

12



### 3. DIIR-Anti-Fraud- Management-Tagung

#### Fraud- und Compliance- Risiken in Unternehmen

- Prävention und wirksames Anti-Fraudmanagement
- Compliance und Fraud-Krisen-Management sowie Response
- CyberCrime und Hackerangriff live demonstriert

01. und 02. März 2012  
Kassel

Mit fachlicher Unterstützung  
der ASW – Arbeitsgemeinschaft für  
Sicherheit der Wirtschaft e.V.

Unter maßgeblicher Beteiligung  
des DIIR-Arbeitskreises „Abwehr  
wirtschaftskrimineller Handlungen  
in Unternehmen“

# DIIR

Deutsches Institut für  
Interne Revision e.V.

01. März 2012

# Programm

08.00 – 09.00 Uhr

**Begrüßungskaffee**

Registrierung und Ausgabe der Tagungsunterlagen

09.00 – 09.15 Uhr

**Eröffnung**

**Horst POHL**

Leitung Group Audit

Commerzbank AG, Frankfurt am Main

Stellv. Sprecher des Vorstands des  
DIIR – Deutsches Institut für Interne  
Revision e.V.

09.15 – 10.00 Uhr

**Grundsatzreferat 1**

Interne Revision, Compliance & Security –  
Partner im Unternehmensschutz?!

**Wolf-Rüdiger MORITZ**

Vice President Business Continuity  
Infineon Technologies AG

10.00 – 10.30 Uhr

**Kaffeepause, Networking**

10.30 – 12.00 Uhr

**Fachsitzung 1**

**Instrumente eines wirksamen Anti-Fraud-Management  
Systems**

- Grundvoraussetzung für ein wirksames Anti-Fraud-Management ist eine klare Organisationsstruktur mit entsprechender Kapazitätszuweisung („Qualität hat ihren Preis“) inkl. eindeutiger Handlungsvorgaben und Kompetenzen.
- Die Struktur von Anti-Fraud-Management-Maßnahmen basiert auf den 3 Säulen Prävention, Erkennung und Ermittlung (Prevention, Detection, Investigation) und beinhaltet u. a. die Themen
  - Risiko-/Gefährdungsanalyse durchführen und weiterentwickeln
  - Hinweisgebersystem installieren und nutzen
  - Ethikgrundsätze gestalten und leben
  - Schulung und Sensibilisierung der Mitarbeiter erfolgreich durchführen
  - Internes Kontrollsystem optimieren und Kontrollkultur fördern
  - Kommunikation mit Fachbereichen incl. Zusammenarbeit mit Interner Revision und Risikocontrolling
  - Researchhandlungen standardisieren und Informationen sammeln
- Die Fachsitzung wird neben einem Erfahrungsbericht über die Implementierung und die Entwicklung des Anti-Fraud-Managements unter Einbeziehung der internen Revision in der Norddeutschen Landesbank eine Standortbeschreibung inkl. eines Ausblicks auf anstehende Weiterentwicklungen geben (Lessons learned).

**Referentin:**

**Bianca HAUSMANN**

Geldwäsche/Fraud/Compliance

NORD/LB Norddeutsche Landesbank  
Girozentrale, Hannover

**Moderator:**

**Frank MÜLLER**

Leiter Revision Privatkunden

NORD/LB Norddeutsche Landesbank  
Girozentrale, Braunschweig

Mitglied des DIIR-Arbeitskreises

„Abwehr wirtschaftskrimineller  
Handlungen in Unternehmen“

# Programm

10.30 – 12.00 Uhr

## Fachsitzung 2

### Dicke Bretter bohren

#### Vermögensaufspürung und Vermögensrückgewinnung – Asset Tracing

- Trau schau wem: Informationsbeschaffung über das Internet, die Täter lassen grüßen
- Schreib mal wieder: Nutzung geldwäscherechtlicher Vorschriften zur Sicherung der Ansprüche von Opfern
- Die Polizei, dein Freund und Helfer: Für und Wider der Einschaltung von Strafverfolgungsbehörden
- Das gibt's doch gar nicht: Anfechtungen durch den Insolvenzverwalter.

#### Referent:

##### RA Bernd KLOSE, CFE

Fachanwalt für Insolvenzrecht  
kkforensic GbR, Friedrichsdorf/Ts  
Vorstand des German Chapter of  
ACFE e. V.

