ISACA®
Trust in, and value from, information systems

Assessing & Managing IT Risks: Using ISACA's CobiT & Risk IT Frameworks

2o InfoCom Security Conference

Anestis Demopoulos, Vice President ISACA Athens Chapter, & Senior Manager, Advisory Services, Ernst & Young

5 April 2012

Contents

- A few words about ISACA
- The need for an IT risk framework
- Risk IT Process model & CobiT
- Risk IT vs. other standards & frameworks
- Conclusions – Benefits & Outcomes

What is ISACA?

ISACA®
Trust in, and value from, information systems

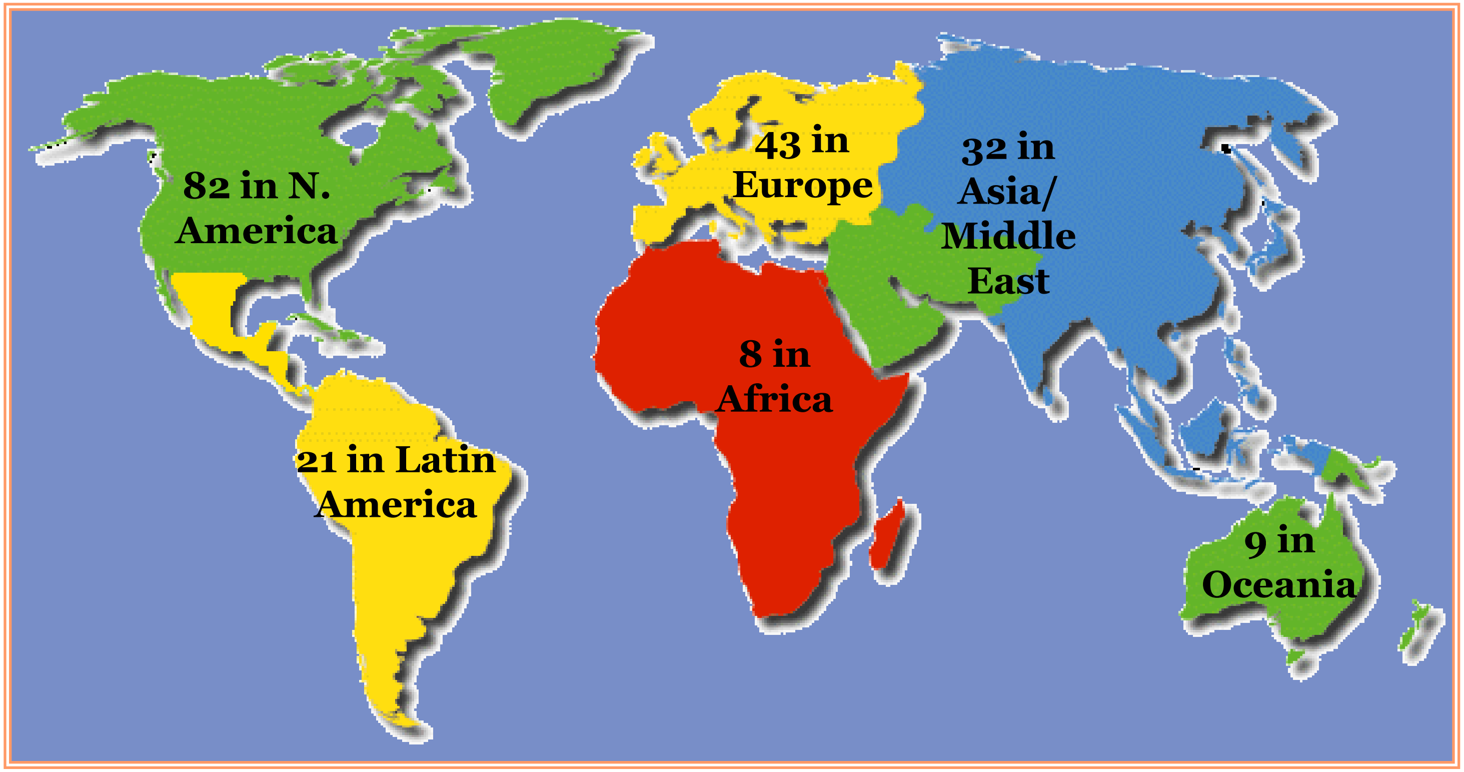
- Non-profit association of individual members:
  - IT auditors
  - IT security professionals
  - IT risk and compliance professionals
  - IT governance professionals and more!
- Nearly all industry categories: financial, public accounting, government/public sector, technology, utilities and manufacturing.
- Formerly, the Information Systems Audit and Control Association -- ISACA now goes by its acronym only.

What is ISACA?

