TOOL-UNTERSTÜTZUNG IT-GRUNDSCHUTZ

TOOL-UNTERSTÜTZUNG IT-GRUNDSCHUTZ

Tool-Unterstützung IT-Grundschutz

Produktvergleich

Andreas Floß, Senior Consultant
Ronny Frankenstein, Senior Manager

HISOLUTIONS

Zusammenfassung

Die folgende Präsentation stellt 4 Software-Tools zur Dokumentation der IT-Sicherheitskonzepte nach BSI IT-Grundschutz vor. Für jedes Tool werden die wesentlichen Features dargestellt. Es wurden betrachtet:

- HiScout der Firma HiScout GmbH,
- i-Doit der Firma synetics GmbH,
- CRISAM der Firma calpana business consulting GmbH sowie
- verinice. der Firma SerNet GmbH.

Alle Tools sind entsprechend den Vorgaben des BSI geeignet das IT-Sicherheitskonzept zu dokumentieren. Es gibt verschiedene Anwendungsbereiche und z.T. auch Zusatzfunktionen, die für eine Entscheidung zum Einsatz in den Einrichtungen maßgeblich sein können.

Technische Unterschiede in der Implementierung (Clientsoftware, Webanwendung) sind ebenfalls bei der Tool-Auswahl zu berücksichtigen.

Abschließend wird ein Vergleich der wichtigen Features und Zusatzfunktionen gegeben, der den jeweiligen Einrichtungen bei der Auswahl helfen soll.

HISOLUTIONS

Übersicht der Tools

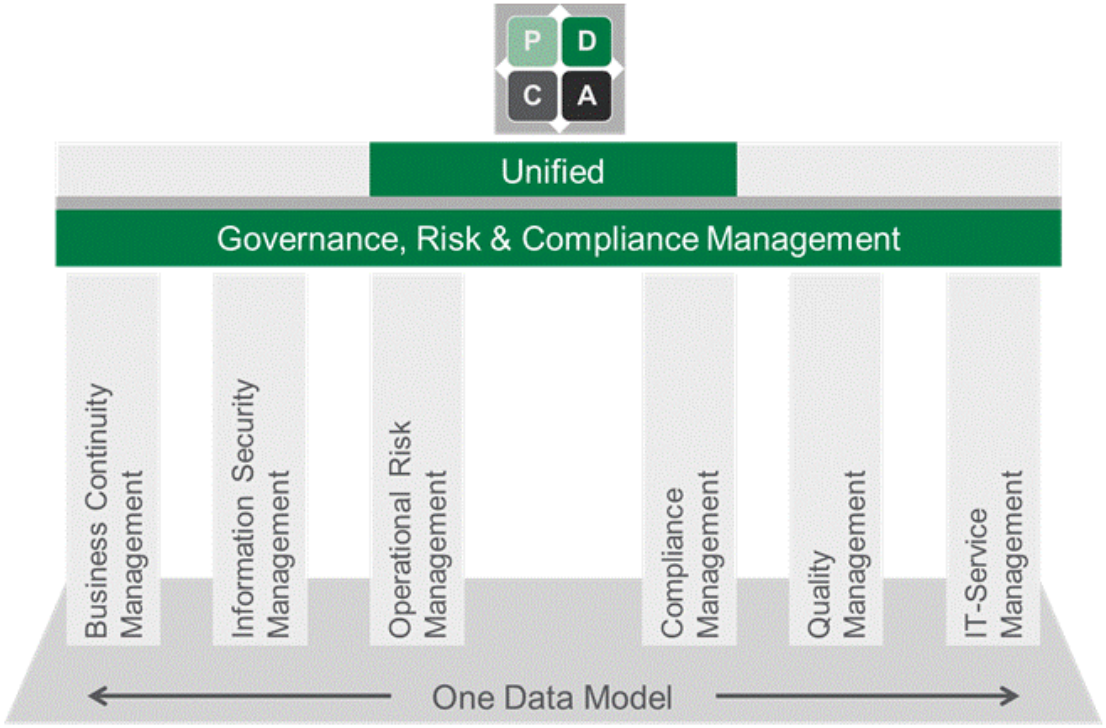
HISOLUTIONS

Produktvorstellung

HiScout

HISOLUTIONS

HiScout GRC Suite



HISOLUTIONS

HiScout

Das HiScout ISM Modul unterstützt die Umsetzung von BSI IT-Grundschutz

- Komplettes ISMS nach BSI 100-1 / 2 / 3
- BCM Modul nach BSI 100-4 / UMRA
- Zertifizierte Grundschutzverbünde durch HiScout
- Flexible Schnittstellen (GS-Tool Import, Metadatenupdate, XML)
- Template-basiertes Reporting
- Browserbasierte Multi-Useranwendung (Zero-Client)
- Vollständige ISO-Konformität (Prozesse, Informationen, Audits, …)

