UNIVERSITÄT
KOBLENZ · LANDAU
Institut für Wirtschafts-
und Verwaltungsinformatik

FB 4
Informatik

Begriffsbestimmung und erwartete Trends im IT-Risk-Management Eine Delphi-Studie

Anastasia Meletiadou
J. Felix Hampe

Nr. 1/2007

Arbeitsberichte aus dem Fachbereich Informatik

Universität Koblenz-Landau • Campus Koblenz • Universitätsstraße 1 • 56070 Koblenz
Telefon +49 261 287-0 • http://www.uni-koblenz.de

Arbeitsberichte des Fachbereichs Informatik

I**SSN:** 1864-0346

Herausgeber / Edited by:

Der Dekan:
Prof. Dr. Paulus

Die Professoren des Fachbereichs:
Prof. Dr. Bátori, Jun.-Prof. Dr. Beckert, Prof. Dr. Burkhardt, Prof. Dr. Diller, Prof. Dr. Ebert, Prof. Dr. Furbach, Prof. Dr. Grimm, Prof. Dr. Hampe, Prof. Dr. Harbusch, Jun.-Prof. Dr. Hass, Prof. Dr. Krause, Prof. Dr. Lautenbach, Prof. Dr. Müller, Prof. Dr. Oppermann, Prof. Dr. Paulus, Prof. Dr. Priese, Prof. Dr. Rosentahl, Prof. Dr. Schubert, Prof. Dr. Staab, Prof. Dr. Steigner, Prof. Dr. Troitzsch, Priv.-Doz. Dr. von Kortzfleisch, Prof. Dr. Walsh, Prof. Dr. Wimmer, Prof. Dr.Zöbel

Kontaktdaten der Verfasser

Anastasia Meletiadou, J. Felix Hampe
Institut für Wirtschafts- und Verwaltungsinformatik
Fachbereich Informatik
Universität Koblenz-Landau
Universitätsstraße 1
D-56070 Koblenz
EMail: nancy@uni-koblenz.de, hampe@uni-koblenz.de

Inhaltsverzeichnis

Zusammenfassung

IT-Risk-Management ist ein Bereich, der in den letzten 2 Jahren stark diskutiert und sich verändert hat. Die Anlässe findet man sowohl in den terroristischen Überfällen und entsprechenden Konsequenzen für Unternehmen als auch an die Naturkatastrophen oder Fehlinvestitionen und undurchsichtigen Geschäfte mancher Unternehmen. Daher wurden Richtlinien und Gesetze entworfen, die Vorstände verpflichten, das eigene Unternehmen gegen konkrete Risiken zu schützen. Der Detaillierungsgrad der Vorschläge ist je nach Bereich unterschiedlich.

Sind aber Unternehmen bereit, die hohen Investitionen, die mit solchen umfangreichen Projekten zusammenhängen, auf sich zu nehmen um diese Richtlinien zu verfolgen? Wo sehen sie die Vorteile einer IT-Risk-Management-Strategie und wo die Herausforderungen? Welche Entwicklungen oder Veränderung wünschen sie sich? Das sind Fragen, die in der vorliegenden Studie, Experten des Bereich IT-Risk-Management gestellt wurden um die Zukunft des IT-Risk-Managements beeinflussen zu können.

Diese Fragestellungen wurden in der vorliegenden Studie untersucht, dazu haben wir Experten des Bereichs IT-Risk-Managements mit Hilfe der Delphi-Methode befragt. Der vorliegende Bericht fasst die wichtigsten Ergebnisse zusammen.

Einleitung

Zunehmende Bedeutung der IT-Infrastruktur

Durch die wachsende Komplexität der Infrastruktur und die steigende Abhängigkeit der Geschäftprozesse von dieser Infrastruktur gewinnt die IT als erfolgskritischer Wettbewerbsfaktor immer mehr an Bedeutung. Um direkte Schäden (verlorene Aufträge, gefährdete Liquidität) oder indirekte materielle Schäden (Vertrauens- und Imageverlust) für das Unternehmen zu vermeiden, muss daher die Zuverlässigkeit und Sicherheit der IT-Infrastruktur gewährleistet werden.

Dieser zunehmenden Bedeutung der IT trägt inzwischen auch die Gesetzgebung in Deutschland und Europa Rechnung, indem Sie entsprechende Maßnahmen einfordert, die helfen sollen, Ereignisse mit großen oder unberechenbaren negativen Auswirkungen vorbeugend zu verhindern. (Bundesamt für Sicherheit in der Informationstechnik 2003)

IT-bezogene Risiken

In all diesen Bereichen treten IT-bezogene Risiken auf: So sind im IT-Management eine unvollständige IT-Sicherheitsstrategie, die Nicht-Einhaltung rechtlicher Rahmenbedingungen oder die falsche Handhabung von Regelungszusammenhängen (Policies) als Gefahren zu nennen. Im Bereich der Organisation und Mitarbeiter können beispielsweise die mangelnde Zuordnung von Verantwortlichkeiten oder fehlende Information und mangelndes Bewusstsein der Mitarbeiter über die aktuellen Sicherheitsrichtlinien Risiken darstellen. Auf der Ebene von Technik und Infrastruktur ist etwa an fehlerhafte technische Schutzmassnahmen vor Zugriffen von außen oder eine fehlende Backup-Strategie zu denken.

IT-Risk-Management

In diesem Bereich wurde die letzte Jahren der Begriff IT-Risk-Management etabliert. Darunter versteht man die systematische Handhabung IT-bezogener Risiken unter integrativer Berücksichtigung relevanter Aspekte wie Technik, Wirtschaftlichkeit oder der organisatorischen Umsetzung beschäftigt sich das IT-Risk-Management.

Die politischen (Harrald and Kim 2003) und wirtschaftlichen Ereignisse (Gerke 2003) der letzen Jahre zwingen die Verantwortlichen in Forschung und Praxis dazu, sich mit ganzheitlichen IT-Risk-Management Ansätzen zu beschäftigen und entsprechende Projekte oder andere organisatorische Maßnahmen einzuleiten (Fischer and Mohs 2002; heise online 2004; KPMG 2004).

ITRM integriert Ansätze aus unterschiedlichen Disziplinen

IT-Risk-Management integriert Ansätze aus unterschiedlichen Disziplinen: Aus der Betriebswirtschaftslehre werden z. B. Verfahren wie "Value at Risk" oder „Balance Scorecard" übernommen, die eine Risikoidentifizierung und -bewertung ermöglichen. In der Wirtschaftsinformatik ist das IT-Risk-Management dem Informationsmanagement zuzuordnen. Von dort können Ansätze des IV-Controllings übernommen werden, die auf eine Effektivität der Planung, Steuerung und Kontrolle aller IV Prozesse abzielen. Aus dem Bereich der Informatik kommen eher technische Konzepte zum Tragen, welche etwa die Authentifizierung der Nutzer sowie die Integrität und Vertraulichkeit von Daten sicherstellen (Krcmar 2000).

Fokus der Studie: Experten-Meinung

Die vorliegende Arbeit ist das Ergebnis einer Studie, die in Frühjahr 2005 im Institut für Wirtschafts- und Verwaltungsinformatik mit dem Ziel durchgeführt wurde, Experten-Meinungen zum Thema IT-Risk-Management zu ermitteln.

In den folgenden Kapiteln sollen zunächst die Rahmenbedingungen der Studie, wie etwa die Motivation zur Durchführung einer Delphi-Studie diskutiert werden. Danach werden Ziele und Ablauf der Studie erläutert. Anschließend werden dann wichtigsten Ergebnissen vorgestellt.

1 Die Delphi-Studie „IT-Risk-Management“

1.1 Ziele dieser Studie

Hauptüberlegung bei der Erstellung der vorliegenden Studie war, den Stand und die erwartende Entwicklungen in den nächsten zwei Jahre im Bereich des IT-Risk-Management zu eruieren. Dabei sollte nicht die momentane Situation des IT-Risk-Managements und dessen Einsatz in Unternehmen im Vordergrund stehen, sondern die Umfrage sollte vor allem eine Diskussion um das Thema IT-Risk-Management und dessen Zukunft anregen.

Fragestellungen

Hierzu sollten insbesondere folgende Fragestellungen untersucht werden:

- Was ist „IT-Risk-Management“? In welcher Beziehung steht dieser Begriff zum Sicherheitsmanagement oder Krisenmanagement?
- Wo liegen die größten Herausforderungen bei der Realisierung eines IT-Risk-Management-Konzeptes?
- Welche Trends werden in diesem Bereich erwartet? Welche Entwicklungen zeichnen sich für die Zukunft ab?
- Welche wichtige Themen werden zur Zeit zu wenig beachtet und diskutiert?

hohe Spezialisierung und Zukunfts-orientierung ⇒ Delphi-Studie

Wegen der Spezialisierung und Zukunftsorientierung der Fragestellungen, wurde beschlossen die Studie in Form einer Delphi-Studie durchzuführen.

Die Delphi-Methode sowie die Rahmenbedingungen der Studie werden im nächsten Kapitel erläutert.

1.2 Methodisches Vorgehen

1.2.1 Definition der Delphi-Methode

Die Delphi-Methode, die nach dem Orakel von Delphi benannt wurde, wurde von den Forschern Norman Dalkey und Olaf Helmer 1950 entwickelt (Ludwig 1997).

Der breiten ¨Öffentlichkeit wurde sie durch die amerikanische RAND Corporation bekannt, die 1964 einen ”Report on Long Rage Forecasting Study“ erarbeitete. In dieser Studie ging es um die Vorhersage von wissenschaftlichen und technischen Entwicklungen in einem Zeitraum von zehn bis fünfzehn Jahren (Gordon and Helmer 1964).

zwei Richtungen:

Mit den Jahren hat sich eine Vielfalt von Definitionen und Aufgaben der Delphi-Methode herauskristallisiert. Nach Meinung von (Häder 2002) zeichnen sich dabei zwei Richtungen ab:

Kommunikations-werkzeug

- Die Delphi-Methode wird voranging als eine spezifische Gruppenkommunikations-werkzeug angesehen und

Bearbeitung von speziellen inhaltlichen Fragestellungen

- Die Delphi-Methode wird als Werkzeug für die Bearbeitung von speziellen inhaltlichen Fragestellungen angesehen.

Der ersten Interpretation folgen (Turoff and Linstone 2002): „Delphi may be characterized as a method for structuring a group communication process so that the process is effective

in allowing a group of individuals, as a whole, to deal with a complex problem." Repräsentanten der zweiten Interpretation sind z. B. (Rowe and Wright 1999) indem sie "Delphi as a judgment or forecasting or decision-aiding tool" sehen.

In einem „kreativen Problemlösungsprozess" kann die Delphi-Methode eingesetzt werden, um Alternativen oder Lösungsvorschläge zu entwickeln. Sie ist dabei den Gruppentechniken, wie etwa Brainstorming, Brainwriting oder der Morphologischen Analyse zuzurechnen (Higgins and G. 1996).

Kombination: Gruppenkommunikation + Beurteilung eines Sachverhalts

Eine andere Definition als Kombination der vorhergegangenen Definitionen, die an dieser Stelle übernommen wird, bieten (Häder 2002): "Die Delphi-Methode ist ein vergleichsweise stark strukturierter Gruppenkommunikationsprozess, in dessen Verlauf Sachverhalte, über die naturgemäß unsicheres und unvollständiges Wissen existiert, von Experten beurteilt werden."(Häder and Häder 1995)

Charakteristika

Unabhängig davon welche Definition favorisiert wird, gibt es bestimmte Charakteristika, die zu jeder Delphi Befragung passen (Rowe and Wright 1999):

- Anonymität: Die Teilnehmer werden anonym befragt
- Interaktion: es werden mehrere Befragungsrunden durchgeführt
- Kontrolliertes Feedback: Kontrolliertes Feedback wird dadurch erreicht. dass die Teilnehmer die Meinungen der anderen Teilnehmer erfahren (anonym)
- Statistische Auswertung: Die Rückmeldung (Feedback) wird in Form einer Statistische Auswertung wie z. B. ein Median oder arithmetisches Mittel präsentiert.

1.2.2 Vorgehensweise der Delphi-Methode

Schritte bei der Durchführung

Eine klassische Delphi-Befragung beinhaltet folgende Schritte (Häder 2002):

1. Es werden konkrete Problem- oder Fragestellungen definiert. Dies geschieht entweder im Forscherteam selbst oder durch eine vorab durchgeführte Befragung der Experten.
2. Es wird ein **Fragebogen** zusammengestellt, mit dem die Experten anonym nach ihrer Meinung zu den fokussierten Sachverhalten befragt werden.
3. Es folgt eine **Aufbereitung** der Ergebnisse und die **Rückmeldung** dieser Ergebnisse an die beteiligten Befragten.
4. Auf Basis der gewonnenen Erkenntnisse und den Rückmeldungen der Befragten wird die **Befragung wiederholt**.

Typen von Delphi-Studien

Diese klassische Variante wurde immer mehr modifiziert und für verschiedene Zwecke eingesetzt. Die gegenwärtig bekannten Delphi-Befragungen lassen sich in vier Typen klassifizieren (Häder 2002):

Ideenaggregation

- **Typ 1 – Ideenaggregation** – Wie der Name schon andeutet, geht es hier um die Aggregation von Ideen zu einem bestimmten Thema. Während im klassischen Delphi die offene Fragerunde lediglich zu Beginn der Befragung genutzt wird, wird bei der Ideenaggregation ausschließlich diese Form der Befragung verwendet. Die Ergebnisse der ersten Runde werden den Experten rückgemeldet und die Fragestellung ihnen erneut vorgelegt. Bei diesen Typ der Delphi-Studie werden nicht nur die Antworten

sondern auch in späteren Runden die entsprechende Argumentation von den Experten erwartet. Dies ist auch der einzige Typ einer Delphi-Studie, in dem man auf die Anonymität verzichtet.

Vorhersage

- **Typ 2 – Möglichst exakte Vorhersage eines unsicheren Sachverhaltes –** Bei diesem Typ der Delphi-Methode geht es darum, Informationen zu bestimmten, diffusen Sachverhalten zu erhalten. Forscher nach dem zweiten Weltkrieg, haben versucht mit Hilfe dieser Methode (bekannt auch als Forecasting) teilweise die Zukunft zu determinieren bzw. zu planen. Der Erfolg einer solchen Befragung wird durch den Vergleich des Resultates mit dem eingetretenen Sachverhalt gemessen.

Expertenmeinung zu diffusem Sachverhalt

- **Typ 3 – Ermittlung und Qualifikation der Expertenansichten zu einem diffusen Sachverhalt** – Das Ziel dieses Typs ist die Bestimmung der Meinung einer Expertengruppe zu einem konkreten Thema um aus diesem Resultat Rückschlüsse für evtl. Maßnahmen abzuleiten. Im Unterschied zum vorherigen Umfragetyp versucht dieser nicht die Zukunft zu determinieren, sondern die Ansichten aller Teilnehmer methodisch einwandfrei abzubilden und dadurch eine Verbesserung der Urteile zu bewirken.

