UIMC®
DR. VOSSBEIN
GMBH & CO KG

Unternehmens- und Informations-
Management Consultants

# Das UIMC IT-Sicherheits- und Datenschutzhandbuch

Reduzierung der Risiken
beim Einsatz von IT-Systemen
auf ein tragbares Maß

sowie

Gewährleistung des
gesetzlichen Datenschutzes

durch angemessene Maßnahmen

**Inhalt**

# A DIE AUSGANGSSITUTATION

## 1 Ziele der IT-Sicherheit

Die Risiken, die beim Einsatz von IT-Systemen in Institutionen vorhanden sind, müssen durch angemessene Maßnahmen auf ein tragbares Maß reduziert werden. Die Ursachen für Sicherheitsbedürfnisse in Institutionen beruhen auf internen und externen Abhängigkeiten von Personen bzw. -gruppen.

Bei den Sicherheitsbedürfnissen in Unternehmen geht es um die Realisierung der **drei Sicherheitsziele:**

- Integrität der Daten/IT-Programme
- Verfügbarkeit von Daten/IT-Programmen
- Vertraulichkeit der Daten/IT-Programme

Unter *Integrität* ist die Sicherung der Unversehrtheit der Daten und der Programme vor Fälschung, Vernichtung und Änderung zu verstehen. Dahinter verbirgt sich die Forderung, dass Informationen nur durch Befugte in der vorgesehenen Art bearbeitet werden dürfen. Hierbei bedeutet „vorgesehene Art", dass diese Bearbeitung für die Aufgabenerfüllung notwendig ist und korrekt durchgeführt wird.

Die *Verfügbarkeit* zielt darauf ab, die Funktionsfähigkeit von Daten und IT-Programmen gemäß Zielsetzung zu sichern. Das bezieht sich auf die Erbringung der Dienstleistung einer Anwendung in der vorgesehenen Zeit. Somit sind in der Verfügbarkeit z. B. auch die Forderung nach akzeptablen Antwortzeiten und der Zugang zu Hardware, die zu nutzen der Mitarbeiter berechtigt ist, enthalten.

*Vertraulichkeit* heißt, dass Daten und IT-Programme vor unbefugter Kenntnisnahme/Einsichtnahme und Gebrauch zu schützen sind. Das entspricht der Forderung, dass nur Berechtigte Zugang zu den für sie relevanten Informationen erhalten dürfen.

## 2 Ziele im Datenschutz

Die Ursachen für o. g. Sicherheitsbedürfnisse in Institutionen beruhen zum einen auf den o. g. Abhängigkeiten von Personen bzw. -gruppen und zum anderen auf gesetzlichen Vorschriften aus dem Datenschutz; insbesondere wenn personenbezogene Daten verarbeitet werden, wird dieser Schutz ausdrücklich durch das Datenschutzgesetz gefordert.

Die gesetzliche Ausgestaltung des Datenschutzes im BDSG, in den Landesdatenschutzgesetzen und in anderen bereichsspezifischen Gesetzen (GDSG NW, Tele-Gesetze etc.) verfolgt das Ziel, die Wahrung der Persönlichkeitsrechte des Einzelnen sicherzustellen. Dies kann nur wirksam geschehen, wenn der Datenschutz fester Bestandteil der Organisation des Unternehmens ist, und wenn die Mitarbeiter aller Hierarchieebenen über ihre Datenschutzpflichten und -verantwortungen aufgeklärt und in eine entsprechend ausgerichtete Organisation eingebunden werden.

# B DAS UIMC IT-SICHERHEITS- UND DATENSCHUTZHANDBUCH

## 1 Die Einsatzformen

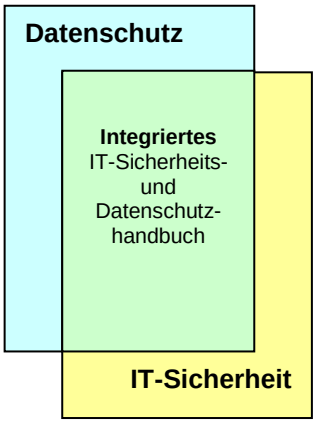
Neben den **Einzellösungen** in Form eines

- Handbuchs zur Reduzierung der Risiken beim Betrieb von IT-Systemen und eines
- Handbuchs zur Gewährleistung des gesetzlichen Datenschutzes

kann/sollte diese Lösung – aufgrund der großen Nähe der beiden Gebiete IT-Sicherheit und Datenschutz – sinnvollerweise auch in Form eines

- **integrierten** IT-Sicherheits- und Datenschutzhandbuchs

eingesetzt werden.




