31.03.20265

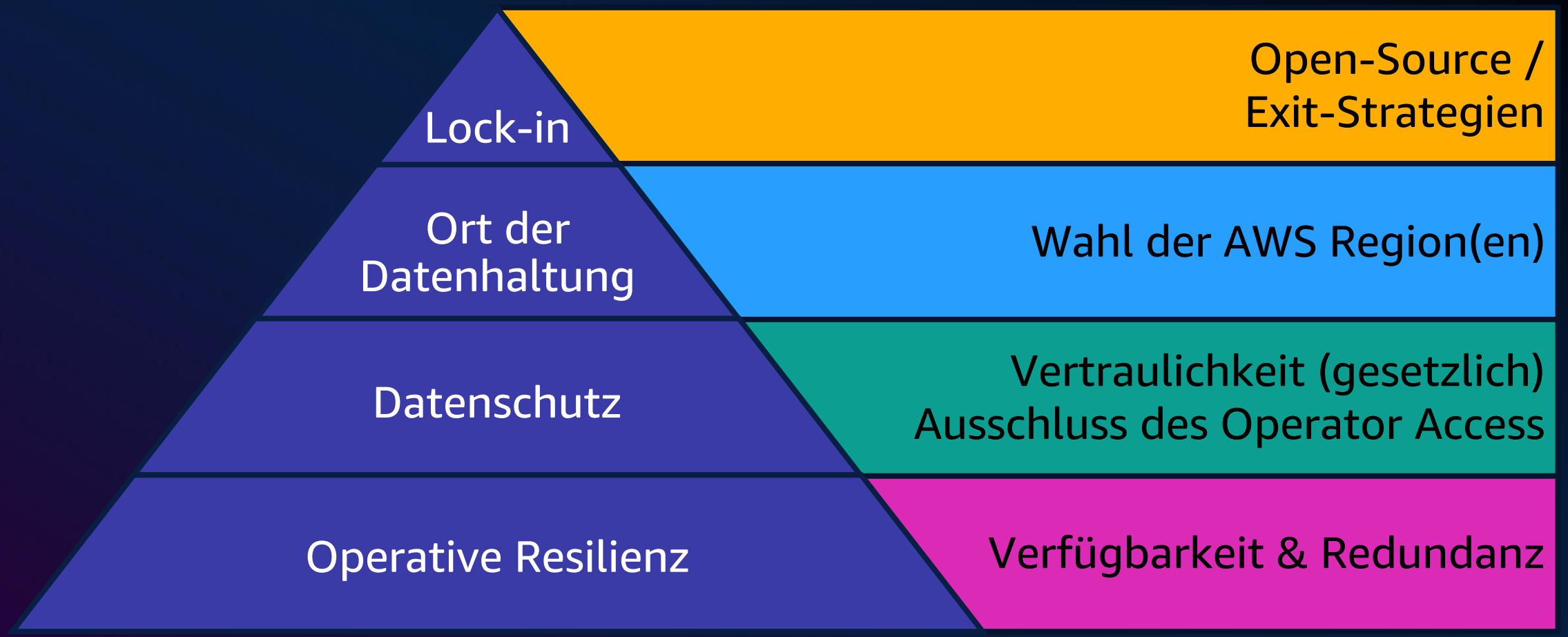
SWICO: INSIGHTS FOR INSIDERS

Digitale Souveränität ermöglichen: Risiko, Compliance und Datenschutz

Daniel Caduff

Security Assurance Principal
AWS

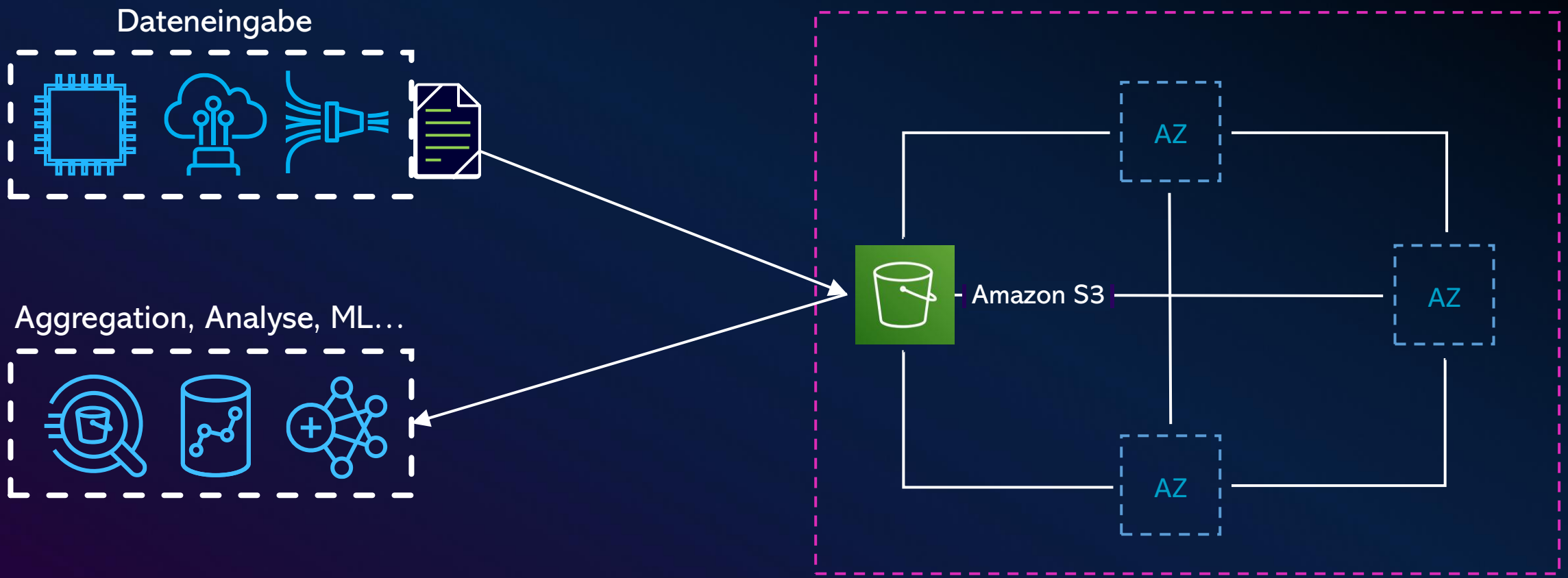
Digitale Souveränität



Operative Resilienz

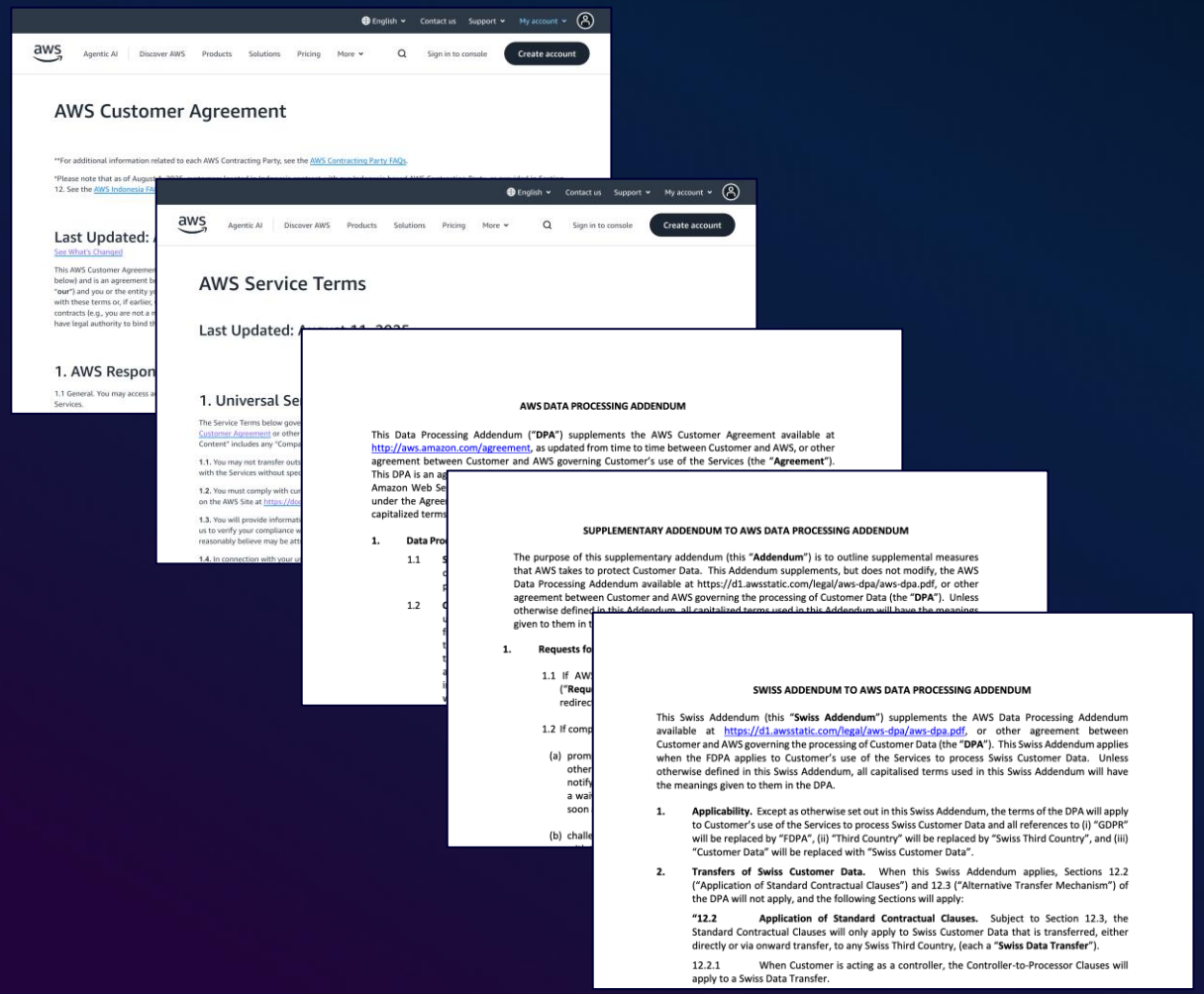
Verteilte, global redundante Infrastruktur

Resilienz durch Redundanz: Daten



Vertraulichkeit und Datenschutz

Datenschutz: Vertragliche Schutzmaßnahmen



- ✓ Sie bestimmen, wo Ihre Daten gespeichert werden
- ✓ Sie bestimmen, wer auf Ihre Daten zugreifen kann
- ✓ AWS greift nicht ohne Ihre Zustimmung auf Ihre Daten zu

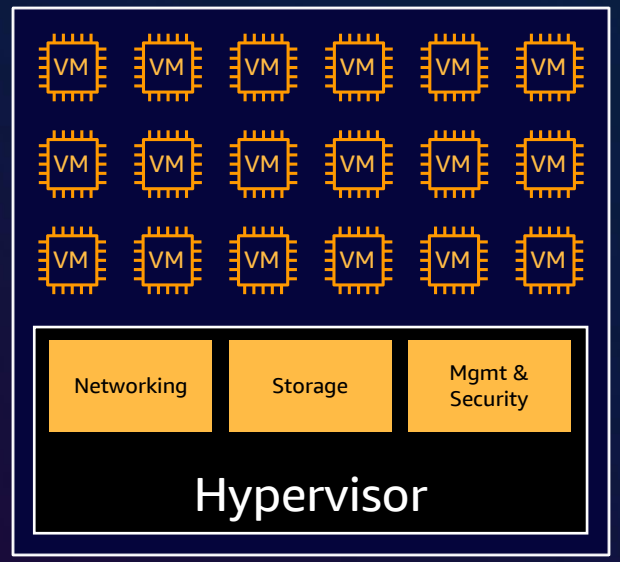
- ✓ Wir leiten Datenanfragen nach Möglichkeit an den Kunden weiter
- ✓ Wir wehren uns gegen übermäßige und unangemessene Datenanfragen (z. B. bei Konflikten mit geltendem lokalem Recht)

