

## Seminarort

CCG-Zentrum, Technologiepark Argelsrieder Feld 11,  
D-82234 Weßling-Oberpaffenhofen

Eine Lageskizze sowie Hinweise für die Anreise und Übernachtung  
schicken wir Ihnen mit der Bestätigung der Anmeldung zu.

## Gebühr

EUR 1.325,-

Die CCG ist als gemeinnützig anerkannt und von der USt befreit.

Mitglieder der CCG erhalten 10% Rabatt, Studenten bei Vorlage des  
Studentenausweises 75%. Bei Anmeldung mehrerer Mitarbeiter einer  
Firma / Dienststelle zum gleichen Seminar erhält jeder Teilnehmer 10%.

Die Rabatte sind nicht miteinander kombinierbar.

Bitte zahlen Sie bargeldlos nach Erhalt der Rechnung.

## Anmeldungen

Bitte möglichst bis 14 Tage vor Seminarbeginn an:

Carl-Cranz-Gesellschaft e.V., Postfach 11 12, D-82230 Weßling  
Tel. +49 (0) 8153 / 88 11 98 -12, Fax -19, E-Mail: [anmelden@ccg-ev.de](mailto:anmelden@ccg-ev.de)  
Internet: [www.ccg-ev.de](http://www.ccg-ev.de)

Die Anmeldungen werden schriftlich bestätigt.

## Weitere Informationen zum Inhalt

K.-D. Wolfenstetter, Deutsche Telekom AG  
Tel. +49 (0) 30 / 8353-58419  
E-Mail: [k.wolfenstetter@telekom.de](mailto:k.wolfenstetter@telekom.de)

## Stornierung

Bei Stornierung mündlich oder schriftlich bestätigter Anmeldungen wird  
eine Bearbeitungsgebühr von EUR 25,- berechnet. Bei Stornierungen,  
die später als 7 Tage vor Seminarbeginn eingehen, werden 25% der  
Gebühr, bei Nichterscheinen die volle Gebühr in Rechnung gestellt. Die  
Vertretung eines angemeldeten Teilnehmers ist möglich.

## Ausfall von Seminaren oder Dozenten

Die CCG behält sich vor, bei zu geringer Teilnehmerzahl oder aus  
anderen triftigen Gründen ein Seminar bis 10 Tage vor Beginn abzusa-  
gen. Sie behält sich weiter vor, entgegen der Ankündigung im Pro-  
gramm auch kurzfristig einen Dozenten und evtl. auch dessen Thema  
zu ersetzen. Ein Schadensersatzanspruch bleibt ausgeschlossen.

## Teilnehmer

Sicherheits- und Datenschutzbeauftragte aus Wirtschaft, Verwaltung und  
Behörden, Mitarbeiter und Verantwortliche für Datenverarbeitung und  
Kommunikation, interne / externe Auditoren, Revisoren, Sicherheits- und  
Unternehmensberater, Risk Manager

## Seminarinhalte

Mit der bereits in wesentlichen Teilen veröffentlichten ISO 27000-Reihe  
liegen wichtige internationale Standards für das Management der Informa-  
tionssicherheit vor. Das praxisorientierte Vorgehensmodell ist anwendbar  
auf Unternehmen und Behörden aller Größen, unterschiedlich hohe  
Sicherheitsansprüche und einfache wie komplexe Anwendungen.

Das Seminar führt Schritt für Schritt in die wesentlichen Begriffe, Metho-  
den und Praktiken ein und stellt exemplarisch die Maßnahmenauswahl für  
wichtige Anwendungen vor. Vertiefungsthemen sind: Dokumentation und  
Aufzeichnungen, Asset Management, Risikoanalysen, Notfallmanagement  
und Wirksamkeitsmessungen.

Mit den vorgestellten Methoden ist es u. a. möglich, viele gesetzliche und  
andere Anforderungen nach einem „Internen Kontrollsystem“ abzudecken.  
Der Standard ermöglicht außerdem eine international anerkannte Zertifi-  
zierung des Sicherheitsmanagements.

