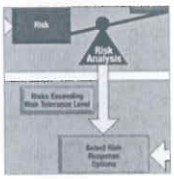
ISACA®
Trust in, and value from, information systems
Switzerland Chapter

Nr. 02 | Juni 2011 | www.isaca.ch
NEWSLETTER



Enterprise Risk
The ISACA research publications are dedicated to helping enterprises manage IT-related risk. **Seite 67**

CRISC
Das neue CRISC-Zertifikat deckt 39 verschiedene Aufgaben in fünf übergeordneten Themenbereichen ab **Seite 70**

ISACA-Training
Aktuelle Aus- und Weiterbildungsmöglichkeiten für Mitglieder und Nicht-Mitglieder **Seite 70**

Enterprise Risk: Identify, Govern and Manage IT Risk[1)]

ISACA's research publications ‚The Risk IT Framework' & ‚Risk IT Practitioner Guide' are dedicated to helping enterprises manage IT-related risk.

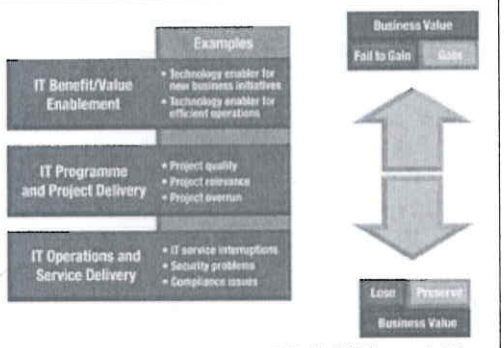
By Urs Fischer, eidg. dipl. Wirtschaftsprüfer, CRISC, CISA, Fischer IT GRC Beratung & Schulung

'IT risk' as defined by the 'Risk IT Framework', is the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise.

IT risk consists of IT-related events that could potentially impact the business. It is characterised by both uncertain frequency and magnitude, and it creates challenges in meeting strategic goals and objectives as well as uncertainty in the pursuit of opportunities. IT risk can be categorised as (refer to Figure 1):

- IT service delivery risk, which is associated with the performance and availability of IT services
- IT solution delivery/benefit realisation risk, which is associated with the contribution of IT to new or improved business solutions, usually in the form of projects and programmes
- IT benefit realisation risk, which is associated with (missed) opportunities to use technology to improve efficiency or effectiveness of business processes, or to use technology as an enabler for new business initiatives – IT risk always exists, whether or not it is detected or recognised by an organisation.

FIGURE 1 – IT RISK CATEGORIES



Source: ISACA, The Risk IT Framework, USA 2009

IT Risk Management Objectives

As risk management is a pervasive and strategic requirement in any enterprise, the main objectives of an IT Risk Management Framework are to enable users to:

- Integrate the management of IT risk into the overall enterprise risk management of the organisation
- Make well-informed decisions about the extent of the risk, the risk appetite and the risk tolerance of the enterprise
- Understand how to respond to the risk

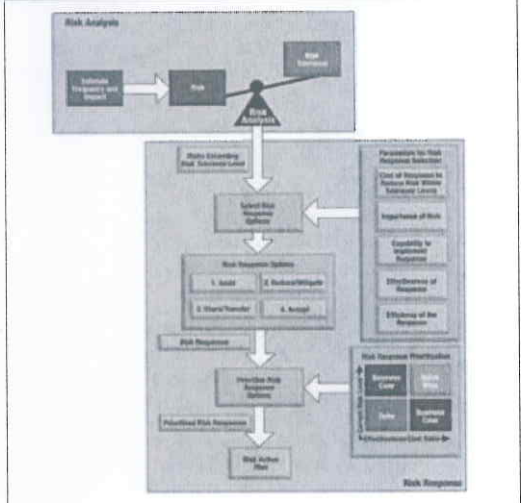
In summary, Risk Management allows an enterprise to make appropriate risk-adjusted decisions.

Benefits

A Risk Management Framework addresses many issues enterprises face today, notably their need for:

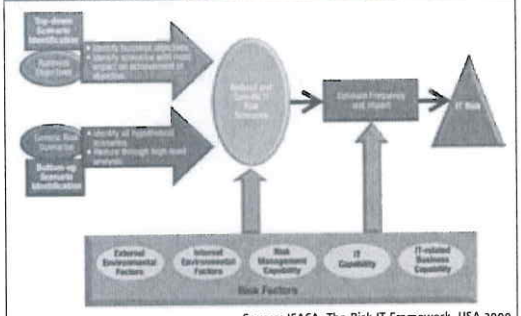
- An accurate view of current and near-future IT-related risks throughout the extended enterprise and the success with which the enterprise is addressing IT risk
- End-to-end guidance on how to manage IT-related risks, beyond both purely technical control measures and security
- Understanding of how to capitalise on an investment made in an IT internal control system already in place to manage IT-related risk
- When assessing and managing IT risk, integration with the overall risk and compliance structures within the enterprise
- A common framework/language to help manage the relationship amongst executive decision makers (board/senior management), the chief information officer (CIO) and enterprise risk management, or between auditors and management
- Promotion of risk responsibility and its acceptance throughout the enterprise
- A complete risk profile to better understand risk, so as to better utilise company resources

