

# Studie zu IT-Risikobewertungen in der Praxis

Stefan Taubenberger<sup>1</sup> Jan Jürjens<sup>2</sup>

<sup>1</sup>MunichRe, Germany  
[staubenberger@munichre.com](mailto:staubenberger@munichre.com)

<sup>2</sup>TU Dortmund & Fraunhofer ISST, Germany  
<http://www.jurjens.de/jan>

## Zusammenfassung

Das Ziel der Studie war, die derzeitige Praxis bei Risikobewertungen unter Sicherheitsexperten zu untersuchen insbesondere das Vorgehen und die Kriterien in der Risikobewertung, die Nutzung von Sicherheitsanforderungen und das Vertrauen in Risikobewertungen. Die Ergebnisse aus der Studie zeigen, dass Risikoergebnisse größtenteils auf Expertenschätzungen beruhen, Best-Practice Risikobewertungsverfahren verwendet werden und eine Datenbank zu Datenobjekten und IT-Systemen vorhanden ist sowie Sicherheitsanforderungen und Bedrohungen dokumentiert sind. Zudem werden Risikobewertungen als durch das Management und externe Ereignisse beeinflusst angesehen sowie als schwierig zu objektivieren. Weiterhin hat eine Risikobewertung durch die Teilnehmer in der Umfrage gezeigt, dass Risiken korrekter identifiziert werden, wenn Informationen wie z.B. Sicherheitsanforderungen vorliegen und benutzt werden sowie auch das falsche Annahmen getroffen werden, wenn diese Informationen fehlen. Zukünftige Weiterentwicklungen von IT-Risikobewertungsverfahren sollten auf die Integration der Risikoergebnisse wie auch des Bewertungsvorgangs in eine unternehmensweite Risikodarstellung abzielen sowie bestehende Daten nutzen und erweitern.

## 1 Gesamtzusammenfassung

Ziel der konfirmativen und explorativen Studie „Durchführung von IT-Risikobewertungen und die Nutzung von Sicherheitsanforderungen in der Praxis“ ist es herauszufinden, welche und wie Kriterien und Objekte in der IT-Risikobewertung verwendet werden sowie aufzuzeigen, dass Daten wie Prozessmodelle, Sicherheitsanforderungen und Datenklassifikation in der Praxis vorhanden sind und wie diese genutzt werden. Die Studie basiert auf einer Umfrage unter ca. 50 Teilnehmern, die im Rahmen eines Vortrags vor Sicherheitsexperten aus der Praxis im Februar 2011 durchgeführt wurde. Im Folgenden werden die Hauptergebnisse der Studie dargestellt, die aus den Fragen und Antworten der Teilnehmer der Studie gewonnen wurden.

Die meisten Unternehmen führen IT-Risikobewertungen periodisch mit Schwerpunkten durch. Die verwendeten Standards/Methoden zur IT-Risikobewertung sind meist Best-Practice-Methoden, die konkrete Maßnahmen vorgeben welche z.B. Sicherheitsprozesse, Kontrollen oder Sicherheitsmaßnahmen zu implementieren sind. Die Identifikation und Bewertung von Risiken von Assets wird hauptsächlich durch Expertenwissen und Systemtests vorgenommen. Andere Methoden oder Hilfsmittel werden kaum verwendet. In etwa 80 Prozent der

Teilnehmer verwendet ein Repository in dem Daten über Assets (Daten, IT-Systeme), Sicherheitsanforderungen und Bedrohungen dokumentiert sind. Im Rahmen der Risikobewertung werden größtenteils die Kontrollen der geprüften Assets mit Schwächen überprüft. Die meisten Teilnehmer stimmen zu, dass Risiken nicht objektiv zu bestimmen sind und dass Risikobewertungen beeinflusst sind durch unternehmensinterne und externe Einflüsse.

Als Treiber für die Geschäftsprozessmodellierung werden regulatorische Anforderungen sowie Produktivitätssteigerungen und Effizienz gesehen. In den meisten Unternehmen, ca. 80 Prozent, sind kritische bzw. wichtige Prozesse modelliert und diese auch aktuell. Risiken, Kontrollen oder Sicherheitsanforderungen werden nicht modelliert. Bei 90 Prozent der Teilnehmer werden Objekte wie z.B. IT-Systeme, Daten oder Prozesse nach Vertraulichkeit, Integrität und Verfügbarkeit klassifiziert und Sicherheitsanforderungen sind dokumentiert. Sicherheitsanforderungen werden teilweise im Rahmen der Risikobewertung für Assets und der Identifikation von Threats verwendet. Zudem sind 70 Prozent der Teilnehmer überzeugt, dass Risiken genauer und besser bestimmt werden können mit der Evaluierung von Sicherheitsanforderungen sowie auch das die Bewertung von Maturity und Performance von IT Prozessen zu beständigeren Risikobewertungen führen könnte. Die meisten Unternehmen messen nicht aktiv die Sicherheit von Daten, nutzen jedoch Sicherheitsanforderungen um die Datensicherheit zu überprüfen.

Die Ergebnisse der Risikobewertung der Teilnehmer in der Studie zeigen, dass Risiken korrekter identifiziert werden je mehr Informationen wie z.B. Sicherheitsanforderungen, Prozessmodelle... vorliegen. Allerdings ist es den Teilnehmer schwer gefallen Risiken bei komplexen Sachverhalten korrekt zu identifizieren. Zudem wurde ersichtlich, dass im Rahmen der Risikobewertung Annahmen getroffen werden, wenn Informationen nicht bzw. nicht präzise vorliegen, die direkten Einfluss auf die Risikoidentifikation sowie das Ergebnis haben. Die Darstellung der Risikoergebnisse auf Basis der betroffenen Daten, der Prozesse und verletzten Sicherheitsanforderungen wurde von ca. 90 Prozent der Teilnehmer als hilfreicher bewertet wie nur eine Darstellung mit Wahrscheinlichkeiten und Auswirkungen.

