



**IHR LOTSE FÜR INFORMATIONSSICHERHEIT**  
Risiken erkennen und handeln



# VORWORT

Sehr geehrte Damen und Herren,  
liebe Interessenten, Kunden und Partner,

wir freuen uns, Ihnen heute mit unserer ersten Imagebroschüre unser Unternehmen mit seinen vielfältigen Dienstleistungen vorstellen zu dürfen. Unter dem Motto „**Ihr Lotse für Informationssicherheitsmanagement**“ haben wir Ihnen ein Dienstleistungsportfolio zusammengestellt, um Ihnen einen optimalen Erfolg zu gewährleisten. Zufriedene, nein, begeisterte Kunden sind unser Anspruch!

Informationssicherheitsmanagement ist in vielen Branchen und Bereichen ein Thema, welches wie kaum ein anderes den Zeitgeist trifft. Sie sind Automobilzulieferer, Sie stellen kritische Infrastruktur bereit, Ihre Kunden wünschen sich Ihre systematische Auseinandersetzung mit diesem und weiteren verwandten Themen?

Informationssicherheit, Datenschutz und Business Continuity sind die Erfolgsfaktoren für Unternehmen in der Zukunft und wir betreuen Sie kompetent und zielgerichtet.

**In diesem Sinne wünschen wir Ihnen viel Spaß mit dieser Broschüre!**



**Andreas Nöh**  
Geschäftsführer

☎ +49 (0)160 979 796 97

✉ andreas.noeh@acm-consultants.de



**Patrick Andreas**  
Managing Consultant / Prokurist

☎ +49 (0) 151 146 655 55

✉ patrick.andreas@acm-consultants.de

# IHR LOTSE FÜR INFORMATIONSSICHERHEIT

Durch Digitalisierung und Globalisierung ändern sich die Anforderungen von und an Unternehmen ständig. Cloud-Computing, stetig wechselnde Regularien, andere Ereignisse, wie etwa mobiles Arbeiten, beeinflussen die sichere Führung eines Unternehmens zu jeder Zeit unterschiedlich. Als Lotse für Informationssicherheit ist es unsere Aufgabe, Ihr Unternehmen und die Mitarbeiter zu schützen sowie sicher und effizient zu organisieren.



## NOTFALL-MANAGEMENT

Legen Sie den Grundstein, um Ihre kritischen Geschäftsprozesse bei Störungen aufrecht zu erhalten.

Seite 4



## INFORMATIONSSICHERHEIT

Von der Analyse des IST-Stands über das Erstellen eines Sicherheitskonzeptes bis zur Einführung des für Sie optimalen ISMS.

Seite 5



## RISIKO- & COMPLIANCE MANAGEMENT

Erfahren Sie, wie IT-Risiken korrekt bewertet werden und treffen Sie die richtigen Entscheidungen!

Seite 6



## PENETRATIONSTESTS UND IT-SICHERHEITSANALYSEN

Wir suchen nach technischen Schwachstellen, wie Fehlkonfigurationen, veralteter Software oder dem ungewollten Zugriff auf Ihre (Kunden-) Daten.

Seite 7



## MANAGED SECURITY SERVICES

Auf Ihr Unternehmen maßgeschneiderte IT-Sicherheits-Services, immer nach dem neusten Stand der Technik.

Seite 8



## SCHULUNGEN

Wir schulen Sie, Ihre Führungskräfte und Ihre Mitarbeiter und stärken somit das schwächste Glied in der Kette – Den Menschen.

Seite 9



## NOTFALLMANAGEMENT

Die IT in einem Unternehmen, egal welcher Branche, wird immer komplexer. Wir virtualisieren immer mehr Geschäftsprozesse und Services und bilden diese auf unseren IT-Systemen ab. SAP-gestützte Produktionsketten, umfangreiche CRM-Systeme in Logistik, Buchhaltung und Vertrieb stellen uns vor die Fragen:

- Wie lange können wir ohne unsere IT-Systeme auskommen?
- Nach welcher Zeitspanne steht die Produktion still und ist der Vertrieb überhaupt arbeitsfähig, wenn keine Kundendaten mehr abrufbar sind?
- Wie ermöglichen wir den zumindest eingeschränkten weiteren Ablauf wichtiger Prozesse und Services, wenn die gewohnten Arbeitsmittel nicht mehr zur Verfügung stehen?

Die Verantwortung der IT wächst ständig. Das wirtschaftlich erfolgreiche Agieren eines Unternehmens hängt immer mehr von einer funktionierenden IT ab, die oft personell unterbesetzt ist. Damit wird das Wissen über die Systeme auf wenige Personen verteilt. Da inzwischen fast alle Geschäftsprozesse von IT-Systemen unterstützt und abgebildet werden, müssen wir uns Gedanken über Verfügbarkeiten und geschäftskritische Ausfälle machen.