Konsensbildung

- **Typ 4 – Konsensbildung unter den Teilnehmern** – Der vierte Typ von Delphibefragungen beschäftigt sich damit, ein hohes Maß an Konsens unter den Teilnehmern zu schaffen. Hierbei hat das Forscherteam die Aufgabe, die quantitativen Fragen auszuarbeiten und an die Teilnehmer weiterzuleiten, deren Konsens gewünscht ist. Als Abbruchkriterium dieser Umfrage kann die Streuung der Antworten zu einem definierten Wert genommen werden.

1.2.3 Kritik an der Delphi-Methode

Kritik

Zu den allgemeinen Betrachtungen der Methode gehört auch die Kritik an dieser Methode: Bei (Lang 1998) findet man eine Diskussion, welche die Delphi- Methode als eine unwissenschaftliche Methode darstellt und ihre Durchführung als äußert fragwürdig befindet. Die Kritikpunkte im einzelnen sind:

- **Zusammenstellung des Panels** – Hier gibt es sehr unterschiedliche Meinungen, wie die Stichprobe zusammengestellt werden sollte und wie viele Teilnehmer das Panel bestimmen. Die Angaben gehen dabei von „drei“ bis „möglichst viele Experten“. (Parente´, Anderson et al. 1984; Woudenberg 1991; Cuhls, Breiner et al. 1995; Rowe and Wright 1999)

- **Langwierige Durchführung** – Die Dauer der Durchführung ist durch die Wiederholung der Runden langwieriger als bei anderen Methoden. Das kann sich auch problematisch bei der Motivation der Teilnehmer

- **Fehlende Unabhängigkeit der Ergebnisse** – Die Ergebnisse sind situations- und personenabhängig und damit nicht immer überprüfbar. Weiterhin werden die Ergebnisse durch Forscher beeinflusst, da sie Zwischenergebnisse bearbeiten und als Daten für die nächsten Runden zusammenstellen.

(Häder 2002) stellt fest, dass bei der Bestimmung der Grenzen und Möglichkeiten der Delphi-Methode zwei Richtungen zu unterscheiden sind.

- Erwartungshaltung: Die Zukunft soll möglichst genau ergründet werden.
- Schlussfolgerung: Es kommt darauf an, die aktuelle Zukunfts- oder Problemsichten von Experten so zu erfassen, um daraus Schlussfolgerungen für Handlungsstrategien zu ziehen.

Allgemein kann man sagen, dass die Enttäuschung beim Umgang mit der Delphi-Methode mit der hohen Erwartung, die Zukunft wirklich vorhersagen zu können zusammenhängt.

1.3 Design und Ablauf dieser Studie

Vorliegende Studie: Typ 3

Im Sinne der o. g. Klassifikation, handelt es sich bei der vorliegenden Befragung um eine Befragung des Typs 3 (Ermittlung und Qualifikation der Expertenansichten zu einem diffusen Sachverhalt).

drei Runden

Die Umfrage wurde in insgesamt drei Runden in Form einer web-basierten Online-Befragung durchgeführt. Zum Ablauf gibt die folgende Abbildung einen Überblick.

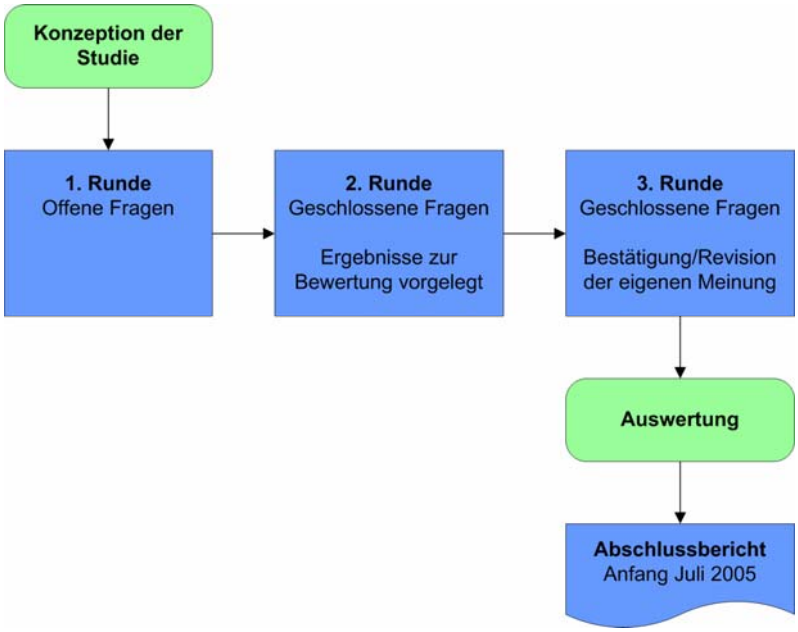


Abbildung 1: Ablauf der Studie

In der ersten Runde wurden offenen Fragen gestellt, die in der zweiten Runde wieder aufgegriffen wurden und in Form von geschlossenen Fragen (basierend auf den Antworten aus der ersten Runde) der Experten erneut vorgelegt wurden. In der dritten Runde hatten die Experte die Möglichkeit die eigene Meinung zu bestätigen oder zu revidieren. Dazu wurde ihnen der gleiche Fragebogen wie in der zweiten Runde vorgelegt, diesmal jedoch ergänzt um ein visuelles Feedback des Mittelwerts der Antworten aller Experten (siehe auch Kapitel 2.3.2).

Die Umfrage wurde auf Grundlage von phpSurveyor realisiert (www.phpsurveyor.org), der wiederum PHP und MySQL verwendet. Als Webserver für phpSurveyor können Apache oder Microsofts IIS verwendet werden. Für die vorliegende Umfrage wurde eine Kombination aus Linux, Apache, MySQL und PHP verwendet.

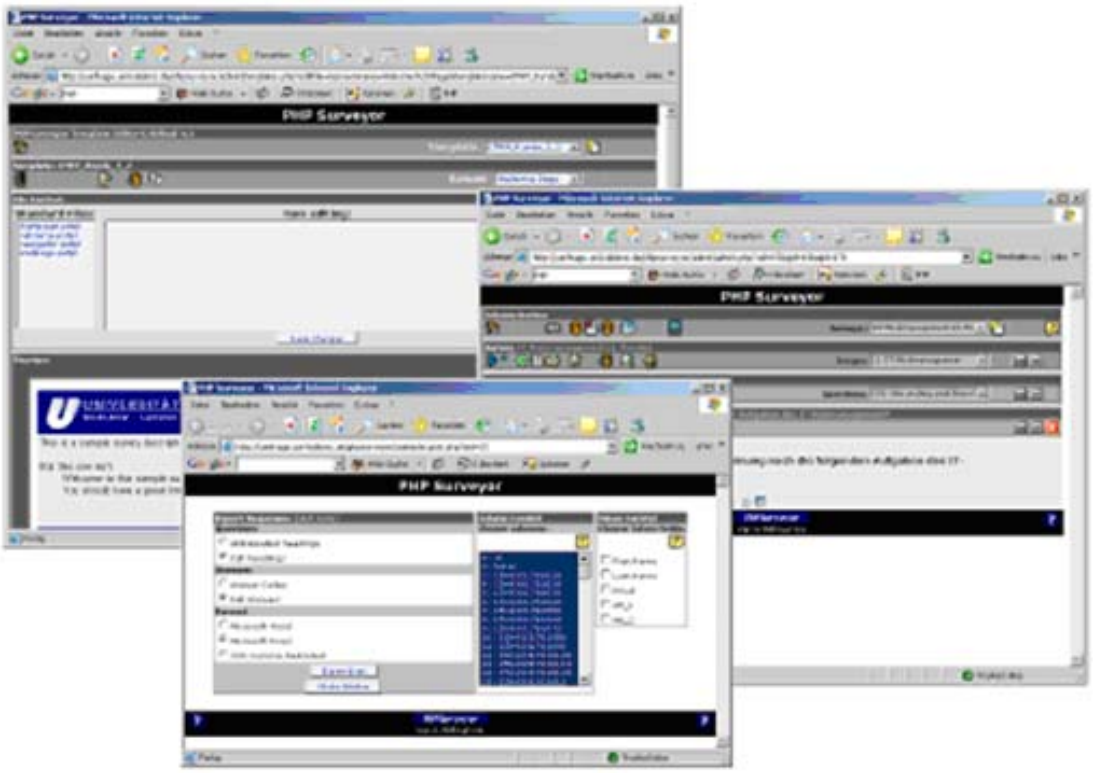


Abbildung 2: phpSurveyor

PhpSurveyor bietet mit seinen HTML-Templates viele Möglichkeiten, eine Online-Befragung zu erstellen. Für die dritte Runde wurde die Funktionalität von phpSurveyor erweitert, um die Anzeige der Ergebnisse aus der vorhergegangenen Runde zu ermöglichen.

1.3.1 Auswahl des Panel

Eine der Herausforderungen war es, die richtige Auswahl für die Experten Runde zu identifizieren. In der Literatur werden unterschiedliche Panelgrößen (z. B. ab 7 Experten) je nach Art der Studie, Bereich oder Forscherpräferenzen angegeben (vgl. (Cuhls, Breiner et al. 1995)). Für die vorliegende Studie wurde keine Obergrenze festgelegt, das Ziel war es, so viele Experten wie möglich zu erreichen. Dabei wurden aber zur Information von potentiellen Teilnehmern ausschließlich Kommunikationsmedien gewählt, die in ihrer Zielgruppe eine Fokussierung auf Fachleute aus dem Bereich IT-Sicherheit und IT-Risk-Management ermöglichen. Dies wurde erreicht durch E-Mail-Listen und Newsletter der Firmen Computas (www.computas.de), DuD (www.datenschutz-und-datensicherheit.de) und Risknews (www.risknews.de).

Die Website auf der die Umfrage durchgeführt wurde, wurde als geschützter Bereich mit entsprechender Passwort-Authentifikation gesichert. In der zweiten und dritten Runde wurde Teilnehmern von vorangegangenen Runden zusätzlich eine Erinnerung zugemailt, die durch einen personalisierten Web-Link einen direkten Zugang ohne gesonderte Passworteingabe ermöglichte.

An der Studie nahmen insgesamt 71 verschiedene Befragte teil. Die Aufteilung während den drei Runden war wie folgt:

- Erste Runde: 42 Teilnehmer

- Zweite Runde: 36 Teilnehmer
- Dritte Runde: 42 Teilnehmer

1.3.2 Erste Runde

erste Runde: offene Fragen

Ziel der Studie war es, die Meinungen und Ansichten von Experten im Bereich IT-Risk-Management zu ermitteln. Um die Ergebnisse nicht durch den Aufbau des Fragebogens zu beeinflussen, wurden in der ersten Runde keine Antwortmöglichkeiten vorgegeben, sondern nur offene Fragen gestellt. So hatten die Befragten die Möglichkeit, ohne weitere Vorgaben ihre Meinung frei zu äußern (siehe Abbildung 3).

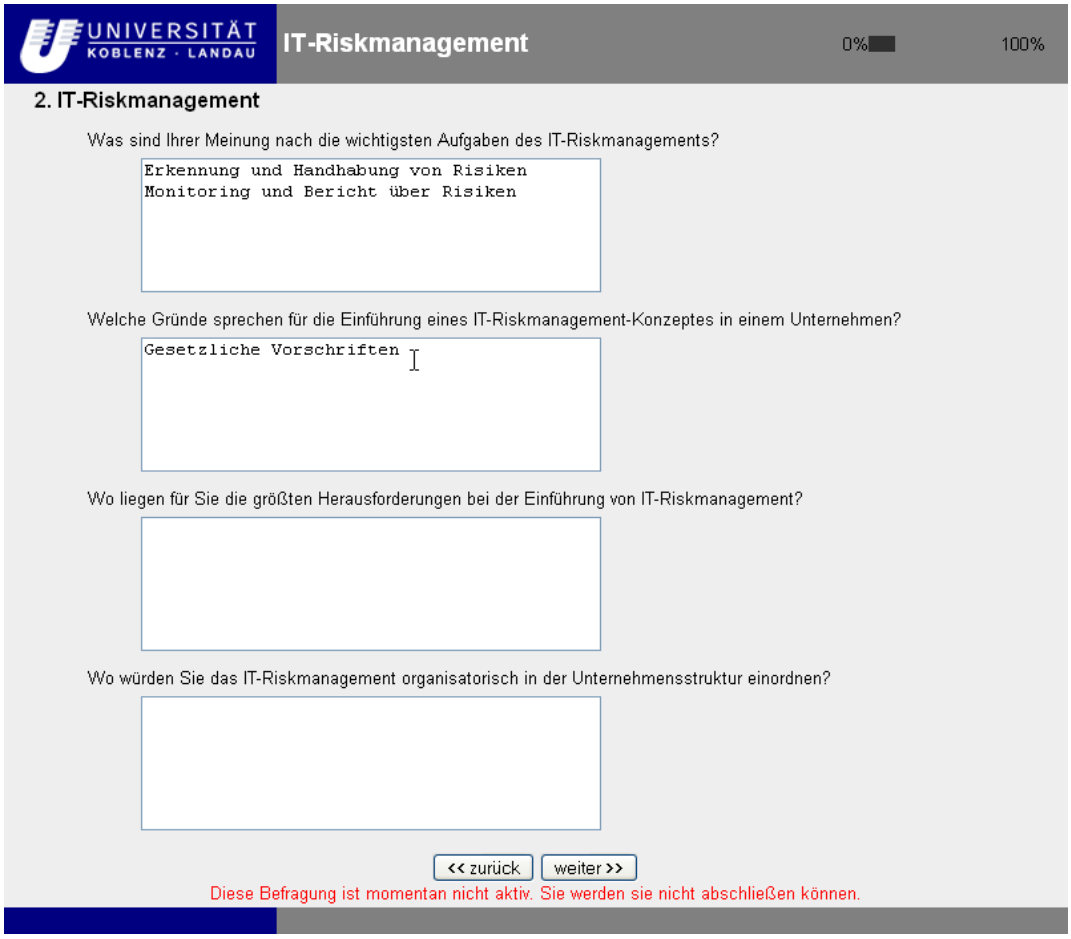


Abbildung 3:Fragebogen der ersten Runde

Außer den IT-Risk-Management bezogenen Fragen erhielt der Fragebogen Fragen um den Ursprungsbereich der Experten definieren zu können:

- Personenbezogenen Daten (Name, Adresse)
- Einordnung in eine Branche
- Unternehmensgröße
- Aktuelle Tätigkeit des Befragten
- Selbsteinschätzung der Expertise der Teilnehmer

1.3.3 Zweite Runde

zweite Runde: geschlossene Fragen

Als Vorbereitung für die zweite Runde (eine Woche nach der ersten Runde) wurden die Antworten der ersten Runde ausgewertet und teilweise zusammengeführt. Anschließend wurden diese konsolidierten Antworten den Befragten zur Qualifizierung vorgelegt (siehe Abbildung 4).