Zukünftige Entwicklungen bei IT-Risikobewertungsverfahren sollten auf die Integration der Risikoergebnisse wie auch des Bewertungsvorgangs in eine unternehmensweite Risikodarstellung abzielen. Erst mit Verbindung zum zentralen Risikomanagement kann eine unternehmensweite Gesamtrisikosicht erstellt werden, die für die Erfüllung von regulatorischen Anforderungen nötig ist. Aber auch die Integration der Verfahren und Ergebnisse in das Sicherheits- und Compliance Monitoring sollte angestrebt werden, nicht nur als Effizienzgründen sondern auch aufgrund der Harmonisierung von Bewertungen. Weiterhin sollte versucht werden die Datenbasis zu erweitern sowie auch den Bewertungsvorgang zu objektivieren. Als Daten sollten nicht nur die Assets, Sicherheitsanforderungen, Kontrollen und Bedrohungen vorliegen sondern auch Schadensvorfälle, -potentiale, Szenarios sowie auch die Abhängigkeiten zwischen Assets, Prozessen und Schadensvorfällen, um Risiken besser und auch automatisiert analysieren und bewerten zu können. Zudem sollten Risikobewertungsverfahren auf unternehmensspezifische Informationen wie z.B. Sicherheitsanforderungen aufbauen die eine präzise Identifikation der Risiken im Kontext des Geschäftsbetriebs ermöglichen, um Annahmen und Schätzfehler zu reduzieren sowie unternehmensspezifische Anforderungen abzubilden. Idealerweise nutzen alle Risikobewertungs- und -monitoringaktivitäten im Unternehmen dieselben Daten.

## 2 Ziel und Grundlage der Studie

IT-Risikobewertungen werden zur Identifikation und Bewertung von Risiken und deren Auswirkungen auf das Unternehmen durchgeführt. Auf Basis der Ergebnisse von Risikobewertungen werden Maßnahmen zum Schutz abgeleitet sowie auch eine Abschätzung der Risikolage abgegeben. Die Identifikation von Bedrohungen, die Einschätzung von Wahrscheinlichkeiten sowie von Auswirkungen ist in der Praxis aber schwierig, da verlässliche Daten oftmals nicht vorhanden sind bzw. die Bewertungen auf Expertenmeinungen beruhen. Die bestehenden Risikobewertungsverfahren basieren auf der Identifikation von Bedrohungen und Schwachstellen für einzelne ausgewählte Objekte (Assets). Dieses Vorgehen macht es aber schwierig Schwachstellen bei bestehenden implementierten Kontrollen (Betrieb) oder auch dem Sicherheitsdesign zu identifizieren, da Bedrohungen und Schwachstellen nicht vollständig identifiziert werden bzw. Betrieb und Design von Kontrollen nicht entsprechend überprüft werden.

Das Ziel der Studie war, die bestehende Praxis bei Risikobewertungen zu untersuchen insbesondere das Vorgehen und die Kriterien in der Risikobewertung, inwieweit Risikobewertungen und -ergebnissen vertraut wird, die Bewertung von Sicherheitskontrollen sowie die Nutzung von Sicherheitsanforderungen und das Vorhandensein von Prozessmodellen.

### 2.1 Fragebogen

Der Fragebogen besteht aus den folgenden drei Bestandteilen:

Der Teil 1 – IT-Risikobewertung, besteht aus Fragen zur IT-Risikobewertung insbesondere welche Kriterien werden benutzt sowie wie werden Risikoergebnisse bewertet.

Der Teil 2 – Geschäftsprozessmodelle und Sicherheitsanforderungen, besteht aus Fragen zur Nutzung von Geschäftsprozessmodellen, der Klassifikation von Daten im Unternehmen sowie der Nutzung von Sicherheitsanforderungen in der Risikobewertung.

Der Teil 3 – Risikobewertung, besteht aus einem Beispiel anhand dessen die Teilnehmer eine Risikobewertung vornehmen sollen.

Der Fragebogen wurde im Rahmen einer Doktorarbeit zu IT-Risikobewertung mit Geschäftsprozessmodellen und Sicherheitsanforderungen entwickelt. Der Fragebogen wurde vorher in einem Testlauf verifiziert, inwieweit die Fragen verständlich sowie Antworten auswertbar sind.

### 2.2 Umfrage

Im Rahmen eines Vortrages unter Sicherheitsexperten im Februar 2011 wurden die Teilnehmer der Veranstaltung zur IT-Risikobewertung und Nutzung von Sicherheitsanforderungen mittels Fragebogen befragt. Die Befragung fand in einem geschlossenen Raum unter Aufsicht statt. Zur Bearbeitung des Fragebogens wurde den Teilnehmern 30 Minuten Zeit gegeben. Von den ca. 55 Teilnehmern der Veranstaltung haben 45 Teilnehmer den Teil 1 und 46 Teilnehmer den Teil 2 des Fragebogen beantwortet. Der Teil 3 des Fragebogens wurde insgesamt von 36 Teilnehmern beantwortet. Mehrfachnennungen waren bei Fragen zulässig. Im Folgenden werden die Einzelergebnisse dargestellt und interpretiert und abschließend zu jedem Teil des Fragebogens eine Zusammenfassung gegeben.

