UIMC®
DR. VOSSBEIN
GMBH & CO KG

IT-Sicherheit mit System

Der effektive und effiziente Aufbau eines Informationssicherheits-Managementsystems

UIMC DR. VOSSBEIN GMBH & CO KG
Nützenberger Straße 119
42115 Wuppertal
Tel.: (0202) 265 74 - 0
Fax: (0202) 265 74 - 19
E-Mail: consultants@uimc.de
Internet: www.UIMC.de

Informationssicherheits-Managementsystem

Anforderungen an die und Probleme in der IT-Sicherheit

UIMC®

Risikoanalyse
siehe Seite 4

Festlegung der IT-Sicherheitsstrategie/-politik
siehe Seite 5

Festlegung des Status quo und des Verbesserungsbedarfs
siehe Seiten 6f.

Erarbeitung eines unternehmensspezifischen IT-Sicherheitskonzepts
siehe Seite 8

Verbesserung durch
- Schulung (S. 11)
- Beratung & Coaching (S. 10)
- standardisierte Konzepte (S. 12)

Revision bzw. Auditierung
siehe Seite 12

weitere Unterstützung
- Notfallmanagement
- Management/Organisation
- Datenschutz u. v. m.

siehe Seiten 13 f.

Anforderungen an die IT, die Informationen und deren Sicherheit

Die Bedeutung der Sicherheit von Informationen sowie der Systeme, auf denen sie verarbeitet werden, steigt mit zunehmender Abhängigkeit von der IT. Eine Geschäftstätigkeit ohne IT ist heutzutage nicht mehr denkbar, eine Beeinträchtigung oder gar Verlust und Ausfall kann katastrophal sein!

Neben den internen Interessen an eine sichere IT stehen Unternehmen diversen externen Anforderungen gegenüber:

- Einhaltung von Gesetzen (BDSG, Steuergesetze, Basel II, etc.)
- Sicherstellung eines adäquaten Qualitätsmanagements
- Wirtschaftsprüfern (Prüfung der Ordnungsmäßigkeit)
- Anforderungen von Kunden (z. B. durch Lieferantenbedingungen)
- Normanforderungen für Auditierung/Zertifizierungen

Dies zeigt die Notwendigkeit eines Informationssicherheits-Managementsystems (ISMS)!

Probleme bei der Gewährleistung von IT-Sicherheit & Aufbau eines ISMS

Es ist keine Seltenheit, dass eine ordnungsgemäße Informationsverarbeitung und entsprechende IT-Sicherheit in punkto Verfügbarkeit, Integrität und Vertraulichkeit nicht gewährleistet ist, da Voraussetzungen wie

- angemessene Kapazitäten zur Erstellung und Pflege des ISMS,
- Sensibilisierung der Geschäftsleitung und der Mitarbeiter,
- IT-sicherheitsbezogenes und -relevantes Know-how und/oder
- Transparenz von Regelungen und Maßnahmen

nicht gegeben sind.

Die Schwierigkeiten, IT sicher zu gestalten, liegen für viele Institutionen insbesondere in der strukturierten Herangehensweise. Die Herausforderung besteht in der effektiven und effizienten

- Durchführung von Analysen,
- Erstellung von Konzepten, Richtlinien, Dokumenten sowie
- deren internen Umsetzung.

Seien Sie vorbereitet!

Die Erfahrung der vergangenen Jahre zeigt, dass zunehmend Unternehmen Ihren Partnern im Hinblick auf die Informationssicherheit „auf den Zahn fühlen“. So werden bspw. Lieferanten, technische Berater und die IT-Dienstleister stärker geprüft und auditiert. In der Regel auf Basis der ISO 27001/-02.

Umsetzung der IT-Sicherheit

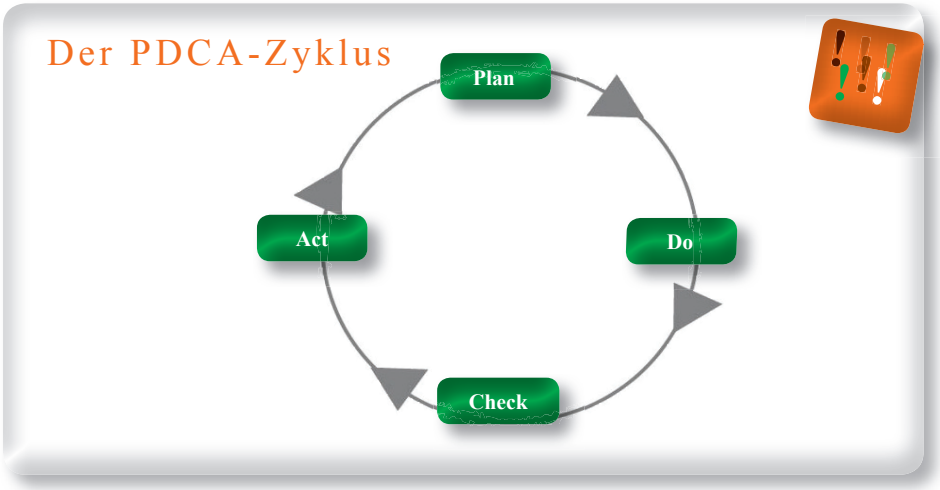
Probleme, Lösungsansätze und Unterstützungsmöglichkeiten

IT-Sicherheit durch Normorientierung

Die ISO/IEC 27002 ist eine internationale Norm, die Anforderungen an ein ISMS in Form von praxiserprobten Sicherheitsanforderungen beschreibt, den sog. Baseline Controls. Sie ist ein anerkannter und empfohlener Leitfaden für die Einrichtung und Verwaltung eines ISMS.

Die ISO 27001 ist wiederum Basis für eine Auditierung und Zertifizierung des ISMS und liefert einen Prüfstandard für das Management der IT-Sicherheit, welches z. B. gemäß ISO/IEC 27002 aufgebaut wurde.

Eine effiziente und effektive Entwicklung, Umsetzung und Verbesserung der Wirksamkeit des ISMS einer Organisation ist durch den integrierten Prozessansatz, das sog. PDCA-Modell (Plan-Do-Check-Act), sichergestellt.



Ansatz und Vorgehensweise zur Etablierung eines ISMS

Jedes ISMS ist ein dynamisches System von Prozessen, das insbesondere durch den Ansatz des PDCA-Modells kontinuierlich optimiert wird. Die Identifizierung und das Zusammenwirken dieser Prozesse und deren Management ist auf alle ISMS-Prozesse anwendbar.

Inhalte des ISMS stellen sich strukturiert nach PDCA-Modell wie folgt dar:

- Plan: Festlegen der Sicherheitspolitik, -ziele, -prozesse, Verfahren, die für das Risikomanagement und die Verbesserung der Informationssicherheit relevant sind.
- Do: Ermittlung des aktuellen Stands der IT-Sicherheit und Umsetzung der Politik, Maßnahmen, Prozesse und Verfahren.
- Check: Prüfung der Angemessenheit und Qualität der Prozessleistung anhand der Politik, Ziele und praktischen Erfahrungen
- Act: Etablierung von Verbesserungs- und Präventivmaßnahmen, basierend auf den Ergebnissen der vorherigen Prüfung.