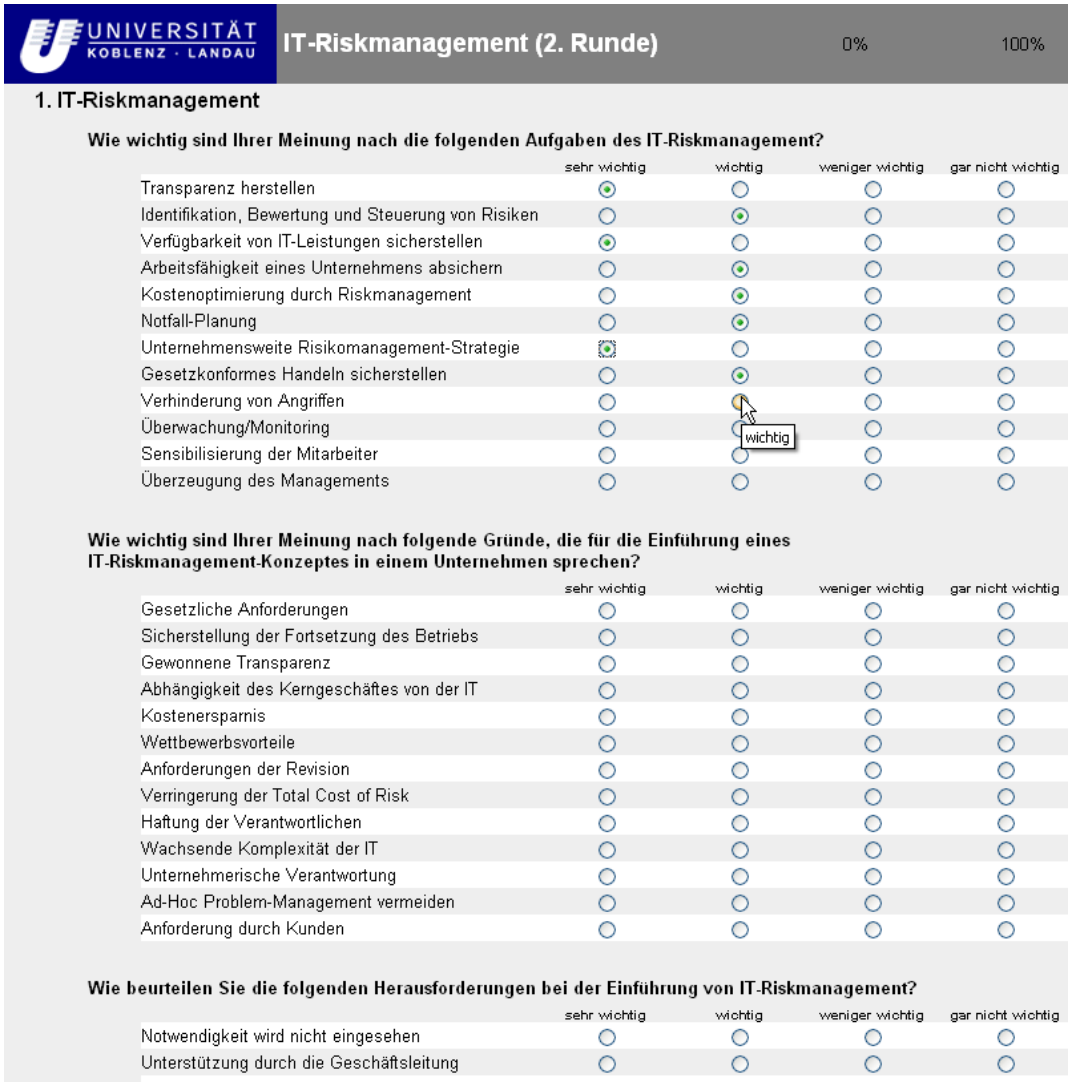


Abbildung 4: Fragebogen der zweiten Runde

Die Webadresse dieses Fragebogens wurde per E-Mail an die Experten verschickt, die sich in der ersten Runde registriert hatten. Zusätzlich wurde, um noch weitere Teilnehmer zu erreichen, weitere E-Mail- und News-Aktionen mit der Unterstützung der Firmen Computas, DuD und Risknews vorgenommen.

1.3.4 Dritte Runde

dritte Runde: geschlossene Fragen und Mittelwert

Der Fragebogen der dritten Runde (zwei Wochen nach der zweiten Runde) hatte den gleichen Aufbau wie in der zweiten Runde – mit dem Unterschied, dass diesmal den Befragten in den Fragebogen als Orientierung die Mittelwerte aus der zweiten Runde eingeblendet wurden (siehe Abbildung 5). So konnten sie ihre eigene Einschätzung des

Sachverhalts mit den Aussagen der anderen Befragten vergleichen und ihre Meinung entweder bekräftigen oder revidieren.

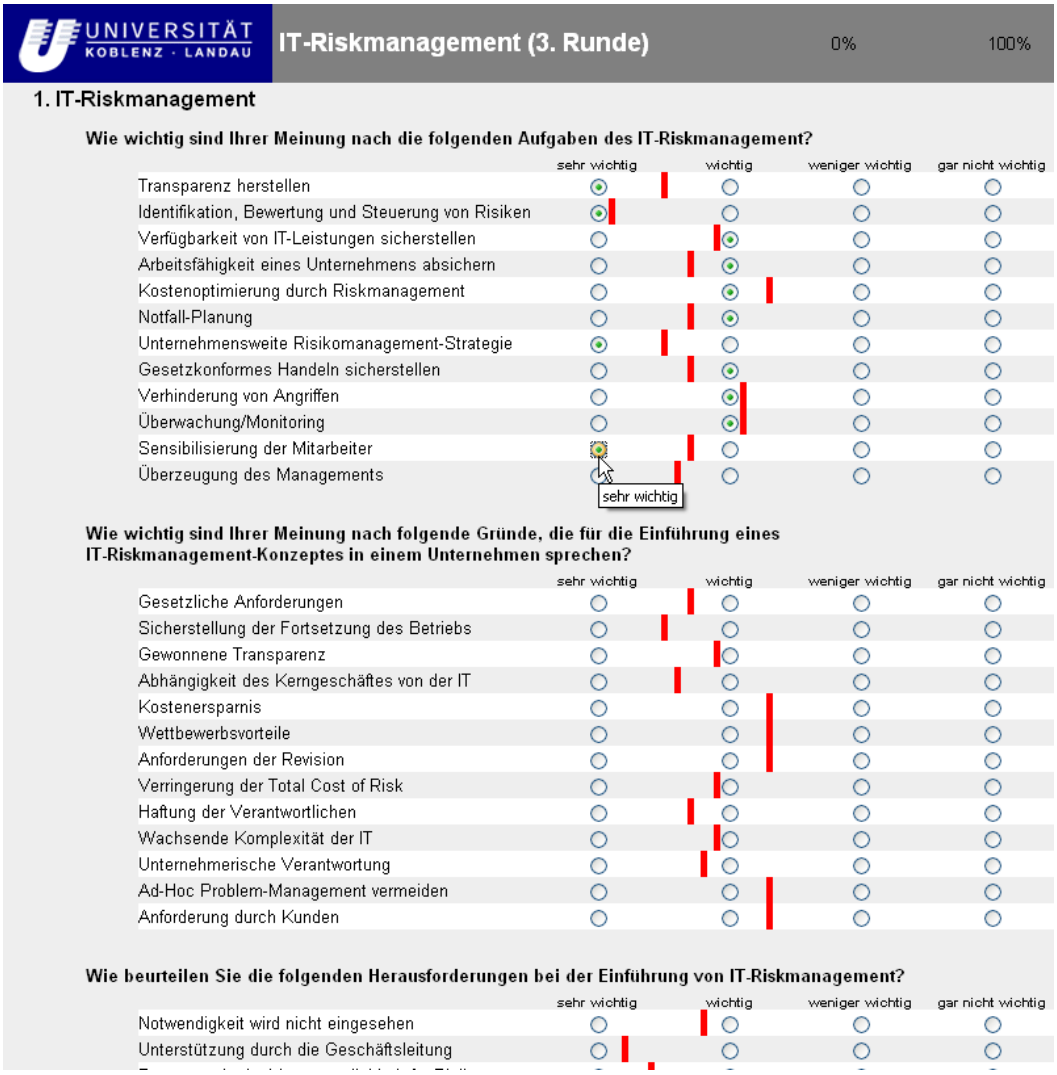


Abbildung 5: Fragebogen der dritten Runde

2 Auswertung der Delphi-Studie

2.1 Panel-Eigenschaften

Zunächst sollen die Ergebnissen zur Einordnung der Teilnehmer (Branche, Unternehmensgröße usw.) vorgestellt. Anschließend werden dann die Antworten zu den inhaltlichen Fragen ausgewertet und interpretiert.

2.1.1 Unternehmensgröße

Die Teilnehmer kamen nach eigenen Angaben zu etwa 44% aus Großunternehmen (mit mehr als 1000 Mitarbeitern), zu etwa 42% aus kleineren Unternehmen (mit unter 200 Mitarbeitern), der Rest aus Unternehmen mit 200 bis 1000 Mitarbeitern.

2.1.2 Branchen

Die Teilnehmer repräsentierten die unterschiedlichsten Branchen, wobei die ersten drei Positionen wie folgt belegt waren:

- Unternehmensberatung 25%
- Telekommunikation 12%
- Logistik und Verkehr mit 10%.

Die vierte Position teilten sich „Versicherungen“ und „Medien und Unterhaltung" mit jeweils 6%. Weitere Branchen wie „Verarbeitende Industrie“, „Versorgungsunternehmen“, „Universitäten und Fachhochschulen“, „Gesundheitswesen“, „Softwareentwicklung“, Öffentliche Verwaltung“, „Forschungsunternehmen“, „Bundeswehr“ oder „Banken“ waren mit weniger als 4 Prozent vertreten.

2.1.3 Selbsteinschätzung als „Experte“

Die Experten wurden zu ihrer Expertise im Bereich IT-Risk-Management befragt. Sie sollten sich dazu selbst auf einer Notenskala von 1 bis 6 (1=Experte und 6=geringe ausgeprägte Kenntnisse) bewerten. Dabei ordneten sich 74% der Befragten als „1“ oder „2“ ein. Weitere 21,8% bewerteten die eigene Expertise als durchschnittlich (mit „3“) und nur 5,1% schätzte sich eher als Laie in diesem Bereich ein. Dieses Ergebnis deutet darauf hin, dass die Fokussierung auf die gewünschte Zielgruppe an Teilnehmern und die Auswahl der Kommunikationsmedien erfolgreich waren – auch wenn man hier die Selbsteinschätzung der Befragten natürlich vorsichtig bewerten muss.

2.2 Ergebnisse der Delphi-Studie

Nachdem die Antworten der ersten Runde vorlagen, wurden teilweise zusammengefasst und als neue Antwortmöglichkeiten für die zweite Runde den Experten vorgelegt. Dabei sollten die Experten die einzelnen Antwortmöglichkeiten mit Hilfe folgender Skala bewerten:

Bewertungsbegriffe	Wertigkeit
Sehr wichtig	3
Wichtig	2
Weniger wichtig	1
Gar nicht wichtig	0

Tabelle 1: Bewertung der Antwortmöglichkeiten

Anhand dieser Antworten aus der 2. Runde wurde zu jeder Teilfrage das arithmetische Mittel berechnet. In der dritten Runde wurde dann der Fragebogen aus der zweiten Runde ergänzt um eine visuelle Markierung dieses Mittelwertes (siehe den roten Strich in Abbildung 6)

Abbildung 6 Bewertungselemente einer Antwortmöglichkeit

2.2.1 Aufgaben des IT-Risk-Managements

Nach der Befragung zur Einordnung des Teilnehmers (Branche, Unternehmen, usw.) beschäftigte sich die erste inhaltliche Frage mit den wichtigsten Aufgaben des IT-Risk-Managements. Dies ergab folgende Antworten und Wertungen:

Abbildung 7 Aufgaben des IT-Risk-Managements

Diese Auswertungsdiagramme sind wie folgt zu lesen: Die Texte zeigen die möglichen Antworten, die sich aus der ersten Runde für diese Frage ergeben hatten. Dazu sind entlang der X-Achse die Bewertungen, d.h. die Mittelwerte der Antworten aller Experten, aus der zweiten Runde (grauer Balken) und dritten Runde (blauer Balken) aufgetragen. Die Skala reicht von 0 bis 3 (siehe auch Tabelle 1).

Als die wichtigste Aufgabe wurden Identifikation, Bewertung und Steuerung von Risiken angegeben. Besonders interessant scheint hier die zweite Antwort "Überzeugung des Management". Anscheinend ist es immer noch eine Herausforderung, das Management von der Wichtigkeit des Themas „IT-Risk-Management" zu überzeugen. Hier ist zu überlegen, ob allgemein Vorgänge, die mit Änderungen und Investitionen verbunden sind, einen gewissen Widerstand im Management erfahren oder ob sich dieser Effekt speziell auf das IT-Risk-Management bezieht, beispielsweise weil dessen Notwendigkeit durch das Management nicht eingesehen wird. Hier könnte eine verknüpfte Befragung von Fachexperten und Mitgliedern des höheren Managements zur Einschätzung des IT-Risk-Managements interessant sein.

Auffällig ist auch, dass die Experten eine Kostenoptimierung durch verbesserten Umgang mit Risiken nicht als vorrangige Aufgabe des ITRM sehen.

2.2.2 Gründe für die Einführung des IT-Risk-Managements

Bei der Frage nach den Gründen für die Einführung des ITRM war die mit Abstand am stärksten gewichtet Antwort die „Sicherstellung der Fortsetzung des Betriebes". Weitere hoch gewichtetet Gründe waren die steigende Abhängigkeit des Kerngeschäftes von der IT sowie die neue Anforderungen des Gesetzgebers.

Abbildung 8 Einführung des IT-Risk-Management

Interessant ist zu beobachten, dass die Verminderung der Kosten sowohl allgemein als auch in Verbindung mit den Total Cost of Risk nicht als herausragend empfunden wurde, obwohl die erste Bewertung (2. Runde, hervorstehender grauer Balken) noch höher ausgefallen war.

2.2.3 Herausforderungen des IT-Risk-Management

Die größten Herausforderungen im IT-Risk-Management sind nach Ansicht der Experten das fehlenden Risikobewusstsein der Verantwortlichen und das Verständnis für die Notwendigkeit des ITRM. So fanden ungefähr 90% der Befragten die Überzeugung des Managements und 73% die daraus resultierende Unterstützung als einen der schwierigsten Herausforderungen.

Abbildung 9 Herausforderungen IT-Risk-Management

Weiterhin sehen die Experten die Schwierigkeiten in den fehlenden Kommunikation und Synergien zwischen den unterschiedlichen Abteilungen sowie in der Sensibilisierung der Mitarbeiter für die Themen IT-Risk-Management und IT-Sicherheit. Ein weiterer wichtiger Aspekt sind die teilweise fehlende Ressourcen oder auch Methodenkompetenz für die Risikoerkennung und -behandlung

2.2.4 Organisatorische Einordnung des IT-Risk-Managements in der Unternehmensstruktur

ITRM als Stabsstelle zur Geschäftsleitung

Bei der Frage nach der organisatorischen Einordnung des IT-Risk-Managements in der Unternehmensstruktur kamen die Experten einhellig zum Schluss, dass das ITRM *nicht* in die IT-Abteilung gehört.