## 3 Ergebnisse der Studie

### 3.1 IT-Risikobewertung (Teil 1)

1. Wie oft führen Sie pro Jahr eine IT-Risikobewertung in Ihrem Unternehmen durch und werden Schwerpunkte gesetzt?  
33 Prozent der Teilnehmer führen Risikobewertungen ad-hoc durch und 67 Prozent periodisch. Im Durchschnitt werden pro Jahr 6 Risikobewertungen durchgeführt. Dabei werden meist Schwerpunkte festgesetzt.
2. Welche Standards/Methoden verwenden Sie für Ihre Risikobewertung?  
Die meisten Teilnehmer verwenden die ISO 27001/27005 Standards (30 Nennungen) sowie Cobit und ISF Practices (jeweils 17 Nennungen) als Grundlage für die Risikobewertung. Hervorzuheben ist, dass fast ausschließlich Standards verwendet werden die Sicherheits- oder Kontrollprozesse vorgeben und keine Risikobewertungsverfahren im engeren Sinne wie z.B. NIST 800-30 oder Octave genutzt werden.
3. Welche Kriterien verwenden Sie bei der Risikobewertung?  
Kontrollen, Sicherheitsanforderungen sowie Häufigkeiten werden nur von ca. 20 Prozent der Teilnehmer in der Risikobewertung verwendet. 80 Prozent verwenden Schwachstellen, Eintrittswahrscheinlichkeit, Auswirkung und Auswirkungshöhe.
4. Wie bestimmen bzw. identifizieren Sie: Ereignisse, Schwachstellen, Wahrscheinlichkeiten, Auswirkungen?  
Ereignisse werden hauptsächlich mit Hilfe von Expertenwissen bestimmt (> 80 Prozent). Andere Hilfsmittel wie Publikationen oder Ereignisdaten werden eher selten verwendet (< 20 Prozent). Schwachstellen werden hauptsächlich mit Hilfe von Expertenwissen (ca. 75 Prozent) sowie mit Systemtests (ca. 50 Prozent) bestimmt. Wahrscheinlichkeiten werden hauptsächlich mit Hilfe von Expertenwissen (ca. 75 Prozent) und Szenarios (ca. 50 Prozent) bestimmt. Auswirkungen werden hauptsächlich mit Hilfe von Expertenwissen (ca. 75 Prozent) und Szenarios (ca. 45 Prozent) bestimmt. Die Identifikation von Ereignissen, Schwachstellen, Wahrscheinlichkeiten und Auswirkungen wird also größtenteils mittels Expertenwissens vorgenommen. Das Ergebnis war so erwartet worden, zeigt aber auch das eine sehr hohe Abhängigkeit zu Experten und deren Einschätzung der Risiken besteht. Außer Systemtests und Szenarios werden andere Möglichkeiten zur Identifikation von Ereignissen, Schwachstellen, Wahrscheinlichkeiten und Auswirkungen kaum genutzt.
5. Verwenden Sie ein Repository mit Objekten für die Risikobewertung?  
Ungefähr 80 Prozent der Teilnehmer verwenden ein Repository auf das Sie in der Risikobewertung zurückgreifen können. Bei den meisten Teilnehmern sind die Bewertungsobjekte (Assets) sowie Kontrollen/Sicherheitskonzepte (jeweils ca. 50 Prozent) in dem Repository hinterlegt. Sicherheitsanforderungen, Bedrohungen und Auswirkungen sind oft auch hinterlegt (jeweils ca. 30 Prozent). Konkrete Schadensfälle (ca. 15 Prozent) werden eher selten dokumentiert.
6. Überprüfen Sie im Rahmen der Risikobewertung implementierte Kontrollen?  
Ein Großteil der Teilnehmer überprüft implementierte Kontrollen gar nicht (22 Prozent) oder nur für Assets mit Schwachstellen (31 Prozent). 36 Prozent der Teilnehmer bewerten Kontrollen für die überprüften Assets aber nur 11 Prozent überprüft die Kontrollen aller Assets.

**Inwieweit stimmen Sie folgenden Aussagen zu?**

7. Risiken sind nicht objektiv zu bestimmen, da Daten über Ereignisse, Wahrscheinlichkeiten und Auswirkungen unzureichend bzw. statistische Daten nicht vorhanden sind. Die meisten Teilnehmer (53 Prozent) stimmen zu, dass Risiken nicht objektiv zu bestimmen sind. Allerdings herrscht die Meinung unter den Teilnehmern vor, dass die Risikobewertungen nachprüfbar sind und deshalb nicht subjektiv sind (siehe Frage 8). Dies würde bedeuten, dass zwar die Risikobewertung nachvollziehbar ist aber die Datengrundlage die genutzt wird nicht verifizierbar ist. Weiterhin sind die Teilnehmer der Meinung, dass die Risikobewertungen beeinflusst sind durch z.B. persönliche Erfahrungen oder Medien (siehe Frage 9). Dies wirft aber die Frage auf, wie Risikobewertungen wirklich nachprüfbar sind, da von den Teilnehmern bestätigt wurde das eine (subjektive) Bewertung aufgrund von negativen Erfahrungen erfolgt.
8. Risikobewertungen sind subjektive Schätzungen, die schwer nachprüfbar sind. Jeweils die Hälfte der Teilnehmer stimmt der Aussage größtenteils zu bzw. nicht zu.
9. Risikobewertungen (Wahrscheinlichkeiten und Auswirkungen) des Bewerter sind beeinflusst durch persönliche Erfahrungen, Medien und unternehmensspezifika. Über 80 Prozent der Teilnehmer sind der Meinung, dass Risikobewertungen und deren Ergebnisse durch z.B. Erfahrungen oder Medien beeinflusst sind.
10. Risiken werden meistens als niedrig bzw. mittel bewertet, deswegen sind hohe Risiken (H) unterrepräsentiert und geringe Risiken (N) überrepräsentiert. Hohen Risiken werden nicht als unterrepräsentiert gesehen (ca. 60 Prozent) und niedrige Risiken nicht als überrepräsentiert (ca. 50 Prozent). Dies ist interessant, da wissenschaftlich nachgewiesen wurde das manche Risikobewertungsverfahren dazu tendieren Risiken als mittel oder niedrig einzustufen. In einer eigenen durchgeführten Studie in einem Unternehmen wurde identifiziert, dass niedrige Risiken dort überrepräsentiert sind ausgehend von einer Normalverteilung.
11. Die Umsetzung von Sicherheitsmaßnahmen durch das Management ist beeinflusst durch persönliche-, abteilungs- oder unternehmensweite Kostenziele. Die Teilnehmer sind der Meinung, dass die Umsetzung von Sicherheitsmaßnahmen durch das Management zu 90 Prozent durch Kostenziele beeinflusst sind.
12. Sicherheitsrichtlinien werden angepasst, wenn Risiken vom Management akzeptiert werden. Uneinigkeit besteht bei den Teilnehmern (jeweils 50 Prozent) inwieweit Sicherheitsrichtlinien angepasst werden, wenn Risiken durch das Management akzeptiert werden. D.h. Sicherheitsrichtlinien werden nur teilweise oder auch nicht angepasst.
13. Die derzeitigen Risikobewertungsverfahren/-methoden sind ausreichend. 51 Prozent der Teilnehmer sind der Meinung, dass die bestehenden Risikobewertungsverfahren ausreichend sind. 49 Prozent sind der Meinung diese seien nicht ausreichend. Als Verbesserungswürdig werden die folgenden Themen gesehen: Risiko Management und Compliance, Objektivität von Bewertungsverfahren, Abhängigkeiten zwischen Systemen und Risiken und der Abdeckungsgrad von Bewertungsverfahren.

