

**TOOL-UNTERSTÜTZUNG
IT-GRUNDSCHUTZ**

**TOOL-UNTERSTÜTZUNG
IT-GRUNDSCHUTZ**

Tool-Unterstützung IT-Grundschutz

Produktvergleich

Andreas Floß, Senior Consultant
Ronny Frankenstein, Senior Manager

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.

Übersicht der Tools



Produktvorstellung



HiScout GRC Suite



Unified

Governance, Risk & Compliance Management

Business Continuity Management

Information Security Management

Operational Risk Management

Compliance Management

Quality Management

IT-Service Management

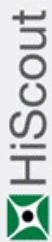
One Data Model



HISOLUTIONS

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 Grundschutzverbände durch HiScout
- Flexible Schnittstellen (GS-Tool Import, Metadatenupdate, XML)
- Template-basiertes Reporting
- Browserbasierte Multi-Useranwendung (Zero-Client)
- Vollständige ISO-Konformität (Prozesse, Informationen, Audits, ...)



Portalbasierte Weboberfläche

Web-basiert, Zero-Client.

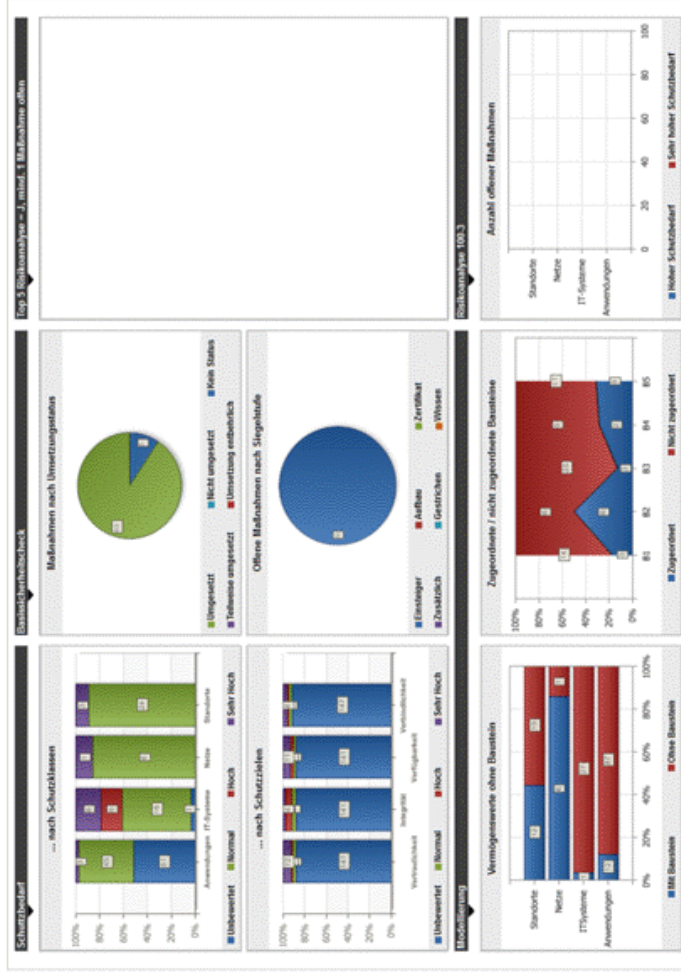
Kontextsensitive Menüs.



The screenshot displays the HiScout web interface. At the top, there is a navigation menu with options like 'Information Security Management', 'Inhalte', 'Anwendungen', 'Bearbeiten', 'Ansicht', 'Rubrik', 'Extras', 'Suche', and '?'. Below the menu, the main content area features a diagram titled 'Unified Governance, Risk & Compliance Management' showing various management components like Business Continuity, Information Security, Operational Risk, Compliance, Quality, and IT-Service. A sidebar on the right contains 'ISM Kontakte' with contact details for 'ISM Verantwortliche' (Madel Meiermann) and 'Häufig genutzte Funktionen' (Schutzbedarfsfeststellung, Sicherheitsmaßnahmen). The footer includes the HiScout logo and version information (HiScout 2.1.0).



Anpassungen können ohne technische Eingriffe durch den Benutzer durchgeführt werden



Lizenzmodell

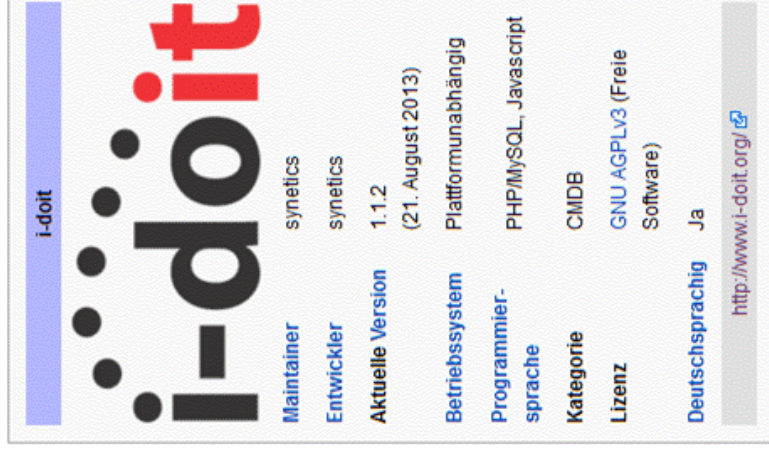
- Lizenzen sind in Abhängigkeit von
 - Umfang Modulauswahl
 - Unternehmens- bzw. Behördengröße
 - Nutzeranzahlen

Produktvorstellung

i-doit

i-doit – VIVA-Modul (synetics)

- Webbasiert
- Dokumentation komplexer IT-Infrastrukturen
- Basiert auf einer CMDB 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)



The screenshot shows the top navigation bar of the i-doit website. It features the i-doit logo in a large, bold, black font with red dots above the 'i'. To the right of the logo, there are several menu items: 'Maintainer' (synetics), 'Entwickler' (synetics), 'Aktuelle Version' (1.1.2 (21. August 2013)), 'Betriebssystem' (Plattformunabhängig), 'Programmiersprache' (PHP/MySQL, Javascript), 'Kategorie' (CMDB), 'Lizenz' (GNU AGPLv3 (Freie Software)), and 'Deutschsprachig' (Ja). At the bottom right of the navigation bar, there is a link to 'http://www.i-doit.org/' with a small globe icon.



i-doit Benutzeroberfläche

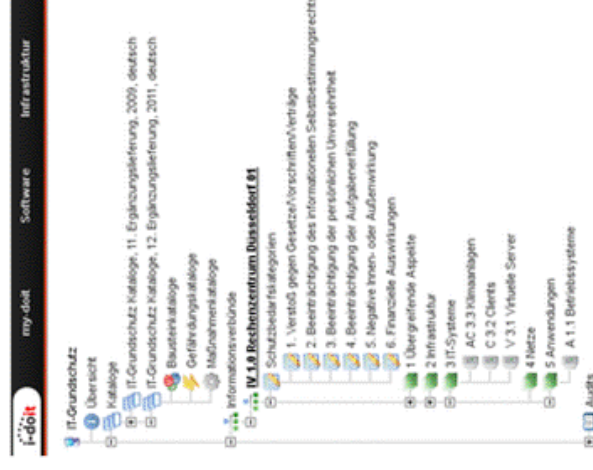
The screenshot displays the i-doit web interface. At the top, there is a navigation bar with tabs for 'Software', 'Infrastructure', 'Other', 'Contact', 'CRMS Explorer', 'Workflows', and 'Extras'. The user is logged in as 'author in synetics'. Below the navigation bar, there is a search bar and a language selector. The main content area shows a list of server objects under the 'Server' category. The list has columns for 'ID', 'Objectlink', 'Location path', 'Last change', and 'CRMS status'. The objects listed are:

| ID | Objectlink | Location path | Last change | CRMS status |
|------|-------------|---|--------------------|--------------|
| 779 | Filserver01 | Deutschland > Düsseldorf > Zentrale > US > IT Serverraum 1 Zentrale > ZH-AA-SRV01 | 2013-01-25 (admin) | in operation |
| 775 | Filserver02 | Deutschland > Düsseldorf > Zentrale > US > IT Serverraum 1 Zentrale > ZH-AA-SRV01 | 2013-01-25 (admin) | in operation |
| 778 | Filserver03 | Deutschland > Düsseldorf > Zentrale > US > IT Serverraum 1 Zentrale > ZH-AA-SRV01 | 2013-01-25 (admin) | in operation |
| 9815 | Test-db | Deutschland > Berlin > Dividende > IT Serverraum 1 Zentrale > DE-AA-SRV00 | 2013-09-23 (admin) | in operation |
| 1186 | ZH-SRV-V001 | Deutschland > Düsseldorf > Zentrale > US > IT Serverraum 1 Zentrale > ZH-AA-SRV01 | 2013-02-22 (admin) | in operation |
| 1198 | ZH-SRV-V002 | Deutschland > Düsseldorf > Zentrale > US > IT Serverraum 1 Zentrale > ZH-AA-SRV01 | 2013-02-22 (admin) | in operation |
| 6537 | ZH-SRV-V003 | Deutschland > Düsseldorf > Zentrale > US > IT Serverraum 1 Zentrale > ZH-AA-SRV01 | 2013-03-03 (admin) | in operation |

At the bottom of the interface, there is a sidebar with a tree view showing the hierarchy of objects, including 'Infrastructure', 'Switch chassis', 'Blade chassis', 'Blade server', 'Building', 'Edge (Subholder, Objecttyp)', 'Room', 'Enclosure', 'Server rack', 'Virtual server', 'Switch', 'Router', 'Wireless Access Point', 'Appliance', 'Desktop', 'Virtual client', 'Printer', 'Storage system', 'PC monitor', 'Monitor', 'Air Condition System', 'Host', 'Virtual host', 'Cable', 'Amplifier', 'Converter', 'Wiring System', 'Patch Panel', 'Emergency power supply', 'Distribution box', and 'Uninterruptible power supply'.

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



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

The screenshot shows the i-doit web application interface for managing BSI IT-Grundschutzkataloge. The interface is organized into several sections:

- Navigation Menu:** Home, Features, Module, Produkte & Services, Ressourcen, Referenzen, Unternehmen, Presse.
- Main Content Area:**
 - Übergreifende Aspekte:** A table listing various IT-Grundschutzkataloge (e.g., 1.1, 1.2, 1.3, 1.4, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11, 1.12, 1.13, 1.14, 1.15, 1.16, 1.17, 1.18, 1.19, 1.20) with columns for 'Bezeichnung' and 'Status'.
 - Mehrfachkataloge:** A table listing various IT-Grundschutzkataloge (e.g., 1.1, 1.2, 1.3, 1.4, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11, 1.12, 1.13, 1.14, 1.15, 1.16, 1.17, 1.18, 1.19, 1.20) with columns for 'Bezeichnung' and 'Status'.
 - Gefährdungskataloge:** A table listing various IT-Grundschutzkataloge (e.g., 1.1, 1.2, 1.3, 1.4, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11, 1.12, 1.13, 1.14, 1.15, 1.16, 1.17, 1.18, 1.19, 1.20) with columns for 'Bezeichnung' and 'Status'.

Im Basis-Sicherheitscheck wird der Umsetzungsstatus dokumentiert

Suche:

| Status | IT-Grundschutz-Maßnahme | Qualifizierungsstufe | Anmerkungen | Datum der Umsetzung | Umsetzer |
|--------|--|----------------------|-------------|---------------------|---------------------------------|
| ● | M 2.192 Erstellung einer Leitlinie zur Informationssicherheit | A (Ersttag) | - | 05.04.2013 | Max Mustermann |
| ● | M 2.335 Festlegung der Sicherheitsziele und -strategie | A (Ersttag) | - | 05.04.2013 | Ella Mustermann |
| ● | M 2.336 Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene | A (Ersttag) | - | 05.04.2013 | Ella Mustermann |
| ● | M 2.193 Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit | A (Ersttag) | - | 05.04.2013 | Enoch Root |
| ● | M 2.195 Erstellung eines Sicherheitskonzepts | A (Ersttag) | - | - | Enoch Root |
| ● | M 2.197 Integration der Mitarbeiter in den Sicherheitsprozess | A (Ersttag) | - | - | - |
| ● | M 2.337 Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse | A (Ersttag) | - | - | - |
| ● | M 2.338 Erstellung von zielgruppenrechten 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 (Ersttag) | - | - | - |
| ● | M 2.199 Aufrechterhaltung der Informationssicherheit | A (Ersttag) | - | - | Max Mustermann, Ella Mustermann |
| ● | M 2.200 Management-Berichte zur Informationssicherheit | C (Zertifiz.) | - | - | - |
| ● | M 2.201 Dokumentation des Sicherheitsprozesses | C (Zertifiz.) | - | - | - |
| ● | 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 Informationsverbänden
 - 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

