

**Wichtiges Bonusmaterial inklusive**  
+ Beispiele und Templates für Notfallübungen  
+ Excel-Templates für Kritikalitätsanalyse  
+ Beispiel einer Sicherheitsleitlinie

## Intensivkurs

# IT-Notfallmanagement

Ein praktischer Leitfaden für effektive Notfallmassnahmen, Business Continuity und Disaster Recovery

28. und 29. März 2012 in Zürich  
20. und 21. Juni 2012 in Düsseldorf  
27. und 28. September 2012 in Dresden  
27. und 28. November 2012 in Hamburg

[vereon.ch](http://vereon.ch)

**»< VEREON**  
*know-how for your success*

### Kursleiter



Dr. Heinrich Kersten



Dr. Gerhard Klett

### Highlights aus dem Programm

- + Methoden zur Risikoanalyse und -bewertung wie Risk Analysis, Business Impact Analysis oder Kritikalitätsanalyse korrekt anwenden
- + Notfallkonzepte und Notfallhandbücher als Arbeitsanweisung für den Notfall
- + Schnittstellen zu Change-, Configuration-, Problem- und Service Level Management
- + Konkrete Massnahmen bei typischen Notfällen in der Informationsverarbeitung: Ausfall zentraler IT-Systeme, Manipulationen oder mangelnde Compliance
- + Planung und Durchführung von Übungen für Notfälle und Wiederanlaufplanung
- + Praxiserfahrungen mit Business Continuity nach ISO 27001
- + Standards für das Notfallmanagement und Sicherheitskonzepte
- + Key Performance Indicators für Reviews und Audits festlegen

***“Extrem hoher Praxisbezug durch reichen Erfahrungsschatz der Referenten und interaktive Übungen sowie Diskussion eigener Fälle”***

## INHALTE DIESER VERANSTALTUNG

### Risikoanalyse und -bewertung

Viele Organisationen haben die Sinnhaftigkeit und Vorteile eines Sicherheitsmanagements für ihre Informationsverarbeitung erkannt: Es werden mögliche Sicherheitsvorfälle nach Eintrittshäufigkeit und Schadenshöhe analysiert und daraus Risiken für die Organisation abgeleitet, klassifiziert und bewertet. Zumindest bei höheren Risiken versucht man, diese durch geeignete "präventive" Massnahmen unter eine noch akzeptable Grenze zu drücken. Weiterhin ist der Compliance-Aspekt zu beachten, der eine Beschäftigung z.B. mit ISO 27001, dem IT-Grundschatz oder weiteren Regularien erfordern kann.

### Risikokategorisierung

Nimmt man sich die Ergebnisse der Risikoanalyse und -bewertung vor, so erkennt man schnell, ob es Risiken gibt, die bei ihrem Eintritt einen gravierenden oder sogar Existenz bedrohenden Schaden für die Organisation nach sich ziehen können. Massgebend ist also die mögliche Schadenshöhe im Einzelfall - weniger die Häufigkeit des Eintritts.

### Typische Notfälle in der IT

- Beim Ausfall wichtiger IT-Anwendungen und IT-Systeme geht es darum, möglichst schnell wieder in einen Normalzustand zu kommen - ggf. auch mit Überbrückung durch einen Notbetrieb -, um Umsatzverluste oder Vertragsstrafen zu vermeiden.
- Ein wichtiger Service oder ein System ist in hohem Masse gestört und stellt ein Disaster dar; eine Rückkehrprozedur zum vollen Leistungsumfang ist erforderlich.
- Manipulationen an Daten und Anwendungen durch einen Innentäter sind erkannt worden.
- Bei Ausfall eines Dienstleisters (z.B. Netzwerk-Provider) sollen durch "Umschaltung" auf einen anderen Dienstleister Verluste und Ausfallzeiten minimiert werden.
- Wird aufgrund fehlender Compliance bei einem Rechenzentrum z.B. von einer Aufsichtsbehörde eine Betriebseinstellung verfügt, resultiert dies möglicherweise in einem massiven Umsatzverlust; hier geht es um eine kurzfristige, nachweisbare Wiederherstellung der Compliance.

### Notfallmanagement

In diesen Fällen kommt es darauf an, durch schnelle sachgerechte Entscheidungen und trainierte, qualitativ überwachte Vorgehensweisen (Notfallübungen) die Auswirkungen auf die Geschäftstätigkeit zu begrenzen.