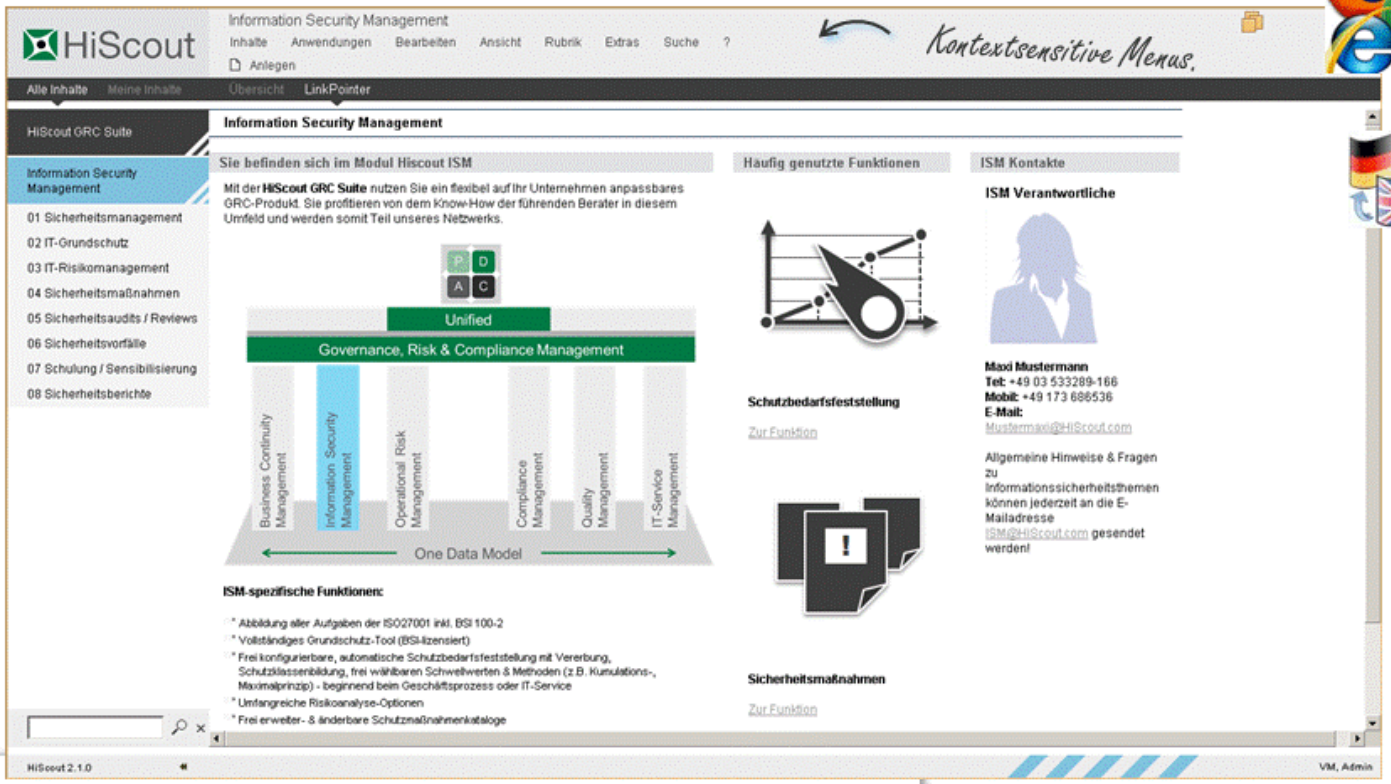
HISOLUTIONS

HiScout

Portalbasierte Weboberfläche

Web-basiert, Zero-Client.

Kontextsensitive Menus.