Die Einführung eines Business Continuity Management Systems (BCMS) nach z.B. ISO 22301, oder BSI 200-4 ist ein strategisches und wichtiges Managementsystem und dabei eng verwandt mit dem Risikomanagement.

Wir unterstützen Sie beim Aufbau eines BCMS mit Beratung und Schulung Ihrer Mitarbeiter, bis zur Begleitung des Auditprozesses.



# INFORMATIONSSICHERHEIT

Um die Informationen in Unternehmen schnell und verantwortungsbewusst zu verarbeiten, bedarf es heute komplexer IT-Systeme. Ihre sichere Handhabung und ihre Prozesse gewährleisten einen sicheren Umgang, da Daten vertraulich, zugänglich und integer sein müssen.

Welche Informationen und welche Systeme, wie stark geschützt werden müssen, das ist die Frage, mit der sich Verantwortliche beschäftigen müssen. Schutzmaßnahmen können erst geplant und eingesetzt werden, wenn die Risiken und Ziele bekannt sind.

Wir starten deshalb mit einer GAP-Analyse Ihrer aktuellen Sicherheitslage. Anschließend bekommen Sie eine geeignete Strategie auf der Grundlage wir Ihr Informationssicherheits-Managementsystem (ISMS) auf der Basis anerkannter Standards wie der ISO 27001 oder VdS 10000 einführen werden.



- Wie lange können wir ohne unsere IT-Systeme auskommen? Dabei gilt jedoch vor allem eins: Erst die richtige Strategie macht aus Einzelmaßnahmen eine wirksame und effiziente Lösung.
- Wir haben dazu ein Prozessmodell für den Aufbau eines ISMS erstellt und nutzen eine Softwarelösung, mit der wir in der Lage sind, ein ISMS aufzubauen, zu messen und zu bewerten.
- Wir unterstützen Sie als Ihr Partner bei der Projektplanung, stellen auf Wunsch Kontakte zu Zertifizierern her und begleiten den gesamten Audit-Prozess.
- Dabei darf die Sicherheit Sie bei der täglichen Arbeit nicht behindern. Bei uns steht der Mensch daher im Vordergrund. Erst wenn alle Mitarbeiter verstanden haben, wie sie Risiken vermeiden und Informationen schützen können, erreichen Sie Ihr Ziel.



# RISIKO- & COMPLIANCE MANAGEMENT

Risikomanagement rückt aktuell stark in den Vordergrund der betrieblichen Unternehmenssteuerung. Schon lange war Risikomanagement im Fokus der Wirtschaftsprüfer, deren Institut für Wirtschaftsprüfer (IDS) hierfür extra Prüfungsstandards entwickelt hat.

Aktuell kommen ebenfalls alle Normen mit dem sogenannten risikoorientierten Ansatz - und das macht es notwendig, über ein ganzheitliches Risikomanagement nachzudenken und im Unternehmen umzusetzen. Hierbei sollte man das betriebswirtschaftliche mit dem technischen Risikomanagement verbinden und zu einem Enterprise Risk Management zusammenführen.

Die ISO 31000 und ISO 27006 definieren hier die Anforderungen an ein Risikomanagement und Risikomanagementsystem, welche auch die Prüfungsanforderungen der Wirtschaftsprüfer, abdeckt.

Ob Informationssicherheitsmanagementsysteme (ISMS), Notfallmanagementsysteme (BCMS) und Datenschutz oder Themen bezüglich des IT-Risiko- und Compliance-Managements - Wir sind Ihr Partner. Unsere Consultants verfügen über fundiertes Wissen zu ISO 31000, ISO 27001 und MaRisk, sodass auch angrenzende Disziplinen bei der Lösungsfindung berücksichtigt werden.



„Risiken erkennen  
und handeln!“



## PENETRATIONSTESTS UND IT-SICHERHEITSANALYSEN

Ein etabliertes Informationssicherheitsmanagementsystem (ISMS) muss in regelmäßigen Abständen durch interne und externe Audits – und somit auch Penetrationstests überprüft werden.

Die regelmäßige Ermittlung des IST-Stands liefert wichtige Kennzahlen (KPI) für den Informationssicherheits- und Risikomanagementprozess und ist ein elementares Instrument innerhalb des PDCA Zyklus (Plan – Do – Check – Act).

Ob einmalig oder regelmäßig wiederkehrend, entsprechend Ihres Schutzbedarfs, ermitteln wir durch gesteuerte Angriffe bei einem Penetrationstest Sicherheitslücken im IT-Betrieb und den Komponenten der IT-Infrastruktur Ihres Unternehmens.

