verinice.

ISMS in der Praxis umsetzen

Alexander Koderman, CISA

SerNet GmbH

SerNet GmbH

- gegründet 1997
- Büros in Göttingen, Berlin, Nürnberg, Menlo Park
- Informationssicherheit und Datenschutz
- spezialisiert auf Open Source Software
- Netzwerksicherheit für Industrie und öffentl. Hand
- Zertifizierungen und Audits
- IT-Grundschutz und ISO 27001
- „Old Economy“, kein Risiko-Kapital, keine Bank-Kredite
- über 700 Bestandskunden in DE, EU, US

Alexander Koderman

- BSI lizenzierter Auditor für ISO 27001 nach IT-Grundschutz
- ISO 27001 LEad Auditor (KPMG)
- Certified Information Systems Auditor (CISA)
- Mitglied im internationalen Berufsverband der IS-Prüfer ISACA
- RHCE, NCLP, LPIC Level 2, IBM Certified Solution Expert DB2
- Auditpraxis: Organisationen von 10 bis 10.000 Mitarbeitern

ISO 27001 PDCA Zyklus

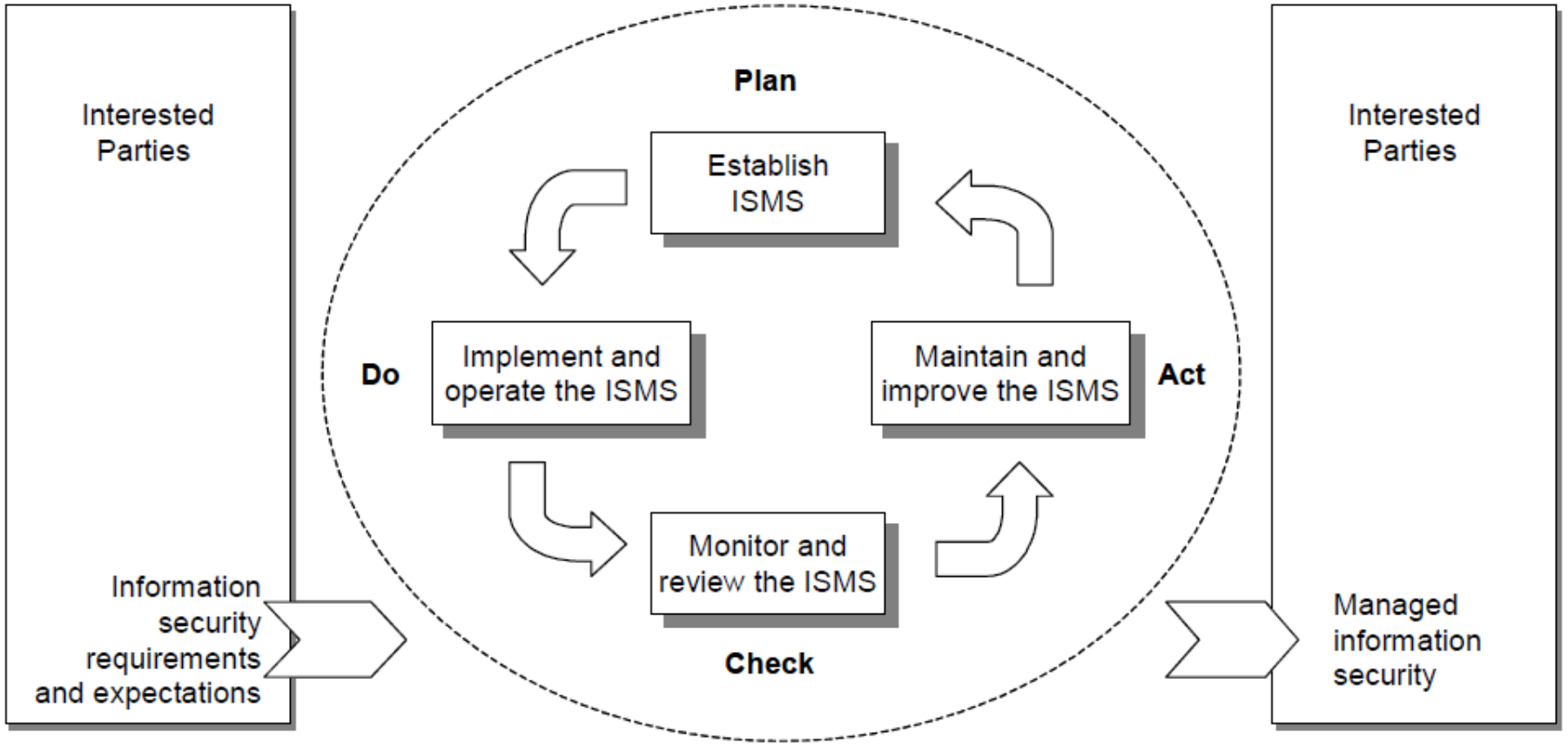
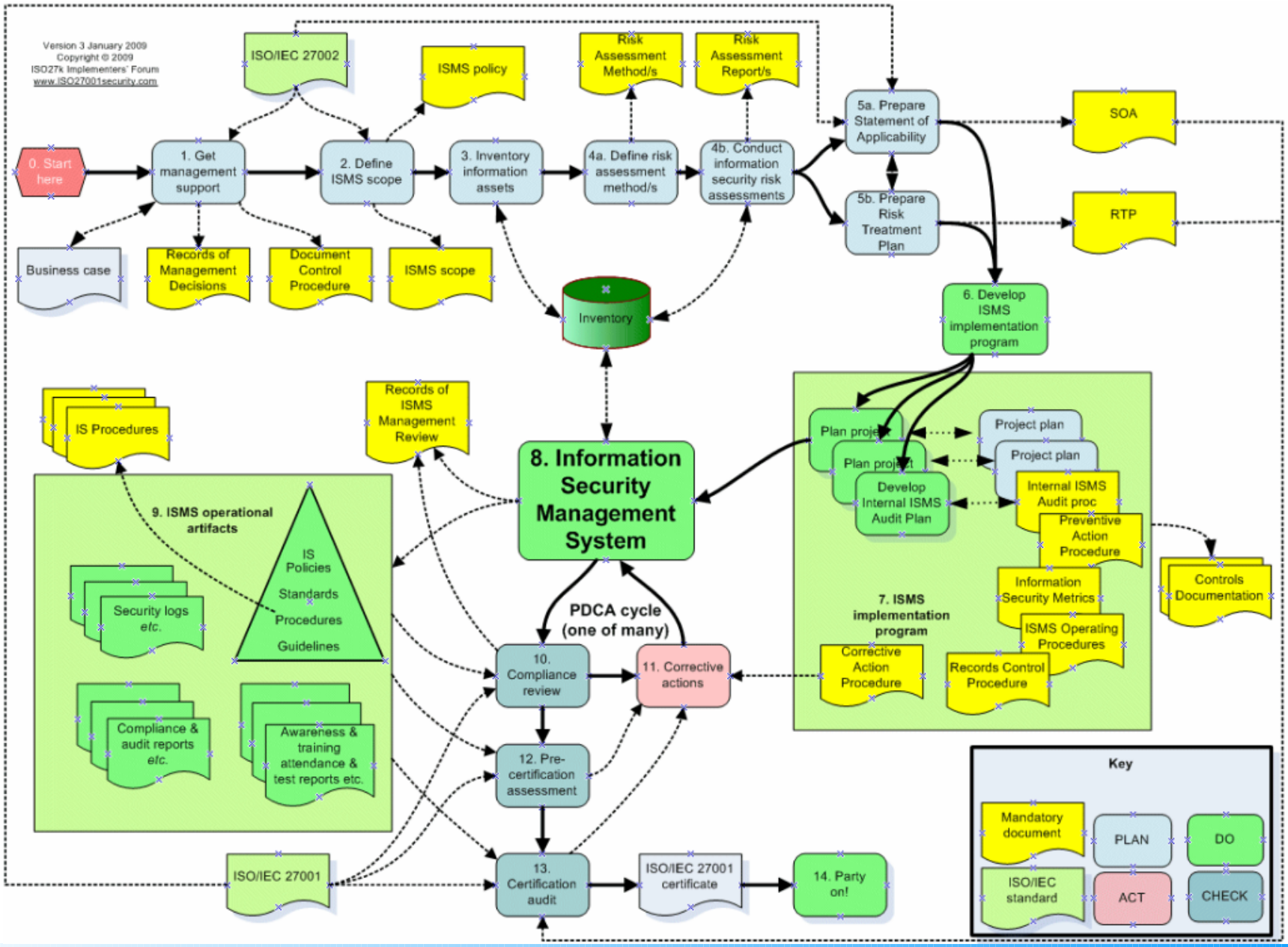