HISOLUTIONS

HiScout

Anpassungen können ohne technische Eingriffe durch den Benutzer durchgeführt werden

HISOLUTIONS

HiScout

Lizenzmodell

- Lizenzen sind in Abhängigkeit von
  - Umfang Modulauswahl
  - Unternehmens- bzw. Behördengröße
  - Nutzeranzahlen

HISOLUTIONS

Produktvorstellung

i-doit

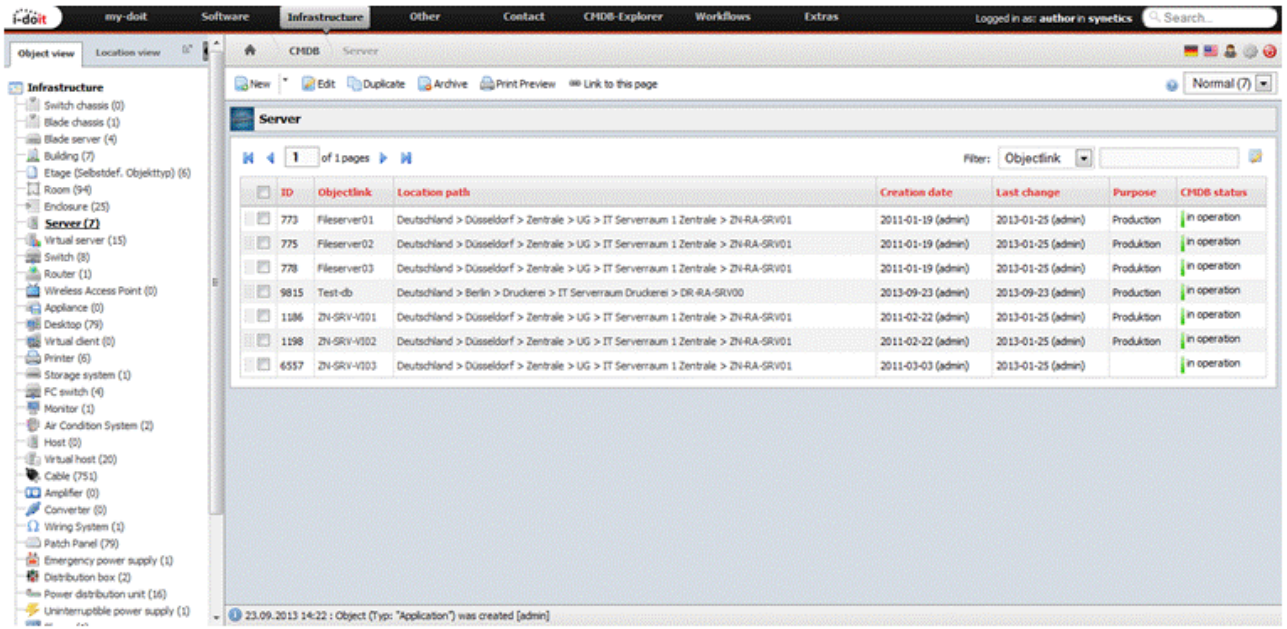
HISOLUTIONS

i-doit – VIVA-Modul (synetics)

- Webbasiert
- Dokumentation komplexer IT-Infrastrukturen
- Basiert auf einer CMBD in Anlehnung an ITIL
- Open- und Pro-Versionen erhältlich
- Erweiterbar durch verschiedene Module
- Kostenpflichtiges Modul VIVA notwendig für IT-Security (ISO, GS)
- Benötigt zwingend i-doit Pro (ab Version 1.1)

HISOLUTIONS

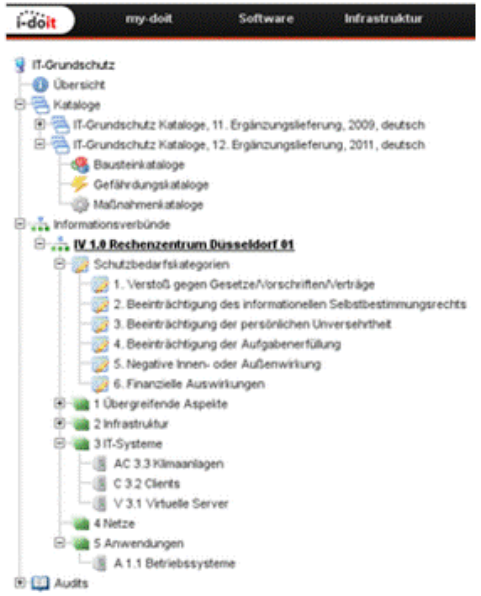
i-doit Benutzeroberfläche



HISOLUTIONS

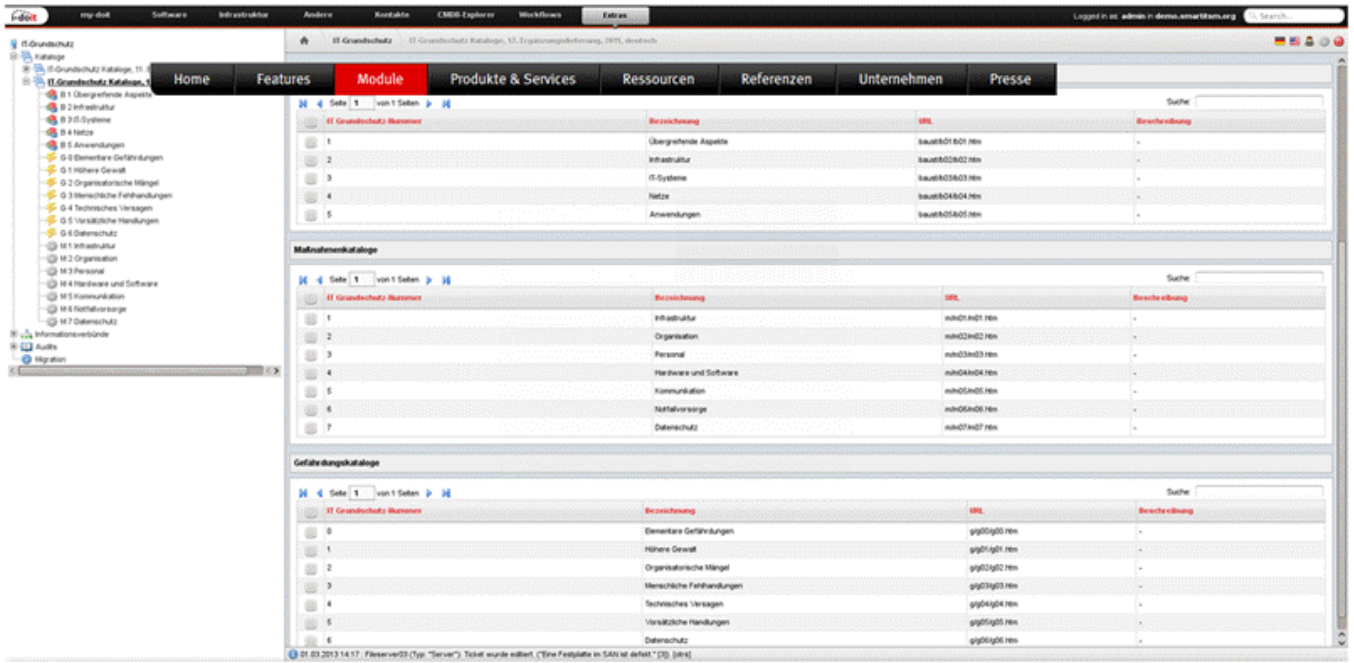
Zusätzliches Modul ermöglicht die Abbildung von BSI IT-Grundschutz

- Import der aktuellen IT-Grundschutz-Kataloge EL11 (2009) und EL12 (2011)
- Anpassen und Erstellen von Bausteinen, Gefährdungen und Maßnahmen
- Übersichten mit Statusanzeige
- Vollständige Unterstützung BSI-Standard 100-2, 100-3,
- Ausgabe der Referenzdokumentation



HISOLUTIONS

i-doit bietet eine Katalogverwaltung zur Pflege BSI IT-Grundschutzkataloge



Im Basis-Sicherheitscheck wird der Umsetzungsstatus dokumentiert

Seite 1 von 1 Seiten Suche:

Status	IT-Grundschutz-Maßnahme	Qualifizierungsstufe	Anmerkungen	Datum der Umsetzung	Umsetzer
●	M 2.192 Erstellung einer Leitlinie zur Informationssicherheit	A (Einstieg)	-	05.04.2013	Max Mustermann
●	M 2.335 Festlegung der Sicherheitsziele und -strategie	A (Einstieg)	-	05.04.2013	Erika Mustermann
●	M 2.336 Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene	A (Einstieg)	-	05.04.2013	Erika Mustermann
●	M 2.193 Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit	A (Einstieg)	-	05.04.2013	Enoch Root
●	M 2.195 Erstellung eines Sicherheitskonzepts	A (Einstieg)	-	-	Enoch Root
-	M 2.197 Integration der Mitarbeiter in den Sicherheitsprozess	A (Einstieg)	-	-	-
-	M 2.337 Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse	A (Einstieg)	-	-	-
●	M 2.338 Erstellung von zielgruppengerechten Sicherheitsrichtlinien	Z (Zusätzlich)	-	-	-
●	M 2.339 Wirtschaftlicher Einsatz von Ressourcen für Informationssicherheit	Z (Zusätzlich)	-	-	-
-	M 2.475 Vertragsgestaltung bei Bestellung eines externen IT-Sicherheitsbeauftragten	A (Einstieg)	-	-	-
●	M 2.199 Aufrechterhaltung der Informationssicherheit	A (Einstieg)	-	-	Max Mustermann, Erika Mustermann
●	M 2.200 Management-Berichte zur Informationssicherheit	C (Zertifikat)	-	-	-
●	M 2.201 Dokumentation des Sicherheitsprozesses	C (Zertifikat)	-	-	-
●	M 6.16 Abschließen von Versicherungen	Z (Zusätzlich)	-	-	-

i-doit unterstützt die Einbindung der CMDB in die Grundschutz-Vorgehensweise

- Vollständige Unterstützung der BSI-Standards 100-2, 100-3
  - Modellierung von Informationsverbünden
  - Ermittlung des Schutzbedarfs
  - Durchführung einer ergänzenden Sicherheitsanalyse
  - Zuordnung von Bausteinen und deren Gefährdungen sowie Maßnahmen
  - Durchführen von BSCs, Umsetzung von Maßnahmen
  - Risikoanalyse von zugeordneten Gefährdungen
- Konzeptionelles Problem: „Zielobjekte“ in CMDB vs. „Zielgruppen“ in VIVA (Einordnung, Vererbung etc.)
- Version 1.0 von Mai 2013, aktuell Version 1.2 von September 2013

Lizenzmodell

- Das Zusatzmodul VIVA ist zusätzlich zum Basismodul erhältlich.

Fakten und Preise

Der Einsatz des VIVA-Moduls orientiert sich preislich am eingesetzten i-doit Objektpaket und ist sowohl im Rahmen der Kaufversion, als auch für die Subskription verfügbar. Die Konditionen sind dabei ergänzend zum Basispaket zu verstehen.

	einmalig	500er	1.000er	5.000er	unlimitiert
Subskription	1.200,00 €	44,00 €	64,00 €	132,00 €	600,00 €
Kaufversion*	-	1.395,00 €	1.495,00 €	1.595.,00 €	2.990,00 €

*** 3 Jahre Updates und Upgrades inklusive, 10% des Kaufpreises ab dem 4. Jahr für jährliche Wartung**

Alle Preise sind netto und verstehen sich zzgl. der gesetzlich fälligen MwSt

Produktvorstellung

crisam®
DECISION ENGINEERING

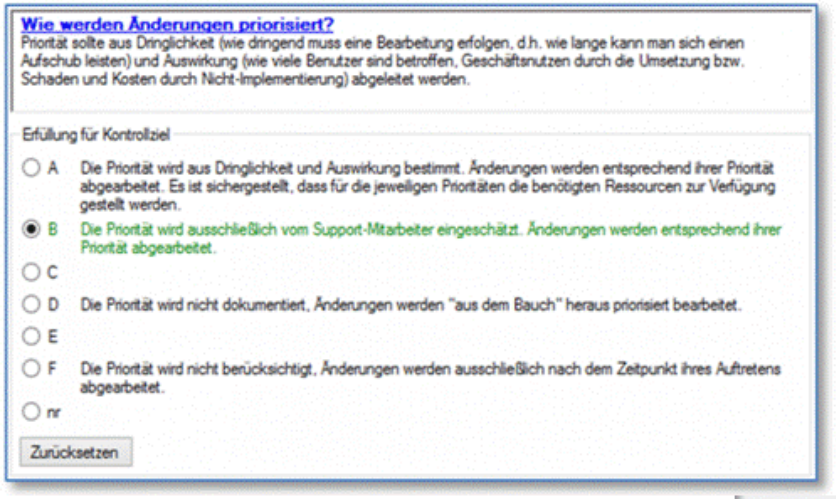
HISOLUTIONS

CRISAM 5

- Hersteller: Calpana Business Consulting (AT)
- CRISAM = „Corporate Risk Application Method“
- Erweiterbar durch Verschiedene Module (Knowledge Pack) u.a.
  - CRISAM ISMS Knowledge Pack
  - CRISAM ISO 27001 Knowledge Pack
  - **CRISAM BSI und GSTOOL Knowledge Pack**
- Benötigt CRISAM Explorer

CRISAM 5 – ISMS Knowledge Pack

- 160 Bausteine und 1.700 Kontrollziele zur Identifikation und Bewertung von IT-Risiken
- Quellen, wie BSI Grundschutz, ISO/IEC 27002, ITIL Version 2 und 3, COBIT und NIST
- Best Practices und Empfehlungen von Herstellern.
- Expertenwissen aus der CRISAM® Community.
- halbjährlichen Zyklus aktualisiert

