

## Collaboration zur Unterstützung eines ISMS in komplexen Systemen



SAVe ist ein ISMS-Werkzeug zur Erstellung von IT-Sicherheitskonzepten für die Überprüfung und Optimierung von IT-Sicherheitsprozessen.

SAVe ist als IT-Grundschutz-Tool seit zwanzig Jahren sowohl im zivilen Umfeld (z.B. bei Banken, Versicherungen, ÖPNV) als auch bei Ämtern und Behörden (z.B. Bundeswehr, Bundespolizei) erfolgreich im Einsatz.

SAVe wird im Rahmen von Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz verwendet und ist von der Zertifizierungsstelle des BSI anerkannt.

SAVe zeigt seine Stärken insbesondere im Umfeld komplexer, verteilter und heterogener IT-Infrastrukturen, mit zum Teil sehr hohen Schutzanforderungen.

SAVe ist modular aufgebaut. Dies ermöglicht die flexible Erweiterbarkeit von Sicherheitsmodellen wie:

- IT-Grundschutz (BSI Standards 100-1 bis 100-3)
- Modernisierter Grundschutz (BSI Standards 200-1 bis 200-2)
- Notfallvorsorge (BSI Standard 100-4 und ISO 22301)
- Datenschutz (BDSG und LDSGs)
- ISO 2700x

Darüber hinaus werden auch kundenspezifische Sicherheitsmodelle unterstützt:

- Militärische Erweiterung
- Erweiterungen für die Bundespolizei

SAVe ermöglicht im Rahmen des Notfallmanagements die Nutzung von Synergien zu bestehenden Sicherheitsmodellen. Die Erfassung von kritischen Prozessen und Teilprozessen und deren Zuordnung auf bestehende Elemente des ISMS (Zielobjekte, Bausteine, Risiken) gestattet eine ganzheitliche Darstellung der Abhängigkeiten zwischen Prozessen und diesen Elementen. Dies bildet die Grundlage für eine prozessbezogene Risikoanalyse entsprechend dem Vorgehen des BSI Standards 100-3.

SAVe als Collaboration-Tool ermöglicht den Informationsaustausch und die übergreifende Zusammenarbeit in der gesamten ISMS-Organisation. Dies betrifft beispielsweise die:

- teambasierte Erstellung und Fortschreibung von IT-Sicherheitskonzepten
- Generische Erstellung von kundenspezifischen Katalogen auf Basis von Segmenten
- Audit- und Revisionsprozesse (Zusammenspiel von Prüfer/Auditor und Bearbeiter)
- Zuweisung und Nachverfolgung von Verantwortlichkeiten

## Arbeiten mit SAVE 5

- **Effiziente und zielgerichtete** Erstellung und Pflege von IT-Sicherheitskonzepten durch definierte Prozessschritte
- **Kontextbezogene** Darstellung durch ganzheitliche und übersichtliche Anzeige aller relevanten Informationen, Relationen und Funktionen eines Prozessschrittes
- **Visualisierung** der Beziehungen und Abhängigkeiten zwischen Elementen des ISMS (Objekte, Bausteine, Maßnahmen, Risiken, Gefährdungen, Prozesse)
- **Erstellung und Pflege** von IT-Sicherheitskonzepten

nach den Vorgehensweisen Basis-, Standard- und Kernabsicherung

- **Echtzeitdarstellung** der Konsistenz- und Vollständigkeitsprüfung sowie deren Bewertung durch den Nutzer
- **Unabhängige** Bearbeitung von Prozessschritten (z.B. IT-Grundschutzcheck ohne Strukturanalyse)
- **Schneller Wechsel** zwischen verschiedenen Ansichten (Prozessschritten) ermöglicht individuelles Arbeiten

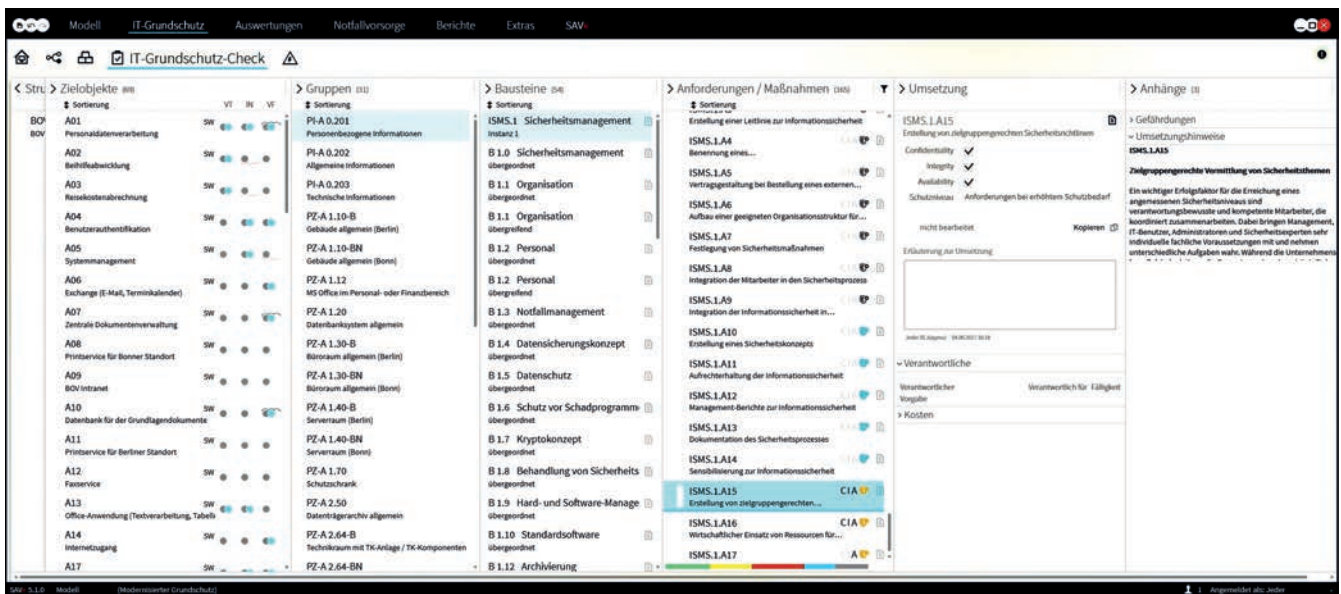


Abb.: IT-Grundschutz-Check in SAVE 5

## Eigenschaften von SAVE 5

- **Importfunktion** der Daten aus dem GSTOOL
- **Abwärtskompatibilität** zu Vorgängerversionen
- **Erweiterter und flexibler Berichtsmanager** für ebenengerechte und anlassbezogene Berichte
- Zukunftssichere Implementierung durch Verwendung von **Standardtechnologien** (.NET-Framework, MS SQL-Server)
- **Mandantenfähigkeit** durch strikte Trennung von Nutzerdaten

- **Skalierbarkeit** des Tools von Stand-Alone-Betrieb bis hin zur Client-Server-Umgebung.
- **Mehrbenutzerfähigkeit** ermöglicht gleichzeitiges, teambasiertes Arbeiten
- Systemvoraussetzung ist MS Windows 7 bis MS Windows 10
- **Integration** weiterer (individueller) Kataloge durch Definition eigener Bausteine mit Maßnahmen und Gefährdungen