IT Risikomanagement

@-yet GmbH
Schloß Eicherhof
42799 Leichlingen

Tel.: 02175/1655-0
Fax: 02175/1655-11
e-mail: info@add-yet.de

IT-Risikomanagement

KonTraG und Basel II machen IT zur Chefsache

Unternehmensrisiken genau zu kalkulieren und abzuschätzen, gehört heute zu den zentralen Aufgaben von Firmenlenkern. Denn durch Globalisierung, Wettbewerb und Rationalisierung (Just-in-Time-Produktion) haben die kritischen Unsicherheiten in den letzten Jahren rasant zugenommen.

Gesetzliche Verpflichtungen: z.B. KonTraG

Bereits 1998 wurden Aktiengesellschaften (heute auch mittelständische Unternehmer) durch das Kontroll- und Transparenzgesetz, kurz KonTr*aG, angewiesen, ihre Geschäftstätigkeiten besser abzusichern. Wer seine Pflichten vernachlässig, kann durch Schadensersatzzahlungen haftbar gemacht werden.

Laut KonTraG müssen Firmenlenker die Risiken interner wie externer Geschäftsprozesse reduzieren und Risikomanagement-Systeme einführen. Sicherheit und Verfügbarkeit der IT haben dabei eine hohe Priorität.

Finanztechnische Rahmenbedingungen: z.B. Basel II

Eine wichtige Verbindlichkeit ergibt sich auch aus der neuen „Eigenkapitalhinterlegungsrichtlinie Basel II" (gilt ab 2006, ist aber heute schon relevant.) Beschlossen von dem internationalen Banken-Konsortium sieht diese Regelung vor, dass Unternehmer auch ihre operativen Risiken mit Eigenkapital hinterlegen müssen.

Anhand von Basel II entscheiden Banken bei der Kreditvergabe auf Basis von Ratings. Schlechte Bewertungen verteuern Kredite und schmälern den Kreditrahmen für Unternehmen. Mit bis zu 20 % fließt die Qualität der IT in ein Rating ein (abhängig von der Bedeutung der IT in der Geschäftsabwicklung.)

Rolle der IT

Die Informationstechnologie ist wichtiger Bestandteil im Risikomanagement und hat nun tatsächlich die prognostizierte Rolle als Produktionsfaktor übernommen: Es gibt kaum noch einen Geschäftsprozess, der heute nicht durch IT unterstützt wird. Auch die Kommunikation ohne IT ist nur noch schwer vorstellbar.

Der Gesetzgeber und die Finanzwelt tragen diesem Umstand zunehmend Rechnung und verpflichten Unternehmen und Unternehmer, auch die IT in das Risikomanagement mit einzubeziehen.

@-yet IT-Risikomanagement

@-yet bietet professionelles IT-Risikomanagement auf Basis der gesetzlichen und finanztechnischen Rahmenbedingungen.
Als erfahrener IT-Dienstleister unterstützt @ yet seine Kunden,

- die IT-Risiken zentraler Geschäftsprozesse zu analysieren und zu beheben,
- Anwendungen samt Daten abzusichern und
- ein effektives IT-Kontroll-System aufzubauen.

In seinem Vorgehen berücksichtigt @-yet die Anforderungen aus KonTraG und Basel II.

@-yet Bausteine des IT-Risikomanagement:

1. Risikoanalyse:

Realistische Einschätzung der Gefahren auf organisatorischer und technischer Ebene erarbeiten. Risiken anwendungsbezogen identifizieren und aus technischer Sicht bewerten:

- ***IT Infrastruktur Design:***
  Analyse des Gesamtdesigns der IT Struktur, wie Data Center, Network, Releasestände.
- ***IT Implementierung:***
  Qualität der Implementierung und anderen Konsisten.
- ***IT Operations:***
  Transparenz und Sicherheit der Betriebsprozesse feststellen.

2. Verfügbarkeitsanalyse:

IT-Infrastruktur analysieren und bewerten; Maßnahmen für die Absicherung von Ausfällen und Notfall-Pläne prüfen.

- ***Strategien und Umsetzung entwickeln***
- ***Anwendungsverfügbarkeit:***
  Optimierung der Server- und Anwendungs-Infrastruktur.
- ***Datenverfügbarkeit:***
  Ausbau bestehender und Entwicklung neuer Storage- und Backup-Konzepte - für sichere und verfügbare Daten.
- ***Kommunikation:***
  Den Datenaustausch über Netze wie LAN, WAN, SAN sicherstellen und an die Verkehrsdichte anpassen.
- ***System Management:***
  Implementierung angemessener Werkzeuge und Methoden zur proaktiven Überwachtung und Trendanalyse der IT Systeme.

3. Sicherheitsanalyse:

Vertraulichkeit von Informationstransfers und Datensicherung bewerten; Werkzeuge wie Authentifizierung oder Richtlinien zur sicheren Zusammenarbeit etablieren.

- ***Security Scan:***
  IT-Systeme auf Sicherheitsrisiken prüfen, sie benennen und einschätzen.
- ***Security Audit:***
  Technik und Organisation und deren Zusammenspiel auf Sicherheitsrisiken prüfen, benennen, einordnen
- ***Security Konfiguration:***
  Implementierung der notwendigen Sicherheitslösungen im organisatorischen Bereich und der IT.