### Konkrete Massnahmen ergreifen

- Erforderlichen Organisationsstrukturen mit ihren Rollen, Prozessen und Dokumentationen (u.a. Notfallkonzept, Notfallhandbuch) einrichten
- Schnittstellen zu bereits existierendem Change-, Configuration-, Problem- und Service Level Management definieren und betreiben
- Wesentliche Methoden (Risk Analysis, Business Impact Analysis, Kritikalitätsanalyse) anwenden
- Notfallübungen planen
- Key Performance Indicators für die Reviews und internen/externen Audits festlegen
- Massnahmen umsetzen, z.B. Notfall- und Wiederanlaufplanung

## AGENDA ERSTER TAG

Leitung: Dr. Gerhard Klett

09.00

### Begrüssung und Eröffnung

- Programmübersicht, Vorstellung, Organisatorisches

### Relevanz von Business Continuity

- Zielsetzung der Business Continuity
- Compliance-Aspekte
- Grundsätzliche Erfahrungen

10.30 - 10.45 Kaffeepause

### Bedeutung von Change-, Configuration- und Risk-Management

- Überbrückungsmassnahmen
- Wiederanlaufplanung / Disaster Recovery
- Notfallübungen: Beispiele und Templates

12.00 - 13.00 Gemeinsames Mittagessen

### Diskussionsrunde mit den Teilnehmenden

- Welche eigenen Erfahrungen wurden bisher gemacht?
- Was kann man hieraus für künftige Projekte lernen?
- Gibt es bereits einen "best-practice"?

### Organisation von Notfallmassnahmen

- Rollen und Zuständigkeiten
- Notfallplanung für kritische Geschäftsprozesse
- Schnittstellen zu ITIL
- Auditierung von Notfallmassnahmen

14.45 - 15.00 Kaffeepause

### Praxiserfahrungen mit Business Continuity nach ISO 27001

- Darstellung der Controls
- Business Continuity und Zertifizierung

### Unterstützung durch Tools

- TNG Advanced Helpdesk (AHD)
- BS 25999-2 Business Continuity Selfassessment Online Tool
- Business Impact Assessment Tool
- Business Continuity Checklist Tool

### Abschliessende Frage- und Diskussionsrunde

17.00 Ende Tag 1

# Tag 2: IT-Grundschutz und Notfallmanagement

## AGENDA ZWEITER TAG

Leitung: Dr. Heinrich Kersten

09.00

### Begrüssung und Eröffnung zweiter Tag

- Programmübersicht, Vorstellung, Organisatorisches

### Notfallmanagement nach IT-Grundschutz

- Anwendung des BSI-Standards 100-4
- IT-Grundschutz-Analyse nach BSI 100-2 als Vorbereitung
- Erweiterte Analyse nach BSI 100-3
- Kataloge und Modellierung
- Schutzbedarf, Basis-Sicherheits-Check
- Bausteingruppe M6 / Notfallvorsorge

10.15 - 10.30 Kaffeepause

### Systematik der Notfallprävention

- Rolle der Sicherheitsleitlinien und -konzepte
- Bedeutung des Risk Managements für die Notfallplanung
- Incident Management

12.00 - 13.15 Gemeinsames Mittagessen

### Business Impact Analysis (BIA) - mit Interaktiven Übungen

- Ermitteln kritischer Geschäftsprozesse
- Einführung in die Methode der BIA
- Anwendung der BIA anhand konkreter Beispiele
- Verfügbare Hilfsmittel

15.15 - 15.30 Kaffeepause

### Gestaltung des reaktiven Notfallmanagements

- Notfalleitlinie als Orientierung: Mit interaktivem Übungsteil
- Notfallkonzept als Planungsgrundlage
- Notfallhandbuch als Praxisgrundlage
- Notfall- und Wiederanlaufpläne als Arbeitsanweisungen für den Notfall
- Aufzeichnungen und Auswertungen über Notfälle

### Brainstorming mit den Teilnehmern

- Welche eigenen Erfahrungen wurden bisher gemacht?
- Was kann man hieraus für künftige Projekte lernen?
- Gibt es bereits einen "best-practice"?
- Abschließende Fragerunde

17.00 Ende Tag 2

## TEILNEHMERSTIMME

‘Sehr umfassende Themenbehandlung.’  
M. Kurz, Die Schweizerische Post

## IHRE KURSLEITER

**Dr. Gerhard Klett** verfügt durch seine langjährige Tätigkeit als Senior Security Consultant bei der BASF SE und der BASF IT Services GmbH im Fachgebiet Informatik-Sicherheit und Netzwerke über umfangreiche Praxiserfahrung. Er leitete die Planung und den Aufbau der gesamten IT-Infrastruktur der Verwaltung der RAO Gazprom in Moskau, einer der grössten Joint-Venture Partner der BASF. Seine Arbeitsschwerpunkte als Leiter des Departments "IT Security-Solutions" bei der BASF IT Services GmbH waren Security Consulting, Risikomanagement und Compliance für ISO 27001, Zertifizierung und Sarbanes Oxley (SOX), Security für E-Commerce, sichere Kommunikation und Authentifizierung, Public Key Infrastructure (PKI), E-Mail-Sicherheit sowie Schwachstellenanalyse und Security Scans. Heute führt er die IT-Security Beratungsfirma GK IT-Security Consulting.