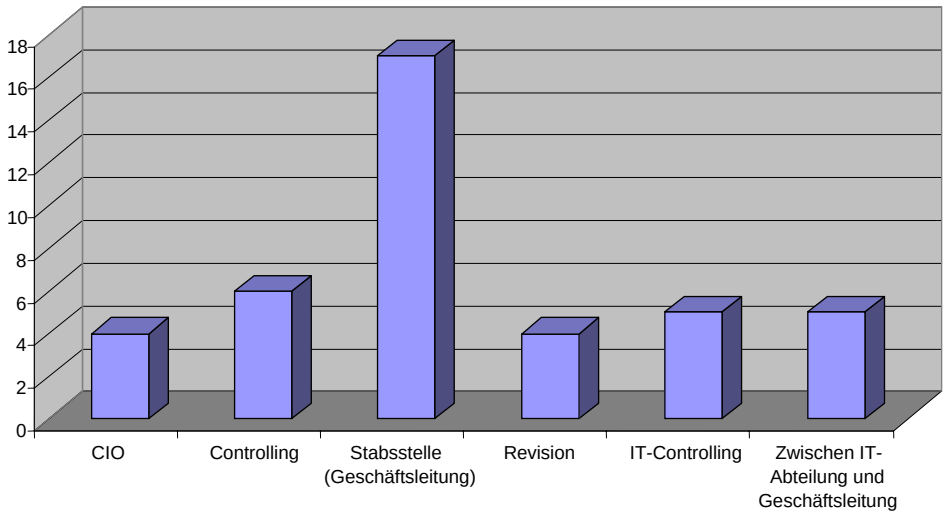


Abbildung 10 Organisatorische Einordnung des IT-Risk-Management

Neben anderen Antworten zur Einordnung des ITRM wie „CIO“, „Controlling“ oder „zwischen IT-Abteilung und Geschäftsleitung“ war die vorwiegende Meinung, dass ITRM als Stabsstelle der Geschäftsleitung zuzuordnen sei.

Hier spielt eventuell die Einsicht mit, dass es einer organisatorischer Einheit bedarf, die einerseits einen Überblick über das Unternehmen und seine Prozess hat und zusätzlich außerhalb der betrachteten Abteilungen steht und so eine gewisse Kontrollfunktion wahrnehmen kann.

2.2.5 Bedeutung des IT-Risk-Management in den letzten Jahren

Bei der Frage „Denken Sie, dass IT-Risk-Management in den letzen Jahren an Bedeutung gewonnen hat?“ waren sich die Experten einig (95%), dass das Thema IT Risk Management in den letzten Jahren eine enorme Entwicklung machte.

Die angegebenen Gründe waren mit unterschiedlicher Wichtigkeit gewichtet:

Ungefähr 60% der Befragten fanden, dass die Regelungen und Vorschriften für IT-Risk-Management eine sehr wichtige Rolle bei dessen Verbreitung gespielt hat. Weitere Gründe wie die hohe Abhängigkeit der Geschäftsprozesse von der IT, die hohe Investitionen in die IT, die Sensibilisierung des Management und die steigende IT-Attacken haben zwar auch dazugeführt, dass die Thematik an Bedeutung gewonnen hat, aber nach der Meinung der Experten haben diese Aspekte keine heraustragend Rolle gespielt.

Eine noch geringere Rolle spielten bei der Verbreitung des IT-Risk-Management einerseits die Erkenntnis der Vorteile eines solchen Konzeptes sowie die zunehmende Anzahl der Wirtschaftspionage oder Naturkatastrophen Fälle, genauso wenig wie die Fälle des Terrorismus die öfters in einem Atemzug mit IT-Risk-Management gebracht werden

2.2.6 Etablierung des IT-Risk-Management in den deutschen Unternehmen

87% der Befragten stellten fest, dass IT-Risk-Management in den deutschen Unternehmen nicht etabliert ist. Dabei wurden unterschiedliche Gründe für dieses fehlende Interesse gegeben, wie die folgende Abbildung zeigt:

Abbildung 11 Etablierung des IT-Risk-Management

Die wichtigsten Gründe für die Nicht-Etablierung, deren Wichtigkeit fast konstant in der zweiten und dritten Runde geblieben sind, waren der nicht erkennbarer Beitrag des IT-Risk-Management zur Wertschöpfung und der Kostenfaktor ohne erkennbaren ROI. Weiterhin wurden Aussagen gemacht wie, dass das Thema nicht systematisch angegangen wird, oder dass nur eine technische IT-Sicherheit betrieben wird

Allerdings haben auch 13% der Befragten eher eine positive Einstellung gegenüber der Etablierung des IT-Risk-Management in Deutschland geäußert, aber mit ein paar Begrenzungen: So waren die Befragten sich einig, dass die gesetzlichen Vorgaben die Etablierung gefördert haben und dass diese Etablierung eher in den Großunternehmen stattgefunden hat.

Ein Teil von 54 % plädierte für die Unwichtigkeit der Antwort, dass der 11 September maßgeblich die Entwicklung des IT-Risk-Management beeinflusst hat.

2.2.7 Zukunft: Risiken und deren Bedeutung

Eine der interessanten Fragenstellungen an dieser Studie war, wie sich der Sektor IT-Risk-Management entwickeln wird. Laut Meinung der Teilnehmer ist als erstes zu beobachten, dass die steigende Komplexität der Geschäftsprozesse und deren Abhängigkeit von der IT-Infrastuktur (mit einer Bewertung von 2,75 bzw. 2,45 in einer Skala zwischen 0 und 3) ein der ausschlaggebende Gründe für erwartende neue Risiken sind. Dabei sind bei der Befragung die Festigung der Meinungen und die Steigerung der Wichtigkeit in der 3.Runde gut zu beobachten.

Abbildung 12 Zukünftige Risiken des IT-Risk-Managements

Ein fast genau so wichtiger Aspekt scheint die neuen Technologien zu sein. Die aufkommende Nutzung von mobilen Endgeräte und Funknetze bilden mit 88% ein der neuen Risikofelder, dabei war für die Teilnehmer die Bedeutsamkeit des Themas mit 66% als sehr wichtig bewertet. Weitere Risiken wie fehlende Qualifikation oder fehlende Dokumentation sind in der Zukunft auch wichtig, aber hier stellt sich die Frage, ob diese Risiken zunehmen werden.

2.2.8 Zukunft: Entwicklungen und Trends im Bereich des IT-Risk-Managements

Ein weiterer interessanter Aspekt dieser Umfrage waren die Ausichten bzgl. der Zukunft des IT-Risk-Managements. Hierbei wurden unterschiedliche Erwartungen gesetzt.

Abbildung 13 Zukünftige Entwicklungen des IT-Risk-Managements

86% der Befragten waren sich einig, dass die bereits gesetzlichen Auflagen weiterentwickelt werden. Diese Meinung bewerten 82% mit sehr wichtig bis wichtig. Genau so wichtig war nach der Meinung der Experten die Erstellung von ganzheitlichen Konzepten mit der entsprechenden Aufhebung von den IT-Bereichen. Die anfängliche geäußerte Meinung, dass keine oder eine langsame Fortentwicklung zu erwarten sein wurde in den späteren Fragerunden nicht bestätigt. Ähnlich schlecht wurde die Aussage, dass das IT-Risk-Management in den Klein- und Mittelunternehmen etabliert sein wird, bewertet.

2.2.9 Vernachlässigte IT-Risk-Management Themen

Auch wenn das Thema IT-Risk-Management die letzten Jahre stark im Kommen ist, gibt es bestimmte Themen, die von der aktuellen Diskussion fehlen

Abbildung 14 Fehlende Themen des IT-Risk-Managements

Die Experten fanden, dass dem menschlichen Faktor auch wenn er ab und zu diskutiert wird mehr Bedeutung beimessen sollte. Dafür erhielt aber die Antwort „Konzepte zur Mitarbeiter Awareness“ eine geringere Bewertung. Hier wäre die Frage zu beantworten welche Aspekte außer der Ausbildung der Mitarbeiter die Experten in Zusammenhang mit dem menschlichen Faktor sehen.

Ein weiterer Punkt der oft losgelöst vom Thema IT Risk Management gesehen wird ist IT-Risk-Management in Projekten. Auch wenn die Bewertung der Experten für die Wichtigkeit des projektorientiertes IT-Risk-Managements abgenommen hat, bleibt mit einer Bewertung von 2,34 in den oberen Bereich den noch wichtig aufkommenden Themen.

2.3 Abschließende Betrachtungen

Als nächstes wird auf Zusammenhänge zwischen den Antworten hingewiesen, die mit Hilfe von statistischen Methoden wie der kombinierten Häufigkeitsverteilung (Kreuztabellen) und Clusteranalyse ermittelt wurden.

So war die Bewertung der Vertreter von Klein- und Mittelständische Unternehmen (KMU) im Vergleich zu Vertretern von Großunternehmen in den folgenden Aspekten unterschiedlich:

- KMU bewerteten die Verhinderung von Angriffen als eine sehr wichtige Aufgabe. Dabei war dies für die Großunternehmen kein herausragender Grund. Hier könnte man vermuten, dass die Großunternehmen bereits eine geeignete Infrastruktur (Firewalls oder IDS-Systeme) und die geeignete Organisation (Rechenzentrum) haben, um IT-Angriffe abzuwehren.
- Das Interesse in der Öffentlichkeit als Faktor für die zunehmende Bedeutung des Themas IT-Risk-Management war KMUs als wichtiger bewertet worden als bei Großunternehmen. Hier könnte man vermuten, dass der Druck für die KMUs durch die Öffentlichkeit oder Presse und die Folgen eines eventuellen Imageverlustes höher sind als für Großunternehmen, da diese sowieso schon durch Regelungen oder

Gesetzte für verpflichtet waren, IT-Risk-Management-Konzepte im Unternehmen einzuführen.

- Im Gegensatz dazu ist Kostenersparnis als Grund für eine IT-Risk-Management Einführung in Großunternehmen von großer Bedeutung, wobei die KMU diesen Punkt als nicht relevant betrachten.

Weitere Beobachtungen lassen sich auf Grund der Expertise der Teilnehmer unterscheiden:

- So ist zu beobachten dass, je höher die Expertise der Teilnehmer gewichtet war, desto wichtiger wurde die Absicherung der Arbeitsfähigkeit des Unternehmens (Business Contingency Planning, Business Continiuty Planning) als Teil des IT-Risk-Management bewertet.
- Weiterhin wurde mit zunehmender Expertise der Aspekt „Kostenfaktor" weniger Beachtung geschenkt. Dies gilt sowohl für die Kostenoptimierung als Aufgabe des IT-Risk-Managements als auch für die Kostensenkung als Grund für die Einführung von IT-Risk-Management.

Zusammenfassend ist festzuhalten, dass das Thema IT-Risk-Management noch sehr aktuell und lange nicht ausgeschöpft ist. Großunternehmen sind zum größten Teil mit der Thematik vertraut, teilweise betonen sie die Notwendigkeit des IT-Risk-Managements und dessen organisatorische Trennung vom reinen IT-Bereich. Für KMUs ist es noch ein langer Weg, welcher durch monetär und personell begrenzte Ressourcen aber auch fehlende Erkenntnis erschwert wird.

In der Zukunft werden neue Technologien wie z.B. mobile Geräte (Notebooks, PDAs, Handys) oder Funknetze und deren Einsatz im Unternehmen eine große Rolle spielen. Es ist schwierig für die Unternehmen die Nutzung derartige Geräten zu unterbinden. Wegen der Mobilität ist hier auch die Nutzung außerhalb der Unternehmensgrenzen zu bedenken. Man denke die Betriebsnahme eines Notebooks auch im privaten Bereich und dessen Virenbefall. Diese Technologien bieten einen großen Grad an Flexibilität und Bequemlichkeit (convenience), die für Unternehmen je nach Einsatzbereich Aspekte von großer Bedeutung sind. Dadurch wird die Abhängigkeit der Geschäftsprozesse von der IT noch verstärkt. Hier sind ganzheitliche Konzepte gefragt, die sowohl Richtlinien und Empfehlungen für die Absicherung der Technologien beinhalten als auch den Umgang mit den daraus resultierenden Risiken behandeln. Dabei sollte besonderes Augenmerk auf die Aufklärung und Sensibilisierung der Mitarbeiter gelegt werden.

A Anhang

A.1 Fragebogen der 1. Runde

UNIVERSITÄT KOBLENZ · LANDAU — IT-Riskmanagement

Herzlich Willkommen!

Wir begrüssen Sie als ausgewälte Gruppe von Experten zur Delphi-Studie IT-Riskmanagement!

Ziel dieser Studie ist es, Trends und Entwicklungen im Bereich des IT-Riskmanagement zu ermitteln und zu Diskussionen über dieses Thema anzuregen.

Dazu verwenden wir eine so genannte Delphi-Studie, die in drei Runden abläuft.

Hinweise

- Die aktuelle Runde läuft bis zum **07.03.2005**.
- Bitte füllen Sie den vorliegenden Fragebogen vollständig aus. Das wird etwa 15 Minuten in Anspruch nehmen.
- Wir garantieren Ihnen, dass der Fragebogen anonym ausgewertet wird. Es werden keinesfalls personenbezogene Antworten an Dritte weitergegeben.
- Als Dankeschön erhalten Sie nach Durchführung der vollständigen Studie ein Exemplar des Abschlußberichts.

Mit freundlicher Unterstützung von:

COMPUTAS — RiskNET — secorvo security consulting

weiter >>

Diese Befragung ist momentan nicht aktiv. Sie werden sie nicht abschließen können.

UNIVERSITÄT KOBLENZ · LANDAU — IT-Riskmanagement — 0% — 100%

1. Fragen zu Person/Unternehmen

In welcher Branche ist Ihr Unternehmen überwiegend tätig?
Bitte wählen Sie einen Punkt aus der Liste aus.

- ○ Banken
- ○ Bundeswehr
- ○ Gesundheitswesen
- ○ Handel
- ○ Hardware
- ○ Logistik und Verkehr
- ○ Medien und Unterhaltung
- ○ Netzwerktechnik
- ○ Öffentliche Verwaltung
- ○ Softwareentwicklung
- ○ Telekommunikation
- ○ Universitäten, Fachhochschulen, Schulen
- ○ Unternehmensberatung
- ○ Verarbeitende Industrie
- ○ Versicherungen
- ○ Versorgungsunternehmen
- ○ Sonstige

Welche ungefähre Größe hat Ihr Unternehmen?

