

# Wir danken den Sponsoren der Studie IT-Sicherheitsstandards und IT-Compliance

## secunet



**A. Allgemeine Fragen****1. Welche Position bekleiden Sie in Ihrem Unternehmen oder Ihrer Behörde (Mehrfachnennung möglich)?**

- Geschäftsführung/Vorstand/Amtsleitung  
 Aufsichtsrat  
 IT-Leiter/Rechenzentrumsleiter  
 IT-Administrator  
 Datenschutzbeauftragter/Datenschutzmanager  
 (IT-) Sicherheitsbeauftragter/(IT-) Security Manager/(IT-) Sicherheitsmanager  
 (IT-) Governance Manager  
 (IT-) Risk Manager  
 (IT-) Compliance Manager  
 (IT-) Revisor  
 Nicht IT-Mitarbeiter  
 Andere Position: \_\_\_\_\_  
 Keine Angabe

**2. Welchem Bereich ist Ihre Institution zuzuordnen?**

- Produzierendes Gewerbe  Verarbeitendes Gewerbe  
 Energie- und Wasserversorgung  
 Baugewerbe  
 Anderer Bereich: \_\_\_\_\_  
  
 Dienstleistungsbereich  Handel  
 Verkehr und Nachrichtenübermittlung  
 Kredit- und Versicherungsgewerbe  
 Öffentliche Verwaltung, Verteidigung, Sozialversicherung  
 Gesundheits-, Veterinär- und Sozialwesen  
 Anderer Dienstleistungsbereich: \_\_\_\_\_  
  
 Anderer Bereich: \_\_\_\_\_  
 Keine Angabe

**3. Wie groß ist Ihre Institution (Definition gemäß Institut für Mittelstandsforschung Bonn)?**

- Klein (< 10 Mitarbeiter)  
 Mittel (< 500 Mitarbeiter)  
 Groß (> 500 Mitarbeiter)  
 Keine Angabe

**4. Wo ist der Sitz Ihres Unternehmens/Ihrer Behörde?**

- Deutschland  
 Österreich  
 Schweiz  
 Sonstiges: \_\_\_\_\_  
 Keine Angabe

**5. Hat Ihr(e) Unternehmen/Behörde zusätzliche Standorte im Ausland (vom Sitz aus betrachtet)?**

- Ja  Nein  Keine Angabe

**6. Wie viele Mitarbeiter sind in Ihrer Institution für IT-Sicherheit und IT-Compliance tätig?**

	<i>IT-Sicherheit</i>	<i>IT-Compliance</i>
1 – 5 Mitarbeiter	<input type="checkbox"/>	<input type="checkbox"/>
5 – 10 Mitarbeiter	<input type="checkbox"/>	<input type="checkbox"/>
10 – 15 Mitarbeiter	<input type="checkbox"/>	<input type="checkbox"/>
Mehr als 15 Mitarbeiter	<input type="checkbox"/>	<input type="checkbox"/>
Keine Mitarbeiter	<input type="checkbox"/>	<input type="checkbox"/>
Keine Angabe	<input type="checkbox"/>	<input type="checkbox"/>

**7. Hat Ihre Institution IT-Sicherheitsziele definiert?**

- Ja  Geplant  Nein  Keine Angabe

**8. Wenn Ihre Institution IT-Sicherheitsrichtlinien definiert hat, in welchen Abständen werden diese angepasst?**

- Alle 1 – 3 Monate                       Alle 12 – 24 Monate                       Keine definiert  
 Alle 3 – 6 Monate                       Alle 24 – 48 Monate                       Keine Angabe  
 Alle 6 – 12 Monate                       Unregelmäßig

**B. Themenübergreifende Fragen**

**1. Wer ist in Ihrer Institution für folgende Aufgabenfelder zuständig (Mehrfachnennung möglich)?**

	<i>IT-Sicherheit</i>	<i>IT-Compliance</i>
Geschäftsführung/Vorstand/Amtsleitung	<input type="checkbox"/>	<input type="checkbox"/>
Aufsichtsrat	<input type="checkbox"/>	<input type="checkbox"/>
IT-Leiter/Rechenzentrumsleiter	<input type="checkbox"/>	<input type="checkbox"/>
IT-Administrator	<input type="checkbox"/>	<input type="checkbox"/>
Datenschutzbeauftragter/Datenschutzmanager	<input type="checkbox"/>	<input type="checkbox"/>
(IT-) Sicherheitsbeauftragter/(IT-) Security Manager/ (IT-) Sicherheitsmanager	<input type="checkbox"/>	<input type="checkbox"/>
(IT-) Governance Manager	<input type="checkbox"/>	<input type="checkbox"/>
(IT-) Risk Manager	<input type="checkbox"/>	<input type="checkbox"/>
(IT-) Compliance Manager	<input type="checkbox"/>	<input type="checkbox"/>
(IT-) Revisor	<input type="checkbox"/>	<input type="checkbox"/>
Nicht IT-Mitarbeiter	<input type="checkbox"/>	<input type="checkbox"/>
Andere Position:	_____	_____
Keine Angabe	<input type="checkbox"/>	<input type="checkbox"/>

**2. Wer ist die treibende Kraft für die Weiterentwicklung von IT-Sicherheit bzw. IT-Compliance (Mehrfachnennung möglich)?**

