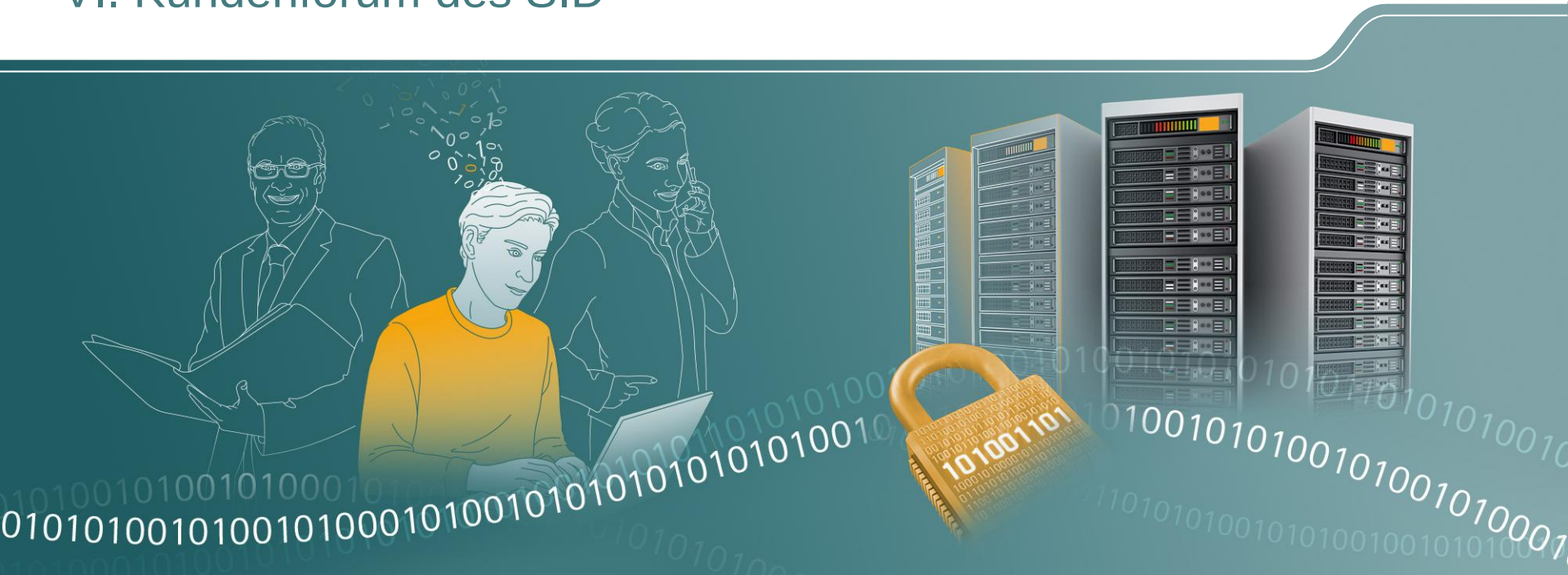
STAATSBETRIEB
SÄCHSISCHE
INFORMATIK DIENSTE

Freistaat
SACHSEN

Informationssicherheit im Fokus

VI. Kundenforum des SID



Agenda

1. Lage
2. Struktur
3. Konzept
4. Haltung

Aus den Meldungen

Fokus: Sachsen

- Notebook verloren
- Switch gestört
- Phishing-Welle erkannt
- DDoS-Angriff abgewehrt
- Verschlüsselungstrojaner unschädlich gemacht
- Rechnungsbetrug aufgedeckt
- Freie Softwarebibliotheken verunreinigt
- Penetrationstest durchgeführt
- Sicherheitslücken in Hardware überprüft
- Sicherheitslücken in Software geschlossen

Aus den Meldungen

Fokus: Europa

Ein gutes Lagebild...

…ist der Anfang von Allem

- Ziel: Klares, handlungsleitendes Lagebild auf regionaler, nationaler und EU-Ebene.
- Warum? Dranbleiben! Vor die Lage kommen!