Structure

ISACA®
Trust in, and value from, information systems

One International Headquarters Office
195 Chapters in 81 Countries



(Source: ISACA International data as of October 2011)

ISACA Athens Chapter

- Founded in 1994
- "Ινστιτούτο Ελέγχου Συστημάτων Πληροφορικής"
- Currently more than 385 members
- Its mission is to:
  - Promote IT audit, security & governance in Greece
  - Contribute in and promote relevant standards
  - Support its members through educational activities
  - Promote ISACA professional certifications
  - Support networking and professional growth
- Governed by a local Board of Directors and supported by three Working Groups / Committees (Education issues, Newsletter and Web site)

What does ISACA do?

Certifications

ISACA®
Trust in, and value from, information systems

CISA® Certified Information Systems Auditor®
An ISACA® Certification

70,000+ CISAs certified since inception in 1978

CISM® Certified Information Security Manager®
An ISACA® Certification

12,000+ CISMs certified since inception in 2003

CGEIT® Certified in the Governance of Enterprise IT®
An ISACA® Certification

4,000+ CGEITs certified since inception in 2007

CRISC™ Certified in Risk and Information Systems Control
An ISACA® Certification

10,000+ CRISCs certified since inception in 2010

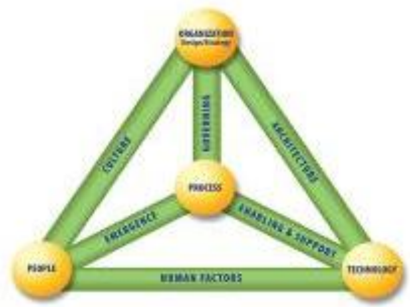
What does ISACA do?

Research

ISACA®
Trust in, and value from, information systems

COBIT® 5
AN ISACA® FRAMEWORK

Val IT™ 2.0
BASED ON COBIT®



BMIS: The Business Model for Information Security

ITAF™
A PROFESSIONAL PRACTICES FRAMEWORK *for* IT ASSURANCE

Risk IT
BASED ON COBIT®

Why Care about IT Risk?

- Risk and value are two sides of the same coin
- Risk is inherent to all enterprises

But…

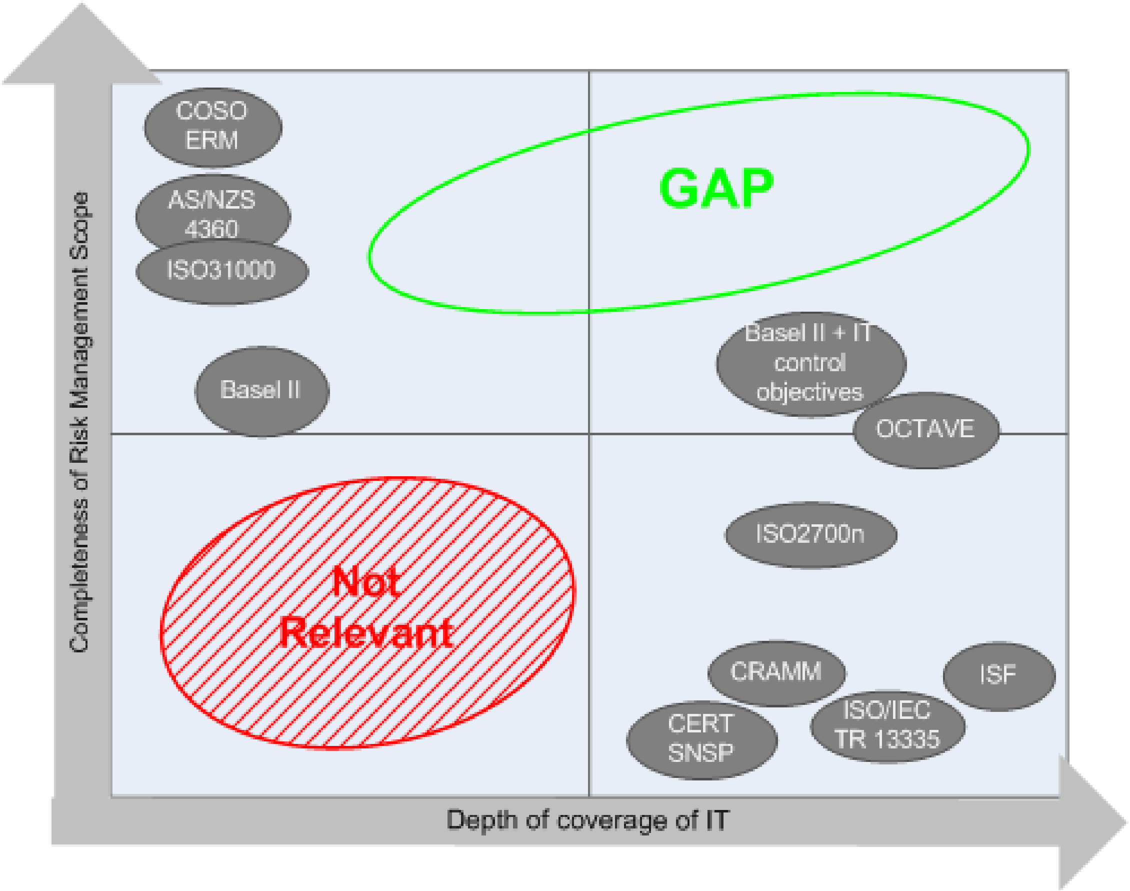
- Need to ensure opportunities for value creation are not missed by trying to eliminate all risk

