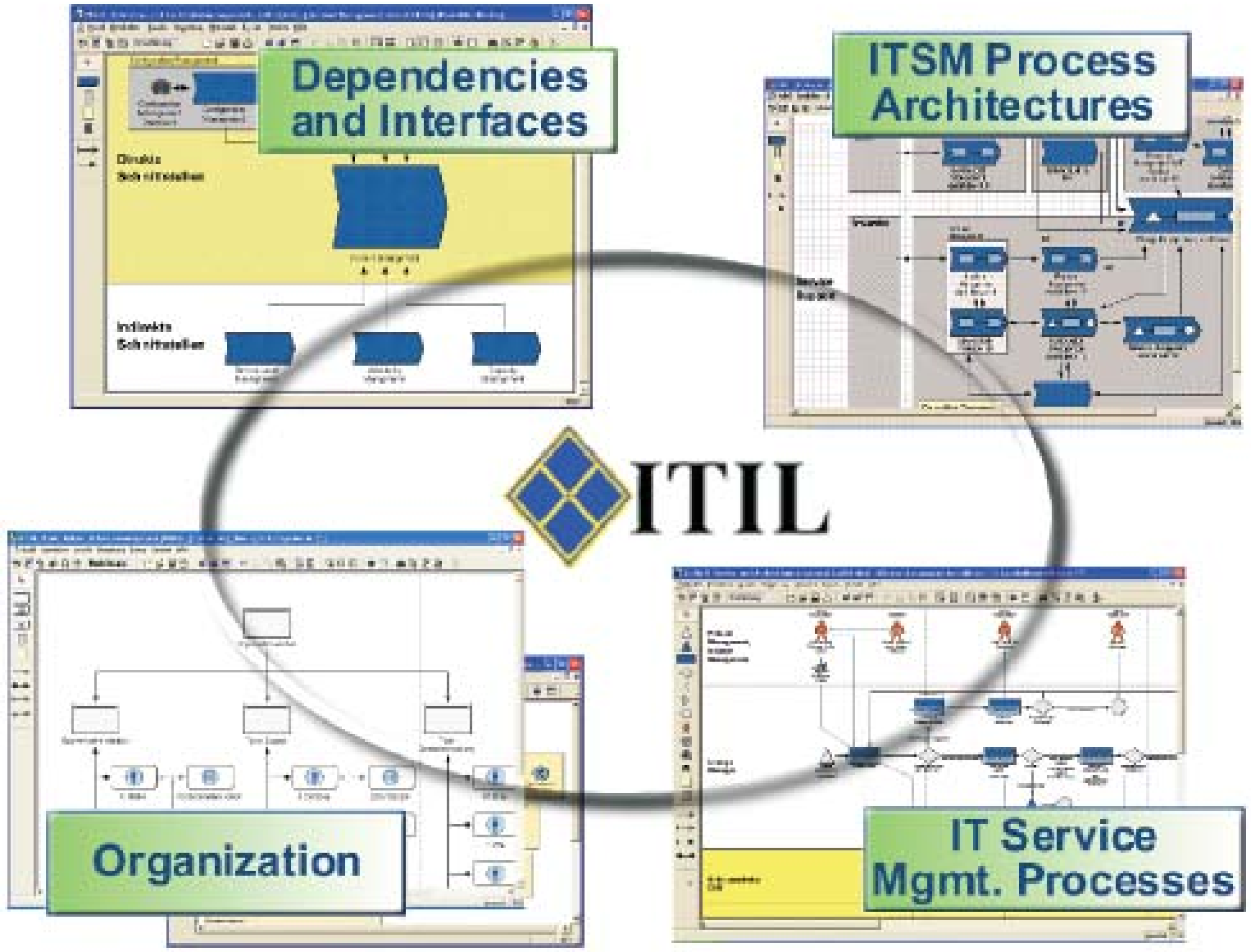
IT-Infrastructure Library (ITIL®)

ITIL provides a comprehensive, consistent and coherent set of best practices for IT service management and related processes, promoting a quality approach for achieving business effectiveness and efficiency in the use of IS.