- Aktuelle Aktivitäten:
  - Abstimmungen der Länder zur Vereinheitlichung der Metadaten (Strukturmodell, ggf. Datenmodell)
  - Sächsische Meldepflichten-VO in Erarbeitung bzw. Abstimmung
  - Revision des Formulars für Meldungen an das SAX.CERT

Ein gutes Lagebild…

…entsteht durch aktives Meldeverhalten

Vorfalldaten

Kurzbezeichnung des Vorfalls *

Bsp.: DDoS_SK_250804

Beschreibung des Sachverhalts

Einordnung nach § 15 (Stellenübergreifende Meldepflichten) oder § 16 Absatz 1 Satz 2 (Meldepflichten der staatlichen Stellen) des
Sächsisches Informationssicherheitsgesetz – SächsISichG *

Beantwortung zentraler W-Fragen

Kategorisierung

Um welche Art von Vorfall handelt es sich? (Mehrfachauswahl möglich) *

- ☐ Ransomware
- ☐ DDoS
- ☐ Störung
- ☐ Drohbrief
- ☐ Einbruch
- ☐ Datenabfluss
- ☐ Diebstahl
- ☐ Manipulation
- ☐ unberechtigte Nutzung
- ☐ Datenmissbrauch
- ☐ Schadprogramm
- ☐ Datenverlust
- ☐ Social Engineering
- ☐ Naturgewalten
- ☐ Geräteverlust
- ☐ Anderer Vorfall

