

Inhalt

Einleitung	3
IT-Risk Assessment	4
Risikoanalyse	4
Messung von IT-Risiken mit ORSA	6
Das Risikoprofil als Basis der Risikomessung.....	7
Durchführung von Self-Assessments mit ORSA	10
Auswertung der Assessments mit ORSA	12
Analyse der Ergebnisse	13
Unser modulares Leistungsangebot	14
Vorbereitungs-Checkliste.....	15

Einleitung

Um auf die raschen Veränderungen des Marktes und die damit einhergehende zunehmende Komplexität reagieren zu können, ist eine leistungsstarke und hundertprozentig zuverlässige IT-Infrastruktur unbedingt notwendig. Die IT ist ein maßgeblicher Faktor zur Sicherstellung der Wettbewerbsfähigkeit.

Hohe Aufwendungen für Wartung, Einbindung neuer Anwendungen sowie die Abbildung neuer Prozesse machen die Datenverarbeitung zeitintensiv und kostspielig. Mit zunehmender Komplexität der IT-Landschaft steigt auch die Zahl der IT-Risiken.

Nicht zuletzt auch als Teilaspekt von Operational Risks sind IT-Risiken allen Geschäftsprozessen inhärent. Zu spät oder schlimmstenfalls nicht erkannte Sicherheitslücken oder unzureichende Notfallplanungen können schnell zu Vorfällen werden, die das gesamte Unternehmen bedrohen. Als Beispiel seien hier nur Virenattacken genannt, die viele Unternehmen in ihrer Geschäftsausübung gefährlich behindern. Viele dieser Ereignisse sind verhältnismäßig leicht zu vermeiden, stehen den potenziell verursachten Schäden doch häufig vergleichsweise geringfügige Investitionen zu ihrer Vermeidung gegenüber.

Die IT steht in vielen Unternehmen vor einem kaum lösbaren Problem. Einerseits muss sie immer komplexere Dienstleistungen erbringen und andererseits die durch sie verursachten Kosten deutlich senken. Damit ein hinreichender Investitionsschutz gewährleistet werden kann, muss das Managen von IT-Risiken Teil des gesamtheitlichen IT-Managements werden und dadurch zur strategischen Aufgabe für das Gesamtunternehmen.

Durch gesetzliche Rahmenbedingungen wie KonTraG oder auch Basel II ist ein extern induzierter Handlungsbedarf gegeben, Operational Risks und somit auch IT-Risiken hinreichend zu messen und zu managen. Nicht zuletzt sind auch andere Unternehmen als Finanzdienstleister durch Basel II gezwungen, ihre Kreditwürdigkeit und damit ihre Kreditkonditionen auch durch das Management von Operational Risks zu verbessern, da sie eines der vielen Rating-Kriterien darstellen.

IT-Risk Assessment

Risikoanalyse

Risiken im IT-Bereich sind, sofern keine Verlustereignisse zu ihrer Abschätzung herangezogen werden können und somit Vergleichswerte bestehen, in den seltensten Fällen eindeutig zu quantifizieren. Ähnlich wie andere Operational Risks werden sie in der Regel nur durch qualitative Indikatoren bestimmbar. Dies liegt im wesentlichen an der Schwierigkeit, die Auswirkungen eingetretener Ereignisse auf das Gesamtunternehmen abzuschätzen. Ursachen für IT-Risiken können vielfältig sein. Sie beschränken sich nicht ausschließlich auf die Technik, sondern sind auch im organisatorischen oder personellen Bereich zu suchen:

- Mangelnde Infrastruktur (fehlende Gebäudeabsicherungen oder überlastete Systeme)
- Fehler im Personalbereich (unzureichend geschultes Personal, unbesetzte Stellen)
- Mängel in der Vertragsgestaltung mit externen Dienstleistern (Stichwort „Service-Level-Agreements“)
- Strategische Fehler (unvollständige Notfallplanung, mangelhafte Backup-Strategie)
- Sicherheitsverletzungen (kriminelle Handlungen, unberechtigte Zugriffe auf geschützte Daten, etc.)

