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

2ο InfoCom Security Conference

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

5 April 2012
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?

► 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

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

- **CISA® Certified Information Systems Auditor®**
  - 70,000+ CISA certified since inception in 1978

- **CISM® Certified Information Security Manager®**
  - 12,000+ CISM certified since inception in 2003

- **CIS® Certified in the Governance of Enterprise IT®**
  - 4,000+ CGEIT certified since inception in 2007

- **CRISC™ Certified in Risk and Information Systems Control**
  - 10,000+ CRISC certified since inception in 2010
What does ISACA do?

Research

BMIS: The Business Model for Information Security
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 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 complements and extends COBIT and Val IT to make a more complete IT governance guidance resource.
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

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

Integrate With ERM

Establish and Maintain a Common Risk View

Make Risk-aware Business Decisions

Business Objectives

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

Collect Data
Maintain Risk Profile

Analyse Risk

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

Manage Risk

Articulate Risk

React to Events

Communication

Risk IT Domains

ISACA
Trust in and value from information systems
Risk IT Process model

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
### Process Model Examples

#### 2. Risk appetite and risk tolerance

<table>
<thead>
<tr>
<th>Event</th>
<th>Enterprise A</th>
<th>Enterprise B</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Event (project delay) with average impact (financial loss &gt; US $100,000) occurring once in a year</td>
<td>Acceptable</td>
<td>Acceptable</td>
</tr>
<tr>
<td>B Event (project delay) with average impact (financial loss &gt; US $100,000) occurring 10 times in a year</td>
<td>Unacceptable</td>
<td>Acceptable</td>
</tr>
<tr>
<td>C Event (security incident) with impact on regulatory compliance (small fines) and public embarrassment (press coverage) occurring once in five years</td>
<td>Acceptable</td>
<td>Unacceptable</td>
</tr>
<tr>
<td>D Event (security incident) with impact on regulatory compliance (large fines) and public embarrassment (extended press coverage) occurring 10 times in a year</td>
<td>Unacceptable</td>
<td>Really Unacceptable</td>
</tr>
<tr>
<td>E Condition (IT architecture obsolescence) preventing future rapid growth through new applications</td>
<td>Really Unacceptable</td>
<td>Unacceptable</td>
</tr>
<tr>
<td>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 $1 million</td>
<td>Really Unacceptable</td>
<td>Unacceptable</td>
</tr>
<tr>
<td>G Event (new application development failure) delaying new business initiatives for two months and hence failing to gain additional revenue of US $250,000</td>
<td>Acceptable</td>
<td>Acceptable</td>
</tr>
</tbody>
</table>
Process Model Examples

5. Risk scenarios

Figure 39—IT Risk Scenario Components

- **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

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

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

- **Time**
  - Duration
  - Timing of occurrence (critical, non-critical)
  - Timing to detect
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
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**
Thank you for your attention!

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