Two principal concepts characterize the basic thinking of ITIL:

- Holistic service management—IT service managers:
- Customer orientation—IT services are provided at a level of quality that allows permanent reliance on them.

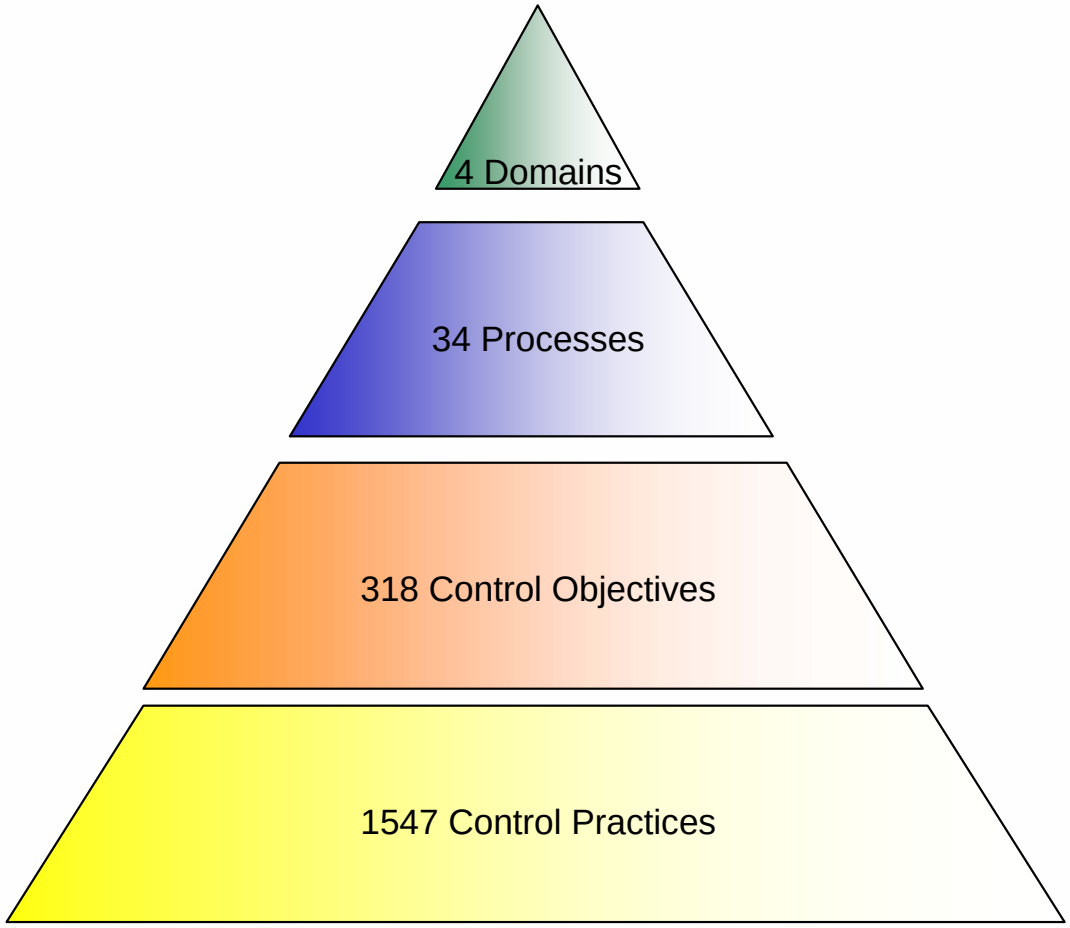
ITIL® Reference Library in ADO*it*®



Control Objectives for Information and Related Technology (COBIT®)

What Is COBIT®?