Aus den Erkenntnissen generieren wir für Sie einen Bericht der gefundenen Gefährdungen und geben Ihnen konkrete Anhaltspunkte zur Behebung der Schwachstellen.

Jeder Bericht enthält daher eine konkrete Dokumentation der Findings, sowie eine Risikobewertung auf Basis der Kriterien Eintrittswahrscheinlichkeit, Schadenshöhe im Eintrittsfall und dem daraus resultierenden Handlungsbedarf. Gern beraten wir Sie bei der Entscheidung, in welchem Umfang und welcher Tiefe die jeweilige Analyse durchgeführt werden soll, um für Sie den größtmöglichen Mehrwert bei tragbarem Risiko zu erzielen.



## MANAGED SECURITY SERVICES

Stillstand bedeutet Arbeitsausfall, erzeugt hohe Folgekosten und bedeutet nicht selten auch Reputationsverlust. Aktualisierungen, Patches, Sicherheitsupdates und die Überwachung wichtiger Prozesse erfordern Zeit, Know-how und Verantwortung. Unternehmen ohne eigenes Fachpersonal scheuen die schlecht planbaren Zusatzkosten für externe Dienstleister.

Nicht selten werden IT-Aufgaben sogar als Zusatzaufgabe an fachfremde Mitarbeiter vergeben.

Teuer wird es immer dann, wenn Fehler auftreten, die aufgrund fehlender Kontrollen nicht erkannt werden. Es drohen Systemausfälle und Datenverlust – die Sicherheit Ihrer Systeme ist gefährdet.

Frühes Erkennen von Fehlern verringert das Ausfallrisiko und reduziert die Kosten. Andere Aufgaben werden von unserem Managed IT-Service-Team routinemäßig durchgeführt. Durch strukturierte Bearbeitung können Kosten drastisch reduziert werden. Alle erbrachten Leistungen werden erfasst und fließen in die laufend aktualisierte Dokumentation ein.

Sollte es trotzdem zu unvorhergesehenen Störungen kommen, bieten Ihnen Managed Services garantierte, kürzeste Reaktionszeiten für die Wiederherstellung des vollen Funktionsumfangs. Kosten entstehen nur, wenn auch Nutzen erzeugt wird – Sie zahlen nicht für Krankheit, Urlaub oder Fortbildungen von eigenen Mitarbeitern. Wir sind immer up-to-date und bieten Ihnen alle Services und Produkte, die Sie für Ihr Unternehmen benötigen.



# SCHULUNGEN

Im Rahmen unseres Schulungsprogramms teilen unsere projekterfahrenen Berater ihr Wissen im Bereich der Informationssicherheit.

Lernen Sie in unseren Seminaren, wie ein Informationssicherheitsmanagementsystem (ISMS) aufgebaut und betrieben wird, wie Risikoanalysen durchgeführt, Sicherheitsvorfälle behandelt oder ein pragmatisches Notfallmanagement eingeführt werden kann. Wir erklären Ihnen, wie Sie Ihre Mitarbeiter sensibilisieren können bzw. führen die Maßnahmen für Sie durch.



## TISAX

Die Teilnehmer erhalten Kenntnisse in TISAX, so dass sie den Aufbau und die Anforderungen der Norm verstehen und anwenden können. Mit dem Wissen ist es möglich, ein ISMS nach TISAX einzuführen, aufzubauen und umzusetzen. Außerdem können die Kenntnisse genutzt werden, um interne Audits bzw. Assessments nach TISAX durchzuführen.



## ISO 27001

Die Teilnehmer erhalten Kenntnisse in die ISO 27001, so dass sie den Aufbau und die Anforderungen der Norm verstehen und anwenden können. Mit dem Wissen ist es möglich, ein ISMS nach ISO 27001 einzuführen, aufzubauen und umzusetzen. Außerdem können die Kenntnisse genutzt werden, um interne Audits nach ISO 27001 durchzuführen.



## GRUNDKENNTNISSE ISMS

Die Teilnehmer erhalten einen Überblick über die Hintergründe und Notwendigkeiten eines Informationssicherheitsmanagementsystems, die Gemeinsamkeiten und Unterschiede der Normen, wichtige Inhalte sowie Beziehungen zu anderen Managementsystemen (z.B. ISO 9001), um die Bedeutung der Thematik zu kennen und weitere Schritte planen zu können, aber auch um vorhandene Grundkenntnisse zu aktualisieren und zu ergänzen.

# INFORMATIONSSICHERHEIT MIT SYSTEM

Die CONTECHNET Deutschland GmbH ist ein deutscher Softwarehersteller und wurde im Jahr 2007 in der Region Hannover gegründet. Angefangen als Spezialist für IT-Notfallplanung hat sich das Portfolio über die Jahre um die Themengebiete Informationssicherheit und Datenschutz erweitert.

