

## TrendTalk

# ISO 27xxx

## Chancen, Grenzen und Erfahrungen in der Praxis

- **Überblick und Erfahrungen mit der Normengruppe ISO/IEC 27xxx**
- **Herausforderungen bei der Einführung eines ISMS nach ISO/IEC 27001:2005**
- **ISO 27001: Bulle oder Bär**

**Dienstag, 28. April 2009**  
**17.00–20.00 Uhr**

**Oesterreichische Kontrollbank,  
Reitersaal**  
**1010 Wien, Strauchgasse 1–3**

**Referenten:**

**Armin Plank** (T-Systems)

**Johannes Puchinger** (Österreichische  
Lotterien)

**Gunther Reimoser** (Ernst & Young)

**Gernot Schmied** (Ziviltechnikerbüro  
IKTech)

**Moderation:**

**Gunther Reimoser** (Ernst & Young)

## Aufbau eines Informationssicherheits-Managements: Überblick und Erfahrungen mit der Normengruppe von ISO/IEC 27xxx

Dieser Vortrag bietet eine Einführung in die Landkarte und Anwendungsbereiche der Normengruppe ISO 27xxx, deren Nützlichkeit und Grenzen sowie Empfehlungen für den Einsatz in der Implementierung eines Management-Systems und der internen IT-Revision.



**Gernot Schmied**  
(Ziviltechnikerbüro  
IKTech)

Aus der Sichtweise des Prüfers und Umsetzungsbegleiters werden Empfehlungen zur Einführungsplanung, Herangehensweise, zu Hilfsmitteln und Frameworks bis hin zum Betrieb gegeben. Erklärtes Ziel des Vortrags ist, einen Eindruck über den zeitlichen Aufwand und die Vorteile einer schlanken, durchdachten und strukturierten Vorgehensweise zu vermitteln, dies im Kontrast zu unreflektierter »Normenhörigkeit« und Verzettelung in Details oder Checklisten.

## Herausforderungen bei der Einführung eines ISMS nach ISO/IEC 27001:2005

Die Österreichischen Lotterien durchliefen im Rahmen der Einführung des Spiels Euromillions eine Zertifizierung nach den Vorgaben gemäß der World Lottery Association. Da der World Lottery Standard weiterentwickelt wurde sind die Österreichischen Lotterien seit 2007 auch ISO/IEC 27001:2005 zertifiziert.

Herr Puchinger gibt einen Erfahrungsbericht über Herausforderungen bei der Zertifizierung. Dabei stehen weniger die Control Objectives und Controls des Anhang A im Vordergrund, sondern vielmehr der Bereich des Aufbaus eines funktionierenden Managementsystems.

Herr Johannes Puchinger ist seit 1995 bei den Österreichischen Lotterien in der Internen Revision tätig. Er übernahm 1999 den Bereich Security und begleitete die Zertifizierungen.



**Johannes Puchinger**  
(Österreichische  
Lotterien)

## ISO 27001: Bulle oder Bär

Mit einer weltumspannenden Infrastruktur aus Rechenzentren und Netzen betreibt T-Systems die Informations- und Kommunikationstechnik (engl. kurz ICT) für multinationale Konzerne und öffentliche Institutionen. Die Zielsetzung des Information Security Management ist, den Kunden des Unternehmens transparent nachzuweisen, dass die Sicherheit ihrer Kundendaten weltweit gewährleistet wird. Rückblickend auf achtjährige Konzern-Zertifizierungshistorie spannt Armin Plank, Senior Security Manager bei der T-Systems International einen Bogen über Nutzen, Kosten und Risiken der ISO-27001-Zertifizierung.

- Welchen Gewinn können lernende Organisationen aus einer ISO-27001-Zertifizierung ziehen?



**Armin Plank**  
(T-Systems Austria  
GesmbH)

## Agenda

- 16.30** **Registration**
- 17.00** **Begrüßung und Einführung**  
Gunther Reimoser (Ernst & Young)
- 17.10** **Aufbau eines Informationssicherheits-Managements: Überblick und Erfahrungen mit der Normengruppe ISO/IEC 27xxx**  
Gernot Schmied (Ziviltechnikerbüro IKTech)
- 18.00** **Herausforderungen bei der Einführung eines ISMS nach ISO/IEC 27001:2005**  
Johannes Puchinger (Österreichische Lotterien)
- 18.20** **ISO 27001: Bulle oder Bär**  
Armin Plank (T-Systems)
- 18.40** **Schlussdiskussion**
- 19.00** **Come-together**
- 20.00** **Ende der Veranstaltung**

- Welchen praxisrelevanten Mehrwert hat ein Kunde, wenn er auf zertifizierte Service-Provider zurückgreift?
- Welche Risiken und Chancen bieten multiple Zertifizierungen (z. B. ISO 9001 / 20000 / 27001 / 14001, SAS70, BS25999, ...)?
- Ist die EBIT-Vernichtung/Sicherung einer ISO-27001-Zertifizierung messbar?