FIGURE 2 – RISK ANALYSIS AND RISK RESPONSE OVERVIEW



Source: ISACA, The Risk IT Framework, USA 2009

FIGURE 3 – IT RISK SCENARIO DEVELOPMENT



Source: ISACA, The Risk IT Framework, USA 2009

IT Risk Management Principles

Guiding principles for effective management of IT risk should be based on generally accepted enterprise risk management principles (COSO, ISO31000 etc.), which should be applied to the domain of IT. ISACA's Risk IT process model is designed and structured to enable enterprises to apply the principles in practice and to benchmark their performance. The principles are split in a governance part and a management part:

- Effective enterprise governance of IT risk:
  > Always connects to business objectives
  > Aligns the management of IT-related business risk with overall enterprise risk management
  > Balances the costs and benefits of managing risk
- Effective management of IT risk:
  > Promotes fair and open communication of IT risk
  > Establishes the right tone from the top while defining and enforcing personal accountability for operating within acceptable and well-defined tolerance levels
  > Is a continuous process and part of daily activities

IT Scenario Analysis in Enterprise Risk Management

One of the challenges for IT risk management is to identify the important and relevant risks that can possibly occur with IT or in relation to IT, given the pervasive presence of IT and the business dependence on it. One of the techniques to overcome this challenge is to develop and use risk scenarios. Scenarios are a powerful tool in a risk manager's armory–they help professionals ask the right questions and prepare for the unexpected. Scenario analysis has become a 'new' and best practice in enterprise risk management (ERM). Scenario analysis is also a centrepiece of ISACA's Risk IT framework.

It is a core approach to bring realism, insight, organisational engagement, improved analysis and structure to the complex matter of IT risk. Once these scenarios are developed, they are used during the risk analysis, where frequency of the scenario actually happening and business impacts are estimated. This is shown in Figure 2.

Risk scenario analysis is a technique to make IT risk more concrete and tangible and to allow for proper risk analysis and assessment . It is a core approach to bring realism, insight, organizational engagement, improved analysis and structure to the complex matter of IT risk. The risk scenario is structured as follows:

- Description of the scenario analysis flow, showing the importance and relevance of risk scenarios
- Discussion of risk factors that need to be taken into account when creating and assessing risk scenarios
- Explanation of the different components in a risk scenario
- Guidelines on how to construct a set of relevant risk scenarios

Once these scenarios are developed, they are used during the risk analysis, where frequency of the scenario occurring and business impacts are estimated.[2)]

Figure 3 (left) shows that IT risk scenarios can be derived by two different ways:

- A Top-Down Approach, where one starts from the overall business objectives and

performs an analysis of the most relevant and probable IT risk scenarios impacting the business objectives
- A Bottom-Up Approach, where a list of generic scenarios is used to define a set of more concrete and customized scenarios

The approaches are complementary and should be used simultaneously. Indeed, risk scenarios must be relevant and linked to real business risk. On the other hand, using a set of example generic risk scenarios helps to ensure that no risks are overlooked and provides a more comprehensive and complete view of IT risk.

The following is a practical approach that proved very helpful in developing a set of relevant and important risk scenarios:

1. Use a list of example generic risk scenarios to define a manageable set of concrete risk scenarios for the organization
2. Perform a validation against the business objectives of the organization
3. Refine the selected scenarios based on the validation; categorize them to a level in line with the criticality of the organization
4. Reduce the number of scenarios to a manageable set
5. Keep all risks in a list so they can be re-evaluated in the next iteration and included for detailed analysis if they have become relevant at that time
6. Include in the scenarios an unspecified event; how to address an incident not covered by other scenarios

An IT risk scenario is a description of an IT-related event that can lead to a business impact, when and if it should occur. For risk scenarios to be complete and usable for risk analysis purposes, they should contain the components as shown in Figure 4.

Scenario Analysis is not rocket science. But why don't organizations use it more often and routinely? Keep in mind, that scenarios are in fact harder to develop as it seems. A good one takes time to build, and so a whole set takes a large investment of time and energy.

Conclusion

The Risk IT Framework and The Risk IT Practitioner Guide are designed to allow business managers to identify and assess IT-related business risks and manage them effectively. It provides the missing link between enterprise risk management (ERM) and IT risk management and control, fitting in the overall IT Governance Framework of ISACA, and building upon all existing risk-related components within the current frameworks of CobiT and Val IT.

FIGURE 4 – IT RISK SCENARIO COMPONENTS

Source: ISACA, The Risk IT Framework, USA 2009

More information

For more information on Risk IT, please visit www.isaca.org/riskit. The publications are available in the ISACA Bookstore, www.isaca.org/bookstore. The Risk IT Framework is available as a complimentary PDF for ISACA members and nonmembers at www.isaca.org/downloads. The Risk IT Practitioner Guide and tool kit are available as complimentary downloads for ISACA members at www.isaca.org/downloads.

1) Based on ISACA's research publications ‚Risk IT Framework' and ‚Risk IT Practitioner Guide, published 2009

2) Risk Analysis and Risk Assessment – Risk Analysis is the actual estimation of frequency and magnitude/impact of a risk scenario. Risk Assessment is a slightly broader term, including the preliminary and ancillary activities around risk analysis, i.e., identification of detailed risk scenarios and definition of responses.

DER AUTOR

Urs Fischer, eidg. dipl. Wirtschaftsprüfer, CRISC, CISA ist unabhängiger Berater und Anbieter von Schulungen im Bereich IT Governance, Risiko Management und Compliance. Als Leiter IT Governance & Risiko Management bei einer grossen Schweizer Lebensversicherung implementierte er ein effektives und effizientes IT Risiko Management- und Kontroll-Framework. Seit 1989 arbeitet er im Bereich IT Governance, Revision und Sicherheit und hat während dieser Zeit umfassende Erfahrung in IT Governance, Risiko Management, Internen Kontroll-Systemen und Informationssicherheit sammeln können.

Urs Fischer ist sehr aktiv in der IT Kontroll- und Sicherheits-Gemeinde. Er war wesentlich beteiligt an der Entwicklung von ISACA's Kontroll-Framework COBIT 4.1 und ist auch in die Weiterentwicklung von COBIT5 involviert. Als Vorsitzender von ISACA's Risk IT Taskforce war er federführend in der Entwicklung des ‚Risk IT Frameworks' und des ‚Risk IT Practitioner Guide' involviert. Als Dank für seine Beiträge zugunsten des Berufsstandes wurde ihm 2010 der ‚John W. Lainhart IV – Common Body of Knowledge Award' verliehen.

IMPRESSUM ISACA NEWS

Herausgeber, Redaktion:	ISACA Switzerland Chapter
Adresse:	Kurssekretariat, c/o ITACS Training AG, Stampfenbachstr. 40, 8006 Zürich
Erscheinungsweise:	4x jährlich in Swiss IT Magazine
Mitgliedschaft:	Wir begrüssen alle, die Interesse an Audit, Governance und Sicherheit von Informationssystemen haben. Es ist nicht notwendig, dass Sie Sicherheitsspezialist oder Revisor sind, um bei uns Mitglied zu werden. Weitere Informationen finden Sie unter www.isaca.ch
Copyright:	© Switzerland Chapter der ISACA

Information des Verbandes

CRISC – riesige Nachfrage nach neuem Zertifikat

Vor knapp einem Jahr stellte ISACA das neue Personen-Zertifikat im Bereich Risikomanagement und IKS im IT-Umfeld CRISC (Certified in Risk Management and Internal Control) vor. Bereits sind fast 9000 Personen zertifiziert – was wesentlich mehr ist als bei der im Jahr 2008 gestarteten CGEIT-Zertifizierung.

Das neue CRISC-Zertifikat deckt 39 verschiedene Aufgaben in fünf übergeordneten Themenbereichen ab: Es geht einerseits um die Identifikation, Einschätzung und Bewertung von Risiken sowie um deren Management und Überwachung. Anderseits geht es um Design und Implementation von IT-Kontrollen sowie deren Überwachung und Unterhalt. In dieser Kombination deckt das neue CRISC-Berufsbild und die entsprechende Zertifizierung ein offensichtliches Markt-Bedürfnis ab.

Interessant ist der Teilaspekt Risikoüberwachung: Zwar gibt es in allen im IT-Umfeld gebräuchlichen Risikomanagement-Methoden wie ISO31000, ISO27005, Risk IT oder dem in der Regel unternehmensweit eingesetzten COSO ERM eine Phase, welche sich Risiko-Monitoring nennt – detaillierte Angaben, was das denn alles beinhaltet und wie so etwas in der Praxis umzusetzen ist, fehlen. Alleine für diesen Teilbereich definiert CRISC vier Aufgaben: die Sammlung und Validierung von Risikoschlüsselindikatoren über deren Überwachung, die Berichterstattung an relevante Stakeholder, die Durchführung unabhängiger Risikobewertungen und Reviews sowie die Überwachung von Compliance-Risiken.

Bereits im ersten Semester hat das ISACA Switzerland Chapter einen berufsbegleitenden Kurs durchgeführt (13 Kurstage verteilt über 4–5 Monate). Der CRISC-Kurs richtet sich an alle Personen, die sich mit unterschiedlichsten Risikomanagementfragen und Frameworks oder mit dem Design, der Implementation, der Überwachung und Wartung von Sicherheitsmassnahmen und anderen Kontrollen beschäftigen – also Risikomanager und Sicherheitsbeauftragte innerhalb und ausserhalb der IT, Compliance-Officer, IKS-Verantwortliche, erfahrene Informatikrevisoren, IT-Anwendungsentwickler oder Projektcontroller. Der nächste Kurs startet anfangs Juli; ein Einstieg ist bis Mitte August möglich.

Der durch ITACS Training AG im Auftrag des ISACA Switzerland Chapter durchgeführte Kurs vermittelt und vertieft theoretisches wie praktisches Fachwissen im breiten Feld von Risikomanagement und internen Kontrollen, bereitet aber auch intensiv auf die von ISACA organisierte CRISC-Prüfung vor.

WEITERE INFORMATIONEN

Weitere Details zum CRISC-Zertifikat und zur entsprechenden Ausbildung finden Sie auf www.isaca.ch

ISACA-TRAINING

Datum	Code	Hauptthema – Kurstitel
27.-29.6.11		**Risk IT - Enterprise RM**
30.6.2011		**COBIT V4.1 Overview IT Governance**
8.9.2011	RM-KK	**Risikomanagement-Methoden wirksam anwenden** Identifikation, Bewertung und Management von (IT-) Risiken mit unterschiedlichsten Methoden wirksam implementieren
9.9.2011	PER-KK	**Effizientes Messen der Performance** Guten Leistungsindikatoren effizient erheben
13.-14.9.11	LAB-WAB	**Web Applications: Basics**
15.-16.9.11	LAB-WAA	**Web 2.0 – Web Applications: Advanced**
20.9.2011	OUT-KMU	**Risiken, Überwachung & Prüfung von Outsourcing-Providern** Bekommen Sie Ihr Outsourcing in Griff – speziell auch für KMUs
26.9.2011	ISMS-KK	**ISMS gemäss ISO 2700x implementieren und verbessern** Ein ISMS in 30 effizienten Schritten implementieren oder verbessern
3.10.2011	RIM-KK	**Risikoprüfungen und kontinuierliche Risikoüberwachungen** Wirksame Überwachung von Risiken
4.10.2011	IKS-KK	**Design, Betrieb, Überwachung & Unterhalt von Kontrollen** Effizientes Design & wirksame Überprüfung von anwendungsabhängigen Kontrollen
7.10.2011	JAVA-KK	**JAVA Enterprise für IT-Revisoren und IT-Sicherheitsbeauftragte** Professionelle Prüfung von Java-basierten Anwendungen
20.-21.10.11	QM-IR	**Qualitätsmanagement in der Internen (IT-) Revision** Bringen Sie Ihre eigene Revisionstätigkeit auf ein ausreichendes Qualitätsniveau !
22.-26.8.11	AVA-IR	**Avaloq-Einführung für (IT-) Revisoren und (IT-) Sicherheitsbeauftragte** Avaloq verstehen als Grundlage für effiziente Prüfungen
26.10.2011	GL-SAP	**Grundlagen zur Prüfung von SAP-Systemlandschaften** Fachkompetenz für die Prüfung & Überwachung von SAP-Systemen erwerben
27.-28.10.11	FIBU-SAP	**Prüfung der Finanzbuchhaltung (FI) in SAP-Systemen**
8.-10.11.11	AVA-REP	**Avaloq-Reporterstellung für Revisoren/Sicherheitsbeauftragte** Effiziente Erstellung von verlässlichen Reports aus dem Avaloq Banking System
10.11.2011	SM-EY	**Audit & Control of Social Media**
21.11.2011	AWA-KK	**Erfolgreiche Awareness-Kampagnen** Systematische Planung/Durchführungvon Aktivitäten und Kampagnen für anhaltende Awareness (mit zahlreichen Beispielen/Erkenntnissen aus der Praxis)

Das gesamte Trainingsangebot mit näheren Informationen finden Sie online unter www.isaca.ch