Die CONTECHNET Suite bietet ein standardisiertes Vorgehensmodell zur Umsetzung von Informationssicherheit, IT-Notfallplanung und Datenschutz.

Hierbei setzt CONTECHNET bei allen Lösungen auf die Nutzung bereits bestehender Daten. Die CONTECHNET Suite zeichnet sich durch eine einheitliche Bedienbarkeit aus und sorgt für eine praxisbezogene und nachvollziehbare Nutzung. Auf diese Weise werden Schulungs- und Betriebsaufwände eingespart, sowohl bei der Einführung als auch im weiteren Betrieb. Alle Lösungen enthalten definierte Schritte, die den Anwender unmittelbar zum Ergebnis führen. Importfunktionen und Schnittstellen ermöglichen eine automatisierte und permanente Aktualisierung der Assets und gewährleisten damit die Nachhaltigkeit der Lösungen. Gleiches gilt für die Aktualität von Dokumenten sowie das Nachhalten von Änderungen bei Personal und Verantwortlichkeiten.

Die verzahnten Module der CONTECHNET Suite lassen sich sowohl einzeln als auch in Kombination verwenden. Die gemeinsame Datenbasis macht einmal angelegte Assets wie Prozesse, Personal und Infrastruktur für alle Bereiche nutzbar.



- INDITOR® ISO: Softwarelösung zur Implementierung und zum Betrieb eines ISMS nach ISO 27001
- INDART Professional®: Softwarelösung zum Aufbau und zur Pflege einer prozessorientierten IT-Notfallplanung
- INPRIVE®: Softwarelösung zur Dokumentation des Datenschutzes gemäß der EU-DSGVO



# NORMTRACKER REVOLUTIONIERT IHRE INFORMATIONSSICHERHEIT

NormTracker, das webbasierte ISMS Tool, führt Anwender zielorientiert und ganzheitlich durch die Anforderungen an die Informationssicherheit.

Profitieren Sie von einem perfekt vorbereiteten Bausteinkasten, der Sie sicher und einfach zu Ihrem Ziel führt. Mit simplen Checklisten werden Sie durch die Anforderungen und die erforderliche Dokumentation geleitet, sodass Sie schnell und übersichtlich eine auditreife Basis schaffen.

Darüber hinaus erhalten Sie alle erforderlichen Features, um den kontinuierlichen Verbesserungsprozess leben zu können. Legen Sie sich ein Assetmanagement an, führen Sie protokollierte Tests durch und nutzen Sie in allen Listen die Möglichkeit Aufgaben anzulegen sowie Dokumente hochladen oder verlinken zu können.

Verbessern Sie die Kollaboration in Ihrer Organisation, indem Sie das durchdachte Rollenkonzept im NormTracker nutzen, ganz ohne User-Limit.

Dabei werden Sie die Motivation steigern und ein besseres Gesamtergebnis erzielen. Ein Risikomanagement hilft Ihnen dabei, die erkannten Gefährdungen zu verwalten und mit Maßnahmen und Wirksamkeitsprüfung sorgsam zu verfolgen.

Mit NormTracker können Sie problemlos mehrere Standorte anlegen und überwachen, vermeiden Auditspitzen und sind zu jeder Zeit auf dem aktuellen Stand.

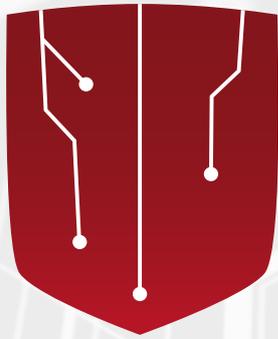
Sie legen Ihre Ziele fest und wählen aus den verschiedenen Normen-Modulen Ihre Projekte aus, zum Beispiel einen guten Basisschutz nach:

- VdS 10000 ISMS für KMU
- VdS 10010 DSMS für KMU
- VDA TISAX
- ISO 27001

Auf Wunsch erhalten Sie umfangreiche Aufgaben- und Gefährdungskataloge zur Verfügung gestellt und können bereits vorhandene Listen und Ergebnisse mühelos importieren.

Gerne zeigen wir Ihnen im Rahmen einer Live-Vorführung die Mehrwerte von NormTracker und stellen auf Wunsch weitere Informationen zur Verfügung.

Fragen Sie nach einer kostenlosen Testphase und beginnen Sie Informationssicherheit zu leben.



**ACM**  
CONSULTANTS



**ACM Consultants GmbH**  
Hauptsitz Warendorf

 Am Holzbach 10, 48231 Warendorf

 [www.acm-consultants.de](http://www.acm-consultants.de)

 [info@acm-consultants.de](mailto:info@acm-consultants.de)