



VdS Sicherheitsstandard 3473

Cyber-Security für kleine und mittlere
Unternehmen

Abbildung des VdS Standards in verinice

secianus

Sachverständige für Datenschutz und Informationssicherheit

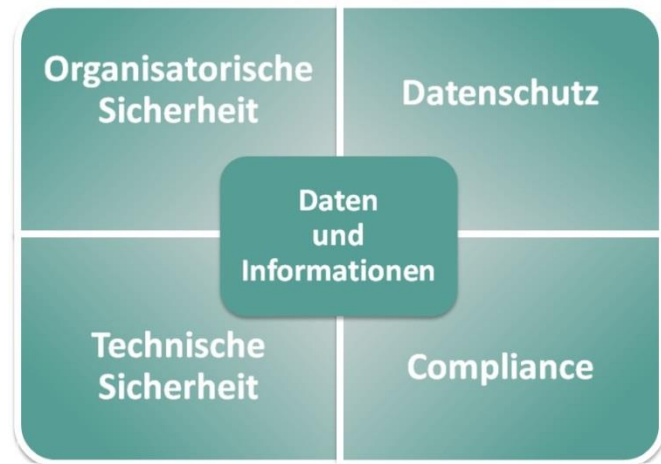


verinice.PARTNERS



Unsere Kernkompetenzen sehen wir in der ganzheitlichen Umsetzung der Informationssicherheit, die sich an den Gegebenheiten unserer Kunden anpasst.

Bei der Umsetzung unserer Kernkompetenzen setzen wir die Standards ISO 27001, Grundschutz/BSI, ISO 9001 ITIL, etc. zielorientierte Lösungen für unsere Kunden ein.





Vom Bundesamt für Sicherheit in der Informationstechnik zertifizierter

- Lead-Auditor für ISO 27001 auf Basis IT-Grundschutz
- IS-Revisor
- Prüfer für Kritis-Unternehmen gemäß §8a BSI-Gesetz.
- Zertifizierter VdS 3473 Berater

Tätig:

- Seit 1985 in der EDV
- Seit 2001 in der IT-Sicherheit
- Seit 2003 als Auditor
- Seit 2005 in der Informationssicherheit

Schwerpunkte:

- Behörden
- Industrie
- Telekommunikation
- SAP-Systeme

Ausgangslage

Informationssicherheitsnormen

- ISO 27001 native (Risikobasierend)
- ISO 27001 auf Basis IT-Grundschutz (Maßnahmenbasierend)
- PCI DSS
- MaRisk
- VDI/VDE2182 (Netzwerksicherheit)
- Standards und Verordnungen mit Sicherheitsanforderungen
 - ITIL, Cobit, IDW PS 330, SOX, Basel II
 - Datenschutzgrundverordnung



ISMS



Ein auf kleine und mittlere Unternehmen (KMU)
zugeschnittenes Verfahren für die Etablierung und
Aufrechterhaltung einer angemessenen
Informationssicherheit



VdS Schadenverhütung GmbH

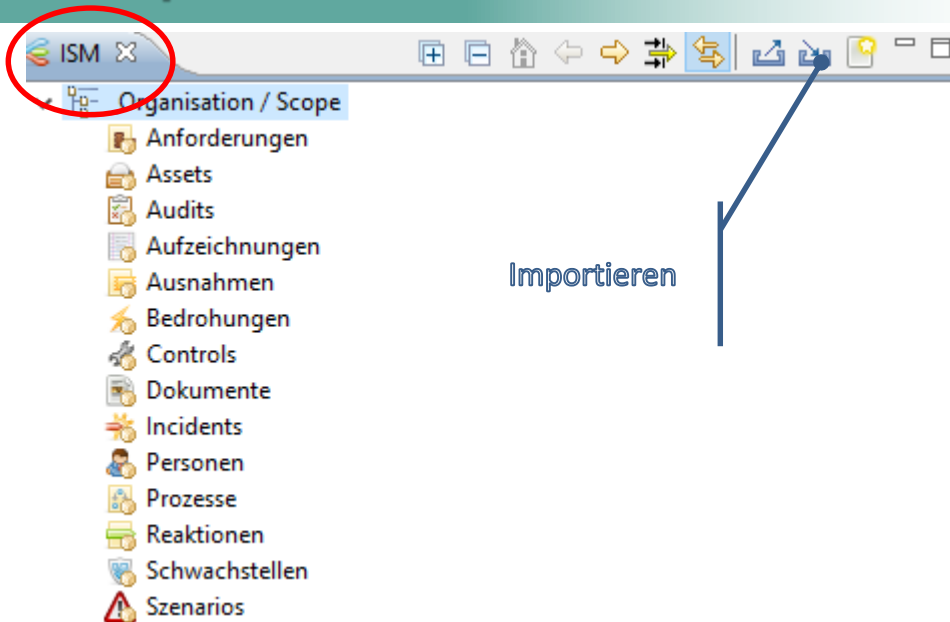
Der VdS Standard 3473



- Organisation der Informationssicherheit (ISMS)
- Leitlinie zur Informationssicherheit (IS-Leitlinie)
- Richtlinien zur Informationssicherheit (IS-Richtlinien)
- Personal
- Wissen
- Identifizieren kritischer IT-Ressourcen
- IT-Systeme
- Netzwerke und Verbindungen
- Mobile Datenträger
- Umgebung
- IT-Outsourcing und Cloud Computing
- Zugänge und Zugriffsrechte
- Datensicherung und Archivierung
- Störungen und Ausfälle
- Sicherheitsvorfälle



Import in verinice



The screenshot shows the ISM application interface. The title bar contains the text 'ISM' and a close button, which is circled in red. Below the title bar is a toolbar with various navigation icons. The main content area is titled 'Organisation / Scope' and contains a list of categories with corresponding icons: Anforderungen, Assets, Audits, Aufzeichnungen, Ausnahmen, Bedrohungen, Controls, Dokumente, Incidents, Personen, Prozesse, Reaktionen, Schwachstellen, and Szenarios. A blue arrow points from the 'Importieren' button in the toolbar to the word 'Importieren' written in the center of the screen.

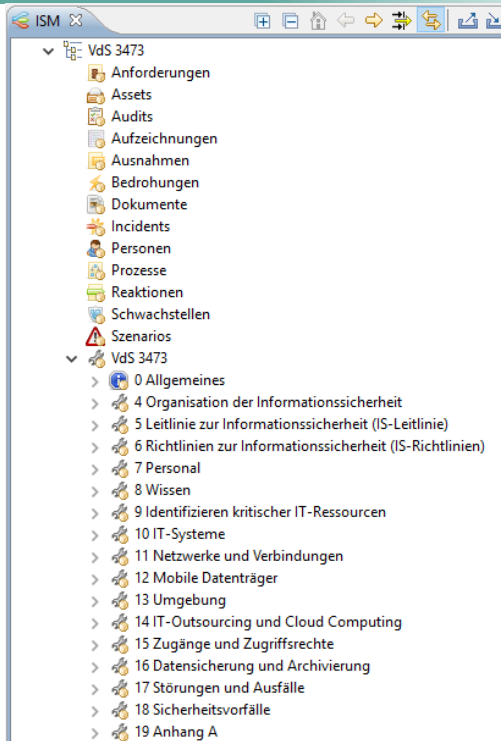
ISM

Organisation / Scope

- Anforderungen
- Assets
- Audits
- Aufzeichnungen
- Ausnahmen
- Bedrohungen
- Controls
- Dokumente
- Incidents
- Personen
- Prozesse
- Reaktionen
- Schwachstellen
- Szenarios

Importieren

Umsetzung in verinice





















The screenshot shows the Verinice ISM (Information Security Management) interface. The main window displays a tree view for a VdS 3473 audit plan. The tree structure is as follows:

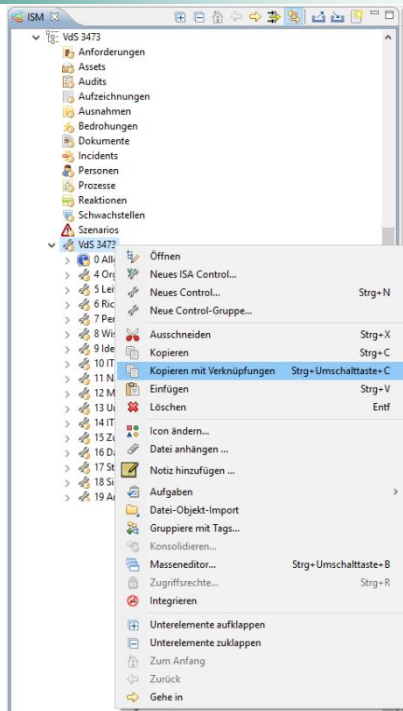
- ISM
- ▼ VdS 3473
 - Anforderungen
 - Assets
 - Audits
 - Aufzeichnungen
 - Ausnahmen
 - Bedrohungen
 - Dokumente
 - Incidents
 - Personen
 - Prozesse
 - Reaktionen
 - Schwachstellen
 - Szenarios
 - ▼ VdS 3473
 - > 0 Allgemeines
 - > 4 Organisation der Informationssicherheit
 - > 5 Leitlinie zur Informationssicherheit (IS-Leitlinie)
 - > 6 Richtlinien zur Informationssicherheit (IS-Richtlinien)
 - > 7 Personal
 - > 8 Wissen
 - > 9 Identifizieren kritischer IT-Ressourcen
 - > 10 IT-Systeme
 - > 11 Netzwerke und Verbindungen
 - > 12 Mobile Datenträger
 - > 13 Umgebung
 - > 14 IT-Outsourcing und Cloud Computing
 - > 15 Zugänge und Zugriffsrechte
 - > 16 Datensicherung und Archivierung
 - > 17 Störungen und Ausfälle
 - > 18 Sicherheitsvorfälle
 - > 19 Anhang A

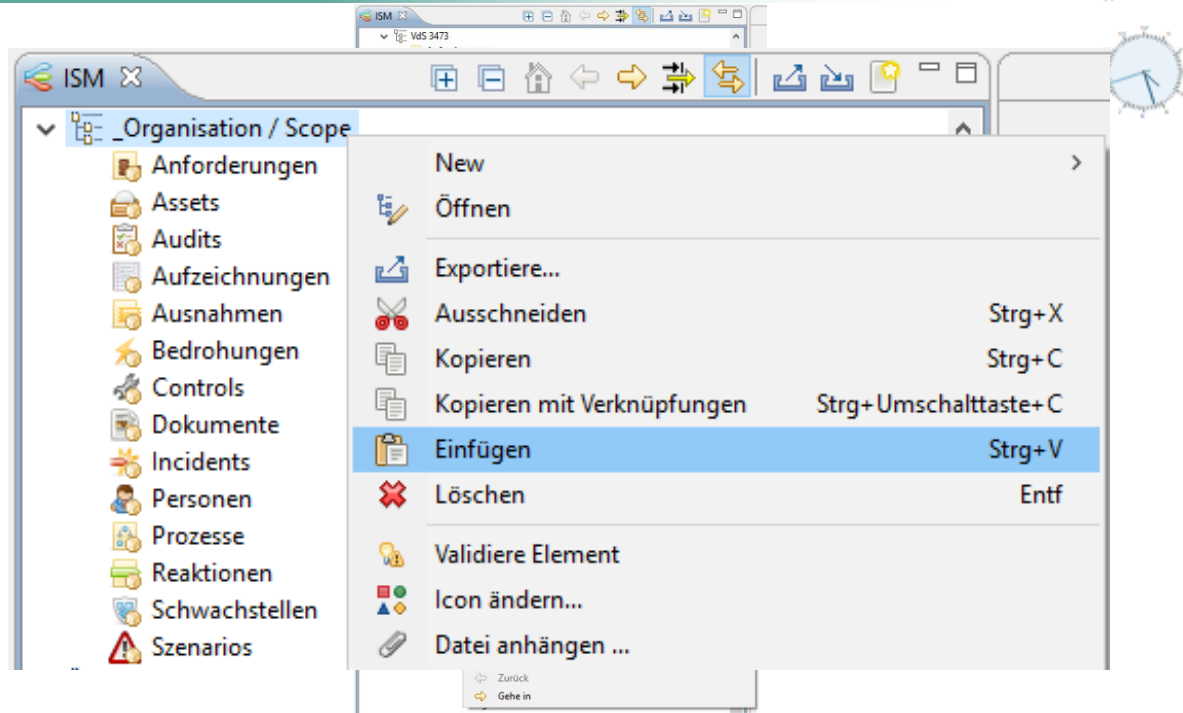
Umsetzung in verinice




























- ▼  VdS 3473
 - >  0 Allgemeines
 - >  4 Organisation der Informationssicherheit
 - >  5 Leitlinie zur Informationssicherheit (IS-Leitlinie)
 - >  6 Richtlinien zur Informationssicherheit (IS-Richtlinien)
 - >  7 Personal
 - >  8 Wissen
 - >  9 Identifizieren kritischer IT-Ressourcen
 - >  10 IT-Systeme
 - >  11 Netzwerke und Verbindungen
 - >  12 Mobile Datenträger
 - >  13 Umgebung
 - >  14 IT-Outsourcing und Cloud Computing
 - >  15 Zugänge und Zugriffsrechte
 - >  16 Datensicherung und Archivierung
 - >  17 Störungen und Ausfälle
 - >  18 Sicherheitsvorfälle
 - >  19 Anhang A

Integration in Sicherheitsmodell







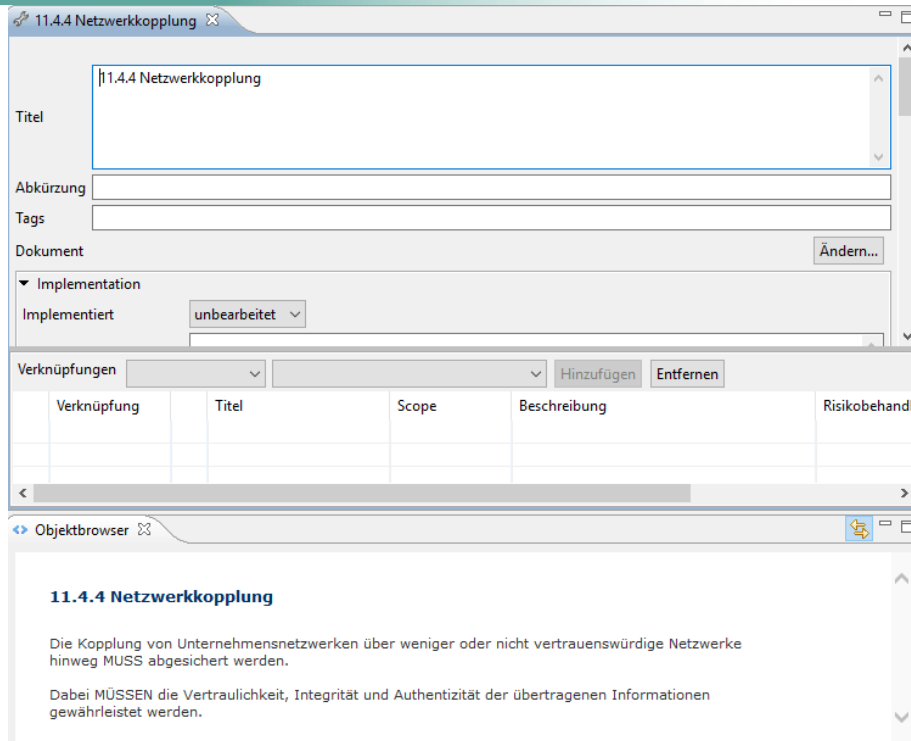


- ▼  VdS 3473
 - ▼  0 Allgemeines
 -  0.1 Motivation
 -  0.2 Geltungsbereich
 -  0.3 Anwendungshinweise
 -  0.4 Gültigkeit
 -  0.5 Normative Verweise
 -  0.6 Copyright
 - ▼  4 Organisation der Informationssicherheit
 - ▼  4.1 Verantwortlichkeiten
 -  4.1.1 Zuweisung und Dokumentation
 -  4.1.2 Funktionstrennungen
 -  4.1.3 Ressourcen
 -  4.1.4 Delegieren von Aufgaben
 -  4.2 Topmanagement
 -  4.3 Informationssicherheitsbeauftragter (ISB)
 -  4.4 Informationssicherheitsteam (IST)
 -  4.5 IT-Verantwortlicher
 -  4.6 Administratoren
 -  4.7 Vorgesetzte mit Personalverantwortung
 -  4.8 Personal
 -  4.9 Projektverantwortliche
 -  4.10 Lieferanten und sonstige Auftragnehmer
 - >  5 Leitlinie zur Informationssicherheit (IS-Leitlinie)
 - >  6 Richtlinien zur Informationssicherheit (IS-Richtlinien)



- ▼  11 Netzwerke und Verbindungen
 - ❗ 11.1 Dokumentation
 - ❗ 11.2 Aktive Netzwerkkomponenten
 - ❗ 11.3 Netzübergänge
- ▼  11.4 Basisschutz
 - ❗ 11.4.1 Netzwerkanschlüsse
 - ❗ 11.4.2 Segmentierung
 - ❗ 11.4.3 Fernzugriff
 - ❗ 11.4.4 Netzwerkkopplung
 - ❗ 11.5 Zusätzliche Maßnahmen für kritische Verbindungen

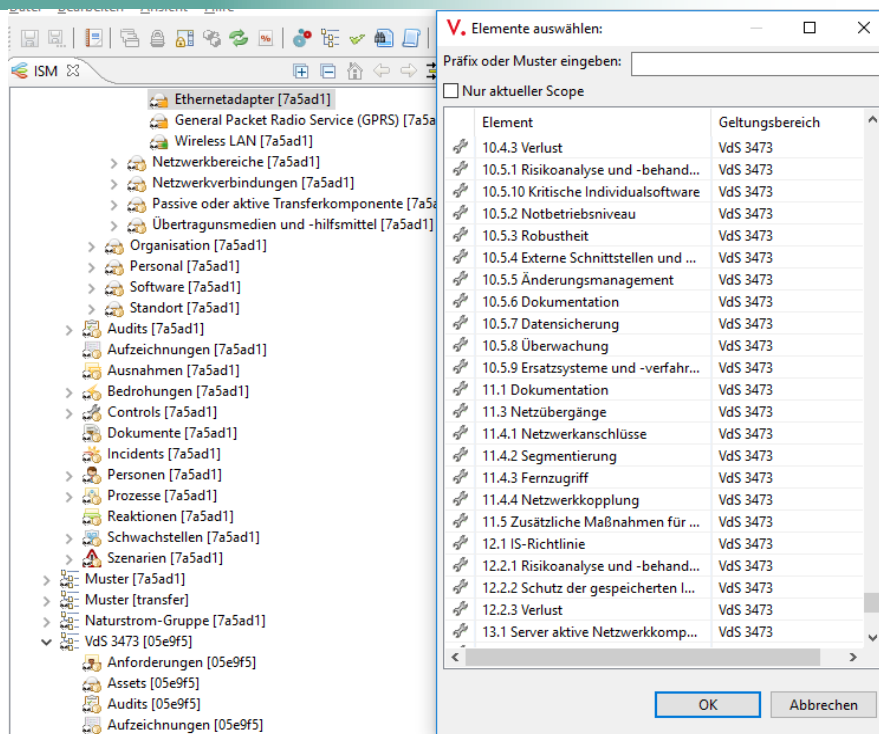
Umsetzung in verinice



The screenshot displays the Verinice software interface for configuring a network connection. The main window is titled '11.4.4 Netzwerkkopplung'. It features several input fields: 'Titel' (containing '11.4.4 Netzwerkkopplung'), 'Abkürzung', and 'Tags'. Below these is a 'Dokument' field with an 'Ändern...' button. The 'Implementation' section is expanded, showing 'Implementiert' set to 'unbearbeitet'. A 'Verknüpfungen' section includes a table with columns for 'Verknüpfung', 'Titel', 'Scope', 'Beschreibung', and 'Risikobehandl'. Below the table are 'Hinzufügen' and 'Entfernen' buttons. At the bottom, an 'Objektbrowser' pane shows the selected object '11.4.4 Netzwerkkopplung' with a detailed description: 'Die Kopplung von Unternehmensnetzwerken über weniger oder nicht vertrauenswürdige Netzwerke hinweg MUSS abgesichert werden. Dabei MÜSSEN die Vertraulichkeit, Integrität und Authentizität der übertragenen Informationen gewährleistet werden.'

| Verknüpfung | Titel | Scope | Beschreibung | Risikobehandl |
|-------------|-------|-------|--------------|---------------|
| | | | | |
| | | | | |

Umsetzung in verinice



The screenshot shows the verinice software interface. On the left is a tree view of a project structure. On the right is a dialog box titled 'V. Elemente auswählen:' (Select elements) with a table of elements and their validity ranges.

