Stand der Technik bei Zero Trust

Der Automatisierungshebel für die Informationssicherheit

Bundesamt
für Sicherheit in der
Informationstechnik

Karger, Sandra

Referatsleitung – Stand der Technik

Herausforderungen bei Zero Trust

Paradigmenwechsel auf mehreren Ebenen

Microsegmentierung

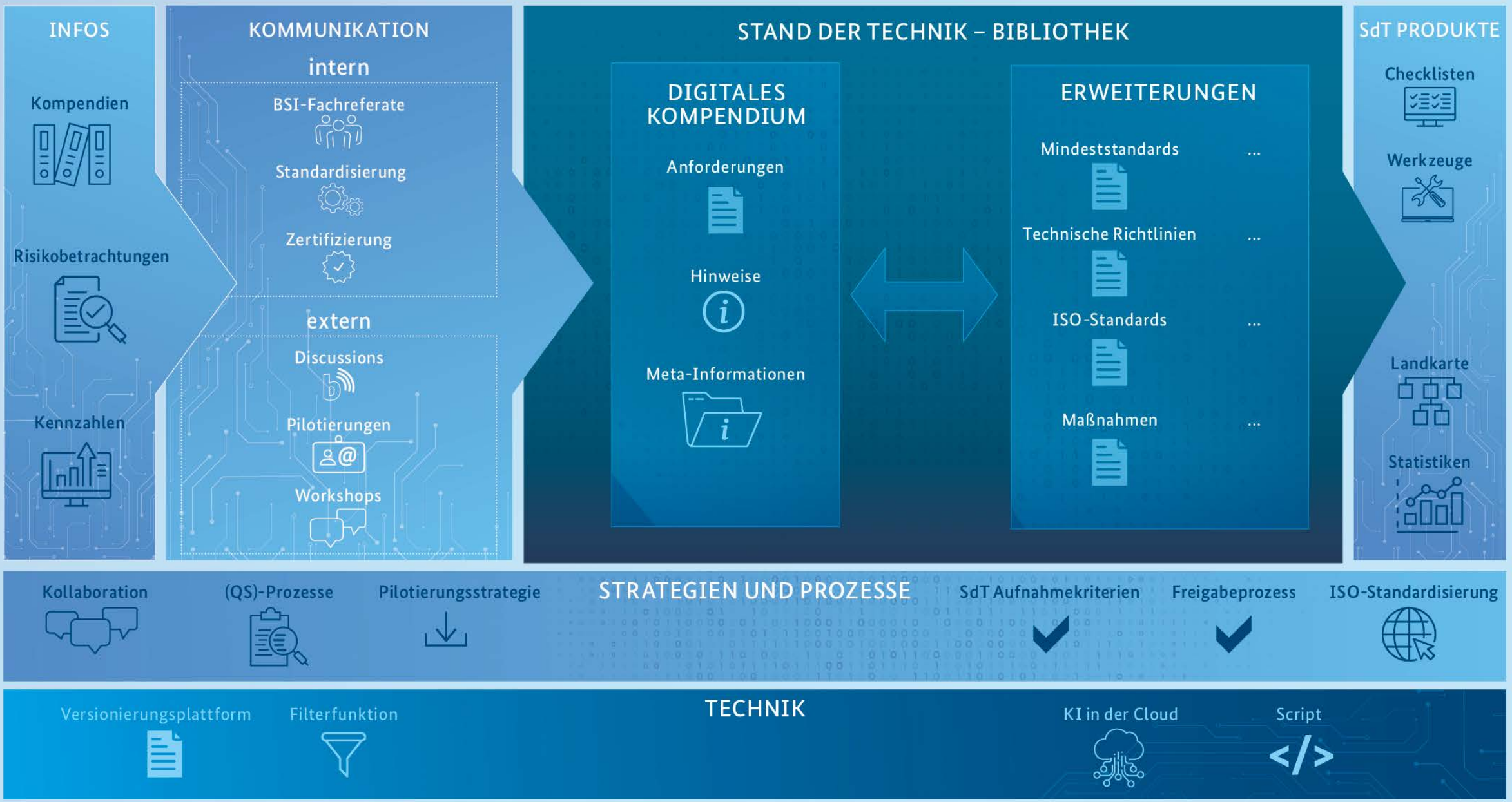
Echtzeitreaktion

DevSecOps-Cycle

Intelligente Sicherheitskonfiguration

Wie kann der Grundschutz zum Automatisierungshebel werden?

ARCHITEKTURBILD STAND DER TECHNIK https://github.com/BSI-Bund/Stand-der-Technik-Bibliothek



Struktur für Anforderungen durch Satzschablonen

Von Prosa zu Datenstrukturen

{Praktik} [für {Zielobjekt}] {MODALVERB} <Ergebnis> {Handlungswort}

Beispiel:


```
},
{
  "id": "KONF.6.5",
  "title": "Dynamische Zugriffskontrolle im System",
  "class": "erhöht",
  "props": [
    {
      "name": "alt-identifier",
      "value": "ced10fd0-a74e-4376-8dac-f3381c6a9482"
    },
    {
      "name": "effort_level",
      "value": "5",
      "ns": "https://github.com/BSI-Bund/Stand-der-Technik-Bibliothek/tree/main/Dokumentation/namespaces/stufen.csv"
    },
    {
      "name": "tags",
      "value": "Produktbeschreibung, Zero Trust",
      "ns": "https://github.com/BSI-Bund/Stand-der-Technik-Bibliothek/tree/main/Dokumentation/namespaces/tags.csv"
    }
```

OSCAL Catalog JSON laden

Durchsuchen... Zero-Trust.json

Suchen (ID, Titel, Text, Tags...)