Die **Vorteile** einer unternehmensweiten IT-Risikoanalyse liegen auf der Hand:

- Erkennung von Schwachstellen durch die Identifikation risikosensitiver Bereiche
- Inventarisierung der firmeninternen IT-Risiken
- Unterstützung der Erfüllung von gesetzlichen Anforderungen aus KonTraG und Basel II (Operational Risks)
- Grundlage zum Aufbau eines unternehmensweiten Sicherheitskonzeptes
- Unterstützung bei der Investitionsplanung
- Stärkung des generellen Sicherheitsbewusstseins
- Schaffung einer allgemeinen Awareness

Eine IT-Risikoanalyse sollte nicht primär zur Berechnung einer potenziellen Schadenshöhe der Risiken benutzt werden. Sie soll vielmehr zur positiven Veränderung der Risikosituation durch Ableitung von Maßnahmen zur Minimierung oder Vermeidung der Risiken beitragen.

Messung von IT-Risiken mit ORSA

Acrys Consult hat sich für einen qualitativen Ansatz zu Messung von IT-Risiken durch Self-Assessments entschieden.

Das Self-Assessment hat anderen Verfahren gegenüber deutliche Vorteile:

- Es ermöglicht die Erfassung aller risikorelevanten Indikatoren
- Qualitative Indikatoren werden messbar
- Es ist im Vergleich zu anderen Methoden kostengünstig
- Der Zeitaufwand für die Implementierung und Durchführung ist vergleichsweise gering

Grundlage des Self-Assessments ist ein Fragenkatalog, der auf ein alle wesentlichen IT-Risiken abdeckendes, kundenspezifisch anpassbares *Risikoprofil* aufbaut. Das *Risikoprofil*, die Durchführung des Self-Assessments mit der Erfassung der Ergebnisse und die anschließende Auswertung und Reportgenerierung sind Teil von ORSA, dem integrierten Tool zur Messung von IT-Risiken.

ORSA unterstützt den gesamten Prozess der Risikomessung durch

- Messbarmachung der über das Self-Assessment erfassten IT-Risiken mit einem flexiblen Scoring-Verfahren.
- Systematische Aufbereitung der Risikobereiche über flexible Gestaltung von Risikoreports
- Anpassung des *Risikoprofils* an die spezifischen Bedürfnisse über den Aufbau benutzerdefinierter Self-Assessments
- Ein flexibles Scoring-Verfahren, das die Hervorhebung risikosensitiver Bereiche ermöglicht
- Langfristige Beobachtung der IT-Risiken durch periodische Überwachung (Trendanalysen)
- Einfache Möglichkeiten zur Erweiterung und Anpassung des *Risikoprofils*

Alle Funktionen in ORSA, wie auch das Risikoprofil, sind zweisprachig in deutsch und englisch verfügbar.

Das Risikoprofil als Basis der Risikomessung

Das Risikoprofil ist die Basis von ORSA. In ihm sind alle Fragen zur Erkennung von IT-Risiken in einem strukturierten Baum abgebildet. Abbildung 1 zeigt einen Ausschnitt aus dem Aufbau des Risikoprofils.