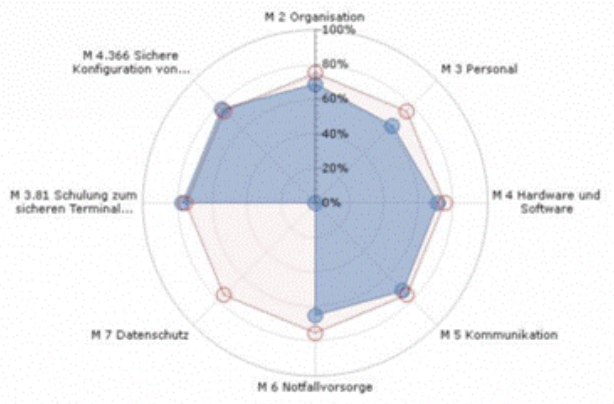


CRISAM 5 – ISO 27001 Knowledge Pack

- Aktuelle Versionen (2005 und 2013) der ISO/IEC 27000 Normenreihe.
- Von Norm geforderte Berichte „Statement of Applicability“ und „Scope Document“
- Compliance Analysebericht um die Konformität Ihres ISMS zu den Normforderungen der ISO/IEC 27001 nachzuweisen und gegenüber 27002 darzustellen
- Unterstützt damit optimal bei der Vorbereitung und (Re-)Zertifizierung
- Auswertung aus CRISAM® ISMS Kontrollen

CRISAM 5 – BSI und GSTOOL Knowledge Pack

- **GSTOOL Import**, um bestehende BSI GSTOOL Daten in das CRISAM Risikomanagement Informationssystem zu übernehmen
- **BSI Compliance Analysebericht**, als Konformitätsnachweis Ihres ISMS nach BSI IT-Grundschutz nachzuweisen
- Unterstützt bei der **Vorbereitung und Zertifizierung** nach BSI IT-Grundschutz-Zertifikat
- Das integrierte Mapping ermöglicht **Auswertungen** aus CRISAM ISMS oder bestehenden **BSI Kontrollen**



Produktvorstellung

verinice.

HISOLUTIONS

verinice.

Verinice.Pro

- IT-Grundschutz, ISO 27001/2, Risikoanalyse nach ISO 27005, IS-Assessments nach VDA Vorgaben, Nachweis von Compliance mit Standards wie IDW PS 330 u. a.
- *Auch* als CMDB verwendbar
- Zentrales IS-Repository, Zentrale Dokumentenablage, Fernzugriff
- VMware-Anbindung möglich
- Mehrbenutzerfähigkeit, Berechtigungskonzept, Directory-Anbindung
- Web-basierter Workflow, Sichere Verbindung (SSL), Mailbenachrichtigungen
- Erstellen einer Verarbeitungsübersicht nach § 4g II i.V.m. § 4e BDSG

HISOLUTIONS

verinice.

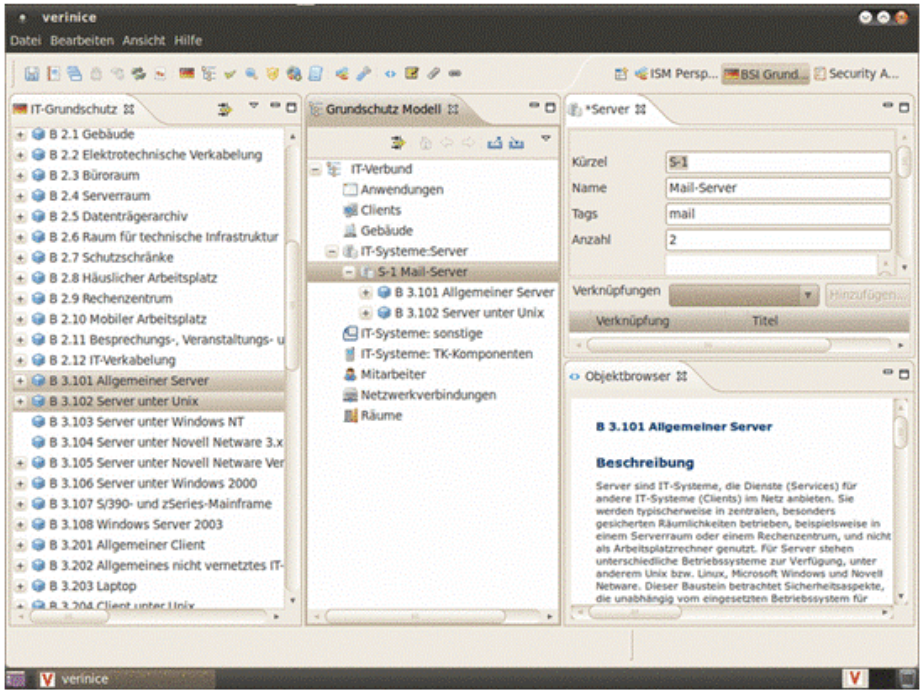
Verinice.Pro

- Import von GS-Tool durch HiSolutions möglich
- Offener Source Code (nicht Server)
- Externe Datenbank (Hibernate: Postgres / Oracle / …),
- Dynamisches Objektmodell (HitroUI)
- BIRT-Reporting
  - Erstellen eigener Reports möglich

HISOLUTIONS

verinice.