KONF

Alle Sicherheitsniveaus

Alle Zielobjekte

Katalog: Zero-Trust.json | 131 Anforderungen | Graph: 20 Knoten

Legende

- Verwandte Anforderung (related)
- Abhängige Anforderung (required)
- {{ }} Parameter (gelbe Schrift inkl. {{ }})

Alles läuft lokal im Browser. Kein Upload.

KONF.6.5 – Dynamische Zugriffskontrolle im System

UUID: ced10fd0-a74e-4376-8dac-f3381c6a9482 Sicherheitsniveau: erhöht Stufe: 5 Zielobjekt: IT-Systeme

▾ Statement

Konfiguration für IT-Systeme SOLLTE dynamische Zugriffskontrolle im System aktivieren.

▾ Guidance

Eine dynamische Zugriffskontrolle (engl. Dynamic Access Control, DAC) bezeichnet ein Verfahren, bei dem Zugriffsentscheidunge
ACLs) beruhen, sondern zusätzlich kontextabhängige Bedingungen wie Gerätezustand, Sensitivität der Daten, Standort, Zeitfenste
zugrundeliegende Regelmenge zur Zugriffsbewertung, fest definiert und nachvollziehbar dokumentiert – lediglich die Entscheidu
Ziel ist eine feinere Steuerung des Datenzugriffs auf Basis aktueller Risikosituationen, ohne dass Administratoren Berechtigungen
dass ein Benutzer sensible Daten von einem nicht verwalteten Endgerät ausliest, während er im internen Netz regulär Zugriff hätt
Auditierung und Protokollierung der DAC zu achten.

KONF.6.13 – Dynamische Zugriffskontrolle in der Anwendung

UUID: 55dfbf64-f1f3-4765-a0d3-78f0a1f00654 Sicherheitsniveau: erhöht Stufe: 5 Zielobjekt: Anwendungen

▾ Statement

Konfiguration für Anwendungen SOLLTE dynamische Zugriffskontrolle in der Anwendung aktivieren.

▸ Guidance

KONF.10.4 – Deaktivierung nicht benötigter Anwendungsfunktionen

UUID: 990f4798-6926-41be-b09d-ee0162c530a0 Sicherheitsniveau: normal-SdT Stufe: 3 Zielobjekt: Anwendungen

▾ Statement

Konfiguration für Anwendungen SOLLTE nicht benötigte Anwendungsfunktionen deaktivieren.

OSCAL – Zukunft der Sicherheitsdokumentation

Open
Security
Controls
Assessment
Language

OSCAL

Einsatzmöglichkeiten im ISMS

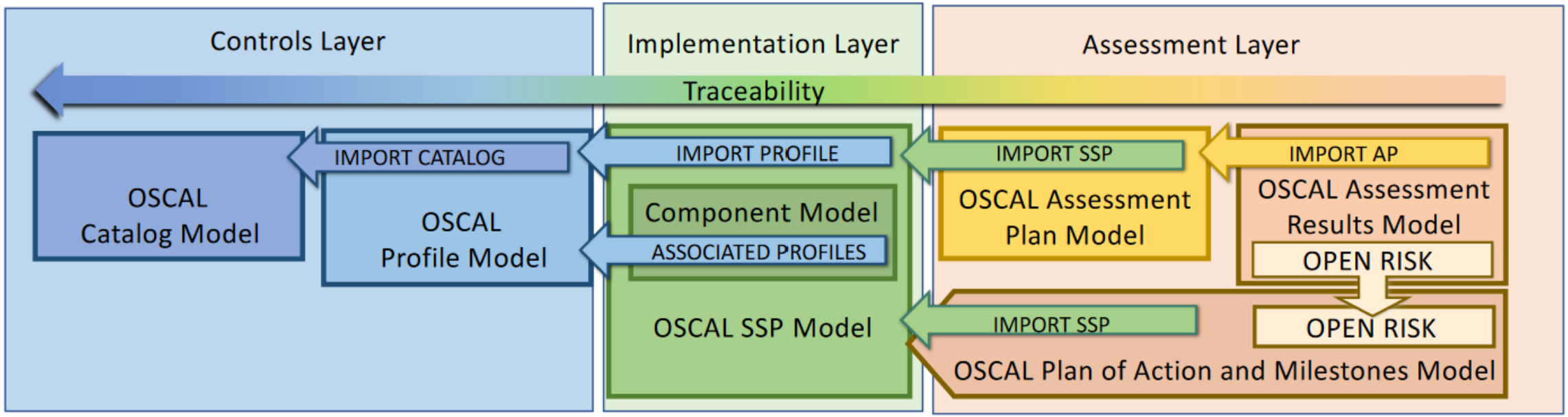
1. Standardisierte Dokumentation
2. Automatisierte Compliance-Prüfungen
3. Kontinuierliche Bewertung
4. Verbessertes Risikomanagement
5. Skalierbare Compliance-Verwaltung

Was es ist:

standardisiertes Framework des National Institute of Standards and Technology (NIST)

Zweck:

durchgängig digitalisieren und automatisieren, um manuelle Arbeit zu reduzieren und die Konsistenz zu erhöhen ➔prüfbarer digitalisierter Sicherheitsnachweisprozess



Bundesamt
für Sicherheit in der
Informationstechnik

Vielen Dank für Ihre Aufmerksamkeit!

Regierungsdirektorin

Sandra Karger

Referatsleitung – Stand der Technik

stand-der-technik@bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 87
53175 Bonn

www.bsi.bund.de

Follow us: