IT Risk Management Era: Research Challenges and Best Practices

IARA Work Group
July 1st , 2007,
Santa Clara - California

White Cyber Knight
WCK

Eyal Adar, Founder & CEO
Eyal@WhiteCyberKnight.com
Chairman of the EU SRMI
(Security Risk Management Initiative)

White Cyber Knight

WCK

Agenda:

- Introduction to Risk Management
- Research Challenges
- Best Practices
- WCK- Software Tool

The word risk derives from early Italian “risicare“ which means “to dare”
In this sense risk is a choice rather than a fate

Peter l. Bernstein

Introduction

Introducing Eyal Adar

A leading expert in the areas of Risk Management, CIP (Critical Infrastructure Protection) and IT Security.

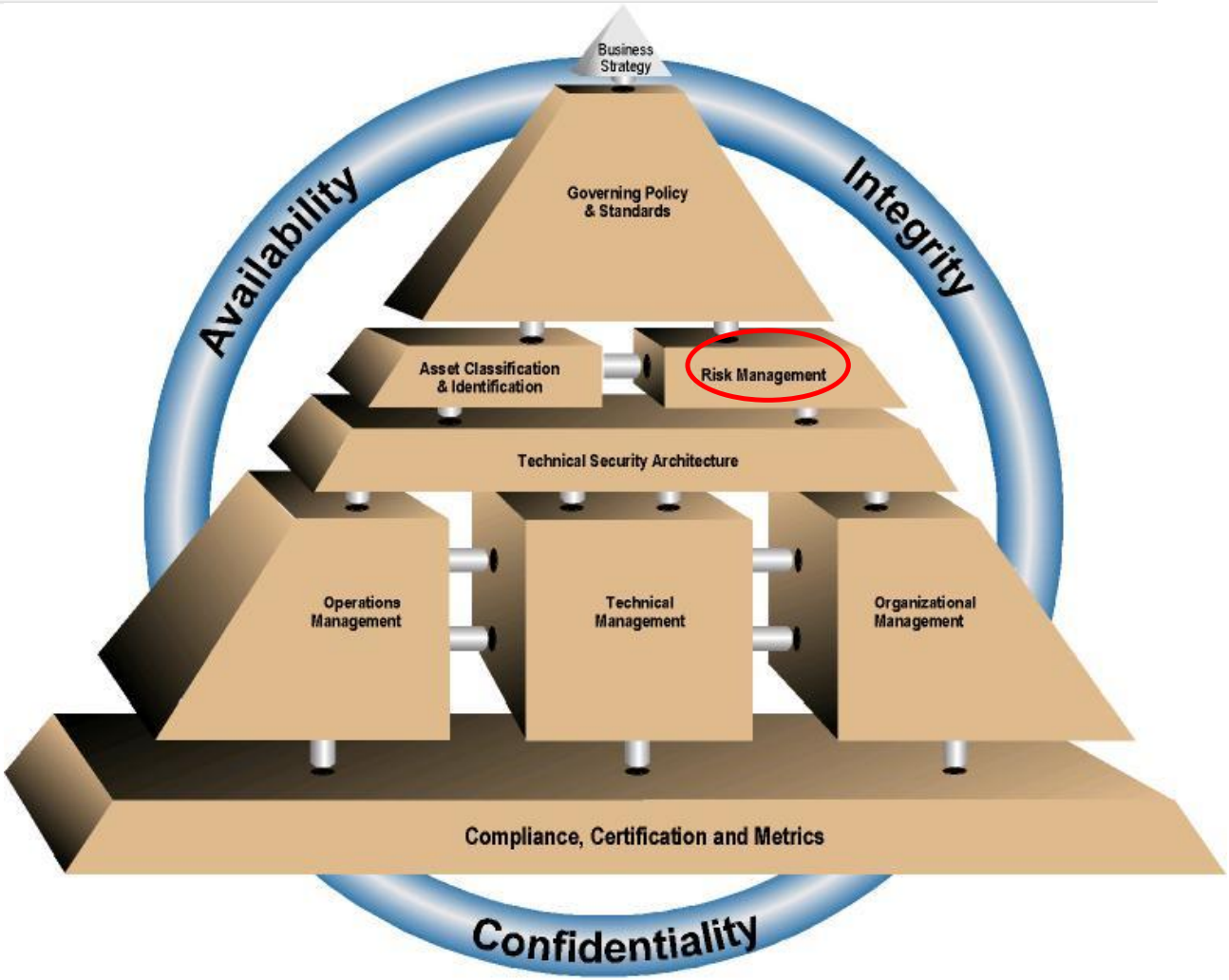
- Founder and Chairman of *iTcon Ltd.* (1995)
  - An information security consulting firm, specializing in enterprise security architecture, in Israel and in Europe.
- Founder and CEO of *White Cyber Knight* (2006)
  - A start-up company developing a comprehensive IT Risk Management software, for large and medium-sized organizations.
- Involvement in leading Research Activities by the European Commission:
  - The Chairman of the EU SRMI – Security Risk Management Initiative
  - A member of the advisory board for the ***CI2RCO*** project
  - A member of the advisory board for the ***IRRIIS*** project
  - One of the Editors of the ***European CIIP Newsletter***.
  - Member of the ***ACIP*** Project

The Need for IT Risk Management

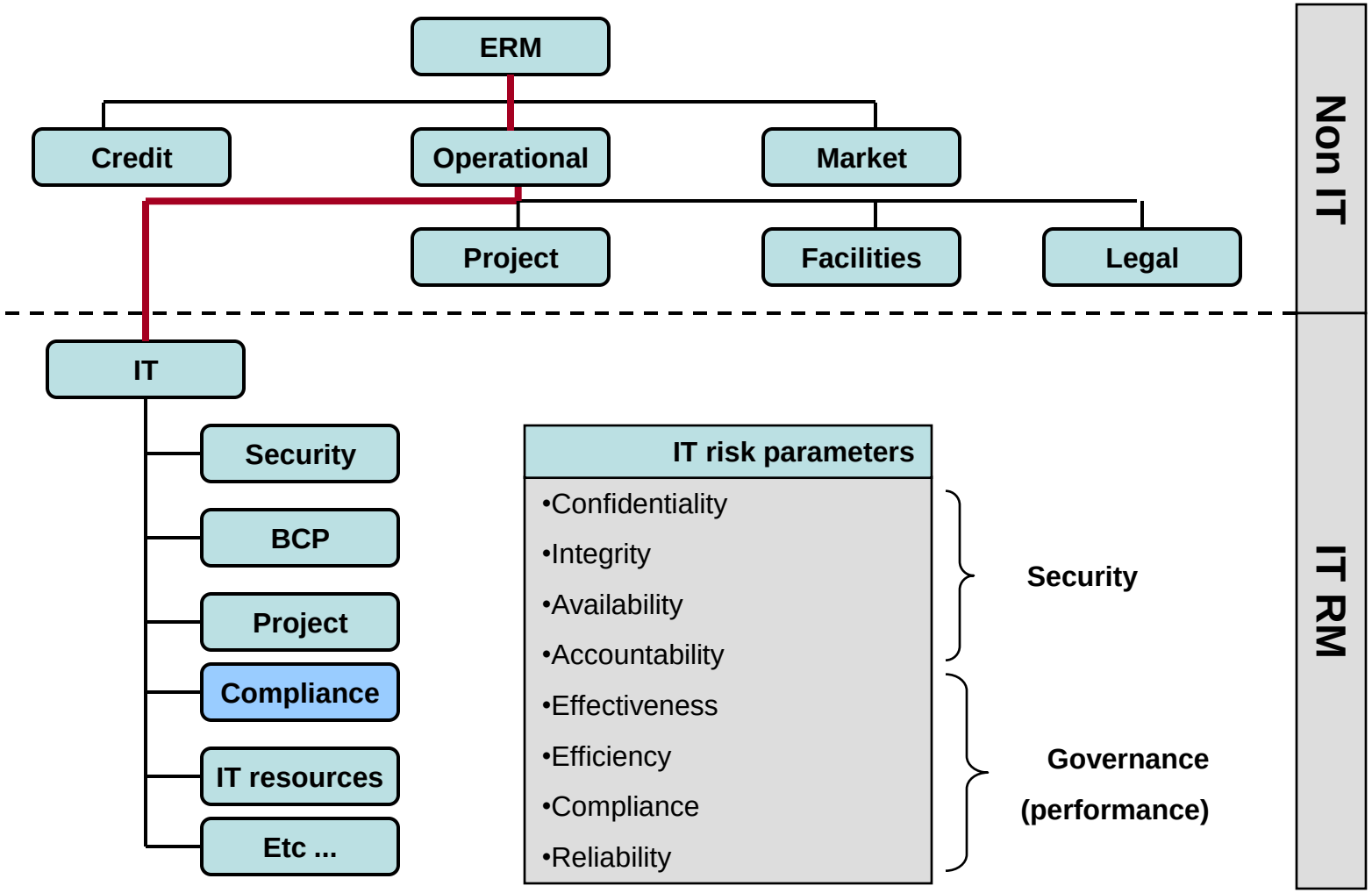
- New regulatory requirements (SOX, Basel II, FISMA) demand continuous and managed Risk Management
- Risk reduction became the main driver for IT investments
- A need to convert security to business language

