

# Hierarchical Security Management

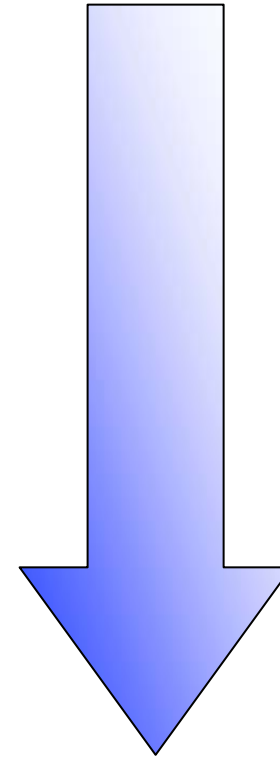
2nd Security Workshop: Future Security  
January 16-17, 2007  
Sophia Antipolis, France

Johan D. Bakker MSc CISSP ISSAP  
Royal Dutch Telecom (KPN)



# Agenda

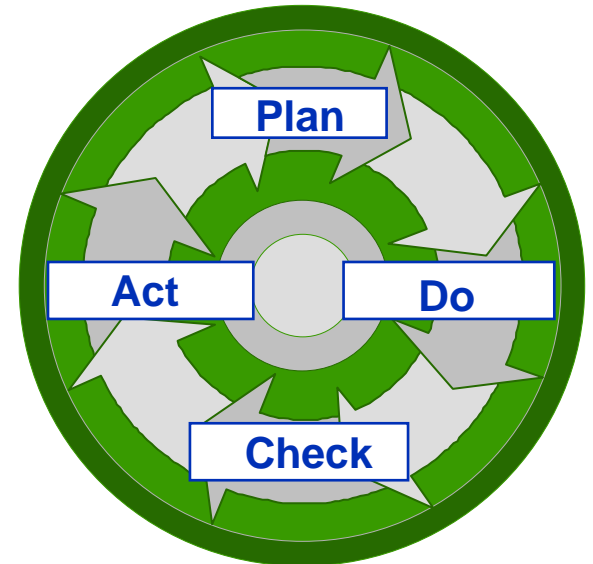
- ISO 27001
- Organizing security governance
- Hierarchical ISMS approach
- Future work
- Questions



# ISO 27001

What ISO 27001 does:

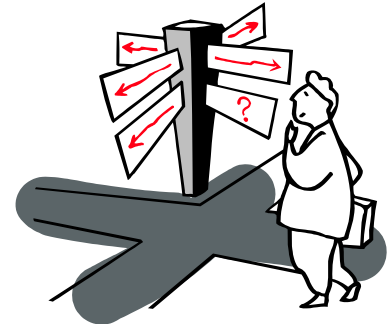
Provides a model and requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS)



