

## IT-Sicherheitsmanagement mit SAVE®

### Überblick

Mit der IT-Sicherheitsdatenbank **SAVE®** der INFODAS GmbH, Köln, steht jedem Anwender des IT-Grundschutz-Handbuchs des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ein leistungsfähiges Werkzeug zur Unterstützung des gesamten IT-Grundschutz-Prozesses zur Verfügung.

„Die aktuelle Version der IT-Sicherheitsdatenbank **SAVE®** ist die konsequente Weiterentwicklung früherer **SAVE®**-Versionen und bildet die aktuellen IT-Grundschutz-Kataloge gemäß der BSI-Standards 100-1 und 100-2 vollständig ab. **SAVE®** wird als innovatives Werkzeug zur Implementierung unternehmensweiter IT-Sicherheitsprozesse entsprechend den Anforderungen des Marktes und der Kunden weiter entwickelt. Durch die Integration der BSI-Standards 100-1, 100-2 und 100-3 sowie des Prüfschemas unterstützt **SAVE®** eine praxis- und ergebnisorientierte Arbeit mit dem Grundschutz und fördert die ISO 27001 Zertifizierung.“ betont Frank Reiländer, Leiter IT-Security der INFODAS GmbH, selbst lizenzierter ISO 27001-Auditor.

Alle Aufgaben im Rahmen der Erstellung und der Pflege einer Sicherheitskonzeption für einen beliebig komplex strukturierten IT-Verbund sind im Werkzeug abgebildet. Die kundenspezifische IT-Landschaft kann flexibel über das Schichtenmodell des IT-Grundschutzes hinaus mittels Szenarien modelliert werden, organisatorische und geografische sowie technische Aspekte fließen in die Modellierung mit ein. Das flexibel anpassbare Rollen- und Rechtemodell sowie die Netzwerkfähigkeit von **SAVE®** ermöglichen einen verteilten und konsistenten behörden- bzw. unternehmensweiten Einsatz des Tools.

Die Ergänzende Risikoanalyse nach BSI Standard 100-3 unterstützt **SAVE®** vollständig. Dies umfasst u.a. umfangreiche Funktionen zur Erzeugung von Risikodefinitionen aus Gefährdungen. Eine grafische Aufbereitung verdeutlicht jederzeit die Risikoabdeckung anhand des erreichten Umsetzungsstatus aller Maßnahmen. Mit einem Plan-Do-Check-Act-Vorgehen werden jederzeit die Fälligkeit und Verantwortlichkeit für die Maßnahmenumsetzung überwacht und eine permanente Kostenkontrolle gewährleistet.

Die Implementierung einer offenen Architektur sowie eines offenen und redundanzarmen Datenmodells dient als Basis für weitere Funktionen und Zusatzmodule, die auf dem IT-Grundschutz aufsetzen. Dies umfasst beispielsweise den Modul Datenschutz zur integrierten Berücksichtigung von Datenschutzaspekten oder den Modul für die Umsetzung der ZDV 54/100, die als verbindliche Grundlage für IT-Sicherheitskonzepte der Bundeswehr gilt. Darüber hinaus können weitere kunden- oder projektspezifische Kriterienkataloge flexibel angebunden werden.

Der Einsatz von **SAVE®** bringt bei einem Zertifikats-Audit weitere Vorteile, da durch Audit-Funktionen die Ergebnisse eines Basis-Sicherheitschecks mit den Ergebnissen eines Zertifikats-Audits direkt verglichen werden können und der geforderte spezifische Audit-Bericht generiert werden kann.

Aus der Datenbank heraus lassen sich mittels Browser oder MS Word jederzeit sämtliche Texte der aktuellen Grundschutz-Kataloge aufrufen, die auf der **SAVE®** Installations-CD bereits mitgeliefert werden.

Das offene und redundanzarme **SAVE®**-Datenmodell stellt sicher, dass auch bei neuen Versionen der Grundschutz-Kataloge kundenspezifische Daten und Szenarien erhalten bleiben und weiter gepflegt werden können. **SAVE®** enthält umfangreiche automatische Hilfen zur Datenübernahme aus vorherigen Versionen sowie dem *GSTOOL®*.