Figure 1 — PDCA model applied to ISMS processes



Anforderungen

- IDW PS 330 / FAIT 1 / PS 9.330.1
- ISO 27001 / 27002
- IT-Grundschutz
- CoBIT

Was macht die IT eigentlich den ganzen Tag?

- Zutrittsschutz
- Zugriffsschutz
- Funktionstrennung
- Datensicherungskonzept
- Virenschutzkonzept
- internes Kontrollsystem
- ...

Was macht die IT eigentlich den ganzen Tag?

- Zutrittsschutz
- Zugriffsschutz
- Funktionstrennung
- Datensicherungskonzept
- Virenschutzkonzept
- internes Kontrollsystem
- ...
- => Informations-*Sicherheitsmanagement*

Was ist IS-Management?

- „Die große Herausforderung besteht darin, in der eigenen Institution ein ISMS zu etablieren, das nicht nur hilft, die gesteckten Sicherheitsziele zu erreichen, sondern auch noch möglichst ***kostengünstig*** und ***wirtschaftlich*** ist.“

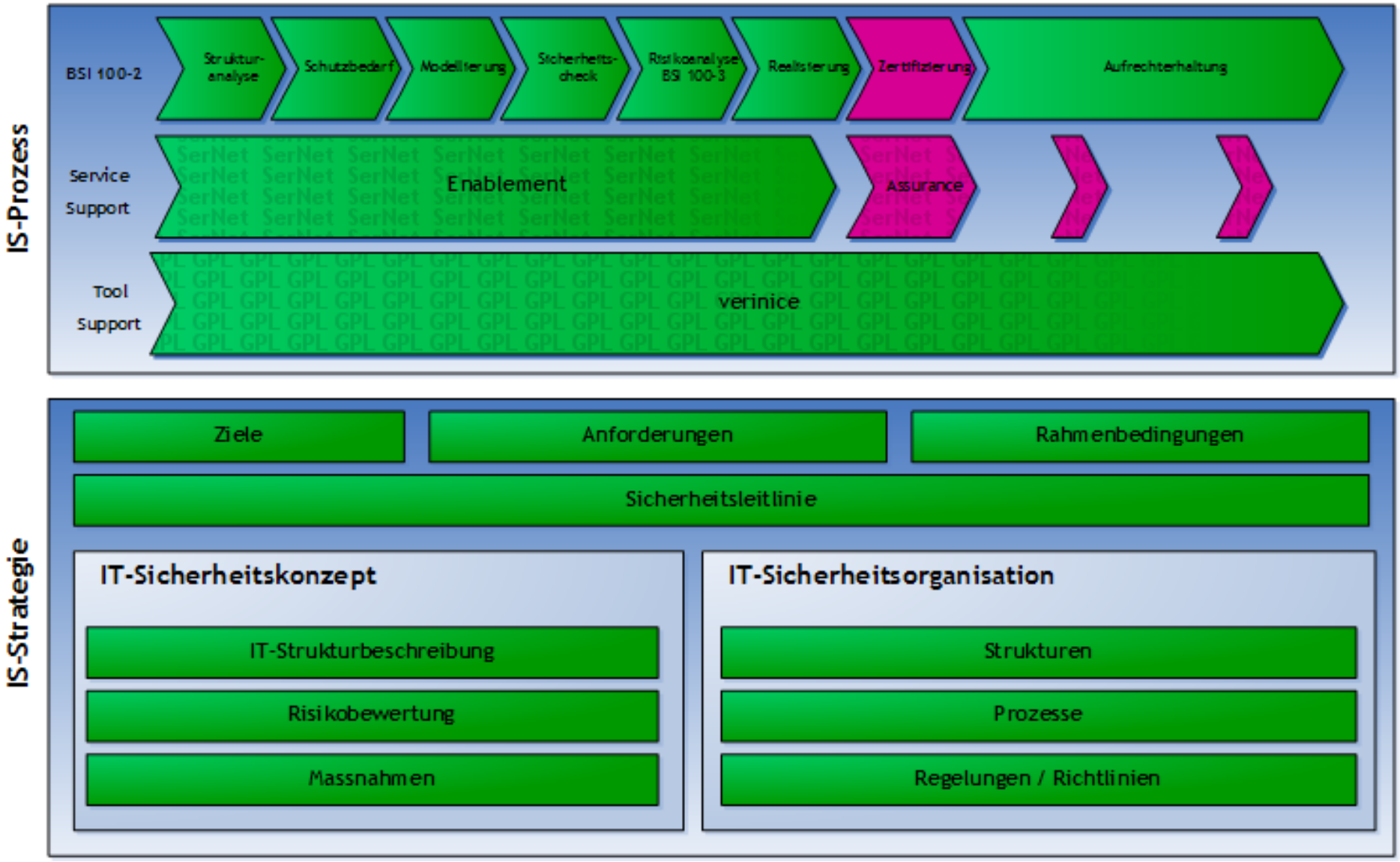
  - BSI Standard 100-1

Informationssicherheit

- ...Informationen sind wertvoll für eine Organisation und müssen deshalb in geeigneter Weise geschützt werden
- ... sollten deshalb unabhängig von ihrer Erscheinungsform sowie Art der Nutzung und Speicherung *immer angemessen* geschützt werden