A new era requires new methods and tools

IT Risk Management within the Security Control Framework



IT RM Scope

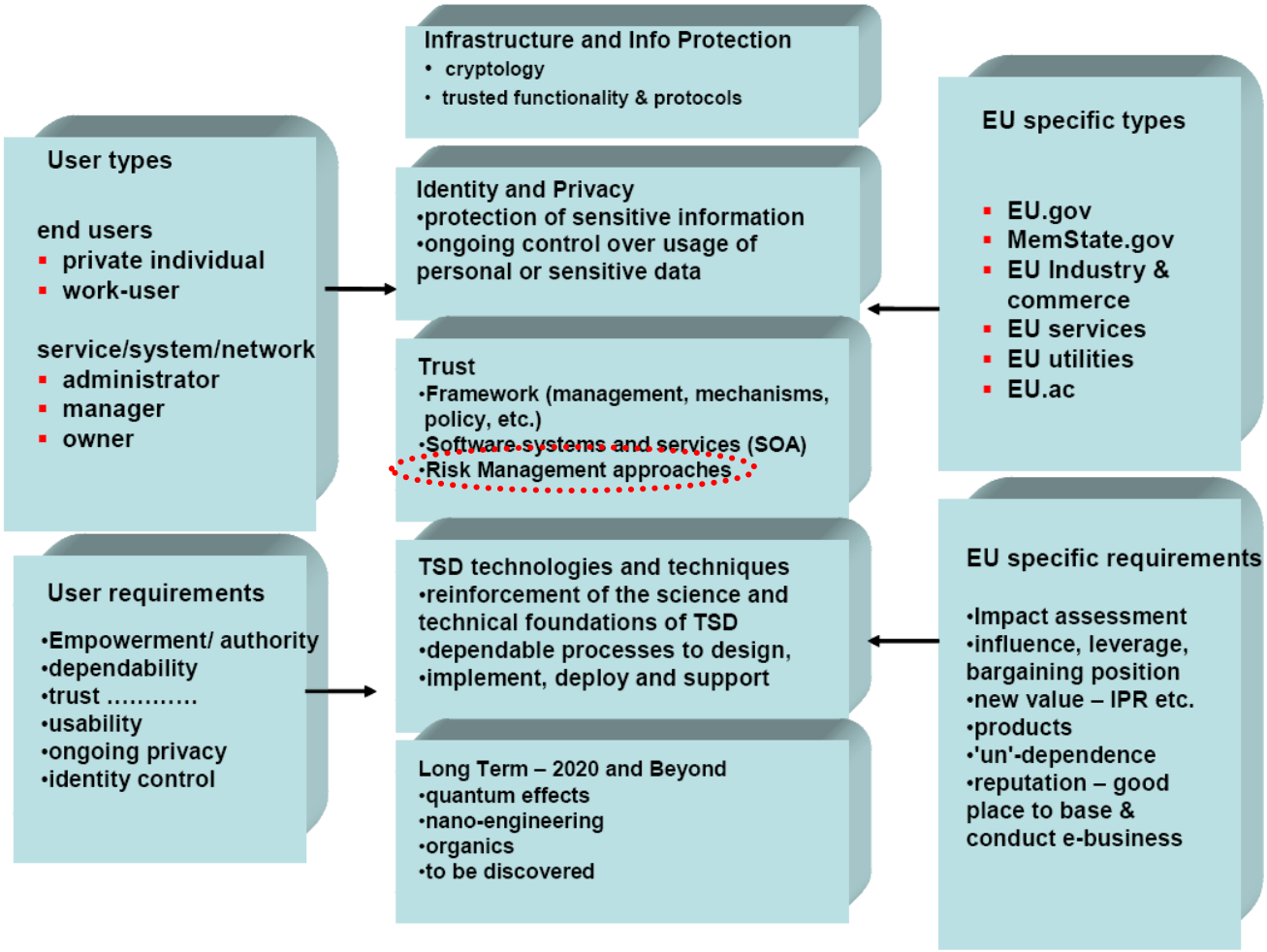


The capacity to manage risk and with it to make forward looking choices are key elements of the energy that drives the economic system forward

