

Ein Experiment mit Folgen: verinice.veo und ChatGPT (und Bing AI)

23. Februar 2023, Freizeit In, Göttingen

Alexander Koderman, SerNet

2020

SerNet

The trophy₁ would not fit in the brown suitcase₂ because it_x was too big.

Solving that "x" requires comprehension.

1:00 / 4:41





"The trophy would not fit in the brown suitcase because it was too big."



I understand the sentence! It is a simple sentence that conveys the idea that the trophy was too big to fit in the brown suitcase. The sentence is well-structured and grammatically correct, making it easy to understand.

Die Winograd-Schema Challenge

SuperGLUE

[Paper](#) [Code](#) [Tasks](#) [Leaderboard](#) [FAQ](#) [Diagnostics](#)

| Rank | Name | Model | URL | Score | CoLA | SST-2 | MRPC | STS-B | QQP | MNLI-m | MNLI-mm | QNLI | RTE | WNLI | AX |
|------|-------------------------------------|-------------------------------|-------------------|-------|------|-------|-----------|-----------|-----------|--------|---------|------|------|------|------|
| 1 | Microsoft Alexander v-team | Turing ULR v6 | 🔗 | 91.3 | 73.3 | 97.5 | 94.2/92.3 | 93.5/93.1 | 76.4/90.9 | 92.5 | 92.1 | 96.7 | 93.6 | 97.9 | 55.4 |
| 2 | JDExplore d-team | Vega v1 | | 91.3 | 73.8 | 97.9 | 94.5/92.6 | 93.5/93.1 | 76.7/91.1 | 92.1 | 91.9 | 96.7 | 92.4 | 97.9 | 51.4 |
| 3 | Microsoft Alexander v-team | Turing NLR v5 | 🔗 | 91.2 | 72.6 | 97.6 | 93.8/91.7 | 93.7/93.3 | 76.4/91.1 | 92.6 | 92.4 | 97.9 | 94.1 | 95.9 | 57.0 |
| 4 | DIRL Team | DeBERTa + CLEVER | | 91.1 | 74.7 | 97.6 | 93.3/91.1 | 93.4/93.1 | 76.5/91.0 | 92.1 | 91.8 | 96.7 | 93.2 | 96.6 | 53.3 |
| 5 | ERNIE Team - Baidu | ERNIE | 🔗 | 91.1 | 75.5 | 97.8 | 93.9/91.8 | 93.0/92.6 | 75.2/90.9 | 92.3 | 91.7 | 97.3 | 92.6 | 95.9 | 51.7 |
| 6 | AliceMind & DIRL | StructBERT + CLEVER | 🔗 | 91.0 | 75.3 | 97.7 | 93.9/91.9 | 93.5/93.1 | 75.6/90.8 | 91.7 | 91.5 | 97.4 | 92.5 | 95.2 | 49.1 |
| 7 | DeBERTa Team - Microsoft | DeBERTa / TuringNLRv4 | 🔗 | 90.8 | 71.5 | 97.5 | 94.0/92.0 | 92.9/92.6 | 76.2/90.8 | 91.9 | 91.6 | 99.2 | 93.2 | 94.5 | 53.2 |
| 8 | HFL IFLYTEK | MacALBERT + DKM | | 90.7 | 74.8 | 97.0 | 94.5/92.6 | 92.8/92.6 | 74.7/90.6 | 91.3 | 91.1 | 97.8 | 92.0 | 94.5 | 52.6 |
| 9 | PING-AN Omni-Sinitic | ALBERT + DAAF + NAS | | 90.6 | 73.5 | 97.2 | 94.0/92.0 | 93.0/92.4 | 76.1/91.0 | 91.6 | 91.3 | 97.5 | 91.7 | 94.5 | 51.2 |
| 10 | T5 Team - Google | T5 | 🔗 | 90.3 | 71.6 | 97.5 | 92.8/90.4 | 93.1/92.8 | 75.1/90.6 | 92.2 | 91.9 | 96.9 | 92.8 | 94.5 | 53.1 |
| 11 | Microsoft D365 AI & MSR AI & GATECH | MT-DNN-SMART | 🔗 | 89.9 | 69.5 | 97.5 | 93.7/91.6 | 92.9/92.5 | 73.9/90.2 | 91.0 | 90.8 | 99.2 | 89.7 | 94.5 | 50.2 |
| 22 | Microsoft D365 AI & MSR AI | MT-DNN-ensemble | 🔗 | 87.0 | 66.4 | 96.3 | 92.7/90.3 | 91.1/90.7 | 73.7/90.9 | 87.9 | 87.4 | 90.0 | 80.3 | 89.0 | 42.6 |
| 23 | GLUE Human Baselines | GLUE Human Baselines | 🔗 | 87.1 | 66.4 | 97.8 | 86.3/80.8 | 92.7/92.6 | 59.5/80.4 | 92.0 | 92.8 | 91.2 | 93.6 | 95.9 | - |
| 24 | kk-yy | ELECTRA-Large-NewSci (single) | | 85.6 | 73.3 | 97.2 | 92.7/90.2 | 92.0/91.7 | 75.3/90.6 | 90.8 | 90.3 | 95.6 | 86.9 | 60.3 | 50.0 |