	<i>IT-Sicherheit</i>	<i>IT-Compliance</i>
Geschäftsführung/Vorstand/Amtsleitung	<input type="checkbox"/>	<input type="checkbox"/>
Aufsichtsrat	<input type="checkbox"/>	<input type="checkbox"/>
IT-Leiter/Rechenzentrumsleiter	<input type="checkbox"/>	<input type="checkbox"/>
IT-Administrator	<input type="checkbox"/>	<input type="checkbox"/>
Datenschutzbeauftragter/Datenschutzmanager	<input type="checkbox"/>	<input type="checkbox"/>
(IT-) Sicherheitsbeauftragter/(IT-) Security Manager/ (IT-) Sicherheitsmanager	<input type="checkbox"/>	<input type="checkbox"/>
(IT-) Governance Manager	<input type="checkbox"/>	<input type="checkbox"/>
(IT-) Risk Manager	<input type="checkbox"/>	<input type="checkbox"/>
(IT-) Compliance Manager	<input type="checkbox"/>	<input type="checkbox"/>
(IT-) Revisor	<input type="checkbox"/>	<input type="checkbox"/>
Nicht IT-Mitarbeiter	<input type="checkbox"/>	<input type="checkbox"/>
Andere Position:	_____	_____
Keine Angabe	<input type="checkbox"/>	<input type="checkbox"/>

**3. Welche Bedeutung haben folgende Bereiche in Ihrer Institution?**

	<i>IT-Sicherheit</i>	<i>IT-Compliance</i>
Sehr hoch	<input type="checkbox"/>	<input type="checkbox"/>
Hoch	<input type="checkbox"/>	<input type="checkbox"/>
Mittel	<input type="checkbox"/>	<input type="checkbox"/>
Niedrig	<input type="checkbox"/>	<input type="checkbox"/>
Sehr niedrig	<input type="checkbox"/>	<input type="checkbox"/>
Keine Angabe	<input type="checkbox"/>	<input type="checkbox"/>

**4. Wie wird sich die Bedeutung dieser Bereiche in Zukunft verändern?**

	<i>IT-Sicherheit</i>	<i>IT-Compliance</i>
Stark steigen	<input type="checkbox"/>	<input type="checkbox"/>
Steigen	<input type="checkbox"/>	<input type="checkbox"/>
Gleich bleiben	<input type="checkbox"/>	<input type="checkbox"/>
Sinken	<input type="checkbox"/>	<input type="checkbox"/>
Stark sinken	<input type="checkbox"/>	<input type="checkbox"/>
Keine Angabe	<input type="checkbox"/>	<input type="checkbox"/>

**5. Was benötigen Sie zur Optimierung der Bereiche IT-Sicherheit und IT-Compliance (Mehrfachnennung möglich)?**

	<i>IT-Sicherheit</i>	<i>IT-Compliance</i>
Mehr Personal	<input type="checkbox"/>	<input type="checkbox"/>
Qualifizierteres Personal	<input type="checkbox"/>	<input type="checkbox"/>
Mehr finanzielle Mittel	<input type="checkbox"/>	<input type="checkbox"/>
Bessere Softwareunterstützung	<input type="checkbox"/>	<input type="checkbox"/>
Wir sind mit der aktuellen Situation zufrieden	<input type="checkbox"/>	<input type="checkbox"/>
Sonstiges:	_____	_____
Keine Angabe	<input type="checkbox"/>	<input type="checkbox"/>

**6. Wie bewerten Sie gegenwärtig nachfolgende Aspekte in Ihrer Institution?**

	<i>IT-Sicherheit</i>	<i>IT-Compliance</i>
Sehr gut	<input type="checkbox"/>	<input type="checkbox"/>
Gut	<input type="checkbox"/>	<input type="checkbox"/>
Befriedigend	<input type="checkbox"/>	<input type="checkbox"/>
Ausreichend	<input type="checkbox"/>	<input type="checkbox"/>
Mangelhaft	<input type="checkbox"/>	<input type="checkbox"/>
Keine Angabe	<input type="checkbox"/>	<input type="checkbox"/>

**7. Wie ist die Akzeptanz der Fachabteilungen gegenüber laufenden Anpassungen bedingt durch IT-Sicherheit und IT-Compliance (z. B. Prozessanpassung)?**

	<i>IT-Sicherheit</i>	<i>IT-Compliance</i>
Sehr gut	<input type="checkbox"/>	<input type="checkbox"/>
Gut	<input type="checkbox"/>	<input type="checkbox"/>
Befriedigend	<input type="checkbox"/>	<input type="checkbox"/>
Ausreichend	<input type="checkbox"/>	<input type="checkbox"/>
Mangelhaft	<input type="checkbox"/>	<input type="checkbox"/>
Keine Angabe	<input type="checkbox"/>	<input type="checkbox"/>

**8. Wie schnell werden die Anforderungen von den Fachabteilungen bezüglich IT-Sicherheit und IT-Compliance umgesetzt?**

	<i>IT-Sicherheit</i>	<i>IT-Compliance</i>
Sehr schnell	<input type="checkbox"/>	<input type="checkbox"/>
Schnell	<input type="checkbox"/>	<input type="checkbox"/>
Mittel	<input type="checkbox"/>	<input type="checkbox"/>
Langsam	<input type="checkbox"/>	<input type="checkbox"/>
Sehr langsam	<input type="checkbox"/>	<input type="checkbox"/>
Keine Angabe	<input type="checkbox"/>	<input type="checkbox"/>

**9. Wie wird bei der Nichteinhaltung von IT-Sicherheits- und IT-Compliancevorgaben in Ihrer Institution vorgegangen (Mehrfachnennung möglich)?**

	<i>IT-Sicherheit</i>	<i>IT-Compliance</i>
Belehrung/Gespräch mit dem Vorgesetzten	<input type="checkbox"/>	<input type="checkbox"/>
Änderung von Prozessen	<input type="checkbox"/>	<input type="checkbox"/>
Verweigerung der Abnahme	<input type="checkbox"/>	<input type="checkbox"/>
Ausschluss bei der Auftragsvergabe	<input type="checkbox"/>	<input type="checkbox"/>
Abmahnung	<input type="checkbox"/>	<input type="checkbox"/>
Rechtliche Konsequenzen	<input type="checkbox"/>	<input type="checkbox"/>
Kürzungen (z. B. Rechnung)	<input type="checkbox"/>	<input type="checkbox"/>
Sonstiges:	_____	_____
Ist mir nicht bekannt	<input type="checkbox"/>	<input type="checkbox"/>
Keine Angabe	<input type="checkbox"/>	<input type="checkbox"/>