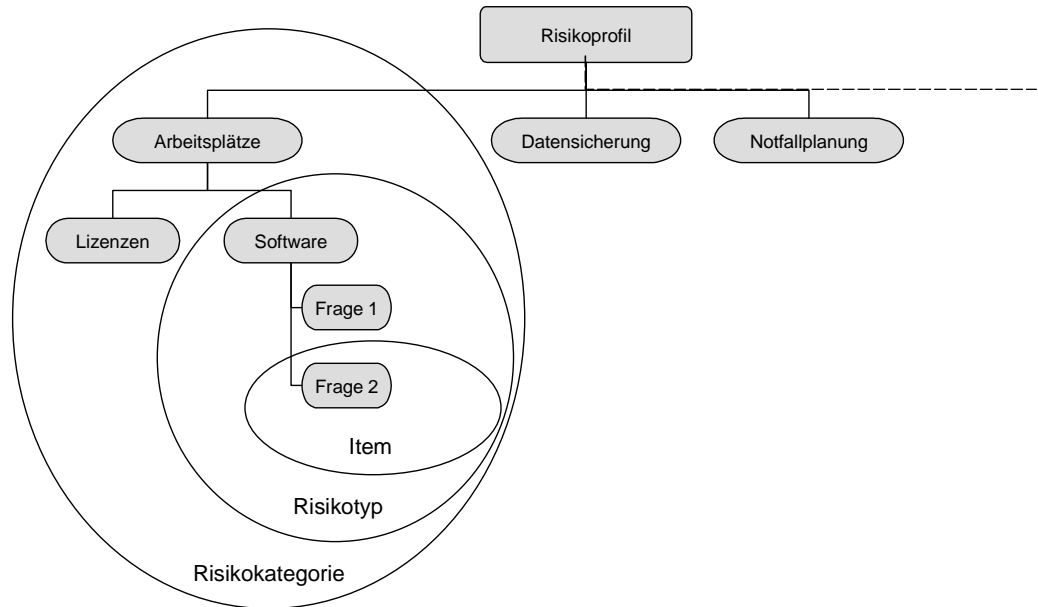


Abbildung 1: Aufbau Risikoprofil

Die einzelnen *Risikokategorien* bilden Teilbäume innerhalb des Risikoprofils. Sie sind thematisch übergeordnete Einheiten, die Themenkomplexe wie beispielsweise ‚Arbeitsplätze‘ oder ‚Datensicherung‘ beschreiben.

Innerhalb dieser Themenkomplexe werden Teilaspekte der Risikokategorien, *Risikotypen* genannt beschrieben. *Risikotypen* sind Teilmengen der Risikokategorien. So sind beispielsweise in der *Risikokategorie* Arbeitsplatz die *Risikotypen* ‚Lizenzen‘, ‚Software‘, usw. angeordnet.

Die spezifischen IT-Risiken, die in der Kombination aus *Risikotyp* und *Risikokategorie* bestehen, werden durch Fragen, *Items* genannt, erfasst. Sie sind die kleinste Einheit des Risikoprofils. Einem *Risikotyp* sind in der Regel mehrere *Items* zugeordnet.

Grundsätzlich ist die Zahl der *Risikokategorien*, die Zahl der ihnen untergeordneten *Risikotypen* als auch die Zahl der *Items* pro Risikotyp nicht beschränkt. Dies erlaubt eine flexible Anpassung des Risikoprofils an unternehmensspezifische Bedürfnisse.

Risikokategorien, *Risikotypen* und *Items* sind so gewählt, dass sie sich flexibel und aufgabengerecht zu verschiedenen, unternehmens- oder bereichsspezifischen Self-Assessments zusammenstellen lassen.

Der in unserem Analyse-Tool ORSA hinterlegte Fragenkatalog enthält etwa 290 einzelne Items auf 19 Risikotypen verteilt. Insgesamt kann damit wahlweise Ihr individuelles IT-Risk Assessment mit folgenden Kategorien abgedeckt werden:

Aktive Komponenten
Akzeptanz
Arbeitsplatz
Betrieb
Controlling
Datenschutz
Datensicherung
Dokumentation
Externe Anbindungen
Management
Notfallplanung
Personal
Räumlichkeiten
Serversysteme
Sicherheitskonzept
Strategie
Support
Peripherie
Verkabelung

Abbildung 2 zeigt einen Ausschnitt des Risikoprofils und seine Abbildung im ORSA-Tool.