## Vortragende

H. Kersten	Dr.	T-Systems GEI GmbH, Bonn
G. Klett	Dr.	BASF IT Services GmbH (ehem.), Ludwigshafen
K.-D. Wolfenstetter	Dipl.-Math.	Deutsche Telekom AG, Labora- tories, Berlin

## Unterlagen

Jeder Teilnehmer erhält die Vortragsunterlagen.  
Die Kosten dafür sind in der Gebühr enthalten.

## Seminar IN 2.12

# Nutzen und Anwendung der ISO 27000-Reihe beim Sicherheits- und Notfallmanagement in der IT

30. November – 2. Dezember 2010  
Oberpaffenhofen bei München

## Wissenschaftliche Leitung

Dipl.-Math. K.-D. Wolfenstetter  
Deutsche Telekom AG, Laboratories, Berlin

## Seminarprogramm

---

**Dienstag, 30.11.2010**  
**09.00 – 16.30 Uhr**

---

- |                     |   |
|---------------------|---|
| 09.00 – 09.15       | Begrüßung, Einführung, Organisation   |
| 09.15 – 10.00       | <b>Einführung in die Normenreihe ISO 27000</b>  |
| 10.30 – 12.00       | <ul style="list-style-type: none"> <li>Nationale Vorläufer der ISO-Reihe</li> <li>Die ISO 2700x-Reihe im Überblick</li> <li>Querverbindungen zu ITIL</li> </ul>                               |
| 13.00 – 14.30       |   |
| 15.00 – 16.30       |   |
| K.-D. Wolfenstetter | <b>Grundbegriffe der Sicherheit nach ISO 27000</b>  |
|                     | <ul style="list-style-type: none"> <li>Ganzheitliche Betrachtungsweise</li> <li>Wichtige Basics</li> <li>Risikoansatz nach ISO 27005</li> <li>Wirksamkeitsmessungen nach ISO 27004</li> </ul> |

**Mittwoch, 1.12.2010**  
**08.30 – 16.00 Uhr**

---

- |               |   |
|---------------|---|
| 08.30 – 10.00 | <b>Der Sicherheitsprozess nach ISO 27001 an Beispielen</b>  |
| 10.30 – 12.00 |   |
| 13.00 – 14.00 | <ul style="list-style-type: none"> <li>Scope und Assets</li> <li>Risikoanalyse und -bewertung</li> <li>Sicherheitsmaßnahmen und SoA</li> <li>Restrisikobehandlungsplan</li> </ul> |
| 14.30 – 16.00 |   |
| H. Kersten    | <b>Optionale Einbindung des IT-Grundschutzes</b>  |
|               | <ul style="list-style-type: none"> <li>Gefährdungs- und Maßnahmenkataloge</li> <li>Ergänzende Analysen</li> </ul>   |
|               | <b>Hilfsmittel (Tools und Charts)</b>   |
|               | <b>Interne Audits nach ISO 27006</b>  |
| ab ca. 17.30  | <b>Social Event</b>   |
|               | Führung durch die Münchener Altstadt (optional)   |

**Donnerstag, 2.12.2010**  
**08.30 – 16.00 Uhr**

---

- |               |  |
|---------------|--|
| 08.30 – 10.00 | <b>Maßnahmen gemäß ISO 27001 (Anhang) und ISO 27002</b>  |
| 10.30 – 12.00 |  |
| 13.00 – 14.00 | Ausgewählte Maßnahmenbereiche: <ul style="list-style-type: none"> <li>Physische Sicherheit; Gebäude, Infrastruktur, Sicherheitszonen</li> <li>Zugriffskontrolle</li> <li>Sichere Mobile Datenverarbeitung</li> <li>Sicherheit von Smartphones</li> <li>Compliance; Beachtung gesetzlicher Vorschriften und anderer Regularien</li> <li>Business Continuity Management / Notfallmanagement</li> </ul> |
| 14.30 – 16.00 |  |
| G. Klett      | <b>Optimale Vorbereitung auf eine Zertifizierung</b>   |

### Weiteres Seminar zum Themenbereich

---

- „Die IEC 61508 – Schlüsselstandard für die Entwicklung und Prüfung sicherheitsrelevanter technischer Steuerungen und deren Software“, 7.–9.12.2010 (Code IN 2.11)