# ISO 27001

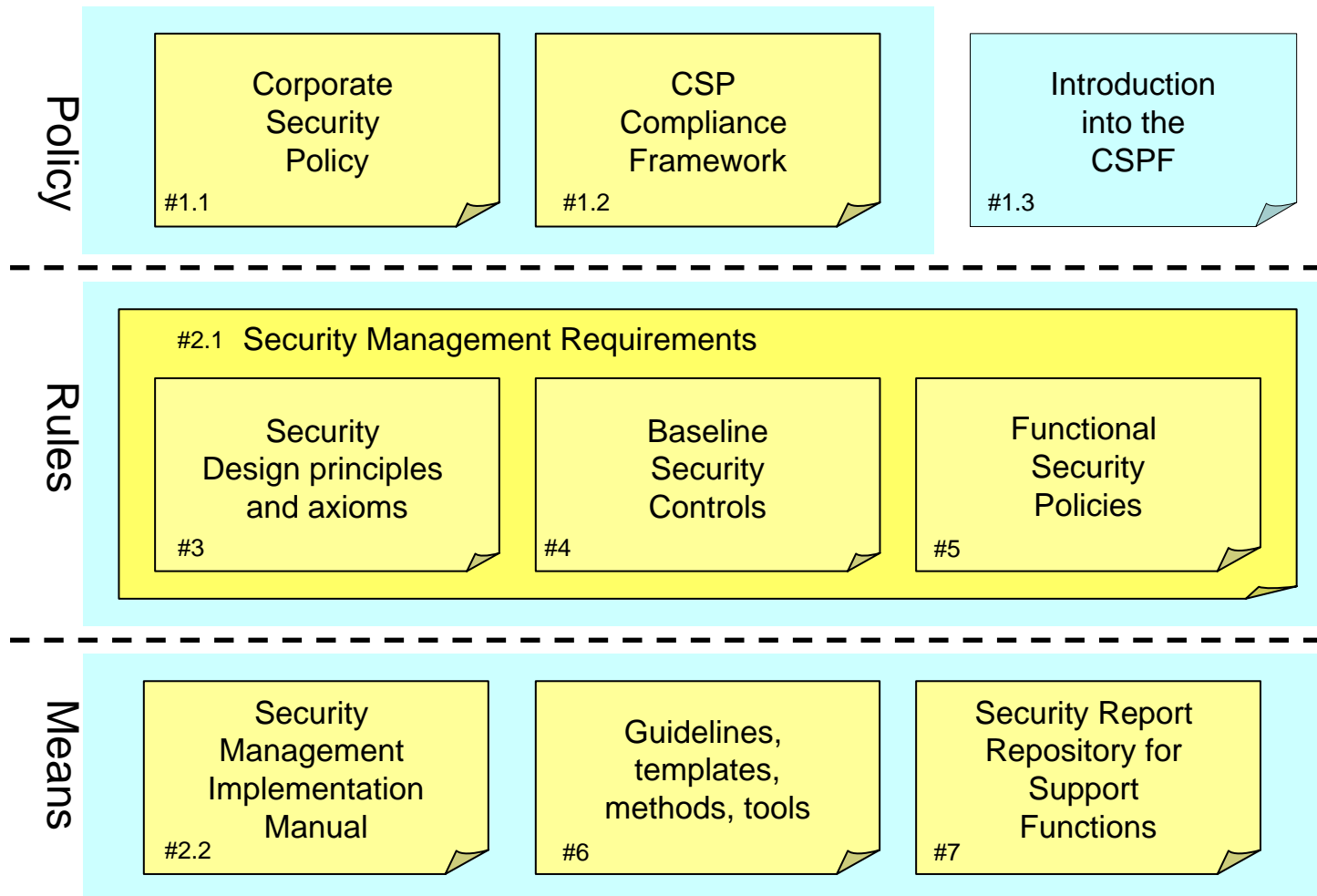
What ISO 27001 doesn't do:

Specify organizational requirements and structure for security governance and compliance reporting for a large and complex organization...