Risikoprofil Items				
Kategorie	Typ	Bezeichnung		
Arbeitsplatz	Software		Sprachauswahl <input checked="" type="radio"/> deutsch <input type="radio"/> english	
Arbeitsplatz	Hardware	204001	Wieviel % der Arbeitsplätze sind für ihren Einsatz ausreichend dimensioniert? Prozent: 100 / < 25	
	Lizenzen	205001	Wieviel % der Arbeitsplatz-Software ist lizenziert? Prozent: 100 / < 25	
	Software	206001	Wie gut ist das Freigabeverfahren für neue SW / HW standardisiert? Schulnoten "sehr gut", "gut" ...	
		206002	Bei wieviel % der SW- Installationen wird vor Installation die ausreichende Leistungsfähigkeit der Zielsysteme sichergestellt? Prozent: 100 / < 25	
		206003	Wieviel % der Arbeitsplätze sind nach einem einheitlichen Standard installiert? Prozent: 100 / < 25	

Datensatz: 16 von 278

Abbildung 2: Ausschnitt Risikoprofil

Jedem Item ist zur Erfassung der Ergebnisse eine spezifische Bewertungsskala zugeordnet, die eine Aufteilung in maximal sechs Bereiche (ähnlich wie beim Schulnotensystem) ermöglicht. Anhand der Skalen werden während des Self-Assessments die Antworten auf die Fragen erfasst. Die Skalen sind so gewählt, dass eine Erfassung sinnvoller Ergebnisse für jedes *Item* sichergestellt ist.

Abbildung 3 zeigt eine Beispielskala in ORSA.

Risikoprofil Skalen						
Name						
Prozent: 100 / < 25						
deutsch english						
Note 1	Note 2	Note 3	Note 4	Note 5	Note 6	
100%	>95%	>75%	>50%	>25%	<25%	
Anmerkungen / Remarks						
<input type="button" value="◀"/> <input type="button" value="🔍"/> <input type="button" value="▶"/> <input type="button" value="▶*"/> <input type="button" value="✖"/> <input type="button" value="🔍"/>						
Datensatz: 13 von 18						

Abbildung 3: Beispielskala

Durchführung von Self-Assessments mit ORSA

Um eine exakte Anpassung der Risikoanalyse an die Anforderungen der IT-Infrastruktur zu ermöglichen, können Self-Assessments gemäß den Anforderungen aus beliebigen *Risikotypen* des Risikoprofils zusammengestellt werden. Dadurch wird es möglich, eine beliebige Anzahl maßgeschneiderter Self-Assessments für verschiedene Zielpersonen wie beispielsweise Sicherheitsbeauftragte oder Administratoren zusammenzustellen.

Der Aufbau der Self-Assessments orientiert sich an der Struktur des Risikoprofils. Die einzelnen Items werden strukturiert nach Risikotypen und Kategorien erfasst.

Abbildung 4 zeigt, wie ein Self-Assessment in ORSA aufgebaut wird.

The screenshot displays the 'Assessment Aufbau' interface. On the left, there are input fields for 'Assessment' (Testassessment), 'Datum', 'Nummer' (5), 'Bearbeiter (Nachname, Vorname)' (User, Test), and 'Einheit, Abteilung' (IT-Management). A table on the right lists categories and risk types:

Kategorie	Risikotyp
aktive Komponenten	Stromversorgung
Arbeitsplatz	Lizenzen
Arbeitsplatz	Software
Arbeitsplatz	Virenschutz
Datensicherung	Konzept
Dokumentation	Allgemein

Navigation buttons (-10, +10, etc.) and a status bar at the bottom indicate the current record (1 von 7) and page (2 von 2).

Abbildung 4: Aufbau eines Self-Assessments

Die Durchführung der Self-Assessments kann entweder direkt mit ORSA erfolgen, oder es können Self-Assessments in Papierform durchgeführt und deren Ergebnisse anschließend in das Tool zur Auswertung und Reportgenerierung übertragen werden.

Abbildung 5 zeigt die Abfrage eines Items mit ORSA.

Assessment Fragebogen bearbeiten

deutsch | **englisch**

Assessment Nr.	Name	Bearbeiter (Nachname, Vorname)		Einheit, Abteilung
5	Testassessment	User	Test	IT-Management

Kategorie	Risikotyp	Bezeichnung
Arbeitsplatz	Software	206002

Assessment Frage

Bei wieviel % der SW- Installationen wird vor Installation die ausreichende Leistungsfähigkeit der Zielsysteme sichergestellt?

