



Erfahrungsaustausch zum Thema Informationssicherheitszertifikate

DATEV: Gerd Kunkat, Andrea Gocke & Bernd Meyer | Sabine Wächter
Digitale Ökosysteme | Strategy & Certifications

DATA Security GmbH: Milomir Mikulovic

05.05.2025

Agenda → Austausch erwünscht

1. DATEV-Marktplatz Privacy & Security

- a. Hintergrund
- b. Set valider Zertifikate
- c. Warum ein Informationssicherheits-
Managementsystem?

2. Erfahrungsaustausch mit DATA Security

- a. Keine Angst vor der Zertifizierung!
 - Struktur zum ISMS Aufbau und Audits
 - Developer Team, Management und Organisation (SDLC)
- b. Gute Gründe für eine Zertifizierung und der Goldstandard
 - Vermarktungsfähigkeit
- c. Zeitaufwand
- d. Umgehung möglicher Fallstricke

3. Weitere Erfahrungsberichte und Fragen aus der Runde

- a. Status und Vorgehen
- b. Bekannte Impediments
- c. Anbieter und Zertifikate
- ...

4. Weiteres Vorgehen

01 DATEV-Marktplatz Privacy & Security

DATEV-Marktplatz Privacy & Security

Premium Partner: Mehr Datenschutz und Informationssicherheit



Sicherheitsanspruch DATEV

DATEV als Auftragsverarbeiter bietet Nachweise über Sicherheit der verarbeiteten Daten.

Umfrage Kundenerwartung
Partnerlösungen haben gleichen Security Level wie DATEV-Lösungen.

Rolle DATEV
Datenschutz und Datensicherheit sicherstellen - im Auftrag unserer Mitglieder und Kunden.

Nachweisfähigkeit

DATEV-Marktplatz zeigt Transparenz und Informationen zur Sicherheit der Partnerlösungen.

Zertifikat als Nachweis zur Sicherheit der Partnerlösung im DATEV-Marktplatz.

Scope der Zertifizierung
min. Entwicklung & Betrieb der SW.

Set akzeptierter Zertifikate
kleine Einstiegshürden, beherrschbare Kosten, Marktverbreitung, Standards.

Vorgehen in Kooperationen

DATEV-Marktplatz Premium Partner erwerben eigenverantwortlich ein für sie passendes Zertifikat bei einem passendem Zertifizierungsanbieter.

Skalierung
je nach Zertifizierungsbedarf
[Internationalität, Branche, Aufwand,, Größe].

Reifegradprüfung
kostenpflichtige Quick Audits zur GAP-Analyse mit externen Zertifizierungsanbietern bei fehlender Zertifizierung als Vorbereitung.

Bestehende DATEV-Marktplatz Premium Partner

müssen eigenverantwortlich ein Datenschutz- und Informationssicherheits-Zertifikat erwerben - **Umsetzungstermin bis zum 01.07.2026.**

Neue DATEV-Marktplatz Premium Partner müssen ein Zertifikat vorweisen - seit 06/2024.

Link: [DATEV-Marktplatz Datenschutz und Informationssicherheit mit Zertifikaten.](#)