### 3.2 Zusammenfassung (Teil 1)

Die meisten Unternehmen führen IT-Risikobewertungen periodisch durch, in denen schwerpunktmäßig die Risiken von bestimmten Assets oder Themenbereichen bewertet werden. Durchschnittlich werden ca. 6 Risikobewertungen pro Jahr durchgeführt. Die Standards/Me-

Methoden die zur Risikobewertung verwendet werden sind meist Best-Practice Methoden, die konkrete Maßnahmen vorgeben welche z.B. Sicherheitsprozesse, Kontrollen oder Sicherheitsmaßnahmen zu implementieren sind. Die meistgenannten Methoden waren Standards wie: ISO27001, Cobit sowie ISF Practices. Teilweise werden auch eigenentwickelte Bewertungsverfahren verwendet, die aus existierenden Best-Practice Standards erstellt werden. Die Identifikation und Bewertung von Risiken von Assets wird hauptsächlich durch Expertenwissen vorgenommen. Teilweise werden auch noch Systemtest und Szenarios verwendet. Andere Methoden oder Hilfsmittel wie z.B. Publikationen, Schaden- oder Ereignisdatenbanken spielen eher eine untergeordnete Rolle. Ungefähr 80 Prozent der Teilnehmer verwenden ein Repository in dem Daten über Assets (Daten, IT-Systeme), Sicherheitsanforderungen und Bedrohungen dokumentiert sind. Im Rahmen der Risikobewertung werden hauptsächlich die implementierte Kontrollen der überprüften Assets oder der Assets mit Schwachstellen überprüft. Allerdings werden implementierte Kontrollmechanismen nicht systematisch für alle Assets überprüft.

Die meisten Teilnehmer stimmen zu das Risiken nicht objektiv zu bestimmen sind, meinen allerdings auch, dass Risikobewertungen nachvollziehbar sind. Zudem sind die Teilnehmer der Meinung, dass Risikobewertungen beeinflusst sind entweder durch den Bewerter und/oder Kostenziele im Unternehmen. Inwieweit Sicherheitsrichtlinien nach der Durchführung der Risikobewertung angepasst werden ist sehr individuell abhängig vom Unternehmen. Von den Teilnehmern wurde nicht bestätigt das eine Konzentration von Risiken in Bewertungsbereichen vorliegt: z.B. bei Risiken die als niedrig oder mittel bewertet werden.

### 3.3 Geschäftsprozesse und Sicherheitsanforderungen (Teil 2)

Im zweiten Teil der Umfrage hatten die Teilnehmer die folgenden Fragen zu beantworten:

1. Was sehen Sie als Treiber für die Modellierung von Geschäftsprozessmodellen?  
Als Treiber für die Geschäftsprozessmodellierung werden regulatorische Anforderungen sowie Produktivitätssteigerungen (jeweils 33 Nennungen) und Effizienz gesehen. Organisationsgestaltung und Organisationsdokumentation spielen eher eine untergeordnete Rolle (ca. jeweils 13 Nennungen).
2. Sind in Ihrem Unternehmen (Konzern oder Tochterunternehmen) Geschäftsprozesse modelliert(1), aktuell(2) und für die wichtigsten/kritischen(3) Prozesse modelliert?  
In den meisten Unternehmen der Teilnehmer sind kritische bzw. wichtige Prozesse modelliert und diese auch aktuell (ca. 70 Prozent).
3. Welche Informationen sind in den Geschäftsprozessmodellen modelliert?  
In den modellierten Prozessen der Unternehmen werden meist Akteure/Rollen (40 Nennungen) und IT-Systeme (30 Nennungen) modelliert. Risiken, Kontrollen oder Sicherheitsanforderungen werden meist nicht modelliert (< 10 Nennungen).
4. Klassifizieren Sie unternehmensweit Objekte nach Vertraulichkeit, Integrität und Verfügbarkeit?  
Bei 90 Prozent der Teilnehmer werden Objekte, hauptsächlich IT-Systeme und Daten, nach Vertraulichkeit, Integrität und Verfügbarkeit klassifiziert.
5. Ist in Ihrem Unternehmen eine Grenze für Sicherheitsrisiken bzw. sind -anforderungen definiert?  
Bei 60 Prozent der Teilnehmer sind Grenzen/Limits für Sicherheitsrisiken definiert bzw. es sind Sicherheitsanforderungen definiert.