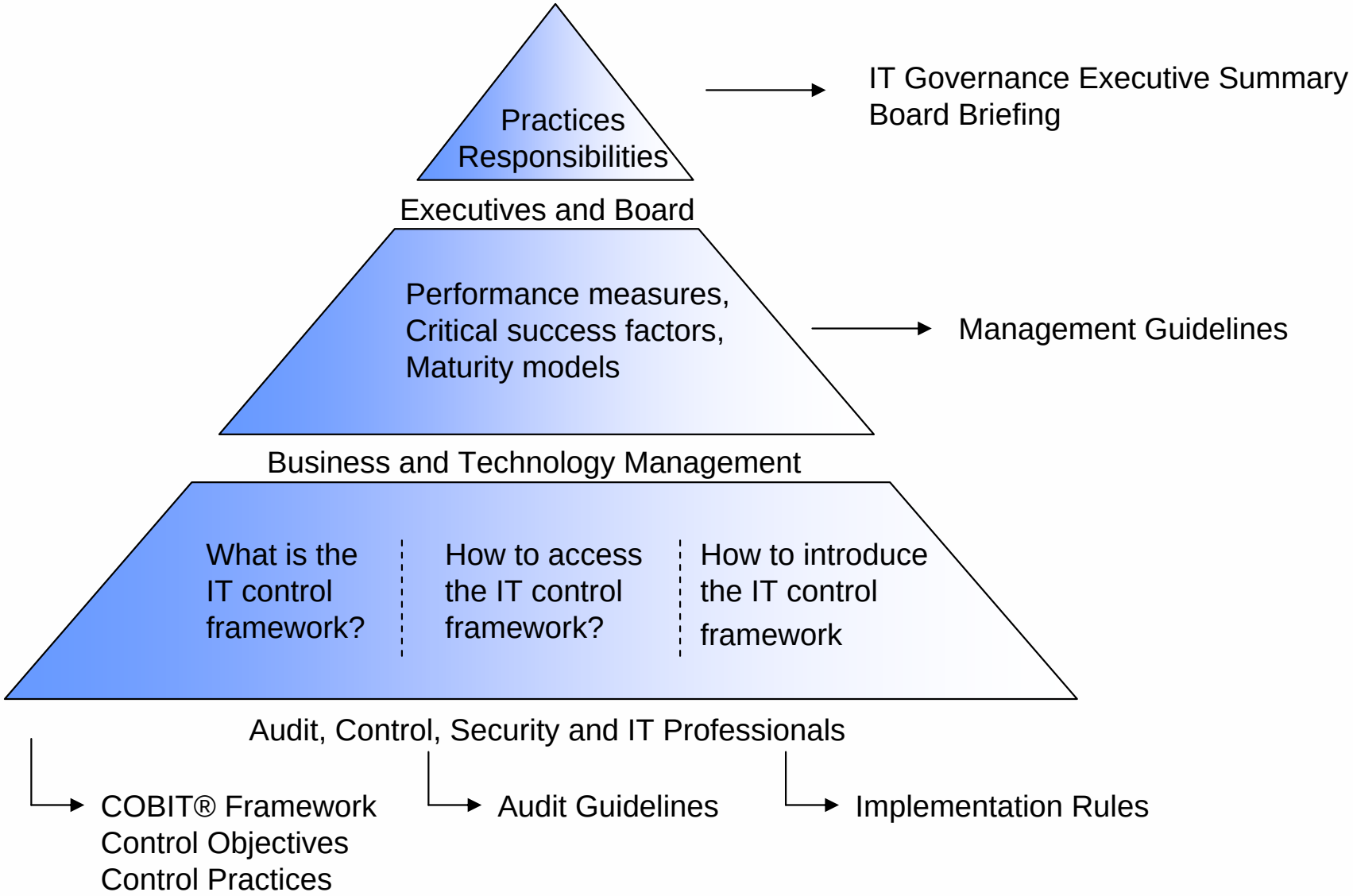
1. COBIT® is a way to implement “IT governance”.
2. It is a “framework that must be tailored to [an] organization”, that “must be used with other resources” in order to customize this general set of guidelines to [one’s own] specific environment”.
3. In structure, COBIT® consists of a set of “Control Objectives” for information technology, designed to enable auditing. The Control Objectives are “guidance,” in that they describe what should be accomplished.