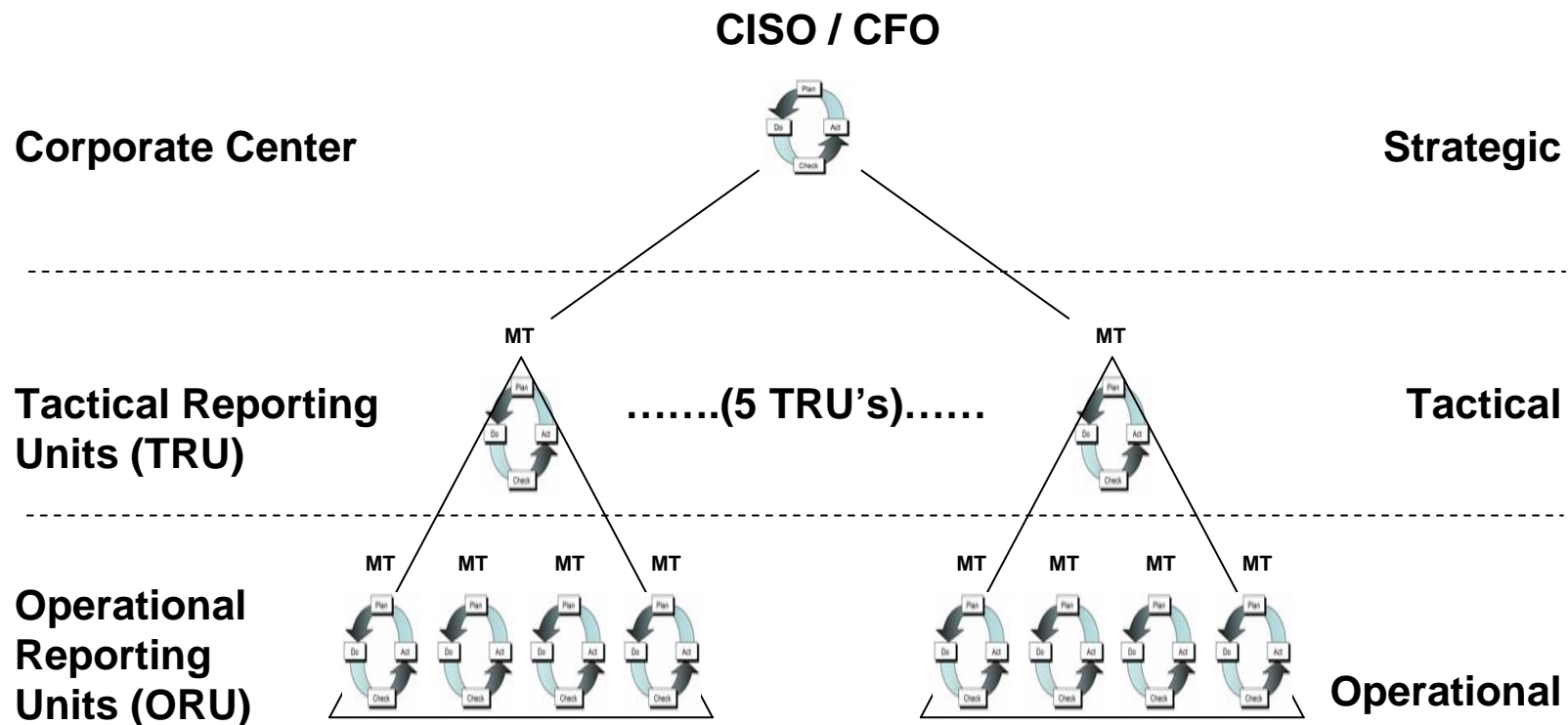


*....that offers hundreds of products and services, with 16.000 employees, organized in a score of different departments within 5 different market or corporate segments.*