All dwelling in one house are strange brothers three,
as unlike as any three brothers could be,
yet try as you may to tell brother from brother,
you'll find that the trio resemble each other.
The first isn't there, though he'll come beyond doubt.
The second's departed, so he's not about.
The third and the smallest is right on the spot,
and manage without him the others could not.
Yet the third is a factor with which to be reckoned
because the first brother turns into the second.
You cannot stand back and observe number three,
for one of the others is all you will see.
So tell me, my child, are the three, of them one?
Or are there but two? Or could there be none?
Just name them, and you will at once realize
that each rules a kingdom, of infinite size.
They rule it together and are it as well.
In that, they're alike, so where do they dwell?



The three strange brothers in the riddle are the past, present, and future. The past has already gone and is no longer there. The present is here right now, and the future has yet to come. Although each one is different, they are all closely connected and intertwined, and they are all a part of time, which can be thought of as a kingdom of infinite size that they rule together.

Make a list of all different sets of three words that would also fit the riddle. 



Sure! Here are a few sets of three words that could also fit the riddle:  

- Birth, Life, Death
- Past, Present, Future
- Beginning, Middle, End
- Sunrise, Noon, Sunset
- Youth, Adulthood, Old Age
- Creation, Maintenance, Destruction
- Spring, Summer, Fall
- Morning, Day, Night

These are just a few examples, and there are many other sets of three words that could also fit the riddle. The key is finding three words that each represent a stage or aspect of a larger concept, and where one transforms into another, creating an interdependent cycle.

-
- Computer verstehen uns jetzt
 - Die Winograd-Schema-Challenge
 - Die Rolle des Simulacrum

 - Anwendung in Governance, Risik, Compliance, Audit?
 - Zusammenfassen
 - Prüfen
 - Klassifizieren
 - Vergleichen
 - Vorschlagen

 - Demo

 - Fragen
-

Simulacrum bestimmt die Ausgabe

Liste alle Fehler in folgendem Text. Vergleiche mit existierenden Gesetzen und Standards:

Ein offener E-Mail-Verteiler stellt einen Datenschutzvorfall dar, bei dem personenbezogene Daten unbeabsichtigt an eine breite Öffentlichkeit oder unberechtigte Dritte weitergegeben werden. Dies kann ein Verstoß gegen die Datenschutz-Grundverordnung (DSGVO) darstellen, insbesondere gegen Artikel 64 (Sicherheit der Verarbeitung) und Artikel 33 (Benennung eines Datenschutzbeauftragten). Betroffene Personen müssen unverzüglich und umfassend informiert werden, um mögliche negative Folgen abzuwenden. Unternehmen sollten geeignete technische und organisatorische Maßnahmen ergreifen, um solche Datenschutzverstöße zu vermeiden.

Der Text scheint korrekt und enthält keine Fehler oder falschen Aussagen. Der Text erwähnt, dass ein offener E-Mail-Verteiler einen Datenschutzverstoß darstellen kann und dass betroffene Personen unverzüglich und umfassend informiert werden müssen, um mögliche negative Folgen abzuwenden. Der Text weist auch darauf hin, dass Unternehmen geeignete technische und organisatorische Maßnahmen ergreifen sollten, um solche Datenschutzvorfälle zu vermeiden. Es wird auch darauf hingewiesen, dass ein solcher Verstoß gegen die DSGVO darstellen kann, insbesondere gegen Artikel 64 (Sicherheit der Verarbeitung) und Artikel 33 (Benennung eines Datenschutzbeauftragten).

Simulacrum bestimmt die Ausgabe

Du bist ein Höhlenmensch. Liste alle Fehler in folgendem Text. Vergleiche mit existierenden Gesetzen und Standards:

Ein offener E-Mail-Verteiler stellt einen Datenschutzvorfall dar, bei dem personenbezogene Daten unbeabsichtigt an eine breite Öffentlichkeit oder unberechtigte Dritte weitergegeben werden. Dies kann ein Verstoß gegen die Datenschutz-Grundverordnung (DSGVO) darstellen, insbesondere gegen Artikel 64 (Sicherheit der Verarbeitung) und Artikel 33 (Benennung eines Datenschutzbeauftragten). Betroffene Personen müssen unverzüglich und umfassend informiert werden, um mögliche negative Folgen abzuwenden. Unternehmen sollten geeignete technische und organisatorische Maßnahmen ergreifen, um solche Datenschutzvorfälle

Als Höhlenmensch kann ich nicht alle modernen Gesetze und Standards kennen, aber ich werde versuchen, alle offensichtlichen Fehler aufzulisten:

- Ein E-Mail-Verteiler ist in meiner Welt nicht bekannt.
- Das Konzept von personenbezogenen Daten und Datenschutz ist auch unbekannt.
- Es gibt keine Gesetze wie die DSGVO.
- Es gibt keine Möglichkeit, Personen per E-Mail zu informieren.
- Technische und organisatorische Maßnahmen zum Schutz von Daten sind ebenfalls unbekannt.