- ○ weniger als 200 Mitarbeiter
- ○ 200 bis 1000 Mitarbeiter
- ○ mehr als 1000 Mitarbeiter

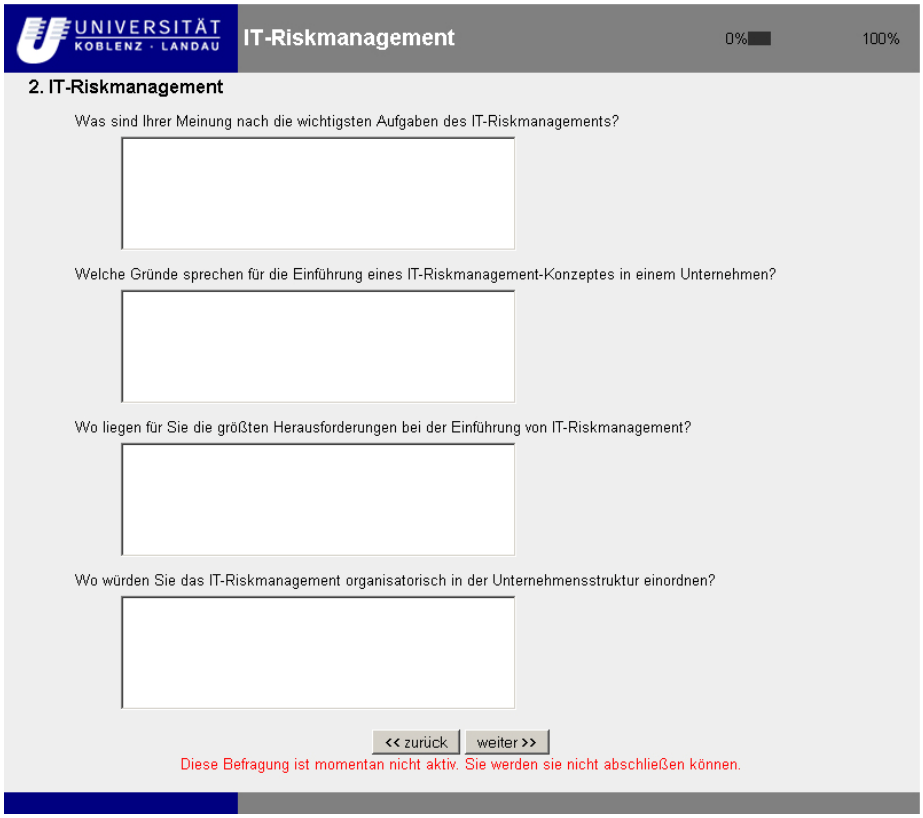
Was ist Ihre momentane Tätigkeit in dem Unternehmen?

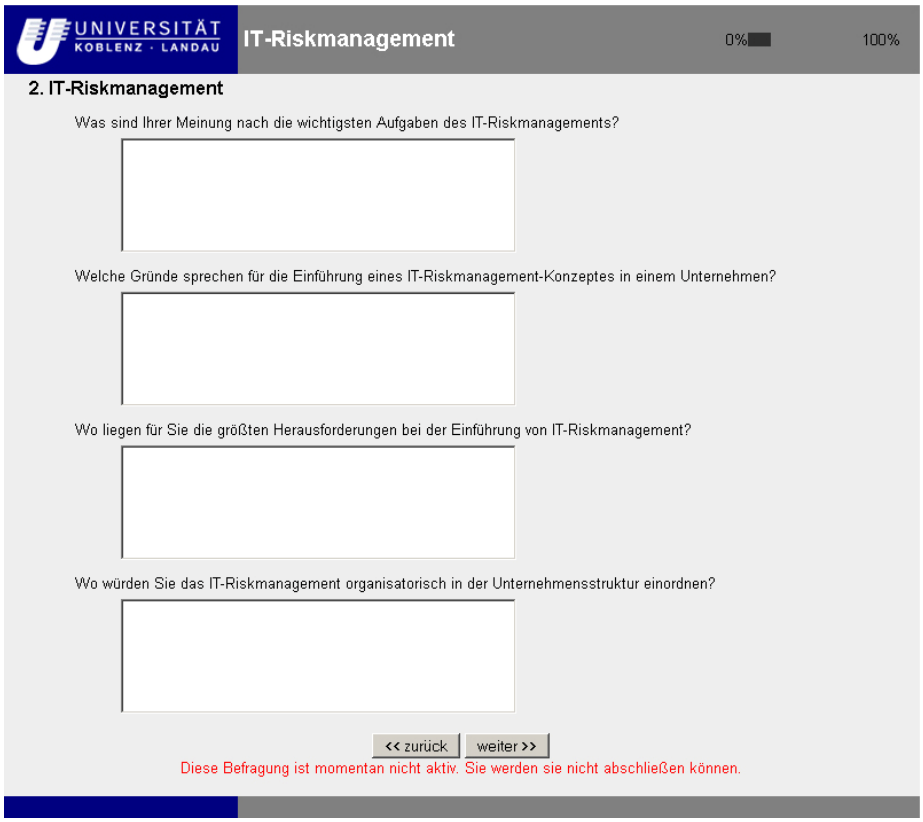
Wie würden Sie Ihre Expertise in Hinblick auf das spezielle Themengebiet IT-Riskmanagement einschätzen?

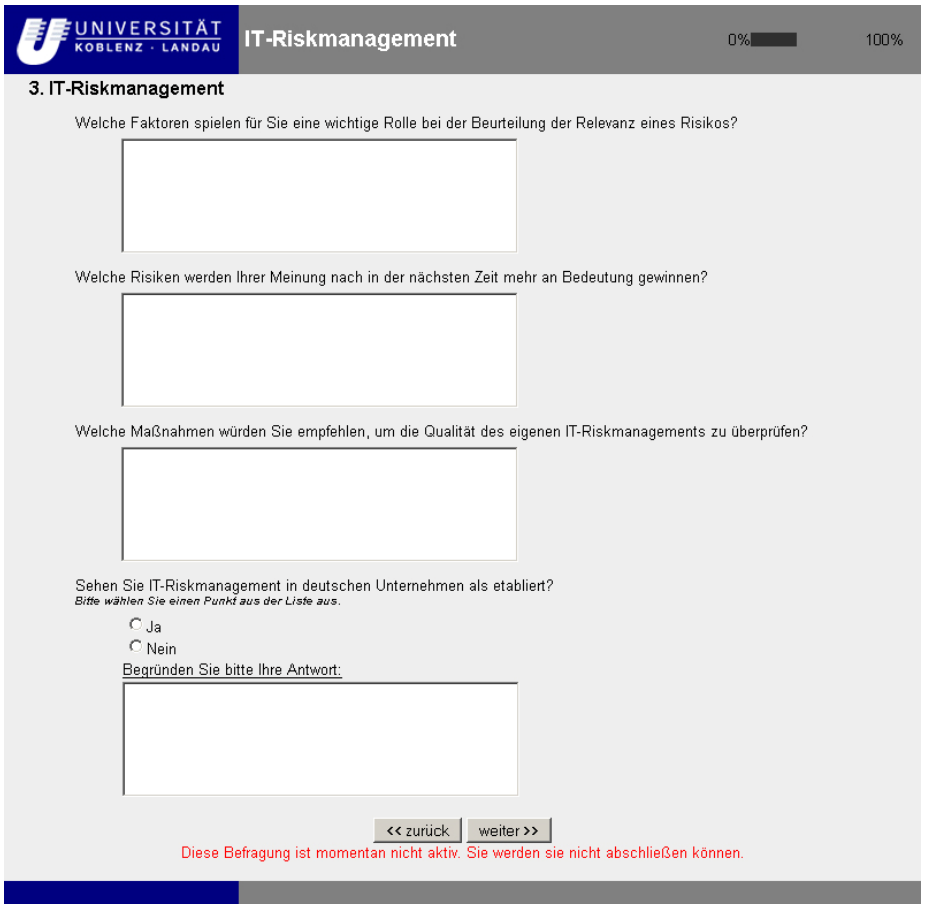
- ○ 1 Experte
- ○ 2
- ○ 3
- ○ 4
- ○ 5
- ○ 6 gering ausgeprägte Kenntnisse

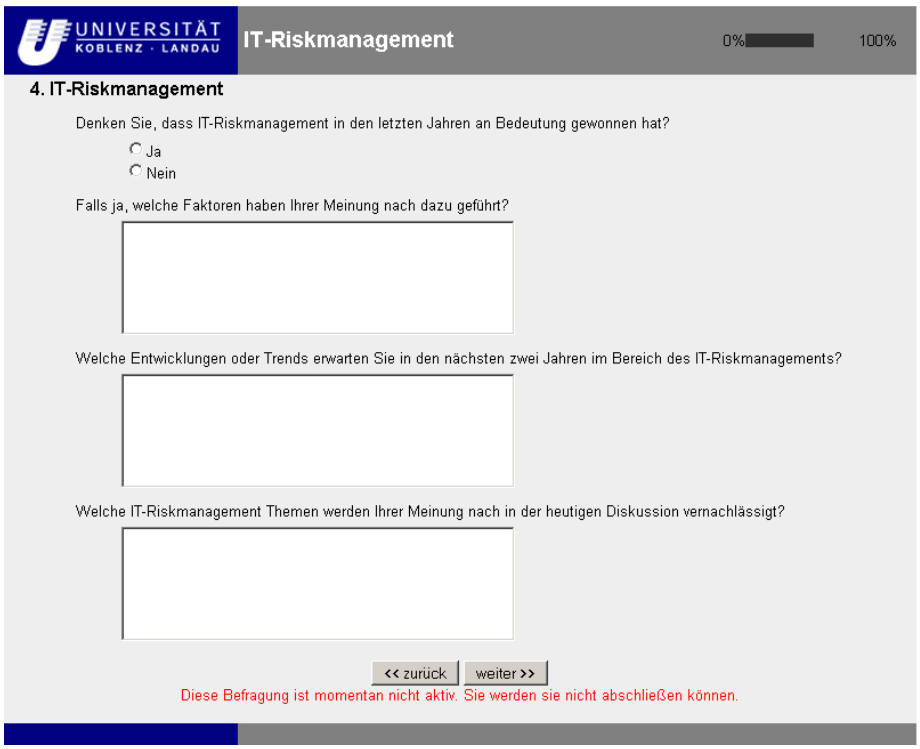
<< zurück | weiter >>

Diese Befragung ist momentan nicht aktiv. Sie werden sie nicht abschließen können.


UNIVERSITÄT KOBLENZ · LANDAU
IT-Riskmanagement
0%
100%
2. IT-Riskmanagement
Was sind Ihrer Meinung nach die wichtigsten Aufgaben des IT-Riskmanagements?
Welche Gründe sprechen für die Einführung eines IT-Riskmanagement-Konzeptes in einem Unternehmen?
Wo liegen für Sie die größten Herausforderungen bei der Einführung von IT-Riskmanagement?
Wo würden Sie das IT-Riskmanagement organisatorisch in der Unternehmensstruktur einordnen?
<< zurück
weiter >>
Diese Befragung ist momentan nicht aktiv. Sie werden sie nicht abschließen können.


UNIVERSITÄT KOBLENZ · LANDAU
IT-Riskmanagement
0%
100%
2. IT-Riskmanagement
Was sind Ihrer Meinung nach die wichtigsten Aufgaben des IT-Riskmanagements?
Welche Gründe sprechen für die Einführung eines IT-Riskmanagement-Konzeptes in einem Unternehmen?
Wo liegen für Sie die größten Herausforderungen bei der Einführung von IT-Riskmanagement?
Wo würden Sie das IT-Riskmanagement organisatorisch in der Unternehmensstruktur einordnen?
<< zurück
weiter >>
Diese Befragung ist momentan nicht aktiv. Sie werden sie nicht abschließen können.


UNIVERSITÄT KOBLENZ · LANDAU
IT-Riskmanagement
0%
100%
3. IT-Riskmanagement
Welche Faktoren spielen für Sie eine wichtige Rolle bei der Beurteilung der Relevanz eines Risikos?
Welche Risiken werden Ihrer Meinung nach in der nächsten Zeit mehr an Bedeutung gewinnen?
Welche Maßnahmen würden Sie empfehlen, um die Qualität des eigenen IT-Riskmanagements zu überprüfen?
Sehen Sie IT-Riskmanagement in deutschen Unternehmen als etabliert?
Bitte wählen Sie einen Punkt aus der Liste aus.
Ja
Nein
Begründen Sie bitte Ihre Antwort:
<< zurück
weiter >>
Diese Befragung ist momentan nicht aktiv. Sie werden sie nicht abschließen können.


UNIVERSITÄT KOBLENZ · LANDAU
IT-Riskmanagement
0%
100%
4. IT-Riskmanagement
Denken Sie, dass IT-Riskmanagement in den letzten Jahren an Bedeutung gewonnen hat?
Ja
Nein
Falls ja, welche Faktoren haben Ihrer Meinung nach dazu geführt?
Welche Entwicklungen oder Trends erwarten Sie in den nächsten zwei Jahren im Bereich des IT-Riskmanagements?
Welche IT-Riskmanagement Themen werden Ihrer Meinung nach in der heutigen Diskussion vernachlässigt?
<< zurück
weiter >>
Diese Befragung ist momentan nicht aktiv. Sie werden sie nicht abschließen können.


UNIVERSITÄT
KOBLENZ · LANDAU
IT-Riskmanagement
Vielen Dank!
Sie haben nun alle Fragen dieser Umfrage beantwortet.
Klicken Sie jetzt auf 'Absenden', um diese Umfrage abzuschlissen und Ihre Antworten endgültig zu speichern.
absenden
Wenn Sie Ihre Antworten nochmal überprüfen und/oder ändern wollen, dann klicken Sie bitte auf den Knop 'Zurück', um durch Ihre Antworten zu blättern.
<< zurück

A.2 Fragebogen der 2. Runde

UNIVERSITÄT KOBLENZ · LANDAU

IT-Riskmanagement (2. Runde) 0% 100%

1. IT-Riskmanagement

Wie wichtig sind Ihrer Meinung nach die folgenden Aufgaben des IT-Riskmanagement?

	sehr wichtig	wichtig	weniger wichtig	gar nicht wichtig
Transparenz herstellen	○	○	○	○
Identifikation, Bewertung und Steuerung von Risiken	○	○	○	○
Verfügbarkeit von IT-Leistungen sicherstellen	○	○	○	○
Arbeitsfähigkeit eines Unternehmens absichern	○	○	○	○
Kostenoptimierung durch Riskmanagement	○	○	○	○
Notfall-Planung	○	○	○	○
Unternehmensweite Risikomanagement-Strategie	○	○	○	○
Gesetzkonformes Handeln sicherstellen	○	○	○	○
Verhinderung von Angriffen	○	○	○	○
Überwachung/Monitoring	○	○	○	○
Sensibilisierung der Mitarbeiter	○	○	○	○
Überzeugung des Managements	○	○	○	○

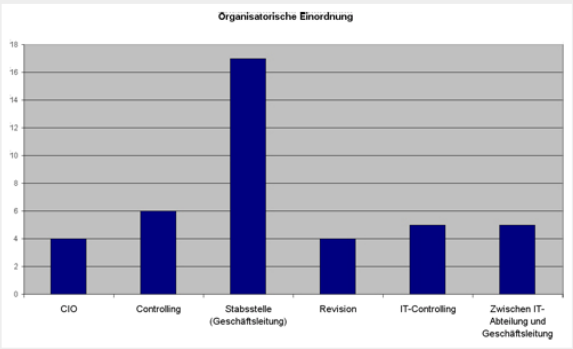
Wie wichtig sind Ihrer Meinung nach folgende Gründe, die für die Einführung eines IT-Riskmanagement-Konzeptes in einem Unternehmen sprechen?

	sehr wichtig	wichtig	weniger wichtig	gar nicht wichtig
Gesetzliche Anforderungen	○	○	○	○
Sicherstellung der Fortsetzung des Betriebs	○	○	○	○
Gewonnene Transparenz	○	○	○	○
Abhängigkeit des Kerngeschäftes von der IT	○	○	○	○
Kostenersparnis	○	○	○	○
Wettbewerbsvorteile	○	○	○	○
Anforderungen der Revision	○	○	○	○
Verringerung der Total Cost of Risk	○	○	○	○
Haftung der Verantwortlichen	○	○	○	○
Wachsende Komplexität der IT	○	○	○	○
Unternehmerische Verantwortung	○	○	○	○
Ad-Hoc Problem-Management vermeiden	○	○	○	○
Anforderung durch Kunden	○	○	○	○

Wie beurteilen Sie die folgenden Herausforderungen bei der Einführung von IT-Riskmanagement?

	sehr wichtig	wichtig	weniger wichtig	gar nicht wichtig
Notwendigkeit wird nicht eingesehen	○	○	○	○
Unterstützung durch die Geschäftsleitung	○	○	○	○
Bewusstsein der Verantwortlichkeit für Risiken	○	○	○	○
Ressourcenorganisation zur Risikobehandlung	○	○	○	○
Mitarbeiter-Awareness	○	○	○	○
Fehlende Methodenkompetenz	○	○	○	○
Monitoring/Reporting zur Überprüfung der Maßnahmen	○	○	○	○
Kommunikation zwischen den Fachbereichen	○	○	○	○
Durchsetzung der Maßnahmen	○	○	○	○
Konflikte innerhalb des Unternehmens	○	○	○	○
Unterschiedliche Perspektiven der Beteiligten	○	○	○	○

Auf die Frage "Wo würden Sie das IT-Riskmanagement organisatorisch in der Unternehmenstruktur einordnen?" gab es die folgenden Antworten:



Was ist Ihre Meinung zu diesem Aspekt?

