Questioning the need for separate IT risk management frameworks

Nicolas Racz, Edgar Weippl, Andreas Seufert

September 28, 2010
Background and motivation

- Risk management domain is revolutionised through integration efforts:
  - Integration of risk management activities: Enterprise Risk Management (ERM)
  - Integration of risk management with governance and compliance (GRC)
- Authors focus on GRC for information technology (IT GRC)
- Relation of IT-RM and ERM is part of the relation of GRC and IT GRC
IT GRC as a subset of GRC

Corporate Governance

IT Governance

Enterprise Risk Management

IT Risk Management

Compliance

IT Compliance
Status quo in the industry

ERM

IT-RM

IT-RM strategy

ERM strategy
Background and motivation

- Lack of research on the relation of IT-RM and ERM

→ Research question: On a process level, is the use of a separate IT-RM framework justified?

- Approach to gain first insight: comparison of ERM and IT-RM process frameworks
Research methodology

Framework selection

Identification of commonalities

Analysis of references of ERM to IT-RM and vice-versa

Discussion and summary
Framework selection: Enterprise Risk Management


  - Hardly any difference in the process models
Selection of COSO ERM: successor of the widely accepted COSO framework for internal control

The COSO ERM cube:
Framework selection: IT Risk Management

- ISO/IEC 27005:2008 vs ISACA Risk IT
- ISO/IEC standard for information security risk management surpasses IT
- Importance of Risk IT Framework will probably rise due to integration with COBIT 5
- Selection of ISACA Risk IT Framework
Framework selection: ISACA Risk IT Framework

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

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

Articulate Risk

React to Events

Manage Risk

Business Objectives

Communication

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

Analyze Risk

Maintain Risk Profile

Collect Data

Framework selection: ISACA Risk IT Framework
Identification of commonalities

- Mapping of 43 Risk IT processes to 41 previously defined sub-processes of COSO ERM
- All but 7 IT-RM processes could be mapped right away
- Five more were mapped after deeper analysis
  - RG3.1: Gain management buy-in for the IT risk analysis approach (→ internal environment)
  - RG3.2: Approve IT risk analysis (→ risk assessment)
  - RG3.5: Prioritise IT risk response activities (→ risk response)
  - RE2.4: Perform a peer review of IT risk analysis (→ risk assessment)
  - RE3.3: Understand IT capabilities (→ internal environment)
- Two processes remained:
  - RG2.2: Co-ordinate IT risk strategy and business risk strategy
  - RG2.3: Adapt IT risk practices to enterprise risk practices
IT-RM in COSO ERM

- Importance of information systems controls due to “widespread reliance on information systems”
- General controls
  - for IT management, IT infrastructure, security mgmt, software acquisition, development and maintenance
- Application controls
  - ensure completeness, accuracy, and validity of information
- IT risk is hardly ever mentioned, but COSO ERM can act as high-level guidance for IT-RM (Moeller, 2007)
ERM in ISACA Risk IT

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
ERM in ISACA Risk IT

- ERM integration is part of process model

**Process Goal RG2:**
Integrate the IT risk strategy and operations with the business strategic risk decisions that have been made at the enterprise level.

**Key Activities:**
- RG2.1 Establish and maintain accountability for IT risk management.
- RG2.2 Co-ordinate IT risk strategy and business risk strategy.
- RG2.3 Adapt IT risk practices to enterprise risk practices.
- RG2.4 Provide adequate resources for IT risk management.
- RG2.5 Provide independent assurance over IT risk management.
ERM in ISACA Risk IT

- RG2.1, RG2.4 and RG2.5 are governance activities that are not ERM specific
- RG2.2
  - “integrate any IT specifics into one enterprise approach”
  - define the IT department’s role in operational RM
- RG2.3
  - understand business context for IT and ERM activities/methods
  - IT-RM should be enhanced with useful ERM activities
  - meet ERM expectations, and identify methods of other functions
  - close gaps between IT risk and ERM
Conclusion

- ISACA Risk IT demands ERM integration – thus questioning its own purpose
- Differences of ERM and IT-RM seem marginal on high process levels
- Separate IT-RM frameworks may not be justified

- But: design of IT-RM within ERM has yet to be defined
Industry case study

- Three companies of software, healthcare and energy sectors
- Link of ERM and IT-RM normally only made through
  - reporting of few (strategic) IT risks to be used in ERM;
  - rare end-to-end business process audits including IT
- Healthcare company has just started to look for synergies in ERM and IT-RM execution
Discussion

- Criticism:
  - Selection of models is somehow arbitrary
  - Comparison of two models can only provide a hint, not a proof
  - Through focus on processes, structural elements were disregarded

- Your experience/opinion?
Thank you!

In case of questions please contact:

Nicolas Racz

info@grc-resource.com

www.grc-resource.com
Frame of reference for research of integrated GRC

Operations managed and supported through GRC

Governance
- internal policies

Strategy
- integrated holistic organisation-wide

Processes
- risk appetite

Technology
- external regulations

People

Risk Management

Compliance
- ethically correct behaviour
- improved efficiency
- improved effectiveness
Orientation and scoping: IT, business operations, GRC and IT GRC
Future research

- Our research:
  - Focus on IT GRC – creation of an IT GRC management process model and translation to a software reference model
  - COSO ERM is used in the process model to enable ERM/IT-RM integration

- Recommended GRC research topics:
  - IT risk in COBIT 5
  - Creation of an integrated approach to IT risk within ERM