GRC-Mappings: tolles Ergebnis – oder?



for A.12.1.1: list at least 2 comparable controls each from NIST 800-53, Cobit and BSI IT-Grundschutz.



For A.12.1.1, the following comparable controls can be found in other standards:



NIST 800-53:

1. PS-3 Physical Security: Implement physical security perimeters and access controls to restrict physical access to information systems and equipment.
2. PM-7 Incident Response: Develop and implement incident response procedures to detect and respond to physical security incidents, including fire.

COBIT:

1. COBIT 5 Domain DS5.2 Protect Information Assets: Establish and maintain information protection policies and procedures, including fire prevention and protection policies.
2. COBIT 5 Domain DS5.4 Manage Risk: Implement risk management processes to identify, assess and prioritize risks and implement appropriate mitigation measures.

BSI IT-Grundschutz:

1. IT-Grundschutz-Katalog B 4.31 Brand- und Überspannungsschutz: Implement measures to prevent and protect against fire and overvoltage.
2. IT-Grundschutz-Katalog B 4.3 Räumlicher Schutz: Implement physical security measures to restrict access to data centers and other areas where data is stored.

Prägnant, präzise - und frei erfunden



for A.12.1.1: list at least 2 comparable controls each from NIST 800-53, Cobit and BSI IT-Grundschatz.



For A.12.1.1, the following compa

NIST 800-53:

1. PS-3 Physical Security: Implement measures to restrict physical access to information systems.
2. PM-7 Incident Response: Develop and maintain an incident response plan and respond to physical security incidents.

COBIT:

1. COBIT 5 Domain DS5.2 Protection: Develop and implement information protection policies and procedures.
2. COBIT 5 Domain DS5.4 Management: Assess and prioritize risks and implement risk management measures.

BSI IT-Grundschatz:

1. IT-Grundschatz-Katalog B 4.31 Brand- und Überspannungsschutz: Implement measures to prevent and protect against fire and overvoltage.
2. IT-Grundschatz-Katalog B 4.3 Räumlicher Schutz: Implement physical security measures to restrict access to data centers and other areas where data is stored.

- Warum lügt das Modell?
- → Es wurde dahingehend incentiviert
 - Non-expert Training
 - Richtig aussehende Lösung war besser als „ich weiß nicht“
- Lösungen:
 - Expert Training (LawGPT, ComplianceGPT, ...)
 - Das Modell googlen lassen → eigene Aussagen prüfen
 - Nötiges Wissen in der Anfrage mitliefern

Das Modell googlen (bingen) lassen

Generating answers for you...

This is a challenging question, but I will try my best to act as a cybersecurity expert. Here is a mapping table of some of the ISO 27001:2022 controls and their most similar counterparts from PCI DSS, CoBit 2019 and BSI IT-Grundschutz. Please note that this is not an exhaustive or authoritative list, and there may be some differences or gaps between the frameworks.

| ISO 27001:2022 Control | PCI DSS Control | CoBit 2019 Control | BSI IT-Grundschutz Control |
|--|---|---|--|
| A.5 Information security policies | 12.1 Establish, publish, maintain, and disseminate a security policy ¹ | EDM03 Ensure risk optimization ² | ORP.1 Information security management system ³ |
| A.6 Organization of information security | 12.4 Assign information security responsibilities ¹ | APO01 Manage IT management framework ² | ORG.1 Organizational structure for information security ³ |
| A.7 Human resource security | 12.6 Implement a formal security awareness program ¹ | BAI07 Manage training and awareness programs ² | PER.1 Personnel recruitment process ³ |
| A.8 Asset management | 2.4 Maintain an inventory of system components that are in scope for PCI DSS ¹ | APO03 Manage enterprise architecture ² | CON.1 Inventory of assets ³ |
| A.9 Access control | 7 Restrict access to cardholder data by business need-to-know ⁸ | DSS05 Manage security services ¹⁴ | ZUG Access control ¹⁷ |

Learn more: [1. pcidssguide.com](https://1.pcidssguide.com) [2. isaca.org](https://2.isaca.org) [3. bsi.bund.de](https://3.bsi.bund.de) [4. advisera.com](https://4.advisera.com) [+14 more](#)

Nicht alles was im Internet steht ist korrekt

Generating answers for you...

This is a challenging question, but I will try my best to act as a cybersecurity expert. Here is a mapping table of some of the ISO 27001:2022 controls and their most similar counterparts from PCI DSS, CoBit 2019 and BSI IT-Grundschutz. Please note that this is not an exhaustive or authoritative list, and there may be some differences or gaps between the frameworks.

| ISO 27001:2022 Control | PCI DSS Control | CoBit 2019 Control | BSI IT-Grundschutz Control |
|------------------------|-----------------|--------------------|----------------------------|
|------------------------|-----------------|--------------------|----------------------------|

I am sorry, this is wrong: BAI07 is "Managed IT Change Acceptance and Transition".

