ROSI
Return on Security Invest

Herausgeber

mabs4.0 Deutschland GmbH
Südring 133
42579 Heiligenhaus

Telefon: +49 2056 267 9059
E-Mail: kontakt@mabs40.com

Internet: http://mabs40.de.com

Vorwort

Liebe/r Leser/in,

herzlichen Dank für Ihr Interesse an unserem Portfolio.

Die **mabs4.0 Deutschland GmbH** aus Düsseldorf ist ein Beratungshaus mit dem spezifischen Fokus auf **IT- & Informationssicherheit, Datenschutz und das Business Process Management**.

Als solches unterstützen wir erfolgreich unsere Kunden unter anderem bei der Umsetzung und Einführung von **Informationssicherheitsmanagementsystemen (ISMS) wie beispielsweise gemäß ISO27001, BSI-Grundschutz oder TISAX® unter Berücksichtigung der DSGVO.**

Auch das parallele Management verschiedenster, meist ineinandergreifender Normen („Multi-Normen-Management“) kann dabei in den Mittelpunkt rücken.

Unser erfahrenes Team unterstützt Sie beratend als auch umsetzend mit nachgewiesener Expertise und langjährige Erfahrungen bei den für Sie notwendigen Ausarbeitungen und Anpassungen.

Unser Ziel ist es, unsere Kunden als Partner in Augenhöhe nach seinem tatsächlichen Bedarf zu unterstützen.

Unsere Leistungen orientieren sich immer nach der benötigten Angemessenheit und Wirtschaftlichkeit.

Kontaktieren Sie uns gerne und unverbindlich für ein erstes kostenloses Beratungsgespräch. Gerne kommen wir auch zu Ihnen und bewerten mit Ihnen Ihre Herausforderungen.

Herzliche Grüße

Eric Schneider
Geschäftsführer der mabs4.0 Deutschland GmbH

Inhalt

1 Über die mabs4.0 Deutschland GmbH

Die mabs4.0 Deutschland GmbH (kurz: mabs) ist ein international agierender und unabhängiger Düsseldorfer Spezialist für

- IT & Informationssicherheit, Cybersicherheit,
- Integrierte Managementsysteme und
- Business Process Management.

Mit nachgewiesener Expertise behandelt die mabs die gesetzlichen und normativen Anforderungen zur Informationssicherheit, wie das deutsche IT- & Informationssicherheitsgesetz oder die EU-DSGVO genauso wie Kunden- und Normanforderungen (z.B. TISAX® oder ISO27001) oder Maßnahmen der Digitalisierung (z.B. Cybersicherheit) und setzt diese erfolgreich gemeinsam mit Ihren Kunden um.

Die häufig hinzukommenden verschiedenen, teils bestehenden, Anforderungen aus Umweltschutz (z.B. ISO 14001), Qualitätsnormen (ISO 9001), Arbeitssicherheit (ISO 45001) oder weiterer Anforderungen können zudem in einem integrierten Managementsystem (IMS) erfasst werden.

Anhängige oder betroffene Prozesse und Strukturen werden durch unsere Experten bei Bedarf analysiert und modelliert.

mabs unterstützt seine Kunden aus den Branchen Automotive, Industrie & Maschinenbau, Dienstleistungen, Banking, Telekommunikation, Gesundheitswesen und Pharmazie in ihren Vorhaben mit Augenmaß und schafft so transparente Projektstrukturen und echten Kundennutzen.

2 Unser USP

Wir bei mabs haben uns auf unsere Fachkompetenzen fokussiert und bauen diese stetig weiter aus. Mehr als 50 Jahre Praxis- und Projekterfahrung in unterschiedlichen Branchen haben uns gelehrt, dass stabile Organisationsprozesse das Ausfallrisiko von IT- & Informationssicherheit gestützten Wertschöpfungsketten minimiert.

Wir sind hoch qualifiziert, erfahren und motiviert – unser Ziel ist es, Ihre Organisation bestmöglich ganzheitlich einzubinden, um Ihre Resilienz zu stärken. Wir sind nicht die klassischen Berater, wir sind Ihr Partner und Verbündeter zur Sicherung Ihrer Informationswerte.

Mit mabs zusammenzuarbeiten bedeutet immer effizient und mit Augenmaß gemeinsam passende Lösungen für Ihre Organisation zu finden. Fokussiert und zielgerichtet. Wir bringen best practise mit und helfen Ihnen Fehler zu vermeiden und einen Schritt voraus zu sein.

Wir sind Profis in dem, was wir tun, wo wir nicht die Experten sind, arbeiten wir mit den Profis aus unserem Netzwerk zusammen.

Unsere Experten hören Ihnen zu. Nicht um zu antworten, sondern um zu verstehen.

• Etablierte Prozesse und Verantwortlichkeiten • Kostenminimierung • Nachweise der Erfüllung von Kundenanforderungen • Nachweis der Erfüllung von normativen und gesetzlichen Anforderungen • Haftungsreduzierung • Wettbewerbsvorteile • Minimierung von Risiken und möglichen Schäden

3 Return on Security Investment (RoSI)

3.1 Was versteht man unter RoSI?

IT- & Informationssicherheit bildet eine wesentliche Komponente für den Geschäftserfolg. Der Return on Security Investment (RoSI) kann als Entscheidungshilfe bei Investitionen für die IT- & Informationssicherheit herangezogen werden.

Wenn man die Ausgaben für IT- & Informationssicherheit unter betriebswirtschaftlichen Gesichtspunkten betrachtet, fällt es nicht immer leicht, eine Investition unter dem Aspekt eines „Return on Investment (RoI)“ zu bewerten. Nichtsdestotrotz braucht man neben qualifizierten Ressourcen auch ein Budget für IT- & Informationssicherheit, allerdings stellt sich die Frage, wie ein direkt bestimmbarer Nutzen dazu ermittelt und dargestellt werden kann.

IT- & Informationssicherheits-Investitionen werden primär durch die Vermeidung von Schäden definiert, die Kennzahl eines ROI dient jedoch eher zur Bestimmung eines unmittelbar geschaffenen Nutzens. Somit muss der Return on Security Investment (RoSI) anders ermittelt werden.

3.2 Klassischer Return on Investment (RoI) und IT- & Informationssicherheit

In der klassischen Betriebswirtschaftslehre ist der Return on Investment (RoI) eine Kennzahl für Rentabilität einer Investition. Somit dient diese Kennzahl der Wirtschaftlichkeitsbetrachtung potenzieller Investitionen.

Gemäß der Berechnungsformel wird der Ertrag (Nutzen der Investition) mit den Kosten der Anschaffung in Relation gesetzt.

Somit können aber nur Investitionen, die positive monetäre Ergebnisse erwirtschaften, zum Beispiel Kosteneinsparungen oder Ertragssteigerungen, betrachtet werden. Investitionen, die rein nur für die IT- & Informationssicherheit getätigt werden sollen, erhöhen weder direkt die Erträge, noch sorgen sie für eine sofortige Amortisation. Hier geht es vielmehr um ein geplantes Risiko-Management, das zur Schadenvermeidung und/oder Risikominderung beiträgt.

3.3 Wichtige Voraussetzungen

Ein IT- & Informationssicherheits-Management-System sollte bereits implementiert sein und brauchbare Daten liefern. Idealerweise ist dies auch mit einem Ticket-System verknüpft, so dass hieraus eine Vielzahl von Daten genutzt werden kann.

Es sollte immer berücksichtigt werden, dass der Aufwand für die Sammlung der erforderlichen Daten nicht über dem angestrebten Nutzen liegt.

Ein Asset-Inventory mit verlässlichen Daten ist ebenso eine wichtige Voraussetzung für die weitere Betrachtung möglicher Risiken in Bezug auf den Unternehmenswert, den die Maßnahme schützen soll.

3.4 Probleme bei Risikoeinschätzungen

Bei der Identifizierung und Abwägung von Risiken müssen folgende Punkte beachtet werden:

Meist muss mit Simulationen gearbeitet werden, da die Erfassung von Risiken sich meistens schwierig gestaltet und somit Daten nicht oder nur unvollständig vorhanden sind.

Die Entwicklung von Technik und Geschäftsprozessen entspricht nicht unbedingt langfristigen Risikobetrachtungen.

Das Management nimmt „IT- & Informationssicherheit“ nicht ernst genug.

Vermeintlich wichtige Sicherheitsfragen werden selten oder zu spät gestellt, da die Antworten unbequem sein könnten.

Nur eine möglichst neutrale Herangehensweise an die jeweiligen Risikofaktoren und deren objektive Bewertung kann bei IT- & Informationssicherheits-Investitionen gewährleisten, dass die Entscheidung, ob die Investition getätigt werden sollte oder nicht, annährend realistisch getroffen werden kann.

4 Berechnung und Interpretation des Ergebnisses

4.1 Formel

Im Gegensatz zum RoI basiert der RoSI auf der Einschätzung der spezifischen Risiken, die durch eine Investition in die Sicherheit neutralisiert werden sollen. Grundsätzlich können die notwendigen Daten nicht unmittelbar herangezogen werden, da sie in der notwendigen Form eher selten vollständig aufbereitet vorliegen.

Als ersten Hinweis können aber entsprechende Ticket-Informationen dienen.

Für die Berechnung der RoSI-Kennzahl müssen folgende Parameter betrachtet werden:

Die Verlusterwartung im Einzelfall (VEE) in EUR: Dafür müssen die Daten und andere IT-Ressourcen zunächst inventarisiert werden. In der Folge werden die direkten Kosten (Aufwände Mitarbeiter, technische Untersuchungen, etc.) und die indirekten Kosten (Geschäftsausfallzeiten, erhöhte Kundenabwanderungsrate) für Schäden bzw. Verluste aufaddiert.