Valides Set von Zertifizierungen

Zertifikat-Testat	Skalierung	Scope	Zielgruppen	Regelwerke/Auditkriterien	Art & Akkreditierung
ISO 27001	High Level	IS (Managementsystem)	Branchenübergreifend	ISO 27001	Zertifikat, DakKS
ISO 27701	High Level	DS (Managementsystem)	Branchenübergreifend	ISO 27001 <u>und</u> aufbauend ISO 27701	Zertifikat
ISO 27017	High Level	IS – Fokus Cloud-Dienstleistungen	Branchenübergreifend	ISO 27001 <u>und</u> aufbauend ISO 27017	Zertifikat, DakKS
ISO 27018	High Level	DS- Fokus Cloud-Dienstleistungen	Branchenübergreifend	ISO 27001 <u>und</u> aufbauend ISO 27018	Zertifikat, DakKS
C5	High Level	IS/DS Cloud-Anbieter	Branchenübergreifend	<u>Cloud Computing Compliance Criteria Catalogue</u>	Zertifikat, BSI
BSI Grundschatz	High Level	IS (Managementsystem)	Branchenübergreifend	<u>BSI - IT-Grundschatz-Bausteine (Edition 2023) (bund.de)</u>	Zertifikat, BSI
TISAX	High Level	IS (Managementsystem)	Branche Automobilssektor	VDA Information Security Assessment https://portal.enx.com/de-DE/TISAX/downloads/	Zertifikat, DakKS
Art 42 - Europrise	High Level	DS (IT-Produkte & Dienstleistungen)	Branchenübergreifend (KMU)	<u>EuroPriSe Criteria</u>	Zertifikat, DakKS
Art 42 - Auditor	High Level	DS Cloud-Anbieter	Branchenübergreifend (KMU)	<u>Kriterienkatalog</u>	Zertifikat, DakKS
VdS 10000	Medium Level	IS (Managementsystem)	Branchenübergreifend (KMU)	<u>VdS 10000-Richtlinien Informationssicherheitsmanagement</u>	Zertifikat, akkreditiert
VdS 10010	Medium Level	DS (Managementsystem)	Branchenübergreifend (KMU)	Valide nur wenn aufbauend auf VdS 10000 <u>VdS-Richtlinien 10010 Datenschutzmanagement</u>	Zertifikat, akkreditiert
CISIS12	Medium Level	IS/DS (Managementsystem)	Branchenübergreifend (KMU)	<u>Compliance & Informationssicherheit, 12 Schritte, Baustein, Maßnahmenkatalog</u>	Zertifikat, akkreditiert
ULD	Medium Level	DS (IT-Produkt)	Branchenübergreifend	<u>Kriterienkatalog</u>	DS-Gütesiegel
BSI Grundschatz Basis-Absicherung	Basis Level	IS (Informationsverbund)	Branchenübergreifend	<u>Leitfaden zur Basis-Absicherung</u> <u>Checklisten Basis-Absicherung</u> BSI führt IT-Grundschatz-Testat nach Basis-Absicherung ein	Testat, BSI, akkreditiert

▪ **Der Scope der Zertifizierung beinhaltet mindestens: „Entwicklung und Betrieb der Marktplatz Lösung“.**

▪ **Fokus der anerkannten Zertifikate:**

Orientierung an ISO27001, Ausrichtung an einer Akkreditierung sowie Umsetzung der Informationssicherheit (IS) mittels verpflichtendem ISMS-Aufbau.

▪ **Besonderheit Datenschutz Zertifikate:**

Art 42 DS-GVO und ULD als Datenschutz (DS) Zertifikate sind jeweils valide, da hohe Informationssicherheitsanteile. Reine DS-Zertifikate wie ISO 27701/27018 benötigen hingegen immer ein IS-Zertifikat ISO 27001 als Voraussetzung. Ein DS-Zertifikat VdS 10010 ist nur valide in Ergänzung zu einem IS-Zertifikat VdS 10000.