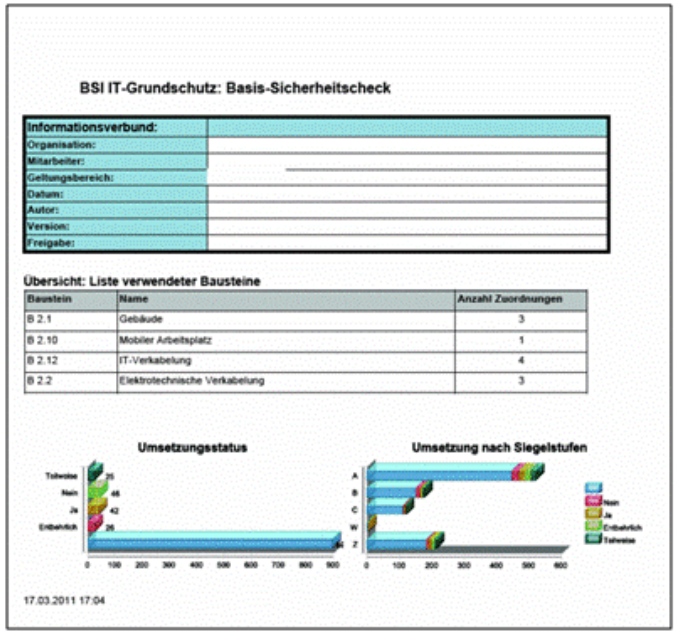
Verinice.Pro bietet deckt das komplette Vorgehen des BSI IT-Grundschutz ab



HISOLUTIONS

verinice.

Verschiedene grafische Darstellungen des ISMS sind möglich



BSI IT-Grundschutz: Basis-Sicherheitscheck

Informationsverbund:	
Organisation:	
Mitarbeiter:	
Geltungsbereich:	
Datum:	
Autor:	
Version:	
Freigabe:	

Übersicht: Liste verwendeter Bausteine

Baustein	Name	Anzahl Zuordnungen
B 2.1	Gebäude	3
B 2.10	Mobiler Arbeitsplatz	1
B 2.12	IT-Verkabelung	4
B 2.2	Elektrotechnische Verkabelung	3

Umsetzungsstatus

Umsetzung nach Siegelstufen

17.03.2011 17:04

Scope / Client: My Company

Date: 17. März 2011

Risk Register

Risk Acceptance Criteria

Category	Tolerable risk level
Confidentiality	7
Integrity	7
Availability	8

The following risk assessment was performed as detailed in the approved risk assessment method and is in accordance with international standard ISO / IEC 27005.
Risk acceptance criteria shown on the left are defined in the risk assessment policy and approved by senior management.

Confidentiality: property that information is not made available or disclosed to unauthorized individuals, entities, or processes
Integrity: property of protecting the accuracy and completeness of assets
Availability: property of information being accessible and usable upon demand by an authorized entity
(ISO/IEC 27000:2009)

Risk Matrix: Confidentiality

Number of identified Risks

Impact / Probability	0	1	2	3
0	0	0	0	60
1	0	0	0	3
2	0	0	0	7
3	0	0	3	20
4	0	0	0	2
5	0	0	0	5
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0

Table shows the number of identified risks and their severity.
See below for classification of probability and business impact levels.

Total Count

HISOLUTIONS

Zusammenfassung

HISOLUTIONS

Die Entscheidung für ein Tool hängt von vielen Faktoren ab

- Spezielle Anforderungen der Organisation?
- Verpflichtende Vorgaben zum Tooleinsatz?
- Wie wichtig ist das verteilte Arbeiten (Webbasiert oder Clientlösung)?
- Komplexität und Bedienerfreundlichkeit der Anwendung?
- Sichere Übertragung möglich?
- Lizenzen / Kosten:
  - Genaue Kenntnisse von Mengengerüsten nötig
  - Synergieeffekte bei Nutzung weiterer Funktionen (BCM, Compliance, CMDB, IT-Servicemanagement, …)?
  - Mieten oder kaufen?
  - Wie viel Support gewünscht?
  - Verhandlungen mit Herstellern…