COBIT’s Hierarchy

(Number of Items per Level)

COBIT®: Family of Products



COBIT®: IT-Governance with ADO*it*®

universität wien

Business Processes

IT-Resources

- Data
- Application
- Technology
- System
- Personal

Criterion (Goals):
- Reliability
- Availability
- Integrity
- Dependability
- Effectiveness
- Efficiency
- Adherence

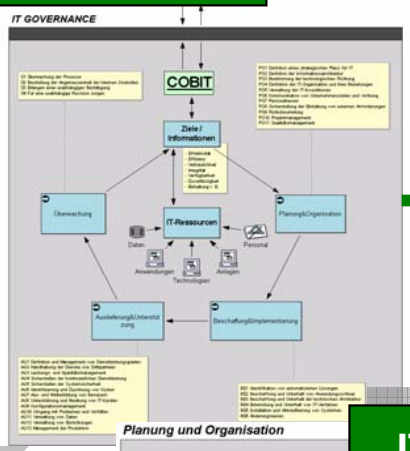
Supervision

Planning & Organization

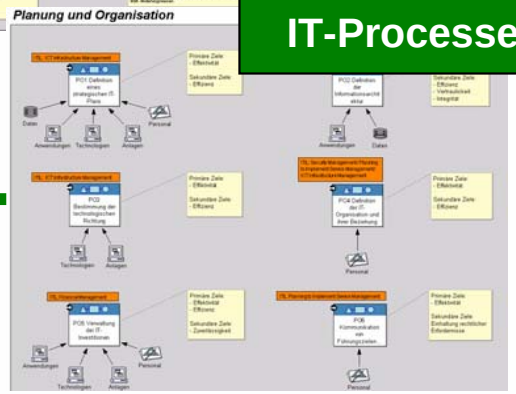
Procurement & Implementation

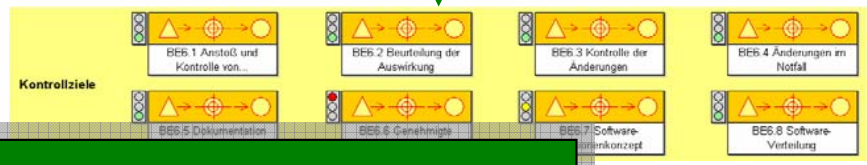
Company Support

Domains



IT-Processes

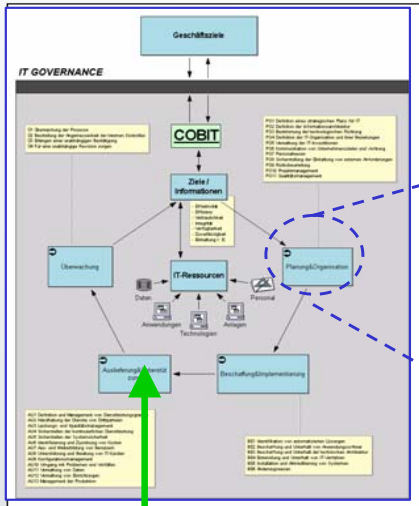




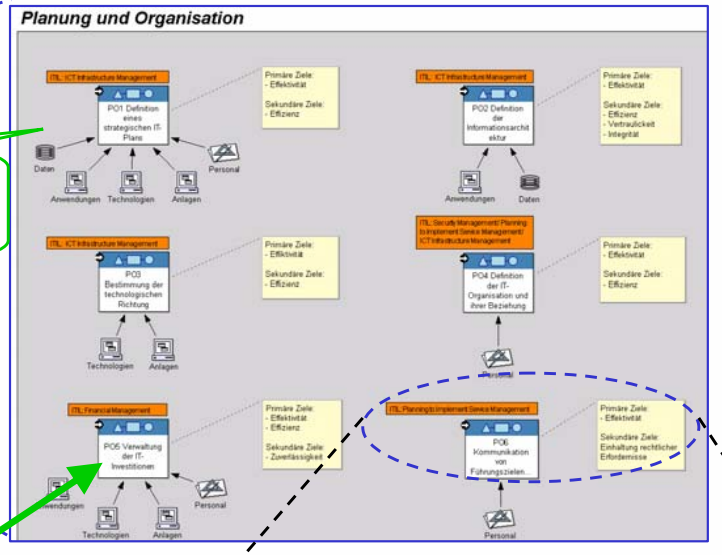
Control Goals, KPIs & KGIs

The COBIT® - Cube in ADO*it*®