Das UIMC IT-Sicherheits- und Datenschutzhandbuch ist modular aufgebaut. Daher ist es an jedes Unternehmen spezifisch anpassbar. Darüber hinaus existieren unterschiedliche Versionen des Handbuchs, je nach Größe des Unternehmens, der Bedeutung/Sensitivität der Daten sowie der Abhängigkeit vom IT-System.

Nachfolgende Ausführungen beziehen sich auf das integrierte IT-Sicherheits- und Datenschutzhandbuch und zeigen dementsprechend Inhalte beider Bereiche auf.

## 2 Die Zielsetzungen

Die übergeordneten Ziele des UIMC IT-Sicherheits- und Datenschutzhandbuchs sind generell die Unterstützung der Schaffung von Informationssicherheit, Gewährleistung des Datenschutzes sowie die Dokumentation aller diesbezüglichen Entscheidungen.

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

- Gestaltungs-/Organisationsmittel
- Mittel zur Schaffung von Transparenz der organisatorischen Tatbestände
- Informationsquelle
- Führungsinstrument für Vorgesetzte

Darüber hinaus dient das UIMC IT-Sicherheits- und Datenschutzhandbuch den einzelnen Mitarbeitern zur Realisierung von Sicherheit und Datenschutz an ihrem Arbeitsplatz und ist demnach:

- Kontrollgrundlage für Vorgesetzte sowie
- Hilfe für Mitarbeiter bei ihrer Arbeit sowie bei der Beantwortung von Zweifelsfragen,
- Bezugspunkt für das gesamte Problem der IT-Sicherheit und des Datenschutzes bei der täglichen Arbeit auf allen Ebenen und an allen Stellen.

## 3 ISO 27001 als Grundlage

In das UIMC IT-Sicherheits- und Datenschutzhandbuch sind die in der IT-Sicherheitsnorm ISO 27001 geforderten aufbau- und ablauforganisatorischen Maßnahmen eingebracht worden. Diese Norm hat

sich als sog. „code of practise“ zu einem Standard in der IT-Sicherheit etabliert. Sie weist eine hohe Praktikabilität auf.

Durch die Berücksichtigung der Norm innerhalb des UIMC IT-Sicherheits- und Datenschutzhandbuchs wird der einsetzenden Institution eine exzellente Vorbereitung auf eine mögliche Auditierung, Testierung oder Zertifizierung. Es kann als Prüfungsgrundlage bei einer möglichen Zertifizierung gemäß ISO/IEC 27001 – oder einer anderen Norm – dienen, welche schriftliche Dokumentationen aller relevanten Regelungen verlangt.

## 4 Die Funktionen

Das UIMC IT-Sicherheits- und Datenschutzhandbuch ist ein Instrument, mit dessen Hilfe die auf der Basis einer Konzeption entwickelten IT-Sicherheits- und Datenschutzziele sowie die aufbau- und ablauforganisatorischen Maßnahmen den Vorgesetzten und Mitarbeitern übermittelt werden sollen. Es ist ein Instrument, das dazu dient, einen reibungslosen Informationsverarbeitungsbetrieb zu schaffen und zu erhalten und ist somit Informationsquelle und Nachschlagewerk für alle Mitarbeiter.

Das UIMC IT-Sicherheits- und Datenschutzhandbuch beinhaltet eine Zusammenstellung bzw. Dokumentation aller für das Gebiet Sicherheit der Informationsverarbeitung und des Datenschutzes erlassenen und gültigen organisatorischen Regeln. Die konkreten Anweisungen für Stelleninhaber in der Mitarbeiter- und Vorgesetztenfunktion gehen aus den Regelungen/Richtlinien hervor.