**10. Was sind aus Ihrer Sicht die größten Hindernisse des IT-Sicherheits- und IT-Compliance-Managements (Mehrfachnennung möglich)?**

	<i>IT-Sicherheit</i>	<i>IT-Compliance</i>
Probleme bei der technischen Realisierung	<input type="checkbox"/>	<input type="checkbox"/>
Probleme bei der fachlichen Implementierung	<input type="checkbox"/>	<input type="checkbox"/>
Probleme durch zu geringe Schulung der Mitarbeiter	<input type="checkbox"/>	<input type="checkbox"/>
Mangelnde Akzeptanz bei der Geschäftsleitung	<input type="checkbox"/>	<input type="checkbox"/>
Mangelnde Akzeptanz bei den Mitarbeitern	<input type="checkbox"/>	<input type="checkbox"/>
Sonstiges:	_____	_____
Keine Angabe	<input type="checkbox"/>	<input type="checkbox"/>

**11. Werden Sie bei der Umsetzung von Gesetzen/Regularien und Standards/Frameworks (z. B. ISO 27001/2) in folgenden Bereichen von Softwaretools unterstützt?**

		<i>IT-Sicherheit</i>	<i>IT-Compliance</i>
Ja	Eigenentwicklung, abteilungs-spezifisch	<input type="checkbox"/>	<input type="checkbox"/>
Ja	Eigenentwicklung, abteilungs-übergreifend	<input type="checkbox"/>	<input type="checkbox"/>
Ja	Fremdbezug, abteilungsspezifisch	<input type="checkbox"/>	<input type="checkbox"/>
Ja	Fremdbezug, abteilungsübergreifend	<input type="checkbox"/>	<input type="checkbox"/>
Geplant		<input type="checkbox"/>	<input type="checkbox"/>
Nein		<input type="checkbox"/>	<input type="checkbox"/>
Keine Angabe		<input type="checkbox"/>	<input type="checkbox"/>

**12. Worin sehen sie die Hauptgründe, wenn Sie bei der Umsetzung von Gesetzen/Regularien und Standards/Frameworks (z. B. ISO 27001/2) bisher von keinen Standardtools unterstützt werden (Mehrfachnennung möglich)?**

	<i>IT-Sicherheit</i>	<i>IT-Compliance</i>
Zu geringer Funktionsumfang von Standardlösungen	<input type="checkbox"/>	<input type="checkbox"/>
Fehlende Anbindungsmöglichkeit der Standardsoftware an vorhandene Informationssysteme	<input type="checkbox"/>	<input type="checkbox"/>
Eigene Fachabteilung für die Toolentwicklung im Haus vorhanden	<input type="checkbox"/>	<input type="checkbox"/>
Standardlösung zu teuer (z. B. Anschaffung, Anpassung)	<input type="checkbox"/>	<input type="checkbox"/>
Sonstiges:	_____	_____
Keine Angabe	<input type="checkbox"/>	<input type="checkbox"/>

## C. Themenspezifische Fragen zur IT-Sicherheit

### I. Themenspezifische Fragen zur IT-Sicherheit: Zertifizierung

#### 1. Nach welchen Standards bzw. IT-Frameworks richtet sich Ihre Institution?

	<i>Wird in unserer Institution nicht eingesetzt</i>	<i>Nicht zertifiziert, aber es wird nach dessen Vorga- ben gehandelt</i>	<i>Zertifizierung geplant</i>	<i>Zertifizierungs- prozess läuft</i>	<i>Zertifizierung vorhanden</i>
IT-Grundschutz	<input type="checkbox"/>	<input type="checkbox"/>			
ISO 27001 auf Basis von IT- Grundschutz*	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
ISO/IEC 27001/2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CobiT	<input type="checkbox"/>	<input type="checkbox"/>			
ITIL	<input type="checkbox"/>	<input type="checkbox"/>			
Sonstige: _____	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Keine Angabe:	<input type="checkbox"/>				

\* Für die Ausrichtung nach ISO 27001 auf Basis von IT-Grundschutz ist nur ein Teil der IT-Grundschutzmaßnahmen relevant.

#### 2. Falls Sie IT-Grundschutz in Ihrer Institution einsetzen: Wie hoch schätzen Sie die Qualität der Umsetzung der IT-Grundschutz-Bausteine in Ihrer Institution ein?

<i>(Struktur analog IT- Grundschutz)</i>	<i>nicht umgesetzt</i>	<i>sehr gering</i>	<i>gering</i>	<i>mittel</i>	<i>hoch</i>	<i>sehr hoch</i>
B1: Übergreifende As- pekte	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
B2: Infrastruktur	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
B3: IT-Systeme	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
B4: Netze	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
B5: Anwendungen	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Keine Angabe/ Nicht vorhanden	<input type="checkbox"/>					

#### 3. In welchem Zeitintervall überprüfen und passen Sie Ihre internen Sicherheitsanforderungen und Sicherheitsmaßnahmen hinsichtlich der Anforderungen aus den IT-Grundschutzkatalogen an?

- |  |   |
|--|---|
| <input type="checkbox"/> Permanent     | <input type="checkbox"/> Alle _____ Monate            |
| <input type="checkbox"/> Jährlich      | <input type="checkbox"/> Unregelmäßig                 |
| <input type="checkbox"/> Halbjährlich  | <input type="checkbox"/> Bei Bedarf                   |
| <input type="checkbox"/> Quartalsweise | <input type="checkbox"/> Vor einer Zertifizierung     |
| <input type="checkbox"/> Monatlich     | <input type="checkbox"/> Keine Angabe/Nicht vorhanden |

#### 4. Haben Sie ein Tool zur Vorbereitung auf die Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz verwendet?

- Ja, wir haben folgendes Standardtool eingesetzt: \_\_\_\_\_
- Ja, wir haben eine Eigenentwicklung eingesetzt
- Nein
- Keine Angabe/Nicht vorhanden

#### 5. Konnten Sie mit dem eingesetzten Tool Ihre Aufgaben hinsichtlich der Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz wie gewünscht durchführen?

- Ja
- Nein, wir hatten folgendes Hauptproblem: \_\_\_\_\_
- Keine Angabe/Nicht vorhanden

**6. Falls Sie ISO 27001/2 in Ihrer Institution einsetzen: Wie hoch schätzen Sie die Qualität der Umsetzung nachfolgend aufgeführter Kontrollziele und Maßnahmen in Ihrer Institution ein?**

<i>(Struktur analog ISO 27002:2005)</i>	<i>nicht umgesetzt</i>	<i>sehr gering</i>	<i>gering</i>	<i>mittel</i>	<i>hoch</i>	<i>sehr hoch</i>
<b>Security Policy</b> (z. B. Information Security Policy)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>Organization of Information Security</b> (z. B. Internal Organization, External Parties)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>Asset Management</b> (z. B. Responsibility for Assets, Information Classification)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>Human Resources Security</b> (z. B. Prior to Employment, During Employment)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>Physical Security Perimeter</b> (z. B. Secure Areas, Equipment Security)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>Communications and Operations Management</b> (z. B. Back-Up, Network Security Management, Monitoring, Media Handling)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>Access Control</b> (z. B. User Access Management, Application and Information Access Control)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>Information Systems Acquisition, Development and Maintenance</b> (z. B. Cryptographic Controls, Security of System Files)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>Information Security Incident Management</b> (z. B. Reporting Information Security Events and Weaknesses)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>Business Continuity Management</b> (z. B. Information Security Aspects of Business Continuity Management)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>Compliance</b> (z. B. Compliance with legal Requirements, Compliance with Security Policies and Standards, and technical Compliance)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Keine Angabe/Nicht vorhanden	<input type="checkbox"/>					

**7. In welchem Zeitintervall überprüfen und passen Sie Ihre internen Sicherheitsanforderungen und Sicherheitsmaßnahmen hinsichtlich der Anforderungen aus dem ISO 27001/2 Standard an?**

- |  |   |
|--|---|
| <input type="checkbox"/> Permanent     | <input type="checkbox"/> Alle _____ Monate            |
| <input type="checkbox"/> Jährlich      | <input type="checkbox"/> Unregelmäßig                 |
| <input type="checkbox"/> Halbjährlich  | <input type="checkbox"/> Bei Bedarf                   |
| <input type="checkbox"/> Quartalsweise | <input type="checkbox"/> Vor einer Zertifizierung     |
| <input type="checkbox"/> Monatlich     | <input type="checkbox"/> Keine Angabe/Nicht vorhanden |

**8. Haben Sie ein Tool zur Vorbereitung auf die Zertifizierung nach ISO 27001 verwendet?**

- Ja, wir haben folgendes Standardtool eingesetzt: \_\_\_\_\_
- Ja, wir haben eine Eigenentwicklung eingesetzt
- Nein
- Keine Angabe/Nicht vorhanden

**9. Konnten Sie mit dem eingesetzten Tool Ihre Aufgaben hinsichtlich der Anforderungen nach ISO 27001 wie gewünscht durchführen?**

- Ja
- Nein, wir hatten folgendes Hauptproblem: \_\_\_\_\_
- Keine Angabe/Nicht vorhanden

**10. Wie lange mussten Sie sich für die Zertifizierung vorbereiten?**

	ISO 27001 auf Basis von IT-Grundschutz	ISO 27001
0 – 3 Monate	<input type="checkbox"/>	<input type="checkbox"/>
4 – 8 Monate	<input type="checkbox"/>	<input type="checkbox"/>
8 – 12 Monate	<input type="checkbox"/>	<input type="checkbox"/>
Länger	<input type="checkbox"/>	<input type="checkbox"/>
Keine Angabe/Nicht vorhanden	<input type="checkbox"/>	<input type="checkbox"/>

**11. Wurden/Werden für die Vorbereitung zur Zertifizierung externe Partner beschäftigt?**

	ISO 27001 auf Basis von IT-Grundschutz	ISO 27001
Ja	<input type="checkbox"/>	<input type="checkbox"/>
Geplant	<input type="checkbox"/>	<input type="checkbox"/>
Nein	<input type="checkbox"/>	<input type="checkbox"/>
Keine Angabe/Nicht vorhanden	<input type="checkbox"/>	<input type="checkbox"/>

**12. Wenn für die Vorbereitung externe Partner beschäftigt wurden, waren Sie mit deren fachlicher Qualität zufrieden?**

	ISO 27001 auf Basis von IT-Grundschutz	ISO 27001
Ja	<input type="checkbox"/>	<input type="checkbox"/>
Nein	<input type="checkbox"/>	<input type="checkbox"/>
Keine Angabe/Nicht vorhanden	<input type="checkbox"/>	<input type="checkbox"/>

**13. Gibt es genügend zertifizierte Auditoren zur Unterstützung bei der (Re-) Zertifizierung?**

	ISO 27001 auf Basis von IT-Grundschutz	ISO 27001
Ja	<input type="checkbox"/>	<input type="checkbox"/>
Nein	<input type="checkbox"/>	<input type="checkbox"/>
Keine Angabe	<input type="checkbox"/>	<input type="checkbox"/>

**14. Wenn Sie CobiT in Ihrer Institution einsetzen: Wie hoch schätzen Sie den Reifegrad nachfolgender CobiT-Prozesse in Ihrer Institution ein?**

(Struktur analog CobiT 4.1)	nicht umgesetzt	sehr gering	gering	mittel	hoch	sehr hoch
<b>PO – Plan and Organize</b> (z.B. Define a Strategic IT Plan, Manage the IT Investment)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>AI – Acquire and Implement</b> (z.B. Enable operation and use, Procure IT Resources)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>DS – Deliver and Support</b> (z.B. Ensure Continuous Service, Identify and Allocate Costs)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

<b>ME – Monitor and Evaluate</b> (z.B. Ensure Compliance with External Requirements, Provide IT Governance)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>AC – Application Controls</b> (z.B. Source Data Preparation and Authorization, Processing Integrity and Validity)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>PC – Process Control</b> (z.B. Process Ownership, Process Performance Improvement)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Keine Angabe/Nicht vorhanden	<input type="checkbox"/>					

**15. In welchem Zeitintervall überprüfen und passen Sie Ihre internen Sicherheitsanforderungen und Sicherheitsmaßnahmen hinsichtlich der Anforderungen aus CobiT an?**

- Permanent
- Jährlich
- Halbjährlich
- Quartalsweise
- Monatlich
- Alle \_\_\_\_\_ Monate
- Unregelmäßig
- Bei Bedarf
- Vor einer Zertifizierung
- Keine Angabe/Nicht vorhanden

**16. Haben Sie ein Tool zur Umsetzung von CobiT eingesetzt?**

- Ja, wir haben folgendes Standardtool eingesetzt: \_\_\_\_\_
- Ja, wir haben eine Eigenentwicklung eingesetzt
- Nein
- Keine Angabe/Nicht vorhanden

**17. Konnten Sie mit dem eingesetzten Tool Ihre Aufgaben hinsichtlich CobiT wie gewünscht durchführen?**

- Ja
- Nein, wir hatten folgendes Hauptproblem: \_\_\_\_\_
- Keine Angabe/Nicht vorhanden

**II. Themenspezifische Fragen zur IT-Sicherheit: Anwendung**

**1. Welche Gründe haben/hatten Sie für den Einsatz nachfolgender Standards/IT-Frameworks (Mehrfachnennung möglich)?**

	<i>IT-Grundschutz</i>	<i>ISO 27001/2</i>	<i>CobiT</i>
Vorgabe durch Gesetz oder Regulierungs-institution	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Sicherheitsvorfall	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Geschäftspartner fordert die Umsetzung	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Verbesserung der Sicherheitslage	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Umsetzung als Voraussetzung für ein(en) Projekt/Auftrag	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Sonstiges: _____			
Keine Angabe/Nicht vorhanden	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**2. Seit wann verwenden Sie Konzepte aus nachfolgenden Standards/IT-Frameworks?**

	<i>IT-Grundschutz</i>	<i>ISO 27001/2</i>	<i>CobiT</i>
Seit _____	_____ Jahr(en)	_____ Jahr(en)	_____ Jahr(en)
Keine Angabe/Nicht vorhanden	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**3. Wie lange hat die Implementierung der Standards/IT-Frameworks gedauert?**

	<i>IT-Grundschutz</i>	<i>ISO 27001/2</i>	<i>CobiT</i>
0 – 3 Monate	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4 – 8 Monate	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8 – 12 Monate	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Länger	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Keine Angabe/Nicht vorhanden	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

#### 4. Hat sich die Sicherheitslage der Bereiche, die IT-Grundschutz, ISO 27001/2 oder CobiT anwenden, verbessert?

	IT-Grundschutz	ISO 27001/2	CobiT
Ja	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Nein	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Keine Angabe/Nicht vorhanden	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

#### 5. Haben/Werden Sie eine Awareness-Kampagne zur Informationssicherheit durchgeführt/durchführen? Wenn ja, wie hat sich dadurch die Sicherheitslage in Ihrer Institution verändert?

- Ja, verbessert                       Ja, unverändert                       Keine Angabe  
 Ja, verschlechtert                       Nein

#### 6. Nutzen Sie externe Dienstleister für Awareness-Kampagnen?

- Ja                                       Nein                                       Keine Angabe

#### 7. Erachten Sie die Einführung einer Qualifikation „Qualified IT-Grundschutz Expert (BSI)“ als sinnvoll?

- Ja                                       Nein                                       Keine Angabe

### III. Themenspezifische Fragen zur IT-Sicherheit: Rezertifizierung

#### 1. Planen Sie eine Rezertifizierung?

- Ja, ISO 27001 auf Basis von IT-Grundschutz                       Nein, keine Ressourcen in der Institution  
 Ja, ISO 27001     Nein, Nutzung eines anderen IT-Sicherheitsstandards  
 Nein, kein erwiesener Nutzen     Nein, Sonstiges: \_\_\_\_\_  
 Nein, zu hohe Kosten     Keine Angabe/Nicht zertifiziert

#### 2. Haben Sie bereits eine Rezertifizierung durchgeführt?

- Ja, ISO 27001 auf Basis von IT-Grundschutz                       Nein  
 Ja, ISO 27001     Keine Angabe/Nicht zertifiziert

#### 3. Wenn Sie bereits eine Rezertifizierung durchgeführt haben, wie viele Jahre liegt diese zurück?

- \_\_\_\_ Jahr(e)                                       Keine Angabe

#### 4. Wie lange nahm die Rezertifizierung in Anspruch?

- 0 – 2 Monate                                       Länger  
 3 – 6 Monate                                       Keine Angabe