universität wien



Critical IT-Processes



4x

34x

Information Criteria

Quality
Orderly
Security

IT-Processes

Domain
Processes
Activities

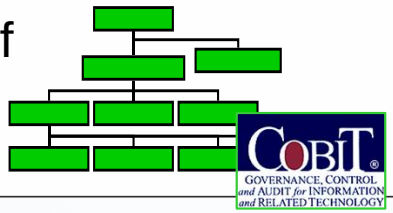
Personal
Application
Technologies
Systems
Data

IT-Resources

318x

Control Goals

The whole COBIT®-"Family of Products" is available in the form of **reference models.**



enisa European Network and Information Security Agency

Legal Risks due to IT

1. Company Risks:

1. IT Systems failure → organization can't meet contractual commitments to customers.
2. Security breaches → private information lost.
3. Inadequate security and anti-virus systems → liability to 3rd parties.

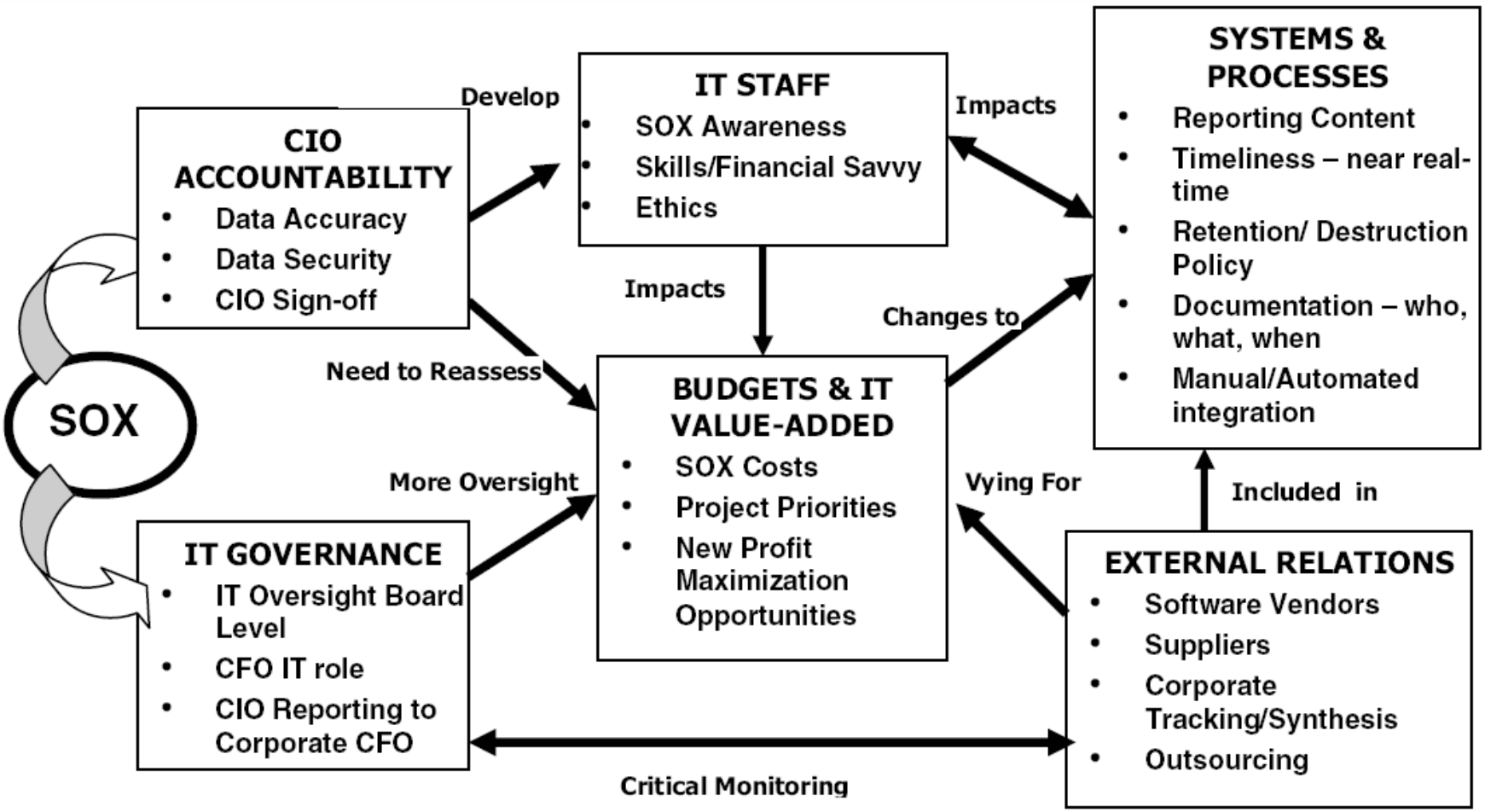
2. Directors Liability:

1. All directors owe duties to their company to exercise the care, diligence and skill that a reasonable director would exercise in the same circumstances.
2. A director is entitled to rely on statements, reports etc, provided by employees,, other directors, professional advisors, and board committees.
3. Board members are heavily reliant upon company staff and specialists. So in terms of corporate governance, they will be particularly concerned about having systems and processes in place, coupled with sufficiently capable and experienced staff.

3. Senior managers Liability:

1. Senior managers can be liable to third parties in relation to their negligence.

SOX Impact

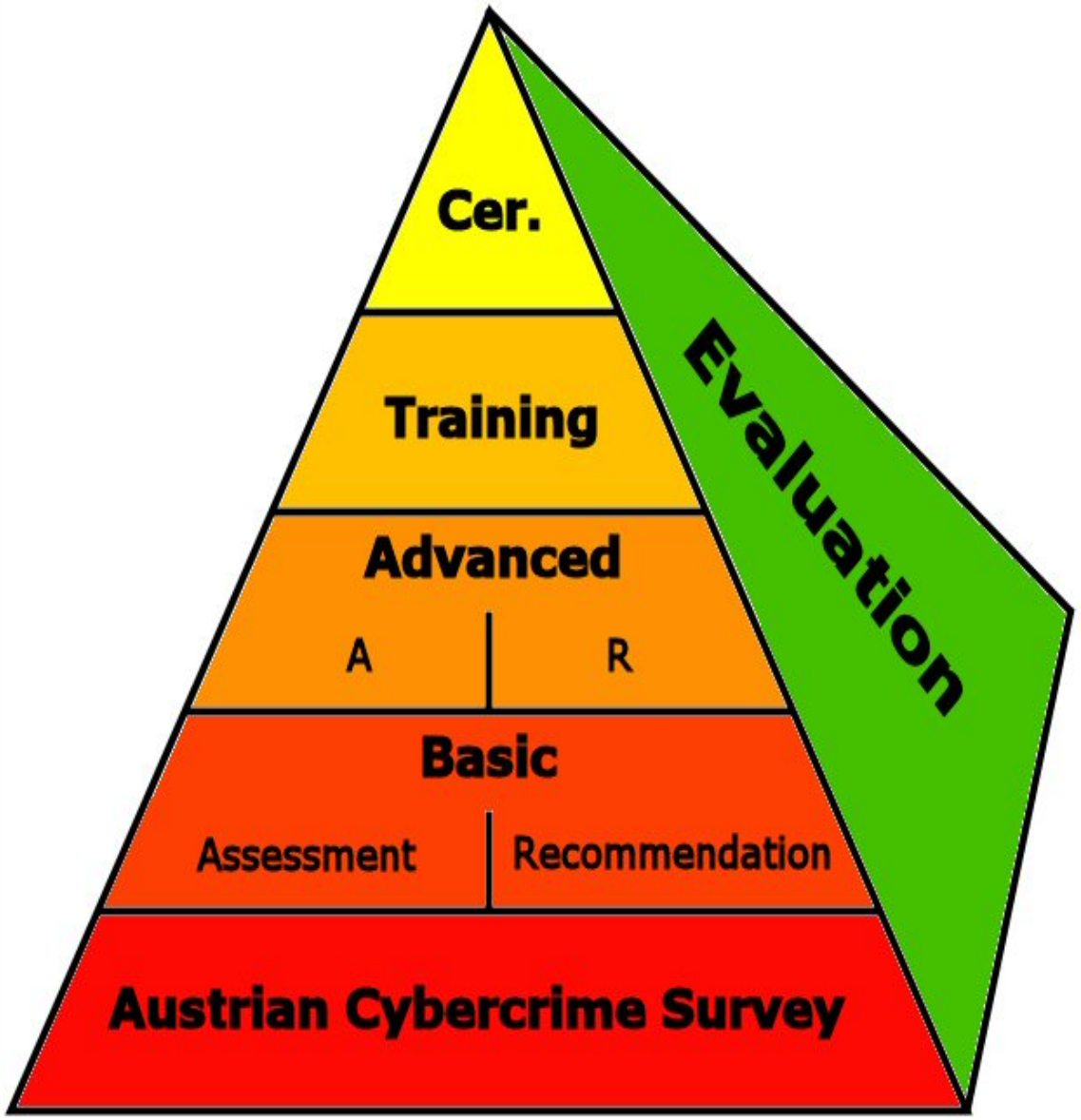

SOX
CIO ACCOUNTABILITY
• Data Accuracy
• Data Security
• CIO Sign-off
Develop
IT STAFF
• SOX Awareness
• Skills/Financial Savvy
• Ethics
Impacts
SYSTEMS & PROCESSES
• Reporting Content
• Timeliness – near real-time
• Retention/ Destruction Policy
• Documentation – who, what, when
• Manual/Automated integration
Impacts
Changes to
Need to Reassess
BUDGETS & IT VALUE-ADDED
• SOX Costs
• Project Priorities
• New Profit Maximization Opportunities
More Oversight
IT GOVERNANCE
• IT Oversight Board Level
• CFO IT role
• CIO Reporting to Corporate CFO
Vying For
Included in
EXTERNAL RELATIONS
• Software Vendors
• Suppliers
• Corporate Tracking/Synthesis
• Outsourcing
Critical Monitoring

SOX Compliance: Simplified Process

universität wien

1. Document processes from an IT perspective.
2. Identify control points in the processes, where manual and automated portions intersect, or where two different systems are linked.