Anzahl max. betroffener Personen *

Anzahl max. betroffener kritischer Prozesse *

Vorfall ist *

Bitte auswählen

Schäden sind *

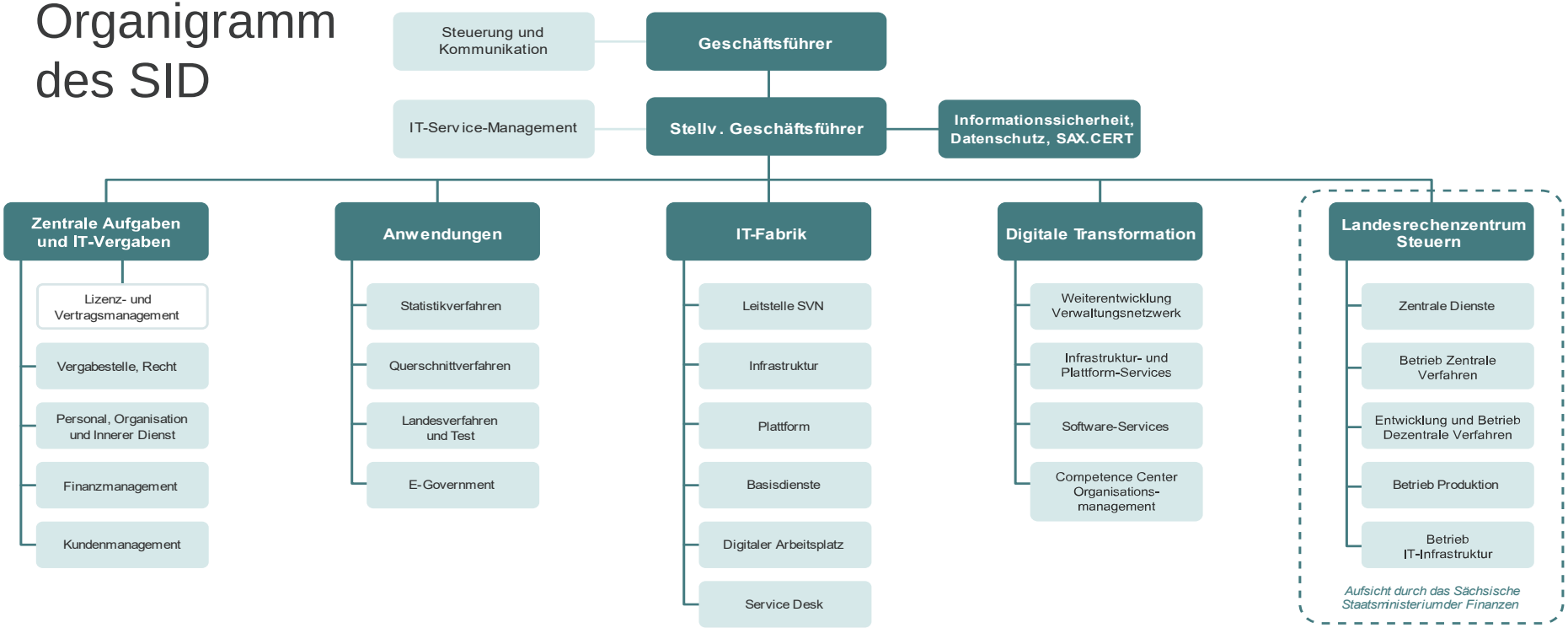
Bitte auswählen

Getroffene Maßnahme(n) *

Agenda

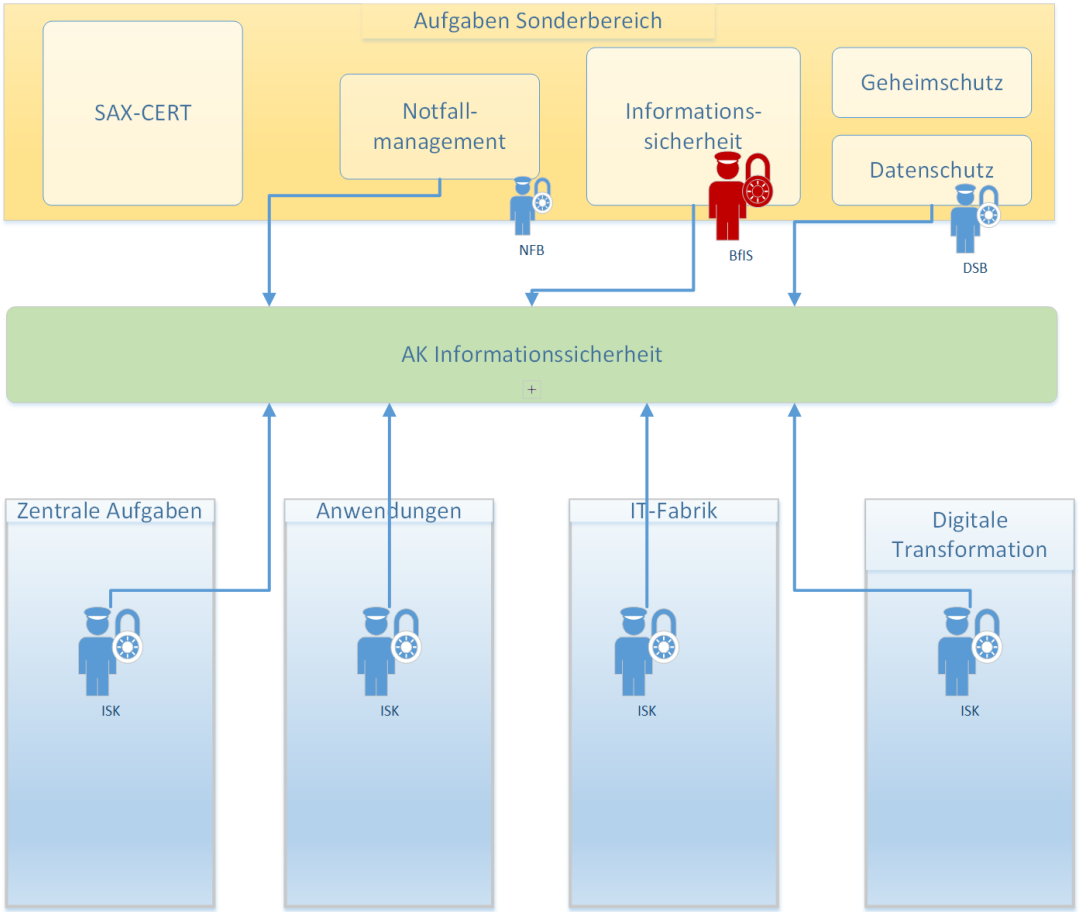
1. Lage
2. Struktur
3. Konzept
4. Haltung

Organigramm des SID



ISM SID

- Integriert
- Vernetzt
- Penetrant



§ 6
Sicherheitsnotfallteam

(1) [1]Das Sicherheitsnotfallteam ist im Staatsbetrieb Sächsische Informatik Dienste angesiedelt. [2]Aufgaben des Sicherheitsnotfallteams sind

