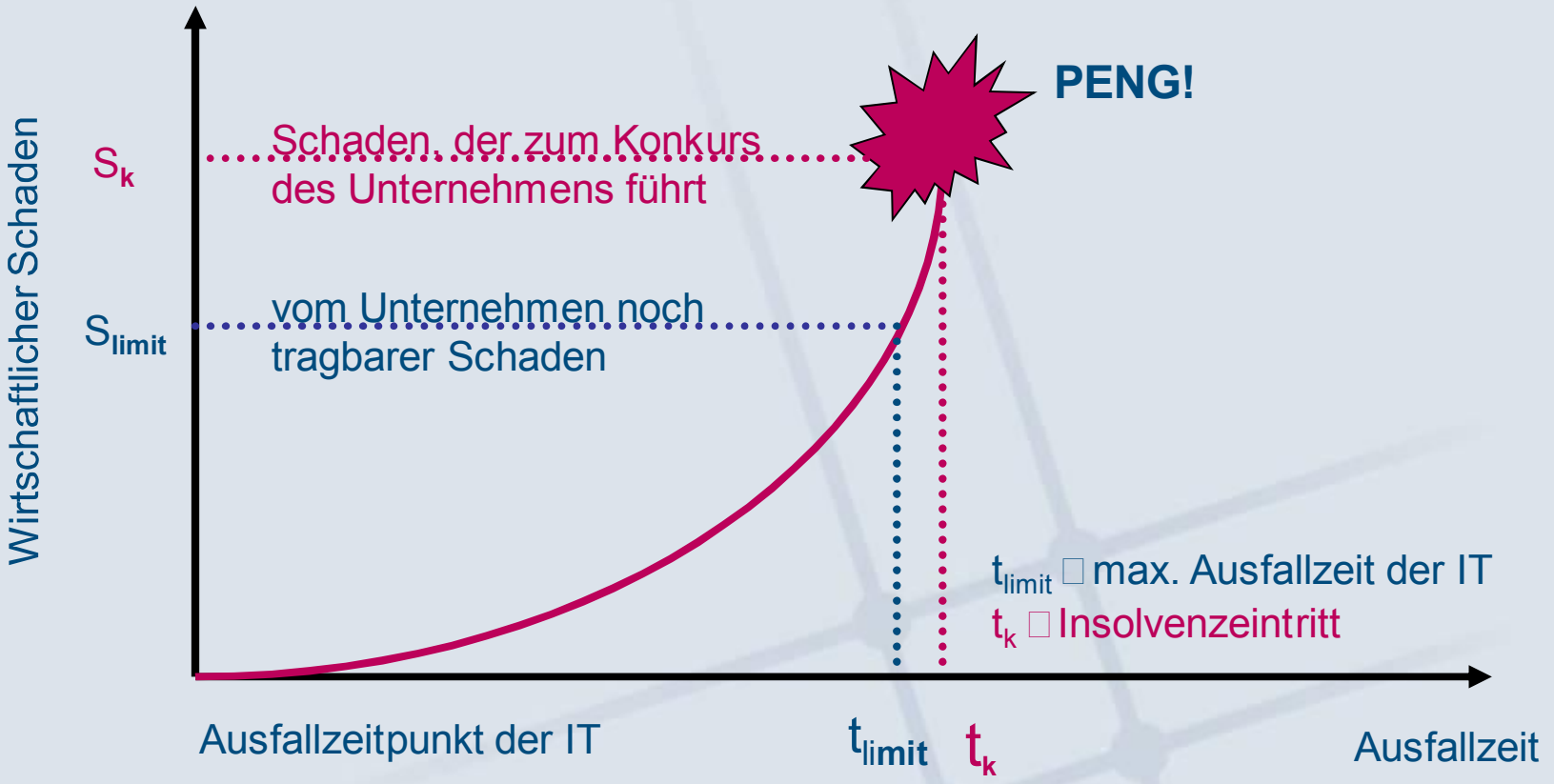
accuris®
Informationssicherheit & Datenschutz

Schon mal an den Notfall gedacht?

Vorgaben und Handlungs-Empfehlungen zur IT-Notfallvorsorge

accuris AG, Agnes-Pockels-Bogen 1, 80992 München, Tel. + 49 (0) 89.903.40 00 Fax. +49 (0) 89.900.19 373, office@accuris.de, www.accuris.de

Wozu IT-Notfallvorsorge?



IT-Notfallvorsorge = Schadensvorbeugung bzw. -minimierung

accuris AG, Agnes-Pockels-Bogen 1, 80992 München, Tel. + 49 (0) 89.903.40 00 Fax. +49 (0) 89.900.19 373, office@accuris.de, www.accuris.de

Vorgaben zum Notfallmanagement

accuris®
Informationssicherheit & Datenschutz

Vorgaben nach ISO 27001

ISO 27001 – Information Security Management System
Seit Oktober 2005 international verbindliche Norm zur Einführung eines IT-Sicherheitsmanagementsystems im Unternehmen,
ISO 27001 enthält die folgenden Vorgaben:

- A.5 Sicherheitspolitik
- A.6 Organisation der IT-Sicherheit
- A.7 Asset Management
- A.8 Personal Sicherheit
- A.9 Physische Sicherheit
- A.10 Management der Kommunikation und des Betriebs
- A.11 Zugangs- und Zugriffskontrolle
- A.12 Anschaffung, Entwicklung und Wartung der IT-Systeme
- A.13 Management von IT-Sicherheitsvorfällen
- A.14 Business Continuity Management
- A.15 Einhaltung von Normen und Verpflichtungen (Compliance)

accuris®
Informationssicherheit & Datenschutz

Business Continuity Management nach ISO 27001

Maßnahmen nach Anhang A der Norm

- A 14.1.1. Integration der IT-Security in den Business Continuity Management Prozess
- A 14.1.2. Business Continuity und Risikobetrachtung/-analyse
- A 14.1 3. Entwicklung und Einführung von Geschäftsfortführungsplänen unter Berücksichtigung der IT-Securityaspekte
- A 14.1.4 Business Continuity Planung
- A 14.1.5 Test, Aufrechterhaltung und Überprüfung der Business Continuity Pläne

Vorgaben zum Notfallmanagement

accuris®
Informationssicherheit & Datenschutz

Vorgaben nach IT-Grundschutz des BSI

- Erstellung einer Übersicht über Verfügbarkeitsanforderungen
- Notfall-Definition, Notfall-Verantwortlicher
- Erstellung eines Notfall-Handbuchs
- Dokumentation der Kapazitätsanforderungen der IT-Anwendungen
- Definition des eingeschränkten Betriebs
- Untersuchung interner und externer Ausweichmöglichkeiten
- Regelung der Verantwortlichkeit im Notfall
- Alarmierungspläne
- Notfallpläne für ausgewählte Schadensereignisse
- Wiederanlaufplan
- Durchführung von Notfallübungen
- Datensicherungsplan
- Ersatzbeschaffungsplan
- Redundanzen

Seit 2007: eigener BSI-Standard 100-4 zur Einführung und Aufrechterhaltung eines IT-Notfallmanagements

accuris®
Informationssicherheit & Datenschutz

Vorgaben nach IDW-Checkliste für den Notbetrieb

(Gliederungspunkte sind Abschnitte in der IDW-Checkliste)

4.5.1. Gibt es ein Notfallkonzept, das regelt, durch welche Maßnahmen □ ?

- Maßnahmen für den Notbetrieb
- Analyse der Geschäftsprozesse

4.5.2. Klassifizierung der Systeme nach ihrer Wichtigkeit für den Geschäftsbetrieb

- Ausweichszenarien
- Konfiguration der Notfallsysteme
- Festlegung von Verantwortlichkeiten
- Alarmierungspläne für Mitarbeiter
- Ansprechpartner von IT-Dienstleistern und Lieferanten
- Datensicherungs- und Wiederanlaufverfahren

4.5.3. Nachvollziehbare Dokumentation der Entwicklung und Wartung der Wiederanlaufprozeduren

4.5.4. Regelmäßiger Test und Überprüfung der Notfall-Lösungen und des Wiederanlaufs innerhalb der definierten Zeit

accuris®
Informationssicherheit & Datenschutz

Maßnahmen zur IT-Notfallvorsorge

1. Planung und Konzeption zur Notfallvorsorge
- Durchführung einer Risikoanalyse (nach BSI 100-3)
- Definition einer Notfallmanagementstrategie
- Erstellung eines Notfallvorsorgekonzepts

2. Erstellung eines Notfallhandbuchs zur Notfallbewältigung
- Sofortmaßnahmen
- Wiederanlauf
- Geschäftsfortführung
- Wiederherstellung
- Rückführung in den Normalbetrieb
- Aufarbeitung, Nachbereitung, Analyse

Handlungsempfehlungen zur IT-Notfallvorsorge

accuris®
Informationssicherheit & Datenschutz

3. Etablierung der Notfallvorsorgemaßnahmen
- Realisierung bzw. Umsetzung der Notfallmaßnahmen
- Schulung und Sensibilisierung der Mitarbeiter

4. Planung und Durchführung von Notfallübungen und Tests

5. Permanente Aufrechterhaltung
- Permanente Aktualisierung der Notfallpläne und des Notfallhandbuchs
- Regelmäßige Überprüfung der Notfallmaßnahmen auf Wirksamkeit
- Kontinuierliche Verbesserungen auf Basis der Ergebnisse aus den Überprüfungen und Tests

Checkliste IT-Notfallvorsorge

accuris®
Informationssicherheit & Datenschutz

- Unterscheidung IT-Ausfall / Notfall
- Regelung der Verantwortung im Notfall
- Notfallentscheidungsweg
- Notfall-Alarmierungspläne, Notrufnummern
- IT-Notfallhandbuch erstellen und regelmäßig überprüfen
- Notfallpläne für ausgewählte Schadensereignisse erstellen und regelmäßig überprüfen
- Verfügbarkeitsanforderungen unter Berücksichtigung interner und externer Anforderungen (Kundenanforderungen berücksichtigen)
- Festlegung max. zulässiger Ausfallzeiten
- Desaster Recovery Konzept für die geschäftskritischen Anwendungen
- Datensicherungsplan
- Wiederanlaufplan
- Festlegung des eingeschränkten Betriebs
- Liste der Kapazitätsanforderungen an die IT-Systeme
- Ersatzbeschaffungsplan
- Durchführung von Notfallübungen

accuris AG, Agnes-Pockels-Bogen 1, 80992 München, Tel. + 49 (0) 89.903.40 00 Fax. +49 (0) 89.900.19 373, office@accuris.de, www.accuris.de