#### Moderator:

##### Mag. Dr.

##### Matthias KOPETZKY, CIA, CPA, CFE, SV

Geschäftsführer  
Business Valuation GmbH, Wien  
Mitglied des DIIR-Arbeitskreises  
„Abwehr wirtschaftskrimineller  
Handlungen in Unternehmen“  
Mitglied des Vorstands im IIA Austria  
und Leiter des Arbeitskreises  
„Wirtschaftskriminalität“ des IIA Austria

10.30 – 12.00 Uhr

## Fachsitzung 3

### Live Hacking – Hackerangriffe live demonstriert

Anonymus, LulzSec & Co lassen grüßen. Täglich erfahren wir von neuen Sicherheitslücken und gelungenen Hackerangriffen: Doch „live“ erlebt man sie in aller Regel nicht. Während dieser Live-Demo wird eine Vielzahl echter Hackertechniken demonstriert, erläutert und diskutiert. Insbesondere finden auch Angriffe auf Systeme im Internet statt. Schauen Sie einem Profi über die Schulter und erleben Sie, wie Sicherheitsbarrieren in Ihrem Unternehmen umgangen werden können.

- Trojanische Angriffe auf Smartphones (z. B. mit Flexy Spy)
- Fremde WebCams anzapfen mittels PDF-Exploit
- Angriff auf drahtlose Überwachungskameras
- Angriff auf ein Webshop-System – günstig einkaufen durch Preisverhandlungen
- Kon-Boot-Attack: ohne Windows-Passwort an Ihren Rechner
- Angriff auf verkryptete USB-Sticks – Kingston, Verbatim, Sandisk: Wer ist wirklich sicher?
- Angriff unter Anwendung von Barcodes/Barcode-Scannern (SQL-Injection)
- Hardwarespion: Angriff auf Systeme von Privatpersonen (Key-Logger)
- Kreditkartenzahlung im Internet am Bsp. eines Standard-Shops
- Google-Hacking: So kann die Suchmaschine fürs Hacken eingesetzt werden
- Hardware-Angriff auf ein gesperrtes und ausgeschaltetes Smartphone/Handy
- Angriff auf ein Computerspiel

#### Referent:

##### Sebastian SCHREIBER

Geschäftsführer  
SySS GmbH, Tübingen

#### Moderator:

##### Klaus-Dieter BAIER

Security Consultant  
DESA Investigation – Risk Protection,  
Berlin

# Programm

12.00 – 13.30 Uhr

Mittagessen

13.30 – 15.00 Uhr

## Fachsitzung 4

### Korruptionsbekämpfung: Kann es einen Fall bei SIEMENS nach dem Korruptionsskandal geben?

- Das Compliance-System bei der SIEMENS AG
- Effektivität und Effizienz der Korruptionsbekämpfung:  
Die Messung
- Theorie und Praxis?

Referentin:

**Susanne GROPP-STADLER**

Head of Compliance Legal  
Siemens AG, München

Moderator:

**Heinz Josef BALLE**

Hauptabteilungsleiter Interne Revision  
Provinzial Nordwest Holding AG,  
Münster

Mitglied des DIIR-Arbeitskreises  
„Abwehr wirtschaftskrimineller  
Handlungen in Unternehmen“

13.30 – 15.00 Uhr

## Fachsitzung 5

### Fraud-Krisenmanagement im Ereignisfall

- Schwerer „Fraud-Unfall“: Was nun? – ein kurzer (Negativ-) Erfahrungsbericht aus der Praxis zur Einführung
- Task Force-Bildung
- Organisation der Task-Force-Arbeit
- Zusammenarbeit mit Staatsanwaltschaft/Polizei
- Beweise beschaffen, erheben, sichern
- Schadensmanagement und Anspruchssicherung
- Berichtswesen
- Externe Spezialisten einschalten?
- Krisenkommunikation: Reduzierung von Risiken negativer Berichterstattung; „Litigation-PR“

Referent:

**RA Dr. Helmut GÖRLING**

Görling Rechtsanwaltsgesellschaft  
mbH, ein Unternehmen der

Görling Unternehmensgruppe für  
forensische Dienstleistungen,  
Frankfurt am Main

Moderator:

**Thomas MATZ**

Senior Prüfungsleiter  
Commerzbank AG, Frankfurt am Main  
Leiter des DIIR-Arbeitskreises „Abwehr  
wirtschaftskrimineller Handlungen in  
Unternehmen“

13.30 – 15.00 Uhr

## Fachsitzung 6

### Die 10 Kardinalsfehler der Internen Netzwerksicherheit: Live-Vorführung und Prüfung durch den Internen Revisor – Schadensbewältigung und -begrenzung

