IT Risk Management Era: Research Challenges and Best Practices

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

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

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

Infrastructure and Info Protection
• cryptology
• trusted functionality & protocols

Identity and Privacy
• protection of sensitive information
• ongoing control over usage of personal or sensitive data

Trust
• Framework (management, mechanisms, policy, etc.)
• Software systems and services (SOA)
• Risk Management approaches

User types
• end users
  • private individual
  • work-user

• service/system/network
  • administrator
  • manager
  • owner

User requirements
• Empowerment/authority
• dependability
• trust
• usability
• ongoing privacy
• identity control

TSD technologies and techniques
• reinforcement of the science and technical foundations of TSD
• dependable processes to design, implement, deploy and support

Long Term – 2020 and Beyond
• quantum effects
• nano-engineering
• organics
• to be discovered

EU specific types
• EU.gov
• MemState.gov
• EU Industry & commerce
• EU services
• EU utilities
• EU.ac

EU specific requirements
• Impact assessment
• influence, leverage, bargaining position
• new value – IPR etc.
• products
• ‘un’-dependence
• reputation – good place to base & conduct e-business
EU Perspective

Building a Trustworthy Service-centric Information Society

- 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

IT Risk Auditors
Off-line, high-level methods: ITIL, COBIT, 27001

Technical Staff
Online, detailed technical information: Vulnerabilities, command, vendor-driven

Business/Management
Cost/Benefit Business risks
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

Data Integrity & Confidentiality Issues – over-billing

Data Integrity Issues
Risk of fraud and service misuse

Sending plain-text CDR

Sending plain-text billing records

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

Copyright © 2007 White Cyber Knight

15
Example of a Complex Scenario, Phase 2: e-Banking Trading

**Data Integrity & Confidentiality issues:** Risk of change and exposure of client instructions

**Data Confidentiality issues:** Risk of exposure of sensitive client information
Example: CIP Dependencies Assessment

- **Intra-dependency**
  - **Strategic Business**
    - Replacement of nuclear power plants
  - **Control and Supervisory**
    - Hardware/software components (SCADA / EMS systems)
  - **Electrical Components**
    - Generators, transformers, breakers, connecting cable, etc.

- **Inter-dependency**
  - **Oil / Gas transport System Infrastructure**
    - Strat. Business Layer
    - Organisational Layer
    - Cyber Layer
    - Physical Layer

Source: ACIP Project, D6.2
RM Models for New Technologies
Bridging The Gaps: Risk Management - Layer Integration

IT Governance and Management
(IT RM Frame Work)

Security Governance Controls
(Assessment Fields)

Detailed Controls
(Technical Risk Assessment, Policy)

Sector & Internal Controls
(Very Detailed Technical Templates)

COBIT (COSO), ITIL, CMMI

ISO17799/ 270000

NIST, BSI, OCTAVE, ISF, EESA

Evaluate Using Automated Software Tool

Banking, Telecom, Energy, Pharma
Control Framework Development

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

ISO 17799: Strong in Security Controls but does not say how (i.e. process flow)

ITIL: Strong in IT processes, but limited in Security and System Development

CoBiT: Strong in IT Controls and Metrics, but does not say how (i.e. process flow)

Relevant Legislation: Interconnects ITIL and CoBiT
Cobit IT Risk Management (FrameWork)

Domains

IT/Security Processes

Activities

Business Requirements

IT Processes

IT Resources

Asset Valuation

Vulnerability Assessment

Risk Assessment

Control Evaluation

Residual Risk

Action Plan

Counter Measures

Threat Assessment

Copyright © 2007 White Cyber Knight
ISO 27001 Areas

- Business Continuity Management
- System Acquisition Development and Maintenance
- Access Control
- Communications and Operations Management
- Physical and Environmental Security
- Human Resource Security
- Incident Management
- Risk Management
- Asset Classification and Control
- Organization of Information Security
- Compliance
- Security Policy

Compliance to ISO-27001 Risk Map
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 800-30**

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

**FIPS 200 / SP 800-53**

**Security Control Implementation**
Implement security controls in new or legacy information systems; implement security configuration checklists

**SP 800-37**

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

**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

---

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

**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

**SP 800-18**

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

Copyright © 2007, White Cyber Knight
Example of Risk Management SW tool
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

IT Risk Auditors

Off-line, high-level methods: ITIL, COBIT, 27001

Business/Management

Cost/Benefit

Business risks

Technical Staff

Online, detailed technical information

Vulnerabilities, command, vendor-driven
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
Unique Approach, IT/Security Compliance and Risk Management SW

- **Business-process**
  - Online dashboard
  - Reporting

- **Integration + Automation**

- **Compliance & IT Governance**
  - (Adaptive Questionnaire, Quantitative and "Fact Based" Model)

- **Technical Assessments**
  - (Complex algorithms to assess the IT risks and to suggest controls)

- **Interfaces to Dynamic IT Sensors**
  - (Asset Management, Vulnerabilities scanners, etc...)

WCK – White Cyber Knight
Product Overview

Users and Main Tasks

WCK System

- Compliance & Risk Management Process
  - Dynamic questionnaire
  - Real Time feeders
  - Compliance reviews
  - Risk assessment
  - Countermeasures

- Activities Management
  - Assignment of tasks
  - Aggregation of results
  - Projects follow-up workflow

- On Line Dashboard
  - Business Processes
  - Compliance status and trends
  - Risk Management status and trends
  - Mitigation Costs

Roles:
- Auditor
- Reviews Evaluator
- Head of Reviews Team
- Management
- Global Compliance Officer
Thank you!