Die **SAVE® Application Services** bieten als **SAVE®**-Produktfamilie einander ergänzende Module für die erforderliche werkzeuggestützte Durchführung an.

#### **SAVE® Grundschutz**

Vollständige und konsistente Umsetzung des aktuellen IT-Grundschutzes gemäß den BSI-Standards mit allen Bausteinen und Maßnahmen für eine umfassende Sicherheitsanalyse und zur Erstellung eines IT-Sicherheitskonzepts.

#### **SAVE® Datenschutz**

Bewertung und Auditierung der Datenschutzorganisation gemäß BDSG oder Landesdatenschutzgesetzgebung. Die Datensicherheitsaspekte können hierbei auf die bereits erfolgte Sicherheitsanalyse mit **SAVE®** Grundschutz abgebildet werden.

Das Werkzeug kann in seinem vollen Funktionsumfang mit einer zeitlich begrenzten Lizenz getestet werden (Download unter <http://www.infodas.de/it-security/save-testversion.html>).



## Fachliche Leistungsmerkmale

Die IT-Sicherheitsdatenbank **SAVE®** bietet dem Bediener eine komfortable und leicht bedienbare Bedienoberfläche, die setzt grundlegende Kenntnisse der im IT-Grundschriftshandbuch beschriebenen Methodik für eine effiziente Nutzung voraus. Alle fachlichen Funktionen für die Erstellung eines IT-Sicherheitskonzepts mit den Arbeitsschritten Erfassung / Analyse, Schutzbedarfsfeststellung, Modellierung, Soll-Ist-Vergleich der Maßnahmenumsetzung, Ergänzende Risikoanalyse und Berichtserstellung sind hinterlegt; der Benutzer kann bei Bedarf durch einen Konzept-Assistenten geführt werden.

### IT-Strukturanalyse und Systemerfassung

Auf der Grundlage einer vorhandenen externen Systembeschreibung oder eines Netzplanes werden die IT-Systeme, Anwendungen, Räume und Kommunikationsverbindungen erfasst. Die Datenbank unterstützt die Bildung von Kategorien für eine vereinfachte strukturierte Betrachtung gleichartiger Objekte.

Zur gezielten Maßnahmenauswahl, beispielsweise aus einem Bündel substituierbarer Maßnahmen, die gleiche Bedrohungen abdecken, stellen die Analyse-Funktionen von **SAVE®** umfangreiche Querbeziehungen zwischen Bausteinen, Bedrohungen und Maßnahmen her. Des Weiteren können Veränderungen der Datenbestände (z.B. für Wiederholungsprüfungen) über Referenzkopien problemlos erfasst und dargestellt werden.

### Schutzbedarfsfeststellung

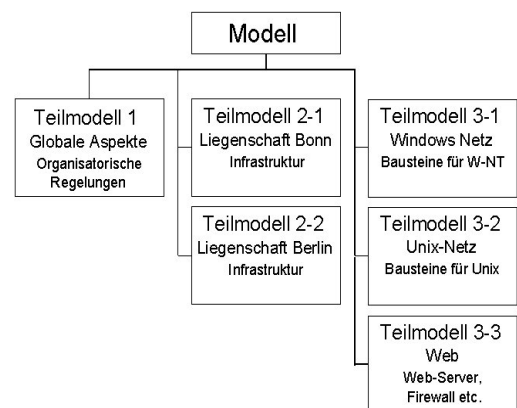
Im nächsten Schritt, oder bereits parallel zur Systemerfassung, bestimmt der Benutzer zunächst den Schutzbedarf seiner IT-Anwendungen hinsichtlich Vertraulichkeit, Verfügbarkeit, Integrität und ggf. Verbindlichkeit. Aus der Zuordnung der Anwendung zu den IT-Systemen ergibt sich der Schutzbedarf für ein spezielles IT-System oder für eine Kategorie von IT-Systemen (Vererbung). Analog erfolgt dies auch für den Schutzbedarf der Räume, der sich aus dem Schutzbedarf der ihnen jeweils zugeordneten IT-Systeme ableitet. Der Schutzbedarf der IT-Systeme wiederum fließt in die Kritikalitätsbestimmung der Kommunikationsverbindungen mit ein. Den so nach Grundschriftsmethodik berechneten Schutzbedarf kann der Benutzer übernehmen oder mit entsprechender Begründung verändern. Diese Veränderung kann jederzeit durchgeführt werden.