**Dr. Heinrich Kersten** war Leiter der Zertifizierungsstelle bei der T-Systems, Bonn, sowie des Sektorkomitees "Security" beim Akkreditierer DATech. In seiner Tätigkeit bei T-Systems hat Dr. Kersten Unternehmen in Belangen der Informationssicherheit auditiert und zertifiziert. Weitere umfangreiche Berufserfahrung konnte Dr. Kersten unter anderem bei der Bayer AG und während seiner Tätigkeit beim Bundesamt für Sicherheit in der Informationstechnik (BSI) als Leitender Regierungsdirektor und Abteilungsleiter für "Wissenschaftliche Grundlagen und Zertifizierung" sammeln. Beim BSI war er u.a. mit der Produktzertifizierung und der Weiterentwicklung und Anwendung von Sicherheitsstandards befasst. Dr. Kersten ist erfolgreicher Fachbuchautor zu Themen des IT-Sicherheitsmanagements.

## WER SOLLTE TEILNEHMEN?

Geschäftsführer, CIO, Leiter IT, Notfallbeauftragte, Incident Manager sowie Sicherheitsverantwortliche und Datenschutzbeauftragte. Darüber hinaus Führungskräfte und Mitarbeiter der Bereiche

- IT-Sicherheit
- IT-Risikomanagement
- IT-Revision
- Datenschutz und -sicherheit
- Betriebliche Sicherheit

## AKTUELLE VERANSTALTUNGSHINWEISE

### iPhone Security

[www.vereon.ch/ips](http://www.vereon.ch/ips)

### Mobile Device Management

[www.vereon.ch/mdm](http://www.vereon.ch/mdm)

### Business Continuity Management

[www.vereon.ch/bcm](http://www.vereon.ch/bcm)

### IT-Sicherheitskonzepte

[www.vereon.ch/ism](http://www.vereon.ch/ism)

### IT-Sicherheits-Audits planen und durchführen mit Kennziffern

[www.vereon.ch/isa](http://www.vereon.ch/isa)

# IT-Notfallmanagement

Ja, hiermit melde ich mich an für:

- 28. und 29. März 2012, Zürich (CHF 2'595.-)
- 20. und 21. Juni 2012, Düsseldorf (EUR 1'895.-)
- 27. und 28. September 2012, Dresden (EUR 1'895.-)
- 27. und 28. November 2012, Hamburg (EUR 1'895.-)

Die Teilnahmegebühr gilt pro Person und Termin zzgl. MwSt.

## 1. PERSON

Anrede, Titel \_\_\_\_\_

Name, Vorname \_\_\_\_\_

Position, Abteilung \_\_\_\_\_

E-Mail \_\_\_\_\_

Firma \_\_\_\_\_

Strasse, Nr. \_\_\_\_\_

Postfach \_\_\_\_\_

PLZ, Ort \_\_\_\_\_

Land \_\_\_\_\_

## 2. PERSON

Anrede, Titel \_\_\_\_\_

Name, Vorname \_\_\_\_\_

Position, Abteilung \_\_\_\_\_

E-Mail \_\_\_\_\_

## RECHNUNGSDetails

Bestellreferenz \_\_\_\_\_

MwSt.-Nr. \_\_\_\_\_

Firma \_\_\_\_\_

Abteilung \_\_\_\_\_

Strasse, Nr. \_\_\_\_\_

PLZ, Ort \_\_\_\_\_

Datum, Unterschrift \_\_\_\_\_

Bei Zahlung per Kreditkarte bitte ausfüllen

Karteninhaber \_\_\_\_\_

Kartenummer \_\_\_\_\_

gültig bis \_\_\_\_\_



## 5 WEGE ZUR ANMELDUNG

Web vereon.ch  
Telefon +41 71 677 8700  
Fax +41 71 677 8701  
E-Mail anmeldung@vereon.ch  
Post Vereon AG  
Postfach 2232  
8280 Kreuzlingen  
Schweiz

## VERANSTALTUNGSORTE

Die Veranstaltungen finden jeweils in zentraler Lage und in gehobenem Ambiente statt. Weitere Details senden wir Ihnen rechtzeitig vor den jeweiligen Terminen per E-Mail.