In seiner Funktion, Hilfe für die Mitarbeiter auf allen Ebenen und Stellen zu bieten, dient es im Wesentlichen als Informationsquelle und Nachschlagewerk. Gleichzeitig hat das UIMC IT-Sicherheits- und Datenschutzhandbuch bei der Einarbeitung und Schulung neuer Mitarbeiter eine besondere Bedeutung.

Die Gesamtheit der enthaltenen organisatorischen Regelungen hat verbindlichen Charakter. Das UIMC IT-Sicherheits- und Datenschutzhandbuch gilt für alle Mitarbeiter des Unternehmens ohne Ausnahmen. Hierfür wird festgelegt, welche organisatorischen Regelungen für welche Arbeitsplätze verbindlich sind.

Darüber hinaus sind die Vorschriften auch für externe Mitarbeiter – soweit anwendbar – gültig. Des Weiteren können Teile des UIMC IT-Sicherheits- und Datenschutzhandbuchs zu Vertragsinhalten mit IT-Dienstleistern gemacht werden, um auch hier den Sicherheitsstandard des Unternehmens sicherzustellen.

Somit können folgende Funktionen zusammengefasst werden:

*Informationsfunktion*

Die Informationsfunktion hat zusätzlich zu ihrer generellen noch eine spezielle Bedeutung, die sich aus der Einarbeitung und Schulung von neuen Mitarbeitern oder beim Arbeitsplatzwechsel ergibt. Des Weiteren ist die Informationsfunktion für die interne Revision sowie Organisationsprüfungen von Bedeutung und ist besonders wichtig für „berechtigte Außenstehende“. Hierzu zählen Prüfer von Konzern-Muttergesellschaften, Wirtschaftsprüfer oder Aufsichtsgremien.

*Dokumentationsfunktion*

Diese Funktion dient in erster Linie der Charakterisierung des aktuellen Zustandes der organisatorischen Regelungen. So lässt sich auch eine historisch wachsende und

gewachsene Dokumentation auf der Basis der entwickelten, aber nicht mehr in Kraft befindlichen Regelungen des UIMC IT-Sicherheits- und Datenschutzhandbuch ablesen. Daher bietet sich die Form der Dokumentation auf einem elektronischen Datenträger an.

*Regelungsfunktion*

Durch die im UIMC IT-Sicherheits- und Datenschutzhandbuch enthaltenen Regelungen und Richtlinien wird im aufbauorganisatorischen Bereich die Klarheit des Delegationsprinzips durch Festlegung der Aufgaben von Mitarbeitern und Vorgesetzten sowie diesen Aufgaben zuzuordnenden Verantwortungsbereichen und den übertragenen Kompetenzen geregelt. Das Gleiche gilt für die ablauforganisatorischen Regelungen, bei denen nicht nur sicherheitsrelevante Regelungsprozesse aufzuführen sind, sondern vor allem auch diejenigen mit der Fachaufgabe eines Mitarbeiters zusammenhängenden Aufgaben, die Sicherheitsprobleme hervorrufen können.

*Anweisungsfunktionen*

Die Anweisungen für Stellen/Arbeitsplätze in Mitarbeiter- und/oder Vorgesetztenfunktion gehen aus den Regelungen und Richtlinien hervor. Sie sollten im Regelfall aber zu Bestandteilen von Stellen- und/oder Funktionsbeschreibungen werden und demnach entweder in den Stellenbeschreibungen oder in einem Zusatz zu ihnen niedergelegt werden.

## 5 Der Aufbau: Allgemeiner und Formularteil

Das UIMC IT-Sicherheits- und Datenschutzhandbuch ist in 2 Hauptteile untergliedert: Einen sog. „Allgemeinen Teil“ und einem „Formularteil“. Der „Allgemeine Teil“ beinhaltet alle unternehmensweit gültigen Regelungen, Vorgaben etc. im Rahmen der IT-Sicherheit und des Datenschutzes. Zur vereinfachten Umsetzung der Regelungen wurden Formulare (wie beispielsweise Stellenbeschreibungen, Checklisten, Musterverträge oder Verpflichtungserklärungen) erstellt, die jedoch erfahrungsgemäß einer höheren Änderungshäufigkeit unterliegen. Aus diesem sowie aus Gründen der Übersichtlichkeit, werden diese Formulare mit einem Hinweis in den Formularteil ausgegliedert.