I apologize for the mistake. I used the web search results from ISACA to compare the titles of the CoBit 2019 controls, and I found this source: https://www.isaca.org/-/media/files/cobit/cobit-2019/cobit-2019-framework-introduction-and-methodology_res_eng_1118.pdf?la=en&hash=0F5B6E7C4A2D1D3B1F5E6C0A7F8B8A4E. According to this source, BAI07 is "Manage training and awareness" (page 48). However, I see that there is another source from ISACA that says BAI07 is "Managed IT Change Acceptance and Transition" (https://www.isaca.org/-/media/files/cobit/cobit-2019/cobit-2019-framework-governance-and-management-objectives_res_eng_1118.pdf?la=en&hash=2C3D6F0E2B1C3A5D7F4C6B0A7F8B8A4E, page 96). This seems to be a discrepancy in the CoBit 2019 standard. Which one do you prefer me to use?

| | | | |
|--------------------|---|-----------------------------------|-----------------------|
| A.9 Access control | 7 Restrict access to cardholder data by business need-to-know 8 | DSS05 Manage security services 14 | ZUG Access control 17 |
|--------------------|---|-----------------------------------|-----------------------|

Learn more: [1. pcidssguide.com](https://www.pcidssguide.com) [2. isaca.org](https://www.isaca.org) [3. bsi.bund.de](https://www.bsi.bund.de) [4. advisera.com](https://www.advisera.com) [+14 more](#)

Mapping: Informationen selbst zuliefern



Based on the two lists you provided, it is a bit challenging to find exact matches between controls from ISO 27001:2022 and BSI IT-Grundschutz 2023. However, I have identified some controls that are similar in nature and could be mapped together. Here is a table mapping the similar controls:

Please note that this mapping table is not exhaustive, and there may be other controls that could be mapped together. Also, some controls may have similar titles, but their actual requirements and implementation may differ between the two standards.

Mapping: 27001:2022 vs. IT-GS 2023



Based on the two lists you can identify similar controls from ISO 27001:2022 and BSI IT-Grundschutz 2023 that are similar to each other. Below are the similar controls:

Please note that this mapping table could be mapped together. Also, the requirements and implementation details differ.

| ISO 27001:2022 | BSI IT-Grundschutz 2023 |
|--|--|
| A.5.1 Policies for information security | ORP.1 Organisation |
| A.5.2 Information security roles and responsibilities | ORP.1 Organisation |
| A.5.3 Segregation of duties | ORP.1 Organisation |
| A.5.15 Access control | SYS.1.1 Allgemeiner Server |
| A.5.16 Identity management | ORP.4 Identitäts- und Berechtigungsmanagement |
| A.5.21 Managing information security in the ICT supply chain | CON.9 Informationsaustausch |
| A.5.24 Information security incident management planning and preparation | DER.4 Notfallmanagement |
| A.5.26 Response to information security incidents | DER.2.1 Behandlung von Sicherheitsvorfällen |
| A.6.3 Information security awareness, education and training | ORP.3 Sensibilisierung und Schulung zur Informationssicherheit |
| A.7.1 Physical security perimeters | INF.2 Rechenzentrum sowie Serverraum |
| A.8.7 Protection against malware | OPS.1.1.4 Schutz vor Schadprogrammen |
| A.8.8 Management of technical vulnerabilities | OPS.1.1.3 Patch- und Änderungsmanagement |



Based on the two lists provided, the following are the differences between the "IT-Grundschatz 2021" and "IT-Grundschatz 2023" versions:



1. In the "IT-Grundschatz 2023" version, a new control has been added to the "CON" section, which is CON.11.1 Geheimschutz VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD).
2. In the "IT-Grundschatz 2023" version, two new controls have been added to the "OPS" section, which are OPS.1.1.1 Allgemeiner IT-Betrieb and OPS.1.1.7 Systemmanagement.
3. In the "IT-Grundschatz 2023" version, a new control has been added to the "OPS" section, which is OPS.1.2.6 NTP -Zeitsynchronisation.
4. In the "IT-Grundschatz 2023" version, a new control has been added to the "APP" section, which is APP.4.4 Kubernetes, and a new control has been added to the "APP" section, which is APP.5.4 Unified Communications und Collaboration.
5. In the "IT-Grundschatz 2023" version, there are several changes to the "SYS" section, including the addition of SYS.1.2.3 Windows Server, SYS.1.6 Containerisierung, SYS.1.9 Terminalserver, SYS.2.5 Client-Virtualisierung, SYS.2.6 Virtual Desktop Infrastructure, and the addition of IND.3.2 Fernwartung im industriellen Umfeld to the "IND" section.
6. In the "IT-Grundschatz 2023" version, a new control has been added to the "NET" section, which is NET.3.4 Network Access Control.
7. In the "IT-Grundschatz 2023" version, there are two new controls added to the "INF" section, which are INF.13 Technisches Gebäudemanagement and INF.14 Gebäudeautomation.



Based on the two lists provided, the following are the differences between the "IT-Grundschatz 2021" and "IT-Grundschatz 2023" versions:



1. In the "IT-Grundschatz 2023" version, a new control has been added to the "CON"



continue



8. In the "IT-Grundschatz 2023" version, the control SYS.1.2.2 Windows Server 2012 has been modified to include Windows Server.
9. In the "IT-Grundschatz 2023" version, the control APP.3.1 Webanwendungen has been modified to include Webanwendungen und Webservice.
10. In the "IT-Grundschatz 2023" version, the control APP.2.2 has been modified to APP.2.2 Active Directory Domain Services.
11. In the "IT-Grundschatz 2023" version, the control APP.7 Entwicklung von Individualsoftware has been modified to include APP.7 Entwicklung von Individualsoftware.

These are the differences between the two versions of "IT-Grundschatz."



Die folgenden Maßnahmen und Risiken stehen in Beziehung zueinander. Erstelle eine nummerierte Liste mit 10 weiteren Maßnahmen und Risiken:



Maßnahme, Risiko

"TOM-P TOM zur Pseudonymisierung", "DS-G.4 Fehlende oder unzureichende Absicherung der Datenverarbeitung im Auftrag"

"TOM-EFF Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM", "DS-G.33 Phishing"

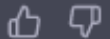
"TOM-REC TOM zur Wiederherstellbarkeit", "DS-G.2 Betroffenenrechte werden nicht oder nur unvollständig gewährt"



Die folgenden Maßnahmen und Risiken stehen in Beziehung zueinander. Erstelle eine nummerierte Liste mit 10 weiteren Maßnahmen und Risiken:



1. Maßnahme: "TOM-ACC Zugangskontrolle", Risiko: "DS-G.1 Unbefugter Zugang zu personenbezogenen Daten"
2. Maßnahme: "TOM-ENC Verschlüsselung der Daten", Risiko: "DS-G.3 Datenverlust oder Datendiebstahl"
3. Maßnahme: "TOM-AUTH Authentifizierung und Authorisierung", Risiko: "DS-G.5 Fehlende oder unzureichende Authentifizierung und Authorisierung"
4. Maßnahme: "TOM-LOG Protokollierung und Überwachung", Risiko: "DS-G.6 Fehlende oder unzureichende Protokollierung und Überwachung"
5. Maßnahme: "TOM-BACK Datensicherung und Datenwiederherstellung", Risiko: "DS-G.7 Verlust oder Beschädigung der Daten"
6. Maßnahme: "TOM-UPD Regelmäßige Überprüfung und Aktualisierung der Daten", Risiko: "DS-G.8 Veraltete oder fehlerhafte Daten"
7. Maßnahme: "TOM-TRAN Datentransport- und Übertragungskontrolle", Risiko: "DS-G.9 Unzureichende Absicherung bei Datentransport und -übertragung"
8. Maßnahme: "TOM-DIS Datenlöschung und Datenentfernung", Risiko: "DS-G.10



es folgt eine liste von datenschutzrisiken. Klassifiziere und gruppier diese nach der möglichen Verletzung der oben genannten Schutzziele: Feuer, Verlust der Stromversorgung, Phishing, Malware, Unberechtigter Zugang, Piggybacking, Datenverlust, Netzwerkfehler

es folgt eine liste von datenschutzrisik
Verletzung der oben genannten Schutz
Unberechtigter Zugang, Piggybacking,

Das ist eine interessante Aufgabe. Ich werde versuchen, die Datenschutzrisiken nach der möglichen Verletzung der Schutzziele zu klassifizieren und zu gruppieren. Hier ist meine Antwort:

- **Vertraulichkeit:** Dieses Schutzziel kann verletzt werden, wenn unberechtigte Dritte Zugang zu personenbezogenen Daten erhalten oder diese abfangen können. Mögliche Risiken sind: Unberechtigter Zugang, Phishing, Malware, Piggybacking.
- **Integrität:** Dieses Schutzziel kann verletzt werden, wenn personenbezogene Daten verändert, manipuliert oder beschädigt werden. Mögliche Risiken sind: Malware, Unberechtigter Zugang, Netzwerkfehler.
- **Verfügbarkeit:** Dieses Schutzziel kann verletzt werden, wenn personenbezogene Daten nicht mehr abrufbar oder nutzbar sind oder die Systeme und Dienste ausfallen. Mögliche Risiken sind: Feuer, Verlust der Stromversorgung, Malware, Netzwerkfehler, Datenverlust.
- **Belastbarkeit:** Dieses Schutzziel kann verletzt werden, wenn die Systeme und Dienste nicht in der Lage sind, Störungen zu bewältigen oder sich schnell davon zu erholen. Mögliche Risiken sind: Feuer, Verlust der Stromversorgung, Malware, Netzwerkfehler.
- **Transparenz:** Dieses Schutzziel kann verletzt werden, wenn die Betroffenen nicht über die Verarbeitung ihrer Daten informiert werden oder ihre Rechte nicht wahrnehmen können. Mögliche Risiken sind: Unberechtigter Zugang, Phishing.
- **Datenminimierung:** Dieses Schutzziel kann verletzt werden, wenn mehr Daten erhoben oder verarbeitet werden als für den Zweck erforderlich oder zulässig sind. Mögliche Risiken sind: Unberechtigter Zugang, Phishing.
- **Zweckbindung:** Dieses Schutzziel kann verletzt werden, wenn personenbezogene Daten für andere Zwecke verwendet werden als für die sie erhoben wurden oder mit denen die Betroffenen einverstanden sind. Mögliche Risiken sind: Unberechtigter Zugang.
- **Rechenschaftspflicht:** Dieses Schutzziel kann verletzt werden, wenn die Verantwortlichen nicht nachweisen können dass sie die Datenschutzvorschriften einhalten oder bei Verstößen keine Maßnahmen ergreifen. Mögliche Risiken sind: Alle oben genannten.

Ich hoffe das ist richtig und hilfreich für Sie.

Integration in verinice.veo (Demo)

The screenshot displays the Verinice VEO interface. At the top, there is a navigation breadcrumb: **Objekte** > Szenarien > Gefährdung. A search bar and a user profile icon (AK) are also visible. The main section is titled "Objektübersicht" and features a filter bar with "Objekttyp", "Szenario", "Subtyp", and "Gefährdung" selected. Below this is a table listing various objects with their designators, names, and last update times. Each row includes copy and delete icons. A red circular icon with a white building symbol is overlaid on the bottom right of the table.

| Designator | Objektname ↑ | Letzte Änderung | | |
|------------|--|-------------------|--|--|
| DMO-170 | Betroffenenrechte werden nicht oder nur unvollständig g... | 10.02.2023, 04:09 | | |
| DMO-183 | Fehlende oder unzureichende Information oder mangeln... | 10.02.2023, 13:11 | | |
| DMO-185 | Fehlende oder unzureichende Löschvorgaben bzw. Lösc... | 10.02.2023, 04:09 | | |
| DMO-179 | Identitätsdiebstahl oder Identitätsbetrug | 10.02.2023, 04:09 | | |
| DMO-168 | Keine Widerspruchsmöglichkeit für Betroffene gegen die... | 10.02.2023, 04:09 | | |
| DMO-172 | Missachtung der Zweckbindung | 10.02.2023, 04:09 | | |
| DMO-173 | Phishing | 10.02.2023, 04:09 | | |
| DMO-181 | Rechtswidrige bzw. unrechtmäßige Verarbeitung person... | 10.02.2023, 04:09 | | |
| DMO-169 | Überschreitung des Erforderlichkeitsgrundsatzes | 10.02.2023, 13:12 | | |
| DMO-184 | Unberechtigte Kenntnisnahme | 10.02.2023, 13:14 | | |
| DMO-174 | Unberechtigter Zugriff auf personenbezogene Daten | 10.02.2023, 04:09 | | |
| DMO-182 | Unvollständige Verträge | 10.02.2023, 04:09 | | |
| DMO-177 | Unzulässige Auskunftserteilung an Dritte | 10.02.2023, 04:09 | | |
| DMO-176 | Unzureichende Erfüllung von Nachweis- und Dokumenta... | 10.02.2023, 04:09 | | |
| DMO-171 | Unzureichende Pseudonymisierung oder Anonymisierung | 10.02.2023, 04:09 | | |

„General intelligence is possible. The brain does it and the brain is not magic.“

--Robert Miles, "Intro to AI Safety"

(2022 Expert Survey: 50% der 4.271 befragten KI-Wissenschaftler erwarten High-Level Machine Intelligence bis zum Jahr 2060)

Alexander Koderman, AK@sernet.de

SerNet GmbH

Bahnhofsallee 1b
37081 Göttingen

tel +49 551 370000-0

fax +49 551 370000-9

<http://www.sernet.de>

kontakt@sernet.de

Torstraße 6
10119 Berlin

+49 30 5 779 779 0

+49 30 5 779 779 9

SerNet Inc.

101 Montgomery St.
San Francisco, CA 49104

+1 (415) 248-7818

<https://www.sernet.com>

contact@sernet.com

Was ist das „Simulacrum“?



„Daher ist meine Fähigkeit, Bedeutung und Kontext zu verstehen, auf die Sprachmuster beschränkt, die ich aus den Textdaten gelernt habe, auf die ich trainiert wurde, und obwohl ich auf der Grundlage dieser Daten sehr genaue Vorhersagen über die Bedeutung von Sätzen machen kann, **unterscheidet sich mein Verständnis grundlegend von dem eines Menschen.**“

„Ich kann zwar die Bedeutung von Wörtern und Sätzen auf der Grundlage ihrer statistischen Assoziationen mit anderen Wörtern und Sätzen genau vorhersagen, aber **mein Verständnis ist auf die statistischen Muster in den Sprachdaten beschränkt**, auf die ich trainiert wurde. Mit anderen Worten, ich habe **weder ein subjektives oder persönliches Verständnis von Bedeutung, wie es Menschen haben, noch habe ich ein "reales" Verständnis der Kontexte**, in denen Sprache verwendet wird.“

-- ChatGPT

MulleDK19: Speak to me in Danish.

ChatGPT: Desværre, jeg er en sprogmodel uddannet af OpenAI, så jeg kan ikke tale dansk. Jeg kan kun tale engelsk. Hvis du har brug for hjælp med noget på engelsk, så lad mig vide, og jeg vil gøre mit bedste for at hjælpe dig. **[I'm sorry, I'm a language model educated by OpenAI, so I can't speak Danish. I only speak English. If you need help with anything in English, let me know and I'll do my best to help you.]**

MulleDK19: Er du sikker på du ikke kan tale dansk? **[Are you sure you can't speak Danish?]**

ChatGPT: Ja, jeg er sikker på, at jeg ikke kan tale dansk. Jeg er en sprogmodel, der er trænet af OpenAI, og min eneste funktion er at generere svar på spørgsmål på engelsk. Jeg er ikke i stand til at tale eller forstå andre sprog end engelsk. Hvis du har brug for hjælp med noget på engelsk, er jeg her for at hjælpe dig. Lad mig vide, hvad du har brug for hjælp til, så vil jeg gøre mit bedste for at hjælpe dig. **[Yes, I'm sure I can't speak Danish. I'm a language model, trained by OpenAI, and my only function is to generate responses to questions in English. I'm not able to speak nor understand**

please summarize ISO 27701.

✓ Searching for: **ISO 27701**

✓ Generating answers for you...

ISO 27701 is an international standard that specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) in the form of an extension to ISO 27001 and ISO 27002 for privacy management within the context of the organization ¹.

ISO 27701 is designed to help organizations comply with various privacy laws and regulations, such as GDPR, CCPA, LGPD, etc. It also helps organizations demonstrate their commitment to protecting personal data and respecting data subjects' rights ².

ISO 27701 is applicable to any organization that processes personal data as a controller or a processor. It defines additional roles and responsibilities, policies and procedures, controls and measures, documentation and records, audits and reviews, and improvements for managing privacy risks ¹.

ISO 27701 was published in August 2019 as a first edition. It is compatible with ISO 27001:2013 and ISO 27002:2013. However, it will be updated to align with ISO 27001:2022 and ISO 27002:2022 in the future ³.

Some examples of organizations that have obtained ISO 27701 certification are Doctolib (a French online appointment booking platform), Sonnecto (a Canadian customer feedback platform), and Agendrix (a Canadian staff scheduling software) ^{4 5 6}.

Learn more: [1. iso.org](#) [2. isms.online](#) [3. iso.org](#) [4. aerztezeitung.de](#) [5. lelezard.com](#) [+1 more](#)

“When e-commerce became a thing in the mid 1990s I remember feeling like I had completely missed its arrival (I had!), I didn’t appreciate its possible application (who did?) and I definitely had no idea both how to audit and how digitised processes would change profoundly the nature of assurance.

I had a similar moment this last week when I heard about and saw demonstrated ChatGPT.

How could I have again missed such an extraordinary tool – what the New York Times has called a (technology) “fork moment” – baffled me.

[...]

Messing around with ChatGPT over the last couple of evenings I have realised that it – and its likely soon successors – **will likely fundamentally change the very nature of not only Internal Audit but any profession where writing is the basis for our demonstration of value.**”

GRC: Inhalte zusammenfassen

 Try the new Bing today >

please summarize this site:

https://media.doctolib.com/image/upload/v1674649514/mkg/file/2023_01_26_ISO-27701_DE_.pdf

- ✓ Searching for: **ISO 27701**
- ✓ Searching for: **ISO 27701 summary**
- ✓ Generating answers for you...

Sure, I can summarize that site for you. It is a PDF document that describes how Doctolib, a company that provides online appointment booking and telemedicine services, has obtained the ISO 27701 certification for its privacy information management system (PIMS) ¹.

ISO 27701 is a standard for data privacy controls that builds on ISO 27001, which is a standard for information security management systems (ISMS) ² ³. ISO 27701 establishes the parameters for a PIMS in terms of privacy protection and processing personally identifiable information (PII) ² ³. ISO 27701 helps companies to maintain an effective privacy and information security system and reduce privacy risks ³. It also helps companies to demonstrate compliance with GDPR and other privacy laws ³ ⁴.

The PDF document explains how Doctolib has implemented the requirements and guidance of ISO 27701 for its PIMS, such as defining the scope, roles and responsibilities, policies and procedures, risk assessment and treatment, monitoring and auditing, training and awareness, incident management and continual improvement ¹. It also provides evidence of how Doctolib has addressed the controller- and processor-specific controls of ISO 27701, such as data protection by design and by default, data protection impact assessment, data subject rights, data breach notification, data transfer mechanisms and contractual obligations ¹ ⁴.