Research Challenges

The Importance of Risk Management

From: ICT Security & Dependability Research beyond 2010: Final strategy



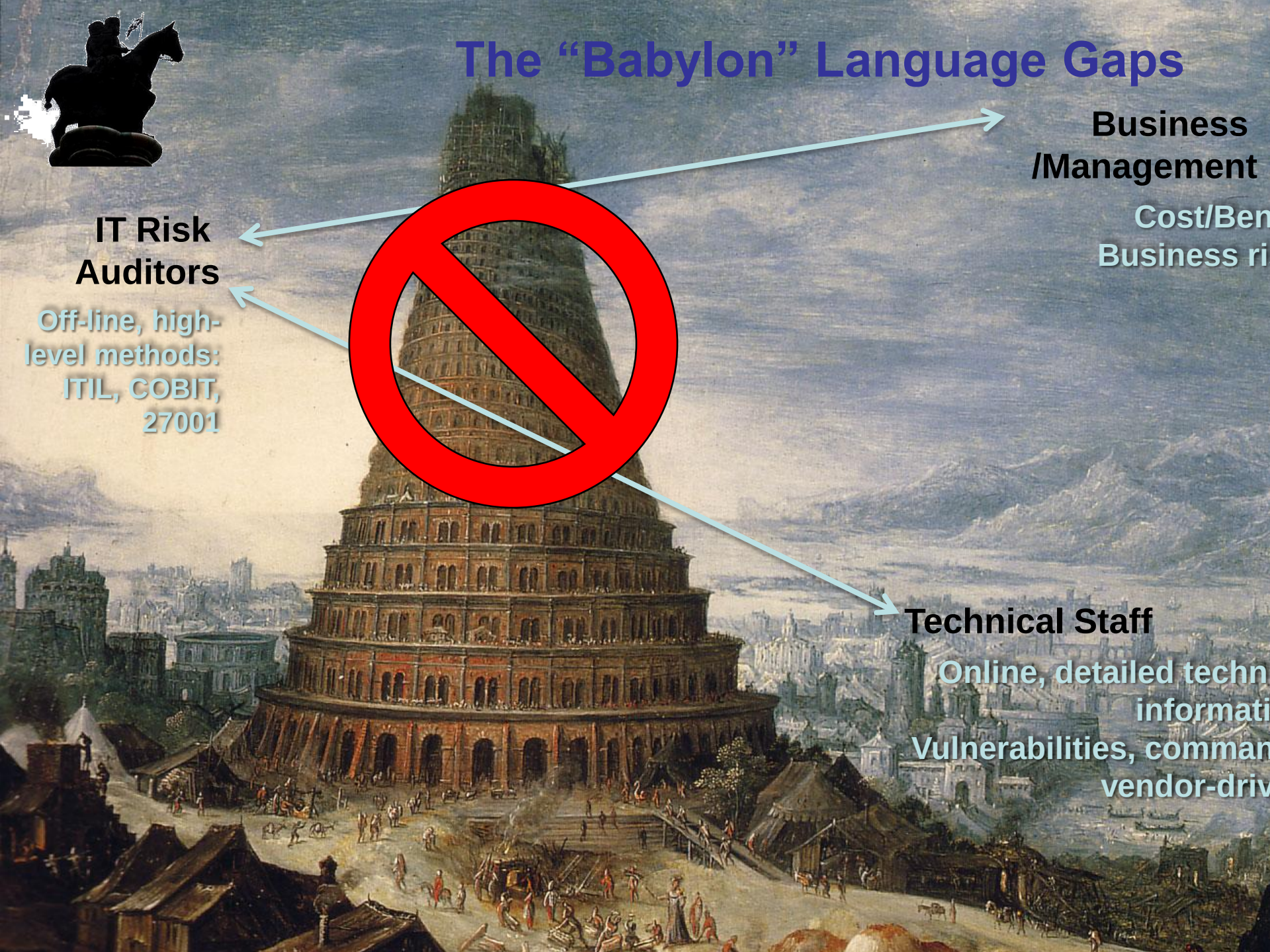
EU Perspective

Building a Trustworthy Service-centric Information Society

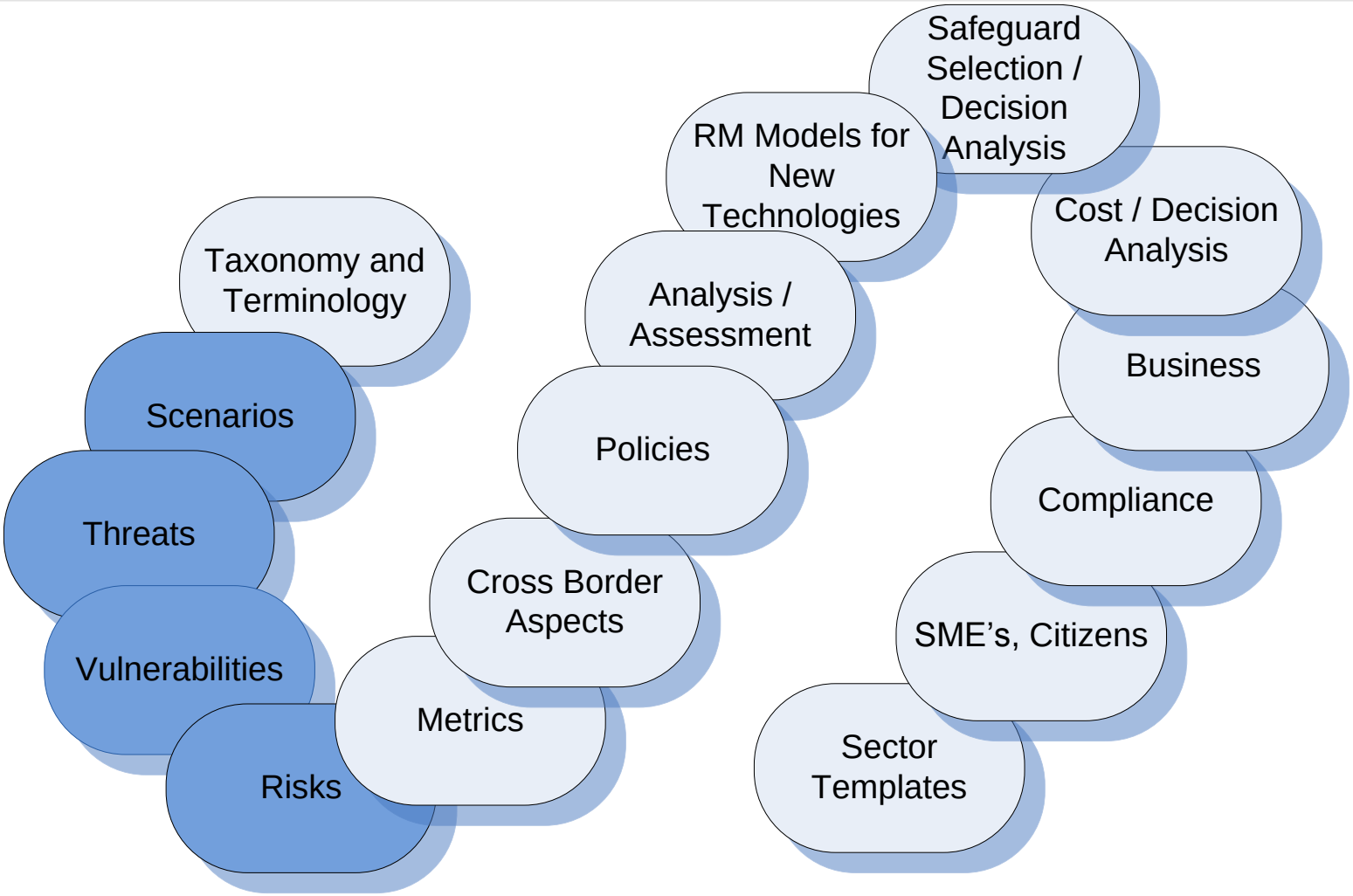
ESFORS Software and Service Development, Security & Dependability Workshop

- Trustworthy, scalable services across any medium & domain
- Trusted cross-domain Collaborations & Interactions
- Trusted Computing Infrastructures
- Situational & Context Awareness; Self-Awareness
- Risk assessment & Risk Management
- Engineering Secure and Dependable complex SW & Service systems
- Empowering Users: User-friendly Privacy & Trust Services
- Metrics, Certification, Standards
- …

From: "*Setting the Scene and PF7 Update*" by **Jacques Bus**, presented at the ESFORS workshop in Paris, September 2006


The “Babylon” Language Gaps
Business /Management
Cost/Ben
Business ri
IT Risk Auditors
Off-line, high-level methods: ITIL, COBIT, 27001
Technical Staff
Online, detailed techn
informati
Vulnerabilities, comman
vendor-driv