3. Test viability of controls to demonstrate that appropriate controls are in place and work as designed. The tests need to show that the controls work in preventing errors and do exception reporting.
4. Report results from testing, including identification of any gaps. Recommendations should be given for correction of errors and closing any gaps.
5. Implement plan of action to close gaps and eliminate known errors.
6. Select a framework to set up internal IT control systems.

The Secure Business Austria Assessment Aproach



Target Group:

Small and Medium Enterprises (SMEs)

Structure:

Building on two levels:

- Basic Level
- Advanced Level

Accompanied by continuous

- Evaluation

Followed by

- Training

Finalised through

- Certification

Activities

- **Development of a Certification Framework:**
  - Cybercrime Survey (Austria)
  - Legal compliance (Basic / “MUST”)
    - ITIL, CobiT, SOX, Basel II,…
  - Competitive and economical issues (Advanced / “CAN”)
  - Training
  - Certification
  - Continuous Evaluation

- **Providing a testbed for other member states**
  - Lessons Learned for further projects / initiatives

Collaboration Activities

Possible collaboration activities:

- **Knowledge exchange (expert knowledge, lessons learned,…)**
- **Access to resources (previous studies, surveys, training material,…)**
- **Support concerning the publication of results**
- **Discussion of milestones and gained results**

Secure Business Austria

universität wien

Thank you for your attention!

o. Univ. Prof. Dr. Dimitris Karagiannis
dk@dke.univie.ac.at

enisa European Network and Information Security Agency