Kommentar

Rating

100%	>95%	>75%	>50%	>25%	<25%
1	2	3	4	5	6

Assessment Status
Daten erfasst am 21.03.2002 um 15.25.48

Datensatz: 12 von 32 (Gefiltert)

Abbildung 5: Self-Assessment Ergebniserfassung

Auswertung der Assessments mit ORSA

Die Self-Assessment-Ergebnisse werden in Reports dargestellt. Ein Report kann aus den Ergebnissen mehrerer Risikotypen aus beliebigen Self-Assessments zusammengestellt werden. Sollen beispielsweise mehrere Self-Assessments, die zu verschiedenen Risikokategorien durchgeführt wurden, zu einem unternehmensweiten Report zusammengestellt werden, so lassen sich die Ergebnisse zu einem IT-Risikoreport zusammenstellen.

Abbildung 6 zeigt einen beispielhaften Report, der aus zwei Risikotypen des gleichen Self-Assessments besteht. Der Score des Risikotyps repräsentiert seine Risikobewertung auf einer Skala von 1 bis 6 (analog dem Schulnotensystem).

Um eine höhere Sensibilisierung des Reports bezüglich einzelner Risikotypen zu erzeugen, kann die Gewichtung der einzelnen Risikotypen innerhalb eines Reports durch den Benutzer zueinander verändert werden.

Zusätzlich zu den Scores, die eine detaillierte Betrachtung der Risiken erlauben, wird über eine Ampel eine schnelle Beurteilung der Ergebnisse ermöglicht. Grün repräsentiert hierbei geringe und Rot hohe Risiken.

Abbildung 6 zeigt die Zusammenfassung mehrerer Risikotypen zu einem Report.

Report Ergebnis

Reportname		Erstellt am	Berichtempfänger (Nachname, Vorname)	
Testassessment		21.03.2002	User	Test
gelb	Ø Score	Reportnummer	Einheit, Abteilung	
	3,05	13	IT-Management	
Score	Kategorie	Typ	Assessmentname	Fällig bis
2,83	aktive Komponenten	Konfiguration	Testassessment	21.03.2002
3,33	aktive Komponenten	Stromversorgung	Testassessment	21.03.2002
1,00	Arbeitsplatz	Lizenzen	Testassessment	21.03.2002
3,22	Arbeitsplatz	Software	Testassessment	21.03.2002
3,50	Arbeitsplatz	Virenschutz	Testassessment	21.03.2002
2,44	Datensicherung	Konzept	Testassessment	21.03.2002
5,00	Dokumentation	Allgemein	Testassessment	21.03.2002

Datensatz: 14 | 2 | von 7 (gefiltert)

Abbildung 6: Report Ergebnis

Analyse der Ergebnisse

Über die Reports von ORSA können die Ergebnisse aus den Assessments in mehreren unterschiedlichen Darstellungsformen und Granularitäten zusammengefasst werden.

Die Zusammenfassung der Ergebnisse in den Reports ist jedoch nicht der Schlusspunkt der Risikoanalyse. Der Bestimmung der Risiken folgt eine Ableitung von Maßnahmen, die nach ihrer Dringlichkeit priorisiert werden. Diese Maßnahmen müssen Teil der IT-Strategie werden, um so aktiv zur Risikoreduzierung beizutragen.

Unterstützt durch Trendanalysen über die regelmäßige Durchführung von Self-Assessments können sowohl risikosensitive Bereiche als auch Bereiche, in denen Routine die Qualität gefährdet, langfristig überprüft werden.

In Abhängigkeit von den Assessment-Ergebnissen können auf Wunsch die besonders risikoempfindlichen bzw. kritischen Bereiche im Anschluss einer detaillierten Analyse unterzogen werden.

Fazit: IT-Risiko Management muss Teil der unternehmensweiten IT-Strategie werden, um gleichbleibende Qualität der IT-Lösungen und IT-Dienstleistungen messen und somit garantieren zu können.

Unser modulares Leistungsangebot

Wir erheben, analysieren und bewerten die IT-Risiken in Ihrem Unternehmen – einmalig bzw. regelmäßig. Gleichzeitig unterstützen wir Sie zielführend bei der Ableitung, Priorisierung und Durchführung von Maßnahmen zur Risikoreduzierung.