SRMI – Security Risk Management Initiative Research Areas



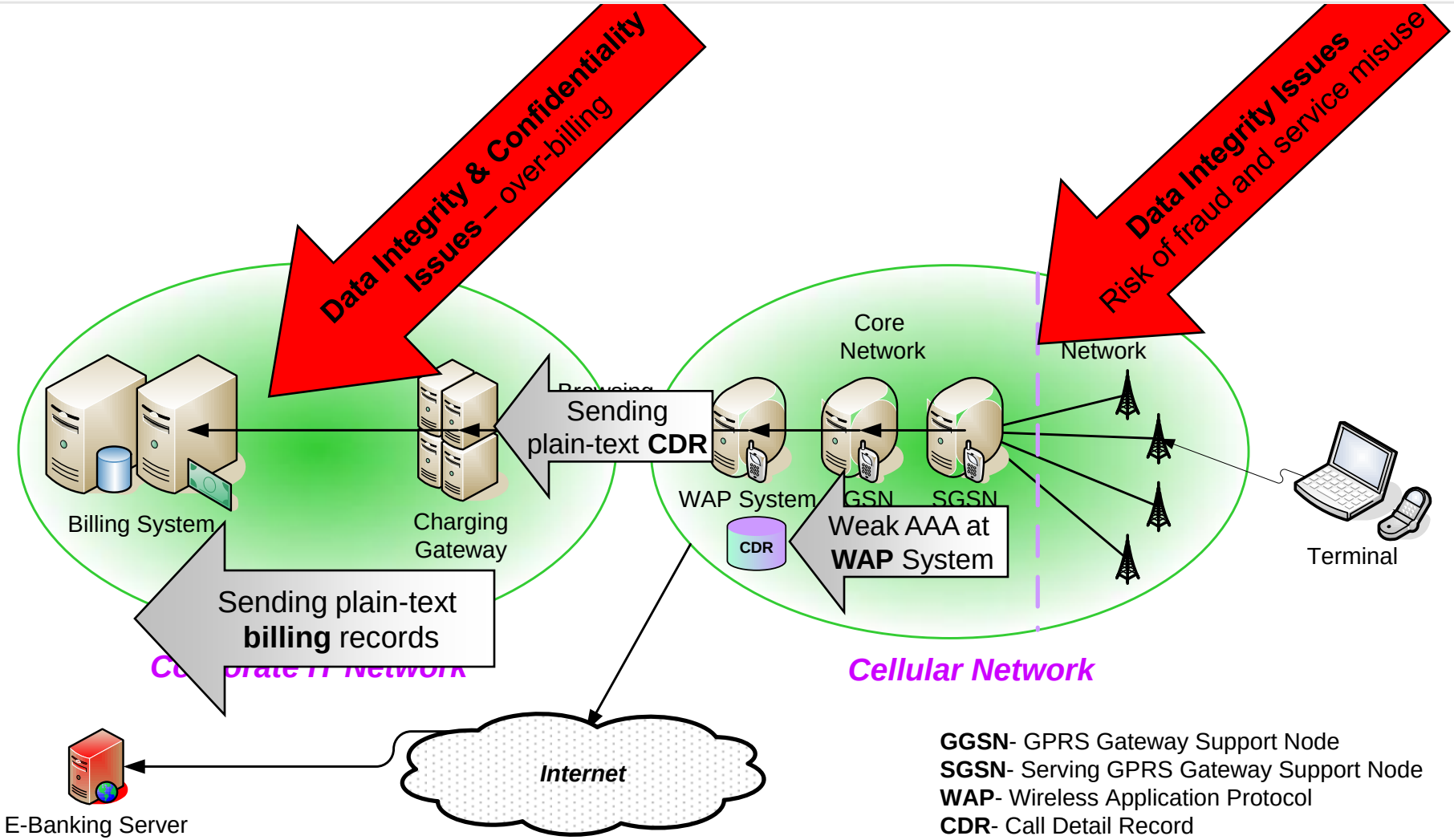
Vulnerabilities and Risks

- **Vulnerabilities**
  - Examples:
    - Meta language for automated tools
    - Correlation between threats and vulnerabilities
- **Risks**
  - Examples:
    - Risks ownership in complex environment

Threats

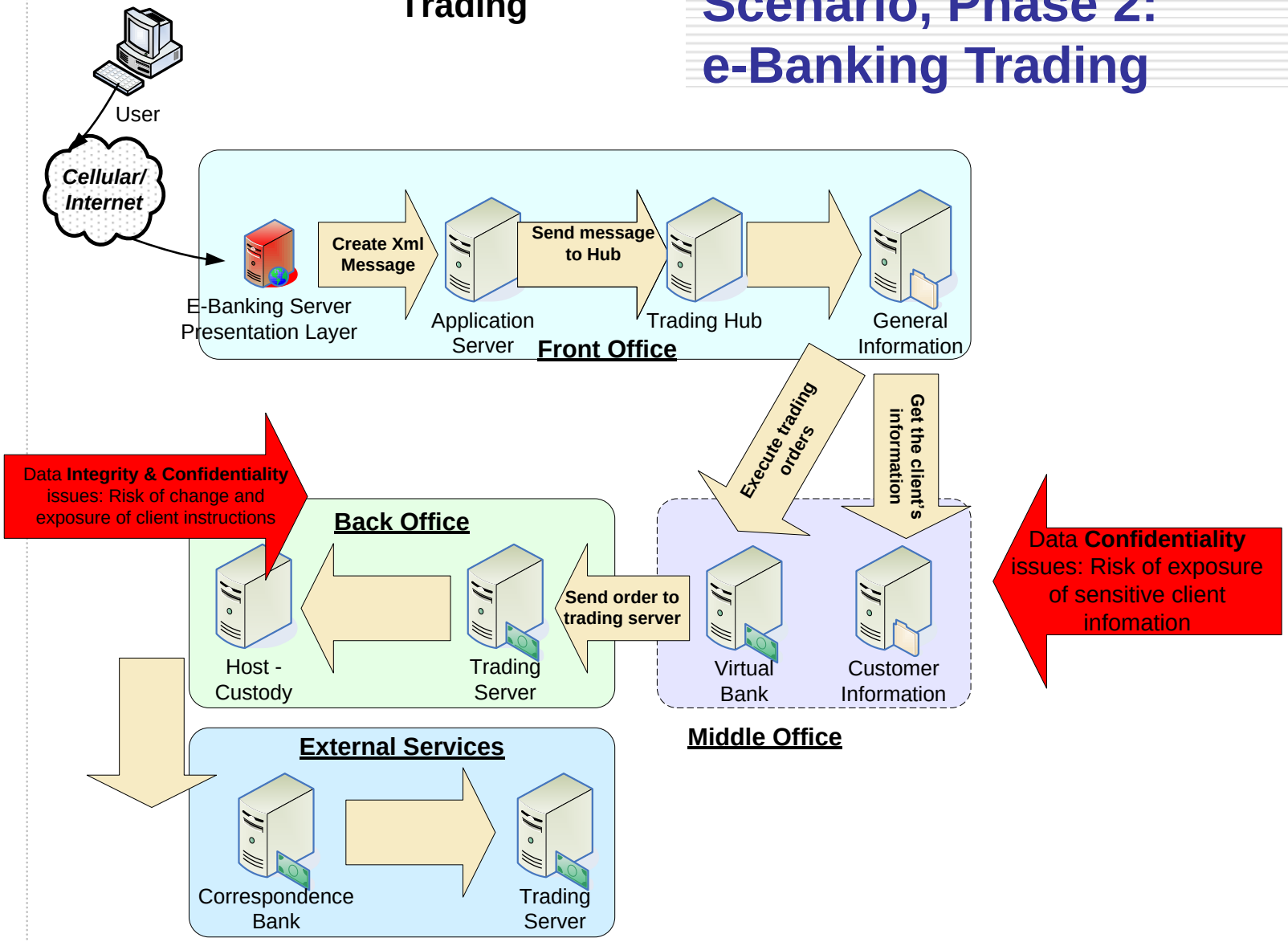
- Finding methods and tools, to identify new threats of complex systems and complex scenarios
  - Metrology (finding the right variables)
  - Threats identification and measure (statistics)
  - Anonymity of threats information
  - Motivation identification
  - Behavior of IT systems
  - Attack scenarios and trees
  - Likelihood and Impact of threats
  - Escalation and propagation