6. Für welche Objekte (Assets) sind bei Ihnen Sicherheitsanforderungen definiert?  
Sicherheitsanforderungen sind hauptsächlich für IT-Systeme (ca. 80 Prozent) und Daten (ca. 60 Prozent) definiert, zum Teil auch für Prozesse (40 Prozent).
7. Wie definieren/formulieren Sie Sicherheitsanforderungen?  
Sicherheitsanforderungen werden meistens entweder in einer strukturierten Vorlage (65 Prozent) oder als Freitext (40 Prozent) dokumentiert.
8. Wo werden bei Ihnen Sicherheitsanforderungen definiert bzw. dokumentiert?  
Sicherheitsanforderungen sind bei den meisten Unternehmen in Security Policies und/oder in Security Standards und/oder in Security Procedures/Guidelines definiert bzw. dokumentiert (jeweils ca. 40 Nennungen).
9. Inwieweit nutzen Sie Sicherheitsanforderungen in der Risikobewertung?  
Sicherheitsanforderungen werden für Assets und/oder für die Identifikation von Threats und/oder der Bewertung von Ereignissen verwendet (jeweils ca. 25 Nennungen).

#### **Inwieweit stimmen Sie folgenden Aussagen zu?**

10. Sicherheitsanforderungen werden systematisch (in der Bedrohungsidentifikation und dem Bewertungsprozess) in Ihren Risikobewertungen berücksichtigt. (2) Mit der systematischen Evaluierung von Sicherheitsanforderungen könnten Risiken genauer/besser bestimmt werden.  
In den meisten Unternehmen der Teilnehmer (60 Prozent) werden Sicherheitsanforderungen bereits systematisch in der Risikobewertung berücksichtigt. Zudem sind 70 Prozent der Teilnehmer überzeugt, dass Risiken genauer und besser bestimmt werden können mit der Evaluierung von Sicherheitsanforderungen.
11. Risiken könnten nur auf Basis von Sicherheitsanforderungen identifiziert und bewertet werden.  
Die meisten Teilnehmer glauben nicht (ca. 55 Prozent), dass Risiken nur auf Basis von Sicherheitsanforderungen identifiziert und bewertet werden können.
12. Die zusätzliche Bewertung von Maturity (Mat) und Performance (Perf) von IT Prozessen könnte zu beständigeren (zeitpunktunabhängigen) Risikobewertungen führen.  
Die Teilnehmer bestätigen, dass die Bewertung von Maturity (61 Prozent) und Performance (48 Prozent) von IT Prozessen zu beständigeren Risikobewertungen führen kann.
13. Wir überprüfen bereits systematisch die Datensicherheit mittels Sicherheitsanforderungen (SR).  
Sicherheitsanforderungen werden zur Bestimmung von Risiken verwendet. Ungefähr 50 Prozent der Teilnehmer überprüft systematisch die Datensicherheit mit Sicherheitsanforderungen.
14. Wir messen (mit Sicherheitsmetriken) bereits aktiv die Sicherheit von Daten im Unternehmen.  
Die meisten Unternehmen (> 60 Prozent) messen nicht aktiv die Sicherheit von Daten.
15. Welche Darstellung eines Risikos ist für Sie transparenter/hilfreicher?  
Die Darstellung von Risiken mit dem zugehörigen Prozess, den Daten sowie der Sicherheitsanforderung die verletzt wird, wird von ca. 90 Prozent der Teilnehmer als sehr hilfreich angesehen bzw. transparenter.

### 3.4 Zusammenfassung (Teil 2)

Als Treiber für die Geschäftsprozessmodellierung werden von den Teilnehmern regulatorische Anforderungen sowie Produktivitätssteigerungen und Effizienz gesehen. Organisationsgestaltung und Organisationsdokumentation spielen eher eine untergeordnete Rolle. In den meisten Unternehmen sind kritische bzw. wichtige Prozesse des Unternehmens modelliert und diese auch aktuell. In den Prozessen sind Akteure/Rollen und IT-Systeme modelliert. Risiken, Kontrollen oder Sicherheitsanforderungen werden meistens nicht modelliert.

Bei 90 Prozent der Teilnehmer werden Objekte wie z.B. IT-Systeme, Daten oder Prozesse nach Vertraulichkeit, Integrität und Verfügbarkeit klassifiziert. Es werden hauptsächlich IT-Systeme und Daten klassifiziert und für IT-Systeme und Daten sind entsprechende Sicherheitsanforderungen definiert. Sicherheitsanforderungen werden entweder in einer strukturierten Vorlage oder als Freitext dokumentiert. Andere Formen der Dokumentation von Sicherheitsanforderungen werden nicht genutzt. Sicherheitsanforderungen sind in Security Policies und/oder in Security Standards und/oder in Security Procedures/Guidelines definiert bzw. dort beschrieben. Sicherheitsanforderungen werden im Rahmen der Risikobewertung für Assets und der Identifikation von Threats verwendet.

Bei 60 Prozent der Teilnehmer werden Sicherheitsanforderungen bereits in der Risikobewertung berücksichtigt. Zudem sind 70 Prozent der Teilnehmer überzeugt, dass Risiken genauer und besser bestimmt werden können mit der Evaluierung von Sicherheitsanforderungen. Die Darstellung eines Risikos nicht nur aus dem Ereignis, der Wahrscheinlichkeit und der Auswirkung sondern mit der Sicherheitsanforderung und der betroffenen Prozesse und Daten wird von ca. 90 Prozent der Teilnehmer als sehr hilfreich bzw. transparenter angesehen.

Die Mehrheit der Teilnehmer (ca. 55 Prozent) bestätigt, dass die Bewertung von Maturity und Performance von IT Prozessen zu beständigeren Risikobewertungen führen könnte. Die meisten Unternehmen messen nicht aktiv die Sicherheit von Daten, nutzen jedoch Sicherheitsanforderungen um die Datensicherheit zu überprüfen.

### 3.5 Risikobewertung anhand eines Beispiels (Teil 3)

Im Rahmen der Studie sollte die Teilnehmer eine Risikobewertung zu einem konstruierten Beispiel vornehmen. Zu diesem Zweck wurde ein Risikoanalysebeispiel mit einer unterschiedlichen Fülle von Informationen unter den Teilnehmern verteilt. Die Beispiele A, B und C die verteilt wurden, unterscheiden sich dadurch dass diese weitere Informationen wie das Prozessmodell und Sicherheitsanforderungen zur Risikobewertung enthalten. Im Beispiel A hatten die Teilnehmer nur eine Risikoanalyse vorliegen (12 auswertbare Rückmeldungen von 20), im Beispiel C die Risikoanalyse und das zugehörige Prozessmodell (13 auswertbare Rückmeldungen von 15) und im Beispiel B (11 auswertbare Rückmeldungen von 20) die Risikoanalyse, das Prozessmodell und die Sicherheitsanforderungen. In den folgenden Tabellen werden die Risikoergebnisse dargestellt, inwieweit die vordefinierten Risiken von den Teilnehmern identifiziert wurden.

**Tab. 1:** Ergebnisse Beispiel A.

Risiken	Anzahl	Prozent
1. Änderbare Datenbankinhalte (im Beispiel A, B und C)	12	100%
2. Unverschlüsselte Datenübertragung von Kunden und Zahlungsdaten (im Beispiel A, B und C)	8	67%

3. Zugriff (lesend) auf Bestelldaten (nur im Beispiel B)	1	8%
4. Verfügbarkeit des Systems (nur im Beispiel B)	12	100%
5. Autorisierung der Bestellung (nur im Beispiel B)	0	0%
6. Andere Risiken (durch Teilnehmer)	9	75%

**Tab. 2:** Ergebnisse Beispiel B.

Risiken	Anzahl	Prozent
1. Änderbare Datenbankinhalte (im Beispiel A, B und C)	8	73%
2. Unverschlüsselte Datenübertragung von Kunden und Zahlungsdaten (im Beispiel A, B und C)	10	91%
3. Zugriff (lesend) auf Bestelldaten (nur im Beispiel B)	5	45%
4. Verfügbarkeit des Systems (nur im Beispiel B)	11	100%
5. Autorisierung der Bestellung (nur im Beispiel B)	2	18%
6. Andere Risiken (durch Teilnehmer)	6	55%

**Tab. 3:** Ergebnisse Beispiel C.

Risiken	Anzahl	Prozent
1. Änderbare Datenbankinhalte (im Beispiel A, B und C)	13	100%
2. Unverschlüsselte Datenübertragung von Kunden und Zahlungsdaten (im Beispiel A, B und C)	11	85%
3. Zugriff (lesend) auf Bestelldaten (nur im Beispiel B)	0	0%
4. Verfügbarkeit des Systems (nur im Beispiel B)	11	85%
5. Autorisierung der Bestellung (nur im Beispiel B)	0	0%
6. Andere Risiken (durch Teilnehmer)	10	77%

### 3.6 Zusammenfassung (Teil 3)

Die durchschnittliche Anzahl der identifizierten Risiken ist in etwa bei allen Beispielen gleich hoch. Im Durchschnitt wurde in den Beispielen A und C zu viele Risiken identifiziert im Beispiel B zu wenige Risiken im Verhältnis zu den vordefinierten Risiken (Risiken 1 bis 5). Im Beispiel A und C wurde größtenteils zusätzlich als Risiko die Verfügbarkeit des CRM Systems identifiziert, wahrscheinlich auf Basis der Aussage in den Beispielen das der Bestellprozess wichtig für das Unternehmen ist, aber ohne eine konkrete Aussage zur Kritikalität der Verfügbarkeit zu haben. An dieser Stelle wird deutlich, dass Informationen interpretiert und Annahmen getroffen werden, die maßgeblich die Identifikation von Risiken sowie die Richtigkeit des Ergebnisses beeinflussen. D.h. je mehr Informationen zu einem Risiko zur Verfügung stehen, wie z.B. die Sicherheitsanforderungen, desto besser ist die Risikobewertung bzw. kann das Ergebnis bewertet oder überprüft werden. Dies wird auch daran deutlich, dass

die zusätzlichen identifizierten Risiken (Risiko 6) in dem Beispiel B seltener auftreten als in den Beispielen A und C. Bemerkenswert ist auch, dass in allen Beispielen zusätzliche Risiken neben den vordefinierten Risiken identifiziert wurden. Die Anzahl der zusätzlich identifizierten Risiken nimmt ab, wenn genauere Informationen z.B. zu den Sicherheitsanforderungen vorliegen.

Im Beispiel B schaffte es nur eine geringe Anzahl der Teilnehmer, die Risiken die mit dem Design des Bestellprozesses (Risiko 3 und 5) verbunden waren, korrekt zu identifizieren. Darauf Einfluss hatte sicherlich die Fülle der Informationen und die limitierte Zeit die zur Verfügung stand. Prinzipiell zeigt dies aber, dass wenn komplexe Sachverhalte und viele Informationen miteinander kombiniert werden müssen die Wahrscheinlichkeit sinkt Risiken korrekt zu identifizieren. Allerdings ist herauszustellen, dass die Korrektheit der Ergebnisse deutlich besser ist als wenn weniger Informationen zur Verfügung stehen. In bestehenden Risikobewertungsverfahren werden, um Komplexität zu verringern, Bewertungen für einzelne Objekte vorgenommen, das wiederum führt zu dem Problem das verbundene oder weitere bestehende Risiken eben nicht korrekt identifiziert werden können.