Die einzelnen Phasen zur Etablierung eines ISMS sind auf der vorherigen Seite dargestellt.

Mehr als nur IT-Sicherheit

Es sei an dieser Stelle angemerkt, dass die UIMC Sie neben dem Aufbau eines Informationssicherheits-Managementsystems auch in anderen, verwandten Themengebieten unterstützen kann, wie beispielsweise in der Datenschutzberatung, im Risikomanagement, in allgemeinen Organisationsfragestellungen und im Notfallmanagement.

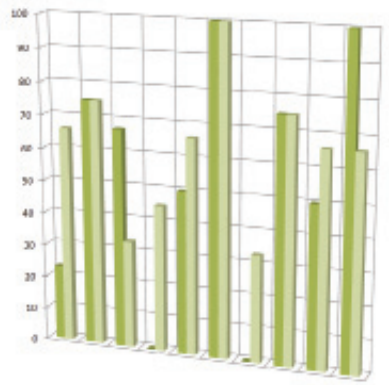
Risikoanalyse

IT-Sicherheitsrisiken erkennen, bewerten und mindern

Aufgabe der Risikoanalyse sowie Probleme bei der Durchführung

Zu Beginn sollte eine Risikoanalyse stehen, welche maßgeblich das weitere Vorgehen beeinflusst. So müssen z. B. existentielle Risiken entsprechend in der IT-Sicherheitsstrategie und in den Zielen berücksichtigt werden.

Bisherige Risikoanalyse-Methoden sind oftmals hochkomplex und sehr aufwändig. Sie beruhen in der Regel auf Schätzwerten - wie bspw. der Eintrittswahrscheinlichkeit, finanzieller Auswirkungen etc. -, die jedoch nicht aussagekräftig sind. Bei diesen quantitativen Ansätzen fehlt der direkte Bezug zu den geschäftsrelevanten Prozessen und den international anerkannten Normen/ Standards.



Die UIMC-Lösung ist toolgestützt

Die Durchführung eines von der UIMC moderierten/gelenkten Workshops bei Ihnen im Hause mit Hilfe des UIMC-Risktools bietet Ihnen:

- qualitative Durchführung der Risikoanalyse
- Ermittlung des bisherigen Stands der Risikobetrachtung
- Ermittlung der Art und des Umfangs der Risikodokumentation
- Bewertung bislang noch nicht erfasster und bewerteter Risiken.

Dabei verfolgt die UIMC-Methodik zwei normbasierte Sichtweisen:

- geschäftsprozessorientiert: Risikoevaluation der vorab unternehmensintern identifizierten und priorisierten Geschäftsprozesse
- inhaltlich normorientiert: Risikoevaluation in Anlehnung an die Controls des ISO 27001.

Risikopapier als dokumentiertes Ergebnis

Ergebnis ist ein Risikopapier, das die geschäftsprozessbezogenen und norm-orientierten Risiken sowie deren Dokumentationsstand aufzeigt. Darüber hinaus erhalten Sie eine Bewertung, die als Grundlage für das ISMS und damit speziell der Implementierung notwendiger Regelungen und Maßnahmen zur Risikobehandlung dienen.

Das UIMC-Risktool ermöglicht zudem eine quantitative Auswertung, so dass die Ergebnisse graphisch dargestellt und z. B. verschiedene Geschäftsprozessevaluationen verglichen und veranschaulicht werden können.

Vorteile und Nutzen

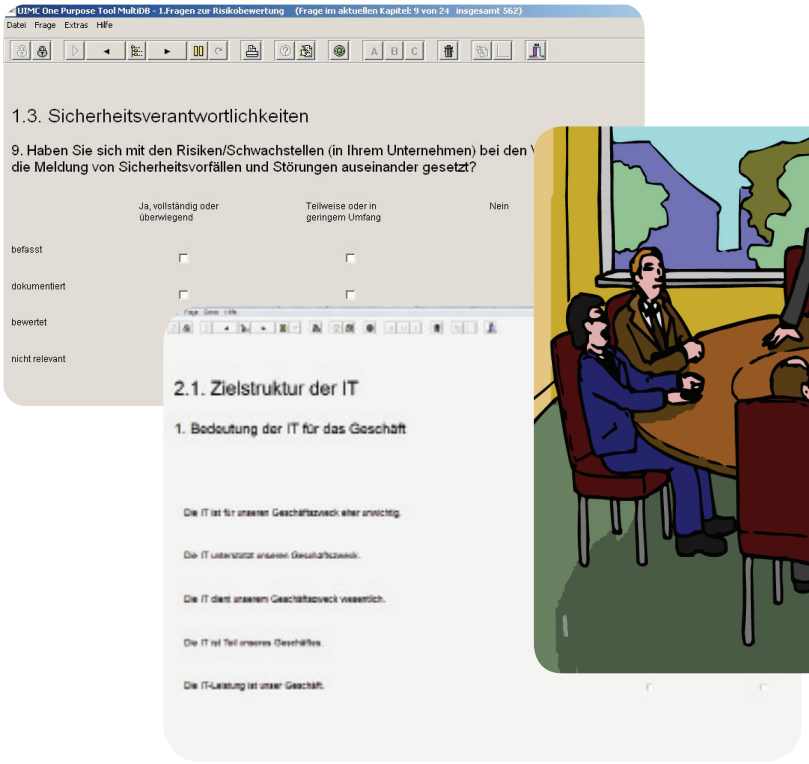
- Normorientierte/-konforme Vorgehensweise
- Berücksichtigung von Auditierungs- und Zertifizierungsanforderungen schon im Aufbau
- Geringe Anforderungen an personelle, zeitliche und finanzielle Kapazitäten
- Überschaubare und zeitsparende Methodik der Risikoerhebung durch quantitatives Vorgehen

IT-Sicherheits-Strategie- & -Zielfindungsworkshop

Zielgerichtetes Arbeiten durch IT-Sicherheitsstrategie

Unternehmerisches Denken benötigt Strategien

Strategien sind sowohl in der IT-Sicherheit als auch im Datenschutz in fast allen Institutionen ein Stiefkind des unternehmerischen Denkens. Da IT-Sicherheit und Datenschutz aber nicht von selbst kommen, sondern nur durch zielgerichtetes Arbeiten am Problem und durch Beseitigung aller Schwachstellen zu erreichen sind, muss am Anfang eine Sicherheitsstrategie sowie die Festlegung der Sicherheitsziele stehen.