Tree View Structure:

- Ethernetadapter [7a5ad1]
- General Packet Radio Service (GPRS) [7a5ad1]
- Wireless LAN [7a5ad1]
- Netzwerkbereiche [7a5ad1]
- Netzwerkverbindungen [7a5ad1]
- Passive oder aktive Transferkomponente [7a5ad1]
- Übertragungsmedien und -hilfsmittel [7a5ad1]
- Organisation [7a5ad1]
- Personal [7a5ad1]
- Software [7a5ad1]
- Standort [7a5ad1]
- Audits [7a5ad1]
- Aufzeichnungen [7a5ad1]
- Ausnahmen [7a5ad1]
- Bedrohungen [7a5ad1]
- Controls [7a5ad1]
- Dokumente [7a5ad1]
- Incidents [7a5ad1]
- Personen [7a5ad1]
- Prozesse [7a5ad1]
- Reaktionen [7a5ad1]
- Schwachstellen [7a5ad1]
- Szenarien [7a5ad1]
- Muster [7a5ad1]
- Muster [transfer]
- Naturstrom-Gruppe [7a5ad1]
- VdS 3473 [05e9f5]
- Anforderungen [05e9f5]
- Assets [05e9f5]
- Audits [05e9f5]
- Aufzeichnungen [05e9f5]

Dialog Box 'V. Elemente auswählen:'

Präfix oder Muster eingeben:

Nur aktueller Scope

| Element | Geltungsbereich |
|---------------------------------------|-----------------|
| 10.4.3 Verlust | VdS 3473 |
| 10.5.1 Risikoanalyse und -behand... | VdS 3473 |
| 10.5.10 Kritische Individualsoftware | VdS 3473 |
| 10.5.2 Notbetriebsniveau | VdS 3473 |
| 10.5.3 Robustheit | VdS 3473 |
| 10.5.4 Externe Schnittstellen und ... | VdS 3473 |
| 10.5.5 Änderungsmanagement | VdS 3473 |
| 10.5.6 Dokumentation | VdS 3473 |
| 10.5.7 Datensicherung | VdS 3473 |
| 10.5.8 Überwachung | VdS 3473 |
| 10.5.9 Ersatzsysteme und -verfahr... | VdS 3473 |
| 11.1 Dokumentation | VdS 3473 |
| 11.3 Netzübergänge | VdS 3473 |
| 11.4.1 Netzwerkanschlüsse | VdS 3473 |
| 11.4.2 Segmentierung | VdS 3473 |
| 11.4.3 Fernzugriff | VdS 3473 |
| 11.4.4 Netzwerkkopplung | VdS 3473 |
| 11.5 Zusätzliche Maßnahmen für ... | VdS 3473 |
| 12.1 IS-Richtlinie | VdS 3473 |
| 12.2.1 Risikoanalyse und -behand... | VdS 3473 |
| 12.2.2 Schutz der gespeicherten I... | VdS 3473 |
| 12.2.3 Verlust | VdS 3473 |
| 13.1 Server aktive Netzwerkkomp... | VdS 3473 |

Buttons: OK, Abbrechen

V. Report



Report erzeugen

Erstellen Sie einen Report mit den Daten in verinice. Reports können schädlichen Code oder andere Sicherheitsrisiken enthalten. Verwenden Sie ausschließlich Reports von Urhebern, denen Sie vertrauen.

| | |
|-----------------------------------|--|
| Report auswählen: | (S) ISM: Assetinventar |
| Geltungsbereich: | (S) ISM: Assetinventar (S) ISM: Control-Maturity-Überblick (S) ISM: Erklärung zur Anwendbarkeit (S) ISM: Export: Anforderungen (S) ISM: Export: Aufgaben (de) (S) ISM: Export: Aufgaben (en) (S) ISM: Export: Aufzeichnungen (S) ISM: Export: Ausnahmen (S) ISM: Export: Bedrohungen (S) ISM: Export: Dokumente (S) ISM: Export: Personen (S) ISM: Export: Prozesse (S) ISM: Export: Reaktionen (S) ISM: Export: Schwachstellen (S) ISM: Export: Szenarios (S) ISM: Export: Vorfälle (S) ISM: IS-Risikobeurteilung (de) (S) ISM: IS-Risikobeurteilung (en) (S) ISM: Risikobehandlung (de) (S) ISM: Risikobehandlung (en) (S) ISM: Sofortmeldung (VV BSIG) (S) ISM: Statistische Gesamtmeldung (VV BSIG) |
| Ausgabeformat | |
| Ausgabedatei | |
| Datum im Dateinamen | |
| Immer dieses Verzeichnis benutzen | |

Kontakt:



SECIANUS GmbH & Co. KG

Hanserauweg 3
D-92342 Freystadt

Tel.: +49 (0) 911 39 38 068

Fax: +49 (0) 911 39 38 069

eMail: info@secianus.de

Internet: www.secianus.de