

IT-Risk Assessment mit ORSA

Eine leistungsfähige IT ist einer der maßgeblichen Faktoren zur Sicherstellung der Wettbewerbsfähigkeit. IT-Risiken sind, nicht zuletzt als Teilaspekt von Operational Risks, allen Geschäftsprozessen inhärent. Sie beschränken sich nicht ausschließlich auf die Technik, sondern sind auch im organisatorischen oder personellen Bereich zu suchen und können schnell zu Vorfällen werden, die das gesamte Unternehmen bedrohen. Viele dieser Ereignisse sind verhältnismäßig leicht zu vermeiden, stehen den potenziell verursachten Schäden doch häufig vergleichsweise geringfügige Investitionen zu ihrer Vermeidung gegenüber.

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.

Risikoanalyse

IT-Risiken sind überwiegend nicht quantifizierbare Risiken, sondern sind in erster Linie qualitativer Natur. Daher führt eine IT-Risikoanalyse durch Berechnung von potenziellen Schadenshöhen der Risiken nicht zum Ziel, da die Mehrzahl der Risiken nicht berücksichtigt würde.

Die Ergebnisse der IT-Risikoanalyse sollen vielmehr zur positiven Veränderung der Risikosituation (Minimie-

rung oder Vermeidung) durch Ableitung von Maßnahmen beitragen.

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

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

Messung von IT-Risiken mit ORSA

Acrys Consult hat sich für einen qualitativen Ansatz zur Messung von IT-Risiken über Assessments entschieden.

Dieser Ansatz hat gegenüber anderen Verfahren gegenüber deutliche Vorteile:

- Er ermöglicht die Erfassung aller risikorelevanten Indikatoren
- Qualitative Indikatoren werden messbar
- Er ist im Vergleich zu anderen Methoden kostengünstig und rasch zu implementieren

ACRYS CONSULT
GMBH & CO. KG

Untermainkai 29-30
D-60329 Frankfurt

Tel: +49-69-24 45 06-0
Fax: +49-69-24 45 06-50

ACRYS CONSULT

Schwerzelweg 18
CH-6315 Oberaegeri

Tel: +41-41-750 7700
Fax: +41-41-750 7677

ACRYS CONSULT USA

310 Carroll Close
Tarrytown, NY 10591

Tel: +1-917-533 5216
Fax: +1-914-206 4254

www.acrys.com

Grundlage des Assessments ist ein Fragenkatalog, der auf ein alle wesentlichen IT-Risiken abdeckendes, kundenspezifisch anpassbares *Risikoprofil* aufbaut.

Das *Risikoprofil*, der Aufbau des Assessments, die Erfassung der Ergebnisse, der Aufbau der Reports mit der Auswertelogik, sowie die Reportgenerierung gruppieren sich als Module von ORSA um eine zentrale Datenbank zur Sicherung und Historisierung aller Parameter (siehe Abbildung 1)

Das in ORSA hinterlegte Risikoprofil, aus dem die Fragebögen zusammengestellt werden, enthält etwa 290 einzelne Items (Einzelfragen), die 19 Risikotypen (thematisch übergeordnete Einheiten wie beispielsweise IT-Strategie, Notfallplanung oder Datenschutz) zugeordnet sind.

Über die Reports in ORSA können die Ergebnisse aus den Assessments in mehreren unterschiedlichen Darstellungsformen und

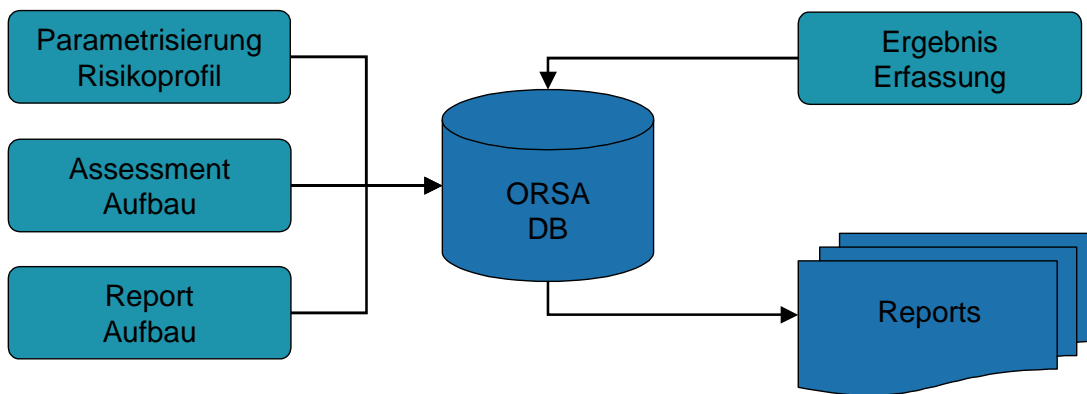


Abbildung1: Modularer Aufbau von ORSA

ORSA unterstützt den gesamten Prozess der Risikomessung durch

- Messbarmachung der über das Assessment erfassten IT-Risiken mit einem flexiblen Scoring-Verfahren, das die Hervorhebung risikosensitiver Bereiche ermöglicht.
- systematische Aufbereitung der Risikobereiche über flexible Gestaltung von Risikoreports.
- Anpassung des *Risikoprofils* an die spezifischen Bedürfnisse über den Aufbau benutzerdefinierter Assessments.
- langfristige Beobachtung der IT-Risiken durch periodische Überwachung (Trendanalysen).
- einfache Erweiterung und Anpassung des *Risikoprofils*.
- Mehrsprachigkeit (deutsch, englisch).

Granularitäten zusammengefasst und dargestellt 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.

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.

Sprechen Sie mit uns. Wir informieren Sie gerne näher.

ACRYS CONSULT
GMBH & Co. KG

Untermainkai 29-30
D-60329 Frankfurt

Tel: +49-69-24 45 06-0
Fax: +49-69-24 45 06-50

ACRYS CONSULT

Schwerzelweg 18
CH-6315 Oberaegeri

Tel: +41-41-750 7700
Fax: +41-41-750 7677

ACRYS CONSULT USA

310 Carroll Close
Tarrytown, NY 10591

Tel: +1-917-533 5216
Fax: +1-914-206 4254

www.acrys.com

YOU CAN'T STAY AHEAD BY STANDING STILL.

Acrys Consult ist Ihr kompetenter Business- und IT-Beratungspartner.