### Modellierung von IT-Verbänden

Der zu betrachtende IT-Verbund wird in diesem Schritt aus den Bausteinen des IT-Grundschriftshandbuchs in einem Modell nachgebildet. Die Struktur des IT-Verbunds und die erfassten Objekte werden als Modell-Daten bezeichnet.

Die Daten zu den Grundschrift-Bausteinen, mit denen die Sicherheit des zu betrachtenden IT-Verbunds oder von Teilen davon modelliert wird, werden in Teilmodellen strukturiert. Es können beliebig viele Teilmodelle gebildet und verwendet werden, um bestimmte Aspekte logisch zusammenzufassen, wobei lediglich die Einschränkung besteht, dass kein Teilmodell denselben Grundschrift-Baustein mehrfach enthalten kann. Dies führt zu einer redundanzarmen Erfassung und Speicherung der Objekte.

Die Aufteilung eines IT-Verbunds in mehrere Teilmodelle kann beispielweise unter dem Aspekt erfolgen, ob eine Gruppe von Bausteinen globale Gültigkeit besitzt, ob sie an bestimmte Liegenschaften gebunden ist oder ob unterschiedliche Zuständigkeiten bestehen und damit verschiedene Sachbearbeiter Zugriff auf die Daten des Modells benötigen.



### Soll-Ist-Vergleich (Basis-Sicherheitscheck)

Mit der Modellierung nach IT-Grundschrift ist die Basis für einen Soll-Ist-Vergleich gelegt, in dem für jede relevante Maßnahme der Umsetzungsstand (umgesetzt, teilweise umgesetzt, nicht umgesetzt, entbehrlich) ermittelt und zugeordnet wird. Zur Sicherstellung der Konsistenz der Maßnahmenumsetzung kann ein Umsetzungsstatus aus der aktuellen Maßnahme in andere Maßnahmen übertragen bzw. aus einer bereits bewerteten Maßnahme der dort ermittelte Status übernommen werden. Diese *Kopierfunktion* wird anhand systemseitiger Plausibilitäten und Konsistenzprüfungen fallweise angeboten.

Für jede Maßnahme können Kosten, Aufwand, Termine (können nach Outlook übertragen werden) und Verantwortlichkeiten zur Umsetzung eingetragen werden. Angaben zur Zertifikatsstufe und den erreichten Umsetzungsstand, in die eine Maßnahme eingeordnet ist, werden angezeigt.

Zu jeder Maßnahme sind Kontrollfragen hinterlegt, die den *Ergänzenden Kontrollfragen* der IT-Grundschrift-Kataloge entsprechen. Auch hierbei hat der Benutzer die Möglichkeit, einen Umsetzungsstatus einzutragen. Der aus den Ausprägungen je Kontrollfrage berechnete Umsetzungsstatus je Maßnahme kann durch eine eigene gewichtete Bewertung in der Datenbank