However…

- Enterprises are dependent on automation and integration
- Need to cross IT silos of risk management
- Important to integrate with existing levels of risk management practices
- Compliance requirements

The need for a Framework...

- Standards and frameworks are available, but are either too:
  - Generic enterprise risk management oriented
  - IT security oriented
- No comprehensive IT- related risk framework available (until now)



Risk IT Framework

Risk IT Includes:

The Risk IT Framework

- Summary + Core Framework
- Helps convey the risk landscape and processes and prioritize activities
- Available as a free download to all

The Risk IT Practitioner Guide

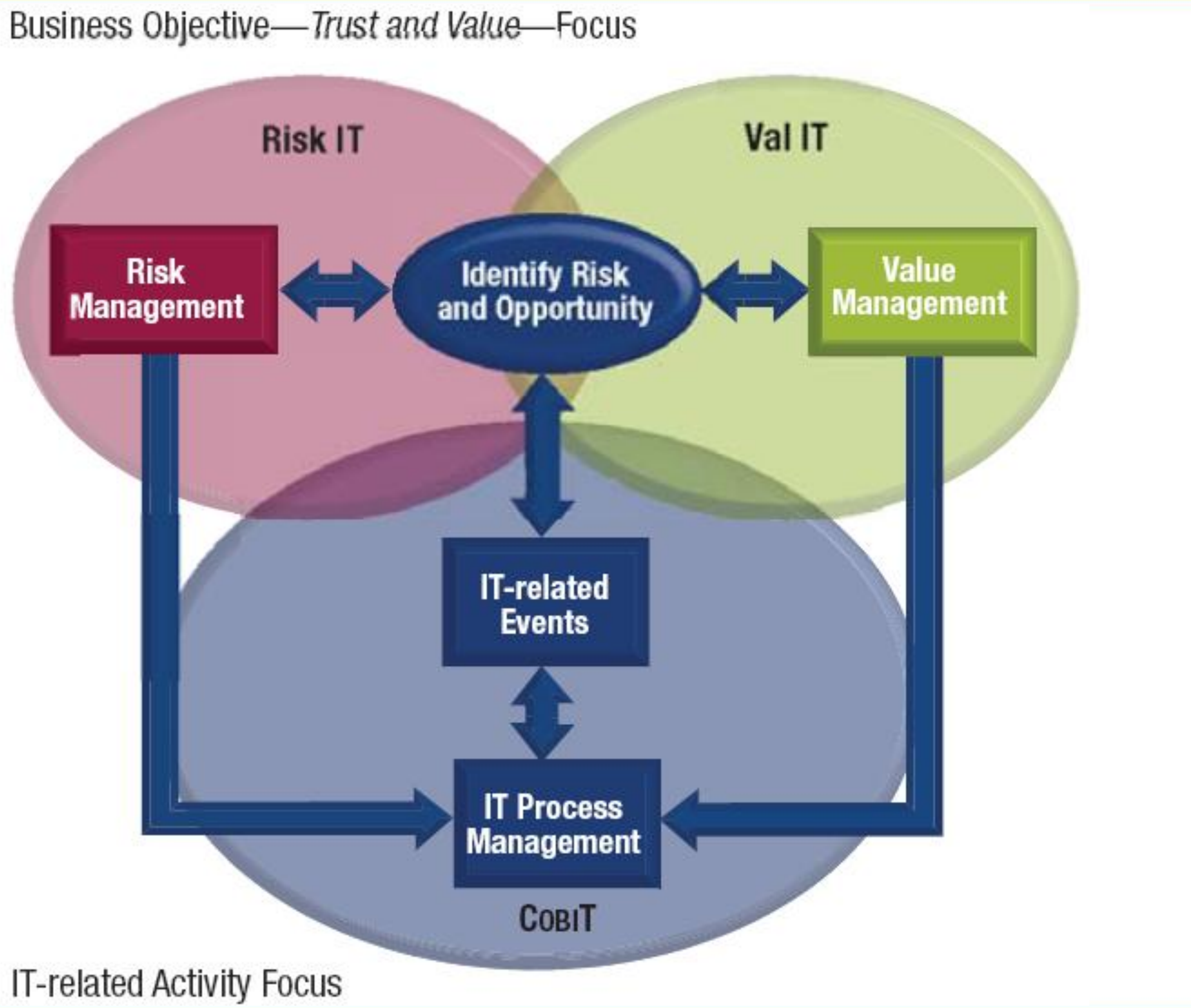
- Provides practical guidance on improving risk management activities
- Available as a free download for ISACA members only

(Both publications are available for purchase in print version)

www.isaca.org/riskit

Risk IT Framework

Risk IT complements and extends COBIT and Val IT to make a more complete IT governance guidance resource.