<< zurück | weiter >>

UNIVERSITÄT KOBLENZ · LANDAU

IT-Riskmanagement (2. Runde) 0% 100%

2. IT-Riskmanagement

Wie empfehlenswert sind folgende Maßnahmen, um die Qualität des eigenen IT-Riskmanagements zu überprüfen?

	sehr empfehlenswert	empfehlenswert	weniger empfehlenswert	gar nicht empfehlenswert
Penetrationstest	○	○	○	○
Systematische Durchführung von Testszenarien	○	○	○	○
Benchmarking der aufkommenden Vorfälle	○	○	○	○
Überprüfung durch externe Audits	○	○	○	○
Überprüfung durch interne Audits	○	○	○	○
Einführung internationaler IT-Sicherheitstandards	○	○	○	○
Ausbildung der Sicherheitsverantwortlichen	○	○	○	○
Einrichten einer Balance Score Card	○	○	○	○
Einrichten eines Qualitäts-Verbesserungprozesses	○	○	○	○

Die Frage "Sehen Sie das IT-Riskmanagement in den deutschen Unternehmen als etabliert?" wurde folgendermaßen beantwortet:

Je nach Sichtweise wurden dabei verschiedene Gründe genannt. Bewerten Sie bitte, ob diese Aussagen zutreffend sind!

Ursachen für eine fehlende Etablierung

	voll zutreffend	zutreffend	teilweise zutreffend	nicht zutreffend
Fehlende Einsicht	○	○	○	○
Kein erkennbarer Beitrag zur Wertschöpfung	○	○	○	○
IT-Riskmanagement wird als Kostenfaktor ohne ROI gesehen	○	○	○	○
Das Thema wird nicht systematisch angegangen	○	○	○	○
In KMUs fehlt es an Sensibilisierung und Bewusstsein	○	○	○	○
Nur technisch betriebene IT-Sicherheit	○	○	○	○
Nicht-einheitliche Literatur	○	○	○	○
Zu geringes Know-How	○	○	○	○
Es werden nur "Feuerwehraktionen" durchgeführt	○	○	○	○

Ursachen für eine vorhandene Etablierung

	voll zutreffend	zutreffend	teilweise zutreffend	nicht zutreffend
Gesetzliche Vorgaben	○	○	○	○
In Grossunternehmen ist ITRM vorhanden	○	○	○	○
Erhöhtes Risikobewusstsein durch den "11. September"	○	○	○	○

Wie wichtig sind folgende Faktoren bei der Beurteilung der Relevanz eines Risikos?

	sehr wichtig	wichtig	weniger wichtig	gar nicht wichtig
Stellenwert der betroffenen Geschäftsprozesse	○	○	○	○
Eintrittswahrscheinlichkeit	○	○	○	○
(Monetäre) Schadenshöhe	○	○	○	○
Gefährdung der Mitarbeiter	○	○	○	○
Stellenwert der betroffenen Daten	○	○	○	○
Gefährdung des Umsatzes	○	○	○	○
Image-Schäden	○	○	○	○
Ressourcenaufwand	○	○	○	○
Ausbildungsstand der Mitarbeiter	○	○	○	○
Verstoß gegen Gesetzte	○	○	○	○
Effektivität von Gegenmaßnahmen	○	○	○	○

Welche Risiken werden Ihrer Meinung nach in der nächsten Zeit mehr an Bedeutung gewinnen?

	sehr wichtig	wichtig	weniger wichtig	gar nicht wichtig
Wirtschaftspionage	○	○	○	○
Die hohe Komplexität der Geschäftsprozesse	○	○	○	○
Fehlerhaftes Verhalten von Mitarbeiter	○	○	○	○
Bewußtes Herbeiführen von fehlerhaftem Verhalten (Social-Engineering)	○	○	○	○
Schadprogramme (Viren, Würmer, Trojaner)	○	○	○	○
Zunehmende Abhängigkeit von der Netzwerk-Infrastruktur	○	○	○	○
Risiken durch mobile Endgeräte und Funknetze	○	○	○	○
Fehlende Qualifikation der Mitarbeiter	○	○	○	○
Fehlende Dokumentation der Maßnahmen	○	○	○	○

<< zurück | weiter >>

UNIVERSITÄT KOBLENZ · LANDAU

IT-Riskmanagement (2. Runde) 0% 100%

3. IT-Riskmanagement

Die Frage "Denken Sie, dass IT-Riskmanagement in den letzten Jahren an Bedeutung gewonnen hat?" wurde folgendermaßen beantwortet:

Dabei wurden folgende Faktoren als Grund für die zunehmende Bedeutung des IT-Riskmanagements genannt. Bitte bewerten Sie diese Faktoren!

	voll zutreffend	zutreffend	teilweise zutreffend	nicht zutreffend
Gesetzliche und regulative Erfordernisse	○	○	○	○
Erkenntnis der Vorteile	○	○	○	○
Zunehmende Abhängigkeit von der IT	○	○	○	○
Hohe IT-Aufwendungen	○	○	○	○
Sensibilisierung des Managements	○	○	○	○
Zunehmende Anzahl von Attacken	○	○	○	○
Zunehmende Vorfälle von Wirtschaftsspionage	○	○	○	○
Zunehmende Vorfälle von Naturkatastrophen	○	○	○	○
Gestiegenes Interesse in der Öffentlichkeit	○	○	○	○
Hohe Anforderungen von Kundenseite	○	○	○	○
Terrorismus	○	○	○	○
Zu viele gescheiterte Projekte	○	○	○	○

Wie wichtig sind folgende Entwicklungen oder Trends, die in den nächsten zwei Jahren im Bereich des IT-Riskmanagements erwartet werden?

	sehr wichtig	wichtig	weniger wichtig	gar nicht wichtig
Einsatz von RM-Tools	○	○	○	○
Entwicklung von gesetzlichen Auflagen und Bestimmungen	○	○	○	○
Entwicklung von ganzheitlichen IT-Riskmanagement-Konzepten	○	○	○	○
Das Thema Datenschutz gewinnt an Bedeutung	○	○	○	○
Steigende Bedeutung und Akzeptanz des IT-Riskmanagements	○	○	○	○
Wenig Fortentwicklung, wegen hoher Kostenaufwendungen oder nicht direkt erkennbarem Nutzen	○	○	○	○
Stärkere Verbreitung der Zertifizierungsanforderungen	○	○	○	○
IT-Riskmanagement auch in KMU etabliert	○	○	○	○
Aufhebung der Konzentration auf die IT-Bereiche	○	○	○	○

Wie wichtig sind Ihrer Meinung nach folgende IT-Riskmanagement Themen, welche in der heutigen Diskussion vernachlässigt werden?

	sehr wichtig	wichtig	weniger wichtig	gar nicht wichtig
IT-Riskmanagement im Rahmen von Projekten	○	○	○	○
Die Auswirkungen auf die Organisationsstruktur	○	○	○	○
Die wirtschaftliche Notwendigkeit und das damit verbundene Einsparpotential	○	○	○	○
Die hohe Komplexität der vorhandenen RM-Informationen und die damit verbundene Intransparenz	○	○	○	○
Die Wirtschaftsspionage als erhöhter Risikofaktor	○	○	○	○
Konzepte zur Mitarbeiter-Awareness	○	○	○	○
Datenschutz im Rahmen des IT-Riskmanagement	○	○	○	○
Die monetäre Bewertung der IT-Risiken	○	○	○	○
Qualität von Software	○	○	○	○
Mitarbeiter; der menschliche Faktor	○	○	○	○

<< zurück | weiter >>


UNIVERSITÄT KOBLENZ · LANDAU
IT-Riskmanagement (2. Runde)
0%
100%
4. Fragen zu Person/Unternehmen
In welcher Branche ist Ihr Unternehmen überwiegend tätig?
Bitte wählen Sie einen Punkt aus der Liste aus.
Banken
Bundeswehr
Gesundheitswesen
Handel
Hardware
Logistik und Verkehr
Medien und Unterhaltung
Netzwerktechnik
Öffentliche Verwaltung
Softwareentwicklung
Telekommunikation
Universitäten, Fachhochschulen, Schulen
Unternehmensberatung
Verarbeitende Industrie
Versicherungen
Versorgungsunternehmen
Sonstige
Welche ungefähre Größe hat Ihr Unternehmen?
weniger als 200 Mitarbeiter
200 bis 1000 Mitarbeiter
mehr als 1000 Mitarbeiter
Was ist Ihre momentane Tätigkeit in dem Unternehmen?
Wie würden Sie Ihre Expertise in Hinblick auf das spezielle Themengebiet IT-Riskmanagement einschätzen?
1 Experte
2
3
4
5
6 gering ausgeprägte Kenntnisse
<< zurück
weiter >>


UNIVERSITÄT KOBLENZ · LANDAU
IT-Riskmanagement (2. Runde)
0%
100%
5. Kontaktdaten
Dürfen wir Ihren Namen in den endgültigen Ergebnissen dieser Studie dankend erwähnen?
Ja
Nein
Möchten Sie ein Exemplar des Abschlußberichtes zu dieser Studie erhalten?
Ja
Nein
Sollten Sie eine der oben stehenden Fragen mit ja beantwortet haben, bitten wir Sie um Ihre Kontaktdaten.
An dieser Stelle garantieren wir Ihnen noch mal, dass der Fragebogen anonym ausgewertet wird. Es werden keinesfalls personenbezogene Antworten an Dritten weitergegeben.
Anrede
Frau
Herr
Vorname
Nachname
Firma
Emailadresse
Haben Sie Anregungen?
<< zurück
abschließen


UNIVERSITÄT KOBLENZ · LANDAU
IT-Riskmanagement (2. Runde)
Vielen Dank!
Sie haben nun alle Fragen dieser Umfrage beantwortet.
Klicken Sie jetzt auf 'Absenden', um diese Umfrage abzuschlissen und Ihre Antworten endgültig zu speichern.
absenden
Wenn Sie Ihre Antworten nochmal überprüfen und/oder ändern wollen, dann klicken Sie bitte auf den Knop 'Zurück', um durch Ihre Antworten zu blättern.
<< zurück

A.3 Fragebogen der 3. Runde

UNIVERSITÄT KOBLENZ · LANDAU

IT-Riskmanagement (3. Runde)

Herzlich Willkommen!

Wir begrüssen Sie als ausgewählte Experten zur dritte (und letzten) Runde der Delphi-Studie IT-Riskmanagement!

Ziel ist diesmal die Validierung und Verdichtung der Ergebnisse. Dazu geben wir Ihnen Feedback zu den bisherigen Aussagen: Sie sehen jeweils den Mittelwert der bisherigen Antworten als rote Markierung.

Beispiel:

sehr wichtig | wichtig | weniger wichtig | gar nicht wichtig

Sie haben jetzt die Möglichkeit, auf Grundlage dieser zusätzlichen Information, Ihre eigene Meinung zu bekräftigen oder zu revidieren.

Hinweise

- Die aktuelle Runde läuft bis zum **18.04.2005**.
- Bitte füllen Sie den vorliegenden Fragebogen vollständig aus. Das wird etwa 10 Minuten in Anspruch nehmen.
- Wir garantieren Ihnen weiterhin, dass der Fragebogen anonym ausgewertet wird. Es werden keinesfalls personenbezogene Antworten an Dritte weitergegeben.