- Ein kurzer Blick auf die Ausgangslage
- Ein Überblick über die geläufigsten Angriffsformen und Vorgehensweisen
  - Aufklärung der Netzwerkinfrastruktur und der weiteren Ziele
  - Angriffe auf die Netzwerkinfrastruktur
  - Angriffe auf Netzwerkprotokolle
  - Tarnung von Angriffen
  - Verwandte Angriffe
- Tätertypen und Motive (Zugehörigkeitsgruppen, Persönlichkeitstypen, Motive)

Referent:

**Andreas MACHT**

Geschäftsbereich Innere Sicherheit  
r.o.l.a. Business Solutions GmbH, Berlin

Moderator:

**Torsten RÖDIGER**

Security Officer  
Vattenfall Europe Information Systems  
GmbH, Hamburg

# Programm

- Warum fehlt es an Awareness? Ein kritischer Blick nach Innen!
- Die 10 Kardinalsfehler in der Internen Netzwerksicherheit
  - Kein Ziel, kein Konzept, keine Risikobewertung
  - Gottvertrauen in die Technik
  - Vertrauen ist gut, Kontrolle ist besser
  - Denn sie wissen nicht, was sie tun (Was fehlende Awareness und fehlendes Wissen beim Anwender anrichtet)
  - Wie fehlendes, zukunftsfähiges Know-how die Wettbewerbsfähigkeit gefährdet
  - Transparenz – fehlt sie, ist keiner verantwortlich
  - Handlungs- und Bewegungsfreiheit im Inneren für Jedermann
  - Fehlende Zusammenarbeit mit den Betroffenen
  - Fehlende Praxistauglichkeit und keine Akzeptanz der Lösungen
  - Fehlen einer regelmäßigen Prüfung (fehlendes IKS)
- Was passiert, wenn doch etwas passiert (Krisenmanagement)?
- State-of-the-art in der Absicherung von Netzwerken
- Prüfung durch den Internen Revisor

15.00 – 15.30 Uhr

**Kaffeepause, Networking**

15.30 – 17.00 Uhr

## **Fachsitzung 7**

### **Geldwäsche in modernen Finanzsystemen**

- Einführung:  
Die Rolle der Financial Intelligence Unit in der Liechtensteinischen Landesverwaltung  
Erkennung von Geldwäscherei, Vortaten der Geldwäscherei und organisierter Kriminalität sowie Terrorismusfinanzierung  
Konzept, System und Kernaufgaben
- Art und Weise, Teilnehmer, Spezifika, Besonderheiten, Schwierigkeiten in der Identifizierung, Grenzen der Wahrnehmung
- Herausforderung dieser Systeme für die FIU
- Praktischer Ansatz, operative Analyse am Fallbeispiel
- Analysehilfsmittel
- Bedeutung für die Interne Revision und die Security

### **Referent:**

**Markus RUEEGG**

Financial Intelligence Unit  
Fürstentum Lichtenstein

### **Moderator:**

**Robert ECK**

Geschäftsführer  
r.o.l.a. Business Solutions GmbH, Berlin  
Stellv. Leiter des DIIR-Arbeitskreises  
„Abwehr wirtschaftskrimineller  
Handlungen in Unternehmen“

01. März 2012

# Programm

15.30 – 17.00 Uhr

## Fachsitzung 8

### Business Continuity Management am Beispiel einer deutschen Großbank: Was ist im Krisenfall zu tun?

- Aufbau und Ablauf Business Continuity Management
- Bewertung der aufgebauten Maßnahmen
- Kriseninfrastruktur und -organisation
- Krisenmanagement, so oder so ähnlich . . .

#### Referent:

##### Dirk B. PAHMEYER

BCM Officer/Abteilungsleiter  
GS-SE Group Security  
Business Continuity Management  
Commerzbank AG, Frankfurt am Main

#### Moderator:

##### Michael HELFER

Geschäftsführer  
AuditManagement LiVE, Berlin  
Mitglied des DIIR-Arbeitskreises  
„Abwehr wirtschaftskrimineller  
Handlungen in Unternehmen  
Mitglied des DIIR-Arbeitskreises  
„MaRisk“

15.30 – 17.00 Uhr

## Fachsitzung 9

### Wirtschaftskriminalität mit Hilfe der Informationstechnologie/Stichwort Cyber Crime

- Der Unterschied zwischen Cybercrime und Cyberwar
- Cyberwar: Das Internet als neuer Kriegsschauplatz?
- Kritische Infrastrukturen: Die Wirtschaft, die Banken, die Börsen
- Stuxnet: Kein Spion, ein Saboteur! – Wer? Wozu? Vier Tage zur Einschätzung der Gefährdung?
- Die Nachfolger von Stuxnet: Duqu („der Vorläufer des Nachfolgers“)
- Wirtschaftsspionage
- Auf konventionellen (!) Wegen zum Ziel
- Augenmerk muss auf der Abwehr von Insider-Spionage liegen
- Netzwerke müssten zurückgebaut und verkleinert werden
- Gibt es einen Cyber-industriellen Komplex?