Ziele im Workshop erarbeiten und definieren

Der IT-Sicherheits-Strategie- & -Zielfindungs-Workshop wird computergestützt mit Hilfe der Szenariomethode abgewickelt. Hierdurch können wesentliche Arbeits-/Ergebnisprotokolle während der Sitzung eingebracht, diskutiert und ggf. berichtigt werden. Die Ergebnisse werden durch die UIMC in einem Zielpapier zusammengefasst und der Institution zur Verfügung gestellt. Dies ist dann die strategische Basis für die weiteren unternehmensorganisatorischen und planenden Aktivitäten.

Ziele im Datenschutz integrieren

Aufgrund der hohen Schnittmenge von Datenschutz und IT-Sicherheit sowie der damit verbundenen Synergiepotentiale ist eine integrierte Festlegung der IT-Sicherheits- und Datenschutzziele bzw. -strategie empfehlenswert. Dies kann die Akzeptanz im Hause erhöhen.

Vorteile und Nutzen

- Vereinfachung der Festlegung durch Szenariomethode
- Moderation durch erfahrenen IT-Sicherheitsberater der UIMC
- Keine Betriebsblindheit bei Zieldefinition
- Zielgerichtes Arbeiten in der IT-Sicherheit durch Zielformulierung
- Angemessenes Zielniveau aufgrund erfahrener Berater
- Sofortige Diskussion und mögliche Verabschiedung von Zwischenergebnissen während des Workshops
- Effiziente Aufgabenerfüllung

IT-Sicherheits-Schwachstellenanalyse

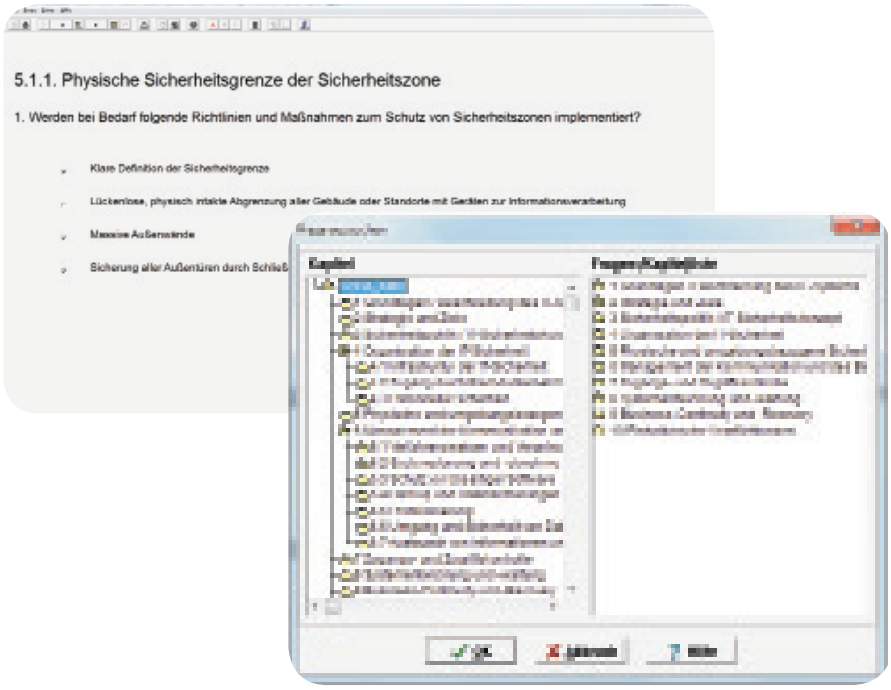
Status quo effizient erheben und IT-Sicherheit verbessern

Vorherige Ist-Analyse ist elementar

Die Abhängigkeit von der Funktionsfähigkeit und Richtigkeit der technischen Informationsverarbeitung steigt ständig. Gleichzeitig schreiben Gesetze vor, welche Anforderungen an „sichere Systeme“ zu stellen sind. Zu diesem Zweck ist es sinnvoll, zunächst den Status quo zu erheben, wodurch Schwachstellen erkannt und nur so auch behoben werden können.

Umsetzungsprobleme

Der bisherige Weg einer komplexen Schwachstellenanalyse erwies sich für viele Unternehmen als nicht praktikabel. Oftmals stellt sich auch neben der Erstellung eines umfassenden Fragenkatalogs die Frage der Effizienz als problematisch dar: Wie kann eine Erhebung und eine Auswertung effektiv und effizient zugleich gestaltet werden?



Vorteile und Nutzen

- Vollständige Prüfung des Status quo in der IT-Sicherheit
- Verzahnung von Auswertung und Ableitung von Maßnahmen
- Zugriff auf ein praxisbewährtes Analyseinstrument
- Effizienzgewinn durch Computerunterstützung
- Neutrale Bewertung des Status quo durch einen Außenstehenden
- Strukturierung der Maßnahmenplanung durch Priorisierung
- Interne Promotion der IT-Sicherheit durch quantitative Auswertung

standardisierte und flexible Analyse

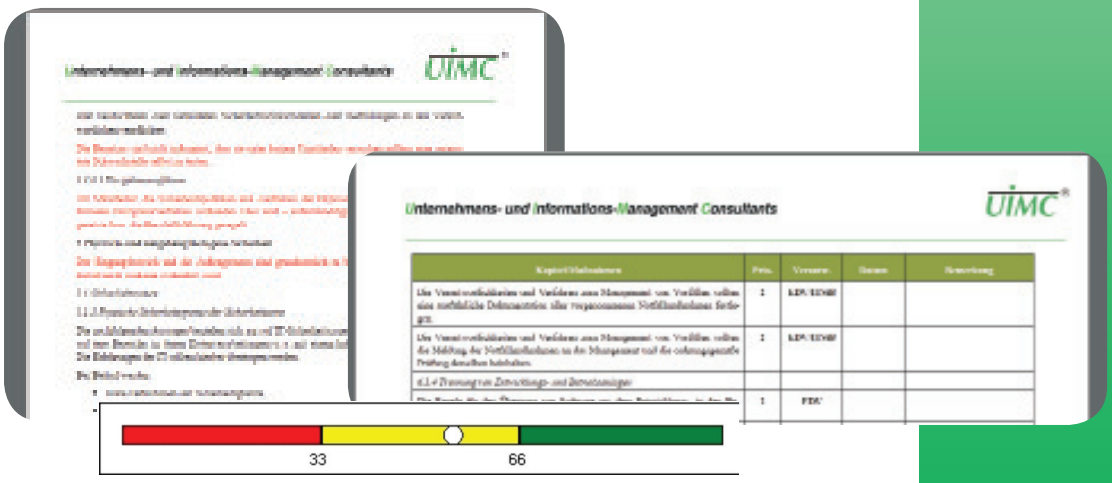
Mit Hilfe des UIMC-Tools für Analyse und Berichterstattung (UTAB) – einem komplexen, modular aufgebauten Programmsystem – wird die Rationalisierung von Analyse- und Beratungsprozessen ermöglicht. Die Prozesse der Konzepterstellung, Umsetzungsvorbereitung sowie Umsetzungsverfolgung laufen computergestützt ab, um Zeit und Ressourcen bei gleichzeitig hoher Qualität der Ergebnisse einzusparen. Aufgrund des computerunterstützten Vorgehens bei der Analyse sowohl in der Erhebungs- als auch in der Auswertungsphase ist eine schnelle Durchführung gewährleistet.