# Organizing security governance

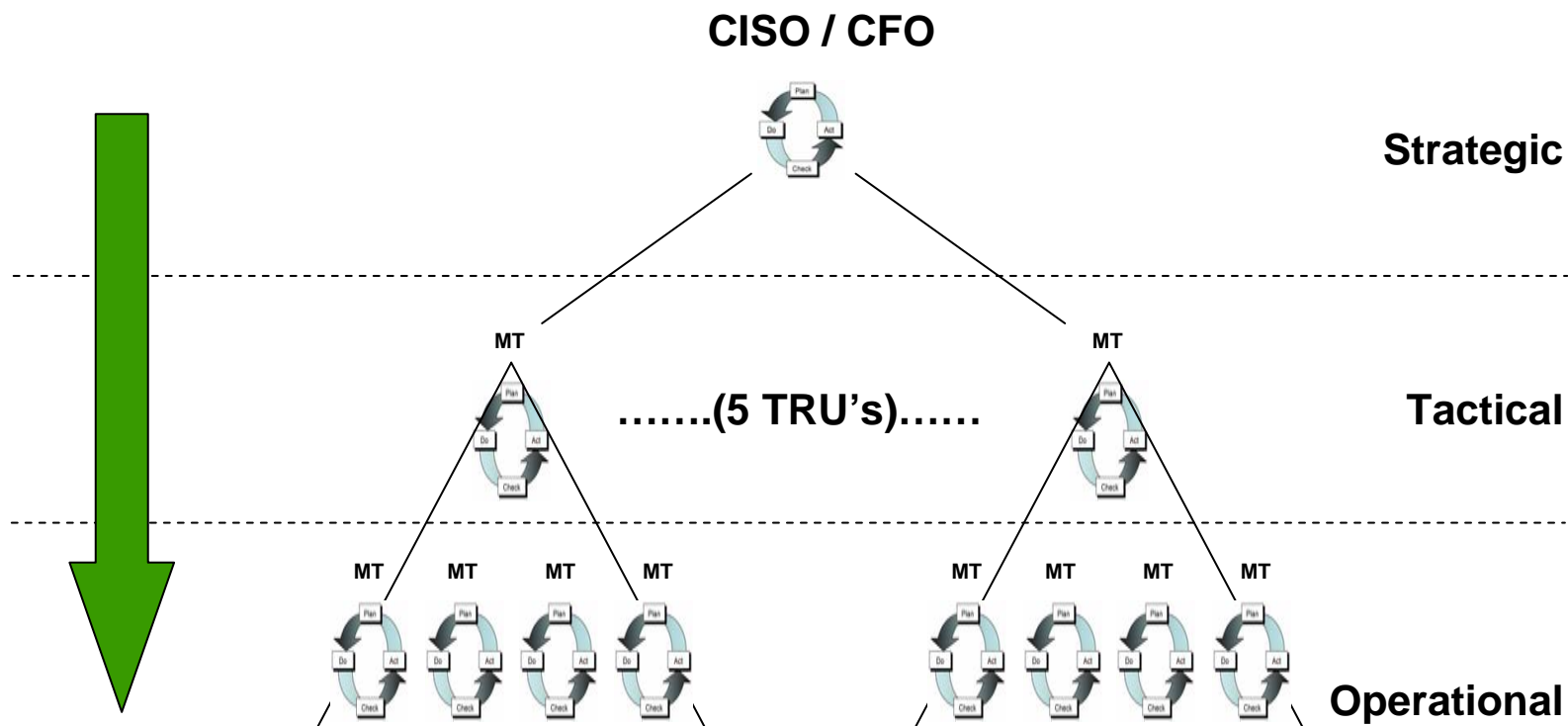


# Organizing security governance



# Organizing security governance

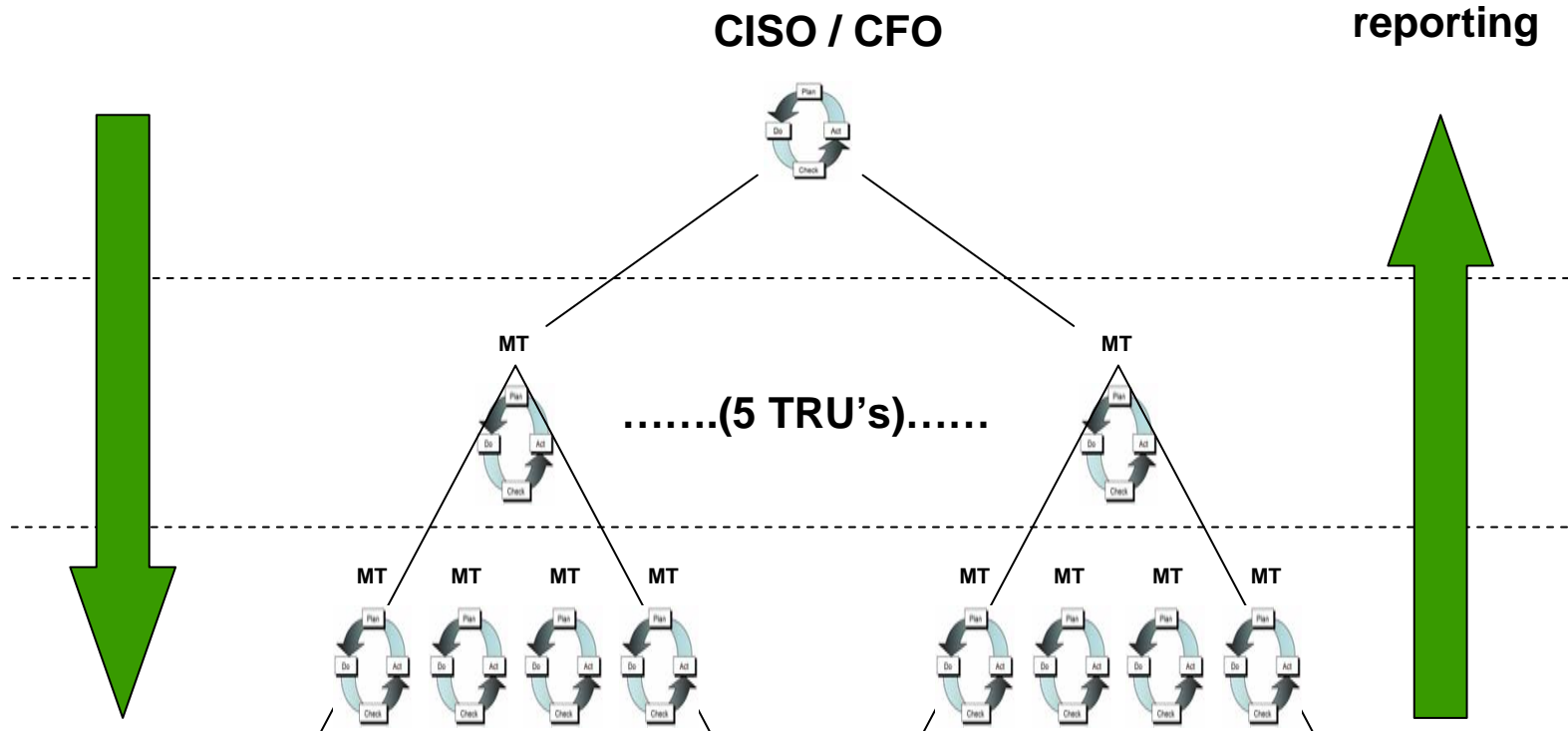
## Governance



# Organizing security governance

Governance

Compliance reporting



## Hierarchical ISMS approach - What if....

...the same ISMS approach could be used for the operational, tactical and strategic level?

Then, all levels could share the same vocabulary, document templates, concepts....

To enable this, it is required to parameterize some concepts in the ISMS process, depending on the scope and abstraction level.

## Hierarchical ISMS approach - Parameters to an ISMS

- What is in Scope of the ISMS?
- What is the Context of the ISMS?
- Related to what type of Assets?
- What Aspects of the assets is focussed on?
- What type of Risks are managed?
- What type of Controls are available?

## Hierarchical ISMS approach - Parameter values

	Strategic	Tactical	Operational (typical 27001)
Scope	KPN Enterprise	Tactical Reporting Unit	Product(s), service(s) or process(es)
Context	Market, legal, regulatory, societal developments, KPN Mission	Business developments, demand/supply chain, tactical scopes, CSP	Cust. requirements, CSP and local policies and procedures
Security aspects	Enterprise impact, tactical level of compliance	Business impact, operational level of compliance	Confidentiality, Integrity and Availability
Assets	The KPN Brand(s)	Products, services and processes	Typical Information assets
Risks	Enterprise risks	Business risks	Security risks
Controls	CSP Framework, tactical ISMS's	SLA's, local policies operational ISMS's	ISO/IEC 17799:2005 controls

## Hierarchical ISMS approach - Benefits

- Defined enterprise-wide governance approach
- Uniform dossier templates
- Shared vocabulary
- Solid bases for compliance reporting

## Future work....

- Risk aggregation
- Compliance metrics
- Integration into a single management system
  - Corporate Baseline - COSO II (SOx), ISO9001 & ISO27001
  - amended with ISO14000, ISO10002, SAS70, ITIL, etc.
    - depending on the type of department

# Questions