ISO/IEC 27002, Einleitung

ISMS nach BSI 100-1



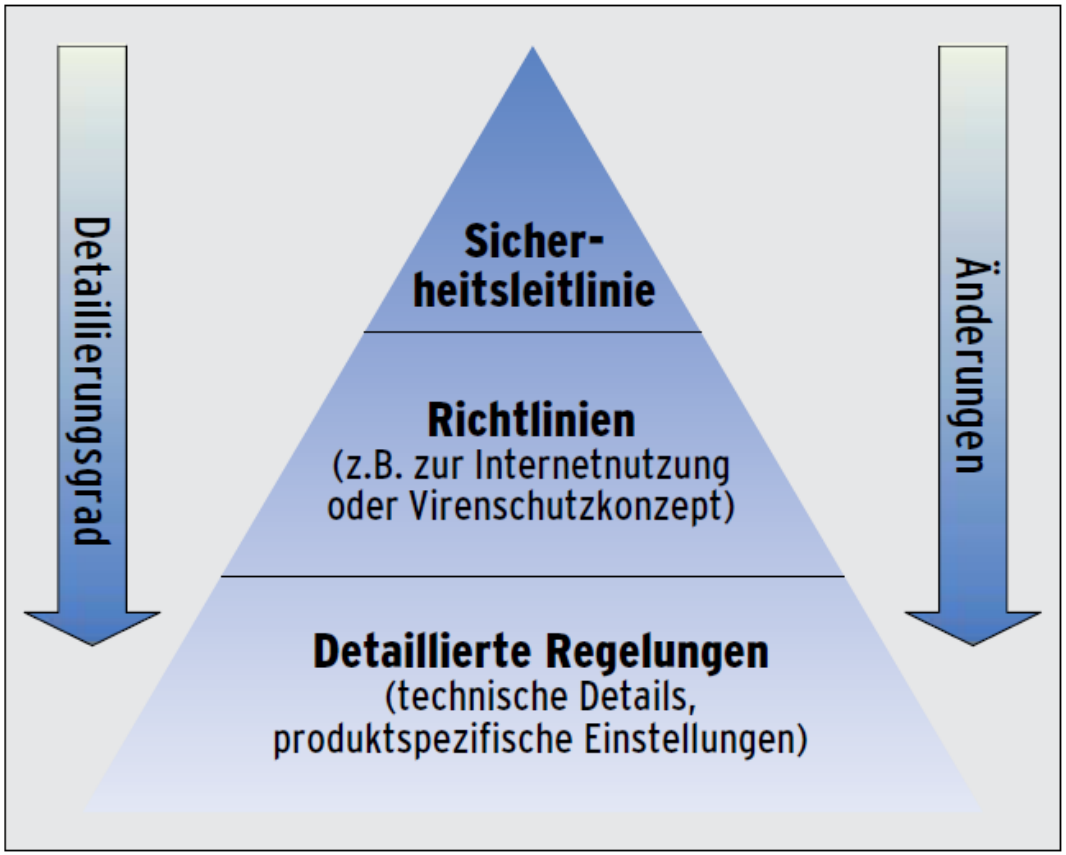
Referenzdokumente

- **IS-Organisation:**
  - IS-Richtlinien (A.0)
- **IS-Konzept**
  - IS-Strukturanalyse (A.1)
  - Schutzbedarfsfeststellung (A.2)
  - Modellierung des IT-Verbunds (A.3)
  - Ergebnis des Basis-Sicherheitschecks (A.4)
  - Ergänzende Sicherheitsanalyse (A.5)
  - Risikoanalyse (A.6)

- **IS-Richtlinien (A.0)**
  - IS-Leitlinie
  - Richtlinie zur Risikoanalyse
    (siehe 100-2, S. 143, & 100-1, S. 27)
  - Richtlinie zur Lenkung von Dokumenten und Aufzeichnungen
    (s. 100-1, S. 20 & M 2.201)
  - Richtlinie zur internen ISMS-Auditierung (Auditierung des Managementsystems für Informationssicherheit)
    (s. 100-1, S. 18)
  - Richtlinie zur Lenkung von Korrektur- und Vorbeugungsmaßnahmen
    (s. 100-1, S. 25)

IS-Organisation

- Format und Freigabeverfahren von Richtlinien anpassen an Detaillierungsgrad und Änderungshäufigkeit:



Richtlinien

- **Beispiel für mögliche Struktur übriger Richtlinien**
  - Benutzerrichtlinie
  - Administrator-Richtlinie
  - Datensicherungskonzept
  - Kryptokonzept
  - Outsourcing-Richtlinie
  - Virenschutzkonzept
  - Richtlinie Sicherheitsgateway
  - Sicherheitsrichtlinie für Router und Switches
  - Notfallvorsorgekonzept
  - Notfallhandbuch
  - Geschäftsfortführungsplan

verinice.

- Open Source
- plattformunabhängig
- Import der IT-Grundschutzkataloge
- Unterstützung der Vorgehensweise nach BSI 100-2
- Such- und Filterfunktionen
- anpassungsfähige Eingabemasken
- Audit-Praxis

verinice. / verinice.PRO

Zentrales IS-Repository		☑
Zentrale Dokumentenablage		☑
Fernzugriff		☑
Berechtigungskonzept		☑
Sichere Verbindung (SSL)		☑
Web-basierter Realisierungsplan		☑
Mailbenachrichtigung		☑
Mehrbenutzerfähigkeit		☑
Externe Datenbank (Postgres / Oracle)		☑
Directory-Anbindung (LDAP / AD)		☑
Import / Export / Synchronisierung	☑	☑
ISO 27001	☑	☑
Risikoanalyse nach ISO 27005	☑	☑
IT-Grundschutz	☑	☑
Import eigener Kataloge	☑	☑
Plattformübergreifend	☑	☑
Offener Sourcecode	☑	☑
BIRT Reporting	☑	☑

Distribution

- Verinice Client
  - Download von: http://verinice.org oder http://v.de
- Verinice Server
  - als Server oder VMWare Appliance
  - integriert in vorhandenen Applikationsserver (Tomcat, Websphere...)
  - Subskription / Support verfügbar über SerNet
- Source Code
  - vollständig unter GPLv3

Danke für Eure Aufmerksamkeit!

verinice.®

http://www.verinice.org

verinice@sernet.de

SerNet GmbH
Bahnhofsallee 1b
37081 Göttingen
Tel: +49 -551-370000-0
Fax: +49 -551-370000-9

Schützenstr. 18
10117 Berlin
+49 -30 -5 779 779-0
+49 -30 -5 779 779-9

http://www.SerNet.DE