IT-Sicherheits-Schwachstellenanalyse

Schwachstellenerkennung und Maßnahmenplanung

Best Practice mit ISO 27002

Die Anforderungen an ein sicheres IT-Management werden auf Basis des ISO/IEC 27002 computergestützt abgeprüft und Schwachstellen im Sinne von Abweichungen von der Norm [s. u.: rote Schrift] erkannt. Da die Auswertung ebenfalls computerunterstützt ist, wird automatisch ein Ergebnisbericht mit Schwachstellen und möglichen Maßnahmen zur Herstellung eines „sicheren IT-Systems“ erstellt (im Rahmen eines Maßnahmenkatalogs).



Qualitative und quantitative Auswertung

Ferner ist eine quantitative Auswertung möglich. Die Exportierbarkeit in Tabellenform erlaubt eine **aggregierte Darstellung** der Befragungsergebnisse. Eine individuelle Interpretationsmöglichkeit durch angepasste Gewichtungen, eine **zusammenfassende Bewertung** von Erhebungsteilgebieten und die Aggregation von unterschiedlichen Erhebungen werden so ermöglicht. Durch die quantitative Komponente wird auch der Vergleich von durchgeführten Analysen im Sinne eines **Benchmarkings** oder **Trendanalyse** erleichtert bzw. unterstützt.

Die vorgeschlagenen Maßnahmen können durch die UIMC innerhalb einer Aktivitätenliste so vorpriorisiert werden, dass eine sukzessive Abarbeitung der Schwachstellen vorstrukturiert werden kann. Dies ist erforderlich, weil Erfahrungswerte zeigen, dass ein gleichzeitiges Beseitigen verschiedenster Schwachstellen u. a. aus Effizienz-, Akzeptanz- und Effektivitätsgründen nicht sinnvoll ist.

Tue Gutes und rede darüber

Wenn Sie Ihr „sicheres System“ auch nach Außen dokumentieren möchten, so haben Sie die Möglichkeit, sich von unserem Schwesterunternehmen auditieren bzw. zertifizieren zu lassen. Mit Hilfe eines Testats/Siegels bzw. eines Zertifikats können Sie Ihre Bemühungen - beispielsweise an der ISO 27001 - intern und extern kommunizieren.

Management-Summary-Funktion

Auch die Erstellung der Ergebnisberichte wird durch das Tool effektiv und effizient unterstützt. Ein Bericht mit farblich hervorgehobenen Erkenntnissen wird computergestützt erstellt, so dass ein schneller Überblick ermöglicht wird. Die neue Management-Summary-Funktion erleichtert zudem die Aufbereitung für die Management-/Entscheidungsebene.

IT-Sicherheits-Handbuch

Transparenz, Information und Verbindlichkeit schaffen

Notwendigkeit eines IT-Sicherheits-Handbuchs

Mehr als die Hälfte aller Schäden bzw. IT-Sicherheitsprobleme innerhalb von Institutionen resultieren aus der Nachlässigkeit und den Irrtümern der eigenen Mitarbeiter. Neben Schulung und Sensibilisierung der Mitarbeiter kann diesem Umstand mit der Schaffung transparenter, verbindlicher Regelungen begegnet werden. Die Erfahrung zeigt, dass in Unternehmen bereits viele Richtlinien und Maßnahmen gelebt werden, jedoch nicht dokumentiert sind; wie z. B. mit Hilfe eines IT-Sicherheitshandbuchs.

Best Practice als Ausgangspunkt

Die übergeordneten Ziele des UIMC-IT-Sicherheits-Handbuchs sind generell die Unterstützung der Sicherstellung von Informationssicherheit sowie die Dokumentation aller diesbezüglichen Entscheidungen.

Das UIMC-IT-Sicherheits-Handbuch ist daher eine ideale Basis, ein Regelwerk aller aufbau- und ablauforganisatorischen Fragestellungen zu schaffen. Das auf langjähriger Erfahrung (Best Practice) und verschiedene Sicherheitsnormen (insbesondere ISO/IEC 27002) basierende Regelwerk ist modular aufgebaut, wodurch es an jede Institution spezifisch anpassbar ist.

Das UIMC-IT-Sicherheits-Handbuch ist in 2 Hauptteile untergliedert

- Allgemeiner Teil: Institutionsweit gültige Regelungen, Vorgaben etc.
- Formularteil: Ermöglicht vereinfachte Umsetzung der Regelungen

Das UIMC-IT-Sicherheits-Handbuch, als Organisationshandbuch verstanden, ist von seinen Zielen her ein(e):

- Gestaltungs-/Organisationsmittel
- Informationsquelle
- Tool zur Schaffung von Transparenz im Hinblick auf die Organisation

Synergien nutzen, Redundanzen vermeiden

Aufgrund der hohen Schnittmenge von Datenschutz und IT-Sicherheit sowie der damit verbundenen Synergiepotentiale ist eine integrierte Regelung von IT-Sicherheit und Datenschutz in Form eines integrierten Handbuchs zu empfehlen. Dies schafft noch mehr Akzeptanz. Redundanzen und Widersprüche werden vermieden.

Vorteile und Nutzen

- Umfassendes Regelwerk
- Verbindliche Regelungen und Führungsinstrument
- Bewährung durch langjährige Praxiserfahrungen der UIMC
- In Anlehnung an anerkannte Normen
- Übersichtlichkeit durch Unterteilung im allgemeinen Regelungs- und Formularteil
- Schaffung von Transparenz durch eindeutige Handlungsanweisungen
- Verbesserung der IT-Sicherheitssituation
- Praxisgerechte Umsetzung der IT-Sicherheit
- Kostengünstiger im Vergleich zur eigenständigen Erstellung eines Regelwerks
- Effiziente Zertifizierungs-vorbereitung
- Abgestimmt mit anderen Hilfsmitteln der UIMC, wie z. B. Schwachstellenanalyse

eUIMCollege

Mitarbeiter rationell und effektiv sensibilisieren und schulen

Zentrales Element der Umsetzung

Über die Schaffung von transparenten und verbindlichen Regelungen ist es zur effektiven und effizienten Umsetzung von IT-Sicherheitsmaßnahmen unerlässlich, die Mitarbeiter im Bereich der IT-Sicherheit zu sensibilisieren und in Bezug auf die Maßnahmen zu schulen.

Nachteile von Präsenzschulungen

Präsenzveranstaltungen müssen nicht nur vorbereitet und organisiert werden, sondern die Mitarbeiter können in diesem Zeitraum nicht produktiv arbeiten. In dezentralen Institutionen kommt hinzu, dass die Mitarbeiter Transferzeiten zum Schulungsort in Kauf nehmen müssen, was ebenfalls die Effizienz weiter senkt.

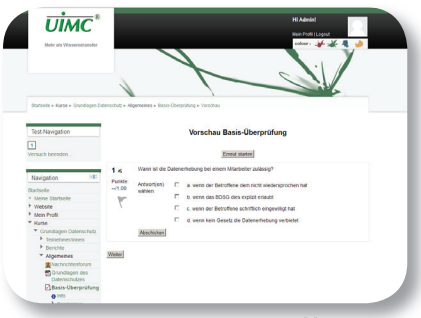
Dezentrales Schulen als Lösungsansatz

In großen und/oder dezentral organisierten Institutionen kann eLearning eine sinnvolle Alternative oder Ergänzung sein. Im eLearning setzen wir auf eine umfassende Identifikation mit den Problemstellungen, so dass ein größeres Verständnis seitens der Mitarbeiter entsteht. Hierdurch und durch die solide Wissensvermittlung wird ein hohes Problembewusstsein erreicht, so dass die zuvor erarbeiteten Regelungen und Verfahren auch tatsächlich gelebt werden.

Multimediale Lern-CD

Identifikation mit der Lernthematik und Wissensvermittlung werden in der multimedialen Lern-CD durch Szenen aus dem beruflichen Alltag kombiniert mit „Hintergrundwissen" erreicht. Vor allem das Problembewusstsein wird durch die animierte Form der Darbietung deutlich verbessert. Im integrierten „College" kann der Wissensstand geprüft werden.

eCollege als browsergestützte Selbstschulung



Über den Browser kann auf die Selbstschulungen via Internet zugegriffen werden, so dass auch von dezentralen Stellen oder von zu Hause gelernt werden kann (auch ohne VPN-Zugang des Mitarbeiters). Je nach gewähltem Modul bzw. Paket können verschiedene Lerninhalte durchgearbeitet sowie zusätzliche Inhalte und Funktionen genutzt werden. eUIMCollege kann jederzeit um weitere UIMC-Module und um eigene Inhalte erweitert werden.

eCollege kann ergänzen! Fragen Sie nach unserer eUIMCollege -Broschüre!

Vorteile und Nutzen

- Kombination aus Sensibilisierung, Schulung und Nachschlagewerk
- Kostengünstige Gewährleistung der Gesetzesforderung
- Ideal auch für dezentrale Organisationen
- Kein interner Schulungsaufwand
- Schulung in produktivitätsschwachen (Tages-) Zeiten
- Effektivitätssteigerung durch starke Sensibilisierungskomponente
- Nutzung eines modernen Mediums

Coaching des IT-Sicherheitsbeauftragten

Fachkunde und Ressourcen durch externe Beratung

Notwendigkeit der Bestellung eines IT-Sicherheitsbeauftragten

Die Einrichtung der Funktion des IT-Sicherheitsbeauftragten (IT-SiB) ist in vielen Institutionen sinnvoll. Der IT-SiB überwacht im Auftrag der Geschäftsleitung die Einhaltung der Sicherheitsbestimmungen. Er hat (die sich ständig ändernden) Gefährdungen der IT zu beachten und zu berücksichtigen. Dazu gehören grundsätzlich alle Aspekte der Installation der IT, der Anwenderschulung und der Überwachung der IT-Sicherheit. Es ist ein einheitliches Sicherheitssystem durchzusetzen, was insbesondere in großen Institutionen mit unterschiedlichen Betriebsstätten sowie zentraler und dezentraler Datenverarbeitung (DV) bedeutend ist.

Zeitliche und fachliche Anforderungen

Das vielschichtige Anforderungsprofil an den IT-Sicherheitsbeauftragten ist jedoch oftmals schwierig intern zu besetzen. Häufig ist dies bis hin zur Implementierung einer funktionierenden Sicherheitsorganisation eine erhebliche zusätzliche Belastung, was schnell zu kapazitären Engpässen in zeitlicher/personeller Hinsicht führen kann. Darüber hinaus wird er trotz Schulungen Erfahrungs- und Wissenslücken insbesondere in der Planung organisatorischer Sicherheitsmaßnahmen haben.

Erfahrung und Entlastung durch Coach

Ein Coaching durch einen externen Berater kann eine praktikable Lösung darstellen. Der Coach kann fachliche Unterstützung bei konkreten Fragestellungen, Unterstützung bei der Einarbeitung in die Thematik sowie beim Aufbau einer IT-Sicherheitsorganisation bieten.

Dem externen Coach können Aufgaben weitergegeben werden, die auch aufgrund von Belastungsspitzen in Kombination mit den übrigen Aufgaben entstehen und IT-Sicherheitsthemen „ausbremsen“ können. Der interne IT-Sicherheitsbeauftragte wird entlastet, ohne dass die IT-Sicherheit zu kurz kommt und die Anforderungen nicht erfüllt werden.

Steigerung der Unabhängigkeit durch Komplett-Outsourcing

Die Funktion des IT-Sicherheitsbeauftragten kann auch komplett an die UIMC ausgelagert werden. Neben den o. g. Vorteilen entfällt auch die aufwändigere Ausbildung und die Unabhängigkeit wird weiter gesteigert.,

Tools zur Effizienzsteigerung

Neben der Nutzung von Beratungsleistungen der UIMC erleichtern unsere Produkte/Hilfsmittel die Verbesserung der IT-Sicherheit in der Institution. Sie stellen eine gute Unterstützung des IT-Sicherheitsbeauftragten dar.

Vorteile und Nutzen

- Nutzung des externen Expertenwissens bei komplexen Fragestellungen
- Keine Betriebsblindheit
- Abfangen von Belastungsspitzen und anfänglichem Mehraufwand (für Aufbau eines ISMS)
- Sofortiger Zugriff auf Know-How
- Schnelle und kurzfristige Hilfestellung bei akuten Problemen
- Zugriff auf praxisbewährte Hilfsmittel
- Effizienzsteigerung durch Zugriff auf Praxiswissen und IT/ IT-Sicherheits-“Spezial“-Wissen

Low-Budget-Konzept

IT-Sicherheit einfach und kostengünstig in KMU organisieren

KMU mit spezifischen Anforderungen und Bedürfnissen

Ein Ausfall der Systeme kann auch in KMU, deren Kerngeschäft weit ab von der IT ist, verheerende Folgen haben. Basis der Anforderungen an die Sicherheit in der Informationstechnik sind zwar generell sehr ähnlich, die Möglichkeiten zur Lösung müssen jedoch wegen unterschiedlicher Gegebenheiten verschieden gestaltet werden. Die Konzeption muss daher für kleine und mittlere Unternehmen (KMU) anders als für Großunternehmen geartet sein.

Kein Geld, keine Zeit... und keine Lust?

Speziell in KMU erschweren vergleichsweise geringe budgetäre Spielräume („low budget“) und das vergleichsweise geringe Wissen sogar das notwendige Erfüllen von Mindeststandards, geschweige denn ein effizientes Erreichen. Oftmals wird die Meinung vertreten, dass für IT-Sicherheit „kein Geld, keine Zeit und keine Lust“ vorhanden ist, da die IT und deren Sicherheit nicht zum Kerngeschäft gehören und „schon nichts passieren wird“.

Ziel eines speziellen Konzepts für KMU muss es daher sein, das Unternehmen trotz geringer Mittel und geringen Know how zum Erreichen des „State of the Art“ zu entwickeln und dabei die Angemessenheit zu berücksichtigen.

Guter Rat ist nicht immer teuer

In der externen Unterstützung sind Vor-Ort-Leistungen des beratenden Unternehmens die teuersten Leistungen. Es ist aus Effizienzgründen Ziel, die kostenintensiven Leistungen zu reduzieren. Durch Nutzung

- moderner Kommunikationstechniken,
- standardisierter Organisationsmittel sowie
- computergestützter Verfahren (z. B. für die Analyse und Schulung)

werden individuelle und Vor-Ort-Leistungen reduziert. Dadurch werden der interne Aufwand und die externen Kosten für Sie optimiert.

Die IT-Sicherheit wird strukturiert angegangen: Auf Basis einer IT-Sicherheits-Schwachstellenanalyse wird ein Maßnahmenkatalog entwickelt, mit dessen Hilfe die IT-Sicherheit sukzessive verbessert wird. Zentrales Instrument ist hierbei das IT-Sicherheits-Handbuch mit allen wesentlichen Anweisungen, Vorgaben, Formblättern etc. Den Mitarbeitern wird das Thema durch etablierte Schulungsmedien näher gebracht und entsprechend sensibilisiert. Spezielle Fragen können per Telefon oder per E-Mail schnell und unbürokratisch geklärt werden.

Einheitliche Umsetzung im Verbund!

Das UIMC-Low-Budget-Konzept eignet sich ebenfalls gut für den Einsatz in Tochterunternehmen, in stark dezentralen Institutionen oder in Konzernen. Das UIMC-Low-Budget-Konzept ist auch für Datenschutz erhältlich. Aufgrund von Schnittmengen ist eine integrierte Betrachtung sogar zu empfehlen; Synergieeffekte geben wir an Sie weiter!

Vorteile und Nutzen

- Berücksichtigung von KMU-Spezifika
- Hohe Verfügbarkeit von Fachkunde ohne teure Vor-Ort-Kosten
- Keine Grauzonen: Transparente Regelungen/Vorgaben für Mitarbeiter
- Nutzung bewährter, computerisierter und dadurch effizienter Verfahrensweisen
- Abgestimmtheit aller Konzeptkomponenten: Schwachstellenanalyse, Organisationsmittel und Schulungen
- Hohe Kostentransparenz
- Verbesserung der Sicherheitssituation in der IT
- Hohe interne Akzeptanz aufgrund optimierter Lösungen (keine Überbetonung der IT-Sicherheit
- Praxisgerechte Umsetzung der IT-Sicherheit
- Kostengünstigkeit durch Standardisierung und Minimierung von Vor-Ort-Leistungen
- Reduzierung/Minimierung des internen Aufwands
- Sofortiger Rückgriff auf langjährige Erfahrung

Auditierung

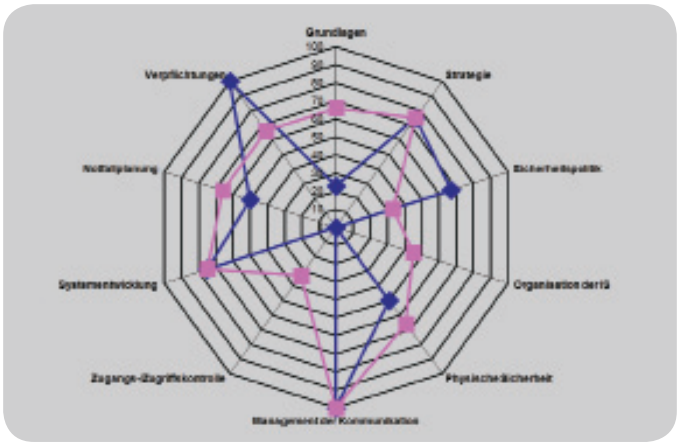
Interne IT-Sicherheitsrevision mit Hilfe anerkannter Normen

IT-Sicherheit ist kein einmaliges Projekt

Aufgrund der ständigen Änderungen der Technologien und der Bedrohungen für die IT, aber auch gesetzlicher und gesellschaftliche Änderungen ist es sinnvoll, regelmäßig eine Status-quo-Erhebung und eine Umsetzungskontrolle durchzuführen. Mit Hilfe eines internen Audits können der Stand der Realisierung des Informationssicherheits-Managementsystems beurteilt sowie Möglichkeiten zur (kontinuierlichen) Verbesserung des IT-Sicherheitsniveaus aufgezeigt werden.

Vergleichbarkeit der Ergebnisse

Analog zu den Schwierigkeiten hinsichtlich der Durchführung einer Schwachstellenanalyse stellt die Erstellung eines umfassenden Fragenkatalogs und die rationelle Durchführung einer solchen Erhebung viele Unternehmen vor eine Herausforderung. Auch sind natürlich gerade bei (regelmäßigen) Audits die Vergleichsmöglichen wichtig, aber mit „Zettel und Stift“ schwer umsetzbar.



Toolgestützte Lösung

Mit Hilfe des UIMC-Auditierungstools - ebenfalls auf Basis des UTAB und analog zur UIMC-IT-Sicherheits-Schwachstellenanalyse strukturiert - werden der Stand der Realisierung des Informationssicherheits-Managementsystems abgebildet, beurteilt sowie Möglichkeiten zur Verbesserung aufzeigt.

Die quantitative Auswertung ermöglicht nicht nur eine zusammenfassende grafische Darstellung der Erhebungsergebnisse, sondern auch den Vergleich von durchgeführten Analysen im Zeitverlauf (**Trendanalyse**). Demnach ist nachvollziehbar, wie sich die IT-Sicherheitssituation nach der letzten Analyse entwickelt hat. Natürlich ist auch ein **Benchmarking** möglich.

Ergebnis ist ein **Gutachten der Qualität** der Sicherheitsorganisation und der Bemühungen sowie eine Mängelliste zur Beseitigung von festgestellten Defiziten und den hieraus resultierenden, nach Prioritäten geordneten Notwendigkeiten, diese Mängel abzustellen sowie eine **Ordnungsmäßigkeitsbestätigung** bzw. ein Testat nach zuvor festgelegter Norm im Anschluss an eine erfolgte Mängelbeseitigung und evtl. notwendiger Nachprüfungen nach Qualitätsnachweis.