- ✓ Übereinstimmung mit Schweizer Recht

https://aws.amazon.com/legal/

Technische Massnahme – Zero Operator Access

Klassische Virtualisierung

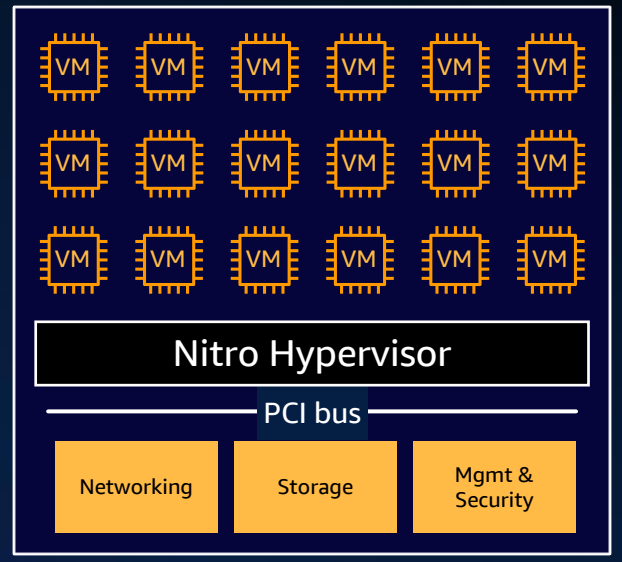


Login

Operator

No Login

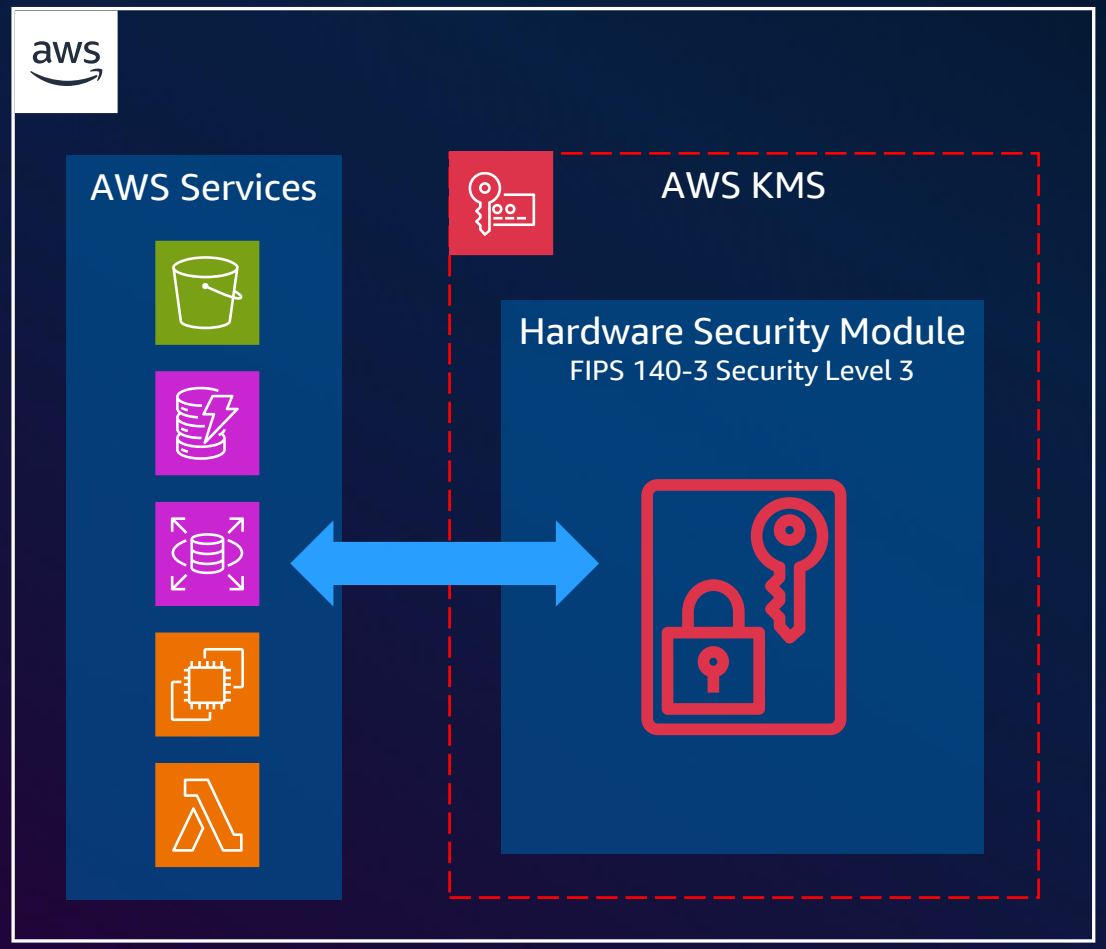
AWS Nitro System



https://aws.amazon.com/trust-center/operator-access/

Verwalten Sie Ihre Schlüssel in der Cloud

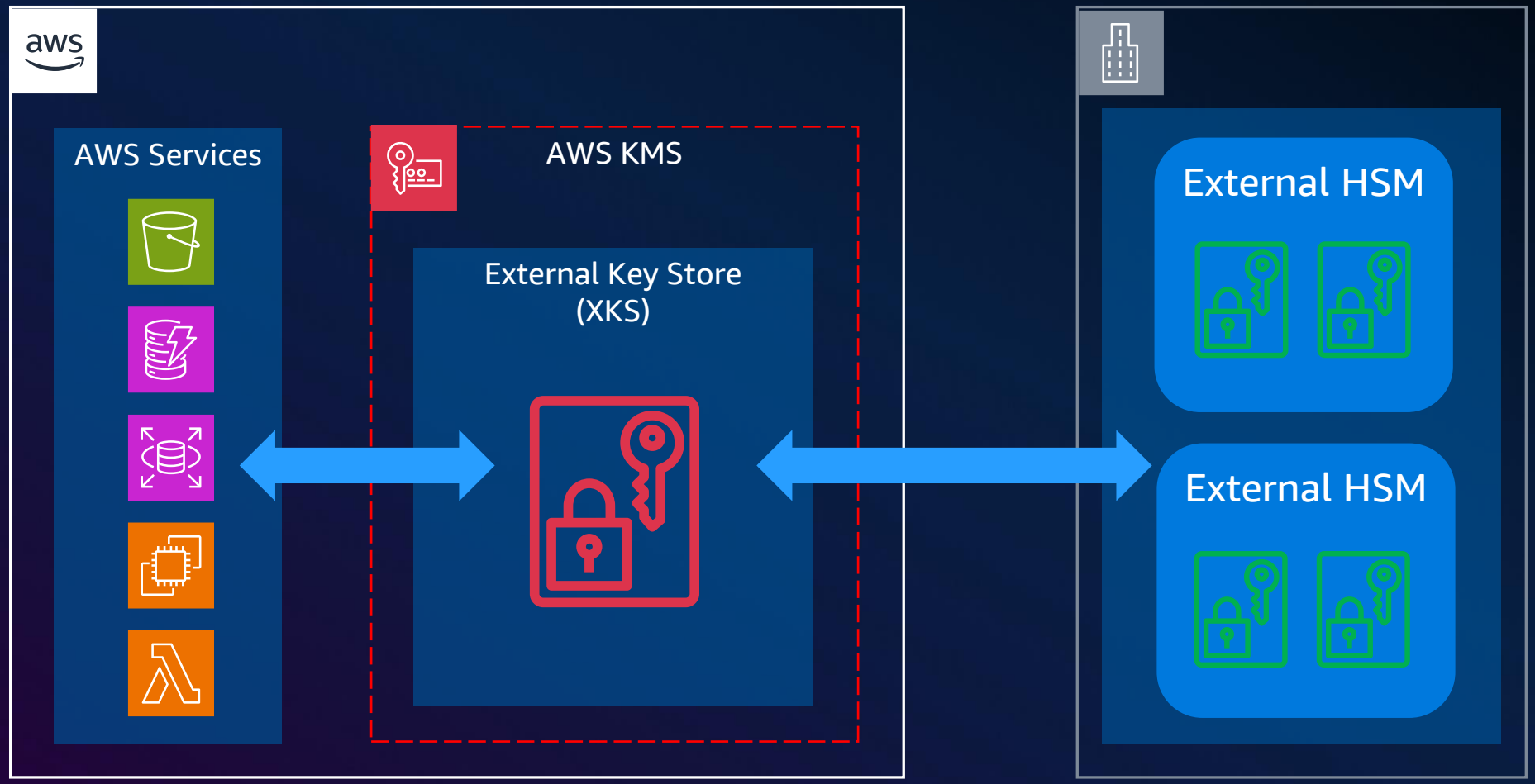
Schlüssel-Verwaltung mit AWS KMS: Von AWS verwaltet, vom Kunden verwaltet und BYOK



Viele AWS-Kerndienste, einschließlich KMS, sind mit Zero Operator Access konzipiert – es gibt keine technischen Möglichkeiten für AWS-Mitarbeiter, auf Kundendaten zuzugreifen.

Verwalten Sie Ihre Schlüssel ausserhalb der Cloud

AWS KMS External Key Store (XKS)



https://docs.aws.amazon.com/kms/latest/developerguide/keystore-external.html

Globale Sicherheitsaudits und - Zertifizierungen

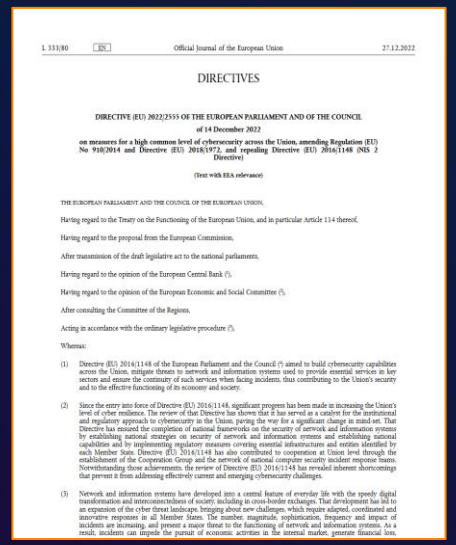
- ✓ 143 Attestierungen und Zertifizierungen von Datenschutz- und Cybersicherheitsstandards weltweit.
- ✓ Kunden können durch den AWS Artifact-Service die vollständigen Audit-Reports herunterladen und prüfen.
- ✓ Vertrauen Sie nicht AWS – Vertrauen Sie Ihrem Auditor!

https://aws.amazon.com/compliance/programs/

Rechtliche Anforderungen

Rechtliche Anforderungen: EU

NIS 2



L 333/80 EN Official Journal of the European Union 27.12.2022

DIRECTIVES

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 14 December 2022
on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)
(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Central Bank (1),

Having regard to the opinion of the European Economic and Social Committee (2),

After consulting the Committee of the Regions,

Acting in accordance with the ordinary legislative procedure (3),

Whereas:

(1) Directive (EU) 2016/1148 of the European Parliament and the Council (4) aimed to build cybersecurity capabilities across the Union, mitigate threats to network and information systems used to provide essential services in key sectors and ensure the continuity of such services when facing incidents, thus contributing to the Union's security and to the effective functioning of its economy and society.

(2) Since the entry into force of Directive (EU) 2016/1148, significant progress has been made in increasing the Union's level of cyber resilience. The review of that Directive has shown that it has served as a catalyst for the institutional and regulatory approach to cybersecurity in the Union, paving the way for a significant change in mind-set. That Directive has ensured the completion of national frameworks on the security of network and information systems by establishing national strategies on security of network and information systems and establishing national capabilities and by implementing regulatory measures covering essential infrastructures and entities identified by each Member State. Directive (EU) 2016/1148 has also contributed to cooperation at Union level through the establishment of the Cooperation Group and the network of national computer security incident response teams. Notwithstanding those achievements, the review of Directive (EU) 2016/1148 has revealed inherent shortcomings that prevent it from addressing effectively current and emerging cybersecurity challenges.

(3) Network and information systems have developed into a central feature of everyday life with the speedy digital transformation and interconnectedness of society, including in cross-border exchanges. That development has led to an expansion of the cyber threat landscape, bringing about new challenges, which require adapted, coordinated and innovative responses in all Member States. The number, magnitude, sophistication, frequency and impact of incidents are increasing, and present a major threat to the functioning of network and information systems. As a result, incidents can impede the pursuit of economic activities in the internal market, generate financial loss,

NIS2 Directive / Eur-Lex

DORA

27.12.2022 EN Official Journal of the European Union L 333/1

I
(Legislative acts)

REGULATIONS

REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 14 December 2022
on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011
(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Central Bank (1),

Having regard to the opinion of the European Economic and Social Committee (2),

Acting in accordance with the ordinary legislative procedure (3),

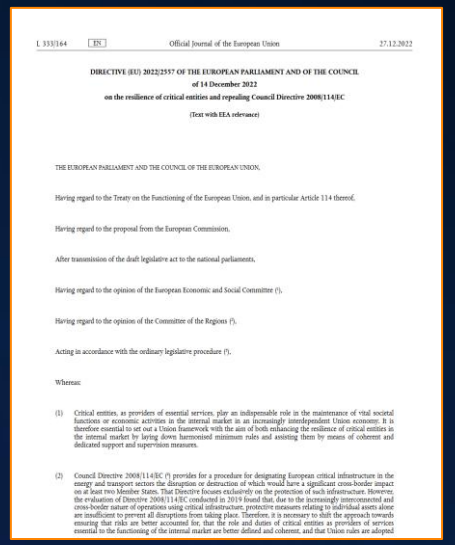
Whereas:

(1) In the digital age, information and communication technology (ICT) supports complex systems used for everyday activities. It keeps our economies running in key sectors, including the financial sector, and enhances the functioning of the internal market. Increased digitalisation and interconnectedness also amplify ICT risk, making society as a whole, and the financial system in particular, more vulnerable to cyber threats or ICT disruptions. While the ubiquitous use of ICT systems and high digitalisation and connectivity are today core features of the activities of Union financial entities, their digital resilience has yet to be better addressed and integrated into their broader operational frameworks.

(2) The use of ICT has in the past decades gained a pivotal role in the provision of financial services, to the point where it has now acquired a critical importance in the operation of typical daily functions of all financial entities. Digitalisation now covers, for instance, payments, which have increasingly moved from cash and paper-based methods to the use of digital solutions, as well as securities clearing and settlement, electronic and algorithmic trading, lending and funding operations, peer-to-peer finance, credit rating, claim management and back-office operations. The insurance sector has also been transformed by the use of ICT, from the emergence of insurance

DORA / EUR-Lex

CER



L 333/164 EN Official Journal of the European Union 27.12.2022

DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 14 December 2022
on the resilience of critical entities and repealing Council Directive 2008/114/EC
(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee (1),

Having regard to the opinion of the Committee of the Regions (2),

Acting in accordance with the ordinary legislative procedure (3),

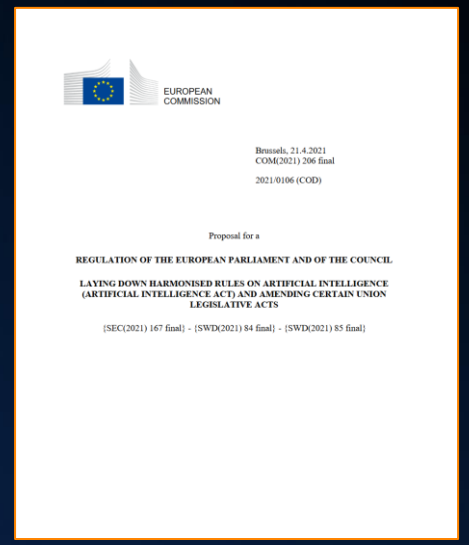
Whereas:

(1) Critical entities, as providers of essential services, play an indispensable role in the maintenance of vital societal functions or economic activities in the internal market in an increasingly interdependent Union economy. It is therefore essential to set out a Union framework with the aim of both enhancing the resilience of critical entities in the internal market by laying down harmonised minimum rules and assisting them by means of coherent and dedicated support and supervision measures.

(2) Council Directive 2008/114/EC (4) provides for a procedure for designating European critical infrastructure in the energy and transport sectors the disruption or destruction of which would have a significant cross-border impact on at least two Member States. That Directive focuses exclusively on the protection of such infrastructure. However, the evaluation of Directive 2008/114/EC conducted in 2019 found that, due to the increasingly interconnected and cross-border nature of operations using critical infrastructure, protective measures relating to individual assets alone are insufficient to prevent all disruptions from taking place. Therefore, it is necessary to shift the approach towards ensuring that risks are better accounted for, that the role and duties of critical entities as providers of services essential to the functioning of the internal market are better defined and coherent, and that Union rules are adopted