#### Referent:

##### Dr. Sandro GAYCKEN

Senior Researcher in der Informatik der  
Freien Universität Berlin  
Freie Universität, Berlin

#### Moderator:

##### Dr. Berthold STOPPELKAMP

Geschäftsführer der ASW –  
Arbeitsgemeinschaft für Sicherheit der  
Wirtschaft e.V., Berlin  
  
Leiter Hauptstadtbüros des  
BUNDESVERBAND DER SICHERHEITS-  
WIRTSCHAFT (BDSW) Wirtschafts- und  
Arbeitgeberverband e. V.  
(ab 01.01.2012)

19.00 – 22.00 Uhr

## Erfahrungsaustausch mit Abendessen

# Programm

08.00 – 08.30 Uhr

**Begrüßungskaffee**

08.30 – 10.00 Uhr

**Fachsitzung 10**

**Kommunikation zwischen Unternehmen und Staatsanwaltschaft im Ermittlungsverfahren**

- Zwangsmaßnahmen gegen das Unternehmen
  - Abwendungsmöglichkeiten/Notfallplan/Ablaufgestaltung
- Öffentlichkeitsarbeit bei eingeleitetem Ermittlungsverfahren
  - Presseberichterstattung – ausgewählte Beispiele aus der Strafverfolgungspraxis/Vermeidung von Reputations-schäden
- Ermittlungen durch das Unternehmen
  - Innenrevision/Anwaltskanzleien/Forensic Services/Privatdetektive
- Maßnahmen zur Sicherung der Gewinnabschöpfung
  - Bruttoprinzip/Abwendungsmöglichkeiten/Abschöpfung im Unternehmensinteresse
- Verfahrensverkürzende Absprachen
  - Unternehmensgeldbuße/Einstellungsmöglichkeiten/ Strafbefehl

**Referent:**

**Oberstaatsanwalt  
Ralf MÖLLMANN**

Sprecher und Koordinator der  
Schwerpunktabteilung für  
Wirtschaftsstrafsachen der

Staatsanwaltschaft Düsseldorf,  
Düsseldorf

**Moderatorin:**

**Melanie SCHMITT**

Audit Compliance Et International  
Deutsche Telekom AG, Bonn

08.30 – 10.00 Uhr

**Fachsitzung 11**

**Auf der Suche nach der Wahrheit – Bewertungen von mündlichen und schriftlichen Angaben**

- Prüfung der Glaubhaftigkeit
  - Methode der Aussagenanalyse anhand von objektiven Kriterien
- Glaubwürdigkeit von Personen, Glaubhaftigkeit von Angaben
- Körpersprachliche Signale
- Warn-Signale
- Wahr und dennoch falsch
  - Die Überprüfung von Angaben auf Irrtümer (Fehler bei der Wahrnehmung und Erinnerungsfehler)
- Aufdecken eines Komplotts

**Referent:**

**Axel WENDLER**

Richter am Oberlandesgericht,  
Stuttgart

Lehrbeauftragter, Uni Tübingen

**Moderator:**

**Stefan BRANDT**

Volkswagen AG, Wolfsburg

Mitglied des DIIR-Arbeitskreises  
„Abwehr wirtschaftskrimineller  
Handlungen in Unternehmen“

# Programm

08.30 – 10.00 Uhr

## Fachsitzung 12

### Grenzen der Freiheit – Wie sicher sind Android, BlackBerry OS, iOS und Windows Phone 7?

Mit zunehmender Leistungsfähigkeit drängen Smartphones und Tablet-Geräte in die Unternehmenswelt. Ob Manager, Vertriebsmitarbeiter oder Techniker – alle wollen von den smarten Allkönnern profitieren und auch mobil produktiv tätig sein. Doch welches Sicherheitsniveau können die verschiedenen Plattformen bieten und welche Herausforderungen warten auf IT-Verantwortliche? Der Vortrag zeigt den aktuellen Stand zum Thema Smartphone- und Tablet-Sicherheit – insbesondere beim Einsatz der Geräte im Unternehmensumfeld.