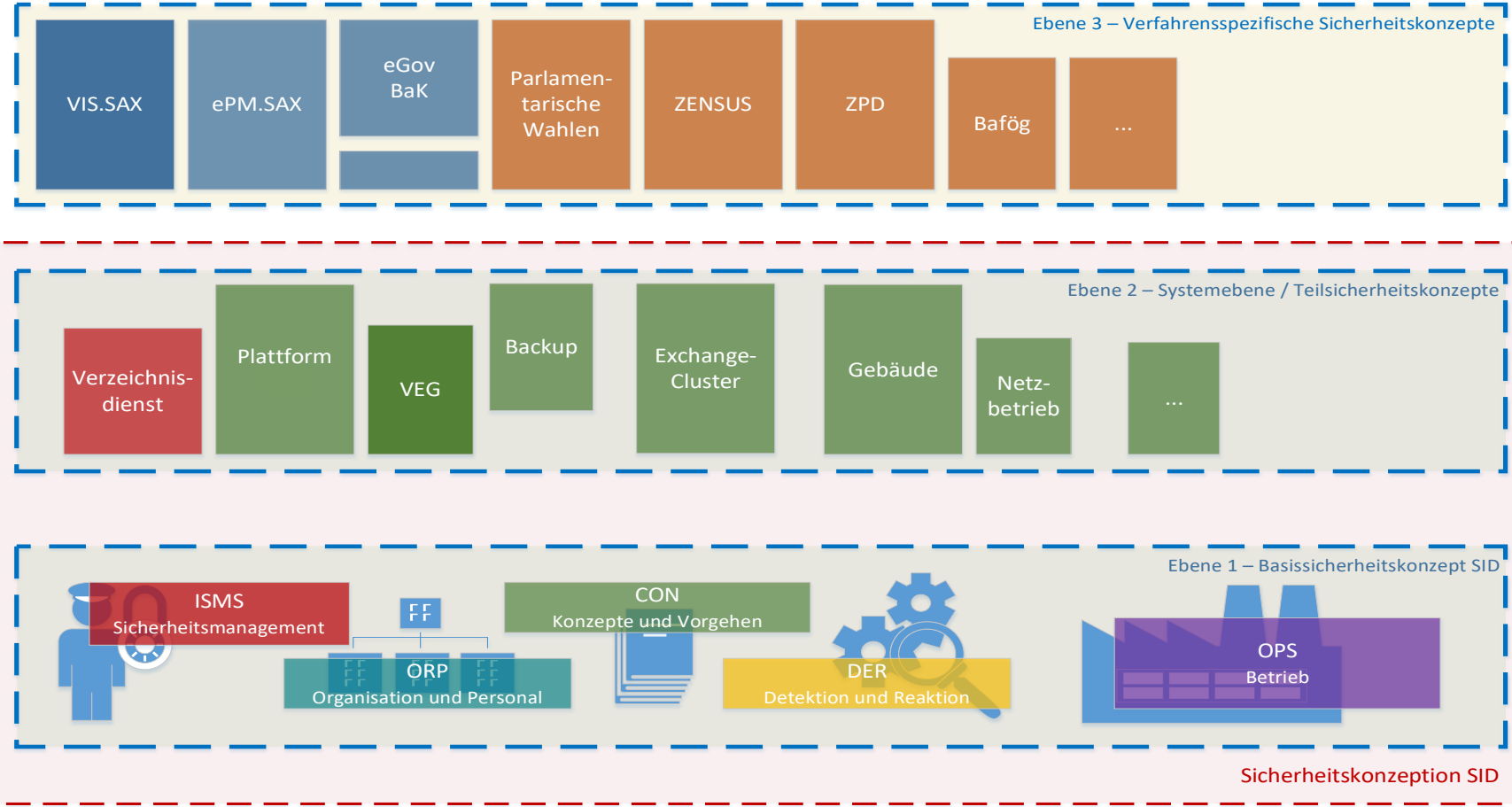
1. die Wahrnehmung der Aufgaben des Computer-Notfallteams nach Artikel 10 und 11 der Richtlinie (EU) 2022/2555 für die staatlichen Stellen,
2. das Aufzeigen von Lösungen bei konkreten Sicherheitsereignissen oder -vorfällen,
3. die Prüfung auf Risiken im Betrieb von informationstechnischen Systemen und die Unterstützung bei ihrer Beseitigung,
4. die Information zu Sicherheitslücken,
5. die Erfassung und Analyse der Lage der Informationssicherheit sowie die Erstellung daraus abgeleiteter Empfehlungen,
6. die Wahrnehmung der zentralen Meldestelle im Sinne des BSI-Gesetzes,
7. die Wahrnehmung der zentralen Meldestelle im Sinne des IT-Planungsrates im Verwaltungs-CERT-Verbund,
8. die Mitwirkung bei der technischen und technologischen Koordinierung der Informationssicherheit in den staatlichen und nicht-staatlichen Stellen sowie
9. die regelmäßige Information über die Lage der Informationssicherheit im Freistaat Sachsen.

[3]Das Sicherheitsnotfallteam unterstützt die Beauftragte oder den Beauftragten für Informationssicherheit des Landes und die Beauftragten für Informationssicherheit der staatlichen oder nicht-staatlichen Stellen des Freistaates Sachsen in technischen Sicherheitsfragen.