Business Objective—*Trust and Value*—Focus
Risk IT
Val IT
Risk Management
Identify Risk and Opportunity
Value Management
IT-related Events
IT Process Management
COBIT
IT-related Activity Focus

Risk IT Framework

IT-related Risk Management

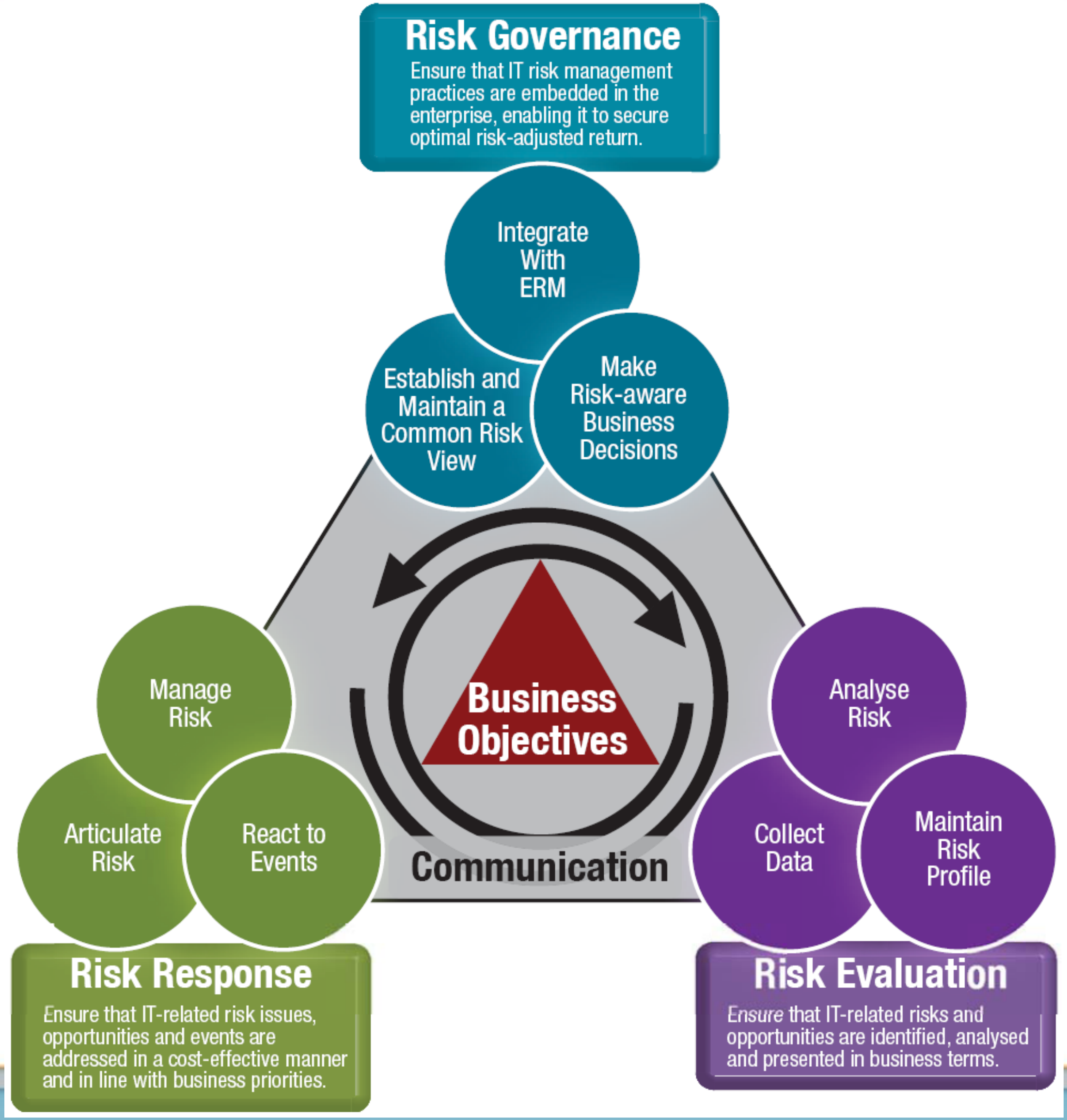
Risk IT is not limited to information security.

