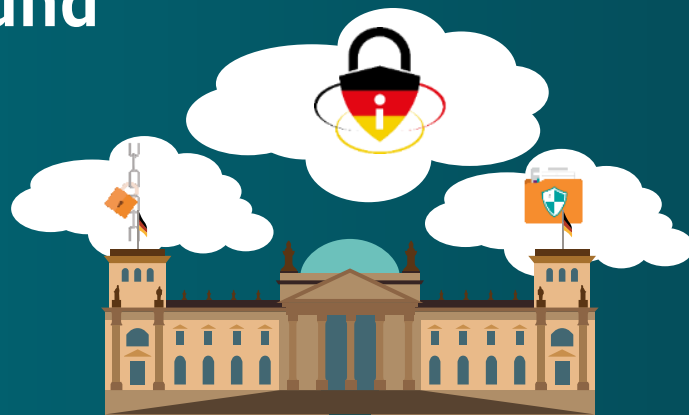


# Vortrag aus der Praxis: ISMS Toolunterstützung im ITZBund - vom Konzept bis zum Audit -

**IT-Grundschutz-Tag 2023**  
Vortrag: Lukas Nowak



**ZeDIS**  
(Zentraler Dienst für  
Informationssicherheit)

# Agenda



1. Was ist ZeDIS?
2. Wie unterstützt ZeDIS den Zertifizierungsprozess?
3. Welche Besonderheiten gibt es im Zertifizierungsprozess mit dem ITZBund und seinen Kunden?



# ZeDIS? Der zentrale Dienst für Informationssicherheit.



## Forderung von Informationssicherheitskonzepten (ISK)

Umsetzungsplan Bund sowie IT-Konsolidierung Bund fordern, dass Bundesbehörden ihre Sicherheitskonzeption erstellen und dokumentieren.



**Zentraler Dienst für Informationssicherheit (ZeDIS)** unterstützt die ISK-Erstellung gemäß BSI-Standards 200-x

ZeDIS basiert auf der Software HiScout GRC Suite, welche auf die Anforderungen behördlicher IT-Sicherheit angepasst wurde.



## ISK-Erstellung nach BSI IT-Grundschutzstandards

ISK-Erstellung erfolgt nach den Anforderungen des IT-Grundschutzes vom Bundesamt für Sicherheit in der Informationstechnik (BSI).

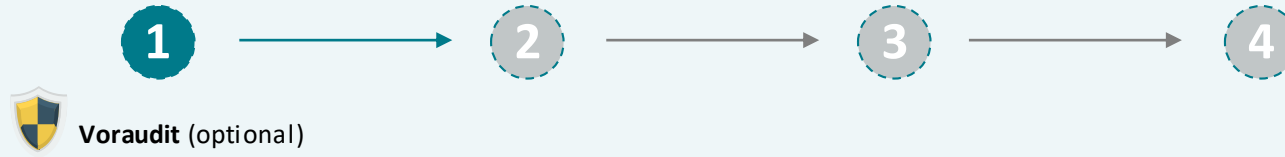


# Der Zertifizierungsprozess in vier Schritten dargestellt.

## Erst-Zertifizierung

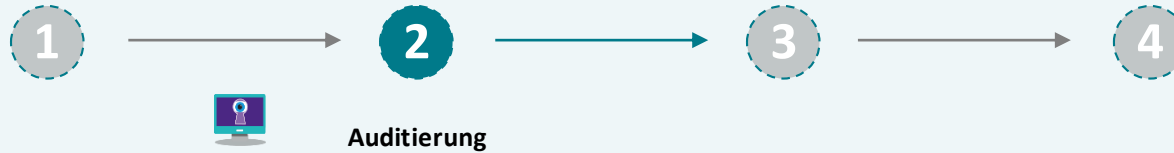


# Wie unterstützt ZeDIS das Voraudit?



- ✓ Bereitstellung einer zentralen Datenbasis von ISK-Informationen
- ✓ Bereitstellung der zertifizierungsrelevanten A-Dokumente (Richtlinien für Informationssicherheit (A.0), Strukturanalyse (A.1), Schutzbedarfsfeststellung (A.2), Modellierung des Informationsverbunds (A.3), Ergebnis des IT-Grundschutz-Checks (A.4), Risikoanalyse (A.5), Realisierungsplan (A.6)) per Knopfdruck
- ✓ Einheitliche und standardisierte Struktur gemäß IT-Grundschutz
- ✓ Individuelle Erstellung von Berichten zur Vorbereitung des Audits
- ✓ Bereitstellung einer Datenbank zum Upload weiterer relevanter Zertifizierungsunterlagen in der ZeDIS-Audit-Instanz