HISOLUTIONS

Zusammenfassung I: Wesentliche Features

Parameter	HiScout	verinice.PRO	i-doit Pro inkl. VIVA	CRISAM 5.0
Fokus	Governance Risk and Control	Information Security Management	Assetmanagement	Governance Risk and Control
Client-Technologie	webbasiert (SSL)	Rich Client (Java)	webbasiert (SSL)	Rich Client / webbasiert
Berechtigungskonzept	++	+	+	++
Erweiterbar durch Module	++	-	o	++
Eigene Berichte	++	++	o	++
Handling / Einarbeitungszeit	-	++	o	+
Übersichten mit Statusanzeige (Cockpit)	+	o	+	++
Lernkurve	+	+	++	+
Kosten	6000-9000€ (nach Organisationsgröße)	freie Version (nur 1 User) oder 1700€/Jahr	2400-4600€ oder 270-800/Jahr (nach Anzahl Objekte)	nicht bekannt (je nach Anzahl der User)

HISOLUTIONS

Zusammenfassung II: weitere Features

Parameter	HiScout	verinice.PRO	i-doit Pro inkl. VIVA	CRISAM 5.0
Server-Technologie	Windows Server, SQL Server, ASP.NET	Java (Tomcat), Postgres/My-SQL (auch als VMware-Appl.)	Apache, MySQL, PHP	Windows Server,SQL Server, ASP.NET
ISO 2700x und IT-Grundschutz	+	+	+	+
Vom BSI akkreditiert für IT-Grundschutz	+	+	+	+
Mappings zu ISO 27001/2	+	-	-	+
Anpassung von Bausteinen	+	+	+	+
Zentrale Dokumentenablage	++	+	+	+
Workflows	++	+	+	++
Import / Export	+	+	+	++
Offener Sourcecode	-	o (nur Client)	- (nur i-doit open)	-
Individuelle Anpassung nötig	-	o	o	-
Produktreife	+	++	-	+
Optionaler Support	+	+	+	+

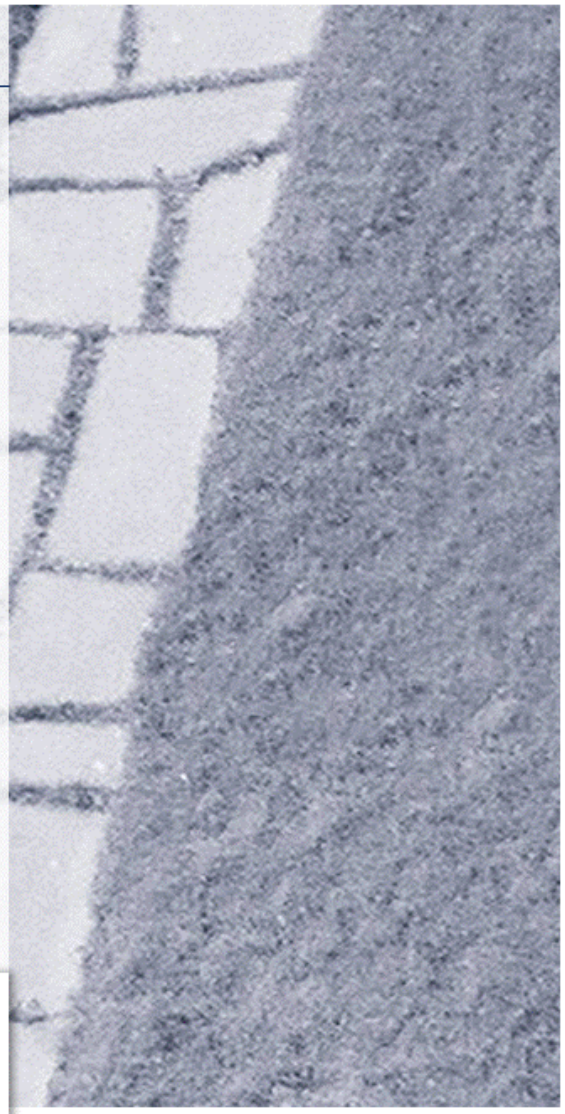
HISOLUTIONS

Kontakt

HiSolutions AG

Bouchéstraße 12
12435 Berlin
www.hisolutions.com
+49 30 533 289 0

Ronny Frankenstein
Senior Manager
Produkt Manager BSI IT-Grundschutz / ISO 27001
Datenschutz- und IT-Sicherheitsbeauftragter
frankenstein@hisolutions.com



HISOLUTIONS

Tool-Unterstützung IT-Grundschutz

Produktvergleich

Andreas Floß, Senior Consultant
Ronny Frankenstein, Senior Manager

HISOLUTIONS