# Wer ist die ISACA Austria?



Die ISACA Austria wurde 1998 gegründet und ist das lokale Chapter der ISACA International. Der Verein mit über 230 Mitgliedern in Österreich hat sich die Förderung und Entwicklung der Bereiche:

- Prüfung von IT-Systemen und IT-Prozessen
- IT-Security
- Begleitende Kontrolle von IT-Systemen und IT-Prozessen
- IT-Governance – Organisation, Steuerung und Kontrolle der IT durch die Unternehmensführung

als Ziel gesetzt und verfolgt dies durch:

- Erarbeitung von Grundsätzen und Methoden für die Bereiche IT-Prüfung, IT-Sicherheit, begleitende Kontrolle von IT-Systemen und -Prozessen und IT-Governance, sowie deren

ständige Anpassung an die betriebswirtschaftlichen, organisatorischen und technischen Entwicklungen

- Diesbezügliche wissenschaftliche und praktische Weiterbildung von Mitgliedern
- Informationsweitergabe und -veranstaltungen
- Intensivierung der Zusammenarbeit zwischen Wissenschaft und Praxis
- Förderungen von wissenschaftlichen und anderen fachorientierten Arbeiten diesen Gebieten
- Anbahnung und Aufrechterhaltung von Beziehungen
  - zu ähnlichen Institutionen des Auslandes, insbesondere zu den ISACA-Organisationen in den verschiedenen Ländern und der als Dachorganisation fungierenden ISACA-Organisation in den USA
  - zu den für angeführte Bereiche relevanten Berufsgruppen

Die ISACA International führt zahlreiche Projekte von globalem Charakter und großer Bedeutung für den IT-Audit-, IT-Governance- und IT-Security-Bereich durch und ist mit seinen weltweit über 80.000 Mitgliedern Vorreiter bei der Entwicklung von IT-Audit Standards.

Die Hauptprodukte der ISACA sind neben CobiT die Zertifizierungen CISA, CISM und CGEIT.

IT-Governance, die aktive Steuerung der IT durch die Unternehmensleitung mittels Vorgaben, Kontrollen und Messgrößen stellt eine große Herausforderung und auch Chance sowohl für die IT-Verantwortlichen als auch Geschäftsführer dar. Weitere Informationen zum Thema gibt es auf den Pages der ISACA Austria ([www.isaca.at](http://www.isaca.at)) und des IT Governance Institute ([www.itgi.org](http://www.itgi.org)), einer Schwesterorganisation der ISACA.

An  
CON•ECT Eventmanagement  
Kaiserstraße 14/2  
1070 Wien  
  
Tel.: +43 / 1 / 522 36 36-37  
Fax: +43 / 1 / 522 36 36-10  
E-Mail: [registration@conect.at](mailto:registration@conect.at)  
<http://www.conect.at>

**CON•ECT**  
EVENTMANAGEMENT

## Anmeldung

- Ich melde mich kostenfrei zum ISACA-TrendTalk »ISO 27xxx« am 28. April 2009 an.
- Ich bin an Informationen über die ISACA interessiert.
- Ich möchte in Zukunft weiter Veranstaltungsprogramme per E-Mail oder Post übermittelt bekommen.

**ACHTUNG: Beschränkte Teilnehmerzahl! Melden Sie sich heute noch an. Anmeldeschluss: 27. April 2009**

ISACA-Mitglieder können sich für die Teilnahme 3 CPEs anrechnen lassen.

Jedes ISACA-Mitglied darf einen Gast mitnehmen.

Anmeldungen bitte zu faxen unter: (01) 522 36 36-10 oder per E-Mail an [registration@conect.at](mailto:registration@conect.at) bis

Firma:	
Titel:	
Vorname:	
Nachname:	
Funktion:	
Straße:	
PLZ:	
Ort:	
Telefon:	
Fax:	
E-Mail:	