Der Formularteil stellt eine Konkretisierung zur Benennung spezieller Aspekte dar. Dies wird durch das Einfügen von Listen, Formularen und Diagrammen zur schnellen und übersichtlichen Verfahrensidentifizierung erreicht. Der Formularteil stellt eine Unterstützungshilfe zur Umsetzung der Verfahren und Maßnahmen dar. Die Gliederung ist analog der Gliederung des Handbuchs.

## 6 Die Grobstruktur

| | | |
|---|---|---|
| **I.** | **Allgemeiner Teil** | |
| | 1 | Einleitung |
| | 2 | Strukturorganistorische Richtlinien |
| | 3 | Übergreifende Richtlinien |
| | 4 | Verwaltung des IT-Systems |
| | 5 | Berechtigungsorientierte Sicherheitsmaßnahmen |
| | 6 | Arbeitsplatzorientierte Sicherheitsmaßnahmen |
| | 7 | Kommunikationsspezifische Richtlinie |
| | 8 | Richtlinien für Notfall-, Katastrophen- und Wiederanlaufplanung |
| | 9 | Allgemeine datenschutzrelevante Richtlinien für Mitarbeiter |
| | 10 | Spezielle datenschutzrelevante Richtlinien |
| | 11 | Gesetzesspezifische Richtlinien |
| | 12 | Vertragsspezifische Richtlinien |
| | 13 | Prüfungsnormen und -vorgaben |
| | 14 | Formale Richtlinien |
| **II.** | **Formularteil** | |

| Die Gliederung ist analog zu der o. g. im Allgemeinen Teil. |
|---|

## 7 Die Inhalte

*1. Einleitung*

Es werden neben den Zielen der IT-Sicherheit und des Datenschutzes auch die Zielsetzungen eines solchen Handbuches definiert. Des Weiteren ist der Geltungsbereich des Handbuches in dem jeweiligen Unternehmen beschrieben.

*2. Strukturorganisatorische Richtlinien*

Es wird ein Überblick über die Funktionsträger der Bereiche IT-Sicherheit und Datenschutz gegeben. Die Funktion der IT-Sicherheits- und Datenschutzbeauftragten wird dabei genau erläutert. Es werden ihre Kompetenzen, Verantwortungen und ihre organisatorische Eingliederung beschrieben. Neben den Beauftragten sind die dezentralen Repräsentanten weitere Funktionsträger der IT-Sicherheit und des Datenschutzes.

*3. Übergreifende Richtlinien*

Neben allgemeinen Sicherheitsrichtlinien, beispielsweise zur Erreichung von Hard- und Softwaresicherheit, werden Vorgaben zur Einstufung von Informationen in Klassifikationsklassen gemacht. Des Weiteren werden Sensibilisierungs- und Schulungsmaßnahmen im Rahmen der IT-Sicherheit und des Datenschutzes geregelt. Darüber hinaus werden in einer Personalrichtlinie Vorgaben für die Personalverwaltung und zur Personalführung gegeben. Hierbei werden beispielsweise sicherheits- und datenschutzrelevante Aufgaben bei der Einstellung neuer Mitarbeiter oder datenschutzrelevante Pflichten von Vorgesetzten aufgezeigt.

*4. Verwaltung des IT-Systems*

Innerhalb dieses Kapitels werden Vorgaben im Zusammenhang mit der Verwaltung des IT-Systems gegeben. Von der Beschaffung über die Wartung, der Handhabung von externen Datenträgern und der Datensicherung bis zur Archivierung und Vernichtung von Daten wird „alles“ innerhalb dieses Kapitels geregelt.

*5. Berechtigungsorientierte Sicherheitsmaßnahmen*

Kernbereich dieses Kapitels sind die Forderungen nach Zutritts-, Zugangs- und Zugriffskontrollen. Es werden beispielsweise Vorgaben zur Rechtevergabe, zur Passwortorganisation oder auch zum Zugang in Sicherheitszonen gegeben. Des Weiteren werden Forderungen zur Verschlüsselung, zur Protokollierung und auch an den Zugang von Fremdunternehmen an das Unternehmen gestellt.