- Bekanntgewordene Sicherheitslücken und -vorfälle sowie ihre Ursachen
- Integrierte Schutzfunktionen der einzelnen Plattformen
- Bedrohungs- und Gefährdungslage
- Sicherheitsmaßnahmen
- State-of-the-Art in der Smartphone-Sicherheit
- Zusammenfassung, Fazit und Empfehlung

#### Referent:

**Ronny SACKMANN**

IT-Sicherheitsberater

CIROSEC GmbH, Heilbronn

#### Moderator:

**Christoph E. RAKOWSKI**

Leiter Revision

Deutsche Factoring Bank, Bremen

Mitglied des DIIR-Arbeitskreises

„Abwehr wirtschaftskrimineller Handlungen in Unternehmen“

10.00 – 10.45 Uhr

## Kaffeepause, Check Out

10.45 – 12.15 Uhr

## Fachsitzung 13

### UK Bribery Act 2010: Additional Compliance Obligations for Global Cooperations

- Hintergründe der Neuregelung ab Juli 2011: Kurze Einführung in die Historie
- Wer ist von dem Gesetz betroffen? Anwendbarkeit, Grundprinzipien und extratoriale Wirkung (Fallbeispiel)
- Kurzgegenüberstellung Unterschiede: Deutsches Strafgesetzbuch/Foreign Corrupt Practices Act (FCPA)/UK Bribery Act
- Darstellung adäquater Maßnahmen („adequate procedures“) zum Schutze des Unternehmens
- Sanktionierung bei Verstößen und Folgeschäden
- Implementierung und Nachweis der Wirksamkeit von Präventionsmaßnahmen
- Auftrag der Revision im Hinblick auf ihre Beratungs- und Prüfungspflicht
- Möglichkeiten und Grenzen der Überprüfung von Dritten – Third-Party Due Diligence
- Erste Ergebnisse und mögliche Folgen

#### Referent:

**Stefan WIELAND**

Geschäftsführer

Business Integrity Management GmbH, Berlin

#### Moderator:

**RA Lars RIETHER**

Konzernrevision und Sicherheit – Ethical Compliance Audits

Deutsche Post DHL, Bonn

Mitglied des DIIR-Arbeitskreises

„Abwehr wirtschaftskrimineller Handlungen in Unternehmen“

# Programm

10.45 – 12.15 Uhr

## Fachsitzung 14

**Compliance zur Verhinderung von Wirtschaftsstraftaten – Strafbarkeit des Compliance-Officers sowie des Internen Revisors – Strafrechtliche Konsequenzen des Versagens von Compliance**

- Kommunikation mit der Staatsanwaltschaft
  - Wie sieht die Struktur der Kommunikation aus
  - Wie wird eine „Vereinbarung“ mit der Staatsanwaltschaft dokumentiert
- Strafbarkeitsrisiken
  - für den Internen Revisor
  - für den Vorstand
  - für den Compliance-Officer

**Referent:**

**Prof. Dr. Jürgen WESSING**

FA für Strafrecht  
Partner

Wessing & Partner, Düsseldorf

**Moderator:**

**Volker HAMPEL**

Geschäftsführer

DIIR – Deutsches Institut für Interne  
Revision e. V., Frankfurt am Main

10.45 – 12.15 Uhr

## Fachsitzung 15

**Beschäftigten-Datenschutz und neue Rechtsrisiken daraus – aus der Praxis**

- Aktueller Stand BDSG und die letzten drei Novellierungen
- Skandalon oder „Holz des Anstoßes“: Neuregelung notwendig?
- BDSG-Erweiterung vs. eigenes Beschäftigtendatenschutzgesetz
- Arbeitnehmerdatenschutz
- Wesentliche geplante Neuregelungen im Beschäftigtendatenschutz
  - Betriebliche Kommunikationsmittel (Telefon, Email, Internet)
  - Überwachungseinrichtungen (Videoaufzeichnungen)
  - Kranken- und Rückkehrgespräche
  - Compliance Rules und ihre Überwachung
- Wesentliche Kritikpunkte der Berufsverbände und Praktiker
- Vorbereitung des Unternehmens auf die Umsetzung
- Betriebsvereinbarungen