Wir bieten Ihnen unser Know-how in Modulen an:

IT-Risk Assessments

- Parametrisierung des Risikoprofils in ORSA an kundenspezifische Anforderungen
- On-Site Durchführung der IT-Risk Assessments
- Analyse und Auswertung von IT-Risk Assessments
- Ableitung von Maßnahmen und Empfehlungen aus den Analyseergebnissen der IT-Risk Assessments
- Trendanalysen und neutrales Monitoring von Maßnahmen und deren Erfolgen

Workshops

- Aufbereitung und Präsentation der Ergebnisse und Maßnahmen
- Schaffung von Awareness
- Schulung zur Durchführung von IT-Risk Assessments mit ORSA

Vorbereitungs-Checkliste

Um die Beantwortung der Fragen des Assessments zu erleichtern und eine zielgerichtete und effiziente Durchführung zu gewährleisten, sind seitens des Kunden einige Vorbereitungen nötig, die in drei Vorbereitungs-Checklisten thematisch zusammengefasst sind. Im Folgenden werden Auszüge aus diesen Listen wiedergegeben.

1) Zugang

Im Rahmen einer Ortsbegehung sollte der Zugang zu folgenden Räumen möglich sein:

Serverräume	
Verteilerschränke	Patch-Schränke, akt. Komponenten, Telefonie etc.
Notstromversorgung	Batterieräume, Notstromaggregate etc.
Datensicherung	Aufbewahrung der Datensicherungsmedien

2) Ansprechpartner

Know-how Träger aus folgenden Bereichen sollten zur Beantwortung der Fragen herangezogen werden können:

Akt. Komponenten	Konfiguration
Verkabelung	Konzeption, Installation
Netzwerk Administration	Serversysteme, Redundanz, Netzwerkmanagement, Benutzerverwaltung
Datensicherung	Konzeption, Durchführung
Support	Help-Desk, interner und externer Support
Arbeitsplatzsysteme	Installation, Hardware
Endanwender	
Betrieb	
Datenschutz	Konzeption
IT-Leitung	Notfallplanung, Sicherheitskonzeption, IT-Strategie
Externe Anbindungen	Internet, Firewall, eMail, Remote Access
IT-Sicherheitsbeauftragter	
Personal	Schulung, Organisation der IT-Abteilungen
Sicherheitsdienst	Zugangskontrollen
Haustechnik	Elektrik etc.

3) Dokumentation

Um spezifische Fragen zur Dokumentation beantworten zu können, müssen folgende Dokumente elektronisch oder in Papierform verfügbar sein:

Dokumentation Netzwerk	<ul style="list-style-type: none"> • Verkabelung (Lage der Kabeltrassen, Patch-Panel etc.) • Belegung der akt. Komponenten, Patch-Panel • Netzplan • Externe Anbindungen
Handbücher	<ul style="list-style-type: none"> • Arbeitsplatzsysteme • Serversysteme • Akt. Komponenten • Software
Bestandslisten	<ul style="list-style-type: none"> • Hardware (Server, akt. Komponenten, Arbeitsplatzsysteme) • Software (Server, akt. Komponenten, Arbeitsplatzsysteme)
Betrieb	<ul style="list-style-type: none"> • Betriebshandbuch • Schichtprotokoll
Datenschutz	Bestimmungen, Richtlinien
Konzepte	<ul style="list-style-type: none"> • Datensicherung • Notfallkonzept, Notfallhandbuch • Benutzerrechte • Sicherheitskonzept • Netzwerk Management • IT-Strategie
Räumlichkeiten	<ul style="list-style-type: none"> • Zugangsrechte • Lage der IT-Komponenten
Administration	Admin-Journal
Support	Supportstatistik

Kontakt

Ihr Ansprechpartner
Acrys Consult GmbH & Co. KG Barbara Dilges-Maruska +49 69 24 45 06 16 barbara.dilges@acrys.com www.acrys.com