## Realisierungsplanung / Berichtserstellung

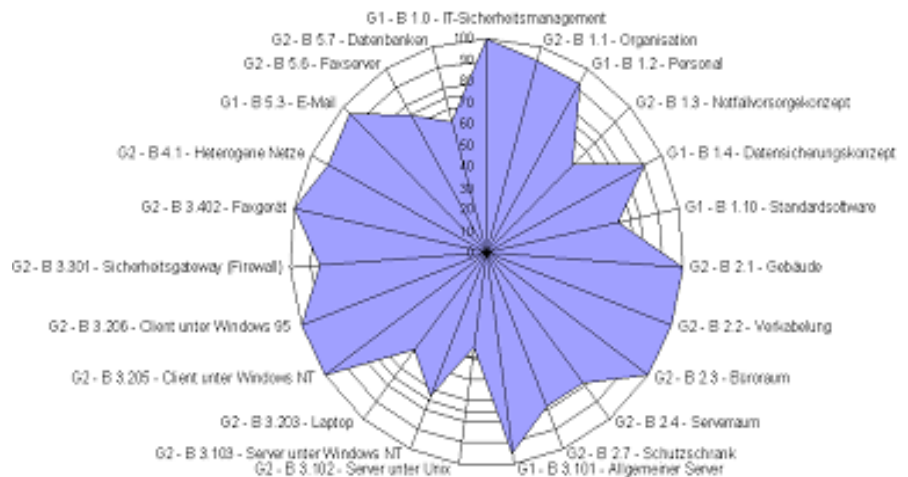
Durch ein umfangreiches Standardreporting können alle statischen und dynamischen Informationen (z.B. über Bausteine, Maßnahmen, Maßnahmenumsetzung, Kosten) abgerufen werden. Über erweiterte Filterfunktionen lassen sich die Ergebnisse gezielt auswerten und darstellen. Aus diesen Berichten werden alle aus dem Basis-Sicherheitscheck abgeleiteten Aufgaben transparent und können so einer Maßnahmenverfolgung (z.B. im Rahmen einer Risikoanalyse) zugeführt werden.

Über das Standardreporting wird für jeden ausgewählten Grundschutzbaustein angegeben, ob die Anforderungen zum Erwerb des Grundschutz-Zertifikats für diesen Baustein erfüllt sind oder ob die Einstiegs- bzw. Aufbaustufe eines Auditor-Testats erreicht wird. Zusätzlich wird der Umsetzungsgrad aller zum Zertifikat benötigten Maßnahmen in einem gewichteten Mittel bewertet und auch graphisch aufbereitet. Damit ist es möglich, den erreichten Umsetzungsgrad für die einzelnen Bausteine qualitativ zu veranschaulichen.

Die performanten MS-Access-Reports

lassen sich durch eigene, ebenfalls

schnell generierbare *List&Label*<sup>®</sup>-Berichte ersetzen und erweitern, so dass sich die **SAVE**<sup>®</sup>-Daten problemlos in die Standard-Konzepte und -Layout der Institutionen einreihen. Zudem ermöglicht ein Berichte-Manager die Festlegung einer Reihe zusammen zu erzeugender Berichte, die dann mit einem einzigen Kommando generiert und ausgegeben werden können.



## Abbildung auf ISO 17799 / ISO 27001

Die IT-Sicherheitsdatenbank **SAVE**<sup>®</sup> bietet dem Benutzer auch weitere, über den Grundschutz hinaus gehende Funktionalitäten an. So können z.B. die Ergebnisse der Maßnahmenumsetzung auf die entsprechenden Anforderungen (clauses, control objectives, controls) der Norm ISO 17799 bzw. ISO 27001 gegen die IT-Grundschutzmaßnahmen bzw. -methodik abgebildet und dargestellt werden.

## Risikoanalyse gemäß BSI-Standard 100-3

**SAVE**<sup>®</sup> unterstützt die Risikoanalyse nach dem BSI-Standard 100-3. Dazu gehören das Erzeugen von Risiko-Definitionen aus den Gefährdungen, die existierenden Schutzprofilen zugeordnet sind, die Möglichkeit der Bearbeitung von Risiken mit Verweis auf die zugrundeliegenden Gefährdungen, die Verwaltung der Zuordnung von Risiken zu Schutzprofilen, die Darstellung der Risikoabdeckung mit Umsetzungsstatus der zugeordneten Maßnahmen und die Anzeige der zu Risiken zugeordneten Maßnahmen und ihres Umsetzungsstatus.