Interessant ist auch, dass im Beispiel A und C eine durchgeführte Risikoklassifikation auf Basis der Sicherheitskategorien Vertraulichkeit, Integrität und Verfügbarkeit zeigt, dass der Fokus in Beispiel A auf der Verfügbarkeit der Daten liegt. Das Prozessmodell hat also dazu beigetragen, dass die Integrität der Daten im Beispiel C risikoreicher von den Teilnehmern bewertet wurde. Die Teilnehmer haben die beschriebenen Risiken also anders wahrgenommen aufgrund der Visualisierung des Prozessablaufes.

## 4 Diskussion der Ergebnisse

Im Rahmen der Studie sollten Informationen zur Durchführung von IT-Risikobewertungen und die Nutzung von Sicherheitsanforderungen in der Praxis gesammelt werden, welche und wie Kriterien und Objekte in der IT-Risikobewertung verwendet werden sowie zu bestätigen das Daten wie Prozessmodelle, Sicherheitsanforderungen und Datenklassifikation in der Praxis vorhanden sind und systematisch genutzt werden. Ziel war es, die folgenden Fragestellungen (Hypothesen) aus Sicht von Sicherheitsspezialisten aus der Praxis näher zu untersuchen inwieweit diese bestätigt oder verneint werden. Die Ergebnisse zu den Hypothesen dienen als Grundlage für die Erstellung eines Risikobewertungsverfahrens auf Basis von Geschäftsprozessmodellen und Sicherheitsanforderungen. Folgende Hypothesen sollten mit der Studie überprüft werden:

*These 1: Risikobewertungsverfahren werden von Sicherheitsexperten als mangelhaft betrachtet aufgrund der Subjektivität von Ergebnissen, unzureichender Datenbasis für die Bewertung, der Risikohäufung, fehlender Systematik (nur Expertenbewertungen), unzureichender Berücksichtigung von Frequenzen.*

Risikobewertungsverfahren werden in der Praxis als mit Mängeln versehene Methoden betrachtet, aber nicht abgelehnt aufgrund dieser Mängel. Dass Risiken nicht objektiv zu bestimmen sind, aufgrund der unzureichenden Datenbasis, wird bestätigt allerdings werden Risikobewertungen von den Teilnehmern nicht als subjektiv angesehen auch wenn Risikobewertungen beeinflusst sind z.B. durch externe Einflüsse. Die Risikohäufung z.B. von mittleren oder hohen Risiken wird in der Praxis nicht als Problem identifiziert bzw. wird nicht als solches erkannt. Die Ereignisfrequenz wird oftmals nicht in der Risikobewertung berücksichtigt. Von den Teilnehmern wird Verbesserungspotenzial bei Bewertungsverfahren gesehen, vor allem die Integration und Verbindung von Compliance und Risiko Management sowie in der Effizi-

enzsteigerung des Bewertungsvorgangs. Größtenteils werden die Bewertungsverfahren als ausreichend angesehen.

*These 2: Alle implementierten Sicherheitskontrollen werden im Rahmen der Risikobewertung auf Basis von Sicherheitsanforderungen überprüft.*

Die Studie gibt ein differenziertes Bild wieder. Teilweise werden Kontrollen gar nicht oder nur für Assets mit Schwächen überprüft, ein anderer Teil der Teilnehmer prüft Kontrollen für Assets die im Rahmen der Risikobewertung geprüft werden. Allerdings wird eine systematische Bewertung der Kontrollen für alle Assets nicht vorgenommen.

*These 3: Geschäftsprozessmodelle sind in der Praxis vorhanden und aktuell.*

Die Studie hat bestätigt, dass Geschäftsprozessmodelle für kritische bzw. wichtige Prozesse eines Unternehmens in der Praxis vorhanden und diese auch aktuell sind. In den Geschäftsprozessmodellen sind hauptsächlich Akteure/Rollen sowie IT-Systeme modelliert. Risiken, Kontrollen oder Sicherheitsanforderungen werden nicht modelliert. Als Treiber für die Geschäftsprozessmodellierung werden Effizienzsteigerungen und Kostenreduzierung sowie regulatorische Anforderungen gesehen.

*These 4: Sicherheitsanforderungen werden teilweise in der Risikobewertung berücksichtigt, aber nicht systematisch für die Bewertung von Risiken verwendet.*

Sicherheitsanforderungen sind für IT-Systeme und Daten definiert und sind meistens in den entsprechenden Security Policies oder Sicherheitsrichtlinien beschrieben. Sicherheitsanforderungen werden meistens bei Risikobewertungen berücksichtigt. Inwieweit Sicherheitsanforderungen systematisch in der Risikobewertung eingesetzt werden, konnte nicht verifiziert werden. Allerdings ist aufgrund der Tatsache das Best-Practice Methoden verwendet werden sowie von den Teilnehmern Kontrollen und Sicherheitsanforderungen oftmals nicht als Kriterien in der Risikobewertung genannt wurden, es unwahrscheinlich das diese systematisch verwendet werden.

*These 5: Sicherheitsanforderungen werden in der Risikobewertung eingesetzt, sind für Assets definiert und werden zur Messung von Risiken verwendet.*

Sicherheitsanforderungen werden im Rahmen der Risikobewertung für Assets (IT-Systeme und Daten und der Identifikation von Threats verwendet und sind für Assets definiert. Die Messung von Risiken wird nicht aktiv durchgeführt, allerdings werden Sicherheitsanforderungen zur Überprüfung der Datensicherheit verwendet.

*These 6: Daten werden unternehmensweit klassifiziert.*

Bei 90 Prozent der Teilnehmer werden IT-Systeme und/oder Daten nach Vertraulichkeit, Integrität und Verfügbarkeit klassifiziert. Die Klassifikation der Daten wird bei der Beschreibung von Sicherheitsanforderungen berücksichtigt und die Klassifikation steht auch bei der Risikobewertung zur Verfügung.