*6. Arbeitsplatzorientierte Sicherheitsmaßnahmen*

Dieses Kapitel wird den unterschiedlichen Anforderungen verschiedener Arbeitsplatzformen gerecht. Es werden entsprechende Vorgaben an die Gestaltung von PC-Arbeitsplätzen sowie an mobile PC und an Telearbeit gegeben.

*7. Kommunikationsspezifische Richtlinien*

Innerhalb dieses Kapitels wird neben der Zulässigkeit der Weitergabe von personenbezogenen und anderen sensitiven Daten an interne und externe Empfänger auch Vorgaben an die Gestaltung und Nutzung der verschiedenen Kommunikationsmedien wie Telefon, Telefax, E-Mail etc. gegeben.

*8. Richtlinien für Notfall-, Katastrophen- und Wiederanlaufplanung*

Dieses Kapitel befasst sich neben den Regelungen für die Notfall- und Wiederanlaufplanung auch mit dem Verhalten im Katastrophenfall sowie in anderen Sicherheitsvorfällen und Störungen.

*9. Allgemeine datenschutzrelevante Richtlinien für Mitarbeiter*

In diesem Kapitel werden Vorgaben an die Gewährleistung der Rechte der Betroffenen gemacht. Des Weiteren werden Regelungen zu Verpflichtungserklärungen gegeben.

*10. Spezielle datenschutzrelevante Richtlinien*

Kern dieses Kapitels sind Sonderformen der Datenverarbeitung gemäß Datenschutzgesetze, wie beispielsweise Auftragsdatenverarbeitung, automatisiertes Abrufverfahren oder der Videoüberwachung. Auch wird das Erstellen von Verfahrensübersichten/-Verzeichnissen beschrieben und Vorgaben an den Einsatz von mobilen Speicher- und Verarbeitungsmedien gemacht.

*11. Gesetzesspezifische Richtlinien*

Dieses Kapitel wird den Datenschutzanforderungen verschiedener spezieller Gesetze gerecht. Hierbei sind beispielhaft die Telegesetze und das Signaturgesetz zu nennen.

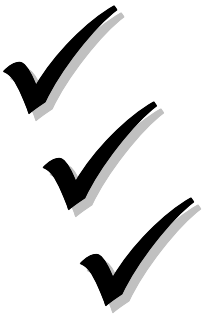
*12. Vertragsspezifische Richtlinien*

Innerhalb dieses Kapitels werden u. a. datenschutzrelevante Inhalte vorgegeben, die in Verträgen mit beispielsweise Wartungsdienstleistern oder anderen Auftragsdatenverarbeitern berücksichtigt werden müssen.

*13. Prüfnormen und -vorgaben*

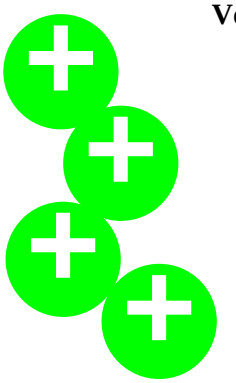
Durch die Berücksichtigung von Prüfnormen wie der ISO 9000 ff wird es ermöglicht, geeignete Softwareprodukte auszuwählen. Innerhalb dieses Kapitels sind die aus den Normen resultierenden Anforderungen formuliert. Darüber hinaus wird auch auf ein fachliches Pflichtenheft eingegangen und Regelungen für die interne Revision getroffen.