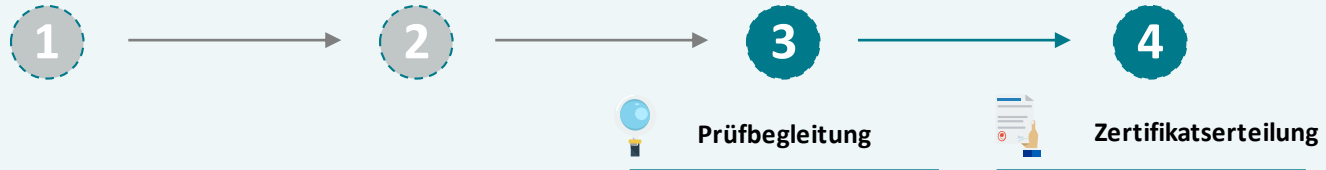
# Wie unterstützt ZeDIS das Zertifizierungsaudit?



- ✓ Detailansicht von Zielobjekten und Anforderungen in der ZeDIS-Audit-Instanz
- ✓ Soll-/Ist-Abgleich der umgesetzten und/oder nicht umgesetzten Anforderungen
- ✓ Differenzierung des Informationssicherheitskonzepts nach unterschiedlichen IT-Grundsatzkompendien (1x ISK mit mehreren Kompendien)



# Wie unterstützt ZeDIS in der Prüfung des Audits?



- ✓ Bereitstellung einer ZeDIS-Audit-Instanz inkl. dem zu zertifizierenden Informationsverbund
- ✓ Vorteile für Auditoren:
  - lesender Zugriff auf die Daten (inkl. Verlinkungen),
  - unveränderbare Sicht auf die Daten (Änderungen nicht möglich),
  - beliebige Aufbewahrungsdauer der Daten möglich,
  - unterschiedliche Auditteams für unterschiedliche Audits berechtigen,
  - mehrere Audits zum gleichen „Audit-Gegenstand“ möglich

# Besonderheiten im Zertifizierungsprozess mit ITZBund und seinen Kunden

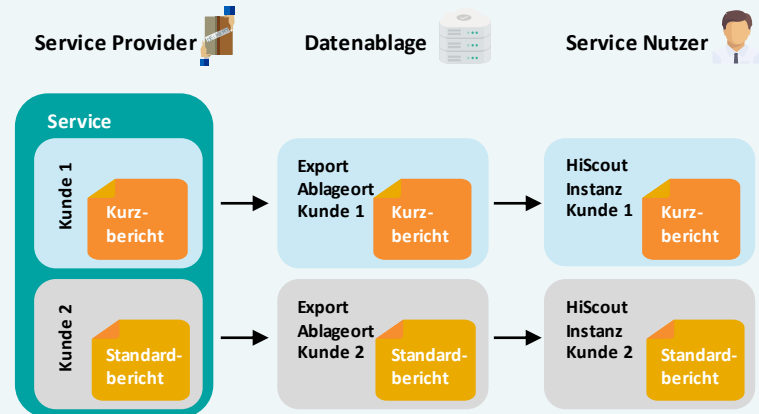


## Besonderheiten

- Outsourcing-Verhältnis zwischen (Kundenbehörde und Dienstleister (ITZBund))
- Reduzierter Zertifizierungsaufwand für Kundeneinrichtungen bei Informationsverbänden, die Basisservices vom ITZBund nutzen
- Klare Trennung der Verantwortlichkeiten (Basis-Service in der Verantwortung des ITZBund / Rest in der Verantwortung der Kundenbehörde)

- Zertifizierungsrelevante Serviceberichte für ITZBund Basis-Services stehen zur Verfügung

## Service Export Funktionalität





# Vielen Dank für Ihre Aufmerksamkeit!

Kommen Sie gern bei individuellen  
Rückfragen auf mich zu.

Lukas Nowak



# Backup

# Auditprozess (ISO 27001 Zertifizierung auf Basis von IT-Grundschutz)