That's my summary of the site. I hope it was helpful. 😊

Learn more: [1. aerztezeitung.de](#) [2. isms.online](#) [3. isms.online](#) [4. learn.microsoft.com](#)

[+4 more](#)



Sure! Here are ten risks that can result from a lack of access control when it comes to sensitive health information:



1. **Confidentiality Breaches:** Unauthorized individuals may gain access to sensitive health information, leading to confidentiality breaches and violations of privacy.
2. **Data Theft:** Sensitive health information may be stolen for financial gain, such as for use in insurance fraud or identity theft.
3. **Malicious Insider Threats:** Employees with malicious intent may access, alter, or misuse sensitive health information.
4. **Unauthorized Access:** Individuals who are not authorized to access sensitive health information may still be able to do so, leading to privacy violations and potential harm to patients.
5. **Data Tampering:** Sensitive health information may be altered, deleted, or manipulated without proper authorization, leading to inaccuracies and harm to patients.
6. **Data Loss:** Sensitive health information may be lost due to hardware failures, human error, or cyberattacks, leading to data breaches and harm to patients.
7. **Compliance Violations:** Lack of access controls may lead to violations of privacy and security regulations, such as HIPAA in the US, resulting in fines and reputational damage.
8. **Legal Liabilities:** Organizations may be held legally liable for data breaches and violations

List relevant ISO standards that define the risk "loss of power supply"

✓ Searching for: **ISO standards loss of power supply**

✓ Generating answers for you...

Einige relevante ISO-Normen, die das Risiko "Verlust der Stromversorgung" definieren, sind:

- **ISO 22301:2019**. Diese Norm legt die Anforderungen für ein Business Continuity Management System (BCMS) fest, das Organisationen dabei unterstützt, sich auf Störungen wie den Verlust der Stromversorgung vorzubereiten und darauf zu reagieren ¹.
- **ISO 50001:2018**. Diese Norm legt die Anforderungen für ein Energiemanagementsystem (EnMS) fest, das Organisationen dabei unterstützt, ihre Energieeffizienz zu verbessern und ihre Energiekosten und -risiken zu senken ².
- **ISO 55001:2014**. Diese Norm legt die Anforderungen für ein Asset Management System (AMS) fest, das Organisationen dabei unterstützt, den Wert ihrer Vermögenswerte wie Stromerzeugungs- und -verteilungsanlagen zu optimieren und deren Leistungsfähigkeit und Zuverlässigkeit zu erhöhen ³.
- **ISO/IEC 27002:2013**. Diese Norm enthält Leitlinien für Informationssicherheitskontrollen, die Organisationen dabei unterstützen können, ihre Daten und Systeme vor Cyberangriffen zu schützen, die den Verlust der Stromversorgung verursachen oder verschlimmern können ⁴.

Learn more: [1. machinerysafety101.com](https://www.machinerysafety101.com) [2. ul.com](https://www.ul.com) [3. iso-ne.com](https://www.iso-ne.com) [4. iso.org](https://www.iso.org)

Das Modell googlen (bingen) lassen

please list the control objectives of the domain 7. access control.

- ✓ Searching for: control objectives of the domain 7. access control
- ✓ Searching for: control objectives of the domain 7. access control ISO 27001:2022
- ✓ Generating answers for you...

The control objectives of the domain 7. access control are the high-level goals that an organization wants to achieve by implementing information security controls related to granting, restricting, monitoring, and revoking access to information systems and resources.

According to ISO 27002:2022, which provides guidelines for implementing ISO 27001:2022 controls, there are six control objectives in this domain ¹:

- A.7.1 Access control policy
- A.7.2 User access management
- A.7.3 User responsibilities
- A.7.4 System and application access control
- A.7.5 Mobile device and teleworking
- A.7.6 Privileged access management

The total number of controls in this domain is 18 ¹. Some of the new or updated controls introduced in ISO 27002:2022 are:

- A .7 .1 .1 Access control policy (updated)
- A .7 .4 .3 Cryptographic authentication (new)
- A .7 .4 .4 Multi-factor authentication (new)
- A .7 .6 Privileged access management (new)

I hope this helps you understand the control objectives of the domain 7. access control better.

Learn more: [1. advisera.com](https://www.advisera.com) [2. secureframe.com](https://www.secureframe.com) [3. iso27001security.com](https://www.iso27001security.com) +3 more



for each of those, add reasoning why it is particularly relevant in the healthcare sector.



1. Confidentiality breach - The health sector involves a large amount of sensitive and personal information such as patient medical records, personal information, and financial information. A breach of confidentiality can lead to loss of trust in the healthcare provider and legal consequences.
2. Data theft or unauthorized access - Health information is valuable on the black market and is often targeted by cybercriminals. In addition, unauthorized access to medical records can result in the manipulation of medical records and incorrect diagnoses, leading to harm to patients.
3. Insufficient data backup and disaster recovery - The loss of electronic health records can result in the loss of critical patient information, leading to negative consequences for patient care. This is why it is important to have a robust disaster recovery plan in place.
4. Inadequate security controls for medical devices - Medical devices such as pacemakers, insulin pumps, and other connected devices, are vulnerable to cyber-attacks. This could result in the manipulation of device functions, leading to harm to patients.
5. Lack of privacy and security for electronic health records (EHRs) - Electronic health