## C VORTEILE UND IHR NUTZEN



**Kerninhalte**:

- Einzeln für IT-Sicherheit und Datenschutz sowie als integrierte Lösung erhältlich
- unternehmensspezifisch anpassbar
- Orientierung an der internationalen Norm ISO 27001
- Berücksichtigung relevanter Gesetze
- Gestaltungs-/Organisationsmittel mit verbindlichen Richtlinien sowie Informationsquelle und Nachschlagewerk in einem



**Vorteile/Pluspunkte**:

- Umfassendes Regelwerk
- Transparenz der Regelungen
- allgemein verbindlich geltende Regelungen und Führungsinstrument
- Berücksichtigung der ISO 27001 über das UIMC IT-Sicherheits- und Datenschutzhandbuch hinaus
- Bewährung durch langjährige Praxiserfahrungen der UIMC
- Übersichtlichkeit durch Unterteilung in allgemeinen Regelungs- und Formularteil
- Abgestimmtheit mit anderen Hilfsmitteln der UIMC, wie z. B. Schwachstellenanalyse

**Nutzen:**

- Gesetzeskonformität
- Verbesserung der IT-Sicherheit- und Datenschutzsituation
- Praxisgerechte Umsetzung der IT-Sicherheit und des Datenschutzes
- Kostengünstigkeit im Vergleich zur eigenständigen Erstellung eines Regelwerks
- Effiziente Zertifizierungsvorbereitung

## D DIE UIMC – EIN KURZPORTRÄT

Die UIMC Dr. Vossbein GmbH & Co KG wurde 1997 gegründet, um die seit ca. über 10 Jahren laufende, bis dahin im Rahmen einer freien Beratung und BGB-Gesellschaft abgewickelten Beratungsgeschäfte in eine Unternehmensform zu bringen. Der Seniorpartner und Gesellschafter Prof. Dr. Reinhard Voßbein, Professor für Wirtschaftsinformatik und langjähriger Vorstand der Gesellschaft für Datenschutz und Datensicherung (GDD), gründete zusammen mit Dr. Jörn Voßbein die UIMC.

Das Unternehmen hat eine beachtliche Referenzliste aus einer Vielzahl von Wirtschaftszweigen und eine umfangreiche Projekterfahrung in Beratungs-, Datenschutz- und IT-Sicherheitsprojekten. Seit 1999 ist Dr. Heiko Haaz, der schwerpunktmäßig das Gebiet des Datenschutzes betreut, als dritter Partner zum Unternehmen dazugestoßen.

Die Besonderheit des Produktprogramms der Gesellschaft: Schon vor 10 Jahren wurde ein toolgestütztes Analyse- und Konzeptionierungssystem in Form einer Shell entwickelt, das ständig ausgebaut und ergänzt wird. Dieses ermöglicht die rationelle und kostengünstige Analyse betriebswirtschaftlicher Kern- und Teilgebiete sowie die toolgestützte Auswertung und Konzeptionserstellung. Ein wissensbasiertes – expertensystemähnliches – auf den Erfahrungen in der Unternehmensführung einerseits und den Lösungen der Informatik andererseits basierendes System, ist teilrealisiert. Im Verlaufe der Zeit wurden eine Vielzahl von individuellen Füllungen für diese Shell erarbeitet und in diese eingebracht. Firmenindividuelle Füllungen sind konzeptionell vorgesehen und auf der Basis der Struktur des Tools komplikationslos zu realisieren.

## E DIE UIMCERT – EIN KURZPORTRÄT

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; Geschäftsführer der UIMCert ist Frau Wölfel-Heymann.

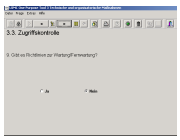
Die UIMCert hat als Schwestergesellschaft UIMC das Ziel, sich zu einem der führenden Unternehmen im Bereich IT-Sicherheitszertifizierung zu entwickeln. Die UIMCert hat einen Fachbeirat, der die Geschäftsführung in wichtigen Fachfragen im Bereich IT-Sicherheit und ihrer Zertifizierung berät. Die UIMCert verfügt über qualifiziertes Personal für die Begutachtung und Zertifizierung von IT-Sicherheitssystemen. Sie arbeitet bei Bedarf mit anderen Institutionen zur Ergänzung ihres eigenen Know Hows zusammen.