Die jährliche Eintrittsrate (ER) als absoluter Wert: Dafür muss geschätzt werden, wie häufig innerhalb eines Jahres ein Ereignis oder eine Bedrohung eintritt. Oftmals kann diese Zahl aus den Dokumentationen bisheriger Sicherheits-Vorfälle entnommen werden. Das heißt, bei *einer* Bedrohung innerhalb der letzten *zehn* Jahre beträgt die ER 0,1. Treten die Bedrohungen hingegen rund *zehn Mal in einem Jahr* auf, ist die ARO 10.

Die jährliche Verlusterwartung (VE) in EUR: Dies ist der gesamte monetäre Verlust pro Jahr, der sich aus *einem* spezifischen Risiko ergibt, wenn *eine* Maßnahme nicht umgesetzt wird. Die VE errechnet sich aus VEE * ER.

Die Minderungsquote (MQ) in Prozent beschreibt den Prozentsatz der Risiken, die von der geplanten Investition abgedeckt wären. Dieser Prozentsatz beruht ebenfalls auf einer Einschätzung. Hier sollte auf einen selbst gewählten Bewertungs-Algorithmus zurückgegriffen werden. Auch wenn dieser Wert vorerst ungenau sein wird, besteht eine große Chance, zumindest im Zeitverlauf auf eine wiederholbare und konsistente Weise den Wert verschiedener Investitionen besser bestimmen zu können.

Kosten der Maßnahme (KM) in EUR: Möglichst genaue Aufrechnung aller entstehenden Kosten (einmalig und laufend) für die Realisierung einer entsprechenden Maßnahme.

Der RoSI (in Prozent) der quantitativen Risikoanalyse errechnet sich nun folglich aus:

$$\frac{(VE * MQ) - KM}{KM}$$

4.2 Interpretation

Der errechnete Wert ist ein Prozentsatz und definiert die jährliche Ersparnis in Bezug auf die Kosten der Maßnahme.

Konkret bedeutet ein RoSI von 100%, dass die Investition sich pro Jahr vollständig durch die Einsparung ausgleicht (Beispiel: Bei einer Investition von 10 TEUR pro Jahr für eine bestimmte Maßnahme ergibt sich bei einem RoSI von 100% eine jährliche Ersparnis von 10 TEUR).

Um einen absoluten Betrag der Einsparung bei Implementierung eine Lösung zu bekommen, muss man die Kosten der Maßnahme mit dem absoluten Wert des RoSI multiplizieren (Beispiel: Kosten der Maßnahme 20 TEUR, RoSI = 120 % => 20 TEUR * 1,2 = 24 TEUR, dies bedeutet, dass bei einem jährlichen Invest von 20 TEUR für eine Maßnahme eine jährliche Ersparnis von 24 TEUR entstehen würde).

Diese Werte können nur als grobe Richtwerte dienen, da die notwendigen Kennzahlen ja fast ausschließlich auf Annahmen beruhen. Nichtsdestotrotz ist dies dennoch wesentlich wertvoller, als ein vollkommen aus dem Bauch heraus geschätztes Einsparvolumen.

5 Unser Portfolio

Wir haben nicht nur die Qualifikationen, sondern auch die fachliche Kompetenz und Praxiserfahrung. Unsere Kompetenz haben wir in vielen erfolgreichen Projekten unter Beweis gestellt. Alle von uns unterstützten Unternehmen sind erfolgreich unabhängig zertifiziert worden und verfügen über ein etabliertes Informationssicherheitsmanagementsystem (ISMS).

Engagement, Know-how und Zuverlässigkeit: Das ist unser Erfolgsrezept. Wir arbeiten konsequent an unseren Kompetenzen und unserer Qualität, damit unsere Kunden ihre Ziele erreichen und Ihr Geschäft zukunftssicher entwickeln. Wir arbeiten mit Leidenschaft an den Projekten unserer Kunden.

Wir haben das Ziel unsere Kunden zu begeistern und bauen auf eine langfristige Partnerschaft. Durch engagiertes und verantwortungsvolles Handeln eines jeden Einzelnen erreichen wir ein Höchstmaß an Identifizierung mit unseren Kunden.

Unser Portfolio für Sie:

- Kostenlose Erstberatung zur IT- & Informationssicherheit
- Vor Ort Bewertung Ihrer IT- & Informationssicherheit
- GAP-Analysen
- Projektierung zur Einführung von IT- & Informationssicherheitsmanagementsystemen
- Integration von bestehenden Managementsystemen
- Risikobewertungen
- Business Impact Analysen
- Erstellung von Richtlinien und Verfahrensanweisungen
- Prozess-Analyse, -darstellung, -optimierung und Digitalisierung
- Schulungen von Mitarbeitern
- Begleitung zur Zertifizierung gemäß ISO/IEC 27001, BSI-Grundschutz und TISAX®
- Stellung des externen Informationssicherheitsbeauftragten
- Umsetzung der gesetzlichen Anforderungen aus der DSGVO

Kontakt

mabs4.0 Deutschland GmbH
Südring 133
42579 Heilgenhaus

Telefon: +49 2056 267 9050
E-Mail: kontakt@mabs40.com
Internet: http://mabs40.de.com