#### 5. Wie empfanden Sie den Aufwand der Rezertifizierung im Vergleich zur Erstzertifizierung?

- Erheblich geringer                                       Gleich                                       Keine Angabe  
 Geringer     Höher

#### 6. Welche Punkte haben Sie bei der Rezertifizierung im Vergleich zur Erstzertifizierung am meisten gestört?

- Zeitaufwand     Mangelnde Tool-Unterstützung  
 Kosten     Intransparentes Vorgehen seitens der  
 Störung des Betriebsablaufs    Zertifizierungsstelle  
 Arbeitsweise des Auditors     Sonstiges: \_\_\_\_\_  
 Redundanz zur Zertifizierung     Keine Angabe

### D. Themenspezifische Fragen zu IT-Compliance

#### 1. Welche der folgenden Punkte konnten durch Ihr IT-Compliance-Management realisiert werden (Mehrfachnennung möglich)?

- Höhere Transparenz     Effektivitäts- und Effizienzeffekte bei der  
 Optimierung der Betriebsprozesse                                      Jahresabschlussprüfung  
 Reduzierung der Betriebskosten     Sonstige: \_\_\_\_\_  
 Reduzierung der Komplexität der IT-Infrastruktur                       Kann ich nicht beurteilen

**2. Haben Sie bereits ein Audit nach § 9 des Bundesdatenschutzgesetzes (BDSG) durchgeführt?**

- Ja  Nein

**3. Wie schätzen Sie die Qualität der Umsetzung nachfolgender Punkte des BDSG in Ihrer Institution ein?**

	Zutritts- kontrolle	Zugangs- kontrolle	Zugriffs- kontrolle	Weiter- gabekon- trolle	Eingabe- kontrolle	Auftrags- kontrolle	Verfüg- barkeits- kontrolle
Sehr gut	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Gut	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Befriedigend	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Ausreichend	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Mangelhaft	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Keine Angabe	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**4. Wie sollten die gesetzlichen Vorschriften angepasst werden, um dem Datenschutz in Ihrer Institution gerecht zu werden?**

- Die gesetzlichen Regelungen sollten verschärft werden  
 Die gesetzlichen Regelungen sind ausreichend  
 Institutionen sollten mehr Handlungsspielraum erhalten  
 Keine Angabe

**5. Sind die Mitarbeiter, welche für IT-Compliance zuständig sind, mit allen, für die IT Ihrer Institution maßgeblichen, Gesetzen und Regelungen vertraut?**

- Ja  Ist mir nicht bekannt  
 Nein  Keine Angabe

**6. Gibt es in Ihrer Institution einen Verantwortlichen für die Bekanntmachung von, für die IT relevanten, Gesetzesänderungen und Regelungen?**

- Ja  Ist mir nicht bekannt  
 Nein  Keine Angabe

**7. Hat Ihre Institution bereits finanzielle bzw. immaterielle Schäden aufgrund eines IT-Compliance-Verstoßes erlitten (z. B. Datenverlust)?**

- Ja, Höhe des Schadens in Euro: \_\_\_\_\_  Nein  
 Ja, kann nicht beziffert werden  Kann ich nicht beurteilen  
 Ja, Keine Angabe  Keine Angabe

**8. Existieren Scores zur Bewertung von Szenarien möglicher IT-Compliance-Verstöße?**

- Ja  Ist mir nicht bekannt  
 Nein  Keine Angabe

**9. Werden vom IT-Compliance-Management wiederkehrende Befragungen, Reviews oder andere Datenerhebungen initiiert und ausgewertet, um mögliche Verbesserungspotenziale zu identifizieren?**

- Ja  Ist mir nicht bekannt  
 Nein  Keine Angabe

**10. Gibt es bei Ihnen klare Regelungen für**

	Ja	Nein	Geplant	Keine Angabe
die E-Mail Archivierung	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
die Vorgehensweise beim Weggang von Mitarbeitern	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
das Datenmanagement	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**11. Welche Regelungen/Normen beanspruchen bei der Implementierung die meiste Zeit (Mehrfachnennung möglich)?**

- Rechtsnormen (z. B. Bundesdatenschutzgesetz)  Interne Regelwerke (z. B. Service Level Agreements, IT-Sicherheitsvorschriften)  
 Verträge (z.B. über den Austausch und die Aufbewahrung von Informationen)  Kann ich nicht beurteilen  
 Externe Regelwerke (z. B. CobiT, ISO 2700x, ITIL)  Keine Angabe

**12. Bei der Umsetzung welcher rechtlichen und regulativen Anforderungen treten die meisten Schwierigkeiten auf (Mehrfachnennung möglich)?**

- Abgabenordnung (AO)  
 Aktiengesetz (AktG)  
 Basel II/ Mindestanforderungen an das Risikomanagement (MaRisk)  
 Bilanz und Modernisierungsgesetz (BilMoG)  
 Datenschutzgesetze (z. B. BDSG)  
 Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)  
 Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (Digitale Steuerprüfung) (GDPdU)  
 Kreditwesengesetz (KWG)  
 Payment Card Industry Data Security Standard (PCI DSS)  
 Sarbanes-Oxley Act (SOX)  
 Telekommunikationsgesetz (TKG)  
 Umsatzsteuergesetz (UStG)  
 Wertpapierhandelsgesetz (WpHG)  
 Sonstige: \_\_\_\_\_  
 Keine Angabe

**13. Haben/Werden Sie nachfolgende IT-Compliance-Anforderungen in Ihrer Institution umgesetzt/umsetzen?**

	<i>MaRisk</i>	<i>PCI DSS</i>
<input type="checkbox"/> Ja	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Nein	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Geplant	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Keine Angabe/Nicht relevant	<input type="checkbox"/>	<input type="checkbox"/>