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 Grundschrift, 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

Wie werden Änderungen priorisiert?

Priorität sollte aus Dringlichkeit (wie dringend muss eine Bearbeitung erfolgen, d.h. wie lange kann man sich einen Aufschub leisten) und Auswirkung (wie viele Benutzer sind betroffen, Geschäftsnutzen durch die Umsetzung bzw. Schaden und Kosten durch Nicht-Implementierung) abgeleitet werden.

Erfüllung für Kontrollziel

- A Die Priorität wird aus Dringlichkeit und Auswirkung bestimmt. Änderungen werden entsprechend ihrer Priorität gestellt werden.
- B Die Priorität wird ausschließlich vom Support-Mitarbeiter eingeschätzt. Änderungen werden entsprechend ihrer Priorität abgearbeitet.
- C
- D Die Priorität wird nicht dokumentiert. Änderungen werden "aus dem Bauch" heraus priorisiert bearbeitet.
- E
- F Die Priorität wird nicht berücksichtigt. Änderungen werden ausschließlich nach dem Zeitpunkt ihres Auftretens abgearbeitet.
- nr

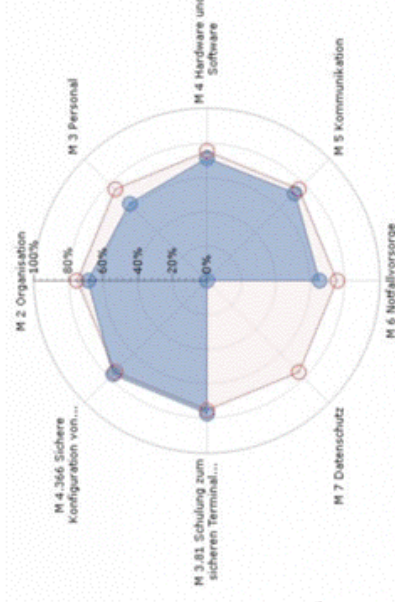
Zurücksetzen

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:

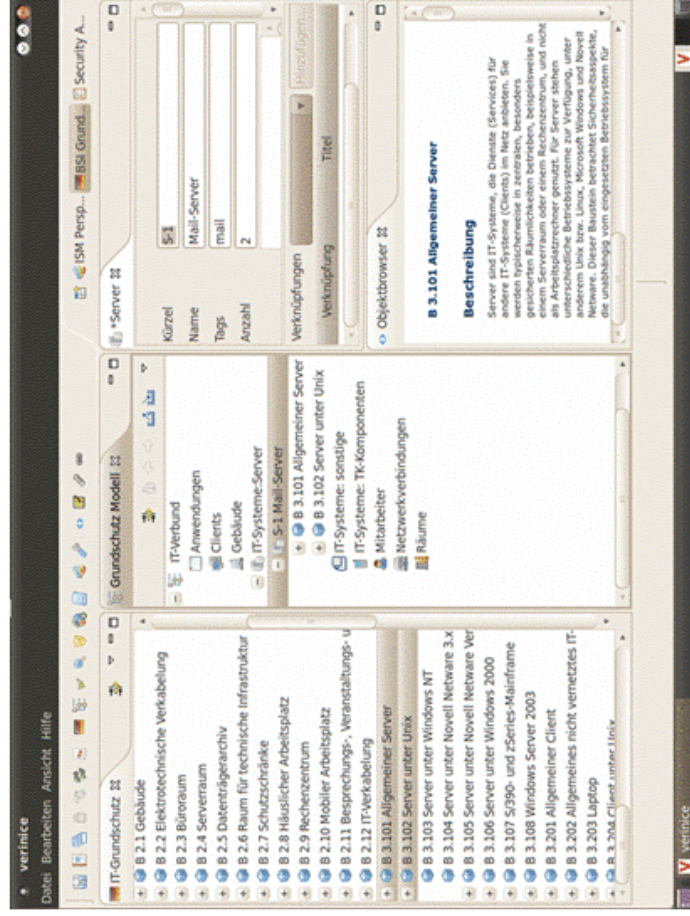
Verinice.Pro

- 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

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

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



Verschiedene grafische Darstellungen des ISMS sind möglich

BSI IT-Grundschutz: Basis-Sicherheitscheck

Informationsverbund:

| | |
|-----------------|--|
| Organisation: | |
| Standort: | |
| Gebäudebereich: | |
| Datum: | |
| Autor: | |
| Version: | |
| Fregabe: | |

Übersicht: Liste verwendeter Bausteine

| Bezeichnung | Name | Anzahl Zuordnungen |
|-------------|--------------------------|--------------------|
| B 2.1 | Gebäude | 3 |
| B 2.10 | Möblier Arbeitsplatz | 1 |
| B 2.12 | IT-Vernetzung | 4 |
| B 2.2 | Elektronische Vernetzung | 3 |

Umsetzung nach Slogestufen

| Slogestufe | Technische | Mensch | IT | Elektrische | Technische |
|------------|------------|--------|----|-------------|------------|
| A | 10 | 10 | 10 | 10 | 10 |
| B | 20 | 20 | 20 | 20 | 20 |
| C | 30 | 30 | 30 | 30 | 30 |
| D | 40 | 40 | 40 | 40 | 40 |
| E | 50 | 50 | 50 | 50 | 50 |
| F | 60 | 60 | 60 | 60 | 60 |
| G | 70 | 70 | 70 | 70 | 70 |

Umsetzungstatus

| Status | Technische | Mensch | IT | Elektrische | Technische |
|------------|------------|--------|----|-------------|------------|
| Entwickelt | 10 | 10 | 10 | 10 | 10 |
| In Arbeit | 20 | 20 | 20 | 20 | 20 |
| Bereit | 30 | 30 | 30 | 30 | 30 |
| Realisiert | 40 | 40 | 40 | 40 | 40 |

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 the risk assessment policy and approved by senior management. 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

| Impact | Number of Identified Risks | | | Total Count |
|-------------|----------------------------|---|---|-------------|
| | 0 | 1 | 2 | |
| Probability | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 0 | 0 |
| 2 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 3 | 20 |
| 4 | 0 | 0 | 0 | 2 |
| 5 | 0 | 0 | 0 | 3 |
| 6 | 0 | 0 | 0 | 3 |
| 7 | 0 | 0 | 3 | 5 |
| 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.

Zusammenfassung



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-Service Management, ...)?
 - Mieten oder kaufen?
 - Wie viel Support gewünscht?
 - Verhandlungen mit Herstellern...

Zusammenfassung I: Wesentliche Features

| Parameter | HiScout | verinice.PRO | i-dot 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 | ++ | - | 0 | ++ |
| Eigene Berichte | ++ | ++ | 0 | ++ |
| Handling / Einarbeitungszeit | - | ++ | 0 | + |
| Übersichten mit Statusanzeige (Cockpit) | + | 0 | + | ++ |
| 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) |

Zusammenfassung II: weitere Features

| Parameter | HiScout | verinice.PRO | i-doit Pro inkl. VIVA | CRISAM 5.0 |
|--|---|--|-------------------------|---|
| Server-Technologie ISO 2700x und IT- Grundschutz | Windows Server, SQL Server, ASP.NET + | Java (Tomcat) Postgres/My-SQL (auch als VMware-Appl.) + | Apache, MySQL, PHP + | Windows Server, SQL Server, ASP.NET + |
| 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 BS/IT-Grundschutz / ISO 27001

Datenschutz- und IT-Sicherheitsbeauftragter

frankenstein@hisolutions.com



Tool-Unterstützung IT-Grundschutz

Produktvergleich

Andreas Floß, Senior Consultant
Ronny Frankenstein, Senior Manager