## Unterstützung der ISO 27001-Zertifizierung auf Basis IT-Grundschutz

In **SAVE**<sup>®</sup> (Consulting Edition) stehen zur Durchführung von Zertifikats-Audits erweiterte Beschreibungsfunktionen, zusätzliche Reporting-Funktionen für den Audit-Bericht, spezielle Funktionen für den direkten Vergleich zwischen den Ergebnissen eines Basis-Sicherheitschecks und des Zertifikats-Audits zur Verfügung.

## Unterstützung Datenschutz-Audit

Die Überprüfung der technisch-organisatorischen Datensicherheitsziele gemäß §9 und Anlage zu §9 BDSG wird durch die Modellierung der entsprechenden Standard-Sicherheitsmaßnahmen nach den IT-Grundschutz-Katalogen erreicht. Diese Sichtweise ermöglicht eine enge Zusammenarbeit des betrieblichen Datenschutzbeauftragten (bDSB) mit dem jeweiligen IT-Sicherheitsbeauftragten des Unternehmens. Die vom Gesetzgeber implizit geforderte Fachkenntnis des bDSB in Fragen der IT-Sicherheit wird hierdurch nachhaltig gefördert. Das Datenschutzmodul ist zusätzlich zu erwerben.

Der Ansatz zur Realisierungsprüfung der Datenschutzorganisation basiert auf einen 1999 vom Bundesbeauftragten für den Datenschutz (BfD) entwickelten Baustein des IT-Grundschutz-Handbuchs, der nie offiziell veröffentlicht wurde. Die vom BfD vorgeschlagenen Maßnahmen sind mit zahlreichen Kontrollfragen unterlegt, die den neuen Aspekten des Datenschutzes hinsichtlich Datenvermeidung und Datensparsamkeit, Pseudonymisierung und Anonymisierung sowie den Transparenzkriterien gerecht werden. Die Landesdatenschutzgesetze, Anforderungen der jeweiligen Sozial-, Tele- und Mediendienste sowie Kirchendatenschutz können über vordefinierte Szenarien eingebunden werden.



## Konvertierung

**SAVe®** stellt eine automatische Konvertierung von Datenbeständen aus vorherigen Versionen der Sicherheitsdatenbank und Ständen des Grundschutzhandbuches sicher. Die Benutzerdaten und benutzerspezifischen permanenten und temporären Erweiterungen werden beim erstmaligen Zugriff automatisch in die neue Struktur des IT-Grundschutzhandbuchs konvertiert. Zudem enthält **SAVe®** einen Datenkonverter für die jeweils aktuelle Version des *GSTOOL®*, so dass von dort übernommene Daten gemäß dem jetzigen Aufbau des Grundschutzes bearbeitet werden können.

## Technische Leistungsmerkmale

Die IT-Sicherheitsdatenbank **SAVe®** ist eine auf MS-Access basierende Anwendung, die sowohl als Einzelplatz-Version auf einem Desktop oder Notebook als auch auf einem Server für eine netzweit verteilte Nutzung installiert werden kann. Kunden, die über keine MS-Office-Umgebung verfügen, können eine Run-Time-Version installieren. Die Mehrbenutzerfähigkeit der Anwendung ermöglicht einen optimalen unternehmens- und konzernweiten Ressourceneinsatz.

Die Menü- und Symbolleisten werden in **SAVe®** kontextsensitiv gesteuert, entsprechend den Rechten eines Benutzers, den durchzuführenden Aufgaben und den zu bearbeitenden Daten. Das flexibel angelegte Rollenmodell erlaubt die Zuweisung mehrerer Rollen zu einem Benutzer. Eine starke Authentifizierung garantiert nur den Zugriff berechtigter Nutzer. Die Menüstruktur ist bewusst flach gehalten, die Verschachtelungstiefe der Eingabe- und Anzeige-Formulare ist gering, so dass jederzeit ein gezielter Ausstieg auf die oberste Bedienebene möglich ist. Durch die Verwendung von MS-Access ist die vollständige Integration des Werkzeugs in eine MS Office-Umgebung garantiert.