CER / EUR-Lex

AI ACT



EUROPEAN COMMISSION

Brussels, 21.4.2021
COM(2021) 206 final

2021/0106 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS

{SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}

AI Act / EUR-Lex

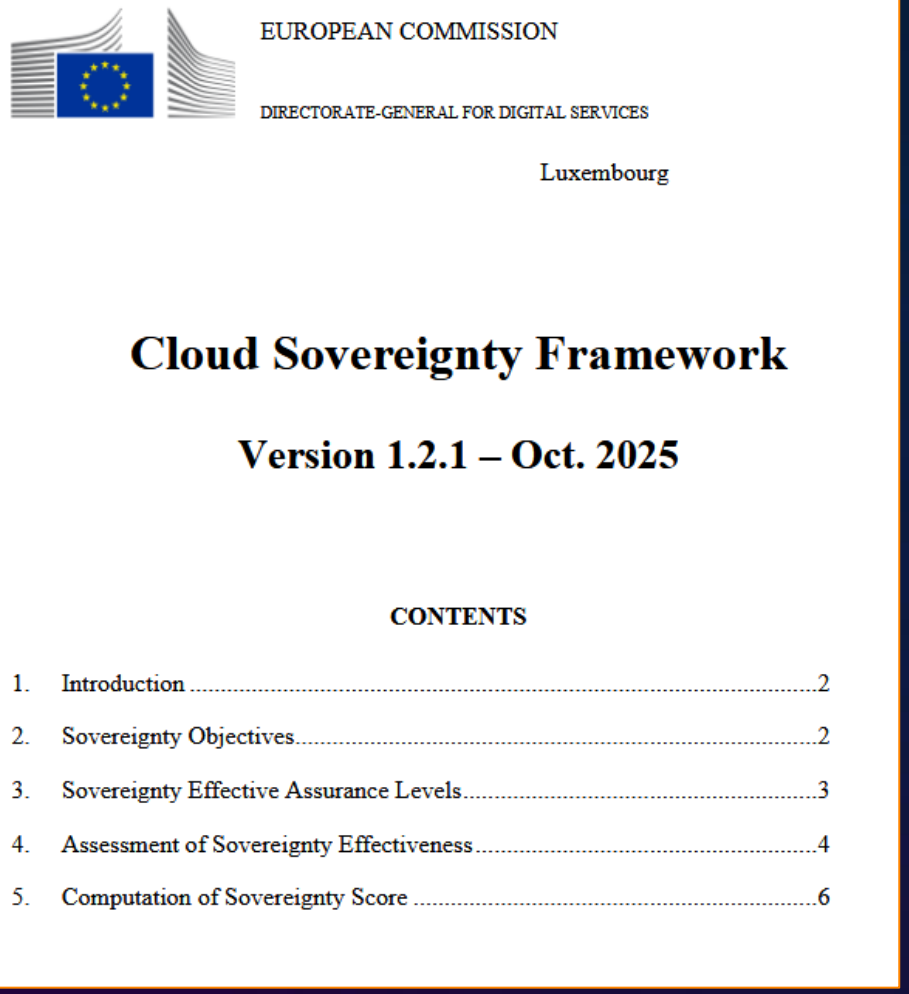
Cybersicherheit

Operative Resilienz

Schutz Kritischer Infrastrukturken

Regulierung von AI

EU Cloud Sovereignty Framework



EUROPEAN COMMISSION

DIRECTORATE-GENERAL FOR DIGITAL SERVICES

Luxembourg

Cloud Sovereignty Framework

Version 1.2.1 – Oct. 2025

CONTENTS

The computation of the Sovereignty Score uses the points allocated to the question proposed in the tender, weighted as below:

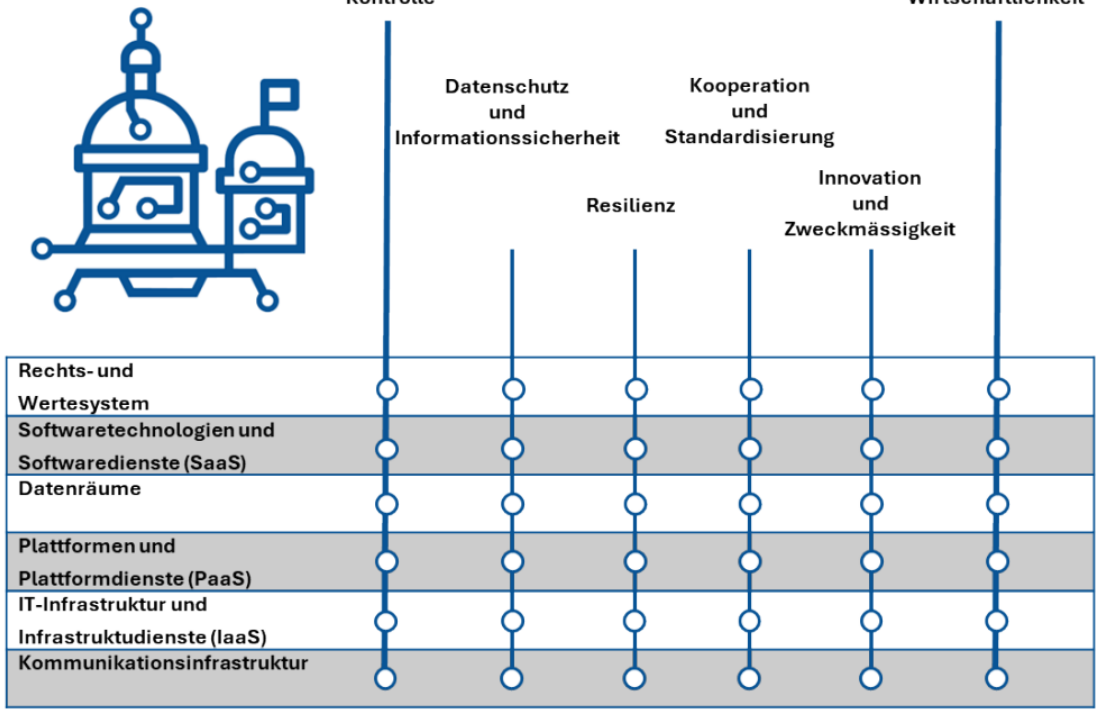
#	Sovereignty Objectives	Weight in Scoring
SOV-1	Strategic Sovereignty	15%
SOV-2	Legal & Jurisdictional Sovereignty	10%
SOV-3	Data & AI Sovereignty	10%
SOV-4	Operational Sovereignty	15%
SOV-5	Supply Chain Sovereignty	20%
SOV-6	Technology Sovereignty	15%
SOV-7	Security & Compliance Sovereignty	10%
SOV-8	Environmental Sustainability	5%
	Total	100%

→ **Anbieterneutral !**

https://commission.europa.eu/document/download/09579818-64a6-4dd5-9577-446ab6219113_en

Digitale Souveränität in der Bundesverwaltung

Ebene	Beschreibung	*Handlungs-spielraum*
8. Rechts- und Wertesystem	*Rechtliche, ethische und sicherheitsbezogene Rahmenbedingungen (Beispiele: Handelsabkommen, E-Identity, Standards).*	
7. Softwaretechnologien und Softwaredienste (SaaS)	*Anwendungen, Betriebssysteme, Middleware und Open-Source-Software, die die Funktionslogik digitaler Systeme bestimmen (Beispiele: Büroautomation, Fachapplikationen, Office-Software, KI-Frameworks).*	
6. Datenräume	*Technische und organisatorische Strukturen, welche die sichere und vertrauenswürdige Bereitstellung, den Austausch und den Bezug von Daten aus verschiedenen Quellen und von verschiedenen Akteuren ermöglicht und regelt (Beispiele: Register, Mobilität, Gesundheit, Finanzen).*	
5. Plattformen und Plattformdienste (PaaS)	*Entwicklungs- und Anwendungsplattformen, Angebote, die Software-Ökosysteme für Unternehmen und Verbraucher bereitstellen. (Beispiele: Kubernetes, Docker, Datenwissenschaftsplattform).*	
4. IT-Infrastruktur und Infrastrukturdienste (IaaS)	*Virtuelle und physische Infrastrukturen, die Rechen-, Speicher- und Netzwerkressourcen über verteilte Systeme ermöglichen (Beispiele: Virtuelle Infrastruktur (Cloud), Storage, VMs, DBs, Rechenzentren, Digitale Arbeitsgeräte).*	
3. Kommunikationsinfrastruktur	*Breitband-, Mobilfunk- und Satellitennetzwerke, die als Rückgrat der digitalen Kommunikation dienen und hohe sicherheitsrelevante Bedeutung haben (Beispiel: Breitbandnetze, Glasfaserinfrastruktur, Mobilfunknetze, Satellitennavigation).*	



→ Anbieterneutral

https://www.bk.admin.ch/bk/de/home/digitale-transformation-ikt-lenkung/vorgaben/w012-weisungen_digitale-souveraenitaet-der-bundesverwaltung.html

PRIVATIM Resolution zur Auslagerung

privatim
Konferenz der schweizerischen Datenschutzbeauftragten
Conférence des préposé(e)s suisses à la protection des données
Conferenza degli incaricati svizzeri per la protezione dei dati

Resolution zur Auslagerung von Datenbearbeitungen in die Cloud

Cloudbasierte Software erscheint heute als so attraktiv wie nie. Infrastrukturen, die potenziell allen Internet-Usern zur Verfügung stehen (sog. «Public Clouds»), erlauben eine dynamische Zuweisung von Rechen- und Speicherleistungen nach dem jeweiligen Bedarf der Kunden. Dieser Skaleneffekt ist umso grösser, je weitreichender – und in der Regel auch internationaler – die Infrastruktur des Cloud-Anbieters ist (man denke an sogenannte «Hyperscaler» wie Microsoft, Google oder Amazon). Nebst Einzelpersonen und Privatunternehmen greifen auch immer mehr öffentliche Organe auf zur direkten Nutzung bereitgestellte Anwendungen («Software-as-a-Service», kurz: SaaS) solcher Anbieter zurück. Auch lässt sich beobachten, dass Anbieter ihre Kunden vermehrt in die Cloud zu drängen versuchen.

Allerdings tragen öffentliche Organe eine besondere Verantwortung gegenüber den Daten ihrer Bürgerinnen und Bürger. Zwar dürfen sie deren Bearbeitung an Dritte auslagern, müssen dabei aber sicherstellen, dass der Datenschutz und die Informationssicherheit gewahrt bleiben. Vor einer Auslagerung von Personendaten in Cloud-Dienste müssen die Behörden deshalb unabhängig von der Sensitivität der Daten die besonderen Risiken im Einzelfall analysieren und mit geeigneten Massnahmen auf ein tragbares Mass reduzieren (vgl. Cloud-Merkblatt von privatim).

Aus folgenden Gründen hält privatim die Auslagerung von besonders schützenswerten oder einer gesetzlichen Geheimhaltungspflicht unterstehenden Personendaten in SaaS-Lösungen von grossen internationalen Anbietern durch öffentliche Organe in den meisten Fällen (wie namentlich M365) für unzulässig:

Fazit: Die Nutzung internationaler SaaS-Lösungen für besonders schützenswerte oder einer gesetzlichen Geheimhaltungspflicht unterstehende Personendaten durch öffentliche Organe ist nur dann möglich, wenn die Daten vom verantwortlichen Organ selbst verschlüsselt werden und der Cloud-Anbieter keinen Zugang zum Schlüssel hat.

Rechtlich nicht bindend («Empfehlungscharakter»)

Unklarer Geltungsbereich («SaaS-Lösungen»)

Bestätigt, dass Verschlüsselung ein Lösungsansatz ist

https://www.privatim.ch/wp-content/uploads/2025/11/20251124_privatim_Resolution-Hyperscaler_DE.pdf

Swiss-U.S. Data Privacy Framework

Medienmitteilung des Eidgenössischen Justiz- und Polizeidepartementes

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement

Veröffentlicht am 14. August 2024

Swiss-U.S. Data Privacy Framework:
Zertifizierte US-Unternehmen bieten einen angemessenen Schutz für Personendaten

Bern, 14.8.2024 - Der neue Datenschutzrahmen ermöglicht einen sicheren Austausch von Personendaten zwischen der Schweiz und den zertifizierten US-Unternehmen. Zu diesem Schluss kommt der Bundesrat an seiner Sitzung vom 14. August 2024 und setzt die USA in diesem Umfang auf die Liste der Länder mit einem angemessenen Datenschutzniveau. Insbesondere die Zertifizierung für US-Unternehmen und ein neues US-Datenschutzgericht erlauben künftig die Übermittlung von Personendaten aus der Schweiz an zertifizierte Unternehmen in die USA ohne zusätzliche Garantien. Der Bundesrat setzt die entsprechende Änderung der Datenschutzverordnung auf den 15. September 2024 in Kraft.