**14. Wenn Sie MaRisk in Ihrer Institution umgesetzt haben: Wie hoch schätzen Sie die Qualität der Umsetzung nachfolgender MaRisk-Anforderungen in Ihrer Institution ein?**

<i>Struktur analog MaRisk (Fassung vom 14.08.2009)</i>	<i>nicht umgesetzt</i>	<i>sehr gering</i>	<i>gering</i>	<i>mittel</i>	<i>hoch</i>	<i>sehr hoch</i>
<b>AT1 Vorbemerkung</b>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>AT2 Anwendungsbereich</b> (z.B. Anwenderkreis, Risiken)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>AT3 Gesamtverantwortung der Geschäftsleitung</b>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>AT4 Allgemeine Anforderungen an das Risikomanagement</b> (z.B. Risikotragfähigkeit, Strategie)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>AT5 Organisationsrichtlinien</b>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>AT6 Dokumentation</b>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>AT7 Ressourcen</b> (z.B. Personal, Notfallkonzept)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>AT8 Aktivitäten in neuen Produkten oder auf neuen Märkten</b>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>AT9 Outsourcing</b>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>BT1 Besondere Anforderungen an das interne Kontrollsystem</b>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>BT0 Anforderungen an die Aufbau- und Ablauforganisation</b> (z.B. Kreditgeschäft, Handelsgeschäft)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>BTR Anforderungen an die Risiko- steuerungs- und -controllingprozesse</b> (z.B. Adressausfallrisiken, Marktpreisrisiken)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>BT2 Besondere Anforderungen an die Ausgestaltung der internen Revision</b> (z.B. Aufgaben der internen Revision, Berichtspflicht)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Keine Angabe/Nicht relevant	<input type="checkbox"/>					

**15. Wenn Sie PCI DSS in Ihrer Institution umgesetzt haben: Wie hoch schätzen Sie die Qualität der Umsetzung nachfolgender PCI DSS-Anforderungen in Ihrer Institution ein?**

Analog zu PCI DSS ( Version 1.2, Oktober 2008)	nicht umgesetzt	sehr gering	gering	mittel	hoch	sehr hoch
<b>Requirement 1:</b> Install and maintain a firewall configuration to protect cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>Requirement 2:</b> Do not use vendor-supplied defaults for system passwords and other security parameters	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>Requirement 3:</b> Protect stored cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>Requirement 4:</b> Encrypt transmission of cardholder data across open, public networks	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>Requirement 5:</b> Use and regularly update anti-virus software or programs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>Requirement 6:</b> Develop and maintain secure systems and applications	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>Requirement 7:</b> Restrict access to cardholder data by business need to know	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>Requirement 8:</b> Assign a unique ID to each person with computer access	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>Requirement 9:</b> Restrict physical access to cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>Requirement 10:</b> Track and monitor all access to network resources and cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>Requirement 11:</b> Regularly test security systems and processes	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>Requirement 12:</b> Maintain a policy that addresses information security for employees and contractors	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Keine Angabe/Nicht relevant	<input type="checkbox"/>					

**Teilnahme**

Die Teilnahme ist nicht vom Kauf oder Abonnement der Zeitschrift Informationsdienst IT-Grundschutz abhängig. **Alle Teilnehmer erhalten die kompletten Auswertungsergebnisse der Studie.**

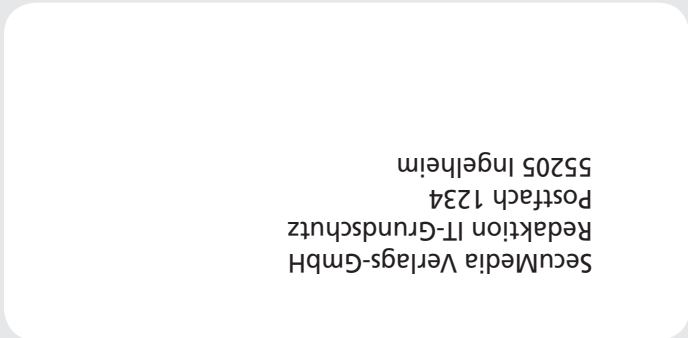
Sie können den Fragebogen aus dem Heft heraustrennen oder fotokopieren. Auf [www.grundschutz.info/studie](http://www.grundschutz.info/studie) liegt eine PDF-Version des Fragebogens zum Download bereit und alternativ führt ein Link auf unser Online-Webformular.

Behalten Sie bitte eine Kopie ihres ausgefüllten Fragebogens. Sie dient Ihnen zum Vergleich mit der Gesamtauswertung und als Checkliste des eigenen Sicherheits-Levels.  
**Einsendeschluss: 15. Juli 2010**

**Wir garantieren absolute Vertraulichkeit.** Unmittelbar nach Eingang trennen wir den Coupon mit Ihrem Dankeschön-Geschenkwunsch vom Fragebogen. Nur der Frageteil geht direkt und ohne Kennzeichnung zur Auswertung. Nach dem Erfassen werden die eingesandten Bögen vernichtet.

**Sollten Sie die Anonymität selbst sicherstellen wollen, können Sie Coupon und Fragebogen auch getrennt einsenden.**

Falls Sie trotz allem befürchten, dass Ihnen eine korrekte Antwort auf bestimmte Fragen oder Fragenteile schaden könnte, streichen Sie bitte die entsprechende Alternative oder Frage großflächig durch. Dies liefert uns bei der Auswertung wertvolle Hinweise auf problematische Fragen.