*These 7: Die Bewertung von Risiken mittels Sicherheitsanforderungen führt zu besseren Ergebnissen, d.h. Risiken können korrekter bestimmt werden.*

Das Risikobewertungsbeispiel in der Studie zeigt, dass Risiken korrekter identifiziert werden je mehr Informationen wie z.B. Sicherheitsanforderungen vorliegen. Allerdings ist es den Teilnehmer schwer gefallen Risiken bei komplexen Sachverhalten korrekt zu identifizieren. Zudem wurde ersichtlich, dass im Rahmen der Risikobewertung Annahmen getroffen werden, wenn Informationen nicht bzw. nicht präzise vorliegen, die direkten Einfluss auf die Risiko-

identifikation sowie das Ergebnis haben. Auch wurde die Darstellung der Risikobewertung auf Basis der betroffenen Daten, des Prozesses und der verletzten Sicherheitsanforderung als hilfreicher bewertet wie nur mit Wahrscheinlichkeit und Auswirkung. Dies spricht dafür Sicherheitsanforderungen sowie Prozessdaten in Bewertungsverfahren systematisch zu nutzen.

## 5 Fazit

IT-Risikobewertungsverfahren werden von den Teilnehmern der Studie, IT Sicherheitsexperten aus der Wirtschaft, als mit Schwächen und Fehlern versehene Methoden eingeschätzt. Risikoergebnisse und der Bewertungsvorgang werden als nicht objektiv sowie beeinflusst durch verschiedene äußere Einflüsse wie Risikobewußtsein, Kostenziele oder Medien angesehen. Zudem sollten bestehende Risikobewertungsmethoden besser mit dem Risikomanagement und Compliance Aktivitäten verbunden werden und die Effektivität und Effizienz von Methoden gesteigert werden.

Im Fokus von zukünftigen Entwicklungen oder Verbesserungen bei Risikobewertungsverfahren sollte die Integration der Risikoergebnisse wie auch des Bewertungsvorgangs in eine unternehmensweite Risikodarstellung sein. Insbesondere die Einbindung der Ergebnisse in das zentrale Risikomanagement eines Unternehmens sollte im Vordergrund stehen sowie auch die Bewertung von übergreifenden operationellen Risiken, die auch IT-Risiken beinhalten aber über alle Unternehmensbereiche zu bewerten sind. Erst mit der Einbindung in das zentrale Risikomanagement kann eine unternehmensweite Gesamtrisikosicht erstellt werden, die für die Erfüllung von regulatorischen Anforderungen nötig ist. Weiterhin sollte versucht werden die Datenbasis zu erweitern sowie auch den Bewertungsvorgang zu objektivieren, um Risikoergebnisse zu erhalten die auch objektiv nachprüfbar sind und nicht nur auf Expertenmeinungen basieren. Als Daten sollten nicht nur die Assets, Sicherheitsanforderungen, Kontrollen und Bedrohungen vorliegen sondern auch Schadensvorfälle, -potentiale, Szenarios sowie auch die Abhängigkeiten zwischen Assets, Prozessen und Schadensvorfällen, um Risiken besser analysieren und bewerten zu können.

Als positiv für die zukünftige Weiterentwicklung von Risikobewertungsverfahren ist zu bewerten, dass in dem meisten Unternehmen Daten wie z.B. Geschäftsprozessmodelle, Sicherheitsanforderungen sowie auch ein Asset Repository vorhanden sind. D.h. auf einen Teil der Daten für die Risikoanalyse und -bewertung kann bereits zurückgegriffen werden bzw. die Daten können weiter angereichert und Automatismen für die Bewertung und Analyse entwickelt werden.

Das Thema Sicherheitsmonitoring und Sicherheitsmessung ist bei den meisten Unternehmen nicht sehr ausgeprägt. Unter beiden Begriffen wird die aktuelle und laufende Überprüfung der Sicherheit von Assets im Unternehmen verstanden. Die bereits bestehenden Daten aus der Risikoanalyse in den Unternehmen könnten als Basis für ein kontinuierliches Monitoring dienen, müssten dafür allerdings weiter angereicht werden sowie erst verlässliche Methoden zu kontinuierlichen Überwachung und Messung von Sicherheit entwickelt werden. Im Bereich Compliance Monitoring gibt es bereits einige Initiativen aus Wissenschaft und Forschung die sich mit dem Thema beschäftigen: z.B. werden Geschäftsprozesse als Grundlage zur Auditierung von Vorschriften verwendet oder Agenten für IT-Infrastrukturen um die Einhaltung von Sicherheitsrichtlinien zu prüfen. Auch für dieses Thema gilt, dass es eine enge Verbindung zwischen Risikoanalyse und -bewertung, Sicherheits- und Compliance Monitoring geben sollte, die idealerweise dieselben Daten nutzen.

Das Risikobewertungsbeispiel in der Studie zeigt, dass Risiken korrekter identifiziert werden je mehr Informationen wie z.B. Sicherheitsanforderungen vorliegen. Allerdings ist es den Teilnehmer schwer gefallen Risiken bei komplexen Sachverhalten korrekt zu identifizieren. Zum einen benötigen wir in der Risikoanalyse und -bewertung mehr Informationen zum anderen müssen diese Informationen in komplexen Sachverhalten auch auswertbar bzw. verständlich sein. D.h. Methoden oder Werkzeuge für die Darstellung von komplexen Sachverhalten und wichtigen Informationen im Kontext der Risikoanalyse und -bewertung sollten entwickelt werden, um die Risikobewertung effizienter und präziser zu machen. Zudem sollten Risikobewertungsverfahren Informationen verwenden, die eine präzise Identifikation der Risiken im Kontext des Geschäftsbetriebs ermöglichen, um Annahmen und Schätzfehler zu reduzieren sowie unternehmensspezifische Anforderungen abzubilden.