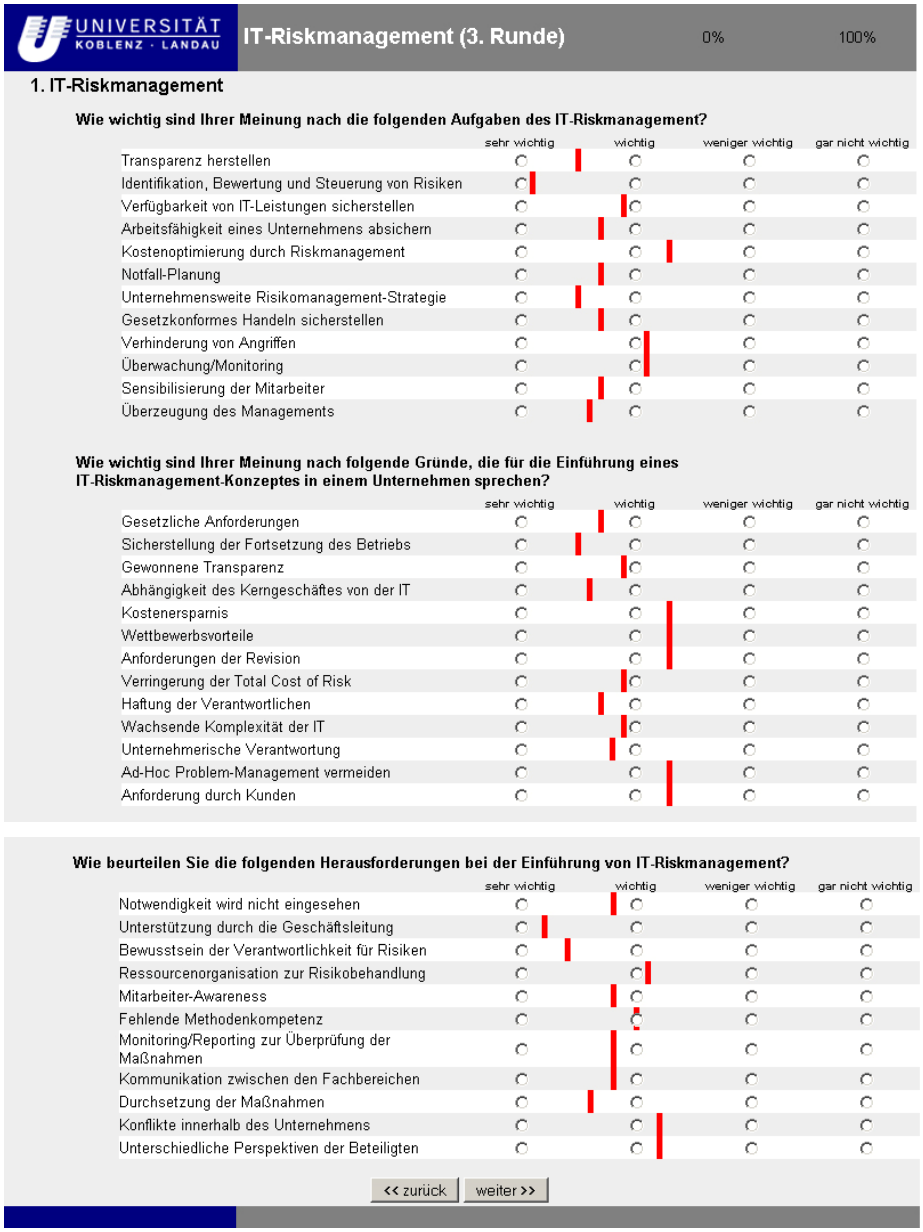
Mit freundlicher Unterstützung von:

COMPUTAS — COMPUTAS G. Geuhs GmbH — Veranstaltungsmanagement und Services in der IT

RiskNET

secorvo security consulting

weiter >>



UNIVERSITÄT KOBLENZ · LANDAU

IT-Riskmanagement (3. Runde) 0% 100%

1. IT-Riskmanagement

Wie wichtig sind Ihrer Meinung nach die folgenden Aufgaben des IT-Riskmanagement?

	sehr wichtig	wichtig	weniger wichtig	gar nicht wichtig
Transparenz herstellen	○	○	○	○
Identifikation, Bewertung und Steuerung von Risiken	○	○	○	○
Verfügbarkeit von IT-Leistungen sicherstellen	○	○	○	○
Arbeitsfähigkeit eines Unternehmens absichern	○	○	○	○
Kostenoptimierung durch Riskmanagement	○	○	○	○
Notfall-Planung	○	○	○	○
Unternehmensweite Risikomanagement-Strategie	○	○	○	○
Gesetzkonformes Handeln sicherstellen	○	○	○	○
Verhinderung von Angriffen	○	○	○	○
Überwachung/Monitoring	○	○	○	○
Sensibilisierung der Mitarbeiter	○	○	○	○
Überzeugung des Managements	○	○	○	○

Wie wichtig sind Ihrer Meinung nach folgende Gründe, die für die Einführung eines IT-Riskmanagement-Konzeptes in einem Unternehmen sprechen?

	sehr wichtig	wichtig	weniger wichtig	gar nicht wichtig
Gesetzliche Anforderungen	○	○	○	○
Sicherstellung der Fortsetzung des Betriebs	○	○	○	○
Gewonnene Transparenz	○	○	○	○
Abhängigkeit des Kerngeschäftes von der IT	○	○	○	○
Kostenersparnis	○	○	○	○
Wettbewerbsvorteile	○	○	○	○
Anforderungen der Revision	○	○	○	○
Verringerung der Total Cost of Risk	○	○	○	○
Haftung der Verantwortlichen	○	○	○	○
Wachsende Komplexität der IT	○	○	○	○
Unternehmerische Verantwortung	○	○	○	○
Ad-Hoc Problem-Management vermeiden	○	○	○	○
Anforderung durch Kunden	○	○	○	○

Wie beurteilen Sie die folgenden Herausforderungen bei der Einführung von IT-Riskmanagement?

	sehr wichtig	wichtig	weniger wichtig	gar nicht wichtig
Notwendigkeit wird nicht eingesehen	○	○	○	○
Unterstützung durch die Geschäftsleitung	○	○	○	○
Bewusstsein der Verantwortlichkeit für Risiken	○	○	○	○
Ressourcenorganisation zur Risikobehandlung	○	○	○	○
Mitarbeiter-Awareness	○	○	○	○
Fehlende Methodenkompetenz	○	○	○	○
Monitoring/Reporting zur Überprüfung der Maßnahmen	○	○	○	○
Kommunikation zwischen den Fachbereichen	○	○	○	○
Durchsetzung der Maßnahmen	○	○	○	○
Konflikte innerhalb des Unternehmens	○	○	○	○
Unterschiedliche Perspektiven der Beteiligten	○	○	○	○

<< zurück | weiter >>

UNIVERSITÄT KOBLENZ · LANDAU

IT-Riskmanagement (3. Runde) 0% 100%

2. IT-Riskmanagement

Wie empfehlenswert sind folgende Maßnahmen, um die Qualität des eigenen IT-Riskmanagements zu überprüfen?

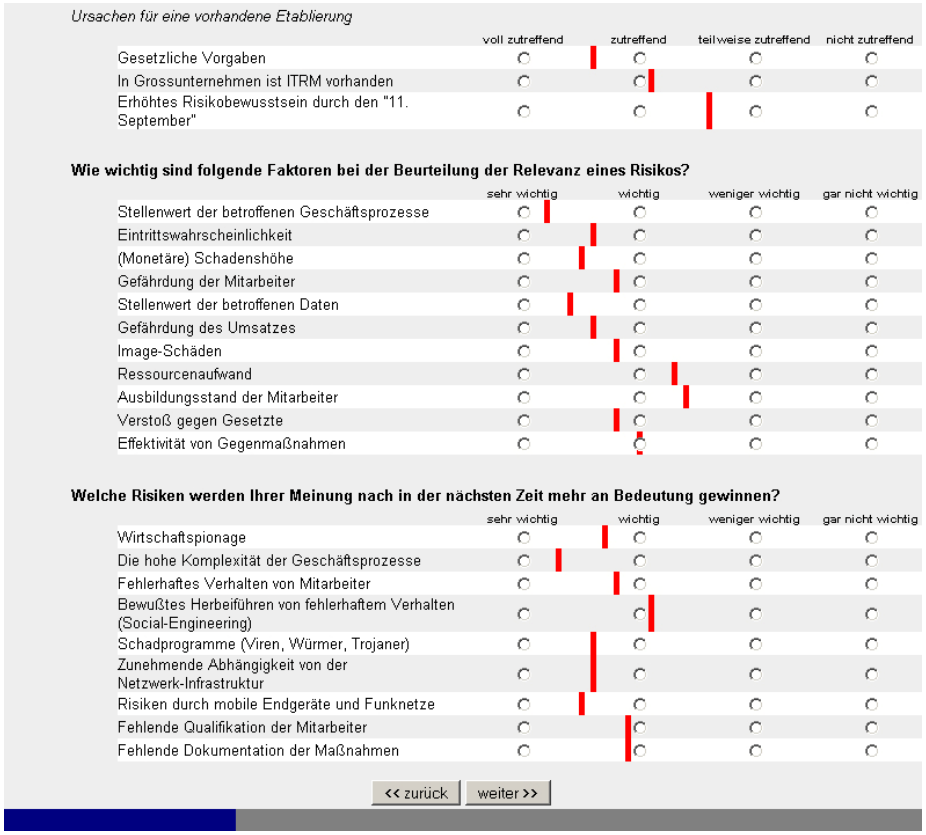
	sehr empfehlenswert	empfehlenswert	weniger empfehlenswert	gar nicht empfehlenswert
Penetrationstest	○	○	○	○
Systematische Durchführung von Testszenarien	○	○	○	○
Benchmarking der aufkommenden Vorfälle	○	○	○	○
Überprüfung durch externe Audits	○	○	○	○
Überprüfung durch interne Audits	○	○	○	○
Einführung internationaler IT-Sicherheitstandards	○	○	○	○
Ausbildung der Sicherheitsverantwortlichen	○	○	○	○
Einrichten einer Balance Score Card	○	○	○	○
Einrichten eines Qualitäts-Verbesserungprozesses	○	○	○	○

Die Frage "Sehen Sie das IT-Riskmanagement in den deutschen Unternehmen als etabliert?" wurde folgendermaßen beantwortet:

Je nach Sichtweise wurden dabei verschiedene Gründe genannt. Bewerten Sie bitte, ob diese Aussagen zutreffend sind!

Ursachen für eine fehlende Etablierung

	voll zutreffend	zutreffend	teilweise zutreffend	nicht zutreffend
Fehlende Einsicht	○	○	○	○
Kein erkennbarer Beitrag zur Wertschöpfung	○	○	○	○
IT-Riskmanagement wird als Kostenfaktor ohne ROI gesehen	○	○	○	○
Das Thema wird nicht systematisch angegangen	○	○	○	○
In KMUs fehlt es an Sensibilisierung und Bewusstsein	○	○	○	○
Nur technisch betriebene IT-Sicherheit	○	○	○	○
Nicht-einheitliche Literatur	○	○	○	○
Zu geringes Know-How	○	○	○	○
Es werden nur "Feuerwehraktionen" durchgeführt	○	○	○	○



Ursachen für eine vorhandene Etablierung

	voll zutreffend	zutreffend	teilweise zutreffend	nicht zutreffend
Gesetzliche Vorgaben	○	○	○	○
In Grossunternehmen ist ITRM vorhanden	○	○	○	○
Erhöhtes Risikobewusstsein durch den "11. September"	○	○	○	○

Wie wichtig sind folgende Faktoren bei der Beurteilung der Relevanz eines Risikos?

	sehr wichtig	wichtig	weniger wichtig	gar nicht wichtig
Stellenwert der betroffenen Geschäftsprozesse	○	○	○	○
Eintrittswahrscheinlichkeit	○	○	○	○
(Monetäre) Schadenshöhe	○	○	○	○
Gefährdung der Mitarbeiter	○	○	○	○
Stellenwert der betroffenen Daten	○	○	○	○
Gefährdung des Umsatzes	○	○	○	○
Image-Schäden	○	○	○	○
Ressourcenaufwand	○	○	○	○
Ausbildungsstand der Mitarbeiter	○	○	○	○
Verstoß gegen Gesetzte	○	○	○	○
Effektivität von Gegenmaßnahmen	○	○	○	○

Welche Risiken werden Ihrer Meinung nach in der nächsten Zeit mehr an Bedeutung gewinnen?

	sehr wichtig	wichtig	weniger wichtig	gar nicht wichtig
Wirtschaftspionage	○	○	○	○
Die hohe Komplexität der Geschäftsprozesse	○	○	○	○
Fehlerhaftes Verhalten von Mitarbeiter	○	○	○	○
Bewußtes Herbeiführen von fehlerhaftem Verhalten (Social-Engineering)	○	○	○	○
Schadprogramme (Viren, Würmer, Trojaner)	○	○	○	○
Zunehmende Abhängigkeit von der Netzwerk-Infrastruktur	○	○	○	○
Risiken durch mobile Endgeräte und Funknetze	○	○	○	○
Fehlende Qualifikation der Mitarbeiter	○	○	○	○
Fehlende Dokumentation der Maßnahmen	○	○	○	○

UNIVERSITÄT KOBLENZ · LANDAU

IT-Riskmanagement (3. Runde) 0% 100%

3. IT-Riskmanagement

Die Frage "Denken Sie, dass IT-Riskmanagement in den letzten Jahren an Bedeutung gewonnen hat?" wurde folgendermaßen beantwortet:

Dabei wurden folgende Faktoren als Grund für die zunehmende Bedeutung des IT-Riskmanagements genannt. Bitte bewerten Sie diese Faktoren!

	voll zutreffend	zutreffend	teilweise zutreffend	nicht zutreffend
Gesetzliche und regulative Erfordernisse	○	○	○	○
Erkenntnis der Vorteile	○	○	○	○
Zunehmende Abhängigkeit von der IT	○	○	○	○
Hohe IT-Aufwendungen	○	○	○	○
Sensibilisierung des Managements	○	○	○	○
Zunehmende Anzahl von Attacken	○	○	○	○
Zunehmende Vorfälle von Wirtschaftsspionage	○	○	○	○
Zunehmende Vorfälle von Naturkatastrophen	○	○	○	○
Gestiegenes Interesse in der Öffentlichkeit	○	○	○	○
Hohe Anforderungen von Kundenseite	○	○	○	○
Terrorismus	○	○	○	○
Zu viele gescheiterte Projekte	○	○	○	○

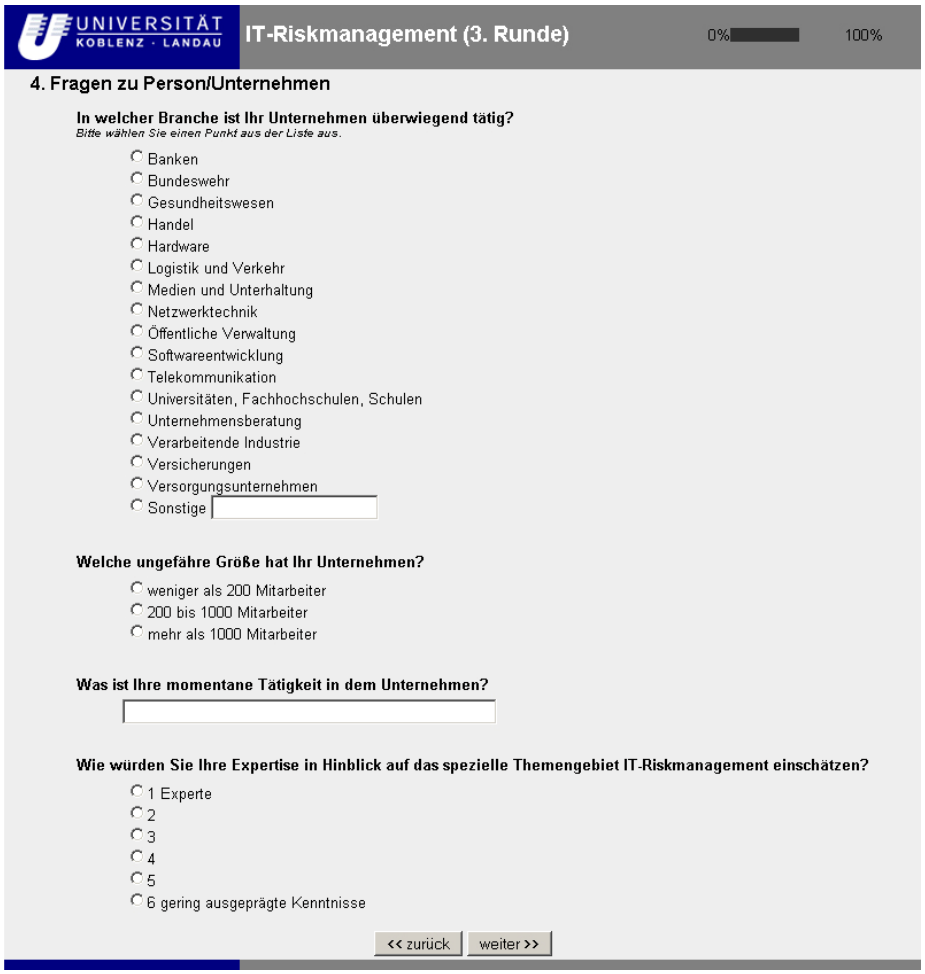
Wie wichtig sind folgende Entwicklungen oder Trends, die in den nächsten zwei Jahren im Bereich des IT-Riskmanagements erwartet werden?