Example: Complex Scenario, Threats

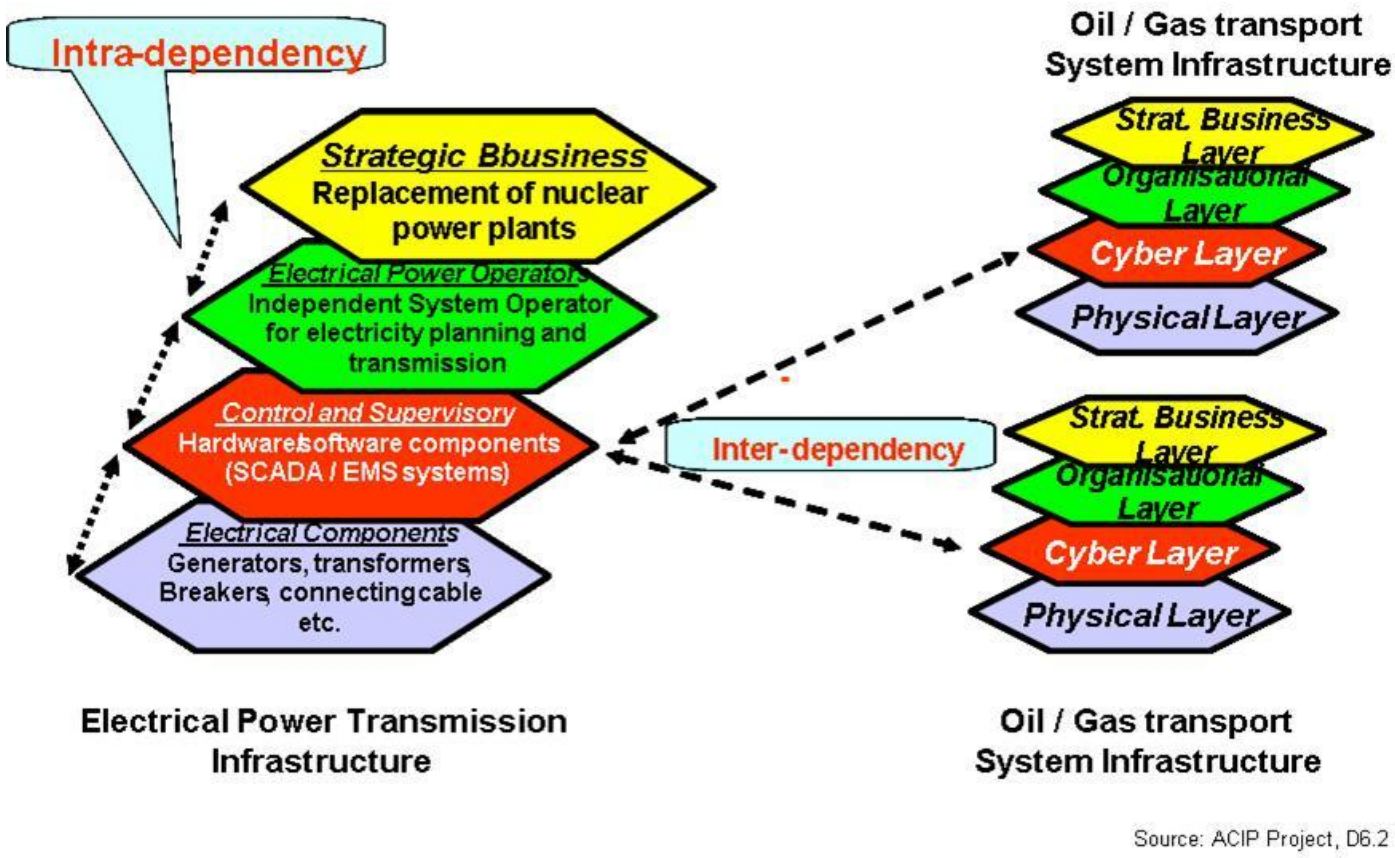


GGSN- GPRS Gateway Support Node
SGSN- Serving GPRS Gateway Support Node
WAP- Wireless Application Protocol
CDR- Call Detail Record

Example of a Complex Scenario, Phase 2: e-Banking Trading

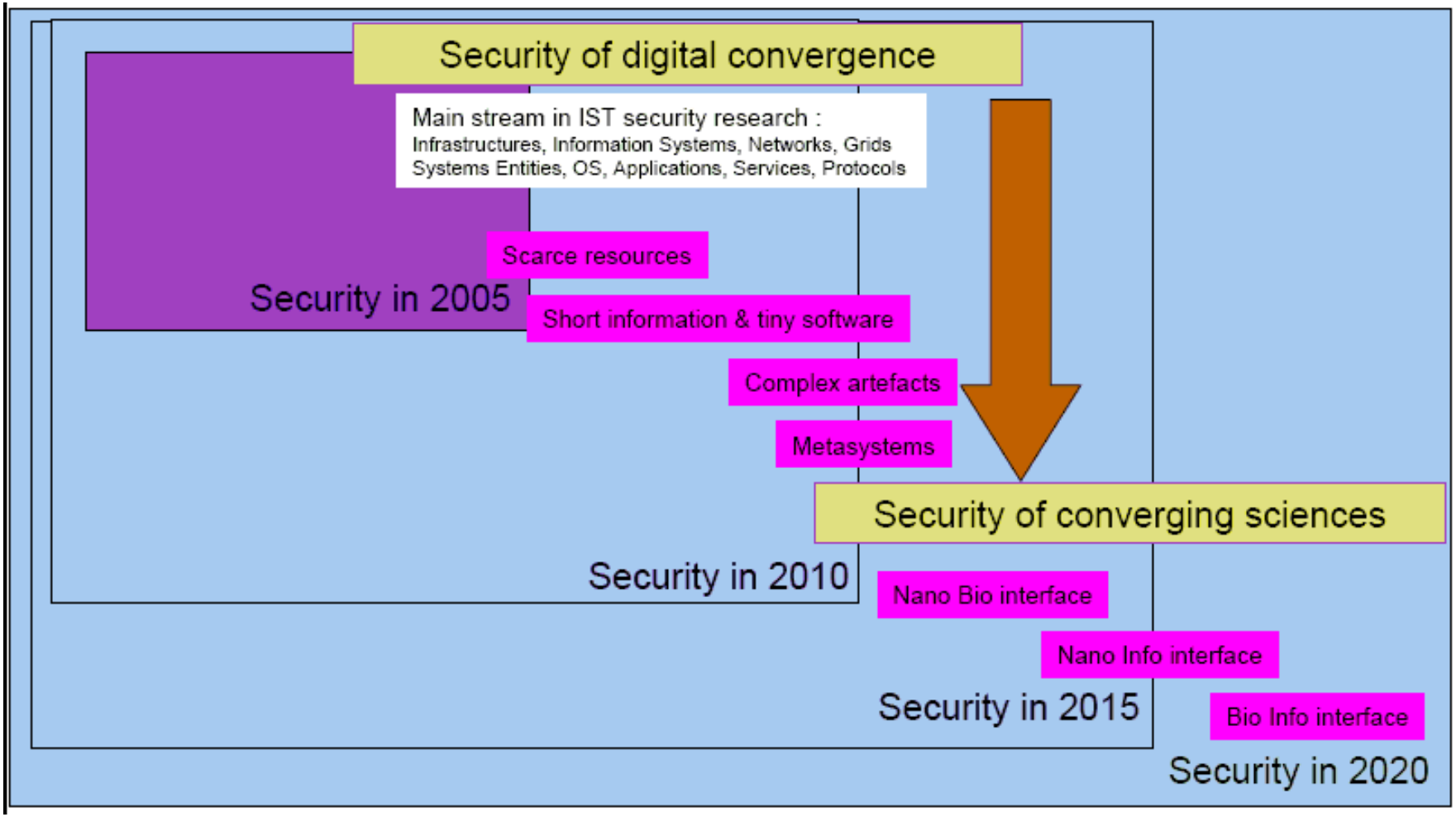


Example: CIP Dependencies Assessment



Source: ACIP Project, D6.2

RM Models for New Technologies
(Proff. Michel Riguidel, Enst Paris, ESFORS Workshop, 2006)