Zertifizierte US-Unternehmen bieten einen angemessenen Schutz für Personendaten

Das Swiss-US Data Privacy erlaubt die Übermittlung von Personendaten ohne zusätzliche Garantien!
– Dies gilt trotz Cloud Act und FISA -

Die Zertifizierung für US-Unternehmen bestätigt, dass die erforderlichen Datenschutzmaßnahmen und Datenschutzgarantien eingehalten werden

https://www.news.admin.ch/de/nsb?id=102054

Lösungen für Kritische Infrastrukturen in der Schweiz





Umgang mit dem Cloud Act

Clarifying Lawful Overseas Use of Data Act

Recht zur Anfechtung

Anfechtung von Anfragen, die übermäßig sind oder in Fällen, in denen die Anfrage mit lokalem Recht in Konflikt steht

Verschlüsselung

Alle AWS-Services bieten die Möglichkeit, Daten im Ruhezustand und während der Übertragung zu verschlüsseln

Informations-anfragen

Halbjährlicher Bericht über Informations-anfragen, die von Strafverfolgungs-behörden an AWS gestellt werden.

Offenlegungen

Anzahl Anfragen, die zur Offenlegung von Kundendaten, die sich außerhalb der USA befinden an US-Behörden führten

https://aws.amazon.com/compliance/amazon-information-requests/

Lock-In vermeiden

Risikomanagement bei Lock-In Risiken

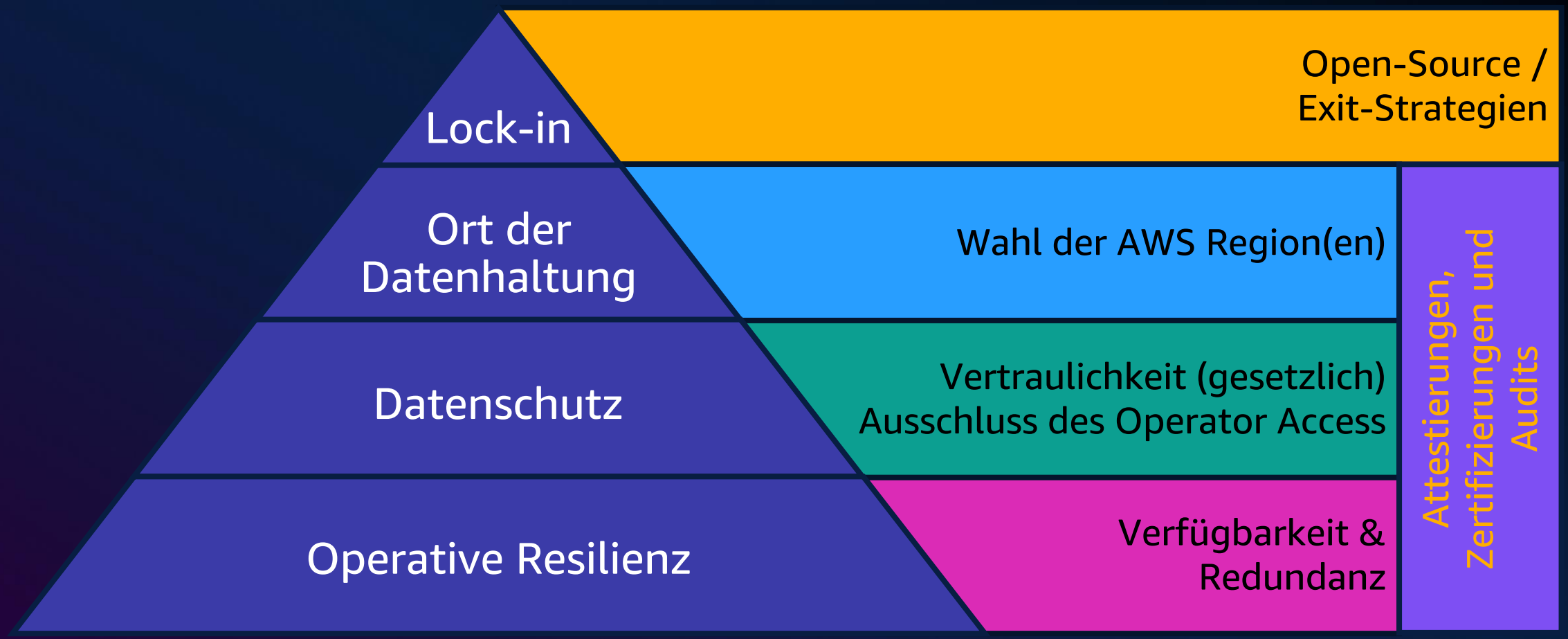
Kosten:
Notwendiger Aufwand, um auf eine alternative Lösung / Produkt zu wechseln.

Nutzen:
Vorteile im Vergleich zu den verfügbaren Alternativen

Zukünftige Anforderungen berücksichtigen:
Wie werden sich meine geschäftlichen Bedürfnisse zukünftig entwickeln?

https://martinfowler.com/articles/oss-lockin.html

Digitale Souveränität



Vielen Dank!

Daniel Caduff
Principal Security Assurance
D/A/CH

Download
Digital Business Card

Connect on
LinkedIN

AWS Trust Center
→ Landing page

Contractual Framework

AWS Encryption Solutions Overview

AWS ALPS Blog
→ Swiss content

AWS Compliance Programs

AWS Fault Isolation Boundaries

Find a Partner

Clarifying Lawful Overseas Use of Data (CLOUD) Act

Unpicking Vendor Lock-in

Weiterführende Quellen

AWS Trust Center: https://aws.amazon.com/de/trust-center/

Five Facts about Cloud Act https://tiny.amazon.com/16hg6lkmu/awsamazdeblogsecufive

AWS Data Processing Addendum (DPA) : https://d1.awsstatic.com/legal/aws-dpa/aws-dpa.pdf

Swiss Addendum to AWS DPA: https://tiny.amazon.com/72p2j2pw/d1awsslegaawsdswispdf

Zero Operator Access on AWS NITRO: https://tiny.amazon.com/17k2nc6f6/nccgmedidqmn_nccpdf

Zero Operator Access on AWS KMS: https://aws.amazon.com/kms/

AWS Compliance Center Switzerland: https://tiny.amazon.com/7ym30p9v/awsamazfinach