Agenda

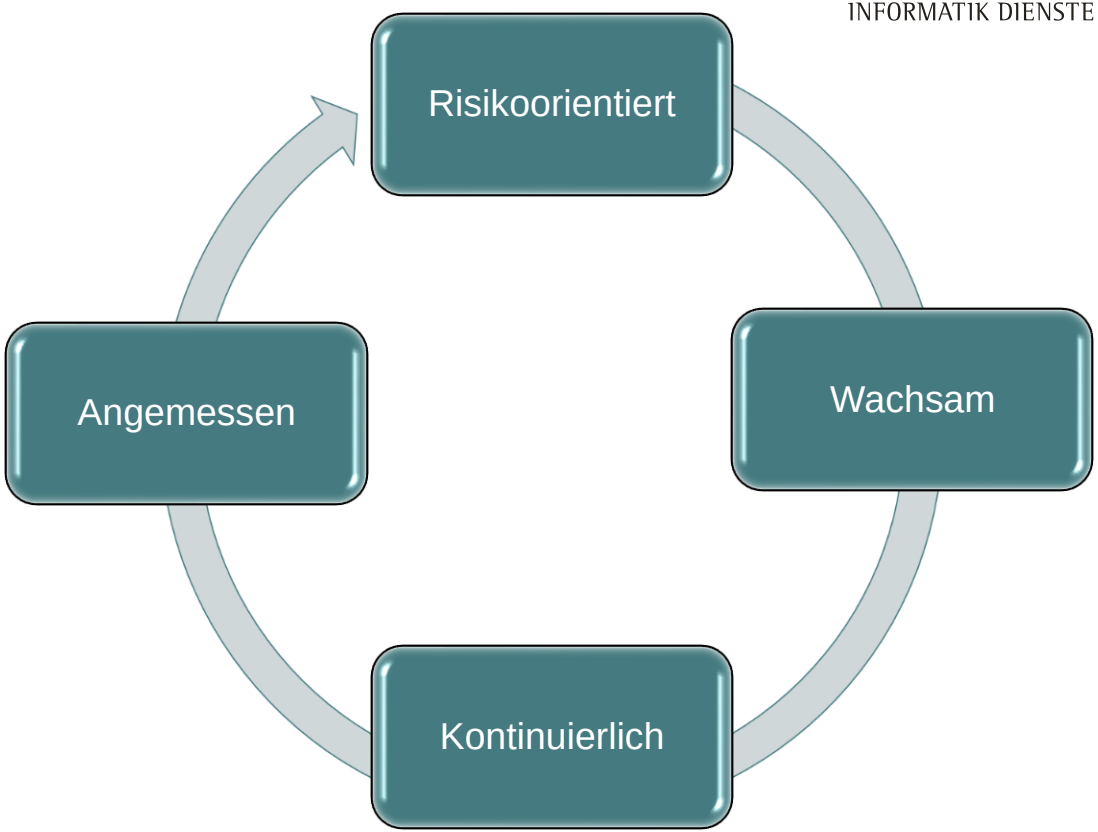
1. Lage
2. Struktur
3. Konzept
4. Haltung

Ebenenmodell - Sicherheitskonzeption des SID



Agenda

1. Lage
2. Struktur
3. Konzept
4. Haltung


Risikoorientiert
Wachsam
Kontinuierlich
Angemessen

Das Management von Abhängigkeiten ist auch eine Haltungsfrage

- Die Systeme sind komplex und werden komplexer.
- Unsere Abhängigkeit vom Funktionieren der Systeme ist hoch und steigt.
- Unsere Abhängigkeit vom Funktionieren von Netzen, Plattformen, Verfahren, Diensten, Entwicklungsbibliotheken, Softwaremodulen, etc. ist hoch und steigt.
- Den Cyber Resilience Act der EU-KOM als Weckruf verstehen.
- Das Management von Abhängigkeiten beginnt beim Dependency Tracking.
- Software-Stücklisten / Software Bills of Materials sind ein mächtiges Werkzeug.

Informationssicherheit für die Behördenleitung

Einführung in das E-Learning

In Kürze verfügbar!

Inhalt dieses E-Books

- Warum ist Informationssicherheit wichtig?
- Was ist Informationssicherheit?
- Was ist unter einem Informationssicherheits-managementsystem zu verstehen?
- Zusammenfassung
- Quiz

Informationssicherheit im Fokus

Danke für Ihre Aufmerksamkeit! Diskussion?

Sie finden uns unter:
www.sid.sachsen.de
Dresdner Straße 78 A
01445 Radebeul

Dr. Steffen Gilge
steffen.gilge@sid.sachsen.de
Tel.: 0351 3264 6220
Kein Fax