Vorteile und Nutzen

- Vollständige Prüfung des Umsetzungsstands des ISMS
- Verzahnung von Auswertung und Ableitung von Maßnahmen
- Zugriff auf ein praxisbewährtes Analyseinstrument
- Effizienzgewinn durch Computerunterstützung
- Kontinuierliche Verbesserung durch regelmäßige Revision
- Interne Promotion der IT-Sicherheit durch Gutachten/ Testat
- Vergleich der Analysen durch quantitative Auswertung

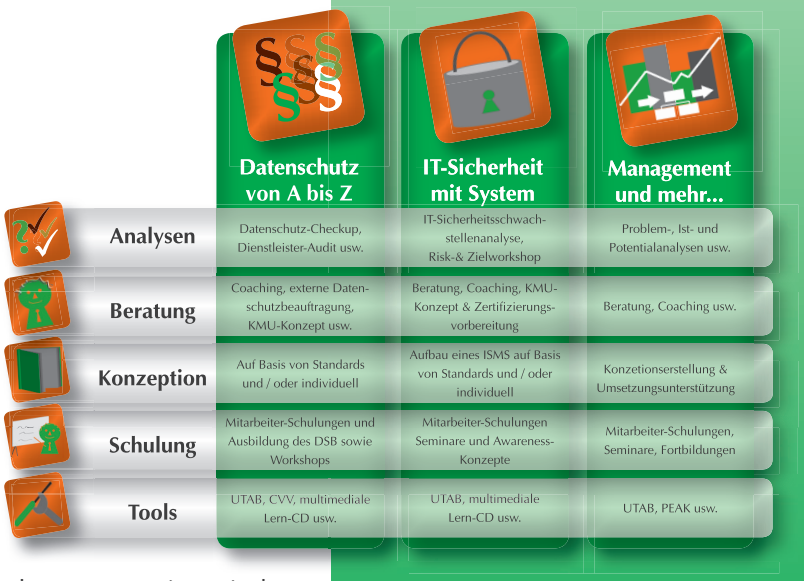
Weitere Unterstützungsmöglichkeiten

Mehr als nur IT-Sicherheit

Wir können Sie in der IT-Sicherheit kompetent und pragmatisch unterstützen. Doch nicht nur hierbei bedienen wir uns Vorgehensweisen, die sich nicht nur in der Praxis bewiesen, sondern auch etabliert haben („Best Practice“). Vielmehr zeigt es sich stets als wertvoll, dass wir auch im Datenschutz, im Informationsmanagement oder der „klassischen“ Management-/Organisationsberatung stark sind.

Notfallvorsorge mit Weitsicht

Ferner ist ein effizientes Notfallmanagement für die Kontinuität und die Fortführung des Geschäfts eines Unternehmens elementar (Business Recovery und Continuity). Hierbei können wir Sie in den Analyse- und Bewertungsprozessen unterstützen, sodass hierauf aufbauende Entscheidungen getroffen werden können, wie „im Fall der Fälle“ vorzugehen ist (Meldewege, Eskalationsstrategien, Notfallpläne etc.). Auch im Rahmen der Umsetzung greifen wir auf langjährige Erfahrungen zurück.



Management und mehr

Die UIMC weist auch Referenzen im Bereich verschiedenster organisatorischer Fragestellungen auf. Von vorstrukturierten Problemen wie der Erstellung eines Archivierungskonzepts oder Erarbeitung von Betriebsvereinbarungen bis hin zu hochindividuellen Problemstellungen wie die Effizienzverbesserung von Geschäftsabläufen: Die UIMC kann Sie unterstützen.

Penetrationstest

Der Zweck des Penetrationstests ist die Prüfung des IT-Systems auf mögliche Mängel und Schwachstellen. Je nach vertraglicher Vereinbarung bietet die UIMC eine Vielzahl hochkomplexer Prüfungsmethoden, wie z. B.:

- Verdeckte und offensichtliche Verifikation von Schwachstellen
- Test von Vertrauensbeziehungen zwischen Systemen
- Verdeckter und offensichtlicher Test der Firewall von außen
- Test des IDS-Systems
- Brute-Force-Attacken
- Abhören von Passwörtern
- Direktes und indirektes, persönliches Social-Engineering mit und ohne physischen Zutritt
- Überprüfung der drahtlosen Kommunikation (z. B. W-LAN)
- Test der administrativen Zugänge zur Telefonanlage/zum Faxsystem
- Überprüfung der Eskalationsprozeduren
- Test der vorhandenen VPN-Schnittstellen und vieles mehr.

Darüber hinaus können auf Wunsch aggressive Scans durchgeführt werden – sowohl solche, bei denen es ein Absturzrisiko gibt, als auch solche, deren Ziel der Absturz des jeweiligen Systems ist.

Datenschutz von A bis Z

Gesetzliche Anforderungen effizienz und effektiv umsetzen

Anforderungen des Datenschutzes

Der Gesetzgeber hat Institutionen aufgrund von diversen gesetzlichen Regelungen unterschiedlichste Vorgaben im Umgang mit personenbezogenen Daten auferlegt: BDSG, Landes- und Gesundheitsdatenschutzgesetze, TKG, TMG, KUG, SGB...

Doch viele Institutionen verstoßen bewusst oder unbewusst gegen Vorschriften! Dabei wird die Einhaltung des Datenschutzes immer wichtiger:

- Die Sensibilität in der Bevölkerung und somit auch der Mitarbeiter und Kunden hinsichtlich des Umgangs und der Sicherheit von Daten steigt zusehends, so dass ein Verstoß zu einem Imageverlust führen kann.
- Datenschutz wird von „gegangenen“ Mitarbeitern instrumentalisiert und als Mittel für deren Zweck missbraucht.
- Qualitätsmanagement verlangt auch sichere, gesetzeskonforme IT-Systeme, was mit steigender IT-Abhängigkeit wichtiger wird.
- Wirtschaftsprüfer gehen dazu über, auch die Ordnungsmäßigkeit hinsichtlich Datenschutz und Informationssicherheit regelmäßig zu prüfen.

Unterstützungsmöglichkeiten durch die UIMC

Im Bereich des Datenschutzes bietet die UIMC Ihnen die unterschiedlichsten Lösungen an. Diese sind sowohl im Hinblick auf die Größe der Unternehmung, der Branche etc. als auch im Hinblick auf Ihre Wünsche angepasst.

Die UIMC hat sich u. a. darauf spezialisiert, mit Hilfe einer kompetenten Beratung, rationalisierenden Hilfsmitteln und durchdachten/praxiserfahrenen Konzepten den gesetzlichen Datenschutz in verschiedenartigen Institutionen zu gewährleisten. Sofern es gewünscht ist, bieten wir eine Betreuung von A bis Z aus einer Hand: Von der

Ausbildung der Mitarbeiter oder des internen DSB durch

- eLearning-Lösungen (z. B. das *eUIMCollege*),
- klassische Schulungen und Seminare sowie
- Coaching des intern bestellten Datenschutzbeauftragten; die

Begutachtung der aktuellen Situation mit Hilfe eines Schwachstellen-Analyse-Tools,

Computergestützte Führung des Verfahrensverzeichnisses,

Datenschutz-Handbuchs bis hin zur Übernahme aller Aufgaben als

Externer Datenschutzbeauftragter;

des Weiteren bieten wir ein an die

KMU-spezifischen Anforderungen angepasstes sog. Low-Budget-Konzept, welches auch zur einheitlichen Umsetzung des Datenschutzes in Konzernen/bei Tochterunternehmen eingesetzt werden kann,

bis hin zur

Zertifizierungsvorbereitung.