Das unterlegte Datenmodell ist offen und erweiterbar hinsichtlich Änderungen / Ergänzungen des IT-Grundschutzes sowie für Erweiterungen durch andere Methoden (z.B. Datenschutz-Audits oder kundenspezifische Kriterienkataloge). Im Modus der abgesetzten Verarbeitung können gezielt Datenbestände auf Datenbankebene ausgelagert werden (z.B. auf Notebooks für eine *Vor-Ort-Bearbeitung*). Dieser *Check-out* bzw. *Check-in*-Vorgang wird systemseitig durch entsprechende Konsistenzprüfungen und eine einfache Bedienung unterstützt.

Die hinterlegten und performanten Standard-Reports können aufgabenbezogen direkt bzw. über ein eigenständiges Menü mit umfangreichen Filterfunktionen aufgerufen werden. Benutzerdefinierte Berichte können ohne Vorkenntnisse flexibel erstellt werden.

## Systemvoraussetzungen

**SAVe®** ist für Windows 2000 und XP sowie für die Access-Versionen 2000 bis 2003 (9.0, 10.0 und 11.0) freigegeben. Für einen zügigen Betrieb der Anwendung werden eine CPU ab 500 MHz und mind. 64 MB RAM Hauptspeicher empfohlen. Die Anwendung nutzt den zugeordneten Standarddrucker. Die Bildschirmauflösung sollte mindestens 1024 x 768 Pixel betragen. Als Browser sind Internet Explorer, Firefox oder Netscape einzusetzen.

## Informationen zum IT-Grundschutz des BSI

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beschreibt im Standard 100-1 den Aufbau eines Informationssicherheitsmanagementsystems (ISMS), der im Standard 100-2 durch die IT-Grundschutzmethodik konkretisiert wird. In den IT-Grundschutz-Katalogen finden sich konkrete Empfehlungen für den Aufbau eines gesteuerten IT-Sicherheitsprozesses bis hin zu Prüffragen zur Umsetzung von Standardmaßnahmen zum Schutz der Informationstechnik. Für stärker zu schützenden Bereiche beschreibt der Standard 100-3 eine ergänzende Risikoanalyse auf Basis IT-Grundschutz.

Das IT-Grundschutzhandbuch (GSHB) wurde erstmals 1995 veröffentlicht und seitdem kontinuierlich weiterentwickelt und ergänzt. Es hat sich im Laufe der Zeit zu einem idealen Hilfsmittel für die Erstellung von IT-Sicherheitskonzepten entwickelt. Die Empfehlungen des GSHB stellen mittlerweile einen Quasi-Standard der IT-Sicherheit dar, der sich durch leichte Anwendbarkeit und Umsetzbarkeit auszeichnet und damit zu einem effizienten Sicherheitsmanagement beiträgt. Hinsichtlich der Berücksichtigung internationaler Normen wurden die Grundschutz-Vorgehensweise und die Grundschutz-Kataloge in der Version des GSHB 2005 grundlegend überarbeitet sowie das IT-Sicherheits- und das Risikomanagement stärker herausgehoben. In diesem Zusammenhang wurde ebenfalls das 2002 eingeführte Zertifizierungsschema angepasst, mit dem der Umsetzungsstand der Sicherheitsmaßnahmen öffentlich dokumentiert werden kann. Die seit dem 1. Januar 2006 mögliche ISO 27001-Zertifizierung auf Basis von IT-Grundschutz umfasst dabei eine prozessorientierte Prüfung des IT-Sicherheitsmanagements sowie technische Bewertung konkreter IT-Sicherheitsmaßnahmen anhand der IT-Grundschutz-Kataloge. Das Zertifizierungsaudit sowie auch das Auditor-Testat (Einstiegs- und Aufbaustufe) wird durch unabhängige, vom BSI lizenzierte Auditoren durchgeführt.

INFODAS GmbH verfügt über erfahrene Auditoren für ISO 27001-Audits auf Basis IT-Grundschutz sowie Audits und Auditor-Testate.