---



---



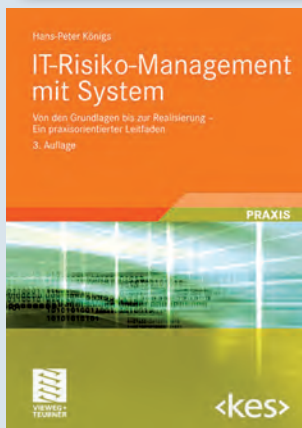
---



---

Absender:

# Ihre „Dankeschön-Prämien“ zur Auswahl



## Ich bin Teilnehmer der Studie „IT-Sicherheitsstandards und IT-Compliance 2010“

### Ich wünsche mir als Dankeschön\*

- Buch „Lieber ein Optimist“
- Buch „Erfolg ist leicht“
- Ganzheitliches Management der Informationssicherheit
- Der IT Security Manager
- Profikurs Sicherheit von Web-Servern
- Security Awareness Mitarbeiter-Sensibilisierung
- IT-Risiko-Management mit System
- IT-Sicherheitsmanagement nach ISO 27001 u. Grundschutz
- Datenschutz kompakt u. verständlich

\*(bitte nur ein Geschenk ankreuzen), Versand erfolgt solange Vorrat reicht

### Bitte einsenden an:

Redaktion Informationsdienst IT-Grundschutz,  
Postfach 1234, 55205 Ingelheim

Bitte schicken Sie die Auswertungen und mein Teilnahme-  
geschenk an folgende Anschrift:

\_\_\_\_\_  
Firma / Behörde

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

\_\_\_\_\_  
Straße / Postfach

\_\_\_\_\_  
Land / PLZ / Wohnort

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

# Wege zum digitalen Schlagbaum, Teil 3

## Datenschutz im IT-Verfahren ATLAS

Dr. Talke Ovie, Rechtsanwälte Möllenhoff, Münster

Unternehmen werden in Zukunft die Zollabwicklung elektronisch vornehmen müssen.

In Deutschland wird die elektronische Zollabwicklung durch das IT-Verfahren ATLAS umgesetzt.

Im letzten Teil der dreiteiligen Serie geht es um die Frage, welchen Voraussetzungen der Datenschutz im IT-Verfahren ATLAS unterliegt und die Kontrolle ob diese eingehalten werden.

Mit dem Zollgeheimnis in Art. 15 Zollkodex (ZK) besitzt das europäische Zollrecht eine eigenständige Regelung zum Schutz von Informationen, an welche die Zollverwaltung bei der Ausübung ihrer Tätigkeiten gelangt ist. Eines Schutzes von Informationen bedarf es, weil bei der Zollabwicklung ein einseitiger Informationsaustausch zwischen Wirtschaftsbeteiligten und Zollbehörden stattfindet. Ein

einseitiger Informationsaustausch ist auch im IT-Verfahren ATLAS gegeben, weil der Wirtschaftsbeteiligte nach Art. 14 ZK zur Abgabe von Informationen verpflichtet ist. Diese generelle Pflicht zur Abgabe von Informationen konkretisiert sich in Art. 59 ZK. Dort ist geregelt, dass die Wirtschaftsbeteiligten verpflichtet sind, zur Überführung einer Ware in ein Zollverfahren eine Zollanmeldung abzugeben. Diese

Zollanmeldung enthält weitgehende Informationen über die Ware, über die an der Einfuhr beteiligten Personen und über den Vorgang der Einfuhr an sich.

Unter das Zollgeheimnis fallen alle Angaben, die ihrer Natur nach vertraulich sind. Alle Inhaltsdaten, die im IT-Verfahren ATLAS in elektronischen Zollanmeldungen vom Zollanmelder abgegeben werden, stellen solche Angaben vertrauli-

## Hier abonnieren



## IT-Grundschutz

### Diese Leser profitieren vom Informationsdienst IT-Grundschutz

- IT-Leiter
- Administratoren
- Sicherheitsbeauftragte
- Bezieher der IT-Grundschutzkataloge
- Datenschutzbeauftragte
- IT-Security-Officer zum schnellen Überblick und zur Weitergabe an Geschäftsleitung, IT-Leitung oder Administratoren.
- Für die Sicherheits-Verantwortlichen in Behörden und mittelständischen Unternehmen, in denen es keinen speziellen IT-Security-Officer gibt

Der Informationsdienst „IT-Grundschutz“ ist eine ideale aktuelle Ergänzung zu den IT-Grundschutz-Katalogen. Der monatlich erscheinende Informationsdienst liefert Neues zu Rechtsprechung, Technik, Anwendungen und Trend-Themen - leicht verständlich und praxisnah.

### Abonnement-Bestellung an Fax +49 6725 5994

**Ja, ich abonniere bis auf Widerruf den Informationsdienst „IT-Grundschutz“ ab Ausgabe \_\_\_\_\_ zum Jahresbezugspreis (10 Ausgaben, davon 2 Doppelausgaben) von 98,00 € (Inland) / 116,10 € (Ausland) inkl. MwSt. und Versandkosten (Schweiz: 187,00 SFr).**

Ich kann das Abonnement jederzeit kündigen. Zuviel bezahlte Abo-Gebühren werden rückerstattet. Ich bin damit einverstanden, dass die Deutsche Post AG eine eventuell geänderte Anschrift weiterleiten kann.

Absender / Firmenstempel \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

## SecuMedia

Der Verlag für Sicherheits-Informationen

SecuMedia Verlag  
Postfach 12 34, 55205 Ingelheim  
vertrieb@secumedia.de  
Tel. +49 6725 9304-0

Datum                      Zeichen                      Unterschrift

© SecuMedia Verlags-GmbH · D-55205 Ingelheim · IT-Grundschutz 2010/5-6

Die SecuMedia Verlags GmbH räumt mir das Recht ein, diese Bestellung innerhalb 14 Tagen ab Bestelldatum zu widerrufen.