Suche eines Datenschutzbeauftragten

„Grundsätzlich ist die Möglichkeit für die Bestellung externer Beauftragter [...] oft eine praktikable Lösung, da sie [die Unternehmen] häufig selbst nicht über Personal verfügen, das die für Datenschutzbeauftragte erforderliche fachliche Eignung hat. Hier kann eine externe Person, die mehrere ähnlich strukturierte Unternehmen betreut, kostengünstiger und fachlich qualifizierter arbeiten.“ Ferner gehen Sie durch die externe Bestellung der Tatsache aus dem Weg, dass ein intern bestellter Datenschutzbeauftragter nahezu unkündbar wird.

[Landesbeauftragte für Datenschutz und Informationsfreiheit NRW;17. Datenschutzbericht]

Consultants, College und Certification

Ein starkes Team bei Datenschutz und IT-Sicherheit

UIMC® Die UIMC Dr. Vossbein GmbH & Co KG wurde 1997 gegründet und hat die damals schon seit über 10 Jahren laufenden Beratungsgeschäfte der Partner und Gesellschafter Prof. Dr. Reinhard Voßbein, Professor für Wirtschaftsinformatik, und Dr. Jörn Voßbein in eine Beratungsgesellschaft eingebracht. Seit 1999 ist Dr. Heiko Haaz, der schwerpunktmäßig den Datenschutz betreut, als dritter Partner zur UIMC gestoßen.

Kerngebiete unserer Arbeit sind die IT-Sicherheit/Informationssicherheit und der Datenschutz. Insbesondere auf dem Gebiet des Datenschutzes sind unsere Erfahrungen branchenführend. Unser Leistungsspektrum/Produktprogramm unterscheidet sich schon seit jeher von dem anderer Beratungsunternehmen: Wir setzen ein toolgestütztes Analyse- und Konzeptionierungssystem mit einer wissensbasierten Expertensystem-Komponente in Form einer Shell ein, das ständig ausgebaut und ergänzt wird. Dieses ermöglicht die rationelle und kostengünstige Analyse betriebswirtschaftlicher sowie IT-sicherheits- und datenschutzspezifischer Kern- und Teilgebiete sowie die Berichterstattung und Konzeptionserstellung, womit Rationalisierungs- und Effizienzvorteile für unsere Kunden generiert werden.

UIMCollege® Wir führen Workshops für Führungskräfte, Schulungen für Mitarbeiter sowie Aus-, Fort- und Weiterbildungsmaßnahmen für Fachkräfte auf den Sektoren IT-Sicherheit und Datenschutz als UIMCollege-Seminar oder als Inhouse-Veranstaltungen durch. Diese Erfahrungen und Kenntnisse haben wir nun auch in ein **eCollege** überführt, so dass unabhängig von Ort und Zeit das Wissen vermittelt und entsprechend sensibilisiert werden kann.

UIMCert® GmbH Die UIMCert GmbH ist eine Schwestergesellschaft der UIMC Dr. Vossbein GmbH & Co KG. Gesellschafter der UIMCert sind die UIMC Dr. Vossbein Betriebs-GmbH und Dr. Heiko Haaz. Wir haben einen unabhängigen Ausschuss, der die Geschäftsführung in wichtigen Fragen im Bereich IT-Management, IT-Sicherheit sowie Datenschutz und Zertifizierung berät.

Wir verfügen über qualifiziertes Personal für die Auditierung und Zertifizierung in den genannten Bereichen. Wir sind bei der **DAkkS** für den Standard ISO 27001 und beim Unabhängigen Landeszentrum für den Datenschutz (**ULD**) für Datenschutzauditierung (für Recht und Technik) akkreditiert. Wir haben darüber hinaus eigene Prüfsysteme für IT-Sicherheit und Datenschutz (datenverarbeitende Stellen und Produkte) entwickelt, innerhalb derer wir nach erfolgreicher Auditierung gemäß prüfbaren standardisierten Normen ein **eingetragenes Gütesiegel** verleihen.

Durch die Verbindung mit der UIMC stehen uns die von der UIMC entwickelten Tools zur Verfügung, die eine hohe Effizienz durch das computerisierte Arbeiten

Referenzen

Wir können beachtliche Referenzen von Institutionen aus einer Vielzahl von Wirtschaftszweigen sowie Behörden aufweisen und haben eine umfangreiche Projekt- und Betreuungserfahrung, auch international. Kerngebiete unserer Arbeit sind die IT-Sicherheit und der Datenschutz: Felder, auf denen unsere Erfahrungen branchenführend sind.

Unternehmens- und Informations-Management Certification

UIMCert® GmbH

Gütesiegel

Die **UIMCert-Unternehmens- und Informations-Management Certification** bestätigt hiermit die ordnungsgemäße Erfüllung der Anforderungen der Datenschutzgesetzgebung durch das Datenschutzmanagement-System der

Max Mustermann GmbH
Musterstr. 12
1000 Musterstadt

gem. Prüfstandard: **UIMCert PS 101**

Das Zertifikat ist gültig bis: 30. August 2014

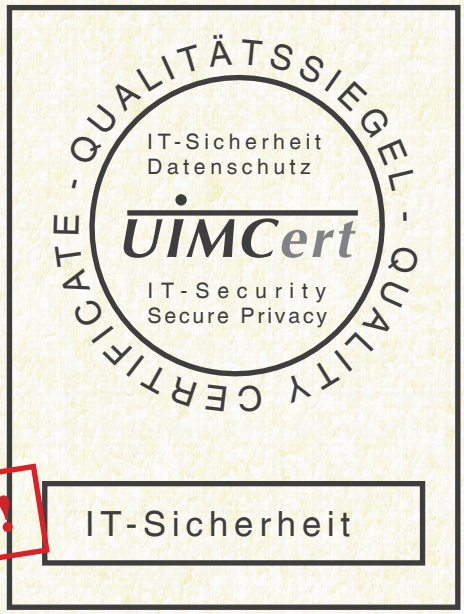
Geltungsbereich:
Servicesystem Cloud Computing

Auditnummer: F-127-01

Revisionsnummer: REV01

UIMCert GmbH - Moltkestr. 19 - 42115 Wuppertal

WUPPERTAL, 01. September 2011



LEITER ZERTIFIZIERUNGSSTELLE

AUDITLEITER