**Referent:**

**RA Thomas BADE**

Handelsverband Deutschland –  
HDE e. V., Berlin

**Moderator:**

**Jörg Wehling, CIA**

Inhaber

Audit and Office Innovation,  
Großostheim

Mitglied des DIIR-Arbeitskreises  
„Abwehr wirtschaftskrimineller  
Handlungen in Unternehmen“

12.15 – 12.30 Uhr

**Raumwechsel**

02. März 2012

# Programm

12.30 – 13.15 Uhr

## Grundsatzreferat 2

### Mechanismen der Kartelle – Methoden der Aufdeckung

- Das Bundeskartellamt
- Die Kartellermittlung
  - Entwicklungen und Erfolge
  - Vorgehensweisen
  - Kartellformen
  - Beweisführung
- Das Spannungsfeld zwischen Kartell, Submissionsbetrug und Bestechung

### Lothar JANTA

Leitender Regierungsdirektor  
12. Beschlussabteilung  
Bundeskartellamt, Bonn

13.15 – 13.30 Uhr

## Schlussworte

### Mag. Dr. Matthias KOPETZKY, CIA, CPA, CFE, SV

Geschäftsführer  
Business Valuation GmbH, Wien  
Mitglied des DIIR-Arbeitskreises  
„Abwehr wirtschaftskrimineller  
Handlungen in Unternehmen“  
  
Mitglied des Vorstands im IIA Austria  
und Leiter des Arbeitskreises  
„Wirtschaftskriminalität“ des IIA Austria

13.30 – 15.00 Uhr

## Abschließendes gemeinsames Mittagessen

# Tagungsdaten

## Ort

### Aukam's La Strada Kassel

Raiffeisenstraße 10  
34121 Kassel  
Telefon: +49 (0)5 61 20 90-0  
Telefax: +49 (0)5 61 20 90-500

## Auskünfte und Anmeldung

### DIIR – DEUTSCHES INSTITUT FÜR INTERNE REVISION e.V.

Ohmstraße 59, 60486 Frankfurt am Main  
Telefon (069) 71 37 69-15, Telefax (069) 71 37 69-69

**Bitte benutzen Sie das beigefügte Anmeldeformular.**

## Tagungsgebühr

### Für Mitglieder

des DIIR – Deutsches Institut für Interne Revision e.V.

und der ASW-Mitgliederorganisationen € 820,-

Für Nichtmitglieder € 870,-

Inklusive: zwei Mittagessen, einem Abendessen, Pausengetränke und Tagungsunterlagen. **Die Teilnehmergebühr wird fällig nach Erhalt der Anmeldebestätigung und Rechnung, spätestens mit Tagungsbeginn.**

Tagungsanmeldungen können **nur** schriftlich zurückgezogen werden. Erfolgt die schriftliche Stornierung innerhalb von 4 Wochen vor Tagungsbeginn, müssen wir eine Stornogebühr von 20% der Teilnehmergebühr berechnen. Erfolgt die schriftliche Stornierung innerhalb von 10 Tagen vor Tagungsbeginn oder erscheint der angemeldete Teilnehmer nicht zur Tagung, ist die volle Tagungsgebühr zu zahlen. Selbstverständlich kann ein Ersatzteilnehmer gestellt werden.

## Hotelzimmer

Der Veranstalter hat in der Zeit vom **01. bis 02. März 2012**

im **Aukam's La Strada Kassel**

Raiffeisenstraße 10  
34121 Kassel  
ein Zimmerkontingent gebucht.

### Zimmerpreis:

Einzelzimmer: EUR 91,50 pro Übernachtung

jeweils inkl. Frühstücksbuffet im Restaurant und

inkl. Mehrwertsteuer.

Bitte reservieren Sie Ihr Zimmer **direkt** beim Hotel. Die Kennung

für den Erhalt des ausgehandelten Zimmerpreises ist „DIIR“.

Die o.a. Hotelkosten sind nicht in der Tagungsgebühr enthalten.

Sie werden Ihnen vom Hotel direkt in Rechnung gestellt.

**Das DIIR – Deutsches Institut für Interne Revision e.V. nimmt keine Hotelzimmerreservierung an.**

## Hinweis

Es werden 11 Stunden CPE für regelmäßige Weiterbildung anerkannt.



# DIIR

**Deutsches Institut für  
Interne Revision e.V.**

Ohmstraße 59  
60486 Frankfurt am Main  
Telefon (069) 71 37 69-15  
Fax (069) 71 37 69-69  
[www.diir.de](http://www.diir.de)  
[akademie@diir.de](mailto:akademie@diir.de)