@ -yet GmbH
Schloß Eicherhof
42799 Leichlingen

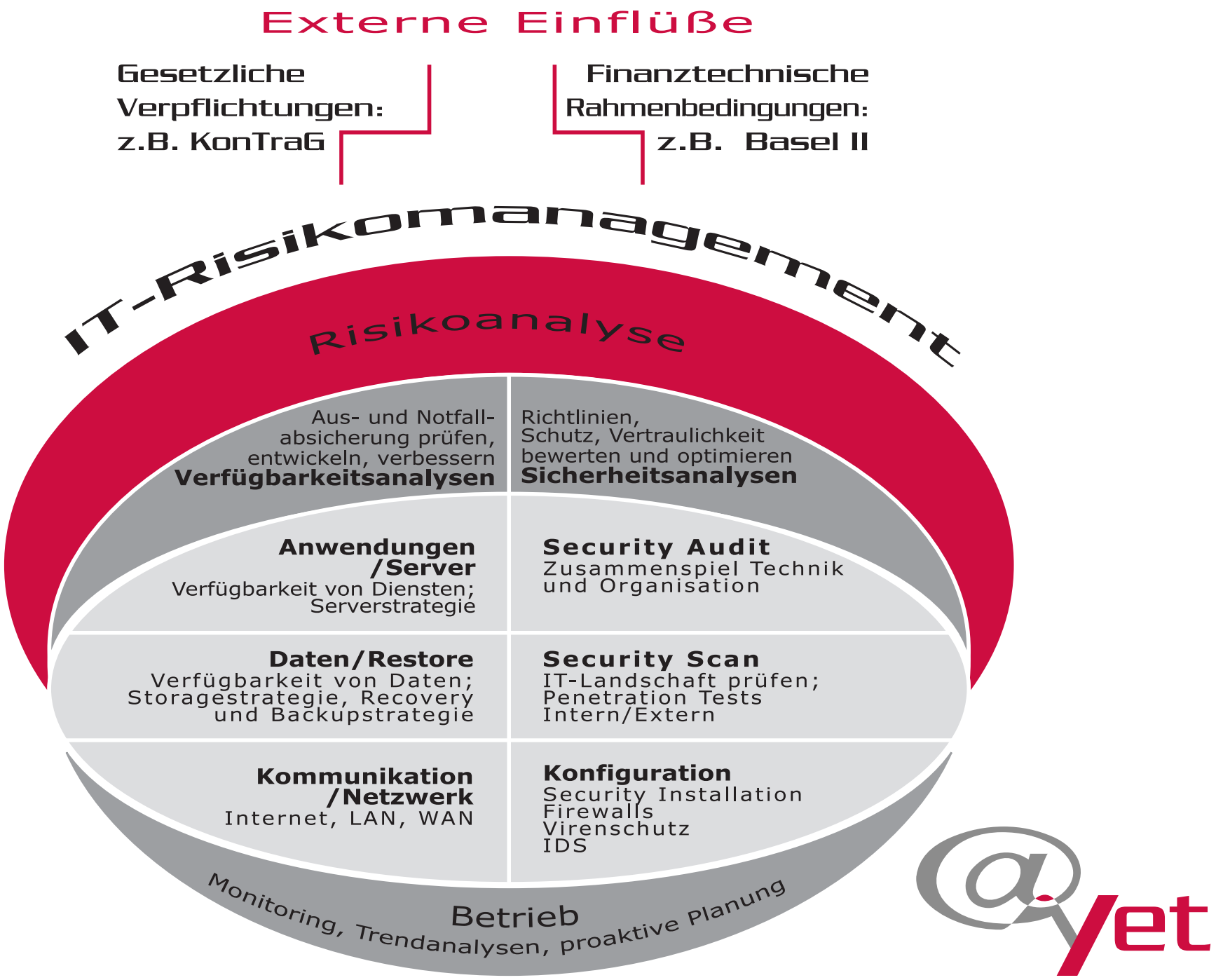
Tel.: 02175/1655-0
Fax: 02175/1655-11
e-mail: info@add-yet.de

Externe Einflüße

Gesetzliche Verpflichtungen: z.B. KonTraG

Finanztechnische Rahmenbedingungen: z.B. Basel II

@yet


Externe Einflüße
Gesetzliche Verpflichtungen: z.B. KonTraG
Finanztechnische Rahmenbedingungen: z.B. Basel II
IT-Risikomanagement
Risikoanalyse
Aus- und Notfall-absicherung prüfen, entwickeln, verbessern
Verfügbarkeitsanalysen
Richtlinien, Schutz, Vertraulichkeit bewerten und optimieren
Sicherheitsanalysen
Anwendungen /Server
Verfügbarkeit von Diensten; Serverstrategie
Security Audit
Zusammenspiel Technik und Organisation
Daten/Restore
Verfügbarkeit von Daten; Storagestrategie, Recovery und Backupstrategie
Security Scan
IT-Landschaft prüfen; Penetration Tests Intern/Extern
Kommunikation /Netzwerk
Internet, LAN, WAN
Konfiguration
Security Installation
Firewalls
Virenschutz
IDS
Betrieb
Monitoring, Trendanalysen, proaktive Planung
@yet