## TEILNAHMEBEDINGUNGEN

**Geltungsbereich**  
Diese Teilnahmebedingungen regeln das Vertragsverhältnis zwischen dem Veranstalter und dem Teilnehmer. Der Teilnehmer erkennt mit seiner Anmeldung diese Teilnahmebedingungen an. Abweichende Allgemeine Geschäftsbedingungen des Teilnehmers haben keine Gültigkeit.

**Teilnahmegebühr**  
Die Teilnahmegebühr beinhaltet die Teilnahme für eine Person. Sie versteht sich inklusive schriftlicher Unterlagen, Mittagessen und Tagungsgetränke zzgl. MwSt. Nach Eingang Ihrer Anmeldung erhalten Sie eine Anmeldebestätigung und eine Rechnung. Diese ist direkt nach Erhalt, in jedem Fall vor Eintritt in die Veranstaltung fällig.

**Anmeldung**  
Die Anmeldung kann schriftlich via Internet, E-Mail, Fax oder per Post oder mündlich per Telefon erfolgen. Sie ist, vorbehaltlich gesetzlicher Widerrufsrechte, verbindlich. Jede Anmeldung erlangt erst durch schriftliche Bestätigung seitens des Veranstalters Gültigkeit. Die Veranstaltungsteilnahme setzt die vollständige Bezahlung der Teilnahmegebühr voraus.

**Urheberrecht**  
Alle im Rahmen der Veranstaltungen ausgegebenen Unterlagen sowie anderweitig erworbene Artikel sind urheberrechtlich geschützt. Vervielfältigungen und anderweitige Nutzung sind schriftlich durch den Veranstalter zu genehmigen.

**Rücktritt des Teilnehmers**  
Sollte der Teilnehmer an der Teilnahme verhindert sein, so ist er berechtigt jederzeit ohne zusätzliche Kosten einen Ersatzteilnehmer zu benennen. Darüber hinaus ist eine vollständige Stornierung bis 30 Tage vor Beginn der Veranstaltung kostenlos möglich. Die Stornierung bedarf der Schriftform. Bei späterem Rücktritt oder Nichterscheinen wird die gesamte Teilnahmegebühr fällig.

**Programmänderungen und Absagen**  
Der Veranstalter behält sich vor, Änderungen am Inhalt des Programms sowie Ersatz und Weglassen der angekündigten Referenten vorzunehmen, wenn der Gesamtcharakter der Veranstaltung gewahrt bleibt. Muss eine Veranstaltung aus wichtigem Grund oder aufgrund höherer Gewalt (kriegerische Auseinandersetzungen, Unruhen, terroristische Bedrohungen, Naturkatastrophen, politische Beschränkungen, erhebliche Beeinflussung des Transportwesens usw.) abgesagt oder verschoben werden, so wird der Veranstalter die zu diesem Zeitpunkt angemeldeten Teilnehmer umgehend schriftlich oder mündlich benachrichtigen. Bereits eingegangene Zahlungen werden für eine zukünftige Veranstaltung gutgeschrieben oder bei einer Terminverschiebung auf den neuen Termin ausgestellt. Kosten seitens des Teilnehmers, die mit der Absage einer Veranstaltung verbunden sind (z.B. Reise- und Übernachtungskosten), werden nicht erstattet.

**Haftung**  
Alle Veranstaltungen werden sorgfältig recherchiert, aufbereitet und durchgeführt. Sollte es dennoch zu Schadensfällen kommen, so übernimmt der Veranstalter keine Haftung für die Vollständigkeit und inhaltliche Richtigkeit in Bezug auf die Vortragsinhalte und die ausgegebenen Unterlagen.

**Datenschutz**  
Überlassene persönliche Daten behandelt der Veranstalter in Übereinstimmung mit den geltenden datenschutzrechtlichen Bestimmungen. Sie werden zum Zwecke der Leistungserbringung elektronisch gespeichert. Einblick und Löschung der gespeicherten Daten kann jederzeit gefordert werden. Anfragen bitte per E-Mail an: info@vereon.ch.

**Schlussbestimmungen**  
Der Vertrag unterliegt dem schweizerischen Recht. Gerichtsstand ist Kreuzlingen (Schweiz).



Jetzt anmelden: [www.vereon.ch/inm](http://www.vereon.ch/inm)