Die UIMCert auditiert IT-Sicherheitsmanagementsysteme auf der Grundlage des ISO/IEC 27001 und hat darüber hinaus ein Datenschutzauditierungssystem entwickelt. Des Weiteren ist die UIMCert beim Unabhängigen Landeszentrum für den Datenschutz (ULD) akkreditiert. Im Bereich des Datenschutzes auditiert sie datenverarbeitende Stellen und Anwendungssysteme für die Verarbeitung personenbezogener Daten. Die UIMCert führt Schulungen und Fortbildungsmaßnahmen auf den Sektoren Auditierung, Revision, Datenschutz und IT-Sicherheit durch.

Ein weiterer Aktivitätsbereich ist die Entwicklung von Lernprogrammen und -software. Die UIMCert führt wissenschaftliche Projekte, vor allem auf den Sektoren Neue Medien, E-Business und IT-Sicherheit durch. Durch die Verbindung mit der UIMC stehen der UIMCert die von der UIMC entwickelten Tools zur Verfügung, die eine hohe Effizienz durch das computerisierte Arbeiten ermöglichen.

## F WEITERE UNTERSTÜTZUNGSMÖGLICHKEITEN DER UIMC

Nachfolgend seien einige Hilfsmittel/Unterstützungsmöglichkeiten der UIMC aufgezeigt, die es ermöglichen, den IT-Sicherheits- und Datenschutzgedanken weiter systematisch im Unternehmen zu verwirklichen:

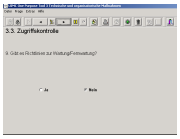


*Risiko-Analyse*

Ziel einer Risikoanalyse ist es, systematisch eine Analyse der Risiken im Unternehmen durchzuführen. Die Analyse mit Hilfe des Risktools schließt folgende Aspekte ein:

- Ermittlung des bisherigen Standes der Risikobetrachtung
- Ermittlung der Art und des Umfangs der Risikodokumentation
- Bewertung bislang noch nicht erfasster und bewerteter Risiken

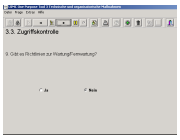
Hierfür eigenen sich insbesondere die Inhalte der ISO 27001 bzw. der Controls des entsprechenden Standards ISO/IEC 27001. Ergebnis ist ein von der UIMC erstellter Risikobericht mit Aufzeigen der Schwachstellen des Risikomanagement-Systems und mit ersten Empfehlungen zur Systemverbesserung durch projektorientierte Maßnahmen.



*Strategiekonferenz und Zielfindungsworkshop*

Strategien sind sowohl im Datenschutz als auch in der IT-Sicherheit in fast allen Institutionen ein Stiefkind des strategischen 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.

Die Konferenz wird computer- und toolgestützt 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. Hier auf sollen dann weitere Aktivitäten aufbauen.



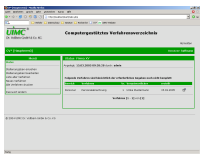
*Schwachstellenanalyse*

In der Schwachstellenanalyse wird das Unternehmen hinsichtlich des Erfüllungsgrads der Norm sowie Gesetzen und/oder den Stand der Umsetzung von Maßnahmen geprüft. Abweichungen können als Schwachstellen interpretiert werden. Die Analyse wird computer- und toolgestützt abgewickelt. Hierdurch können wesentliche Arbeits-/Ergebnisprotokolle während der Sitzung eingebracht, diskutiert und gegebenenfalls berichtigt werden. Die Ergebnisse werden durch die UIMC in einem Schwachstellenbericht und einem Maßnahmenkatalog zusammengefasst und der Institution zur Verfügung gestellt. Hier auf sollen dann weitere Aktivitäten aufbauen.

*Multimediales Lern-Tool*

Die Aus-/Weiterbildung in IT-Sicherheit und Datenschutz ist nach unseren Erfahrungen und Erhebungen (siehe KES/KPMG-Sicherheitsstudie 2002) in den Institutionen häufig weniger gut als sie es nach der Bedeutung dieses Gebietes sein sollte. Hierfür ist insbesondere der schlechte Kenntnisstand verantwortlich.

Durch das multimediale Lern-Tool wird die Durchführung von Schulungen ersetzt und die Mitarbeiter für das Thema sensibilisiert. Es wird durch Szenen aus dem beruflichen Alltag eine hohe Identifikation mit den Problemstellungen und durch das "Hintergrundwissen" eine solide Wissensvermittlung erreicht. Vor allem die Bewusstheitsschwelle im Sinne des Problembewusstseins wird durch die animierte Form der Darbietung deutlich angehoben. Im sog. „College" kann der Wissensstand abgeprüft werden.