Security Prozesse und Security Architektur → ISMS Aufbau

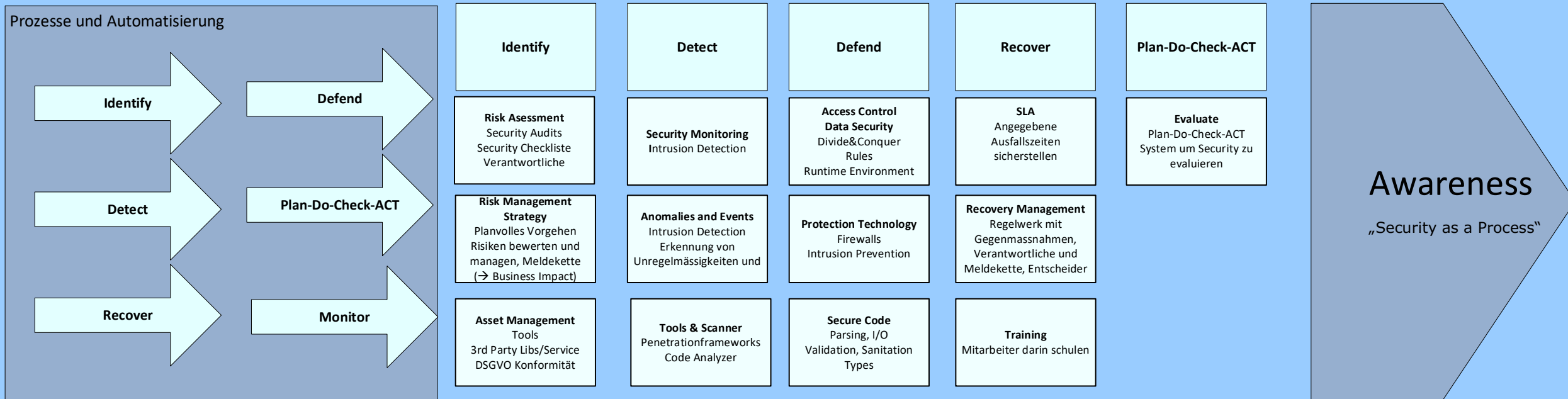
Issue Beschreibung

- Security kann als Snapshot fehlverstanden werden
- Verantwortlichkeiten, Prozesse, Dokumente sind dann oft ungeklärt
- Was passiert dann, wenn ein Angriff erfolgt
...Wer macht was?...Zeitdruck...Panik...Downtimes...Nachweise...pot. Klagen

Lösung

- Prozesse Security implementieren und dokumentieren, stetig
- Aufbau von Struktur: Informationssicherheitsmanagementsystem
- An gesetzliche Vorgaben orientieren und diese beachten

Realisierung eines Security Frameworks



02 Erfahrungsaustausch mit DATA Security GmbH

DATA Security GmbH: Milomir Mikulovic

Dipl. Wirtschaftsingenieur (FH) | Zert. Datenschutzauditor TÜV-SÜD
Zert. Geldwäsche-Compliance Experte | Geschäftsleitung

Tel: +49 8031 2300 100

m.mikulovic@data-security.one

[data-security.one](https://www.data-security.one)

1. Keine Angst vor der Zertifizierung!

- a. Strukturen zum ISMS Aufbau und Ablauf von Audits
- b. Developer Team, Management und Organisation (SDLC)

2. Unsere Gründe der Zertifizierung und der Goldstandard →Vermarktungsfähigkeit

3. Zeitaufwand

4. Umgehung möglicher Fallstricke

Guest Speaker Milomir Mikulovic von Data Security: Erfahrungen am Beispiel ISO 27001

- **Wichtigste Botschaft:** Keine Angst vor der Zertifizierung! Aber wichtig ist: Wo fange ich bei den Themen an und wo hören sie auf → Strukturieren! Abgrenzen!
- **ISO 27001 gibt eine Template Struktur in Form von Kapiteln vor, insbes.:**
 - **Kapitel 4: Scope der Zertifizierung** muss definieren (was soll alles zertifiziert werden, bspw. eine SW-Lösung, mehrere SW-Lösungen, ganze Geschäftsbereiche oder das Gesamtunternehmen).
 - **Kapitel 5: Managementunterstützung** muss vorliegen für eine erfolgreiche Zertifizierung: Ressourcen, Zeit, Geld.
 - **Kapitel 6: Konkrete Planung** der Zertifizierung.
 - **Dokumentation der Prozesse/Artefakte/TOMs** mittels SW oder fertiger Musterdokumente usw.
→ Individualisierung auf das jeweilige Unternehmen und Ausrichtung nötig.
→ Zertifizierung hilft und motiviert die eigenen Prozesse zu hinterfragen und zu verbessern.
→ SW Tool Einsatz empfohlen, denn man muss immer wieder aktualisieren (mindest. jährlich).
- **Prüfung:**
 - Auditoren legen Wert auf kontinuierliche Verbesserung (von erster Zertifizierung bis zur Rezertifizierung, Erstzertifizierung ist ein erster und größerer Step wo die Doku erstmalig vollständig vorliegen muss, dann darauf aufbauend sollen weitere Schritte jährlich erfolgen).
 - Auditoren versuchen zu ermitteln, ob Widersprüche existieren und ob das Dokumentierte stimmig ist mit der Realität im Unternehmen
- **Managementwille und Interner Rollenaufbau notwendig:**
 - Der Wille zur Zertifizierung muss im Unternehmen (Management & Organisation) verankert sein.
 - Ein fest definierter interner Kümmerer/Treiber und Koordinator im Team wird benötigt, dieser benötigt kontinuierlich Zeit und Freiraum.
- **Beratungen empfohlen, um Managementprozesse zu implementieren:**
 - Externe Berater sind Treiber bringen wichtige Impulse+Expertise.
 - Vorlaufzeiten beachten.
 - Beratungstag kostet zwischen 1000-2500€.
- **Skalierungen:** Die Zertifizierung benötigt je nach Zertifikatsart, strateg. Ausprägung, Umfang, Scope, Unternehmensgröße, Internationalität eine sehr differenten Aufwand.