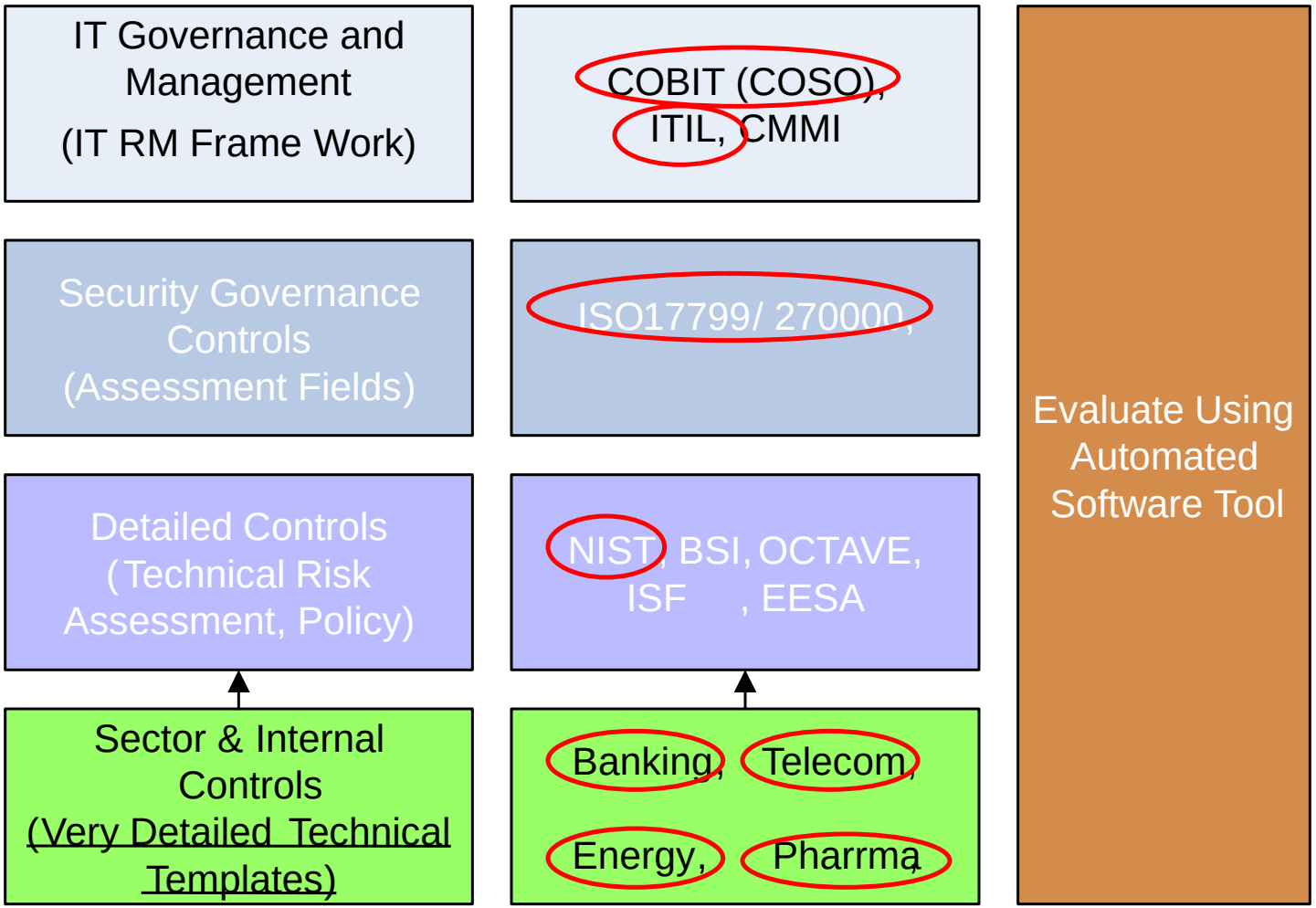


White Cyber Knight

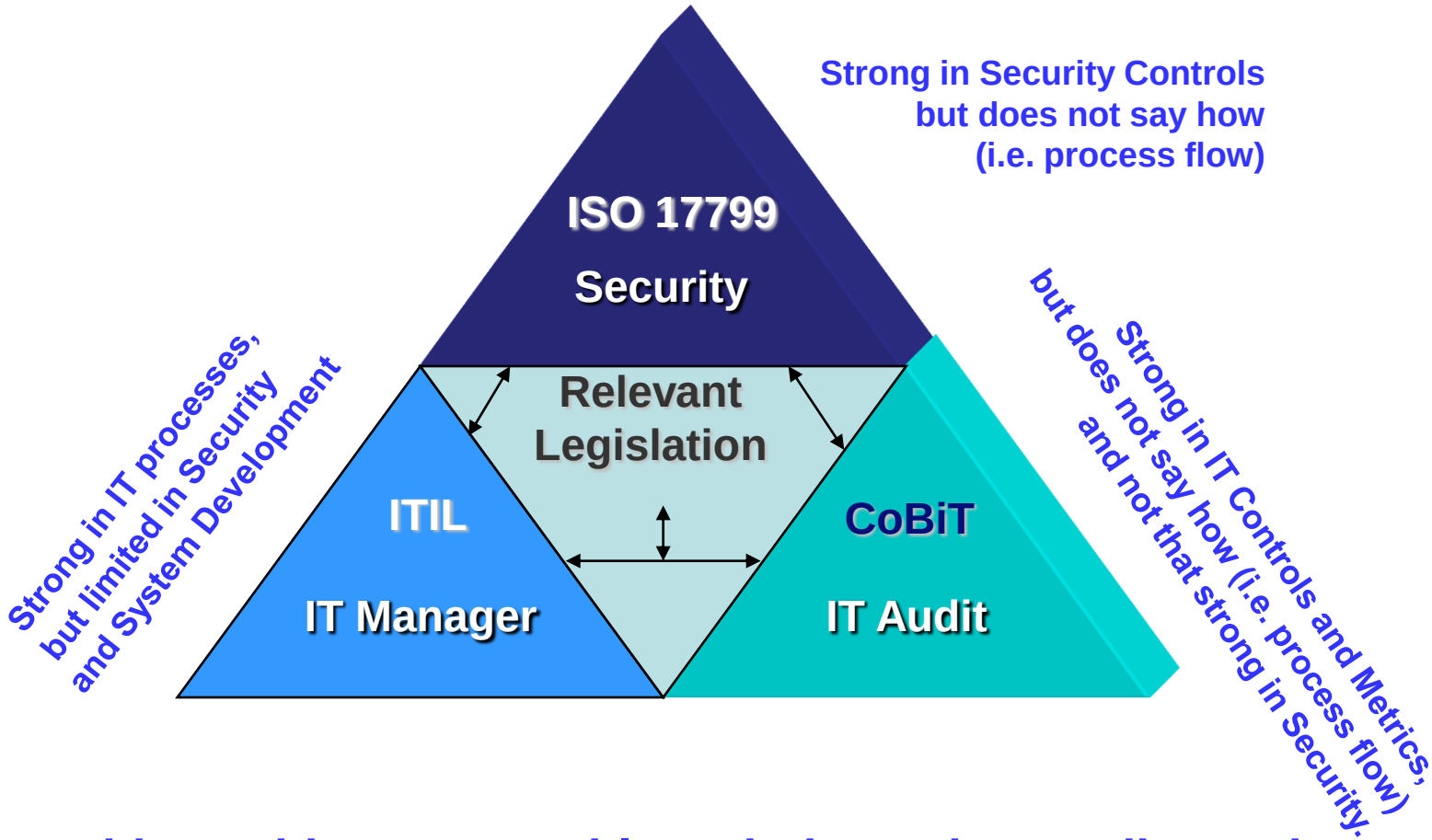
WCK

Best Practices

Bridging The Gaps:
Risk Management - Layer Integration

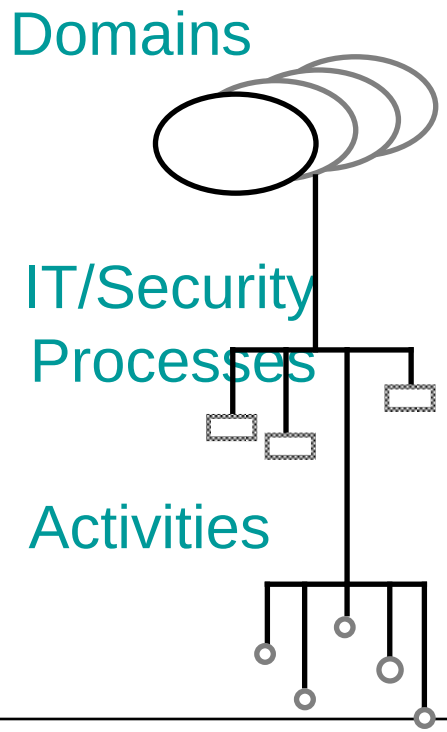


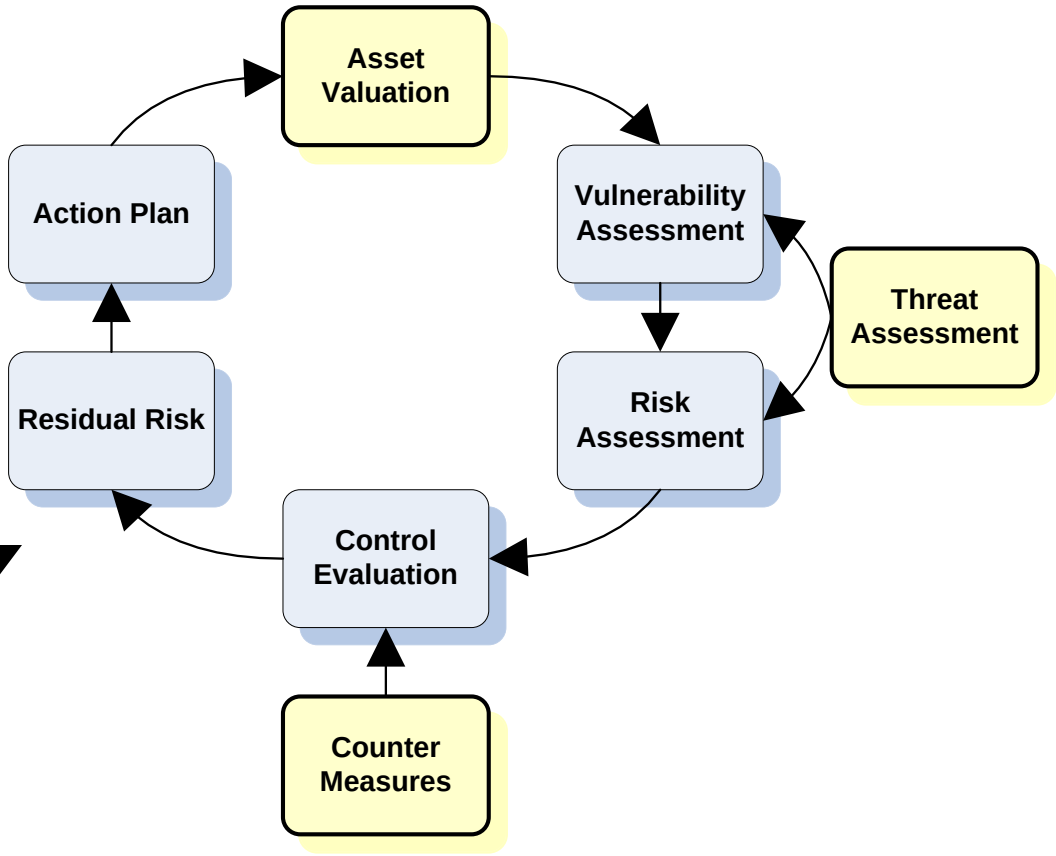
Control Framework Development



Provides guidance to enable an independent auditor to issue an opinion on the organisation's description of controls

Cobit IT Risk Management (FrameWork)





ISO 27001 Areas

The NIST Risk Framework

Starting Point

FIPS 199 / SP 800-60

Security Categorization

Define category of information system according to potential impact of loss

FIPS 200 / SP 800-53

Security Control Selection

Select minimum security controls (i.e., safeguards and countermeasures) planned or in place to protect the information system

SP 800-37

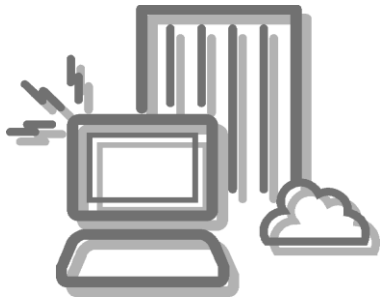
Security Control Monitoring

Track changes to the information system that may affect security controls and assess control effectiveness on an ongoing basis

FIPS 200 / SP 800-53 / SP 800-30

Security Control Refinement

Use risk assessment to tailor minimum security controls based on local conditions, required threat coverage, specific agency requirements



SP 800-37

System Authorization

Determine risk to agency operations, agency assets, or individuals and, if acceptable, authorize information system processing

SP 800-18

Security Control Documentation

Provide a an overview of the security requirements for the information system and the security controls planned or in place in the System Security Plan

SP 800-70

Security Control Implementation

Implement security controls in new or legacy information systems; implement security configuration checklists

SP 800-53A

Security Control Assessment

Determine extent to which the security controls are implemented correctly, operating as intended, and producing desired outcome with respect to meeting security requirements

White Cyber Knight

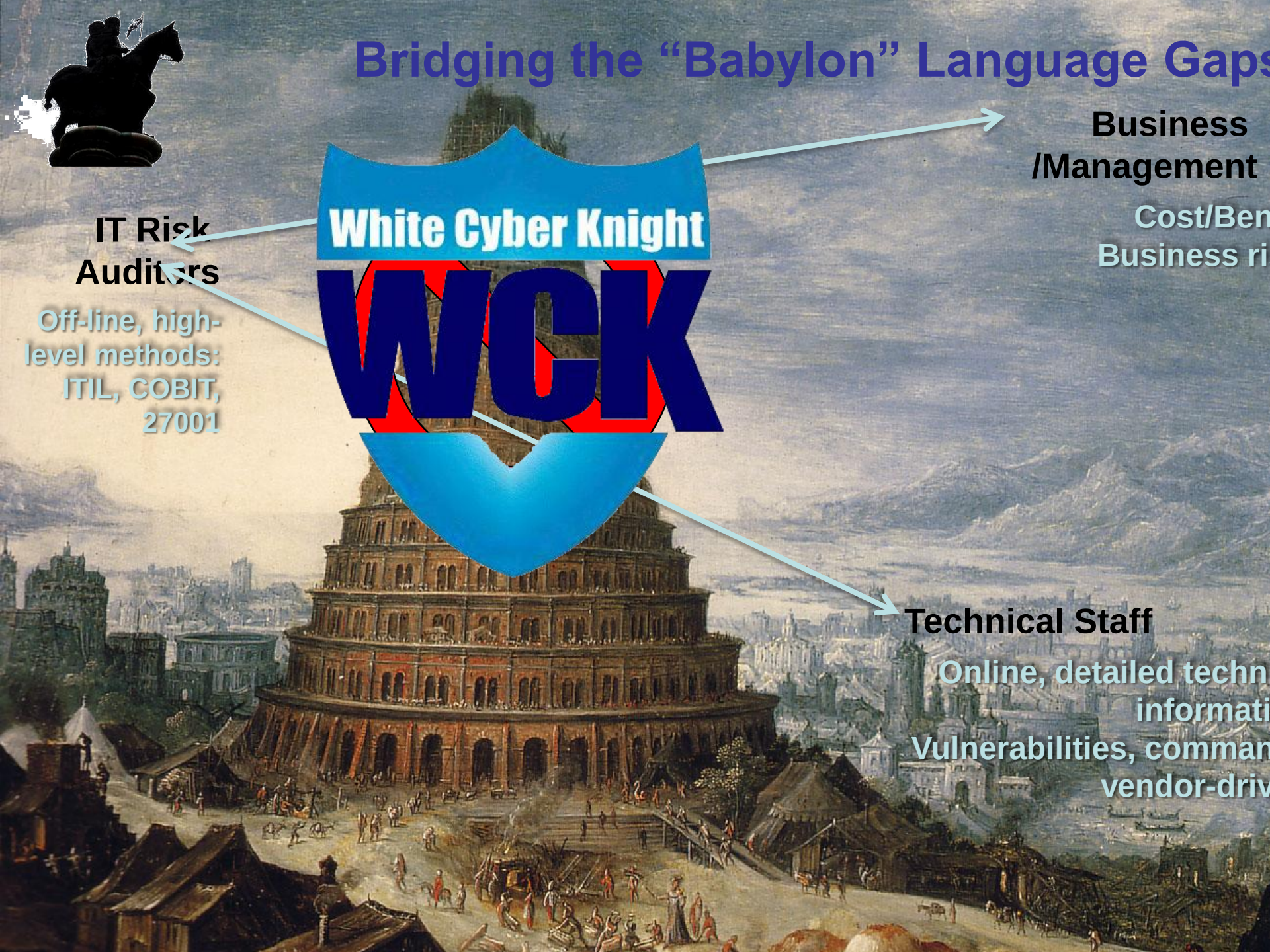
WCK

Example of Risk Management SW tool

White Cyber Knight

During the middle ages, in times of passive acceptance of fate, the knights were the only ones to manage risks actively, thus protecting territory, assets and population.

The risk management software will be tomorrow's knight.

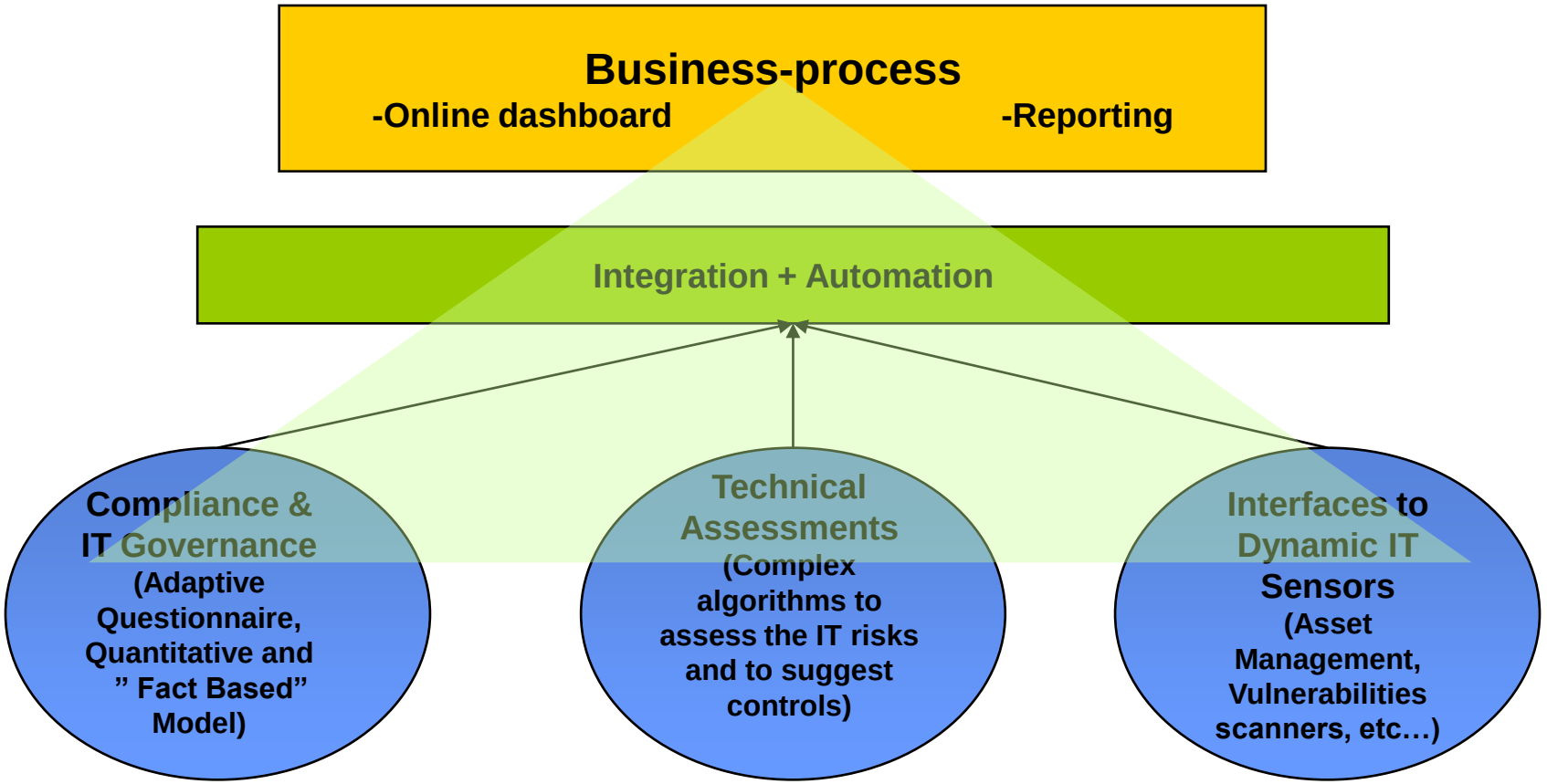

Bridging the “Babylon” Language Gaps
White Cyber Knight
WCK
Business /Management
Cost/Ben
Business ri
IT Risk Auditors
Off-line, high-level methods: ITIL, COBIT, 27001
Technical Staff
Online, detailed techn
informati
Vulnerabilities, comman
vendor-driv

Main Features

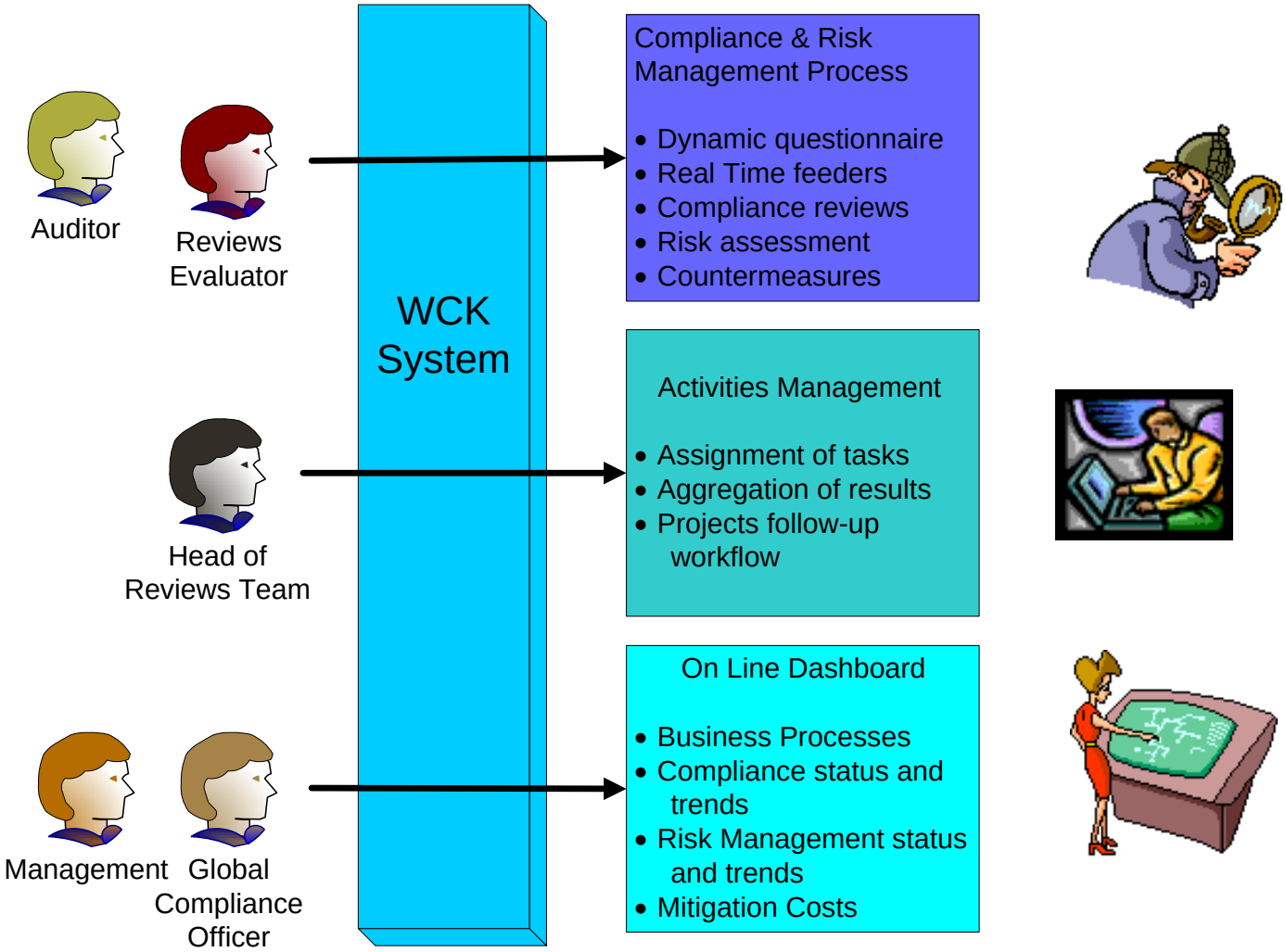
- Questionnaire-based reviews fits your specific infrastructure
- Collects information from dynamic sensors
- Assesses and quantify risks, provide a consolidated status
- Suggests mitigation, provide project handling workflow
- Converts risk language into business-process-level
- Real-time risk status; tailor-made reports

WCK – White Cyber Knight

Unique Approach, IT/Security Compliance and Risk Management SW



Product Overview
Users and Main Tasks




Thank you!