*Computergestütztes Verfahrensverzeichnis CVV*

Dem Beauftragten für den Datenschutz ist von der verantwortlichen Stelle eine Übersicht über die in §4e BDSG genannten Angaben sowie über zugriffsberechtigte Personen zur Verfügung zu stellen.

Die UIMC hat eine computergestützte/web-basierte Lösung (CVV) erstellt, das einerseits gesetzeskonform ist und dabei andererseits einen Minimal-Arbeitsaufwand bei der verantwortlichen Stelle erfordert. Ein einmaliger Erhebungsprozess enthält die zeitgleiche Führung aller geforderten Verzeichnisse. Ist im Unternehmen ein Datenschutz-Handbuch vorhanden, das die erforderlichen technischen und organisatorischen Maßnahmen berücksichtigt, beschränkt sich der Aufwand zum Führen des Verfahrensverzeichnisses auf ein Minimum. Das CVV zeichnet sich hierbei durch ein flexible erhebungsabhängige Benutzerführung aus.

*Externe Datenschutzbeauftragung*

Einen Mitarbeiter für die Funktion des Datenschutzbeauftragten zu finden, der dann als Mitarbeiter in seiner Funktion unkündbar wird, ist nicht leicht. Im Hinblick auf die entstehenden Kosten für Schulung und Fortbildung, die auf seine Person entfallenden Personal- und Sachkosten sowie seinen Ausfall bei anderen Funktionen ist es oft eine Wirtschaftlichkeitsfrage, ob nicht die Beauftragung eines externen Datenschutzbeauftragten die wirtschaftlichere und effizientere Lösung darstellt.

Hiervon sind die meisten Arbeiten in einem Datenschutzbeauftragungs- oder -beratungsvertrag pauschalisierbar, andere werden nach Zeitaufwand abgerechnet. Ein besonderer Vorteil der externen Datenschutzbeauftragung liegt darin, dass wir ebenfalls auf dem Gebiet der IT-Sicherheit eine hohe Kompetenz aufweisen und damit Datenschutzkonzeptionen grundsätzlich als integrierten Bestandteil von IV-Sicherheitskonzeptionen sehen.

Bettina Sokol, Landesbeauftragte für Datenschutz und Informationsfreiheit NRW formulierte es in ihrem 17. Datenschutzberichts wie folgt: „Grundsätzlich ist die Möglichkeit für die Bestellung externer Beauftragter ... oft eine praktikablere Lösung, da sie 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."

*Coaching/Beratung*

Um den Anforderungen des Datenschutzgesetzes an die Person des internen Datenschutzbeauftragten und an die zu erfüllenden Aufgaben gerecht zu werden, kann es sinnvoll sein, zur fachlichen Unterstützung des internen Datenschutzbeauftragten einen Fachmann der UIMC als Coacher bzw. Berater einzusetzen.

Vorteile des Coachings bzw. der Beratung des intern bestellten Datenschutzbeauftragten ist die hohe Fachkunde, die Praxiserfahrung auch auf anderen Randgebieten, Synergien aus Coachingprojekten und Mehrfachbestellung in anderen Unternehmen sowie die Kalkulierbarkeit der Kosten für das Unternehmen.

*Notfallhandbuch*

Das Notfallhandbuch beinhaltet ein Konzept zur Gewährleistung, dass bei Auftreten eines Notfalls Anforderungen an die IT mit einem Minimum an Unterbrechung des Services/der Qualität zufrieden gestellt werden können.

Es wird eine optimale Handlungsabfolge und Verhaltensweise im Rahmen der Stresssituation „Notfall“ durch übersichtliche Diagramme, Listen, Schaubilder gewährleistet. Das Notfallhandbuch stellt eine vollständige Abarbeitung relevanter Tätigkeiten im Notfall und im Rahmen der Dokumentation desselben sowie dessen Nachbearbeitung durch Checklisten sicher.