	sehr wichtig	wichtig	weniger wichtig	gar nicht wichtig
Einsatz von RM-Tools	○	○	○	○
Entwicklung von gesetzlichen Auflagen und Bestimmungen	○	○	○	○
Entwicklung von ganzheitlichen IT-Riskmanagement-Konzepten	○	○	○	○
Das Thema Datenschutz gewinnt an Bedeutung	○	○	○	○
Steigende Bedeutung und Akzeptanz des IT-Riskmanagements	○	○	○	○
Wenig Fortentwicklung, wegen hoher Kostenaufwendungen oder nicht direkt erkennbarem Nutzen	○	○	○	○
Stärkere Verbreitung der Zertifizierungsanforderungen	○	○	○	○
IT-Riskmanagement auch in KMU etabliert	○	○	○	○
Aufhebung der Konzentration auf die IT-Bereiche	○	○	○	○

Wie wichtig sind Ihrer Meinung nach folgende IT-Riskmanagement Themen, welche in der heutigen Diskussion vernachlässigt werden?

	sehr wichtig	wichtig	weniger wichtig	gar nicht wichtig
IT-Riskmanagement im Rahmen von Projekten	○	○	○	○
Die Auswirkungen auf die Organisationsstruktur	○	○	○	○
Die wirtschaftliche Notwendigkeit und das damit verbundene Einsparpotential	○	○	○	○
Die hohe Komplexität der vorhandenen RM-Informationen und die damit verbundene Intransparenz	○	○	○	○
Die Wirtschaftsspionage als erhöhter Risikofaktor	○	○	○	○
Konzepte zur Mitarbeiter-Awareness	○	○	○	○
Datenschutz im Rahmen des IT-Riskmanagement	○	○	○	○
Die monetäre Bewertung der IT-Risiken	○	○	○	○
Qualität von Software	○	○	○	○
Mitarbeiter; der menschliche Faktor	○	○	○	○

<< zurück | weiter >>


UNIVERSITÄT KOBLENZ · LANDAU
IT-Riskmanagement (3. Runde)
0%
100%
4. Fragen zu Person/Unternehmen
In welcher Branche ist Ihr Unternehmen überwiegend tätig?
Bitte wählen Sie einen Punkt aus der Liste aus.
Banken
Bundeswehr
Gesundheitswesen
Handel
Hardware
Logistik und Verkehr
Medien und Unterhaltung
Netzwerktechnik
Öffentliche Verwaltung
Softwareentwicklung
Telekommunikation
Universitäten, Fachhochschulen, Schulen
Unternehmensberatung
Verarbeitende Industrie
Versicherungen
Versorgungsunternehmen
Sonstige
Welche ungefähre Größe hat Ihr Unternehmen?
weniger als 200 Mitarbeiter
200 bis 1000 Mitarbeiter
mehr als 1000 Mitarbeiter
Was ist Ihre momentane Tätigkeit in dem Unternehmen?
Wie würden Sie Ihre Expertise in Hinblick auf das spezielle Themengebiet IT-Riskmanagement einschätzen?
1 Experte
2
3
4
5
6 gering ausgeprägte Kenntnisse
<< zurück
weiter >>


UNIVERSITÄT KOBLENZ · LANDAU
IT-Riskmanagement (3. Runde)
0%
100%
5. Kontaktdaten
Dürfen wir Ihren Namen in den endgültigen Ergebnissen dieser Studie dankend erwähnen?
Ja
Nein
Möchten Sie ein Exemplar des Abschlußberichtes zu dieser Studie erhalten?
Ja
Nein
Sollten Sie eine der oben stehenden Fragen mit ja beantwortet haben, bitten wir Sie um Ihre Kontaktdaten.
An dieser Stelle garantieren wir Ihnen noch mal, dass der Fragebogen anonym ausgewertet wird. Es werden keinesfalls personenbezogene Antworten an Dritten weitergegeben.
Anrede
Frau
Herr
Vorname
Nachname
Firma
Emailadresse
Haben Sie Anregungen?
<< zurück
abschließen


UNIVERSITÄT KOBLENZ · LANDAU
IT-Riskmanagement (3. Runde)
Vielen Dank!
Sie haben nun alle Fragen dieser Umfrage beantwortet.
Klicken Sie jetzt auf 'Absenden', um diese Umfrage abzuschlissen und Ihre Antworten endgültig zu speichern.
absenden
Wenn Sie Ihre Antworten nochmal überprüfen und/oder ändern wollen, dann klicken Sie bitte auf den Knop 'Zurück', um durch Ihre Antworten zu blättern.
<< zurück

A.4 Beteiligte Firmen

Zunächst möchten wir uns bei Frau Geuhs (Computer GmbH), Herrn Fox (DuD), Herrn Romeike (risknews) für die Unterstützung bei der Kontaktierung der Experten bedanken.

Folgende Personen haben Ihr Einverständnis gegeben, namentlich als Teilnehmer dieser Studie erwähnt zu werden. Ihnen und allen anonymen Teilnehmer gilt unser besonderer Dank für Ihre Mühe und aufgewendete Zeit!

Name	Firma
Herr Herbert König	Umweltbundesamt
Herr Klaus-Guntmar Goldberg	DVZ Consulting GmbH
Herr Werner Metterhausen	VZM GmbH
Herr Wolfgang Reinert	Deutsche Telekom, T-Com
Herr Oliver Thiel	Axel Springer Verlag
Herr Jörg Metzel	Deutsche Post AG
Herr Dr. Dirk Loomans	Dr.Loomans Unternehmensberatung
Herr Karlheinz Hinterland	KHD-Consulting
Herr Gernot Sander	Universität Duisburg-Essen
Herr Olaf Krause	MIPcost GmbH
Herr Rüdiger Grimm	Technische Universität Ilmenau
Herr Dr. Christoph Herrmann	Schering
Herr Wolfgang Böhm	Fachberatung für Datenschutz und Datensicherheit
Herr Gerald Spiegel	SerCon GmbH
Herr Norbert Hermes	Broadnet AG
Herr Michael J. Erner	Datenschutz & Informationssicherheit
Herr Prof. Dr. Michael Bartsch	Bartsch und Partner Rechtsanwälte
Herr Dr. Thilo Tilemann	Linde AG
Herr Osfried Tillmanns	Siemens AG
Frau Eva Maria Knirsch	FORUM für Informationstechnologie GmbH
Herr Jürgen Grüne	Verlag M. DuMont Schauberg
Herr Thomas Schoen	Informatikzentrum der Sparkassenorganisation GmbH
Herr Gerd Jäckle	Deutsche Telekom CardService GmbH
Herr Rolf Reinema	Fraunhofer-Institut Sichere Informationstechnologie

Herr Rolf Hennig	Schott AG
Herr Matthias Temme	BTP Consulting
Herr Wolfgang Scholz	FinanazIT GmbH
Herr Olav Seyfarth	Telefónica Deutschland GmbH
Herr Holger Schönemann	TelcoMedia Consult GmbH & Co. KG
Herr Oliver Holz	Siemens AG
Herr Herbert Bieber	BWsecure
Herr Clemens Bloß	welivit AG
Herr Torsten Henkel	VICCON GmbH
Herr Tim Cole	Kuppinger Cole + Partner
Herr Paul R. Schmitz	KEVAG
Herr Günther Otten	Gothaer Finanzholding AG
Herr Oliver Prokein	Albert-Ludwigs-Universität Freiburg
Herr Berthold Heinz	Steria GmbH
Herr Firoz Kaderali	FernUniversität Hagen
Herr Norbert Book	ConSecur

Literatur

Bundesamt für Sicherheit in der Informationstechnik (2003). Leitfaden IT-Sicherheit, IT-Grundschutz kompakt. Bonn, Bundesamt für Sicherheit in der Informationstechnik, from http://www.bsi.de/gshb/Leitfaden/GS-Leitfaden.pdf.

Cuhls, K., S. Breiner, et al. (1995). Delphi-Bericht 1995 zur Entwicklung von Wissenschaft und Technik - Mini-Delphi - Endbericht an das Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie (BMBF).

Fischer, D. and J. Mohs (2002). Hacker auch im Mittelstand? Wirtschaftskriminalität mit Hilfe der IT. PriceWaterhouseCoopers Mandanten-Magazin pwc.

Gerke, W. (2003). Das Pflichtenheft des Risikomanagement. Frankfurter Allgemeine Zeitung vom 28. April 2003. Frankfurt.

Gordon, T. J. and O. Helmer (1964). Report on a long-range forecasting study. Santa Monica, California from http://www.rand.org/publications/P/P2982/P2982.pdf.

Häder, M. (2002). Delphi-Befragungen. Wiesbaden, Westdeutscher Verlag

Häder, M. and S. Häder (1995). Delphi und Kognitionsphychologie. Ein Zugang zur theoretischen Fundierung der Delphi-Methode. ZUMA-Nachrichten (Zentrum für Umfragen, Methoden und Analysen) "37" 37**:** 8-34.

Harrald, J. R. and Y. H. Kim (2003). The Survival of eCommerce Systems after the World Trade Center Attacks. eCommerce, Terrorism, and Security - Panel at the 16th Bled eCommerce Conference, Bled, Slovenia, June 9 - 11, 2003.

heise online. (2004). "Marktforscher beziffern Umsatzverluste durch schädliche Software." from http://www.heise.de/security/news/meldung/48915.

Higgins, J. M. and W. G. G. (1996). Innovationamanagement - Kreativitätstechniken für den unternehmerischen Erfolg. Berlin, Heidelberg et.al., Springer Verlag

KPMG (2004). WWW.SICHERHEIT - Angriffe auf IT-Systeme - und wie man sich schützt from http://www.kpmg.de/editvalue/pdf/sicherheit.pdf.

Krcmar, H. (2000). Informationsmanagement (2. Auflage). Berlin, Springer.

Lang, T. (1998). "An Overview of Four Futures Methodologies." from http://www.futures.hawaii.edu/j7/LANG.html.

Ludwig, B. (1997). "Predicting the Future: Have you considered using the Delphi Methodology?" Journal of Extension 35(5) from http://www.joe.org/joe/1997october/tt2.html.

Parente´, F. J., J. K. Anderson, et al. (1984). "An examination of factors contributing to Delphi accuracy." Journal of Forecasting 3(2): 173–182.

Rowe, G. and G. Wright (1999). "The Delphi technique as a forecasting tool: issues and analysis." International Journal of Forecasting 15: 353–375 from http://www-marketing.wharton.upenn.edu/forecast/paperpdf/delphi%20technique%20Rowe%20Wright.pdf.

Turoff, M. and H. Linstone (2002). The Delphi Method: Techniques and Applications from http://www.is.njit.edu/pubs/delphibook/.

Woudenberg, F. (1991). "An Evaluation of Delphi." Technological Forecasting and Social Change 40: 131–150.

Bisher erschienen

Arbeitsberichte des Fachbereichs Informatik

(http://www.uni-koblenz.de/fb4/publikationen/arbeitsberichte)

Anastasia Meletiadou, J.Felix Hampe: Begriffsbestimmung und erwartete Trends im IT-Risk-Management, Arbeitsberichte aus dem Fachbereich Informatik, 1/2007

„Gelbe Reihe“

(http://www.uni-koblenz.de/fb4/publikationen/gelbereihe)

Lutz Priese: Some Examples of Semi-rational and Non-semi-rational DAG Languages. Extended Version, Fachberichte Informatik 3-2006

Kurt Lautenbach, Stephan Philippi, and Alexander Pinl: Bayesian Networks and Petri Nets, Fachberichte Informatik 2-2006

Rainer Gimnich and Andreas Winter: Workshop Software-Reengineering und Services, Fachberichte Informatik 1-2006

Kurt Lautenbach and Alexander Pinl: Probability Propagation in Petri Nets, Fachberichte Informatik 16-2005

Rainer Gimnich, Uwe Kaiser, and Andreas Winter: 2. Workshop "Reengineering Prozesse" – Software Migration, Fachberichte Informatik 15-2005

Jan Murray, Frieder Stolzenburg, and Toshiaki Arai: Hybrid State Machines with Timed Synchronization for Multi-Robot System Specification, Fachberichte Informatik 14-2005

Reinhold Letz: FTP 2005 – Fifth International Workshop on First-Order Theorem Proving, Fachberichte Informatik 13-2005

Bernhard Beckert: TABLEAUX 2005 – Position Papers and Tutorial Descriptions, Fachberichte Informatik 12-2005

Dietrich Paulus and Detlev Droege: Mixed-reality as a challenge to image understanding and artificial intelligence, Fachberichte Informatik 11-2005

Jürgen Sauer: 19. Workshop Planen, Scheduling und Konfigurieren / Entwerfen, Fachberichte Informatik 10-2005

Pascal Hitzler, Carsten Lutz, and Gerd Stumme: Foundational Aspects of Ontologies, Fachberichte Informatik 9-2005

Joachim Baumeister and Dietmar Seipel: Knowledge Engineering and Software Engineering, Fachberichte Informatik 8-2005

Benno Stein and Sven Meier zu Eißen: Proceedings of the Second International Workshop on Text-Based Information Retrieval, Fachberichte Informatik 7-2005

Andreas Winter and Jürgen Ebert: Metamodel-driven Service Interoperability, Fachberichte Informatik 6-2005

Joschka Boedecker, Norbert Michael Mayer, Masaki Ogino, Rodrigo da Silva Guerra, Masaaki Kikuchi, and Minoru Asada: Getting closer: How Simulation and Humanoid League can benefit from each other, Fachberichte Informatik 5-2005

Torsten Gipp and Jürgen Ebert: Web Engineering does profit from a Functional Approach, Fachberichte Informatik 4-2005

Oliver Obst, Anita Maas, and Joschka Boedecker: HTN Planning for Flexible Coordination Of Multiagent Team Behavior, Fachberichte Informatik 3-2005

Andreas von Hessling, Thomas Kleemann, and Alex Sinner: Semantic User Profiles and their Applications in a Mobile Environment, Fachberichte Informatik 2-2005

Heni Ben Amor and Achim Rettinger: Intelligent Exploration for Genetic Algorithms – Using Self-Organizing Maps in Evolutionary Computation, Fachberichte Informatik 1-2005