Hinweis von TASSlink Software GmbH – durch Hrn. Georg Vogginger:

→ Förderung von Sicherheit (Zertifizierungen) spez. in Bayern mit bis zu 10.000€ , auch Digitalisierung von Prozessen, <http://www.digitalbonus.bayern/foerderprogramm/>

03 **Erfahrungsberichte aus der Runde und Fragen**

- **Auftrag und Strategie**

muss vom Management ausgehen

soll Projektteam ausreichend Freiraum einräumen

Chance bestehende Themen/Prozesse zu hinterfragen und zu optimieren (nicht nur Siegel als Fokus!)

Sportlicher, aber realistischer Zeitraum

- **Projektteam**

- **Mit zunehmender Unternehmensgröße und Anzahl "eigenständiger" Units/Geschäftsbereiche steigt in der Regel Aufwand und Komplexität**

→ Dafür größere Chance Synergien zu identifizieren und nachhaltiger zu wirken

- **Aufstellung (Beispiel: Unternehmen mit ca. 500MA und mehrere Geschäftsbereiche zertifiziert sich in CISIS12/SWI)**

→ 1 bis 2 Projektleiter

- Aufwand ca. 30% der Arbeitszeit (min. 1 Tag pro Woche)

→ Experten aus IT/Technik o.ä.

- je nach Anzahl beteiligter Units
- Aufwand ca. 10%

→ Experten aus Prozessberatung

- je nach übergreifenden Prozessen
- Aufwand ca. 10%

→ Externer Berater/Experte

- begleitet, moderiert, Teilt Erfahrung

- **Vorgehen**

- **Regelmäßige Projektmeetings mit klarer Agenda**

- **Regelmäßige Lenkungskreissitzungen bei GF (min. Projektleitung und Management) zur Transparenz und Steuerung**

- **Lösung zur Abbildung der Prozesse/Dokumentationen etc. klar empfohlen**

Ansprechpartner CAS Software AG: Marcus Bär

Mitglied der Geschäftsführung
Telefon 0721/9638-678 www.cas-mittelstand.de

CAS Software AG · CAS-Weg 1-5 · 76131 Karlsruhe
Telefon +49 721 9638-0
www.cas.de · [twitter](#) · [facebook](#) [Impressum](#) und [AGB](#)

04 Weiteres Vorgehen

Vorgehen Zertifizierung für Partner

Beispielhafte Auswahl möglicher Zertifizierungsanbieter im Bereich Informationssicherheit und Datenschutz - ohne Anspruch auf Vollständigkeit.



1. Frist beachten

DATEV-Marktplatz Premium Partner

müssen *eigenverantwortlich* ein Zertifikat bei einem für Sie passenden Anbieter erwerben

- **bis zum 01.07.2026.**

2. Follow Up und weitere Workshops

Je nach Bedarf können weitere Workshops mit anderen Anbietern organisiert werden.