It covers **all** IT-related risks, including:

- Late project delivery
- Not achieving enough value from IT
- Compliance
- Misalignment
- Obsolete or inflexible IT architecture
- IT service delivery problems

Risk IT Domains

ISACA®
Trust in, and value from, information systems



Risk Governance

Ensure that IT risk management practices are embedded in the enterprise, enabling it to secure optimal risk-adjusted return.

Risk Response

Ensure that IT-related risk issues, opportunities and events are addressed in a cost-effective manner and in line with business priorities.

Risk Evaluation

Ensure that IT-related risks and opportunities are identified, analysed and presented in business terms.

Risk IT Process model

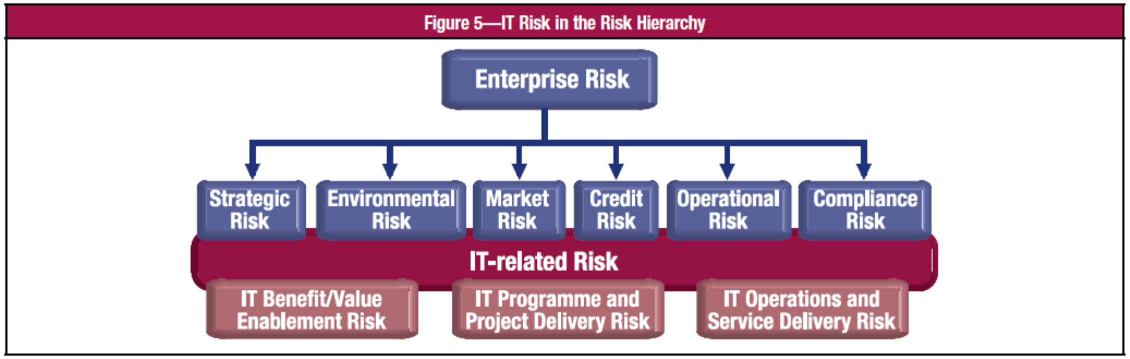
ISACA
Trust in, and value from, information systems

1. Define a risk universe and scoping risk management
2. Risk appetite and risk tolerance
3. Risk awareness, communication and reporting: includes key risk indicators, risk profiles, risk aggregation and risk culture
4. Express and describe risk: guidance on business context, frequency, impact, COBIT business goals, risk maps, risk registers
5. Risk scenarios: includes capability risk factors and environmental risk factors
6. Risk response and prioritization
7. A risk analysis workflow: “swim lane” flow chart, including role context
8. Mitigation of IT risk using COBIT and Val IT

Process Model Examples

1.Define a risk universe and scoping risk management

Figure 5—IT Risk in the Risk Hierarchy



Enterprise Risk

Strategic Risk

Environmental Risk

Market Risk

Credit Risk

Operational Risk

Compliance Risk

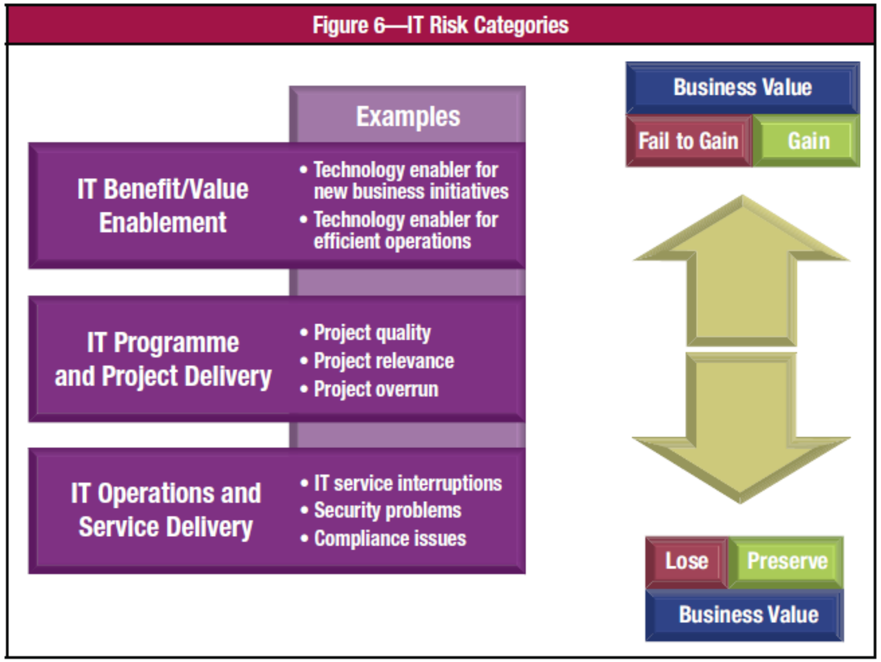
IT-related Risk

IT Benefit/Value Enablement Risk

IT Programme and Project Delivery Risk

IT Operations and Service Delivery Risk

Figure 6—IT Risk Categories



	Examples
IT Benefit/Value Enablement	• Technology enabler for new business initiatives • Technology enabler for efficient operations
IT Programme and Project Delivery	• Project quality • Project relevance • Project overrun
IT Operations and Service Delivery	• IT service interruptions • Security problems • Compliance issues

Process Model Examples

2.Risk appetite and risk tolerance

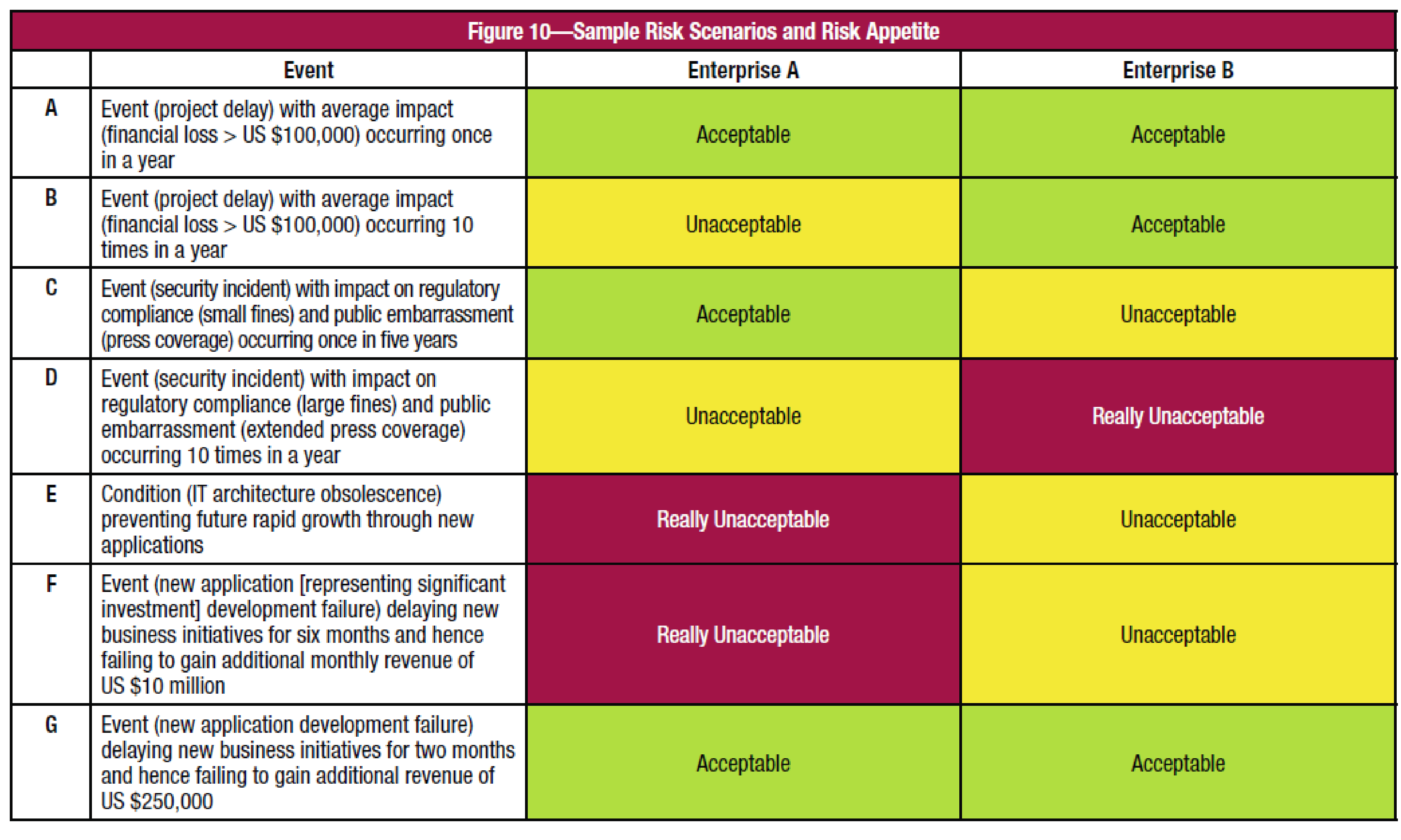


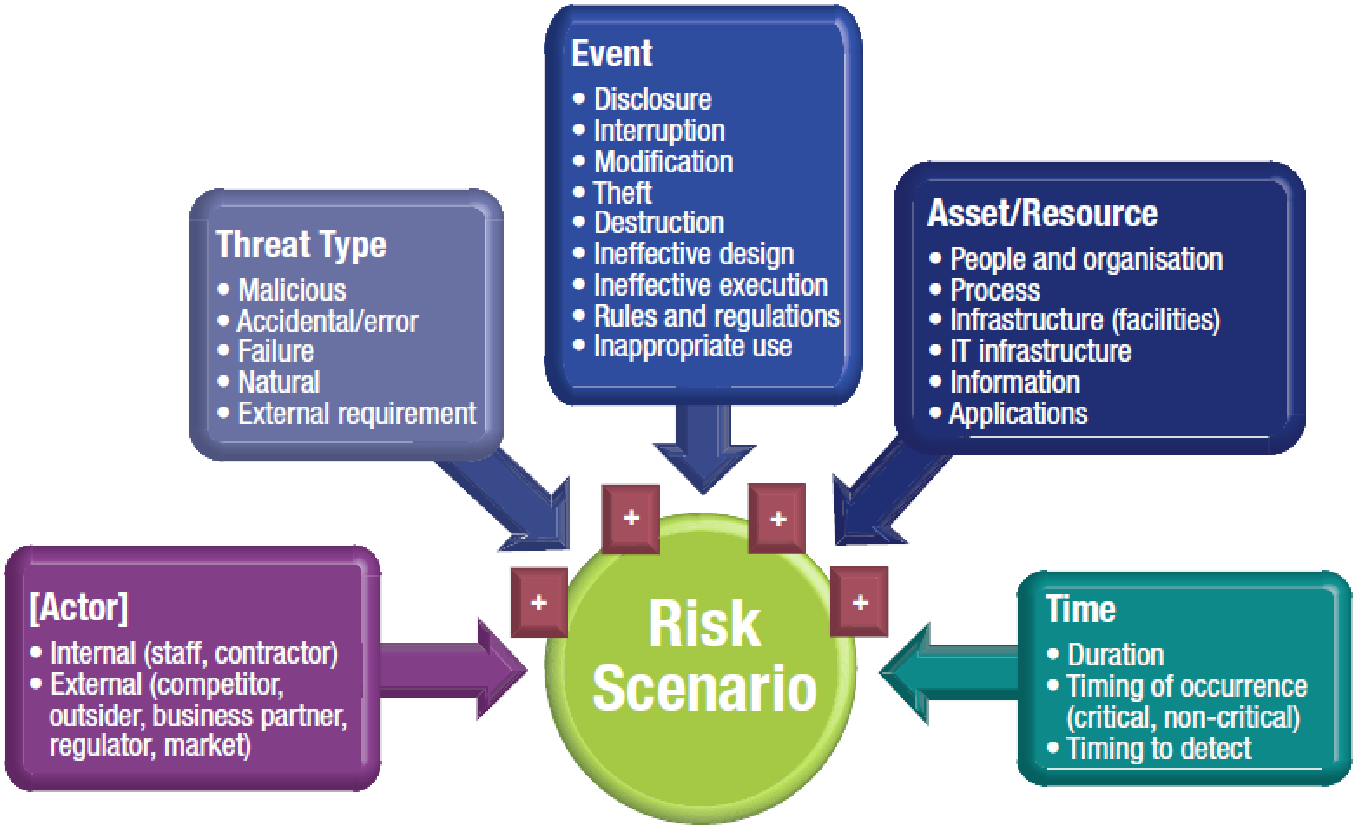
Figure 10—Sample Risk Scenarios and Risk Appetite

	Event	Enterprise A	Enterprise B
A	Event (project delay) with average impact (financial loss > US $100,000) occurring once in a year	Acceptable	Acceptable
B	Event (project delay) with average impact (financial loss > US $100,000) occurring 10 times in a year	Unacceptable	Acceptable
C	Event (security incident) with impact on regulatory compliance (small fines) and public embarrassment (press coverage) occurring once in five years	Acceptable	Unacceptable
D	Event (security incident) with impact on regulatory compliance (large fines) and public embarrassment (extended press coverage) occurring 10 times in a year	Unacceptable	Really Unacceptable
E	Condition (IT architecture obsolescence) preventing future rapid growth through new applications	Really Unacceptable	Unacceptable
F	Event (new application [representing significant investment] development failure) delaying new business initiatives for six months and hence failing to gain additional monthly revenue of US $10 million	Really Unacceptable	Unacceptable
G	Event (new application development failure) delaying new business initiatives for two months and hence failing to gain additional revenue of US $250,000	Acceptable	Acceptable

Process Model Examples

5.Risk scenarios

Figure 39—IT Risk Scenario Components



Threat Type
- Malicious
- Accidental/error
- Failure
- Natural
- External requirement

Event
- Disclosure
- Interruption
- Modification
- Theft
- Destruction
- Ineffective design
- Ineffective execution
- Rules and regulations
- Inappropriate use

Asset/Resource
- People and organisation
- Process
- Infrastructure (facilities)
- IT infrastructure
- Information
- Applications

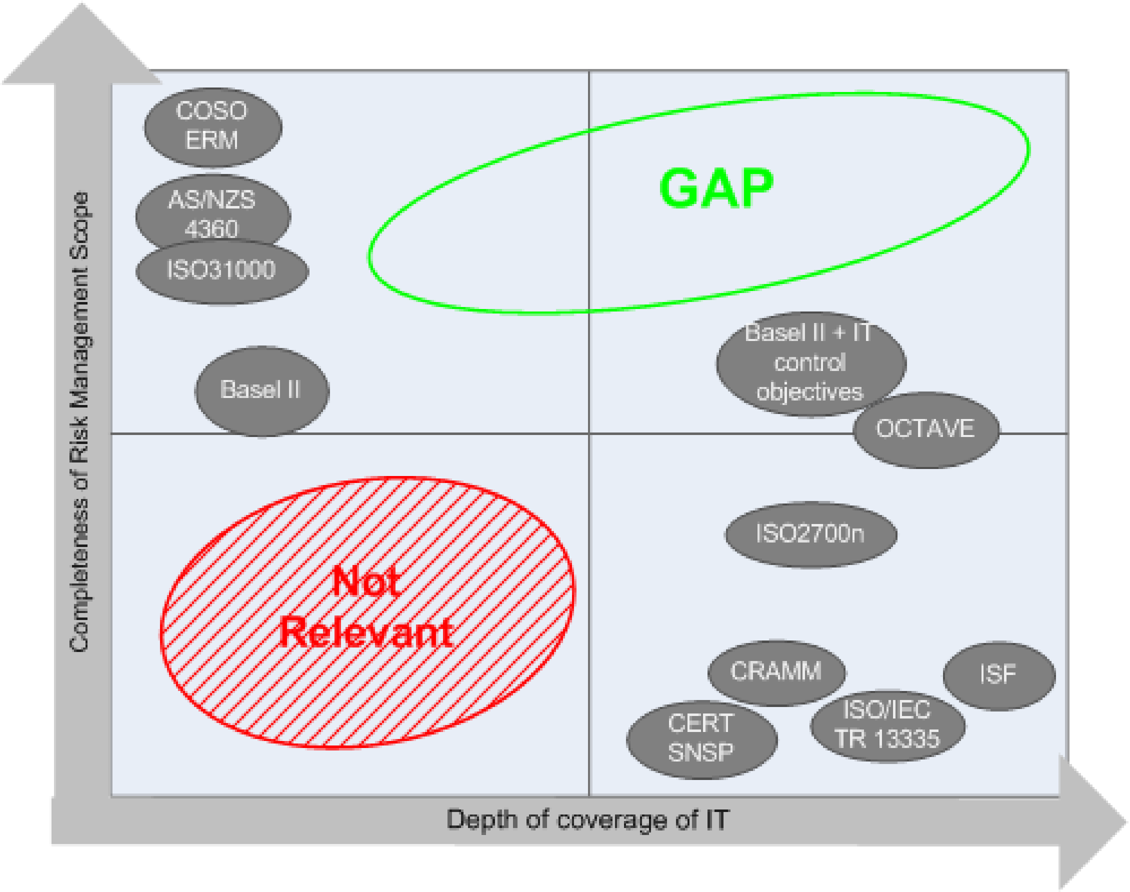
[Actor]
- Internal (staff, contractor)
- External (competitor, outsider, business partner, regulator, market)

Time
- Duration
- Timing of occurrence (critical, non-critical)
- Timing to detect

Risk Scenario

Risk IT vs. other standards

- Standards and frameworks are available, but are either too:
  - Generic enterprise risk management oriented
  - IT security oriented
- No comprehensive IT- related risk framework available (until now)



Benefits & Outcomes

- Accurate view on current and near-future IT-related events
- End-to-end guidance on how to manage IT-related risks
- Understanding of how to capitalize on the investment made in an IT internal control system already in place
- Integration with the overall risk and compliance structures within the enterprise
- Common language to help manage the relationships
- Promotion of risk ownership throughout the organization
- Complete risk profile to better understand risk

COBIT 5

- Brings together the **principles** that
- allow the enterprise to build an effective **governance** and **management** framework based on
- an holistic set of **enablers** that
- optimises **information** and **technology** investment and use for the benefit of stakeholders
- **COBIT 5 is Coming: General Availability 10 April 2012**

COBIT® 5
AN ISACA® FRAMEWORK

Questions?

Thank you for your attention!

Anestis Demopoulos
info@isaca.gr
www.isaca.gr
anestis.demopoulos@gr.ey.com