IDW PS 860

Bericht über die Angemessenheitsprüfung des Cloud-Service Avvia

Hyperscaler-Umgebung: Amazon Web Services (AWS)

30. Juni 2024
Arvato Systems GmbH
Gütersloh, Deutschland

Dr. Stückmann und Partner mbB
Wirtschaftsprüfungsgesellschaft
Steuerberatungsgesellschaft

Elsa-Brändström-Straße 7
33602 Bielefeld
www.stueckmann.de

HLB STÜCKMANN.

INHALTSVERZEICHNIS

Abkürzungsverzeichnis 4

Abbildungsverzeichnis 4

Prüfungsbericht des unabhängigen Wirtschaftsprüfers über die Prüfung einer Erklärung der gesetzlichen Vertreter Erstellt durch HLB Dr. Stückmann und Partner mbB 5

Anlage 1
Darstellung des Cloud-Serviceangebot „Avvia“ in der Hyperscaler-Umgebung von Amazon Web Services (AWS) (Erklärung der gesetzlichen Vertreter)
Erstellt durch Arvato Systems GmbH 10

1. Unternehmenshintergrund 11
2. Arvato Systems-Gruppe 11
3. Arvato Systems Services 12
4. Produktbeschreibung: Cloud-Service „Avvia” 13
5. Informationssicherheitsmanagement 15
6. Informationssicherheitsmaßnahmen 18
7. Personalsicherheit 21
8. Asset Management 22
9. Service Desk 23
10. Konfigurationsmanagement 23
11. Ereignisverwaltung und Überwachung 24
12. Störungsmanagement 25
13. Dokumentationen 26
14. Zugangskontrollen und Berechtigungsmanagement 26
15. Kryptografie, Schlüsselmanagement und Backup 29
16. Lieferantenmanagement 31
17. Business Continuity Management 32
18. Umgang mit Ermittlungsfragen staatlicher Stellen 36

Anlage 2
Darstellung der durchgeführten Prüfungshandlungen, geprüften Grundsätze, Verfahren und Maßnahmen sowie deren Ergebnisse
Erstellt durch HLB Dr. Stückmann und Partner mbB 37

1. Organisation der Informationssicherheit (OIS) 38
2. Sicherheitsrichtlinien und Arbeitsanweisungen (SP) 43
3. Personal (HR) 45
4. Asset Management (AM) 48
5. Regelbetrieb (OPS) 52
6. Identitäts- und Berechtigungsmanagement (IDM) 66
7. Kryptographie und Schlüsselmanagement (CRY) 75
8. Steuerung und Überwachung von Dienstleistern und Lieferanten (SSO) 78
9. Umgang mit Sicherheitsvorfällen (SIM) 84
10. Kontinuität des Geschäftsbetriebs und Notfallmanagement (BCM) 87
11. Compliance (COM) 91
12. Umgang mit Ermittlungsfragen staatlicher Stellen (INQ) 94

Anlage 3

Allgemeine Auftragsbedingungen 96

ABKÜRZUNGSVERZEICHNIS

Abkürzung	Beschreibung
BCM	Business Continuity Management
BIA	Business Impact Analyse
CERT	Computer Emergency Response Team
CMDB	Configuration Management Database
CVSS	Common Vulnerability Scoring System
IaC	Infrastructure as Code
IAM	Identity Access Management
ISMS	Informationssicherheitsmanagementsystem
ISO	Information Security Officer
ISREG	Information Security Regulation
PAM	Priviledged Access Management
PDCA	Plan-Do-Check-Act
TLS	Transport Layer Security

ABBILDUNGSVERZEICHNIS

Abbildung	Beschreibung	Seite
Abb. 1	ISMS-Dokumentenhierarchie	18
Abb. 2	Überblick Configuration Management Database	24
Abb. 3	Ereignisüberwachung	25
Abb. 4	IAM-Prozess	29
Abb. 5	BCM-Organisation und Meldewege	34

PRÜFUNGSBERICHT DES UNABHÄNGIGEN WIRTSCHAFTSPRÜFERS ÜBER DIE PRÜFUNG EINER ERKLÄRUNG DER GESETZLICHEN VERTRETER

ERSTELLT DURCH

HLB DR. STÜCKMANN UND PARTNER MBB

PRÜFUNGSBERICHT DES UNABHÄNGIGEN WIRTSCHAFTSPRÜFERS ÜBER DIE PRÜFUNG EINER ERKLÄRUNG DER GESETZLICHEN VERTRETER

An die gesetzlichen Vertreter der

Arvato Systems GmbH, Gütersloh, Deutschland,
– im Folgenden kurz “Arvato Systems”, “Gesellschaft” oder „Cloudanbieter“ –

Auftrag

Wir haben die in der Anlage 1 beigefügte Erklärung der gesetzlichen Vertreter zur Beschreibung der von Arvato Systems für die Cloud-Serviceerbringung „Avvia“ in der Hyperscaler-Umgebung von Amazon Web Service (AWS) umzusetzenden Maßnahmen sowie die Geeignetheit und Implementierung dieser Maßnahmen zum 30. Juni 2024 mit hinreichender Sicherheit geprüft. Die Maßnahmen sind geeignet, wenn sie den Risiken der Nichterreichung der untengenannten Kriterien mit hinreichender Sicherheit begegnen.

Verantwortung der gesetzlichen Vertreter

Die gesetzlichen Vertreter der Arvato Systems sind für die Aufstellung der Erklärung des Cloud-Anbieters verantwortlich. Dies schließt die Verantwortung für die internen Kontrollen ein, die sie als notwendig erachten, um eine Erklärung aufzustellen, die frei von wesentlichen - beabsichtigten und unbeabsichtigten - Fehlern ist.

Des Weiteren sind die gesetzlichen Vertreter dafür verantwortlich, dass die Maßnahmen gemäß den unten genannten Kriterien in allen wesentlichen Belangen

- so konzipiert werden, dass sie geeignet sind,
- implementiert werden und wirksam sind, d.h. auch
- überwacht und dokumentiert werden.

Aufgrund bestehender inhärenter Grenzen von Systemen können diese Maßnahmen die Kriterien nur mit hinreichender statt absoluter Sicherheit erfüllen.

Die Kriterien zur Aufstellung der Erklärung der gesetzlichen Vertreter sowie zur Geeignetheit der umzusetzenden Maßnahmen umfassen die in dem IDW Prüfungshinweis: Die Prüfung von Cloud-Diensten (IDW PH 9.860.3 n.F.) (10.2021) für das Servicemodell „Avvia“ in der Hyperscaler-Umgebung von AWS enthaltenen Ziele.

Folgende BSI C5 Kriterienbereiche waren nicht Teil der Beschreibung der gesetzlichen Vertreter, weil sie ausschließlich im Verantwortungsbereich von AWS liegen:

- Physische Sicherheit (PS)
- Kommunikationssicherheit (COS)
- Portabilität und Interoperabilität (PI)
- Beschaffung, Entwicklung und Änderung von Informationssystemen (DEV)
- Produktsicherheit (PSS)

Verantwortung des Wirtschaftsprüfers

Unsere Aufgabe ist es, auf der Grundlage unserer Prüfung ein Urteil mit hinreichender Sicherheit darüber abzugeben, ob die Erklärung der gesetzlichen Vertreter in allen wesentlichen Belangen frei von wesentlichen Fehlern ist. Dieses Urteil erstreckt sich auch darauf, ob die in der Erklärung der gesetzlichen Vertreter beschriebenen und von Arvato Systems umzusetzenden Maßnahmen in allen wesentlichen Belangen

- geeignet und
- zum 30. Juni 2024 implementiert waren.

Wir haben unsere Prüfung unter Beachtung des IDW Prüfungsstandards: IT-Prüfung außerhalb der Abschlussprüfung (IDW PS 860) und des IDW Prüfungshinweises: Die Prüfung von Cloud-Diensten (IDW PH 9.860.3 n.F.) (10.2021) durchgeführt.

Die in der Beschreibung der gesetzlichen Vertreter (Anlage 1) dargestellten Kriterien, die nicht Teil der Beschreibung waren, waren ebenso nicht Prüfungsgegenstand.

Unsere Wirtschaftsprüfungsgesellschaft hat die Anforderungen an das Qualitätssicherungssystem des IDW Qualitätssicherungsstandards: Anforderungen an das Qualitätsmanagement in der Wirtschaftsprüferpraxis (IDW QMS 1 (09.2022)) angewendet. Die Berufspflichten gemäß der WPO und der BS WP/vBP einschließlich der Anforderungen an die Unabhängigkeit haben wir eingehalten.

Nach diesen Anforderungen haben wir die Prüfung so zu planen und durchzuführen, dass wir mit hinreichender Sicherheit die vorgenannten Urteile abgeben können.

Eine Prüfung gemäß IDW PS 860 und IDW PH 9.860.3 n.F. (10.2021) umfasst die Durchführung von Prüfungshandlungen zur Erlangung ausreichender geeigneter Prüfungsnachweise, um entsprechende Prüfungsurteile abgeben zu können. Dies schließt die Beurteilung von Risiken wesentlicher - beabsichtigter oder unbeabsichtigter - Fehler in der Erklärung der gesetzlichen Vertreter ein. Eine Prüfung umfasst auch die Beurteilung der bei der Aufstellung der Erklärung der gesetzlichen Vertreter angewandten Grundsätze, Verfahren und Maßnahmen sowie der Vertretbarkeit des von den gesetzlichen Vertretern ausgeübten Ermessens.

Ziel hierbei ist es jedoch nicht, ein Prüfungsurteil über das für die Aufstellung der Erklärung der gesetzlichen Vertreter relevante interne Kontrollsystem abzugeben.

Für die Beurteilung der umzusetzenden Maßnahmen ist die Prüfung so zu planen und durchzuführen, dass wesentliche Mängel der Geeignetheit und Implementierung der umgesetzten Maßnahmen mit hinreichender Sicherheit aufgedeckt werden. Diese Prüfung umfasst die Durchführung von Prüfungshandlungen im Rahmen einer Aufbauprüfung zur Erlangung ausreichender geeigneter Prüfungsnachweise, um ein entsprechendes Prüfungsurteil abgeben zu können.

Prüfungshandlungen und Prüfungsfeststellungen

Die Auswahl der Prüfungshandlungen liegt im pflichtgemäßen Ermessen des Wirtschaftsprüfers. Im Rahmen unseres Auftrags haben wir u.a. die folgenden Prüfungshandlungen überwiegend auf der Basis einer Auswahl durchgeführt:

- Befragung von Mitarbeitern
- Einsichtnahme in Unterlagen und Dokumentationen, wie bspw. Richtlinien, Arbeits- und Verfahrensanweisungen, Prozessdokumentationen
- Durchsicht von Nachweisen über die Umsetzung und Durchführung der Maßnahmen
- Systemeinsichtnahmen

Die Ergebnisse der von uns durchgeführten Prüfungshandlungen sowie die im Rahmen unserer Prüfung getroffenen Feststellungen sind in Anlage 2 aufgeführt.

Wir sind der Auffassung, dass die von uns erlangten Prüfungsnachweise ausreichend und geeignet sind, um als Grundlage für unser Prüfungsurteil zu dienen.

Prüfungsurteil

Nach unserer Beurteilung

- ist die Erklärung der gesetzlichen Vertreter in allen wesentlichen Belangen frei von wesentlichen Fehlern,
- waren die in der Erklärung der gesetzlichen Vertreter beschriebenen und vom Unternehmen umzusetzenden Maßnahmen in allen wesentlichen Belangen
    - geeignet und
    - zum geprüften Zeitpunkt (30. Juni 2024) implementiert.

Inhärente Grenzen des geprüften für die Erbringung von Cloud-Diensten relevanten IT-Systems

Auch ein wirksames System unterliegt inhärenten Grenzen, so dass möglicherweise die Kriterien in wesentlichen Belangen nicht eingehalten werden, ohne dass dies systemseitig rechtzeitig erkannt und verhindert bzw. aufgedeckt wird.

Die Erklärung der gesetzlichen Vertreter zu den umzusetzenden Maßnahmen wurde zum 31. Mai 2024 erstellt; die Ausführungen zu den Prüfungshandlungen zur Beurteilung der Geeignetheit und Implementierung dieser Maßnahmen beziehen sich auf den Zeitpunkt zum 30. Juni 2024.

Eine Übertragung dieser Angaben auf einen zukünftigen Zeitpunkt birgt die Gefahr, dass aufgrund von durchgeführten Änderungen der Grundsätze, Verfahren und Maßnahmen falsche Schlussfolgerungen gezogen werden.

Verwendete Kriterien sowie Verwendungsbeschränkung

Ohne unser Urteil einzuschränken, verweisen wir auf die im Abschnitt "Verantwortung der gesetzlichen Vertreter" beschriebenen Kriterien, die für Zwecke der Informationssicherheit des Cloud-Dienstes konzipiert wurden. Die umzusetzenden Maßnahmen wurden durch Arvato Systems abgegrenzt und beinhalten daher möglicherweise nicht jeden Aspekt, der aus individueller Sicht eines vorgesehenen Nutzers oder seines Abschlussprüfers ggf. von Bedeutung sein könnte.

Auftragsbedingungen

Wir erteilen diesen Prüfungsbericht auf Grundlage des mit der Gesellschaft geschlossenen Auftrags, dem auch mit Wirkung gegenüber Dritten die diesem Prüfungsbericht beigefügten Allgemeinen Auftragsbedingungen (AAB) vom 1. Januar 2024 (Anlage 3) zugrunde liegen.

Bielefeld, 17. Dezember 2024

HLB Dr. Stückmann und Partner mbB
Wirtschaftsprüfungsgesellschaft
Steuerberatungsgesellschaft

DocuSigned by:
A4919FBBCE864AF...
Gregor Teipel
Wirtschaftsprüfer

DocuSigned by:
4F1F83E9A6C64B6...
André Schneider
Certified Information Systems Auditor
(CISA)

ANLAGE 1

DARSTELLUNG DES CLOUD-SERVICEANGEBOT „AVVIA“ IN DER HYPERSCALER-UMGEBUNG VON AMAZON WEB SERVICES (AWS)

(ERKLÄRUNG DER GESETZLICHEN VERTRETER)

ERSTELLT DURCH
ARVATO SYSTEMS GMBH

DARSTELLUNG DES CLOUD-SERVICE „AVVIA“

1. UNTERNEHMENSHINTERGRUND

Arvato Systems ist ein international tätiges Dienstleistungsunternehmen und einer von acht Unternehmensbereichen der Bertelsmann SE & Co. KGaA, Gütersloh ("Bertelsmann").

Mehr als 80.000 Mitarbeiter in rund 50 Ländern entwickeln und implementieren innovative Lösungen für Geschäftskunden auf der ganzen Welt. Dazu gehören SCM- und IT-Lösungen sowie Finanz- und Kundenkommunikationsdienste, die kontinuierlich mit dem Fokus auf Innovationen in den Bereichen Automatisierung und Daten-Analytik weiterentwickelt werden.

Weltweit renommierte Unternehmen aus den unterschiedlichsten Branchen - von Telekommunikationsanbietern und Energieversorgern über Banken und Versicherungen bis hin zu E-Commerce-, IT- und Internet-Anbietern - vertrauen auf das Lösungsportfolio der Arvato-Gruppe.

2. ARVATO SYSTEMS-GRUPPE

Die global aufgestellte Arvato Systems-Gruppe - im folgenden Arvato Systems - unterstützt als IT-Spezialist mit seinen Einzelgesellschaften große Unternehmen bei der digitalen Transformation. Mehr als 3.400 Mitarbeiter an über 25 Standorten in Deutschland, Schweiz, Rumänien, USA, Malaysia und Lettland stehen für tiefgreifendes Technologie-Know-how, Branchenkenntnis und Kundenorientierung. Im Team entwickelt Arvato Systems innovative IT-Lösungen, bringt unsere Kunden in die Cloud, integriert digitale Prozesse und übernimmt den Betrieb und Support von IT-Systemen.

Arvato Systems bietet

- umfassende IT-Lösungen für den Handel, die Medienbranche sowie für Versorgungsunternehmen und das Gesundheitswesen
- langjährige Erfahrung in der digitalen Transformation
- Kompetenz in Schlüsselbereichen wie Künstliche Intelligenz, Cloud Computing, IT-Security, BPM, Customer Experience und E-Commerce
- Know-how in robusten Technologien und ein starkes Partner-Ökosystem mit Unternehmen wie Amazon Web Services (AWS), Google, Microsoft und SAP
- ein breites Spektrum an Infrastrukturdiensten, einschließlich Managed Services, und ein entsprechendes Anwendungsmanagement

Zur permanenten internen und externen Kontrolle und Qualitätssteigerung des Informationssicherheitsmanagementsystem (ISMS) ist Arvato Systems seit 2006 nach der international anerkannten Norm ISO/IEC 27001 zertifiziert. Diese Norm erfordert ein jährliches internes und externes Auditverfahren.

Ein Verlust der Geschäftsfähigkeit kann direkte Auswirkungen auf die Wettbewerbsfähigkeit, das Vertrauen von Kunden und Geschäftspartner sowie auf das öffentliche Image haben. Arvato Systems ist sich dieser Tatsache bewusst und hat sich einer Zertifizierung nach dem international anerkannten Standard ISO 22301 unterziehen lassen und ist seit 2019 entsprechend zertifiziert. Diese Norm erfordert ebenfalls ein jährliches internes und externes Auditverfahren.

Mit dem implementierten Business Continuity Management (BCM) werden zeitkritische Geschäftsprozesse bei Arvato Systems identifiziert und gegen ungeplante Unterbrechungen durch einen Vorfall mit hohem Schadenspotenzial abgesichert. Dabei geht das BCM auf vorhersehbare Sicherheitsvorfälle ein, die ein Risiko für die Ressourcenverfügbarkeit in den folgenden Bereichen darstellen können:

– Personal
– Gebäude und Gebäudeinfrastruktur
– IT
– Dienstleister

3. ARVATO SYSTEMS SERVICES

Das breite Produkt- und Dienstleistungsspektrum der Arvato Systems reicht von Standard- und Individualsoftwareentwicklungen über komplette ERP-Systeme, zuverlässige Business Intelligence- und Logistiklösungen, Geschäftsprozessmanagement, Softwarelösungen für diverse Branchen bis hin zu innovativen Lösungen zur Kundenbindung.

Arvato Systems bietet umfassende IT-Lösungen für die Branchen Handel, Logistik/Versand, Produktion und Medien sowie für Versorgungsunternehmen und öffentliche Verwaltungen, basierend auf Kompetenzen in den Kernbereichen Business Process Management (BPM), Cloud Computing, Customer Relationship Management (CRM) und E-Commerce.

Dienstleistungen und Lösungen sind:

– Services für Geschäftsanwendungen
– Beratung & Projektleitung
– Infrastruktur-Dienstleistungen
– Bürodienstleistungen
– Sprachdienste und Call Center-Lösungen

4. PRODUKTBESCHREIBUNG: CLOUD-SERVICE “AVVIA”

Die Arvato Systems-Gruppe ist mit ihren Tochtergesellschaften seit vielen Jahren im Cloud Geschäft etabliert und pflegt enge Partnerschaften mit den führenden Anbietern im Markt: Amazon Web Services (AWS), Google, Microsoft und SAP. Aus diesen haben sich tiefgehende Kompetenz- und Know-How-Gebiete in Bezug auf die jeweiligen Hyperscaler-Plattformen entwickelt. Zusätzlich dazu bietet Arvato Systems seit mehreren Jahren auch erfolgreich eine eigene Virtual Private Cloud (VPC) inklusive Services für sensiblere Workloads an. Mit diesem Portfolio bedienen die Unternehmen der Arvato Systems-Gruppe den Cloud-Markt mit steigender Nachfrage und können insbesondere auch Multi-Cloud Bedarfe abdecken.

Arvato Systems hat erkannt, dass es speziell für diesen zunehmenden Bedarf, Cloud-IT unternehmensweit strukturiert und skalierbar einsatzfähig zu machen, eines umfassenden Leistungsportfolios bedarf, das sich aus einem passgenauen Maß an Standardisierung und Automatisierung zusammensetzt und dabei die Best Practice-Erfahrungswerte von Arvato Systems aus vergangenen Cloud Transformationen aufgreift und bereitstellt. Alle diese Punkte werden durch Avvia realisiert.

Avvia ist der Baukasten für moderne Cloud-IT der Arvato Systems-Gruppe. Alle darin befindlichen Komponenten sind darauf ausgelegt, eine Cloud Journey nach ganzheitlichen, unabhängigen und sicheren IT-Kriterien aufzuzeichnen. Alle Module und Services basieren auf Best-Practices und erprobten Verfahren sowie Templates und ermöglichen dadurch einen schnellen und einfachen Einstieg in moderne Cloud-IT im Unternehmensmaßstab, der zugleich durch seine Modularität individuell und passgenau gestaltet werden kann.

Mit Avvia wird das Prinzip „so viel Individualisierung wie nötig und so viel Standardisierung wie möglich“ verfolgt. Dabei wird einerseits auf Standard-Templates, Best Practices und Automatisierungstechniken zurückgegriffen, aber gleichzeitig – wo es sinnvoll und notwendig ist – individueller Spielraum vorgesehen. So wird ein effizienter und effektiver Weg in die Cloud bei hohem Sicherheitsniveau möglich.

Auf technischer Ebene werden mit Avvia komplette IT-Landschaften als Infrastructure-as-Code (IaC) abgebildet und in geteilten Code-Repositories gepflegt. Dieser Lösungsansatz wird der immer größeren Heterogenität und stetigen Modernisierung von Applikationslandschaften optimal gerecht.

Kunden erhalten über Avvia einen zentralen Standard für die Verlagerung von Anwendungen in die Cloud, der einerseits schnell und einfach aufgesetzt ist und grundlegenden Unternehmens-anforderungen und Richtlinien gerecht wird sowie andererseits genügend Spielraum für Konfigurationen aufgrund der natürlichen Heterogenität der vorliegenden Landschaft lässt.

Individuelle Zusammenarbeitsmodelle zwischen Kunde und Arvato Systems unterstützen Anwender der Avvia-Produktfamilie bei ihrer täglichen Arbeit. Der Kunde kann dabei zwischen den Verarbeitungsmodellen „self-managed“ (unverwaltet durch Arvato Systems), „co-managed“ (Kunde und Arvato Systems verwalten partnerschaftlich gemeinsam) oder „full-managed“ (vollständige Verwaltung durch Arvato Systems) wählen.

Die Bereitstellung im Co-Managed Service erfolgt zunächst durch Arvato Systems in Form von Infrastructure-as-Code (IaC). Änderungen können vom Kunden direkt im IaC vorgenommen werden. Vor der Bereitstellung führt Arvato Systems eine Qualitätsprüfung durch.

Die Bereitstellung und der Betrieb im Full-Managed Service erfolgt hingegen ausschließlich durch Arvato Systems in Form von Infrastructure-as-Code (IaC). Änderungen können über Change Request beantragt werden.

Bei der Service-Erbringung von Avvia nutzt Arvato Systems Public Hyperscaler wie z.B. Amazon Web Services, Microsoft Azure oder Google Cloud Platform sowie die von Arvato Systems entwickelte und betriebene Virtual Private Cloud, um die jeweiligen Cloud-Infrastrukturen für Kunden aufzubauen. Die Hyperscaler sind dabei in der Verantwortung, die dafür benötigten Infrastrukturkomponenten zu betreiben, zu verwalten und fortlaufend zu kontrollieren. Im Rahmen des Lieferantenmanagements von Arvato Systems werden aus Sicherheits-, Verfügbarkeits- und Vertraulichkeitsgründen entsprechende Zertifizierungen und Prüfungsbericht der Hyperscaler jährlich eingesehen (z.B. BSI C5 Berichte oder ISO 27001 Zertifikate) und Maßnahmen abgeleitet im Fall von identifizierten Feststellungen.

Auf Basis des Cloud-Service Avvia und den Kriterien des BSI C5:2020 liegen folgende Kriterienbereiche in der Verantwortung des jeweiligen Hyperscalers und somit nicht in der Verantwortung von Arvato Systems:

- Physische Sicherheit (PS)
- Kommunikationssicherheit (COS)
- Portabilität und Interoperabilität (PI)
- Beschaffung, Entwicklung und Änderung von Informationssystemen (DEV)
- Produktsicherheit (PSS)

5. INFORMATIONSSICHERHEITSMANAGEMENT

Managementsystem

Das Informationssicherheitsmanagementsystem von Arvato Systems erfüllt die Anforderungen der ISO/IEC 27001. Die im Bertelsmann-ISMS etablierten allgemeinen Prozesse sind

– Verwaltung von Informationsbeständen und Analyse der Auswirkungen auf das Geschäft
– Risikofolgenanalyse und Risikomanagement
– Managementprüfung und Berichterstattung
– Schulung zum Sicherheitsbewusstsein
– Management von Sicherheitsvorfällen
– Interne Audits und Überprüfungen der Einhaltung von Vorschriften

Die ISMS-Policy definiert den grundlegenden Rahmen für die Einrichtung, Überwachung, Aufrechterhaltung und kontinuierliche Verbesserung eines Informationssicherheits-managementsystems. Sie umfasst die erforderliche Organisation und alle notwendigen Kontrollen, Prozesse und Verfahren zur Verwaltung und Verbesserung der Informationssicherheit, um den damit verbundenen Risiken zu begegnen. Die Ergebnisse sind der zuständigen Geschäftsführungsebene zur Überprüfung durch die Sicherheitsorganisation zu melden.

Das Ergebnis dieser Prozesse sind Anweisungen für den Umgang mit Informationen und Einrichtungen, die im Rahmen des Bertelsmann-Regelwerks und zusätzlicher Richtlinien für Arvato Systems festgelegt werden.

ISMS-Organisation

Um die Überwachung und Verbesserung der Informationssicherheit zu unterstützen, ist ein kontinuierlicher und überprüfbarer Managementprozess eingeführt. Ein zentrales Element des ISMS-Prozesses ist das vierteljährlich durchgeführte Management-Review, bei dem der Informationssicherheitsmanager der Geschäftsleitung Bericht erstattet, einschließlich der Präsentation und Diskussion von

– Stand der Umsetzung des ISMS
– Status und Entscheidungen über die Behandlung der aktuellen Risiken
– relevante Sicherheitsvorfälle
– relevante Änderungen in der Business Impact Analyse
– weitere Inhalte

ISMS-Rollen

Der ISMS-Prozess wird durch Sicherheitsrollen unterstützt, wie in nachfolgender Tabelle beschrieben.

Rolle	Verantwortlichkeiten
Chief Executive Officer Arvato Systems	Der Chief Executive Officer (CEO) ist für das Unternehmen Arvato Systems verantwortlich. Der CEO muss die Unternehmens-sicherheitspolitik genehmigen und ist die letzte Stufe im Eskalationsmodell von Arvato Systems. Zu seiner Verantwortung gehört auch, dass die Aktivitäten von Arvato Systems mit den gesetzlichen Datenschutzbestimmungen übereinstimmen.
Chief Information Officer Arvato Systems	Der Chief Information Officer (CIO) ist verantwortlich für das Management der IT innerhalb von Arvato Systems.
Datenschutzbeauftragter	Der Datenschutzbeauftragte hat die Hauptaufgabe, die Einhaltung der gesetzlichen Datenschutzbestimmungen durch die Orga-nisation zu gewährleisten. Dies kann z.B. in Form von speziellen Schulungen geschehen.
Personalleiter	Der Personalleiter (HR Manager) ist zuständig, dass alle Mitarbeiter, Angestellten und Auftragnehmer die Sicherheits-vorgaben und Nutzungsbedingungen einhalten.
Chief Compliance Officer Arvato Systems	Der Chief Compliance Officer ist verantwortlich für das Manage-ment von Compliance-Problemen innerhalb von Arvato Systems, um die Einhaltung gesetzlicher Vorschriften und interner Richtlinien und Verfahren zu gewährleisten.
Business Continuity Manager	Der Business Continuity Manager (BC Manager) entwickelt und managed eine wirksame, systemübergreifende Geschäfts-kontinuitätsplanung und verwaltet alle Geschäftskontinuitäts-aktivitäten.
Manager On Call	Der Manager on Call (MOC) ist die erste Eskalationsstufe im Fall eines kritischen Ausfalls oder Sicherheitsvorfalls. Der MOC ist rund um die Uhr einsatzbereit.
Information Security Manager	Der Informationssicherheitsbeauftragte (ISM) ist zuständig für alle Aspekte der Informationssicherheit der Arvato Systems-Organisationen.
Security Incident Manager	Der Security Incident Manager ist verantwortlich für den Security Incident Management Process und dessen kontinuierliche Verbesserung.
Risk Manager	Der Risikomanager ist verantwortlich für das Risikomanagement-system (RMS) und das interne Kontrollsystem (IKS), einschließlich des zugehörigen Risikoberichterstattungsverfahrens und der Dokumentation der internen Kontrollen.

Sicherheitsrichtlinien

Wie in der internen Acceptable Use Policy beschrieben, ist das allgemeine Ziel der Schutz von eigenem und kundeneigenem geistigem Eigentum, Geschäftsgeheimnissen und anderen Informationen. Die ISMS-Policy definiert den grundlegenden Rahmen für die Einrichtung, Überwachung, Aufrechterhaltung und kontinuierliche Verbesserung eines Informationssicherheitsmanagementsystems, während die detaillierten Anforderungen Inhalt der nachfolgenden Konzernvorschriften sind:

- ISREG01: Security Organization
- ISREG02: Risk Management
- ISREG03: Information Security Assurance
- ISREG04: Human Resource Security
- ISREG05: Physical Security
- ISREG06: Supplier Relationship Management
- ISREG07: Legal and Compliance
- ISREG08: Security in IT Operations
  - ISREG08.01: Identity and Access Management
  - ISREG08.02: Network
  - ISREG08.03: Systems and Services
  - ISREG08.04: Secure Development
  - ISREG08.05: Application Security
  - ISREG08.06: Security Operations
- ISREG09: Cyber Crisis Management

Weitere Regeln und Verfahren entsprechend den Geschäftsprozessen und Schutzanforderungen von Arvato Systems sind im Intranet verfügbar. Regelmäßige Überprüfungen der Dokumente durch die Prozessverantwortlichen sind obligatorisch.

Dokumente der operativen Einheiten, die in den Geltungsbereich des ISMS fallen, befinden sich im Dokumentenmanagementsystem „Papyrus“ des Unternehmens. Relevante Werte für die Metadaten jedes Dokuments, einschließlich Eigentümer, Klassifizierung, Typ, Beschreibung und Standort, sind ebenso erfasst wie ein Wiedervorlagedatum. Die Verwaltung von Dokumenten wurde unter umfassender Einbeziehung der Mitarbeiter erarbeitet und ein Leitfaden beschreibt die Prozesse für die Änderungskontrolle sowie Versionskontrolle von Dokumenten. Folgende Abbildung zeigt die Struktur der ISMS-Dokumentenhierarchie.

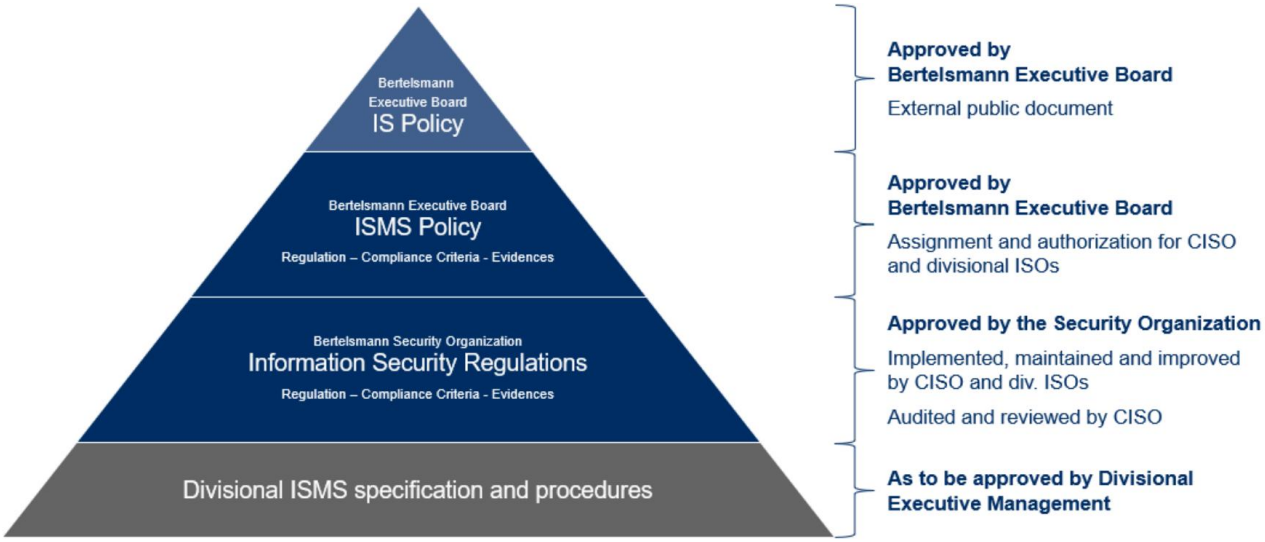

Abb. 1: ISMS-Dokumentenhierarchie

6. INFORMATIONSSICHERHEITSMAßNAHMEN

Risikomanagement der Informationssicherheit

Das Risikomanagement wird zentral für die gesamte Arvato Systems Gruppe geführt. Für jede Business Unit gibt es einen Informationssicherheitsverantwortlichen (ISO). Es gibt regelmäßige Abstimmungsroutinen über alle Unternehmensebenen hinweg, bei denen über relevante Informationssicherheitsthemen und damit verbundene Risiken gesprochen wird. Assets werden regelmäßig hinsichtlich ihrer Kritikalität bewertet. Dazu finden interne Assessments gegen die Konzernregularien und die Anforderungen der ISO 27001 statt. Dazu gibt es externe Audits ISO 27001, ISO 22301, ISO 22237 und ISO 9001.

Risiken werden auf der Grundlage von Szenarien erfasst und gemäß den Vorschriften kategorisiert. Anhand der Eintrittswahrscheinlichkeit eines Risikoszenarios und der potenziellen Auswirkungen wird es Risikoklassen zugeordnet. Das Risikoregister enthält Einträge für alle Risiken. Die kritischsten Risiken werden auch im Rahmen des vierteljährlichen Management-Reviews behandelt.

Management von Sicherheitsvorfällen

Ein Sicherheitsvorfall ist jedes Ereignis, das zum Verlust, zur Beschädigung, Veränderung oder Manipulation von Geschäftsfunktionen führen kann. Bei Arvato Systems basiert der Prozess auf der Norm ISO/EN 27035. Generell liegt es in der Verantwortung jedes internen oder externen Mitarbeiters, alle konkreten oder vermuteten Sicherheitsvorfälle, wie z.B. Bedienungsfehler, verdächtige Softwarefehler, Gefährdungen für Personen, Systeme oder Dienste, unverzüglich zu melden.

Die folgenden Ereignisse sind Beispiele, die sich in der Acceptable Use Policy speziell an Mitarbeiter richten:

– Schädliche oder bösartige Software, z. B. erkennbar an einer unerklärlichen Leistungsverschlechterung
– Verlust von kritischen, sensiblen Daten oder Informationen
– Unbefugte Änderung von kritischen, sensiblen Daten oder Informationen
– Verstoß gegen den Schutz der Privatsphäre
– Anhäufung von unerwünschten E-Mails (Spam-Mails)
– Telefonische oder elektronische Umfragen zur Sammlung von Informationen
– Verlust von ID-Ausweisen oder anderen Zugangskontrollgeräten
– Verlust/Diebstahl von Firmeneigentum (Laptop, Smartphone, Handy usw.)
– Passwort-Verletzungen
– Vorfälle, die eine Benachrichtigung der Polizei, der Feuerwehr oder des Krankenhauses erfordern
– Diebstahl, Veruntreuung von Geldern, Eigentum, Verkauf von illegalen Inhalten oder persönliche Angriffe

Der allgemeine Ansprechpartner für alle Sicherheitsvorfälle ist der zentrale Service Desk. Ausnahmen sind Vorfälle mit sehr sensiblem Inhalt, die einem Direktor oder der Personalabteilung gemeldet werden, oder Vorfälle, die sich auf einen Notfall beziehen (z.B. Feuer, Polizei), die an eine spezielle interne Helpline gerichtet werden. Für bekannte Szenarien gibt es Reaktionspläne, die regelmäßig überprüft werden.

Sicherheitsvorfälle und -ereignisse werden nach ihren Auswirkungen und dem potenziellen Risiko, das sie verursachen können, klassifiziert. Die Einstufung eines Sicherheitsvorfalls ist mit verschiedenen Eskalationsverfahren verbunden, zu denen die Einrichtung von Incident Response Teams und die Unterrichtung oder Einbeziehung der zuständigen Leitung gehören.

Der Prozess umfasst auch regelmäßige Überprüfungen und Trendanalysen, die in der "Sicherheitsvorfallbesprechung" des Security Incident Manager und des Information Security Manager ausgewertet werden. Relevante Ergebnisse dieser Überprüfung können an das Risikomanagement gerichtet und im Rahmen des ISMS-Management-Reviews oder an das zuständige operative Team gemeldet werden, um den entsprechenden Plan zur Reaktion auf Vorfälle zu verbessern.

Verfahren zur Ermittlung neuer Schwachstellen

Das Verfahren zur Ermittlung neu entdeckter Sicherheitslücken basiert auf zuverlässigen externen Quellen. Listen mit gemeldeten Schwachstellen - insbesondere vom Bundesamt für Sicherheit in der Informationsverarbeitung (BSI) oder von relevanten Herstellern - werden regelmäßig auf Aktualität geprüft. Die Informationen des BSI werden nach Auswirkungen und Relevanz für die von Arvato Systems erbrachten Dienstleistungen bewertet. Wird ein betroffenes System erwähnt, so wird über ein Service-Request-Ticket eine Anfrage zur detaillierten Recherche an das zuständige Operationsteam gerichtet.

Ergibt die Bewertung durch das BSI oder andere vertrauenswürdige Quellen, dass eine Schwachstelle besonders kritisch ist und dringende Maßnahmen erfordert, wird ein Ad-hoc-Gremium eingesetzt. Teilnehmer des Gremiums sind Experten für das betroffene Produkt, Servicemanagement, Produktionsmanagement, Informationssicherheit und Management. In diesem Gremium wird entschieden, ob Abhilfemaßnahmen im jeweiligen Szenario angewendet werden müssen.

Schwachstellenmanagement

Der Schwachstellenmanagementprozess ermöglicht es Arvato Systems, Schwachstellen in einem standardisierten Verfahren durch Analyse, Dokumentation und Reporting zu behandeln. Die Einrichtung des Prozesses liefert eine Baseline und verbessert das Bewusstsein für IT-Sicherheit, um die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen zu schützen.

Zusätzlich zu einer regelmäßigen Suche nach Schwachstellen und den entsprechenden Berichten werden neue Scan-Attribute auf der Grundlage externer Informationen eingerichtet, z. B. Informationen von Softwareanbietern oder Plattformen, die aktuelle Informationen zu den aktuell identifizierten Schwachstellen liefern.

Die Ergebnisse des Scanprozesses werden den verantwortlichen Eigentümern des Assets zur Bewertung und den daraus resultierenden Aktivitäten, wie z.B. Änderungen an der Konfiguration eines Assets oder Implementierung von Patches, zugewiesen.

Interne Audits und Compliance

Wie Prüfungen im Allgemeinen geplant, durchgeführt, berichtet und nachverfolgt werden, wird in einer Audit-Policy beschrieben. Sie legt die Zuständigkeit für die Organisation einer Prüfung fest und erläutert, wie Prüfungen vorbereitet und durchgeführt werden.

Bei internen Audits liefert ein Rahmenwerk Vorlagen für die Organisation, Dokumentation und die daraus resultierenden Auditberichte. Außerdem wird beschrieben, wie Maßnahmen im Zusammenhang mit Feststellungen gehandhabt werden sollen.

Die Ergebnisse interner und externer Audits können ebenfalls in die ISMS-Managementbewertung einfließen.

Zusätzlich zu den Audits wird ein fortlaufendes Programm zur technischen Überprüfung der sicherheitskritischen technischen Komponenten sowie der Pläne zur Aufrechterhaltung des Geschäftsbetriebs durchgeführt.

Zu diesem Zweck hat Arvato Systems die notwendigen technischen und organisatorischen Voraussetzungen geschaffen, um die jeweiligen Schutzanforderungen in Abstimmung mit seinen Kunden zu erfüllen. Dies bezieht sich auf: Zutrittskontrollen, Benutzerkontrollen, Zugriffskontrollen, Übertragungskontrollen, Eingabekontrollen, Auftragskontrollen, Verfügbarkeitskontrollen und vorgeschriebene Datentrennung.

7. PERSONALSICHERHEIT

Einstellungen und Austritte

Arvato Systems hat formale Einstellungspraktiken entwickelt, um zu überprüfen, ob neue Mitarbeiter für die Ausübung ihrer Aufgaben qualifiziert sind. Neueinstellungen müssen gemeinsam von der Personalabteilung und dem Abteilungsleiter genehmigt werden. Die Einstellungsrichtlinien verlangen von den Bewerbern ein Mindestmaß an Ausbildung und Erfahrung, schriftliche Referenzen und die Unterzeichnung von Vertraulichkeitsvereinbarungen durch die Mitarbeiter.

Die Arbeitsverträge beinhalten die IT-Sicherheitspolicy und eine Zustimmung zur Breitbandverpflichtung (einschließlich Datenschutz, Fernmeldegeheimnis, Sozialgeheimnis, Postgeheimnis usw.). Bei Verstößen gibt es individuelle disziplinarische Maßnahmen. Verträge werden in einem digitalen Vertragsregister (digitale Personalakte) gespeichert und enthalten alle notwendigen unterschriebenen Sicherheitsanforderungen.

In besonderen Fällen, wenn die Arbeit eines Mitarbeiters mit sehr sensiblen Daten oder Kommunikation zu tun hat oder dies von einem Kunden verlangt wird, können zusätzliche Nachweise (z. B. weitere Sicherheitsüberprüfungen) verlangt und Hintergrundprüfungen durchgeführt werden.

Tritt ein neuer Mitarbeiter in das Unternehmen ein, werden die mit seiner Position verbundenen Rollen und Zuständigkeiten für administrative Aufgaben durch den internen Starter-Changer-Leaver-Prozess von Arvato Systems dokumentiert. Eine Änderung, die die Rolle eines Mitarbeiters innerhalb des Unternehmens oder sein Ausscheiden aus dem Unternehmen betrifft, ist mit Genehmigungsmaßnahmen dieses Prozesses verbunden, bevor sie bei den Administratoren der jeweiligen Systeme beantragt und umgesetzt wird.

Sicherheitsbewusstsein

Ein Sicherheitsmanagementsystem kann nur dann wirksam sein, wenn alle Mitarbeiter es unterstützen und sich mit dem Thema identifizieren. Anweisungen oder sogar Einschränkungen müssen jeder Person erklärt werden, um ein angemessenes Sicherheitsbewusstsein zu gewährleisten.

Das Thema Informationssicherheit wird in Abteilungsbesprechungen mit dem Information Security Manager besprochen (z.B. technische IT-Sicherheitsfragen oder organisatorische Sicherheitsaspekte). In regelmäßigen Abständen werden Newsletter und Memoranden per E-Mail verschickt, in denen wichtige Ereignisse und Änderungen oder Erinnerungen in Bezug auf die Informationssicherheit zusammengefasst werden (z.B. neue Sicherheitsrichtlinien oder Erinnerung an die Einhaltung der Zugangsrichtlinien). Neue Mitarbeiter werden bei ihrem Eintritt bei Arvato Systems über die Richtlinien und Methoden der Informationssicherheit informiert.

Die Informationssicherheitsbeauftragten halten außerdem regelmäßig Mitarbeiterversammlungen und bei Bedarf Einzelgespräche ab. Alle Mitarbeiter von Arvato Systems nehmen darüber hinaus jährlich an einer virtuellen Schulung zum Thema IT-Sicherheit teil.

Die Schulung vermittelt ein klares Verständnis der internen Acceptable Use Policy und den individuellen Verantwortlichkeiten der Arvato Systems Mitarbeiter im Hinblick auf die Informationssicherheit in ihren jeweiligen Rollen. Die Schulung wird auf einer E-Learning-Plattform durchgeführt und der Information Security Manager führt Teilnehmerquoten. Darüber hinaus sind mitarbeiterbezogenen Sicherheitsdokumente und Schulungsunterlagen im Intranet von Arvato Systems zu finden. Dies ist die zentrale Anlaufstelle für alle Mitarbeiter, um Anleitungen zu finden, wie man mit Informationssicherheit umgeht.

Des Weiteren müssen alle Mitarbeiter von Arvato Systems regelmäßig an Schulungen zum Bertelsmann-Verhaltenskodex und zur Arbeitssicherheit teilnehmen.

8. ASSET MANAGEMENT

Arvato Systems nutzt in Absprache mit dem Kunden Asset Management-Policies des Hyperscalers Amazon Web Services (AWS), welche die kundenspezifischen Anforderungen im Rahmen der Provisionierung der primären und unterstützenden Assets abdecken. Die Anforderungen an diese Policy umfassen Aspekte von der Herstellung/Beschaffung, Verwaltung und Stilllegung der Assets sowie die Klassifizierung der Anlagen auf der Grundlage ihrer Kritikalität für den abzubildenden Business Case.

Für die im Rahmen dieser Policy verwalteten Assets existieren definierte Prozesse für Asset-Einrichtung, -Inventarisierung und Dekommissionierung. Änderungen, die während der Nutzung an den Assets vorgenommen werden, stehen im Einklang mit den Management-Anforderungen.

Die Asset-Inventarisierung für Avvia findet sowohl auf nativer Ebene des Hyperscalers AWS als auch in der Arvato Systems-internen Configuration Management Database (CMDB) statt. Letztere dient dem Endkunden-Reporting (Customer Service Reporting; CSR) als Datenquelle, sodass auch Kunden mit entsprechenden Zugriffsrechten das Reporting ihrer Assets außerhalb des Hyperscaler vornehmen können. CMDB als auch CSR werden dabei in regelmäßigen Abständen mehrfach täglich mittels automatischer Prozesse mit den Inhalten aus der jeweiligen Hyperscaler-Plattform synchronisiert.

Alle über diese Prozesse bereitgestellten Asset-Informationen enthalten notwendige Informationen in derjenigen Granularität, die für die Nachverfolgung, die Berichterstattung und den Betrieb der jeweiligen Services erforderlich ist.

Dekommissionierung von Assets werden ebenfalls durch das Asset Management abgedeckt und gemäß der geltenden Aufbewahrungsrichtlinien protokolliert und bereitgestellt. Die zugehörigen vertraglichen Anforderungen können dabei den von Arvato Systems ausgefertigten Dokumenten der „Public Cloud – Allgemeiner Rahmen“ sowie der hyperscalerspezifischen „Anlage Datenschutz AV – Solution Provider Account Model“ entnommen werden.

9. SERVICE DESK

Der Servicedesk ist die zentrale Anlaufstelle für alle Anfragen und Probleme im Zusammenhang mit der Dienstleistungserbringung seitens Arvato Systems. Er bietet den First-Level-Support und ist 24 Stunden am Tag und 365 Tage im Jahr erreichbar. Um die Integrität geschäftskritischer Transaktionen zu schützen, wurden beim Service Desk klare Prozesse zur Überprüfung der Identität der anfragenden Personen eingeführt.

Diese Ausrichtung auf die Kundenbedürfnisse erfordert den Einsatz eines Incident-Management-Systems sowie eine umfassende Schulung des Service-Desk-Personals im Hinblick auf die zu erwartenden Probleme bei den angebotenen IT-Services. Die Einführung oder Änderung eines IT-Services beinhaltet daher immer ein Schulungsprogramm für das Service-Desk-Team. Im Rahmen dieser Schulung werden mögliche Geschäftsvorfälle mit wiederkehrendem Bearbeitungsablauf beschrieben, die direkt vom Service Desk durchgeführt werden können. Je nach Vertragsinhalt ist es sogar möglich, neue IT-Services zu aktivieren oder Deployments für Kundenapplikationen durchzuführen.

Insbesondere außerhalb der Bürozeiten, bei Vorfällen mit hoher und dringender Priorität, ist der Service Desk auch dafür verantwortlich, den Bereitschaftsdienst der Second-Level-Support-Gruppen zu benachrichtigen und den Manager On Call über kritische Vorfälle zu informieren.

10. KONFIGURATIONSMANAGEMENT

Alle Avvia-Assets werden automatisch durch Amazon Web Services (AWS) inventarisiert und verwaltet. Diese nahtlose Integration von Avvia-Ressourcen in AWS ermöglicht Anwendern jederzeit einen detaillierten Überblick über ihre gesamten AWS-Ressourcen, einschließlich virtueller Maschinen, Speicherkonten, Netzwerke und weiteren Ressourcen.

Mit Hilfe des von Arvato Systems entwickelten Service Cockpits erhalten alle Avvia-Kunden Kunden zusätzliche Möglichkeiten zum Reporting über ihre Assets. Das Service Cockpit ist ein Portal, welches aus dem Internet erreichbar ist. Für einen benutzerfreundlichen Zugriff kann die AD des Kunden als Identity-Provider an das Service-Cockpit zur Authentifizierung gekoppelt werden; die Einrichtung lokaler Benutzer ist ebenfalls möglich.

Der Benutzer erhält über das Service Cockpit die Möglichkeit, auf zusätzliche Leistungsangebote von Arvato Systems per Single Sign-On zuzugreifen. Das User- und Accessmanagement erfolgt über Key-User des Kunden; diese können dabei eigenverantwortlich User-Konten im Service-Cockpit anlegen und Zugriff auf Services gewähren Das Service Cockpit ist mandantenfähig und unterstützt mehrere Sprachen. Im Service Cockpit erhalten Anwender vertraulichen Informationen u.a. auch Zugriff auf das 360° Customer Service Reporting, die ARGOS-Monitoring-Plattform, sowie das Cloud Financial Management “Kira” der Arvato Systems.

ARGOS ist die Visualisierungsplattform der Monitoring- und Reportingdaten des Kunden. Neben einer Vielzahl von technischen Performance-Daten werden auch die Verfügbarkeit von Systemen, Komponenten und Anwendungen sowie aufgetretene Störungen angezeigt Die ARGOS-Korrelation dient als zusätzliches Werkzeug zur Asset-Verwaltung in AWS, um vorhandene Daten einzelner Komponenten miteinander in Beziehung zu setzen und weiterführende Analysen durchzuführen.

Das 360 Grad Reporting wird allen Kunden zur Verfügung gestellt und bietet dem Anwender einen gezielten Überblick zu den Themen Process Quality, Service Availability, Security, Service Portfolio und Service Assets sowie Patch- und Backup-Informationen. Userindividuelle Reports können über Lesezeichen abgespeichert werden. Lernvideos und FAQ ergänzen diesen Service.

Über das Cloud Financial Management-Tools „Kira“ stellt Arvato Systems seinen Kunden ein leistungsfähiges Tool zur Kostenoptimierung von Cloud-Ressourcen zur Verfügung.

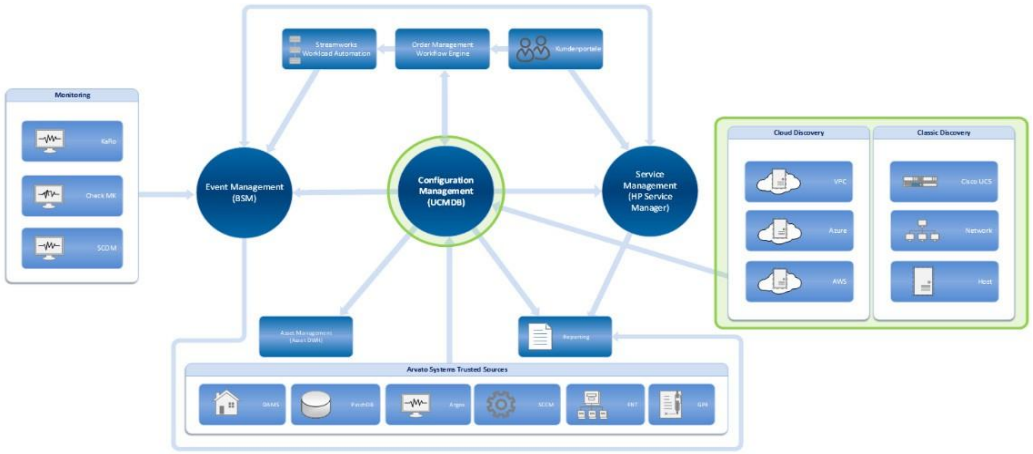

Abb. 2: Überblick Configuration Management Database

11. EREIGNISVERWALTUNG UND ÜBERWACHUNG

Avvia nutzt durch Amazon Web Services (AWS) bereitgestellte Monitoring-Möglichkeiten, um Komponenten wie etwa virtuelle Maschinen, Netzwerke, Datenbanken und andere Cloud-Services rund um die Uhr auf Ausfälle, Anomalien und Kapazitätsbedarfe zu überwachen. Alle in diesem Kontext generierten Events und Alerts werden zentral in AWS gespeichert und ausgewertet. Auf Wunsch des Kunden können zusätzliche Monitoring-Systeme eingebunden werden.

Events und Alerts können neben ihrer zentralen Speicherung in AWS zur automatischen Generierung von Tickets im ITSM-System von Arvato Systems genutzt werden; eine manuelle Erstellung von Tickets ist ebenfalls möglich.

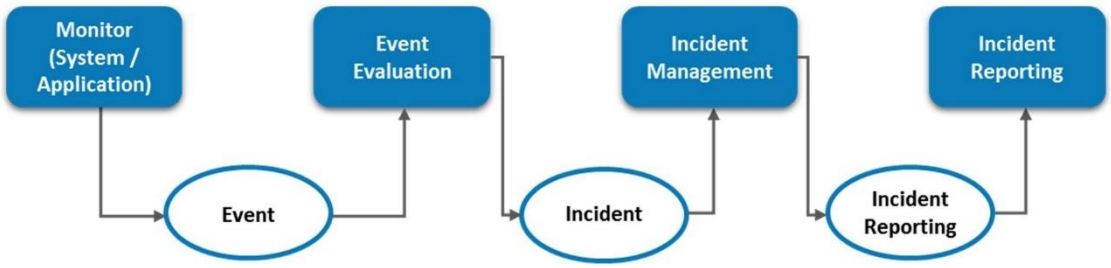

Abb. 3: Ereignisüberwachung

12. STÖRUNGSMANAGEMENT

Der Incident-Management-Prozess von Arvato Systems ist an ITIL angelehnt. Der Service Desk ist für das gesamte Management eines Incidents oder Service Requests verantwortlich. Die fachliche Eskalation an die zuständige Second-Level-Support-Gruppe sowie die organisatorische Eskalation zur Erfüllung der Service Level Agreements und die Koordination der Informationen liegen in der Verantwortung des Service Desks.

Für jedes eingehende Problem, das von Endanwendern an den Service Desk adressiert wird, wird ein Incident Ticket erstellt, das durch verschiedene Service Management Merkmale qualifiziert wird.

Je nach Auswirkung und Dringlichkeit wird die Priorität eines Vorfalls definiert. Diese Definition und die SLA der betroffenen Dienste werden automatisch zur Berechnung der Zeitfenster für den Eskalationsprozess verwendet. Informationen über Warnungen zur Eskalation werden durch automatische E-Mails an die zuständige Gruppe bekannt gegeben.

Der Inhalt eines Vorfalls wird systematisch durch Incident-Kategorien und im Detail im Arbeitsprotokoll beschrieben. Detaillierte Informationen zum betroffenen Service sind automatisch aus der Service-Datenbank verfügbar. Dies ermöglicht es dem Service Desk, sofort nach Eingang des Calls das für den Kunden relevante Service Level Agreement einzusehen und somit gezielt auf die Kundenanfrage zu reagieren.

Wenn ein Incident nicht direkt vom Service Desk gelöst werden kann, wird er an den Second Level Support weitergeleitet. Während der Lösung eines Vorfalls wird der Status durch ein Statusfeld und im Arbeitsprotokoll dokumentiert. Je nach Komplexität eines Incidents oder bei vermuteten Ausfällen von Hard- oder Software wird das Problem ggf. an den Hard- oder Softwarehersteller weitergeleitet. Darüber hinaus können weitere externe Dienstleister, wie z.B. spezialisierte Softwareentwicklungseinheiten innerhalb von Arvato Systems, hinzugezogen und entsprechende Maßnahmen eingeleitet werden.

Wenn ein Incident gelöst ist, wird der Status auf "Gelöst" gesetzt und der Kunde wird durch eine automatisch versandte E-Mail über die Lösung des Vorfalls informiert.

Für Vorfälle mit großen Auswirkungen hat Arvato Systems ein spezielles Verfahren definiert. Ein Major Incident Response Team unter der Leitung des Manager On Call (MOC) wird eingerichtet, um das Problem zu bearbeiten und die beteiligten Parteien über den Fortschritt der Lösung zu informieren.

Es werden monatliche Berichte über wichtige Leistungsindikatoren erstellt und ausgewertet, um den laufenden Prozess zu verbessern. Darüber hinaus werden auf der Grundlage der Berichte des "Incident Boards" Vorschläge für Problemtickets erstellt, wenn ein Configuration Item oder Service häufig mit Vorfällen in Verbindung gebracht wird.

13. DOKUMENTATIONEN

Alle Betriebseinheiten verwenden hauptsächlich ein zentrales System namens Papyrus, um Dokumente mit formalem Charakter, wie Prozessbeschreibungen oder Betriebshandbücher, zu verwalten. Papyrus ist ein Dokumentenmanagementsystem auf Basis von Microsoft SharePoint. Neben den Standardabfragefunktionen stehen vordefinierte Abfragen bezogen auf den Zuständigkeitsbereich eines Dokuments und spezielle Kategorien zur Verfügung.

Das Berechtigungskonzept entspricht der Organisationsstruktur und erlaubt es dem Eigentümer eines Dokuments, Dokumente für die eigene Gruppe, für andere Abteilungen (z.B. den Service Desk) oder ggf. für alle Benutzer im System zu veröffentlichen. Dokumente, die für alle Gruppen innerhalb des Betriebs verfügbar sind, sind zum Beispiel die Beschreibungen der Service-Support-Prozesse.

Das Wissensmanagement für das operative Tagesgeschäft erfolgt durch den Einsatz des Tools Confluence, das es den Nutzern ermöglicht, Wissensbasisartikel direkt auf Basis ihrer aktuellen Erfahrungen zu schreiben und zu modifizieren. Das Berechtigungskonzept basiert auf den gleichen Prinzipien wie bei Papyrus.

14. ZUGANGSKONTROLLEN UND BERECHTIGUNGSMANAGEMENT

Access Control Policy

Das Zugangskontrollmodell für Informationen und IT-Systeme wurde im Hinblick auf die Acceptable Use Policy von Arvato Systems entwickelt, die besagt, dass Informationen in einer ihrer Sensibilität, ihrem Wert und ihrer Kritikalität angemessenen Weise geschützt werden müssen und dass der Zugang zu ihnen auf einer Need-to-know-Basis eingeschränkt werden muss.

Arvato Systems steuert den Zugriff auf Informationen nach dem Konzept der "geringsten" Privilegien. Diese Strategie gewährt Zugriffsrechte durch definierte Autorisierungsregeln in Übereinstimmung mit minimalen Geschäftsanforderungen. Bei der Entwicklung der Zugriffskontrollrichtlinien für den Netzwerk- und logischen Zugriff hat Arvato Systems Folgendes berücksichtigt:

- Zugriffsanforderungen legitimer Nutzer auf der Basis ihrer Geschäftsfunktion/Rolle
- Bedarf dieser Nutzer, auf verschiedene Systeme und Geschäftsanwendungen zuzugreifen, zusätzlich zu dem Bedarf, auf die von diesen Systemen und Anwendungen verarbeiteten Daten zuzugreifen
- Die Tatsache, dass der Zugang zu Informationen und Informationsverarbeitungseinrichtungen aus der Ferne erfolgen kann
- Die Notwendigkeit einer regelmäßigen Überprüfung des Zugangsbedarfs der Nutzer
- Die Notwendigkeit, IT- und Nicht-IT-Systeme angemessen zu konfigurieren und dann zu überwachen, um bestehende oder versuchte Zugriffsverletzungen zu erkennen
- die Notwendigkeit, das Personal in den Grundsätzen der guten Sicherheitspraxis zu schulen, bevor es Zugang zu Systemen oder Informationen erhält

Um diese Ziele zu erreichen, wurden Verfahren für die Benutzerregistrierung und die Verwaltung von Privilegien eingeführt, Maßnahmen für den Fernzugriff auf das Netz (unter Verwendung einer starken Authentifizierung) ergriffen und eine Protokollierung und Analyse eingerichtet, um die Wirksamkeit dieser Maßnahmen zu verbessern.

Berechtigungsvergabeprozess und Benutzerverwaltung

Die Servicegruppen von Arvato Systems verfügen über eine definierte Liste von Systemrollen für ihre jeweiligen Servicefunktionen und eine Liste der jeweiligen Personen, die anderen Benutzern Rechte und Privilegien erteilen oder diese entziehen können. Zur Steuerung des Prozesses zur Vergabe bzw. zum Entzug von Zugriffsrechten für Mitarbeiter verwendet Arvato Systems einen Starter-Changer-Leaver-Prozess, der durch ein Workflow-Tool unterstützt wird. Einige Zugriffsrechte (Jedermannsrechte) werden automatisch vergeben, wenn der Personalstammdatensatz gültig gesetzt ist.

Der Starter-Prozess, der für die Einstellung neuer Mitarbeiter, neuer externer Mitarbeiter oder Praktikanten relevant ist, umfasst die folgenden administrativen Schritte:

- Registrierung der Mitarbeiterdaten in der Benutzerdatenbank (Initiierung durch die Personalabteilung (interne Mitarbeiter), Beschaffungsabteilung (externe Auftragnehmer)). Keine HR-Checkliste für externe Auftragnehmer.
- Administrative Schritte der Personalabteilung gemäß der Checkliste (interne Mitarbeiter)
- Qualitätskontrolle und Nachbearbeitung der Ergebnisse von Verwaltungsschritten der Personalabteilung (interne Mitarbeiter)
- Administrative Schritte der verantwortlichen Abteilungsleitung gemäß Checkliste (Beschaffung von Arbeitsmitteln, Ausweis, E-Mail-Konto, Berechtigungen)
- Überprüfung des aktuellen Status

Der Changer-Prozess ist für alle Änderungen relevant, die die organisatorischen Daten eines internen Mitarbeiters betreffen (z.B. Abteilungswechsel, Wechsel des Arbeitsortes, etc.):

- Administrative Schritte gemäß der dazugehörigen HR-Checkliste (Human Resources)

- Start von Teilprozessen zur Bestätigung der eingeleiteten Veränderung (z.B. Mitarbeiter, Betriebsrat, Vorgesetzte, etc.)
- Qualitätskontrolle und Nachbearbeitung der Ergebnisse der administrativen Schritte der Personalabteilung
- Administrative Schritte der verantwortlichen Abteilungsleitung gemäß Checkliste (z.B. Beschaffung von Arbeitsmitteln, Ausweis, E-Mail-Account, Berechtigungen)
- Überprüfung des aktuellen Status

Der Leaver-Prozess ist für jeden Mitarbeiter, der das Unternehmen verlässt, relevant:

- Administrative Schritte gemäß der Checkliste (Human Resources)
- Qualitätskontrolle und Nachbearbeitung der Ergebnisse von Verwaltungsschritten der Personalabteilung (interne Mitarbeiter)
- Administrative Schritte der verantwortlichen Abteilungsleitung gemäß Checkliste (Deaktivierung des Mitarbeiterausweises, des E-Mail-Kontos, Berechtigungen)
- Überprüfung des aktuellen Status

Identitätsmanagement

Arvato Systems verwendet ein Identity Access Management (IAM) System, um privilegierte Zugriffsrechte zu verwalten. Privilegierte Zugriffsrechte werden von Rolleninhabern (z.B. Abteilungsleiter/Stellvertreter) auf der Grundlage der Zuweisung einer Identität zu Business-Rollen gewährt. Im IAM-System wurden für den Zugriff auf Hyperscaler-Plattformen und deren Daten (inkl. Metadaten) dazugehörige Hyperscaler-Business-Rollen definiert, die restriktiv an Identitäten vergeben werden können. Das IAM-System dokumentiert bzw. protokolliert alle Änderungen an den Identitätsstammdaten (z.B. Startdatum, Rollenzuweisungen, Rollenwiderrufe, organisatorische Änderungen usw.).

<u>IAM-Prozessbeschreibung</u>

- Jeden Kalendertag werden die aktuellen Identitätsstammdaten aus den HR-Systemen geladen
- Die Personalstammdaten enthalten alle relevanten organisatorischen Informationen (z.B. Eintrittsdatum, Organisationseinheit, Austrittsdatum), um eine Identität innerhalb des IAM-Systems zu verwalten (z.B. Starter, Wechsler, Austretender)
- Im IAM-System weist der Abteilungsleiter (oder sein Stellvertreter) seinen Mitarbeitern alle Business-Rollen zu, die sie zur Erfüllung ihrer täglichen Arbeitsaufgaben benötigen oder nicht mehr benötigen (z. B. Starter, Wechsler).
- Jeder Inhaber einer IAM-Systemrolle (oder sein Stellvertreter) muss die Zuweisungen der Rollen genehmigen
- Basierend auf den geschäftlichen Rollenzuweisungen stellt und dokumentiert das IAM-System alle notwendigen Provisionierungs-/Deprovisionierungsschritte zur Verfügung, um die zugewiesenen privilegierten Zugriffsrechte in den Zielsystemen umzusetzen

– Sobald ein Mitarbeiter das Unternehmen verlässt, werden alle Rollenzuweisungen "spätestens" am Tag nach dem letzten Arbeitstag vom IAM-System widerrufen. Alle verwalteten Konten werden dann deaktiviert (d.h. Leaver).
– Im Falle eines Verstoßes oder eines potenziellen Verstoßes gegen die Sicherheit kann der Abteilungsleiter (oder sein Stellvertreter), der Rolleninhaber (oder sein Stellvertreter) oder der rund um die Uhr verfügbare Manager On Call (MOC) jederzeit alle Business-Rollen für jede Identität entfernen.
– Zweimal im Jahr initiiert der IAM-Systemeigentümer einen Review, um die korrekten Business-Rollen-Zuweisungen für alle Mitarbeiter zu dokumentieren. Jeder Rolleninhaber (Stellvertreter) muss die Rollenzuweisungen für jeden Mitarbeiter "akzeptieren oder widerrufen". Die Ergebnisse des Reviews werden im IAM-System protokolliert und anschließend umgesetzt.

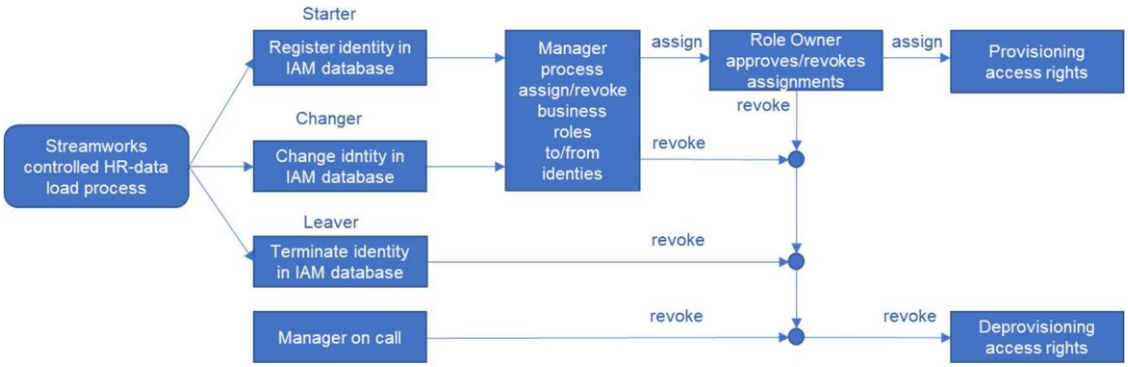

Abb. 4: IAM-Prozess

15. KRYPTOGRAFIE, SCHLÜSSELMANAGEMENT UND BACKUP

Datentransport

Für den verschlüsselten Transport von Daten (data in transit) nutzt Arvato Systems eine Verschlüsselung basierend auf TLS (Transport Layer Security) in der Version 1.3. Bei Anbindung älterer Kunden-Systemkomponenten, für die ein Einsatz dieser TLS-Version nicht möglich ist, kann auf Wunsch des Kunden alternativ TLS 1.2 verwendet werden.

AWS S3

Eine Speicherung von Daten innerhalb von Amazon Web Services (AWS) erfolgt grundsätzlich nur mittels verschlüsselter Form (data at rest).

– In der Standardeinstellung wird der jeweilige AWS Encryption Key durch AWS erstellt und verwaltet (Service Side Encryption; SSE). Die Ablage der zugehörigen Schlüssel-Dateien erfolgt dabei standardmäßig im AWS Key Management Service (KMS) und verwendet im Standard AES-256 zur Verschlüsselung. Die Rotation der Schlüssel kann dabei individuell festgelegt werden.
– Auf Kundenwunsch ist der Einsatz von Customer-Managed-Keys (SSE mit CMK) sowie eines dedizierten Hardware Security Modules (HSM) mittels AWS CloudHSM möglich.

Datenbanken

Amazon Relation Database Service (RDS) stellt folgende SQL-Datenbanken zu Verfügung: DB2, Oracle DB, Microsoft SQL Server, PostgreSQL. MySQL und MariaDB. Um die Sicherheit dieser Datenbanken zu erhöhen, können diese mit einer Verschlüsselung der Daten at Rest (im Ruhezustand) eingerichtet werden. Datenbanken werden somit mittels eines integrierten Serverzertifikats verschlüsselt. Neben der eigentlichen Datenbank sind so auch sämtliche Backups und Transaktionslogs geschützt. AWS setzt für die Verschlüsselung die FIPS 140-2 zertifizierte Methode AES-256-Bit ein. Die Datenbank ermöglicht Anwendern mit entsprechenden Lese- oder Schreibrechten einen Zugriff auf diese verschlüsselten Daten. Eine entsprechende Berechtigung von Anwendern mittels RBAC-Rollen (Role-based Access Control) wird hierfür zwischen Kunde und Arvato Systems festgelegt und konfiguriert.

Backups

Bei der Nutzung von nativen AWS-Backup-Optionen wie etwa AWS Backup oder AWS S3 werden Daten mittels AES-256 verschlüsselt übertragen und gespeichert. Die Passphrase zum Entschlüsseln dieser Daten liegt ausschließlich dem AWS-Kunden selbst vor. Bei Verlust des Schlüssels können die gesicherten Daten auch seitens AWS nicht wiederhergestellt werden.

Die Systemarchitektur ist auf Basis eines Best-Practice-Ansatzes (oder alternativ in Absprache nach Kundenanforderungen) hochverfügbar bzw. je nach Kritikalität des Systems redundant implementiert. Dies gilt auch für die regelmäßige Erstellung der Backups (beispielsweise Ablage in verschiedene Regionen).

16. LIEFERANTENMANAGEMENT

Das Lieferantenmanagement gestaltet, steuert und entwickelt die allgemeinen Kunden-Lieferanten-Beziehungen. Darüber hinaus sorgt es für den kontinuierlichen Informationsaustausch mit den Fachabteilungen der Arvato Systems Group. Arvato Systems betreibt Lieferantenmanagement für Lieferanten, welche unserem Geschäftszweck dienen.

Ziele des Lieferantenmanagements bei Arvato Systems sind:

– Reduzierung oder Minimierung der Beschaffungskosten
– Optimierung des Beschaffungsprozesses, um so zeiteffizient wie möglich zu arbeiten und eine Steigerung der Wettbewerbsfähigkeit zu erzielen
– Einhaltung von gesetzlichen Vorschriften und Unternehmensrichtlinien
– Optimierung der Zusammenarbeit mit Lieferanten (langfristig + stabil)
– Verbesserung der Liefertermintreue + Minimierung von Risiken (z. B. Ausfallrisiko, mangelhafte Leistungserfüllung)
– Sicherstellung einer zuverlässigen und qualitativ hochwertigen Lieferkette

Definition der Lieferantenklassifizierung:

Mithilfe der **ABC-Analyse** erfolgt die Klassifizierung der Lieferanten der Arvato Systems nach Einkaufsvolumen des Vorjahres:

- **A-Lieferant:** wichtigste und umsatzstärkste Gruppe. A-Lieferanten sind von großer Bedeutung, da sie die wichtigen umsatzstarken A-Güter liefern. Sie genießen in der Regel bevorzugte Behandlung. Die Kunden-Lieferanten-Beziehung ist sehr eng. A-Lieferanten > 3,0% gemessen am Einkaufsvolumen*

- **B-Lieferant:** diese Gruppe ist wichtig und bringt eine mittlere Umsatzstärke, die Kunden-Lieferanten-Beziehung ist nicht so intensiv wie die der Gruppe A.
  B-Lieferanten > 1,0% gemessen am Einkaufsvolumen

- **C-Lieferant:** weniger wichtig und geringeres Einkaufsvolumen
  C-Lieferanten > 0,0%

- **A*-Lieferant:** wichtige Lieferanten, welche anhand des Einkaufsvolumens nicht in A oder B klassifiziert werden. Diese werden individuell und in enger Abstimmung zwischen Einkauf und Fachbereich definiert, da sie von wichtiger, strategischer Bedeutung sind. Hier erfolgt eine Risikoeinschätzung (Versorgungsrisiko) über eine toolbasierte Abfrage.

- **IS-Kategorie-Lieferant:** Lieferant der eine Informationssicherheitskategorie von IS2 oder IS3 vorzuweisen hat.

Kontrollmaßnahmen für Lieferanten seitens des Lieferantenmanagements:

- Lieferantenaudit
    - Der Auditplan wird am Anfang des Geschäftsjahres aktualisiert und veröffentlicht
    - A-Lieferanten (gegebenenfalls für A*) werden regelmäßig alle drei Jahre vor Ort oder Remote auditiert
    - Die Teilnehmer des Audits werden durch das Lieferantenmanagement bestimmt
- Strategischer Lieferantendialog: Wird für A und B Lieferanten (gegebenenfalls für A*) durchgeführt. Über den Austausch der normalen Abnehmer – Lieferanten Kommunikation, werden beim Strategischen Lieferantendialog, zusammen mit dem Management, Entwicklungspotentiale der Partnerschaft besprochen (neue Services, Produkte, Prozesse, etc.) Der strategische Lieferantendialog wird nicht für Lieferanten durchgeführt, welche die Z-CIT betreut.
- Einladung Lieferantenplattform IntegrityNext: A, B, A* und IS-Kategorie Lieferanten werden auf die Plattform eingeladen. Lieferanten, welche die Plattformprozesse nicht durchlaufen, werden durch das Lieferantenmanagement, Risikomanagement und die Themenverantwortlichen kontaktiert.
- Internes Business Review Meeting: Wird für A, B und A* Lieferanten durchgeführt und findet zum Beginn eines Geschäftsjahres statt. In dem Meeting werden Verbesserungspotentiale besprochen und welcher Lieferant auditiert werden soll. Die Organisation wird durch den Projektleiter Lieferantenmanagement geregelt. Die Teilnehmer werden durch den Einkaufsleiter bestimmt
- Ansprechpartner/ Eskalationsmatrix: Für A, B und A* Lieferanten werden Ansprechpartner mit Hierarchieebene auf der Einkaufsplattform abgefragt und hinterlegt
- AEBs / Rahmenvereinbarungen: Es wird sichergestellt, dass für alle Lieferanten entweder auf Basis der AEB oder eines Rahmenvertrages bestellt wird

17. BUSINESS CONTINUITY MANAGEMENT

Das Business Continuity Management identifiziert die Gefährdung durch interne und externe Bedrohungen und kombiniert Hard- und Soft-Assets, um eine effektive Vorbeugung und Wiederherstellung für das Unternehmen zu gewährleisten und gleichzeitig den Wettbewerbsvorteil und die Integrität des Wertesystems zu erhalten.

Für Arvato Systems ist es das Ziel, den Servicebetrieb in allen Ausnahmesituationen wiederherzustellen. Zu diesem Zweck hat Arvato Systems ein Business Continuity Management System (BCMS) nach DIN EN ISO 22301 etabliert, das direkt mit den Geschäftsstrategien und -zielen von Arvato Systems verknüpft ist.

Im Rahmen des Business Continuity Management Systems werden alle zeitkritischen Geschäftsprozesse von Arvato Systems identifiziert und gegen ungeplante Unterbrechungen infolge eines Vorfalls mit hohem Schadenspotenzial abgesichert.

Das BCMS befasst sich mit vorhersehbaren Sicherheitsvorfällen, die ein Risiko für die Ressourcenverfügbarkeit in den folgenden Bereichen darstellen können:

– Personal
– Gebäude und Gebäudeinfrastruktur
– IT-Dienste
– Anbieter von Dienstleistungen

Die BCM-Policy dient als Grundlage für die Entwicklung, Einführung und den Betrieb des BCMS. Sie steht allen Mitarbeitern, Kunden und Geschäftspartnern sowie anderen interessierten Kreisen (z.B. Bertelsmann-Einheiten) zur Verfügung. Die BCM-Policy definiert den grundlegenden Rahmen für die Einrichtung, Überwachung, Aufrechterhaltung und kontinuierliche Verbesserung des Business Continuity Management Systems. Sie umfasst die erforderliche Organisation und notwendigen Kontrollen, Prozesse und Verfahren, um die Geschäftskontinuität des IT-Betriebs zu steuern und zu verbessern und damit verbundenen Risiken zu begegnen.

Im Rahmen des BCM-Konzepts setzt Arvato Systems Hochverfügbarkeitslösungen für alle Infrastrukturebenen seiner zentralen Geschäftsprozesse ein. Um dies zu erreichen, wird das Business Continuity Management (BCM) als aktiver Prozess definiert, der kontinuierlich überprüft, getestet und verbessert wird. Auf Basis dieses Konzepts bietet Arvato Systems auch verschiedene Szenarien zur Sicherstellung der Verfügbarkeit von Kundenanwendungen an und erbringt dafür Beratungs- und Implementierungsdienstleistungen für Kunden.

BCM-Organisation

Die Geschäftsleitung von Arvato Systems definiert die Bedeutung des Business Continuity Managements für das Unternehmen und gibt eine strategische Ausrichtung für die Umsetzung der Ablauf- und Aufbauorganisation vor. Der Vorstand stellt auch die erforderlichen finanziellen, technischen und personellen Ressourcen zur Verfügung. Im Ernstfall leitet ein Mitglied des Vorstands den Krisenstab, wie in folgender Abbildung dargestellt.

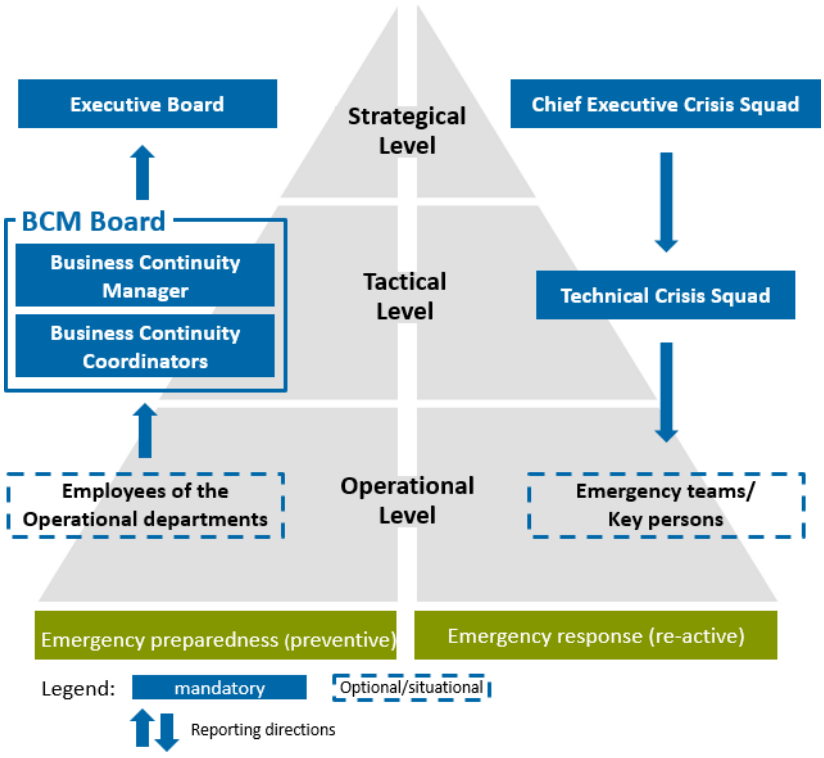

Abb. 5: BCM-Organisation und Meldewege

Hauptansprechpartner für alle relevanten Themen des BCMS ist der Business Continuity Manager. Der BC-Manager ist für die operative Umsetzung der strategischen Anforderungen des Business Continuity Management verantwortlich und berichtet an die Geschäftsführung. Der BC-Manager ist für die Koordination der BCM-Aktivitäten der operativen Abteilungen bei der Notfallvorsorge zuständig und unterstützt den technischen Krisenstab im Notfall.

Die Business-Continuity-Koordinatoren in den einzelnen operativen Abteilungen sind die Hauptansprechpartner des BC-Managers, um alle erforderlichen Aktivitäten für die Notfallvorsorge zu koordinieren, einschließlich der Unterstützung bei der Analyse der Auswirkungen auf den Betrieb, der Konzeption und Durchführung von Business-Continuity-Tests sowie der Dokumentation der BC-relevanten Kontrollen und Verfahren. Die Business-Continuity-Koordinatoren berichten im BCM-Board an den BC-Manager.

BCM-Prozess

Die verfolgte Strategie von Arvato Systems ist es, die Verfügbarkeit des IT-Betriebs für alle bewerteten Geschäftsbereiche sicherzustellen. Im Falle einer Unterbrechung werden die Auswirkungen des Vorfalls durch einen Standardansatz mit Disaster Recovery Management minimiert.

Um dies zu erreichen, wird das BCM als aktiver Prozess definiert, der kontinuierlich überprüft, getestet und verbessert wird. Im Rahmen des regelmäßigen Prozesses werden die unten aufgeführten BCM-Dokumente kontinuierlich und zentral überprüft, bewertet und verbessert:

– BCM-Policy
– Dokumente zur Vorbereitung auf Notfälle, einschließlich Risikomanagementplänen und Analysen der Auswirkungen auf das Geschäft
– Wiederherstellungs- und Wiederanlaufpläne des technischen Krisenstabs
– Wiederherstellungs- und Wiederanlaufpläne für die Abteilungen des Betriebsmanagements
– Managementbewertung und Berichterstattung für die Geschäftsleitung
– Schulungen zum Thema Geschäftskontinuität auf Managementebene und für die Mitarbeiter

Zur Unterstützung der Überwachung und Verbesserung der Geschäftskontinuität des IT-Betriebs wird ein kontinuierlicher und überprüfbarer Managementprozess eingerichtet. Ein zentrales Element des BCM-Prozesses ist die halbjährlich durchgeführte Managementbewertung, bei der der Business Continuity Manager der Geschäftsleitung Bericht erstattet, einschließlich der Präsentation und Diskussion von

– Status des Business Continuity Management Systems
– Entscheidungen über die Behandlung von Bedrohungen, die sich aus aktuellen und zukünftigen Geschäftsrisiken ergeben
– Entwicklung der Analyse der Auswirkungen auf das Geschäft sowie die Einbeziehung neuer Dienste
– Einschlägige größere Vorfälle und Notfälle

Alle Managementebenen von Arvato Systems sind für die Aufrechterhaltung eines funktionierenden BCM-Prozesses auf taktischer Ebene verantwortlich. Zusätzlich zu ihren normalen Geschäftsaufgaben sind sie auch verantwortlich für:

– Genehmigung der endgültigen Betriebskonzepte und Unterstützung bei der Umsetzung des BCM
– Entscheidung über notwendige Änderungen der Betriebskonzepte auf der Grundlage von Zielen und Strategien
– alle BCM-bezogenen Aufgaben, die sich aus dem operativen Geschäft ergeben
– die Durchführung erforderlicher Maßnahmen im Zusammenhang mit der disziplinarischen Verantwortung
– die Durchführung notwendiger Maßnahmen im Zusammenhang mit der technischen Verantwortung

Jeder Mitarbeiter ist dafür verantwortlich, in seinem Arbeitsbereich Maßnahmen zu unterstützen, die für das Business Continuity Management erforderlich sind, und alle notwendigen Maßnahmen zu ergreifen, um einen unterbrechungsfreien Betrieb zu gewährleisten. Diese Maßnahmen beziehen sich insbesondere auf die Erstellung, das Testen und die Durchführung von Disaster-Recovery-Plänen (sofern auf Basis des Servicemodells anwendbar).

Der BCM-Prozess umfasst mehrere Phasen, die von der Risikoermittlung über Aktivitäten bis zur kontinuierlichen Verbesserung reichen. Er kann daher als Qualitätszirkel betrachtet werden, der der kontinuierlichen Bewertung und Verbesserung des BCMS dient.

18. UMGANG MIT ERMITTLUNGSFRAGEN STAATLICHER STELLEN

Der Umgang mit qualifizierten staatlichen Ermittlungsanfragen wird in einem gesonderten Dokument der Arvato Systems mit dem Titel „Handbuch Behördliche Auskunftsersuchen und Durchsuchungen“ durch eindeutig definierte Prozesse und Handlungsanweisungen beschrieben und dokumentiert. Hierbei werden mögliche Szenarien staatlicher Ermittlungsanfragen wie beispielsweise

- Dawn Raid (Durchsuchung der Geschäftsräume und Rechenzentren) oder
- Umgang mit behördlichem Auskunftsersuchen

dokumentiert. Alle zugehörigen Personen, Verhaltensregeln und bereitzustellende Dokumente werden ebenfalls durch dieses Handbuch erfasst, sodass im Falle einer qualifizierten staatlichen Ermittlungsanfrage die für diese Ermittlung notwendigen Dokumente und Informationen den zuständigen Ermittlungsbehörden bereitgestellt werden können.

Das zugehörige Dokument „Handbuch Behördliche Auskunftsersuchen und Durchsuchungen“ unterliegt einem regelmäßigen Überprüfungszyklus von zwei Jahren und wird durch die Rechtsabteilung der Arvato Systems verantwortet.

Ermittlungsanfragen werden von der Rechtsabteilung geprüft und die betroffenen Kunden werden in Übereinstimmung mit den geltenden Gesetzen und Vorschriften sowie abhängig von der Ermittlungsabfrage der staatlichen Stellen informiert. Alle Ermittlungsanfragen werden durch die Rechtsabteilung auf Richtigkeit und Gültigkeit geprüft. Die Datenerhebung und -weitergabe beschränkt sich dabei auf das rechtlich Erforderliche. Sofern der Kunde eine eigene Schlüsselverwaltung zur Verschlüsselung seiner Daten realisiert hat (SSE mit CMK bzw. HSM), können Daten des Kunden ggf. durch Arvato Systems nicht entschlüsselt werden, da nur der Kunde in Besitz besagter Schlüssel ist.

ANLAGE 2

DARSTELLUNG DER DURCHGEFÜHRTEN PRÜFUNGSHANDLUNGEN, GEPRÜFTEN GRUNDSÄTZE, VERFAHREN UND MAßNAHMEN SOWIE DEREN ERGEBNISSE

ERSTELLT DURCH
HLB DR. STÜCKMANN UND PARTNER MBB

Gemäß der Beschreibung der gesetzlichen Vertreter waren folgende BSI C5 Kriterienbereiche nicht Teil unserer Prüfung, weil sie ausschließlich im Verantwortungsbereich von Amazon Web Services (AWS) liegen:

- Physische Sicherheit (PS)
- Kommunikationssicherheit (COS)
- Portabilität und Interoperabilität (PI)
- Beschaffung, Entwicklung und Änderung von Informationssystemen (DEV)
- Produktsicherheit (PSS)

1. ORGANISATION DER INFORMATIONSSICHERHEIT (OIS)

Referenz BSI C5	Kriterium des BSI C5:2020	Arvato Systems Kontrollbeschreibung	Prüfungshandlung	Ergebnis
OIS: Planung, Umsetzung, Aufrechterhaltung und kontinuierliche Verbesserung eines Rahmenwerks zur Informationssicherheit innerhalb der Organisation				
OIS-01	Der Cloud-Anbieter betreibt ein Informationssicherheitsmanagementsystem (ISMS) nach ISO/IEC 27001. Der Anwendungsbereich des ISMS umfasst die Organisationseinheiten, Standorte und Verfahren des Cloud-Anbieters zur Bereitstellung des Cloud-Dienstes. Die Maßnahmen für Aufbau, Verwirklichung, Aufrechterhaltung und fortlaufende Verbesserung des ISMS sind dokumentiert. Die Dokumentation umfasst: – Anwendungsbereich des ISMS (Abschnitt 4.3 von ISO/IEC 27001) – Erklärung zur Anwendbarkeit (Abschnitt 6.1.3) – Ergebnisse der letzten Managementbewertung (Abschnitt 9.3). <u>Zusatzkriterium</u> Das ISMS weist eine gültige Zertifizierung nach ISO/IEC 27001 oder ISO 27001 auf Basis von IT-Grundschutz auf.	Arvato Systems betreibt ein ISMS nach ISO/IEC 27001 und lässt sich in regelmäßigen Abständen dahingehend zertifizieren. Die Anwendungsbereiche des ISMS sind über ein „Statement of Applicability“ definiert. Die Ergebnisse von internen und externen Audits werden an das Management kommuniziert und bewertet.	Einsichtnahme in die Verfahrensanweisung zum ISMS und dessen Anwendungsbereich. Einsichtnahme in die Erklärung zur Anwendbarkeit (Statement of Applicability). Befragung des ISMS-Verantwortlichen hinsichtlich der Ergebnisse der letzten Managementbewertung sowie zur Steuerung und Überwachung der Informationssicherheit. Einsichtnahme in das ISO 27001 Zertifikat und dessen Gültigkeit.	Keine Abweichung festgestellt.

OIS-02	Die oberste Leitung des Cloud-Anbieters hat eine Leitlinie zur Informationssicherheit verabschiedet und an die internen und externen Mitarbeiter sowie die Cloud-Kunden kommuniziert. Die Leitlinie beschreibt – den Stellenwert der Informationssicherheit, abgeleitet von den Anforderungen der Cloud-Kunden mit Bezug zur Informationssicherheit, – die Sicherheitsziele und das angestrebte Sicherheitsniveau, abgeleitet von den Geschäftszielen und Aufgaben des Cloud-Anbieters, – die wichtigsten Aspekte der Sicherheitsstrategie zum Erreichen der gesetzten Sicherheitsziele – die Organisationsstruktur für Informationssicherheit im Anwendungsbereich des ISMS.	Es sind Konzernrichtlinien zur Informationssicherheit (ISREG) definiert und verabschiedet, die an alle Mitarbeiter kommuniziert sind. Die Konzernrichtlinien werden jährlich auf Aktualität hin überprüft und ggf. aktualisiert.	Einsichtnahme in die Konzernrichtlinien zur Informationssicherheit und Beurteilung, ob diese verabschiedet ist sowie relevante Inhalte (Stellenwert der Informationssicherheit, Sicherheitsziele, Sicherheitsstrategie, Organisationsstruktur) enthalten und aktuell sind. Einsichtnahme in das Intranet und festgestellt, dass die Konzernrichtlinien zur Informationssicherheit für alle Mitarbeiter verfügbar und einsehbar sind.	Keine Abweichung festgestellt.
OIS-03	Schnittstellen und Abhängigkeiten zwischen Tätigkeiten zur Bereitstellung des Cloud-Dienstes, die vom Cloud-Anbieter selbst durchgeführt werden und Tätigkeiten, die von Dritten durchgeführt werden, sind dokumentiert und kommuniziert. Dies umfasst den Umgang mit folgenden Ereignissen: – Schwachstellen – Sicherheitsvorfälle und – Störungen Art und Umfang der Dokumentation orientieren sich am Informationsbedarf sachverständigen Personals der betroffenen Organisationen, um die Tätigkeiten angemessen durchführen zu können. Die Kommunikation von Änderungen an den Schnittstellen und Abhängigkeiten erfolgt so zeitnah, dass die betroffenen Dritten mit organisatorischen und technischen Maßnahmen angemessen darauf reagieren können, bevor diese wirksam werden.	Nicht anwendbar – im Verantwortungsbereich von AWS.		

OIS-04	Miteinander in Konflikt stehende Aufgaben und Verantwortlichkeitsbereiche sind auf Basis einer Risikobeurteilung gemäß OIS-06 getrennt, um Risiken unbefugter oder unbeabsichtigter Änderungen oder Missbrauch der im Cloud-Dienst verarbeiteten, gespeicherten oder übertragenen Daten der Cloud-Kunden zu reduzieren. Die Risikobeurteilung umfasst folgende Bereiche, soweit diese zur Bereitstellung des Cloud-Dienstes anwendbar sind und im Verantwortungsbereich des Cloud-Anbieters liegen: – Verwaltung von Rechteprofilen, Genehmigung und Zuweisung von Zugangs- und Zugriffsberechtigungen (vgl. IDM-01), – Entwicklung, Test und Freigabe von Änderungen (vgl. DEV-01), – Betrieb der Systemkomponenten. Kann aus organisatorischen oder technischen Gründen keine Trennung eingerichtet werden, sind Maßnahmen zur Überwachung der Tätigkeiten eingerichtet, um unbefugte oder unbeabsichtigte Änderungen sowie Missbrauch aufzudecken und entsprechende Gegenmaßnahmen einzuleiten.	Die Einhaltung von Funktionstrennungen wird über ein Identity Access Management System sichergestellt, in dem auf Basis von Risikobeurteilungen entsprechende Business-Rollen je Zuständigkeitsbereich definiert sind. Diese Business-Rollen und die dazugehörigen Berechtigungen werden den Mitarbeitern im Rahmen des internen User Access Managements zugewiesen und entsprechen ihrem Verantwortlichkeitsbereich.	Einsichtnahme in das Identity Access Management System und Beurteilung, ob Business-Rollen zu Funktionstrennungszwecken definiert und implementiert sind.	Keine Abweichung festgestellt.
OIS-05	Der Cloud-Anbieter pflegt Kontakte zu relevanten Behörden und Ministerien, um sich über aktuelle Schwachstellen und Gefährdungen zu informieren. Die Informationen fließen in die Verfahren zum Umgang mit Risiken (vgl. OIS-06) und Schwachstellen (vgl. OPS-19) ein. <u>Zusatzkriterium</u> Soweit der Cloud-Dienst durch Organisationen des öffentlichen Sektors in Deutschland genutzt wird, pflegt der Cloud-Anbieter Kontakte zum Nationalen IT-Lagezentrum und dem CERT-Bund des BSI.	Verantwortliche Systemadministratoren sowie ein etabliertes Security Operations Center informieren sich fortlaufend bei Behörden, Ministerien oder auch Softwareanbietern (z.B. CERT-Bund oder BSI) zu Schwachstellen oder Sicherheitsrisiken. Die Informationen und sich daraus ergebene Maßnahmen fließen in die dafür vorgesehenen Prozesse ein (z.B. Patch Management).	Befragung des Security Managers hinsichtlich des Kontakts mit relevanten Behörden und Interessensverbänden (z.B. IT-Lagezentrum oder CERT-Bund des BSI) zu Schwachstellen. Einsichtnahme in Dokumentationen (z.B. Schwachstellenlisten) und Beurteilung, ob sich fortlaufend zu aktuellen Schwachstellen informiert wird und wie empfohlene Maßnahmen beim Umgang mit Risiken und Schwachstellen einfließen.	Keine Abweichung festgestellt.

OIS-06	Richtlinien und Anweisungen für das Verfahren zum Umgang mit Risiken sind gemäß SP-01 hinsichtlich der folgenden Aspekte dokumentiert, kommuniziert und bereitgestellt: – Identifikation von Risiken im Zusammenhang mit dem Verlust der Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität von Informationen innerhalb des Anwendungsbereichs des ISMS und Zuweisung von Risikoeigentümern, – Analyse der Eintrittswahrscheinlichkeiten und Auswirkungen bei Eintritt sowie Bestimmung des Risikoniveaus, – Bewertung der Risikoanalyse auf Basis definierter Kriterien zur Risikoakzeptanz und Priorisierung der Behandlung, – Behandlung der Risiken durch Maßnahmen, einschließlich Genehmigung der Maßnahmen und Akzeptanz der Restrisiken durch Risikoeigentümer, – Dokumentation der Tätigkeiten zur Anwendung des Verfahrens, um bei wiederholter Anwendung konsistente, gültige und vergleichbare Ergebnisse zu erhalten.	Ein IT-Risikomanagement-prozess ist definiert und implementiert, der das Vorgehen und die Dokumentation zur Risikoanalyse und Risikobewertung sowie die Ableitung von notwendigen Maßnahmen beschreibt.	Befragung des Risikomanagers hinsichtlich den Verfahrensanweisungen zum Risikomanagement betreffend die im Kriterium genannten Aspekte. Einsichtnahme in den definierten IT-Risikomanagementprozess und Beurteilung, ob die im Kriterium genannten Aspekte Teil des Verfahrens zum Umgang mit Risiken sind.	Keine Abweichung festgestellt.

OIS-07	Der Cloud-Anbieter wendet das Verfahren zum Umgang mit Risiken anlassbezogen, aber mindestens jährlich an. Beim Identifizieren von Risiken werden folgende Aspekte berücksichtigt, soweit diese für den bereitgestellten Cloud-Dienst anwendbar sind und im Verantwortungsbereich des Cloud-Anbieters liegen: – Verarbeitung, Speicherung oder Übertragung von Daten der Cloud-Kunden mit unterschiedlichen Schutzbedarfen, – Auftreten von Schwachstellen und Störungen in technischen Schutzmaßnahmen zur Separierung gemeinsam genutzter Ressourcen, – Angriffe über Zugangspunkte, einschließlich Schnittstellen, die aus öffentlichen Netzen erreichbar sind, – Miteinander in Konflikt stehende Aufgaben und Verantwortlichkeitsbereiche, die aus organisatorischen oder technischen Gründen nicht getrennt werden können, – Abhängigkeiten von Subdienstleistern. Die Analyse, Bewertung und Behandlung der Risiken, einschließlich der Genehmigung der Maßnahmen und Akzeptanz der Restrisiken, wird mindestens jährlich durch die Risikoeigentümer auf Angemessenheit überprüft.	Es wird jährlich ein Risiko-Assessment durchgeführt und dokumentiert, mittels dem Sicherheitsrisiken für Assets analysiert, bewertet und notwendige Risikobehandlungen abgeleitet werden. Die Ergebnisse des Risiko-Assessments und die dazugehörigen Risikomaßnahmen werden seitens der Asset-Owner umgesetzt bzw. Restrisiken akzeptiert.	Einsichtnahme in das Risikomanagement-Inventar sowie einem Risiko-Assessment hinsichtlich der Dokumentation von Risiken sowie deren Bewertung und Behandlung. Einsichtnahme in die entsprechende Dokumentation zum Nachweis der implementierten Maßnahmen bei identifizierten Veränderungen/Abweichungen und Risiken.	Keine Abweichung festgestellt.
Die Kontrollen sind zutreffend dargestellt sowie angemessen eingerichtet, um das oben genannte Kontrollziel zu erreichen.				

2. SICHERHEITSRICHTLINIEN UND ARBEITSANWEISUNGEN (SP)

Referenz BSI C5	Kriterium des BSI C5:2020	Arvato Systems Kontrollbeschreibung	Prüfungshandlung	Ergebnis
SP: Bereitstellen von Richtlinien und Anweisungen bzgl. des Sicherheitsanspruchs und zur Unterstützung der geschäftlichen Anforderungen.				
SP-01	Von der Leitlinie zur Informationssicherheit abgeleitete Richtlinien und Anweisungen sind nach einer einheitlichen Struktur dokumentiert. Sie werden sach- und bedarfsgerecht an alle internen und externen Mitarbeiter des Cloud-Anbieters kommuniziert und bereitgestellt. Die Richtlinien und Anweisungen sind versioniert und von der obersten Leitung des Cloud-Anbieters oder von dazu autorisiertem Personal genehmigt. Die Richtlinien und Anweisungen beschreiben mindestens die folgenden Aspekte: – Ziele, – Anwendungsbereiche, – Rollen und Verantwortlichkeiten, einschließlich Anforderungen an die Qualifikation des Personals und das Einrichten von Vertretungsregelungen, – Rollen und Abhängigkeiten von anderen Organisationen (insbesondere Cloud-Kunden und Subdienstleister), – Maßnahmen zur Umsetzung der Sicherheitsstrategie, – anwendbare rechtliche und regulatorischer Anforderungen.	Die Konzernrichtlinien zur Informationssicherheit (ISREG) teilen sich thematisch auf mehrere Sicherheitsrichtlinien auf. Auf Basis dieser Sicherheitsrichtlinien hat Arvato Systems weitere Richtlinien und Anweisungen definiert sowie dokumentiert. Die Richtlinien werden dabei fortlaufend versioniert und sind über das Intranet sowie über interne Sicherheitsschulungen an alle Mitarbeiter kommuniziert.	Einsichtnahme in die Richtlinienpyramide und Beurteilung, ob von den Konzernrichtlinien zur Informationssicherheit weitere Richtlinien und Anweisungen sach- und bedarfsgerecht abgeleitet und kommuniziert wurden. Einsichtnahme in abgeleitete Richtlinien (z.B. hinsichtlich des sicheren Umgangs mit Informationssystemen) und Beurteilung, ob diese versioniert und genehmigt sind.	Keine Abweichung festgestellt.

SP-02	Die Richtlinien und Anweisungen zur Informationssicherheit werden mindestens jährlich durch sachverständiges Personal des Cloud-Anbieters auf ihre Angemessenheit überprüft. Die Überprüfung berücksichtigt mindestens die folgenden Aspekte: – Organisatorische und technische Änderungen in den Verfahren zur Bereitstellung des Cloud-Dienstes, – rechtliche und regulatorische Änderungen im Umfeld des Cloud-Anbieters. Überarbeitete Richtlinien und Anweisungen werden genehmigt, bevor diese Gültigkeit erlangen.	Die Konzernsicherheits-richtlinien sowie die Arvato Systems Sicherheitsrichtlinien und Anweisungen werden jährlich auf Aktualität und notwendigen Änderungen (z.B. aufgrund von regulatorischen Änderungen) hin überprüft und überarbeitet. Der zuständige Information Security Officer prüft neue Versionen der Richtlinien und gibt diese vor Veröffentlichungen frei.	Befragung des ISO hinsichtlich der Verfahrensanweisung zur Überprüfung und Freigabe von Richtlinien und Anweisungen. Einsichtnahme in Richtlinien und Beurteilung, ob eine mindestens jährliche Überprüfung und ggf. Versionierung durchgeführt wird.	Keine Abweichung festgestellt.
SP-03	Ausnahmen von Richtlinien und Anweisungen zur Informationssicherheit durchlaufen das Verfahren zum Umgang mit Risiken gemäß OIS-06, einschließlich Genehmigung der Ausnahmen und Akzeptanz der damit einhergehenden Risiken durch die Risikoeigentümer. Die Genehmigung von Ausnahmen ist dokumentiert, zeitlich befristet und wird mindestens jährlich durch die Risikoeigentümer auf Angemessenheit überprüft.	Jede Ausnahme einer Richtlinie ("operational exception") muss über einen dafür vorgesehenen Prozess gemeldet und dokumentiert werden. Das interne Compliance Team sowie der Risiko-Owner müssen vor Umsetzung der Ausnahme diese genehmigen. Die Ausnahme ist zeitlich befristet und wird im Rahmen des Risiko-Assessments mindestens jährlich neu bewertet.	Befragung des Risikomanagers hinsichtlich der Vorgehensweise bei der Umsetzung und Dokumentation von Ausnahmen. Einsichtnahme in die Dokumentation einer Ausnahme und Beurteilung, ob diese wie vorgesehen bearbeitet und zeitlich befristet genehmigt wurde.	Keine Abweichung festgestellt.
Die Kontrollen sind zutreffend dargestellt sowie angemessen eingerichtet, um das oben genannte Kontrollziel zu erreichen.				

3. PERSONAL (HR)

Referenz BSI C5	Kriterium des BSI C5:2020	Arvato Systems Kontrollbeschreibung	Prüfungshandlung	Ergebnis
HR: Sicherstellen, dass Mitarbeiter ihre Aufgaben verstehen, sich ihrer Verantwortung in Bezug auf Informationssicherheit bewusst sind und die Assets der Organisation bei Änderung der Aufgaben oder Beendigung geschützt werden.				
HR-01	Die Qualifikation und Vertrauenswürdigkeit aller internen und externen Mitarbeiter des Cloud-Anbieters mit Zugriff auf Daten der Cloud-Kunden oder Systemkomponenten im Verantwortungsbereich des Cloud-Anbieters, die für die Bereitstellung des Cloud-Dienstes in der Produktionsumgebung zuständig sind, wird vor Beginn des Beschäftigungsverhältnisses gemäß der lokalen Gesetzgebung und Regulierung durch den Cloud-Anbieter überprüft. Soweit rechtlich zulässig, umfasst die Überprüfung folgende Bereiche: – Verifikation der Person durch Personalausweis – Verifikation des Lebenslaufs – Verifikation von akademischen Titeln und Abschlüssen – Führungszeugnis bzw. nationale Pendants – Bewerten des Risikos der Erpressbarkeit.	Neu eingestellte Mitarbeiter werden einer Zuverlässigkeitsüberprüfung unterzogen, die auch eine Überprüfung der Ausbildung und der Berufserfahrung sowie der persönlichen Referenzen umfasst. Sofern rechtlich geboten (z.B. aus dem relevanten Kundenvertrag oder aus anwendbaren Gesetzen) sind weitergehende Prozesse zur tiefergehenden Überprüfung (z.B. Führungszeugnisse) unter Beteiligung der betroffenen Abteilungen (z.B. HR-Abteilung, Betriebsrat) eingerichtet.	Einsichtnahme in die Verfahrensanweisung zur Überprüfung der Qualifikation und Vertrauenswürdigkeit von internen und externen Mitarbeitern sowie in eine durchgeführte Zuverlässigkeitsprüfung und Beurteilung, ob die für die Personenüberprüfung rechtlich zulässigen Schritte durchgeführt werden.	Keine Abweichung festgestellt.
HR-02	Die internen und externen Mitarbeiter des Cloud-Anbieters werden in Beschäftigungs- und Vertragsbedingungen auf die Einhaltung anwendbarer Richtlinien und Anweisungen mit Bezug zur Informationssicherheit verpflichtet. Die Leitlinie zur Informationssicherheit sowie die davon abgeleiteten Richtlinien und Anweisungen sind durch die internen und externen Mitarbeiter nachweislich zur Kenntnis zu nehmen, bevor Zugriff auf Daten der Cloud-Kunden oder Systemkomponenten im Verantwortungsbereich des Cloud-Anbieters, die für die Bereitstellung des Cloud-Dienstes in der Produktionsumgebung verwendet werden, gewährt wird.	Neue Mitarbeiter müssen bei Eintritt die Kenntnisnahme der IT-Sicherheitsrichtlinie sowie eine Vertraulichkeitserklärung unterzeichnen, die bestätigt, dass sie sich der Bedeutung von Kundendaten bewusst sind. Externe Mitarbeiter werden schriftlich im Rahmen des jeweiligen Lieferantenvertrags zur Vertraulichkeit verpflichtet.	Einsichtnahme in eine Beschäftigungsvereinbarung für Mitarbeiter und in einen Lieferantenvertrag hinsichtlich Einhaltung der Vorgaben zur Informationssicherheit und Vertraulichkeit für interne und externe Mitarbeiter.	Keine Abweichung festgestellt.

HR-03	Der Cloud-Anbieter betreibt ein zielgruppenorientiertes Sensibilisierungs- und Schulungsprogramm, das von allen internen und externen Mitarbeitern des Cloud-Anbieters regelmäßig durchlaufen wird. Das Programm wird, ausgehend von Änderungen an Richtlinien und Anweisungen sowie der aktuellen Bedrohungslage, regelmäßig aktualisiert und umfasst die folgenden Aspekte: – Umgang mit Systemkomponenten, die für die Bereitstellung des Cloud-Dienstes in der Produktionsumgebung verwendet werden, gemäß den anwendbaren Richtlinien und Anweisungen, – Umgang mit Daten der Cloud-Kunden gemäß den anwendbaren Richtlinien und Anweisungen, – Information über die aktuelle Bedrohungslage, – richtiges Verhalten bei Sicherheitsvorfällen. <u>Zusatzkriterium</u> Die durch das Sensibilisierungs- und Schulungsprogramm erzielten Lernerfolge werden zielgruppenbezogen gemessen und ausgewertet. Die Messungen umfassen quantitative und qualitative Aspekte. Die Ergebnisse fließen in die Verbesserung des Sensibilisierungs- und Schulungsangebots ein.	Mitarbeiter erhalten im Rahmen der Einarbeitung sowie jährlich eine Schulung zum Sicherheitsbewusstsein über eine bereitgestellte Schulungsplattform (Konzernschulung und Arvato Systems spezifische Informationssicherheitsschulung). Die Durchführung der Schulungen wird dabei seitens der Vorgesetzten überwacht. Darüber hinaus finden regelmäßige Cyber Security Schulungen seitens der Abteilung "Information Security" für die Arvato Systems Teams statt.	Einsichtnahme in Sicherheitsschulungen hinsichtlich der im Kriterium genannten Aspekte. Einsichtnahme in Cyber Security Schulungs-maßnahmen und Auswertungen der Lernerfolge von Mitarbeitern sowie daraus abgeleiteten Maßnahmen zur Verbesserung des Schulungsprogramms.	Keine Abweichung festgestellt.
HR-04	Bei Verstößen gegen Richtlinien und Anweisungen erfolgen Maßregelungen gemäß eines definierten Prozesses, der folgende Aspekte umfasst: – Prüfung, ob tatsächlich ein Verstoß vorliegt – Berücksichtigung der Art und Schwere des Verstoßes sowie dessen Auswirkung. Die internen und externen Mitarbeiter des Cloud-Anbieters sind über mögliche Maßregelungen informiert. Die Anwendung von Maßregelungen wird in geeigneter Weise dokumentiert.	Für Verstöße gegen die Informationssicherheit sind Disziplinarmaßnahmen und dazugehörige Verfahren definiert, die je nach Schwere des Verstoßes angewendet und dokumentiert werden. Die Mitarbeiter werden im Rahmen Ihrer Einstellung vertraglich auf mögliche Disziplinarmaßnahmen bei Verstößen hingewiesen.	Einsichtnahme in die Richtlinien und Anweisungen zu gemeldeten Verstößen und deren Sanktionierung. Einsichtnahme in die Kommunikation dieser Regelungen an Mitarbeiter und Dienstleister.	Keine Abweichung festgestellt.

HR-05	Interne sowie externe Mitarbeiter sind nachweislich darüber informiert, wie lange welche Verantwortlichkeiten, die sich aus den Richtlinien und Anweisungen mit Bezug zur Informationssicherheit ergeben, auch bei Beendigung oder Änderung der Beschäftigung bestehen bleiben.	Über die Verschwiegenheitserklärung als Teil des Arbeitsvertrages werden Mitarbeiter darüber informiert, dass sie auch nach Unternehmensaustritt zur Verschwiegenheit von Kundendaten und Informationen verpflichtet sind.	Einsichtnahme in eine Mitarbeiterverpflichtungs-erklärung und Beurteilung, ob bei Auflösung oder Änderung eines Beschäftigungsverhältnisses die Richtlinien und Anweisungen mit Bezug zur Informationssicherheit für einen definierten Zeitraum weiter einzuhalten sind.	Keine Abweichung festgestellt.
HR-06	Die mit internen Mitarbeitern, externen Dienstleistern sowie Lieferanten des Cloud-Anbieters zu schließenden Geheimhaltungs- oder Vertraulichkeits-vereinbarungen basieren auf den vom Cloud-Anbieter identifizierten Anforderungen zum Schutz vertraulicher Informationen und betrieblicher Details. Die Vereinbarungen sind mit externen Dienstleistern und Lieferanten bei Vertragsabschluss zu schließen. Mit internen Mitarbeitern des Cloud-Anbieters sind die Vereinbarungen zu schließen, bevor die Berechtigung zum Zugriff auf Daten der Cloud-Kunden erteilt wird. Die Anforderungen sind zu dokumentieren sowie in regelmäßigen Abständen (mindestens jährlich) zu überprüfen. Soweit sich aus der Überprüfung ergibt, dass die Anforderungen anzupassen sind, werden die Geheimhaltungs- oder Vertraulichkeitsvereinbarungen aktualisiert. Der Cloud-Anbieter hat die internen Mitarbeiter, externen Dienstleister und Lieferanten hierüber zu informieren und mit diesen die aktualisierten Geheimhaltungs- oder Vertraulichkeits-vereinbarungen zu schließen.	Neue Mitarbeiter müssen eine Verschwiegenheitserklärung (als Teil des Arbeitsvertrages) unterzeichnen, die bestätigt, dass sie sich der Bedeutung der Kundendaten bewusst sind. Verträge mit Externen werden im Vertragsregister von Arvato Systems gespeichert und enthalten alle notwendigen Sicherheitsanforderungen (z.B. Vertraulichkeit und Datenschutz). Alle Verträge werden durch den Rechtsberater von Arvato Systems geprüft. Klauseln zur Vertraulichkeit werden laufend durch Rechtsberater überprüft und bei Bedarf aktualisiert zur Verfügung gestellt, so dass stets aktuelle Klauseln verwendet werden.	Befragung des Rechtsberaters hinsichtlich der Prüfung von Verträgen sowie Einsichtnahme in jeweils eine Vertraulichkeits-vereinbarung für einen Mitarbeiter und einen Dienstleister sowie Beurteilung, ob die Geheimhaltungs- und Vertraulichkeitspflichten berücksichtigt sind und regelmäßig aktualisiert werden.	Keine Abweichung festgestellt.
Die Kontrollen sind zutreffend dargestellt sowie angemessen eingerichtet, um das oben genannte Kontrollziel zu erreichen.				

4. ASSET MANAGEMENT (AM)

Referenz BSI C5	Kriterium des BSI C5:2020	Arvato Systems Kontrollbeschreibung	Prüfungshandlung	Ergebnis
AM: Identifizieren der organisationseigenen Assets gewährleisten und ein angemessenen Schutzniveau über deren gesamten Lebenszyklus sicherstellen.				
AM-01	Der Cloud-Anbieter hat Verfahren für eine Inventarisierung der Assets eingerichtet. Die Inventarisierung erfolgt automatisch und/oder durch für die Assets zuständige Personen oder Gruppen, um eine vollständige, richtige, gültige und konsistente Erfassung über den Lebenszyklus der Assets sicherzustellen. Zu den Assets werden jene Informationen erfasst, die zur Anwendung des Verfahrens für den Umgang mit Risiken (vgl. OIS-07), einschließlich der Maßnahmen zur Behandlung dieser Risiken über den Lebenszyklus der Assets benötigt werden. Änderungen an diesen Informationen werden protokolliert. <u>Zusatzkriterium</u> Anwendungen zur Protokollierung und Überwachung berücksichtigen die zu den Assets erfassten Informationen, um bei Ereignissen, die zu einer Verletzung der Schutzziele führen können, die Auswirkungen auf Dienste und Funktionen des Cloud-Dienstes zu erkennen und eine Information der betroffenen Cloud-Kunden gemäß den vertraglichen Vereinbarungen zu unterstützen.	Die Inventarisierung der Assets liegt im Verantwortungsbereich von AWS. Aktuelle und vollständige Informationen zu den jeweiligen Assets können bei Bedarf über das AWS-Portal eingesehen werden. Zusätzlich erfolgt seitens Arvato Systems eine Synchronisation der Asset-Daten in eine interne Configuration Management Datenbank (CMDB). Arvato Systems hat hierzu einen Deployment-Prozess von Systemkomponenten definiert und eingerichtet. AWS-Assets und dazugehörige Informationen (z.B. Systemnamen oder Kunde) werden im Rahmen eines Deployments innerhalb der CMDB inventarisiert. Änderungen an den Informationen werden automatisch protokolliert und über das Incident Management überwacht.	Einsichtnahme in die Vorgehensweise zum Deployment von Systemkomponenten und Beurteilung, ob Asset-Informationen in einem dazugehörigen Inventar festgehalten werden. Einsichtnahme in die Verfahren zur Inventarisierung und der Protokollierung von Änderungen an den Asset-Informationen. Einsichtnahme in das Incident Management, ob eine Verknüpfung zum Asset-Inventar vorhanden ist, um Cloud-Kunden bei kritischen Ereignissen identifizieren und informieren zu können.	Keine Abweichung festgestellt.

AM-02	Richtlinien und Anweisungen für den zulässigen Gebrauch und den sicheren Umgang mit Assets sind gemäß SP-01 dokumentiert, kommuniziert und bereitgestellt und adressieren folgende Aspekte im Lebenszyklus von Assets, soweit diese für das Asset anwendbar sind: – Genehmigungsverfahren für Anschaffung, Inbetriebnahme, Instandhaltung, Außerbetriebnahme und Entsorgung durch autorisiertes Personal oder Systemkomponenten, – Inventarisierung, – Klassifizierung und Kennzeichnung auf Basis des Schutzbedarfs der Informationen sowie Maßnahmen zur ermittelten Schutzstufe, – sichere Konfiguration der Mechanismen für Fehlerbehandlung, Protokollierung, Verschlüsselung, Authentisierung und Autorisierung, – Anforderungen an Software- und Image-Versionen sowie Anwendung von Patches, – Umgang mit Software für die kein Support und keine Sicherheitsaktualisierungen mehr verfügbar sind, – Einschränkung von Software-Installationen oder Nutzung von Diensten, – Schutz vor Schadsoftware, – Remote-Deaktivierung, Löschung oder Sperrung, – physische Übergabe und Transport; – Umgang mit Störungen und Schwachstellen, – vollständige und unwiderrufliche Löschung der Daten bei Außerbetriebnahme.	Vorgaben zum Umgang mit Assets verteilen sich auf verschiedene Richtlinien sowie dem AWS-Betriebshandbuch und sind dort geregelt.	Befragung von Systemadministratoren hinsichtlich des Umgangs mit Assets. Einsichtnahme in Richtlinien und Anweisungen sowie dem AWS-Betriebs-handbuch zum Umgang mit Assets und Beurteilung, ob Vorgaben für die im Kriterium genannten Aspekte getroffen sind.	Keine Abweichung festgestellt.

AM-03	Der Cloud-Anbieter hat einen Freigabeprozess für den Einsatz von in Betrieb zunehmender Hardware, welche zur Bereitstellung des Cloud-Dienstes in der Produktionsumgebung verwendet wird, in welchem die aus der Inbetriebnahme entstehenden Risiken identifiziert, analysiert und mitigiert werden. Die Genehmigung erfolgt nach Verifikation der sicheren Konfiguration der Mechanismen für Fehlerbehandlung, Protokollierung, Verschlüsselung, Authentisierung und Autorisierung gemäß der vorgesehenen Verwendung und auf Basis der anwendbaren Richtlinien.	Nicht anwendbar – im Verantwortungsbereich von AWS.
AM-04	Die Außerbetriebnahme von Hardware, welche der Cloud-Anbieter in der Produktionsumgebung zum Betrieb von Systemkomponenten einsetzt, erfordert eine Genehmigung auf Basis der anwendbaren Richtlinien. Die Außerbetriebnahme beinhaltet die vollständige und unwiderrufliche Löschung der Daten oder die ordnungsgemäße Vernichtung der Datenträger.	Nicht anwendbar – im Verantwortungsbereich von AWS.
AM-05	Interne und externe Mitarbeiter des Cloud-Anbieters werden nachweislich auf die Richtlinien und Anweisungen für den zulässigen Gebrauch und den sicheren Umgang mit Assets verpflichtet, bevor diese verwendet werden dürfen, soweit der Cloud-Anbieter in einer Risikobewertung festgestellt hat, dass diese bei Verlust oder unautorisierten Zugriffen die Informationssicherheit des Cloud-Dienstes gefährden könnten. Ausgehändigte Assets werden bei der Beendigung des Beschäftigungs-verhältnisses nachweislich zurückgegeben. <u>Zusatzkriterium</u> Physische Assets der internen und externen Mitarbeiter unterliegen einer zentralen Verwaltung. Die zentrale Verwaltung ermöglicht eine Software-, Daten- und Richtlinienverteilung sowie eine Remote-Deaktivierung, -Löschung, oder -Sperrung.	Nicht anwendbar – im Verantwortungsbereich von AWS.

AM-06	Assets werden klassifiziert und, falls möglich, gekennzeichnet. Klassifizierung und Kennzeichnung eines Assets entsprechen dem Schutzbedarf der Informationen, die es verarbeitet, speichert oder übermittelt. Der Schutzbedarf wird durch die für Assets zuständigen Personen oder Gruppen des Cloud-Anbieters nach einem einheitlichen Schema ermittelt. Das Schema sieht Schutzstufen für die Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität vor. Zusatzkriterium Anwendungen zur Protokollierung und Überwachung berücksichtigen den Schutzbedarf der Assets, um bei Ereignissen, die zu einer Verletzung der Schutzziele führen können, das dafür zuständige Personal so zu informieren, dass erforderliche Maßnahmen mit einer geeigneten Priorität eingeleitet werden. Maßnahmen für Ereignisse bei Assets mit einem erhöhten Schutzbedarf haben Priorität vor Ereignissen bei Assets mit einem geringeren Schutzbedarf.	Der Prozess zur Klassifizierung von Assets ist in Richtlinien und im AWS-Betriebshandbuch einheitlich definiert und etabliert. Die Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität haben für die Kundendaten bereits im Design der Architektur höchste Priorität und damit verbunden den höchsten Schutzbedarf. Dementsprechend ist die Architektur der Infrastruktur bereits auf das höchste Schutzniveau der Daten ausgelegt und wird ausschließlich auf Verlangen des Kunden für definierte Services auf das vom Kunden vorgegebene Level reduziert. Der Schutzbedarf der Assets wird im Rahmen der Überwachung von protokollierten Ereignissen und des Incident Managements berücksichtigt. Wird bei der Überwachung eine Verletzung der Schutzziele festgestellt, erfolgt eine Benachrichtigung zur Einleitung von erforderlichen Maßnahmen an zuständige Mitarbeiter. Eine Priorisierung für Ereignisse mit erhöhtem Schutzbedarf ist definiert.	Einsichtnahme in Richtlinien und Verfahren im Hinblick auf Vorgaben zur Klassifizierung und Kennzeichnung von Informationen und Assets betreffend die Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität. Einsichtnahme in die Überwachung von Ereignissen und das Incident Management mit Beurteilung, ob eine Verknüpfung zum Asset-Inventar vorhanden ist, um bei kritischen Ereignissen und Verletzung von Schutzzielen zeitnah reagieren zu können. Einsichtnahme in abgeleitete Maßnahmen zur priorisierten Behebung von Ereignissen mit erhöhtem Schutzbedarf.	Keine Abweichung festgestellt.
Die Kontrollen sind zutreffend dargestellt sowie angemessen eingerichtet, um das oben genannte Kontrollziel zu erreichen.				

5. REGELBETRIEB (OPS)

Referenz BSI C5	Kriterium des BSI C5:2020	Arvato Systems Kontrollbeschreibung	Prüfungshandlung	Ergebnis
OPS: Sicherstellen eines ordnungsgemäßen Regelbetriebs einschließlich angemessener Maßnahmen für Planung und Überwachung der Kapazität, Schutz vor Schadprogrammen, Protokollierung und Überwachung von Ereignissen sowie den Umgang mit Schwachstellen, Störungen und Fehlern.				
OPS-01	Die Planung von Kapazitäten und Ressourcen (Personal und IT-Ressourcen) folgt einem etablierten Verfahren, um mögliche Kapazitätsengpässe zu vermeiden. Die Verfahren umfassen Prognosen von zukünftigen Kapazitätsanforderungen, um Nutzungstrends zu identifizieren und Risiken der Systemüberlastung zu beherrschen. Cloud-Anbieter stellen durch geeignete Maßnahmen sicher, dass sie bei Kapazitätsengpässen oder Ausfällen hinsichtlich Personal und IT-Ressourcen die mit den Cloud-Kunden vereinbarten Anforderungen an die Bereitstellung des Cloud-Dienstes, gemäß der jeweiligen Vereinbarungen weiterhin erfüllen, insbesondere solche hinsichtlich dedizierter Nutzung von Systemkomponenten. <u>Zusatzkriterium</u> Die Prognosen werden in Abstimmung mit der Dienstgütevereinbarung zur Planung und Vorbereitung der Provisionierung berücksichtigt.	Kapazitätsplanungen werden im Rahmen einer Geschäftsjahresplanung unter Berücksichtigung von zu erwartendem Neugeschäft (Prognosen) sowie Erfahrungswerten und Daten aus bestehendem Geschäft seitens des Managements (Führungskreis) durchgeführt. Die Planung berücksichtigt neben den Dienstgütevereinbarungen u.a. auch Elternzeiten, Vertretungen sowie Ausbildung und Einarbeitungszeiten.	Befragung von Managern des Führungskreises zu Planungen von Personal- und IT-Ressourcen im Rahmen des Capacity Management und dessen Dokumentation. Einsichtnahme in eine dokumentierte Ressourcenplanung im Rahmen der Geschäftsjahresplanung. Beurteilung, inwieweit der gemeldete Bedarf zur Vermeidung von Engpässen durch neue Personal- bzw. IT-Ressourcen gedeckt wurde und die Kapazitätsplanung in Einklang mit den Dienstgütevereinbarungen steht.	Keine Abweichung festgestellt.

OPS-02	Technische und organisatorische Maßnahmen zur Überwachung und Provisionierung bzw. De-Provisionierung von Cloud-Dienstleistungen sind definiert. Dadurch stellt der Cloud-Anbieter sicher, dass Ressourcen bereitgestellt bzw. Leistungen gemäß den vertraglichen Vereinbarungen erbracht werden und die Einhaltung der Dienstgütevereinbarungen sichergestellt ist. Zusatzkriterium Zur Überwachung der Kapazität und der Verfügbarkeit stehen dem Cloud-Kunden die relevanten Informationen in einem Self-Service-Portal zur Verfügung.	Kundenumgebungen und dazugehörige Systemkomponenten werden fortlaufend hinsichtlich notwendiger Ressourcen überwacht. Bei Überschreitung von definierten Schwellenwerten werden automatisch Alertings und Service-Tickets generiert und die zuständigen IT-Mitarbeiter informiert. Cloud-Kunden können über ein Self-Service-Portal (AWS-Portal) jederzeit die Ressourcenüberwachung einsehen.	Systemeinsichtnahme und Beurteilung, ob die Ressourcen von Kundenumgebungen überwacht werden. Einsichtnahme in das AWS-Self-Service-Portal und in das Arvato-internes OpsWatch-Portal für Kunden und Beurteilung, ob Kunden SLA-Metriken einsehen können.	Keine Abweichung festgestellt.
OPS-03	Entsprechend den Möglichkeiten des jeweiligen Servicemodells ist der Cloud-Kunde in der Lage die Aufteilung der ihm zur Verwaltung/Nutzung zugeordneten Systemressourcen zu steuern und zu überwachen, um eine Überbelegung der Ressourcen zu vermeiden und eine hinreichende Performance zu erreichen.	Der individuelle Kundenvertrag regelt das Zusammenarbeitsmodell und ermöglicht dem jeweiligen Cloud-Kunden seine Kundenumgebung selbst zu verwalten und die Bereitstellung von Systemressourcen eigenständig zu steuern.	Einsichtnahme in vertragliche Vereinbarungen (Kundenverträge) und Beurteilung, ob der Kunde die Möglichkeit hat, die Nutzung der Systemressourcen festzulegen und zu überwachen.	Keine Abweichung festgestellt.
OPS-04	Richtlinien und Anweisungen mit Vorgaben zum Schutz vor Schadprogrammen sind hinsichtlich der folgenden Aspekte gemäß SP-01 dokumentiert, kommuniziert und bereitgestellt: – Nutzung systemspezifischer Schutzmechanismen, – Betrieb von Schutzprogrammen auf Systemkomponenten im Verantwortungsbereich des Cloud-Anbieters, die für die Bereitstellung des Cloud-Dienstes in der Produktionsumgebung verwendet werden,	Die Anti-Virus-Policy definiert die Vorgaben zum Schutz vor Schadprogrammen und steht den Mitarbeitern über das Intranet zur Einsicht zur Verfügung. Die physischen Endgeräte der IT-Mitarbeiter sind vor Schadprogrammen geschützt und werden systemseitig überwacht. Der vorkonfigurierte Echtzeitschutz kann vom Endanwender nicht deaktiviert werden (Manipulationsschutz).	Einsichtnahme in die Anti-Virus-Policy sowie Verfahren und eingesetzte Tools betreffend die im Kriterium genannten Aspekte. Einsichtnahme in das Microsoft Defender Vulnerability Management Dashboard und Beurteilung, ob aktuelle und regelmäßige Auswertungen erstellt und durch autorisiertes Personal überprüft werden.	Keine Abweichung festgestellt.

	– Betrieb von Schutzprogrammen für Endgeräte der Mitarbeiter. Zusatzkriterium Der Cloud-Anbieter erstellt regelmäßige Reports über die durchgeführten Überprüfungen, welche durch autorisiertes Personal oder Gremien überprüft und analysiert werden. Richtlinien und Anweisungen beschreiben die technischen Maßnahmen zur sicheren Konfiguration und Überwachung der Managementkonsole (sowohl des Self-Service vom Kunden als auch die Cloud-Administration des Dienstleisters), um diese vor Schadprogrammen zu schützen. Die Aktualisierung erfolgt mit der höchsten Frequenz, die der/die Hersteller vertraglich anbietet/anbieten.	Regelmäßige und aktuelle Auswertungen über durchgeführte Überprüfungen, Angriffen und Bedrohungslagen stehen im Microsoft Defender Vulnerability Management Dashboard zur Verfügung und werden überwacht. Der individuelle Kundenvertrag regelt das Zusammenarbeitsmodell und ermöglicht dem jeweiligen Cloud-Kunden die Dashboard-Auswertungen selbst zu verwalten und eigenständig zu prüfen.	Einsichtnahme in vertragliche Vereinbarungen (Kundenverträge) und Beurteilung, ob der Kunde die Möglichkeit hat, die Auswertungen im Dashboard selbst zu überwachen.	
OPS-05	Systemkomponenten im Verantwortungsbereich des Cloud-Anbieters, die für die Bereitstellung des Cloud-Dienstes in der Produktionsumgebung verwendet werden, sind gemäß der in den Richtlinien und Anweisungen zum Schutz vor Schadprogrammen definierten Vorgaben geschützt. Soweit Schutzprogramme mit einer signatur- und/oder verhaltensbasierten Erkennung und Entfernung von Schadprogrammen eingerichtet sind, werden diese Schutzprogramme mindestens täglich aktualisiert. Zusatzkriterium Die Konfiguration der Schutzmechanismen wird automatisch überwacht. Abweichungen von den Vorgaben werden automatisch an das dafür sachverständige Personal berichtet, um diese umgehend einer Beurteilung zu unterziehen und erforderliche Maßnahmen einzuleiten.	Schutzprogramme (z.B. Antiviren-Software) werden gemäß der Anti-Virus-Policy automatisch auf Client-Computer verteilt und täglich aktuell gehalten. Zuständige Systemadministratoren werden auf Basis einer Überwachung über Abweichungen/ Änderungen an den zentralen Konfigurationen der Antivirus-Software automatisch informiert.	Systemeinsichtnahme und Beurteilung, ob Systeme und Client-Computer einen Schutz vor Schad-programmen erhalten, dieser täglich aktualisiert wird und ob Abweichungen/ Änderungen von Konfigurationen überwacht werden.	Keine Abweichung festgestellt.

OPS-06	Richtlinien und Anweisungen mit Vorgaben zur Datensicherung- und Wiederherstellung sind hinsichtlich der folgenden Aspekte gemäß SP-01 dokumentiert, kommuniziert und bereitgestellt. – Umfang und Häufigkeit der Datensicherung sowie die Dauer der Aufbewahrung entsprechen den vertraglichen Vereinbarungen mit den Cloud-Kunden sowie den Anforderungen an die betriebliche Kontinuität des Cloud-Anbieters hinsichtlich maximal tolerierbarer Ausfallzeit (Recovery Time Objective, RTO) und maximal zulässigem Datenverlust (Recovery Point Objective, RPO), – Die Datensicherung erfolgt in verschlüsselter Form, die dem aktuellen Stand der Technik entspricht, – Der Zugriff auf die gesicherten Daten und die Durchführung von Wiederherstellungen erfolgt nur durch autorisierte Personen, – Tests von Wiederherstellungsverfahren (vgl. OPS-08).	Auf Basis von Verträgen und Kundenvereinbarungen werden Sicherungs-, Speicher- und Verschlüsselungsverfahren definiert, dokumentiert und den zuständigen IT-Administratoren mitgeteilt. Teil dessen ist die Festlegung des Speicherumfangs, die Häufigkeiten, die Wiederherstellungstestverfahren, die Aufbewahrungsdauer sowie das Verschlüsselungsverfahren. Der Zugriff auf die gesicherten Daten und die Durchführung von Wiederherstellungen ist auf autorisierte Personen beschränkt.	Einsichtnahme in Kundenvereinbarungen und Betriebskonzepte und Beurteilung, ob Sicherungs- und Speicherverfahren betreffend der im Kriterium genannten Aspekte definiert und dokumentiert sind. Einsichtnahme in Datensicherungen und Beurteilung, ob vertraglich vereinbarte Verschlüsselungsverfahren eingerichtet wurden und nur autorisierte Personen Zugriff auf Daten und Wiederherstellungen hatten.	Keine Abweichung festgestellt.

OPS-07	Der Cloud-Anbieter überwacht die Durchführung der Datensicherung mit technischen und organisatorischen Maßnahmen. Störungen werden durch qualifizierte Mitarbeiter des Cloud-Anbieters untersucht und zeitnah behoben, um die Einhaltung der vertraglichen Verpflichtungen gegenüber den Cloud-Kunden oder den geschäftlichen Anforderungen des Cloud-Anbieters bezüglich des Umfangs und der Häufigkeit der Datensicherung sowie der Dauer der Aufbewahrung zu gewährleisten. Zusatzkriterium Zur Überwachung der Datensicherung stehen dem Cloud-Kunden die relevanten Protokolle oder die zusammengefassten Ergebnisse in einem Self-Service Portal zur Verfügung.	Die Durchführung von Datensicherungen wird technisch überwacht. Im Fall von Störungen beim Erzeugen der Sicherungen werden automatisch Fehlermeldungen an die zuständigen IT-Administratoren gemeldet. Im Rahmen des Incident Management Prozesses werden die jeweiligen Meldungen zeitnah untersucht und behoben. Im AWS-Portal stehen den Kunden die Ergebnisse der Datensicherung zur Verfügung.	Einsichtnahme in Verfahren und Maßnahmen zur Überwachung von Backup- und Recovery-Prozeduren innerhalb des AWS-Betriebshandbuchs im Hinblick auf die im Kriterium genannten Aspekte. Systemeinsichtnahme in Kundenumgebung und Beurteilung ob, Datensicherung und deren Durchführung von Cloud-Kunden überwacht werden können.	Keine Abweichung festgestellt.
OPS-08	Wiederherstellungsverfahren werden vom Cloud-Anbieter regelmäßig, mindestens jährlich, getestet. Die Tests erlauben eine Beurteilung darüber, ob die vertraglichen Vereinbarungen sowie die Vorgaben zur maximal tolerierbarer Ausfallzeit (Recovery Time Objective, RTO) und zum maximal zulässigem Datenverlust (Recovery Point Objective, RPO) eingehalten werden (vgl. BCM-02). Abweichungen von den Vorgaben werden an das dafür zuständige Personal oder die dafür zuständigen Systemkomponenten beim Cloud-Anbieter berichtet, damit diese die Abweichungen umgehend beurteilen und erforderliche Maßnahmen einleiten können. Zusatzkriterium Auf Kundenwunsch informiert der Cloud-Anbieter den Cloud-Kunden über die Ergebnisse der Wiederherstellungstests. Wiederherstellungstests sind in das Notfallmanagement des Cloud-Anbieters eingebettet.	Nicht anwendbar – im Verantwortungsbereich von AWS.		

OPS-09	Der Cloud-Anbieter überträgt zu sichernde Daten an einen Remote-Standort oder transportiert diese auf Sicherungsdatenträgern an einen Remote-Standort. Soweit die Datensicherung über ein Netz zum Remote-Standort übertragen wird, erfolgt die Datensicherung oder die Übertragung der Daten in einer verschlüsselten Form, die dem Stand der Technik entspricht. Die Entfernung zum Hauptstandort ist nach hinreichender Abwägung der Faktoren Wiederherstellungszeiten und Auswirkung von Katastrophen auf beide Standorte gewählt. Die Maßnahmen zur physischen und umgebungsbezogenen Sicherheit am Remote-Standort entsprechen dem Niveau am Hauptstandort.	Nicht anwendbar – im Verantwortungsbereich von AWS.		
OPS-10	Der Cloud-Anbieter hat Richtlinien und Anweisungen etabliert, welche das Protokollieren und Überwachen von Ereignissen auf Systemkomponenten in seinem Verantwortungsbereich regeln. Diese Richtlinien und Anweisungen sind hinsichtlich der folgenden Aspekte gemäß SP-01 dokumentiert, kommuniziert und bereitgestellt und enthalten folgende Aspekte: – Definition von Ereignissen, die zu einer Verletzung der Schutzziele führen können, – Vorgaben zum Aktivieren, Stoppen und Pausieren der verschiedenen Protokollierungen, – Informationen bezüglich des Zwecks sowie des Aufbewahrungszeitraums der Protokollierungen, – Festlegung von Rollen und Verantwortlichkeiten für die Einrichtung und Überwachung der Protokollierung, – Zeitsynchronisation von Systemkomponenten, – Einhaltung rechtlicher und regulatorischer Rahmenbedingungen.	Protokollierungsfunktionalitäten und deren Überwachung sind in der Leistungsbeschreibung, in dem Cloud Foundation Service Katalog (SKA) und Cloud Foundation Datenschutz (DS) geregelt und orientieren sich im Sinne eines Best Practice Ansatzes an einem Cloud Adoption Framework, das als Konfigurationsorientierung beim Aufbau von Kundenumgebungen und deren Protokollierung dient. Darüberhinausgehende Anforderungen an Protokollierungen können individuell mit dem Kunden vereinbart werden und werden im Rahmen des technischen Aufbaus der Cloudsystemumgebung berücksichtigt.	Einsichtnahme in das AWS-Betriebshandbuch und Beurteilung, ob die im Kriterium genannten Aspekte (z.B. Vorgaben zu Protokollierungs-konfigurationen) definiert und geregelt sind.	Keine Abweichung festgestellt.

OPS-11	Richtlinien und Anweisungen mit Vorgaben zur sicheren Handhabung von Metadaten (Nutzungsdaten) sind hinsichtlich der folgenden Aspekte gemäß SP-01 dokumentiert, kommuniziert und bereitgestellt: – Sammlung und Nutzung von Metadaten erfolgt ausschließlich für Abrechnungszwecke, zum Beheben von Störungen und Fehlern (Incident Management) sowie zum Bearbeiten von Sicherheitsvorfällen (Security Incident Management), – Ausschließliche Nutzung anonymisierter Metadaten zur Bereitstellung und Verbesserung des Cloud-Dienstes, sodass kein Rückschluss auf den Cloud Kunden oder Nutzer möglich ist, – keine kommerzielle Nutzung, – Speicherung für einen festgelegten Zeitraum, der in einem angemessenen Zusammenhang mit den Zwecken der Erhebung steht, – unverzügliche Löschung, wenn die Zwecke der Erhebung erfüllt sind und eine weitere Speicherung nicht mehr erforderlich ist, – Bereitstellung an Cloud-Kunden gemäß den vertraglichen Vereinbarungen. <u>Zusatzkriterium</u> Personenbezogene Daten werden automatisiert und soweit technisch möglich aus den Protokolldaten entfernt, bevor der Cloud-Anbieter diese verarbeitet. Die Entfernung erfolgt in einer Form, die es dem Cloud-Anbieter weiterhin ermöglicht, die Protokolldaten für den Zweck zu nutzen, zu dem sie erhoben wurden.	Die Erfassung, Verwendung und Löschung sowie die vertragliche Bereitstellung von Metadaten (Nutzungsdaten) erfolgt durch den Cloudanbieter AWS. Diese stehen den Kunden und Arvato Systems zur Verfügung. Interne Richtlinien wie der Cloud Foundation Service Katalog (SKA), der Cloud Foundation Datenschutz (DS) und das AWS-Betriebs-handbuch machen Vorgaben zur Handhabung von Metadaten und sind über das Intranet sowie das Knowledge Management System dokumentiert und für Mitarbeiter jederzeit einsehbar. Personenbezogene Daten werden automatisiert und soweit technisch möglich aus den Protokolldaten entfernt.	Einsichtnahme in Richtlinien, in Datenschutzrichtlinien und in das AWS-Betriebshandbuch sowie Beurteilung, ob Vorgaben zur Handhabung von Metadaten betreffend der im Kriterium genannten Aspekte dokumentiert und an die Mitarbeiter kommuniziert sind. Beurteilung, ob die Metadaten ausschließlich für die vertraglich festgelegten Zwecke verwendet werden. Einsichtnahme in Protokolldaten und Beurteilung, ob personenbezogene Daten gemäß den internen Richtlinien entfernt wurden.	Keine Abweichung festgestellt.

OPS-12	Die Vorgaben zur Protokollierung und Überwachung von Ereignissen sowie zur sicheren Handhabung von Metadaten werden durch technisch gestützte Verfahren hinsichtlich der folgenden Beschränkungen umgesetzt: – Zugriff nur für auf autorisierte Benutzer und Systeme – Speicherung für den festgelegten Zeitraum – Löschung, wenn weitere Speicherung für den Zweck der Erhebung nicht mehr erforderlich ist.	Der Zugriff auf Metadaten sowie die Konfiguration von Protokollierungen (z.B. Aufbewahrungszeitraum) in Cloudumgebungen wird über das interne Identity Access Management System und den dazugehörigen Berechtigungsrollen gesteuert, sodass nur autorisierte IT-Administratoren Zugriff erlangen können.	Einsichtnahme in die Konfiguration der für die Protokollierung und Überwachung eingesetzten IT-Systeme und Beurteilung, ob diese gemäß des Identity Management Systems Zugriffsbeschränkungen für autorisierte Mitarbeiter unterliegen.	Keine Abweichung festgestellt.
OPS-13	Die Protokollierungsdaten werden gemäß den Vorgaben zur Protokollierung und Überwachung automatisch auf Ereignisse überwacht, die zu einer Verletzung der Schutzziele führen können. Dies umfasst auch die Erkennung von Beziehungen zwischen Ereignissen (Ereigniskorrelation). Identifizierte Ereignisse werden automatisch an das dafür zuständige Personal oder die dafür zuständigen Systemkomponenten des Cloud-Anbieters berichtet, um die Ereignisse umgehend einer Beurteilung zu unterziehen und erforderliche Maßnahmen einzuleiten.	Cloudumgebungen werden mittels implementierter Monitoringsysteme fortlaufend überwacht, die zu einer Verletzung der Schutzziele führen können. Die Systeme prüfen, ob Schwellenwerte (z.B. Kapazitätsengpässe) überschritten oder festgelegte Events ausgelöst werden. Für identifizierte Ereignisse werden automatisch Alertings und dazugehörige Incident-Tickets erzeugt, die von den zuständigen IT-Administratoren zeitnah bearbeitet werden.	Einsichtnahme in Monitoringsysteme und Beurteilung, ob Kundensysteme überwacht und im Fall von Events Alertings und dazugehörige Incident Tickets generiert werden.	Keine Abweichung festgestellt.

OPS-14	Der Cloud-Anbieter bewahrt die erstellten Protokollierungsdaten unabhängig von der Quelle dieser Daten, geeignet und unveränderlich aggregiert auf, sodass eine zentrale, autorisierte Auswertung der Daten möglich ist. Protokollierungsdaten werden gelöscht, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind. Zwischen Protokollierungsservern und den zu protokollierenden Assets erfolgt eine Authentisierung, um die Integrität und Authentizität der übertragenen und gespeicherten Informationen zu schützen. Die Übertragung erfolgt nach einer dem Stand der Technik entsprechenden Verschlüsselung oder über ein eigenes Administrationsnetz (Out-of-Band-Management). <u>Zusatzkriterium</u> Der Cloud-Anbieter bietet auf Anfrage des Cloud-Kunden eine kundenspezifische Protokollierung (in Bezug auf Umfang und Dauer der Aufbewahrung) an und stellt diese dem Kunden zur Verfügung. In Abhängigkeit des Schutzbedarfs des Cloud-Anbieters und der technischen Realisierbarkeit wird eine logische oder eine physikalische Trennung von Protokoll- und Nutzdaten vorgenommen.	Im AWS-Betriebshandbuch sowie der internen Datenschutzrichtlinie ist die Aufbewahrungsdauer von Protokolldaten geregelt. Diese stehen unveränderlich für zentrale und autorisierte Auswertungen zur Verfügung. Darüber hinaus benötigte Anforderungen werden kundenindividuell vereinbart und im Betriebshandbuch dokumentiert. Datenübertragungen an Protokollserver außerhalb der AWS-Cloudumgebung finden nicht statt.	Einsichtnahme in die Richtlinie und das Betriebshandbuch hinsichtlich der Aufbewahrung von Protokolldaten betreffend der im Kriterium genannten Aspekte. Systemeinsichtnahme einer Kundenumgebung und Beurteilung, ob eine Verschlüsselung für Datenübertragung außerhalb der Cloud-Umgebung konfiguriert ist.	Keine Abweichung festgestellt.

OPS-15	Die erstellten Protokollierungsdaten erlauben eine eindeutige Identifizierung von Benutzerzugriffen auf Tenant-Ebene, um (forensische) Analysen im Falle eines Sicherheitsvorfalls zu unterstützen. Für die Durchführung der forensischen Analysen und Sicherungen von Infrastrukturkomponenten sowie deren Netzkommunikation stehen Schnittstellen zur Verfügung. Zusatzkriterium Der Cloud-Anbieter stellt auf Anfrage des Cloud-Kunden die ihn betreffenden Protokolle in angemessener Form und zeitnah zur Verfügung, damit dieser die ihn betreffenden Vorfälle selbst untersuchen kann.	Die implementierte Standardprotokollierungs-funktionalität für Cloudumgebungen (gemäß Cloud Adoption Framework) ermöglicht die Auswertung und Identifizierung von Benutzerzugriffen. Die Protokolle können über Standardschnittstellen bei Bedarf exportiert werden.	Systemeinsichtnahme und Beurteilung, ob auf Basis der Protokollierungsdaten Benutzerzugriffe zuzuordnen sind. Systemeinsichtnahme und Beurteilung, ob Schnittstellen für forensische Analysen von Protokollierungsdaten zur Verfügung stehen.	Keine Abweichung festgestellt.
OPS-16	Der Zugriff auf Systemkomponenten zur Protokollierung- und Überwachung im Verantwortungsbereich des Cloud-Anbieters ist auf autorisierte Benutzer beschränkt. Änderungen an der Konfiguration erfolgen gemäß den anwendbaren Richtlinien und Anweisungen (vgl. DEV-03). Zusatzkriterium Der Zugriff auf Systemkomponenten zur Protokollierung und Überwachung im Verantwortungsbereich des Cloud-Anbieters erfordert eine Zwei-Faktor-Authentifizierung.	Im AWS-Betriebshandbuch ist geregelt, welche Mitarbeiter für die Administration der Systemkomponenten und der dazugehörigen Konfiguration autorisiert sind. Der Zugriff erfolgt gemäß der Business-Rollen des Identity Access Management Systems und den dazugehörigen Sicherheitsgruppen restriktiv für autorisierte IT-Administratoren.	Einsichtnahme in das Identity Access Management System und Beurteilung, ob der Zugriff auf und die Verwaltung von Systemkomponenten zur Protokollierung- und Überwachung auf autorisierte Benutzer gemäß den eingerichteten Business-Rollen beschränkt ist. Beobachtung eines autorisierten Benutzers beim Zugriff auf eine Cloudumgebung und Beurteilung, ob eine Zwei-Faktor-Authentifizierung implementiert ist.	Keine Abweichung festgestellt.

OPS-17	Der Cloud-Anbieter überwacht die Protokollierungs- und Überwachungssysteme in seinem Verantwortungsbereich. Ausfälle werden automatisch und umgehend an das dafür zuständige Personal oder die dafür zuständigen Systemkomponenten des Cloud-Anbieters berichtet, sodass diese die Ausfälle beurteilen und erforderliche Maßnahmen einleiten können. Zusatzkriterium Die Systemkomponenten zur Protokollierung- und Überwachung sind so aufgebaut, dass bei Ausfällen einzelner Komponenten die Funktionalität insgesamt nicht eingeschränkt ist.	Nicht anwendbar – im Verantwortungsbereich von AWS.
OPS-18	Richtlinien und Anweisungen mit technischen und organisatorischen Maßnahmen sind gemäß SP-01 dokumentiert, kommuniziert und bereitgestellt, um das zeitnahe Identifizieren und Adressieren von Schwachstellen der Systemkomponenten, die für die Bereitstellung des Cloud-Dienstes verwendet werden, zu gewährleisten. Diese Richtlinien und Anweisungen enthalten Vorgaben zu folgenden Aspekten: – Regelmäßiges Identifizieren von Schwachstellen (Vulnerabilities), – Beurteilen des Schweregrads identifizierter Schwachstellen, – Priorisieren und Umsetzen von Maßnahmen zur zeitnahen Behebung oder Mitigation identifizierter Schwachstellen auf Basis des Schweregrades gemäß definierter Zeitvorgaben, – Umgang mit Systemkomponenten, für die basierend auf einer Risikobewertung keine Maßnahmen zur zeitnahen Behebung oder Mitigation der Schwachstellen eingeleitet werden.	Nicht anwendbar – im Verantwortungsbereich von AWS.

OPS-19	Der Cloud-Anbieter lässt mindestens jährlich Penetrationstests durch qualifiziertes internes Personal oder externe Dienstleister durchführen. Die Penetrationstests erfolgen nach einer dokumentierten Testmethodik und umfassen die für die Erbringung des Cloud-Dienstes relevanten Systemkomponenten im Verantwortungsbereich des Cloud-Anbieters, die im Rahmen einer Risiko-Analyse als solche identifiziert wurden. Der Cloud-Anbieter hat den Schweregrad der in Penetrationstests getroffenen Feststellungen nach definierten Kriterien zu beurteilen. Für Feststellungen mit mittlerer oder hoher Kritikalität in Bezug auf die Vertraulichkeit, Integrität oder Verfügbarkeit des Cloud-Dienstes sind innerhalb definierter Zeitfenster Maßnahmen zur zeitnahen Behebung oder Mitigation durchzuführen. <u>Zusatzkriterium</u> Die Tests finden halbjährlich statt. Diese müssen zwingend durch unabhängige Externe durchgeführt werden. Internes Personal für Penetrationstests darf die externen Dienstleister dabei unterstützen.	Nicht anwendbar – im Verantwortungsbereich von AWS.
OPS-20	Der Cloud-Anbieter führt regelmäßige Messungen, Analysen und Bewertungen der Verfahren zum Umgang mit Schwachstellen (Vulnerabilities) und Störungen (Incidents) durch, um deren fortdauernde Eignung, Angemessenheit und Wirksamkeit zu überprüfen. Ergebnisse werden mindestens quartalsweise durch verantwortliches Personal des Cloud-Anbieters bewertet, um Maßnahmen zur fortlaufenden Verbesserung zu initiieren oder deren Wirksamkeit zu überprüfen.	Nicht anwendbar – im Verantwortungsbereich von AWS.

OPS-21	Der Cloud-Anbieter informiert den Cloud-Kunden regelmäßig und in angemessener Form, die den vertraglichen Vereinbarungen entspricht, über den Status der den Cloud-Kunden betreffenden Störungen (Incidents) und bindet diesen, soweit angemessen und erforderlich, in deren Behebung ein. Sobald eine Störung aus Sicht des Cloud-Anbieters behoben wurde, wird der Cloud-Kunde gemäß den vertraglichen Vereinbarungen über die getroffenen Maßnahmen informiert.	Störungen werden über den internen Incident Management Prozess verwaltet und in einem Service Management System dokumentiert. Auf Basis der vertraglichen Vereinbarung wird der Cloud-Kunde über den Bearbeitungsstatus der jeweiligen Störung und deren Behebung informiert. Ebenso wird der Kunde informiert, falls Handlungsbedarf auf Seite des Kunden besteht, um die Störung zu beheben.	Einsichtnahme in das Incident Management System und Beurteilung, ob Kunden gemäß ihres SLA hinsichtlich des Bearbeitungsstatus von Störungen informiert werden.	Keine Abweichung festgestellt.
OPS-22	Systemkomponenten im Verantwortungsbereich des Cloud-Anbieters für die Erbringung des Cloud-Dienstes werden gemäß den Vorgaben zum Umgang mit Schwachstellen (vgl. OPS-18), mindestens monatlich, automatisiert auf bekannte Schwachstellen (Vulnerabilities) geprüft, der Schweregrad nach definierten Kriterien beurteilt und Maßnahmen zur zeitnahen Behebung oder Mitigation innerhalb definierter Zeitfenster eingeleitet. <u>Zusatzkriterium</u> Sicherheitspatches werden ab dem Zeitpunkt ihrer Verfügbarkeit in Abhängigkeit des nach der jüngsten Version des Common Vulnerability Scoring Systems (CVSS) eingeordneten Schweregrades der dadurch adressierten Schwachstellen eingespielt: Kritisch (CVSS = 9.0 - 10.0): 3 h Hoch (CVSS = 7.0 - 8.9): 3 Tage Mittel (CVSS = 4.0 - 6.9): 1 Monat Niedrig (CVSS = 0.1 - 3.9): 3 Monate	Nicht anwendbar – im Verantwortungsbereich von AWS.		

OPS-23	Systemkomponenten im Verantwortungsbereich des Cloud-Anbieters, die für die Bereitstellung des Cloud-Dienstes in der Produktionsumgebung verwendet werden, sind gemäß allgemein akzeptierter Branchenstandards gehärtet. Die je Systemkomponente anzuwendenden Vorgaben zur Härtung sind dokumentiert. Soweit nicht veränderliche ("immutable") Images eingesetzt werden, wird die Einhaltung der Vorgaben zur Härtung bei der Erstellung der Images in einem konsistenten Verfahren überprüft. Konfigurations- und Log-Dateien bezüglich der kontinuierlichen Bereitstellung dieser Images werden aufbewahrt. <u>Zusatzkriterium</u> Systemkomponenten im Verantwortungsbereich des Cloud-Anbieters werden automatisch auf Einhaltung der Vorgaben zur Härtung überwacht. Abweichungen von den Vorgaben werden automatisch an das dafür zuständige Personal oder die dafür zuständigen Systemkomponenten des Cloud-Anbieters berichtet, um sodass diese die Abweichungen umgehend einer Beurteilung unterziehen und erforderliche Maßnahmen einleiten können.	Nicht anwendbar – im Verantwortungsbereich von AWS.
OPS-24	Auf gemeinsam genutzten virtuellen und physischen Ressourcen gespeicherte und verarbeitete Daten der Cloud-Kunden sind gemäß eines dokumentierten Konzepts auf Basis einer Risikoanalyse gemäß OIS-07 sicher und strikt separiert, um die Vertraulichkeit und Integrität dieser Daten zu gewährleisten. <u>Zusatzkriterium</u> Ressourcen im Speichernetz (Storage) sind durch sichere Zonierung (LUN Binding und LUN Masking) segmentiert.	Nicht anwendbar – im Verantwortungsbereich von AWS.
Die Kontrollen sind zutreffend dargestellt sowie angemessen eingerichtet, um das oben genannte Kontrollziel zu erreichen.		

6. IDENTITÄTS- UND BERECHTIGUNGSMANAGEMENT (IDM)

Referenz BSI C5	Kriterium des BSI C5:2020	Arvato Systems Kontrollbeschreibung	Prüfungshandlung	Ergebnis
IDM: Absichern der Autorisierung und Authentifizierung von Benutzern des Cloud-Anbieters (i.d.R. privilegierte Benutzer) zur Verhinderung von unberechtigten Zugriffen.				
IDM-01	Ein auf den Geschäfts- und Sicherheitsanforderungen des Cloud-Anbieters basierendes Rollen- und Rechtekonzept sowie eine Richtlinie zur Verwaltung von Zugangs- und Zugriffs-berechtigungen für interne und externe Mitarbeiter des Cloud-Anbieters sowie für System-komponenten, die eine Rolle in automatisierten Autorisierungs-prozessen des Cloud-Anbieters innehaben, sind gemäß SP-01 mit folgenden Vorgaben dokumentiert, kommuniziert und bereitgestellt: – Vergabe eindeutiger Benutzernamen, – Vergabe und Änderung von Zugangs- und Zugriffsberechtigungen auf Basis des Prinzips der geringsten Berechtigung („Least-Privilege-Prinzip") und wie es für die Aufgaben-wahrnehmung notwendig ist („Need-to-Know-Prinzip"), – Funktionstrennung zwischen operativen und kontrollierenden Funktionen („Segregation of Duties"), – Funktionstrennung in der Verwaltung von Rechteprofilen, Genehmigung und Zuweisung von Zugangs- und Zugriffsberechtigungen, – Genehmigung der Vergabe oder Änderung durch autorisiertes Personal oder autorisierte System-komponenten bevor auf Daten der Cloud-Kunden oder Systemkomponenten zur Bereitstellung des Cloud-Dienstes zugegriffen werden kann, – regelmäßige Überprüfung vergebener Zugangs- und Zugriffsberechtigungen,	Eine Access Control Policy ist definiert, dokumentiert und an die Mitarbeiter über das Intranet kommuniziert. Die Policy macht Vorgaben zur Einrichtung und Verwaltung von Benutzern und Berechtigungsrollen (z.B. Berechtigungsvergabe, Benutzersperren oder Überprüfung bestehender Berechtigungen) sowie deren Dokumentation.	Einsichtnahme in die Access Control Policy und Beurteilung, ob die Inhalte betreffend der im Kriterium genannten Aspekte (z.B. Berechtigungsvergabe nach dem „Least-Privilege-Prinzip“) innerhalb der Policy geregelt sind.	Keine Abweichung festgestellt.

	– Sperrung und Entzug von Zugangsberechtigungen bei Inaktivität, – Zeitbasierter oder anlassbezogener Entzug bzw. Anpassung von Zugriffsberechtigungen bei Veränderungen des Aufgabengebiets, – Zwei- oder Mehr-Faktor-Authentisierung für Benutzer mit privilegierten Zugriffsberechtigungen, – Anforderungen an Genehmigung und Dokumentation der Verwaltung von Zugangs- und Zugriffsberechtigungen.			
IDM-02	Geregelte Verfahren für die Vergabe und Änderung von Zugangs- und Zugriffsberechtigungen für interne und externe Mitarbeiter des Cloud-Anbieters sowie für Systemkomponenten, die eine Rolle in automatisierten Autorisierungsprozessen des Cloud-Anbieters innehaben, stellen die Einhaltung des Rollen- und Rechtekonzepts sowie der Richtlinie zur Verwaltung von Zugangs- und Zugriffsberechtigungen sicher. <u>Zusatzkriterium</u> Der Cloud-Anbieter bietet Cloud-Kunden einen Self-Service an, mit welchem diese Zugangs- und Zugriffsberechtigungen eigenständig vergeben und ändern können.	Ein User Access Management Prozess ist definiert, der mittels eines implementierten Identity Access Management Systems (IAM) die Vergabe und Änderung von Berechtigungen für alle Mitarbeiter steuert und verwaltet. Über eingerichtete Business-Rollen innerhalb des IAM und dazugehörige Sicherheitsgruppen werden Funktionstrennungen eingehalten sowie die Berechtigungsvergabe bzw. Berechtigungsänderung dokumentiert. Abhängig vom jeweiligen Kundenvertrag hat der Kunde die Möglichkeit, Zugriffberechtigungen selbst zu steuern.	Einsichtnahme in den dokumentierten User Access Management Prozess sowie des IAM Systems und Beurteilung, ob die Vergabe und Änderung von Zugangs- und Zugriffsberechtigungen für interne und externe Mitarbeiter sowie Systemkomponenten entsprechend den Vorgaben erfolgten.	Keine Abweichung festgestellt.

IDM-03	Zugangsberechtigungen interner und externer Mitarbeiter des Cloud-Anbieters sowie von Systemkomponenten, die eine Rolle in automatisierten Autorisierungsprozessen des Cloud-Anbieters innehaben, werden gesperrt, wenn diese über einen Zeitraum von zwei Monaten nicht genutzt wurden. Das Entsperren erfordert die Genehmigung durch eine hierzu autorisierte Instanz. Nach spätestens sechs Monaten werden die gesperrten Zugangsberechtigungen entzogen. Nach Entzug ist das Verfahren für die Vergabe (vgl. IDM-02) erneut zu durchlaufen.	Ungenutzte Zugangs-berechtigungen, die länger als 30 Tage nicht aktiv waren, werden nach 35 Tagen gesperrt. Vorab werden Mitarbeiter auf den Ablauf der Berechtigung hingewiesen. Eine Entsperrung kann über den User Access Management Prozess angefordert und genehmigt werden. Nach drei Monaten werden Zugangsberechtigungen entzogen und gelöscht. Eine erneute Vergabe kann über den User Access Management Prozess angefordert und genehmigt werden. Darüber hinaus werden vergebene Berechtigungen im Rahmen eines Rezertifizierungsprozesses (Benutzerreviews) spätestens halbjährlich durch Business-Rollen-Owner geprüft. Die Entscheidung, ob eine Berechtigung entzogen wird, wird individuell entschieden.	Einsichtnahme in das IAM-System und Beurteilung, ob Meldungen zu ungenutzten Zugangsberechtigungen an die Mitarbeiter des User-Access-Managements gemeldet werden. Einsichtnahme in Konfigurationsdateien zu Sperrungs- und Löschfristen von Zugangsberechtigungen sowie in administrative Protokolle zu Sperrungen und Löschungen mit Beurteilung, ob die im Kriterium genannten Vorgaben umgesetzt sind. Einsichtnahme in einen dokumentierten Rezertifizierungsprozess und Beurteilung, ob ungenutzte bzw. gesperrte Zugangsberechtigungen eine Prüfung durch Business-Rollen-Owner unterzogen werden und ob das Entsperren genehmigt wurde.	Keine Abweichung festgestellt.

IDM-04	Zugriffsberechtigungen werden bei Änderungen im Aufgabengebiet der internen und externen Mitarbeiter des Cloud-Anbieters oder der Systemkomponenten, die eine Rolle in automatisierten Autorisierungsprozessen des Cloud-Anbieters innehaben, zeitnah entzogen. Privilegierte Zugriffsberechtigungen werden spätestens 48 Stunden nach Inkrafttreten der Änderung angepasst oder entzogen. Alle anderen Zugriffsberechtigungen werden spätestens nach 14 Tagen angepasst oder entzogen. Nach Entzug ist das Verfahren für die Vergabe (vgl. IDM-02) erneut zu durchlaufen.	Änderungen von Zugriffsberechtigungen werden seitens der Führungskräfte nach Bekanntwerden der Änderung innerhalb des Identity Access Management Systems eingepflegt. Bei Austritten findet über das System Tag genau automatisch eine Deprovisionierung der Berechtigungsrolle bzw. eine Accountdeaktivierung statt. Für notwendige Anpassungen der Sicherheitsgruppen für den jeweiligen Mitarbeiter (z.B. aufgrund von Abteilungswechseln) werden entsprechende Service-Tickets für das User Management erzeugt und diese zeitnah umgesetzt.	Einsichtnahme in den User Access Management Prozess, ob Regelungen zum Entzug oder zur Anpassung von Berechtigungen bei Wechsel des Aufgabengebiets definiert sind. Einsichtnahme in einen Austritt innerhalb des IAM-Systems und Beurteilung, ob automatische Deprovisionierungen stattfinden sowie Service-Tickets bei Änderungen erzeugt werden.	Keine Abweichung festgestellt.

IDM-05	Zugriffsberechtigungen interner und externer Mitarbeiter des Cloud-Anbieters sowie von Systemkomponenten, die eine Rolle in automatisierten Autorisierungsprozessen des Cloud-Anbieters innehaben, werden mindestens jährlich daraufhin überprüft, ob diese noch dem tatsächlichen Aufgaben- bzw. Einsatzgebiet entsprechen. Die Überprüfung erfolgt durch hierzu autorisierte Personen aus den Organisationseinheiten des Cloud-Anbieters, die aufgrund ihres Wissens über die Aufgabengebiete der Mitarbeiter oder Systemkomponenten die Angemessenheit der vergebenen Zugriffsberechtigungen beurteilen können. Identifizierte Abweichungen werden zeitnah, spätestens aber 7 Tage nach ihrer Feststellung durch geeignetes Ändern oder Entziehen der Zugriffsberechtigungen behandelt. Zusatzkriterium Privilegierte Berechtigungen werden mindestens halbjährlich überprüft.	Im Rahmen der Access Control Policy ist ein Rezertifizierungsprozess definiert, der mittels des Identity Access Management Systems gesteuert wird. Mindestens zwei Mal im Jahr werden die Zuweisungen von Business-Rollen zu Mitarbeiteraccounts seitens der Business-Rollen-Owner überprüft. Identifizierte unautorisierte Zuweisungen werden innerhalb von 7 Tagen durch Entzug oder Änderung der Berechtigungen (z.B. durch Löschen aus einer Sicherheitsgruppe) bearbeitet.	Einsichtnahme in die Access Control Policy im Hinblick auf eine mindestens jährliche (bei privilegierten Berechtigungen halbjährliche) Überprüfung der Zugriffsberechtigungen (Rezertifizierung) durch Business-Rollen-Owner und Nachvollzug, ob daraus abgeleitete Berechtigungsanpassungen zeitnah, spätestens aber 7 Tage nach ihrer Feststellung durch autorisierte Personen vorgenommen wurden. Einsichtnahme in einen dokumentierten Rezertifizierungsprozess mittels des IAM-Systems.	Keine Abweichung festgestellt.

IDM-06	Vergabe und Änderung von privilegierten Zugriffsberechtigungen für interne und externe Mitarbeiter sowie technische Benutzer des Cloud-Anbieters erfolgen gemäß der Richtlinie zur Verwaltung von Zugangs- und Zugriffs-berechtigungen (vgl. IDM-01) oder einer separaten Richtlinie. Privilegierte Zugriffsberechtigungen werden personalisiert sowie gemäß einer Risikobewertung zeitlich befristet und wie es für die Aufgabenwahrnehmung notwendig ist („Need-to-Know-Prinzip") zugewiesen. Technische Benutzer werden zudem internen oder externen Mitarbeitern des Cloud-Anbieters zugewiesen. Die Aktivitäten von Benutzern mit privilegierten Zugriffsberechtigungen werden protokolliert, um einen Missbrauch dieser Berechtigungen im Verdachtsfall aufdecken zu können. Die protokollierten Informationen werden automatisch auf definierte Ereignisse überwacht, die einen Missbrauch darstellen können. Bei Identifikation eines solchen Ereignisses wird das dafür zuständige Personal des Cloud-Anbieters automatisch informiert, um unverzüglich beurteilen zu können, ob ein Missbrauch vorliegt und entsprechende Maßnahmen einzuleiten sind. Bei nachweislich missbräuchlicher Nutzung privilegierter Zugriffsberechtigungen werden Disziplinarmaßnahmen gemäß HR-04 eingeleitet.	Die Vergabe von privilegierten Zugriffsberechtigungen erfolgt auf Basis des vorgesehenen User Access Management Prozesses mittels des IAM Systems (in Verbindung mit einem Priviledged Access Management Systems (PAM)). Eine Berechtigungszuweisung erfolgt immer zeitlich befristet sowie personalisiert, sodass über Protokollfunktionalitäten Benutzeraktivitäten auswertbar sind. Protokolldaten werden hinsichtlich eines Missbrauchs fortlaufend überwacht. Zuständige Systemadministratoren werden beim Auslösen von definierten Ereignissen informiert und prüfen die jeweiligen Meldungen. Im Fall von missbräuchlicher Nutzung von Zugriffsberechtigungen werden Disziplinarmaßnahmen eingeleitet.	Einsichtnahme in die Access Control Policy und Beurteilung, ob die im Kriterium genannten Aspekte (z.B. zeitlich befristete Vergabe von privilegierten Berechtigungen, Benutzerprotokollierung etc.) geregelt sind. Systemeinsichtnahme in das PAM-System und Beurteilung, ob Benutzeraktivitäten protokolliert und überwacht werden. Systemeinsichtnahme in das Monitoring und Beurteilung, ob zuständige Systemadministratoren über Ereignisse mit potenziellem Missbrauch informiert werden. Befragung HR-Manager hinsichtlich eingeleiteter Disziplinarmaßnahmen.	Keine Abweichung festgestellt.

IDM-07	Der Cloud-Kunde wird durch den Cloud-Anbieter über Ereignisse informiert, bei denen interne oder externe Mitarbeiter des Cloud-Anbieters, ohne vorherige Zustimmung des Cloud-Kunden, lesend oder schreibend auf die im Cloud-Dienst verarbeiteten, gespeicherten oder übertragenen Daten der Cloud-Kunden zugreifen werden oder zugegriffen haben. Die Information erfolgt je Ereignis, soweit die Daten des Cloud-Kunden nicht verschlüsselt sind/waren, die Verschlüsselung für den Zugriff aufgehoben wird/wurde oder die vertraglichen Vereinbarungen eine solche Information nicht explizit ausschließen. Aus der Information gehen Anlass, Zeitpunkt, Dauer, Art und Umfang des Zugriffs hervor. Die Informationen sind hinreichend detailliert, um sachverständigen Personen des Cloud-Kunden eine Risikobeurteilung des Zugriffs zu ermöglichen. Die Information erfolgt gemäß der vertraglichen Vereinbarung, spätestens aber 72 Stunden nach dem Zugriff. <u>Zusatzkriterium</u> Zugriffe auf die im Cloud-Dienst verarbeiteten, gespeicherten oder übertragenen Daten durch interne oder externe Mitarbeiter des Cloud-Anbieters bedürfen der vorherigen Zustimmung durch autorisiertes Personal des Cloud-Kunden, soweit die Daten des Cloud-Kunden nicht verschlüsselt sind, die Verschlüsselung für den Zugriff aufgehoben wird oder die vertraglichen Vereinbarungen eine solche Zustimmung nicht explizit ausschließen. Für die Zustimmung werden dem autorisierten Personal aussagekräftige Information über Anlass, Zeitpunkt, Dauer, Art und Umfang des Zugriffs vorgelegt, um eine Risikobeurteilung des Zugriffs zu ermöglichen.	Zugriffe auf Kundendaten ohne vorherige Zustimmung des Cloud-Kunden sind im Rahmen der Serviceerbringung nicht vorgesehen und werden nur zu Supportzwecken auf Basis einer Kundenaufforderung temporär durchgeführt und sind im Service Management Tool dokumentiert. Arvato Systems stellt eine optionale Funktion zur Verfügung, mit deren Hilfe sich Kunden aktiv benachrichtigen lassen können, sofern ein vom Kunden berechtigter Mitarbeiter der Arvato Systems Wartungs-tätigkeiten im Account des Kunden vornimmt. Diese Funktion wird standardmäßig nicht für ein Kundenkonto aktiviert und ist bei Bedarf durch den Kunden zu beantragen. Es lassen sich dabei neben Ereignissen wie etwa Anlass, Zeitpunkt, Dauer, Art und Umfang des Zugriffs auch weitere Ereignisse des Kunden-Accounts überwachen und bei Bedarf als automatische Mailbenachrichtigung einrichten.	Befragung von Systemadministratoren hinsichtlich des Zugriffs auf Kundendaten und der dazugehörigen Vorgehensweise. Einsichtnahme in das Service Management Tool und Beurteilung, ob eine vorherige Zustimmung des Cloud Kunden vorlag, die Kundenaufforderung temporär durchgeführt und dokumentiert wurde. Einsichtnahme in einen AWS-Account mit kundenseitig aktivierter Benachrichtigungsfunktion und Beurteilung, ob die automatische Mailbenachrichtigung über Ereignisse wie Anlass, Zeitpunkt, Dauer, Art und Umfang des Zugriffs informiert.	Keine Abweichung festgestellt.

IDM-08	Die Zuteilung von Authentisierungs-informationen zum Zugriff auf Systemkomponenten zur Bereitstellung des Cloud-Dienstes an interne und externe Benutzer des Cloud-Anbieters und System-komponenten, die eine Rolle in automatisierten Autorisierungs-prozessen des Cloud-Anbieters innehaben, erfolgt in einem geordneten Verfahren, das die Vertraulichkeit der Informationen sicherstellt. Soweit Passwörter als Authentisierungsinformationen eingesetzt werden, ist deren Vertraulichkeit durch folgende Verfahren sichergestellt, soweit dies technisch möglich ist: – Benutzer können das Passwort initial selbst erstellen oder müssen ein initial vorgegebenes Passwort bei der ersten Anmeldung an der Systemkomponente ändern. Ein initial vorgegebenes Passwort verliert nach maximal 14 Tagen seine Gültigkeit – Beim Erstellen von Passwörtern wird das Einhalten der Passwort-Vorgaben erzwungen, soweit dies technisch möglich ist – Der Benutzer wird über das Ändern oder Zurücksetzen des Passworts informiert – Die serverseitige Speicherung erfolgt unter Anwendung kryptographisch starker Passworthashfunktionen – Abweichungen sind durch eine Risikoanalyse bewertet und daraus abgeleitete, mitigierende Maßnahmen umgesetzt. <u>Zusatzkriterium</u> Die Benutzer bestätigen in einer Erklärung (vgl. HR-06), dass sie persönliche (bzw. geteilte) Authentisierungsinformationen vertraulich behandeln und ausschließlich für sich (bzw. innerhalb der Gruppe) behalten.	Die Access Control Policy sowie die Passwortlichtlinie definieren die Anforderungen und die Vergabe von Passwörtern an Benutzer. Die technische Umsetzung der Richtlinien erfolgt über die implementierten Active Directory Policy Parameter. Jeder Mitarbeiter bestätigt im Rahmen der Unterzeichnung der Breitbandverpflichtung, dass Authentisierungs-informationen vertraulich behandelt werden.	Einsichtnahme in die Passwortrichtlinie und Beurteilung, ob die im Kriterium genannten Aspekte definiert und geregelt sind. Einsichtnahme in die technische Implementierung der Passwortparameter der Active Directory Policy. Einsichtnahme in eine Breitbandverpflichtung und Beurteilung, ob Mitarbeiter bestätigen, dass sie geteilte oder persönliche Authentisierungs-informationen (z.B. Kennwörter) vertraulich behandeln.	Keine Abweichung festgestellt.

IDM-09	Systemkomponenten im Verantwortungsbereich des Cloud-Anbieters, die für die Bereitstellung des Cloud-Dienstes verwendet werden, authentifizieren Benutzer der internen und externen Mitarbeiter des Cloud-Anbieters sowie der Systemkomponenten, die eine Rolle in automatisierten Autorisierungsprozessen des Cloud-Anbieters innehaben. Der Zugriff auf die Produktionsumgebung erfordert eine Zwei- oder Mehr-Faktor-Authentisierung. Innerhalb der Produktionsumgebung erfolgt die Authentifizierung der Benutzer durch Passwörter, digital signierte Zertifikate oder Verfahren, die ein mindestens gleichwertiges Sicherheitsniveau erreichen. Soweit digital signierte Zertifikate verwendet werden, erfolgt die Verwaltung gemäß der Richtlinie zur Schlüsselverwaltung (vgl. CRY-01). Die Passwort-Vorgaben sind aus einer Risikobewertung abgeleitet sowie in einer Richtlinie für Passwörter gemäß SP-01, dokumentiert, kommuniziert und bereitgestellt. Die Einhaltung der Vorgaben wird durch die Konfiguration der Systemkomponenten erzwungen, soweit dies technisch möglich ist. <u>Zusatzkriterium</u> Der Zugriff auf die nicht-Produktionsumgebung erfordert eine Zwei- oder Mehr-Faktor-Authentisierung. Innerhalb der nicht-Produktionsumgebung erfolgt die Authentifizierung der Benutzer durch Passwörter, digital signierte Zertifikate oder Verfahren, die ein mindestens gleichwertiges Sicherheitsniveau erreichen.	Auf Basis der Passwortrichtlinie und dem AWS-Betriebshandbuch wird eine Multi-Faktor-Authentifizierung für Produktions- und nicht-Produktionsumgebungen technisch verpflichtend umgesetzt und entsprechend für die Cloudumgebungen konfiguriert.	Einsichtnahme in das AWS-Betriebshandbuch und Beurteilung, ob die im Kriterium genannten Aspekte (z.B. Multi-Faktor-Authentifizierung) berücksichtigt sind. Systemeinsichtnahme einer Cloudumgebung und Beurteilung, ob eine Mehrfaktor-Authentifizierung eingerichtet ist und Systemadministratoren entsprechende Abfragen im Rahmen der Benutzeranmeldung erhalten.	Keine Abweichung festgestellt.
Die Kontrollen sind zutreffend dargestellt sowie angemessen eingerichtet, um das oben genannte Kontrollziel zu erreichen.				

7. KRYPTOGRAPHIE UND SCHLÜSSELMANAGEMENT (CRY)

Referenz BSI C5	Kriterium des BSI C5:2020	Arvato Systems Kontrollbeschreibung	Prüfungshandlung	Ergebnis
CRY: Sicherstellen eines angemessenen und wirksamen Gebrauchs von Kryptographie zum Schutz der Vertraulichkeit, Authentizität oder Integrität von Information.				
CRY-01	Richtlinien und Anweisungen mit technischen und organisatorischen Maßnahmen für Verschlüsselungsverfahren und Schlüsselverwaltung sind gemäß SP-01 dokumentiert, kommuniziert und bereitgestellt, in denen die folgenden Aspekte beschrieben sind: – die Nutzung starker Verschlüsselungsverfahren und die Verwendung sicherer Netzprotokolle, die dem Stand der Technik entsprechen, – risikobasierte Vorschriften für den Einsatz von Verschlüsselung, die mit Schemata zur Informationsklassifikation abgeglichen sind und den Kommunikationskanal sowie die Art, Stärke und Qualität der Verschlüsselung berücksichtigen, – Anforderungen für das sichere Erzeugen, Speichern, Archivieren, Abrufen, Verteilen, Entziehen und Löschen der Schlüssel, – Berücksichtigung der relevanten rechtlichen und regulatorischen Verpflichtungen und Anforderungen.	Die Nutzung von Verschlüsselungsverfahren wird in den Konzernsicherheitsrichtlinien sowie im AWS-Betriebshandbuch beschrieben bzw. vorgegeben. Etwaige weitere Anforderungen an die Verschlüsselung werden je nach Kundenvereinbarung bzw. regulatorischen Verpflichtungen im Rahmen des Aufbaus der Cloudumgebung berücksichtigt und dokumentiert.	Einsichtnahme in die Sicherheitsrichtlinien sowie das AWS-Betriebshandbuch und Beurteilung, ob die im Kriterium genannten Aspekte zur Verschlüsselung dokumentiert sind und den Mitarbeiter zur Verfügung stehen.	Keine Abweichung festgestellt.
CRY-02	Der Cloud-Anbieter hat für das Übertragen von Daten der Cloud-Kunden über öffentliche Netze Verfahren und technische Maßnahmen zur starken Verschlüsselung und Authentifizierung etabliert. <u>Zusatzkriterium</u> Der Cloud-Anbieter hat für das Übertragen aller Daten Verfahren und technische Maßnahmen zur starken Verschlüsselung und Authentifizierung etabliert.	Datenübertragungen über öffentliche Netze sind auf Basis der Konfiguration im Standard (Orientierung am Cloud Adoption Framework und dem Avvia Betriebshandbuch) TLS-verschlüsselt.	Einsichtnahme in das AWS-Betriebshandbuch und Beurteilung, ob für die Datenübertragung eine starke Verschlüsselung sowie Authentifizierung geregelt sind. Systemeinsichtnahme in eine Kundenumgebung und Beurteilung, ob eine TLS-Verschlüsselung konfiguriert ist.	Keine Abweichung festgestellt.

CRY-03	Der Cloud-Anbieter hat Verfahren und technische Maßnahmen zur Verschlüsselung von Daten der Cloud-Kunden bei der Speicherung etabliert. Die für die Verschlüsselung verwendeten privaten Schlüssel sind ausschließlich dem Cloud-Kunden nach geltenden rechtlichen und regulatorischen Verpflichtungen und Anforderungen bekannt. Ausnahmen folgen einem geregelten Verfahren. Die Verfahren zur Verwendung privater Schlüssel, inklusive gegebenenfalls bestehender Ausnahmen, sind mit dem Cloud-Kunden vertraglich zu vereinbaren. Zusatzkriterium Die für die Verschlüsselung verwendeten privaten Schlüssel sind ausschließlich und ohne Ausnahme dem Kunden nach geltenden rechtlichen und regulatorischen Verpflichtungen und Anforderungen bekannt.	Die Nutzung von customer-managed keys zur Verschlüsselung von Kundendaten wird individuell vereinbart und vertraglich festgehalten sowie dokumentiert. Es ist ein organisatorisches Verfahren etabliert, das die notwendigen Schritte und Abstimmungen mit dem Kunden vorgibt, um die Cloudumgebung mittels eines privaten Schlüssels zu verschlüsseln (ohne, dass Arvato Systems in Besitz des Schlüssels kommt).	Befragung von Systemadministratoren hinsichtlich des Vorgehens zur Verschlüsselung mittels customer-managed-keys und den dazugehörigen Schritten. Einsichtnahme in vertragliche Vereinbarungen und Kommunikationen zwischen Arvato Systems und Cloudkunden hinsichtlich der Nutzung von customer-managed-keys und Beurteilung, ob ein Verfahren besteht, das sicherstellt, dass der private Schlüssel zur Datenverschlüsselung nur dem Cloudkunden bekannt ist. Einsichtnahme in Systemkonfiguration hinsichtlich aktivierter Verschlüsselung.	Keine Abweichung festgestellt.

CRY-04	Die Verfahren und technische Maßnahmen zur sicheren Verwaltung von Schlüsseln im Verantwortungsbereich des Cloud-Anbieters beinhalten mindestens die folgenden Aspekte: – Schlüsselgenerierung für unterschiedliche kryptographische Systeme und Applikationen, – Ausstellung und Einholung von Public-Key-Zertifikaten, – Provisionierung und Aktivierung von Schlüsseln, – Sicheres Speichern von Schlüsseln (Separierung des Key-Management-Systems von Anwendungs- und Middleware Ebene), einschließlich der Beschreibung wie autorisierte Nutzer den Zugriff erhalten, – Ändern oder Aktualisieren von kryptographischen Schlüsseln einschließlich Richtlinien, die festlegen, unter welchen Bedingungen und auf welche Weise die Änderungen bzw. Aktualisierungen zu realisieren sind, – Umgang mit kompromittierten Schlüsseln, – Entzug und Löschen von Schlüsseln, – Falls pre-shared keys verwendet werden, sind die Besonderheiten in Bezug auf sichere Nutzung dieses Verfahrens gesondert aufgeführt.	Nicht anwendbar – im Verantwortungsbereich von AWS.
Die Kontrollen sind zutreffend dargestellt sowie angemessen eingerichtet, um das oben genannte Kontrollziel zu erreichen.		

8. STEUERUNG UND ÜBERWACHUNG VON DIENSTLEISTERN UND LIEFERANTEN (SSO)

Referenz BSI C5	Kriterium des BSI C5:2020	Arvato Systems Kontrollbeschreibung	Prüfungshandlung	Ergebnis
SSO: Sicherstellen des Schutzes von Informationen auf die Dienstleister bzw. Lieferanten des Cloud-Anbieters (Unterauftragnehmer) zugreifen können, sowie Überwachung der vereinbarten Leistungen und Sicherheitsanforderungen.				
SSO-01	Richtlinien und Anweisungen zur Steuerung und Überwachung Dritter (z. B. Dienstleister bzw. Lieferanten), deren Leistungen zur Bereitstellung des Cloud-Dienstes beitragen, sind hinsichtlich der folgenden Aspekte gemäß SP-01 dokumentiert, kommuniziert und bereitgestellt: – Vorgaben für die Beurteilung der Risiken, die aus dem Bezug von Leistungen Dritter resultieren, – Vorgaben für die Klassifizierung der Dritten auf Basis einer Risikobeurteilung durch den Cloud-Anbieter und der Feststellung, ob es sich um ein Subdienstleistungsunternehmen handelt (vgl. Ergänzende Information), – Anforderungen an die Informationssicherheit bei der	Über einen definierten Supplier Management Prozess werden Dienstleister und Lieferanten sowie deren Leistungen überwacht. Der dokumentierte Prozess sieht dabei u.a. eine jährliche Risikobeurteilung und Klassifizierung auf Basis von Audits und/oder Prüfberichten vor. Subdienstleistungsunternehmen des Cloud-Anbieters werden vertraglich dazu verpflichtet, regelmäßige Berichterstattungen unabhängiger Dritter über die Angemessenheit und Wirksamkeit ihres dienstleistungsbezogenen	Einsichtnahme in die Prozessbeschreibung zum Lieferantenmanagement („Playbook“) und Beurteilung, ob die im Kriterium genannten Aspekte (z.B. Klassifizierung von Lieferanten) geregelt und dokumentiert sind.	Keine Abweichung festgestellt.

	Verarbeitung, Speicherung oder Übertragung von Informationen durch Dritte, die sich an anerkannten Branchenstandards orientieren, – Anforderungen an die Sensibilisierung und Schulung des Personals für Informationssicherheit, – anwendbare rechtliche und regulatorische Anforderungen, – Anforderungen an den Umgang mit Schwachstellen, Sicherheitsvorfällen und Störungen, – Vorgaben für die vertragliche Vereinbarung dieser Anforderungen, – Vorgaben für die Überwachung dieser Anforderungen, – Vorgaben für die Weitergabe dieser Anforderungen auch an Dienstleister, die von den Dritten eingesetzt werden, soweit Leistungen dieser Dienstleister ebenso zur Bereitstellung des Cloud-Dienstes beitragen. <u>Zusatzkriterium</u> Subdienstleistungsunternehmen des Cloud-Anbieters werden vertraglich dazu verpflichtet, regelmäßige Berichterstattungen unabhängiger Dritter über die Angemessenheit und Wirksamkeit ihres dienstleistungsbezogenen internen Kontrollsystems vorzulegen. Die Berichterstattungen umfassen die korrespondierenden Kontrollen beim Subdienstleister, die erforderlich sind, um zusammen mit den Kontrollen des Cloud-Anbieters, die anwendbaren Basiskriterien des BSI C5 mit hinreichender Sicherheit zu erfüllen. Soweit keine Berichterstattungen vorgelegt werden können, vereinbart der Cloud-Anbieter entsprechende Informations- und Prüfungsrechte, um die Angemessenheit und Wirksamkeit des dienstleistungsbezogenen internen Kontrollsystems einschließlich der korrespondierenden Kontrollen durch qualifiziertes Personal zu beurteilen.	internen Kontrollsystems vorzulegen.	Befragung von Mitarbeitern des Einkaufs und Einsichtnahme in das Lieferantenmanagement-Portal, ob in Verträgen mit Subdienstleistern eine Berichterstattung durch Dritte oder Informations- und Prüfrechte vereinbart sind.	

SSO-02	Dienstleister und Lieferanten des Cloud-Anbieters werden einer Risikobeurteilung gemäß den Richtlinien und Anweisungen zur Steuerung und Überwachung Dritter unterzogen, bevor sie zur Bereitstellung des Cloud-Dienstes beitragen. Die Angemessenheit der Risikobeurteilung wird während des Leitungsbezugs regelmäßig, mindestens jährlich, durch qualifiziertes Personal des Cloud-Anbieters überprüft. Die Risikobeurteilung umfasst die Identifikation, Analyse, Bewertung, Behandlung und Dokumentation von Risiken hinsichtlich der folgenden Aspekte: – Schutzbedarf der Informationen hinsichtlich der Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität, die durch den Dritten verarbeitet, gespeichert oder übertragen werden, – Auswirkungen einer Schutzbedarfsverletzung auf die Bereitstellung des Cloud-Dienstes, – Abhängigkeit des Cloud-Anbieters vom Dienstleister oder Lieferanten hinsichtlich Umfang, Komplexität und Einzigartigkeit der bezogenen Leistung, einschließlich der Betrachtung möglicher Alternativen.	Es findet ein jährliches Risk-Assessment der genutzten Dienstleister und Lieferanten hinsichtlich Sicherheitsrisiken statt. Die Risikobeurteilung für Hyperscaler übernimmt das Konzern-Risikomanagement, das die Ergebnisse dokumentiert und den Konzerntöchtern bereitstellt bzw. diese an sie kommuniziert. Teil des Risk-Assessments ist z.B. die Identifizierung von möglichen Schutzbedarfsverletzungen und deren Auswirkungen sowie Behandlungen.	Befragung von Mitarbeitern des Einkaufs hinsichtlich der regelmäßigen Risikobeurteilung von Lieferanten und deren Dokumentation Einsichtnahme in eine dokumentierte Risikobeurteilung und Beurteilung, ob Risiken bewertet und ggf. daraus resultierende Maßnahmen festgehalten wurden.	Keine Abweichung festgestellt.

SSO-03	Der Cloud-Anbieter registriert Dienstleister und Lieferanten, die Leistungen zur Bereitstellung des Cloud-Dienstes beitragen. Folgende Informationen sind nachzuhalten: – Firmenname – Anschrift – Lokationen der Verarbeitung und Speicherung von Daten – Verantwortlicher Ansprechpartner beim Dienstleister/Lieferanten – Verantwortlicher Ansprechpartner beim Cloud-Anbieter – Beschreibung der Leistung – Klassifizierung auf Basis der Risikobeurteilung – Beginn des Leistungsbezugs – Nachweise über die Einhaltung der vertraglich vereinbarten Anforderungen. Die Angaben im Verzeichnis werden mindestens jährlich auf Vollständigkeit, Richtigkeit und Gültigkeit überprüft.	Innerhalb eines Vertragsregisters sowie einem Lieferantenmanagement-Tools werden Information von Dienstleistern und Lieferanten (u.a. Firmennamen, Ansprechpartner, Leistungsbeschreibungen) zentral festgehalten und dokumentiert.	Einsichtnahme in das Lieferantenmanagement-Tool und Beurteilung, ob Informationen (gemäß der im Kriterium genannten Aspekte) über Dienstleister und Lieferanten dokumentiert werden.	Keine Abweichung festgestellt.
SSO-04	Der Cloud-Anbieter überwacht die Einhaltung der Anforderungen an die Informationssicherheit sowie der anwendbaren rechtlichen und regulatorischen Anforderungen gemäß den Richtlinien und Anweisungen zur Steuerung und Überwachung Dritter. Die Überwachung umfasst eine regelmäßige Durchsicht der folgenden Nachweise, soweit diese von den Dritten gemäß den vertraglichen Vereinbarungen zur Verfügung zu stellen sind: – Berichte über die Qualität der Leistungserbringung, – Zertifikate über die Konformität der Managementsysteme mit internationalen Standards,	Im Rahmen des Supplier Managements werden jährlich Informationen zur Informationssicherheit der genutzten Dienstleister und Lieferanten eingeholt. Hierzu zählen z.B. Zertifikate, Bescheinigungen oder Prüfberichte. Sofern keine Nachweise in dieser Form seitens der Dienstleister und Lieferanten bereitgestellt werden, findet ein Audit seitens Arvato Systems statt, um die Einhaltung der Anforderungen zur Informationssicherheit bewerten zu können.	Befragung von Mitarbeitern des Einkaufs hinsichtlich der Überwachung von Lieferanten und Dienstleister (z.B. Einsichtnahme in Prüfberichte).	Keine Abweichung festgestellt.

	– Berichterstattungen unabhängiger Dritter über die Angemessenheit und Wirksamkeit ihres dienstleistungsbezogenen internen Kontrollsystems, – Aufzeichnungen zum Umgang der Dritten mit Schwachstellen, Sicherheitsvorfällen und Störungen. Die Regelmäßigkeit der Durchführung entspricht der Klassifizierung der Dritten auf Basis der Risikobeurteilung des Cloud-Anbieters (vgl. SSO-02). Die Ergebnisse der Überwachung fließen in die Überprüfung der Risikobeurteilung ein. Identifizierte Verstöße und Abweichungen werden gemäß dem Verfahren zum Umgang mit Risiken (vgl. OIS-07) einer Analyse, Bewertung und Behandlung unterzogen. <u>Zusatzkriterium</u> Die Verfahren zur Überwachung der Einhaltung der Anforderungen werden durch automatische Verfahren hinsichtlich der folgenden Aspekte ergänzt: • Konfiguration von Systemkomponenten • Leistung und Verfügbarkeit von Systemkomponenten • Reaktionszeit bei Störungen und Sicherheitsvorfällen • Wiederherstellungszeit (Zeitraum bis zum Abschluss der Störungsbeseitigung). Identifizierte Verstöße und Abweichungen werden automatisch an das dafür zuständigen Personal oder die dafür zuständigen Systemkomponenten des Cloud-Anbieters berichtet, um diese umgehend einer Beurteilung zu unterziehen und erforderliche Maßnahmen einzuleiten.	Die Überwachung der Einhaltung von Anforderungen an die Systemkonfiguration, Qualität der Leistungserbringung und an Reaktionszeiten erfolgt in Echtzeit durch das eingesetzte Monitoring System.	Einsichtnahme in das Lieferantenmanagement-Tool und Beurteilung, ob für Lieferanten regelmäßig Nachweise (z.B. Prüfberichte oder Zertifikate zur Informationssicherheit) angefordert, eingesehen und dokumentiert werden. Einsichtnahme in das Monitoring der Systeme und Beurteilung, ob Systemkomponenten hinsichtlich Konfiguration, Leistung- und Verfügbarkeiten, Reaktionszeiten und Wiederherstellungszeiten überwacht werden.	

SSO-05	Der Cloud-Anbieter hat Ausstiegsstrategien für den Bezug von Leistungen definiert und dokumentiert, bei denen die Risikobeurteilung der Dienstleister und Lieferanten hinsichtlich Umfang, Komplexität und Einzigartigkeit der bezogenen Leistung, eine sehr hohe Abhängigkeit ergab (vgl. ergänzende Informationen). Die Ausstiegsstrategien sind mit den Plänen zur betrieblichen Kontinuität abgestimmt und umfassen die folgenden Aspekte: – Analyse der potenziellen Kosten, Auswirkungen, Ressourcen und zeitlichen Auswirkungen des Übergangs einer bezogenen Leistung auf einen alternativen Dienstleister oder Lieferanten, – Definition und Zuweisung von Rollen, Verantwortlichkeiten und ausreichenden Ressourcen zur Durchführung der Aktivitäten für einen Übergang, – Definition von Erfolgskriterien für den Übergang, – Definition von Indikatoren für die Überwachung der Leistungserbringung, die bei inakzeptablen Ergebnissen den Ausstieg für den Bezug der Leistung einleiten sollten.	Im Rahmen der jährlichen Risikobeurteilung werden Ausstiegsstrategien von Dienstleistern und Lieferanten evaluiert und - sofern bei Monopolstellungen marktseitig möglich – definiert.	Befragung von Mitarbeitern des Einkaufs hinsichtlich definierter Ausstiegs-strategien im Rahmen der jährlichen Risikobeurteilung. Einsichtnahme in eine dokumentierte Ausstiegsstrategie und Beurteilung, ob die im Kriterium genannten Aspekte geregelt sind.	Keine Abweichung festgestellt.
Die Kontrollen sind zutreffend dargestellt sowie angemessen eingerichtet, um das oben genannte Kontrollziel zu erreichen.				

9. UMGANG MIT SICHERHEITSVORFÄLLEN (SIM)

Referenz BSI C5	Kriterium des BSI C5:2020	Arvato Systems Kontrollbeschreibung	Prüfungshandlung	Ergebnis
SIM: Gewährleisten eines konsistenten und umfassenden Vorgehens zur Erfassung, Bewertung, Kommunikation und Behandlung von Sicherheitsvorfällen.				
SIM-01	Richtlinien und Anweisungen mit technischen und organisatorischen Maßnahmen sind gemäß SP-01 dokumentiert, kommuniziert und bereitgestellt, um eine schnelle, effektive und ordnungsgemäße Reaktion auf alle bekannten Sicherheitsvorfälle zu gewährleisten. Der Cloud-Anbieter definiert Vorgaben zur Klassifizierung, Priorisierung und Eskalation von Sicherheitsvorfällen und schafft Schnittstellen zum Incident Management und zum Business Continuity Management. Zusätzlich hat der Cloud-Anbieter ein "Computer Emergency Response Team" (CERT) eingerichtet, das zur koordinierten Lösung von konkreten Sicherheitsvorfällen beiträgt. Von Sicherheitsvorfällen betroffene Kunden werden zeitnah und in angemessener Form darüber informiert. <u>Zusatzkriterium</u> Es gibt Anweisungen, wie bei einem Sicherheitsvorfall die Daten eines verdächtigen Systems beweisfest gesammelt werden können. Weiterhin existieren Analysepläne für typische Sicherheitsvorfälle sowie eine Auswertemethodik, so dass die gesammelten Informationen in einer eventuell späteren juristischen Würdigung ihre Beweiskraft nicht verlieren.	Es ist eine Security Incident Management Richtlinie definiert, dokumentiert und an die zuständigen IT-Mitarbeiter kommuniziert. In der Richtlinie sind Aufgabenbeschreibungen, Organisationstrukturen, Meldewege und Verfahren beschrieben, wie Sicherheitsvorfälle koordiniert behandelt, kommuniziert und dokumentiert werden sollen.	Einsichtnahme in die Richtlinie zum Security Incident Management und Beurteilung, ob die im Kriterium genannten Aspekte (z.B. Klassifizierung und Eskalationswege) definiert und geregelt sind sowie ein CERT bestimmt ist. Befragung von Security Managern hinsichtlich der Vorgehensweise zur Analyse und Auswertung von Sicherheitsvorfällen auf Basis von gesammelten Daten.	Keine Abweichung festgestellt.

SIM-02	Qualifiziertes Personal des Cloud-Anbieters führt, gegebenenfalls gemeinsam mit externen Sicherheitsdienstleistern, für Ereignisse die einen Sicherheitsvorfall darstellen könnten, Klassifizierungen, Priorisierungen sowie Ursachenanalysen durch. Zusatzkriterium Der Cloud-Anbieter simuliert das Identifizieren, Analysieren und Abwehren von Sicherheitsvorfällen und Angriffen mindestens jährlich durch geeignete Tests und Übungen (z. B. Red Team-Übungen).	Die Bearbeitung von potentiellen Sicherheitsvorfällen folgt den beschriebenen Verfahren der Security Incident Management Richtlinie. Hierzu zählt z.B. die Klassifizierung und Priorisierung des Vorfalls sowie die Ursachenanalyse durch das Security Operations Center (mit Unterstützung der zuständigen IT-Administratoren). Es wird mindestens jährlich das Vorgehen und die Bearbeitung von Sicherheitsvorfällen mittels geeigneter Tests (z.B. Planspiele) geübt.	Einsichtnahme eines dokumentierten Sicherheitsvorfalls hinsichtlich Klassifizierung, Priorisierung und Ursachenanalyse. Einsichtnahme in einen dokumentierten Sicherheitsvorfalltest und Beurteilung, ob das Vorgehen zur Behandlung von Sicherheitsvorfällen mindestens jährlich geübt wird.	Keine Abweichung festgestellt.
SIM-03	Nach Verarbeitung eines Sicherheitsvorfalls wird die Lösung gemäß den vertraglichen Vereinbarungen dokumentiert und der Bericht zur abschließenden Kenntnisnahme oder ggf. als Bestätigung an betroffene Kunden übermittelt. Zusatzkriterium Der Kunde kann Lösungen entweder aktiv zustimmen oder der Lösung wird nach Ablauf eines bestimmten Zeitraumes automatisch zugestimmt. Informationen zu Sicherheitsvorfällen oder bestätigten Sicherheitsverstößen werden allen betroffenen Kunden zur Verfügung gestellt. Zwischen Cloud-Anbieter und Cloud-Kunden ist vertraglich geregelt, welche Daten dem Cloud-Kunden bei Sicherheitsvorfällen zur eigenen Analyse zur Verfügung gestellt werden.	Auf Basis der vertraglichen Vereinbarung wird nach Behandlung eines Sicherheitsvorfalls ein dazugehöriger Incident Report (root cause analysis) seitens Arvato Systems erstellt und die Ergebnisse an die betroffenen Kunden kommuniziert.	Einsichtnahme in die Security Incident Richtlinie und Beurteilung, ob Vorgaben zur Dokumentation und Berichterstattung (an Kunden) von Sicherheits-vorfällen definiert sind. Einsichtnahme in einen Sicherheitsvorfall und zugehörigem Incident Report und Beurteilung, ob die Ergebnisse dokumentiert und wie vertraglich vereinbart an den Kunden kommuniziert werden.	Keine Abweichung festgestellt.

SIM-04	Der Cloud-Anbieter informiert Mitarbeiter und externe Geschäftspartner über ihre Verpflichtungen. Falls erforderlich willigen sie dazu ein oder verpflichten sich vertraglich dazu, alle Sicherheitsereignisse, die ihnen bekannt werden und direkt mit dem vom Cloud-Anbieter bereitgestellten Cloud-Dienst in Verbindung stehen, zeitnah an eine zuvor benannte zentrale Stelle des Cloud-Anbieters zu melden. Der Cloud-Anbieter kommuniziert, dass "Falschmeldungen" von Ereignissen, die sich im Nachhinein nicht als Vorfälle herausstellen, keine negativen Folgen nach sich ziehen.	Mitarbeiter und Externe werden im Rahmen von Informationssicherheitsschulungen sowie durch vertragliche Vereinbarungen dazu aufgefordert, identifizierte Sicherheitsvorfälle zeitnah an das Incident Management Team oder dem Service Desk zu melden, damit der jeweilige Vorfall aufgenommen und bearbeitet werden kann.	Einsichtnahme in Sensibilisierungsmaßnahmen hinsichtlich der Verpflichtung von Mitarbeitern und Geschäftspartnern zur zeitnahen Meldung von Sicherheitsereignissen. Einsichtnahme in vertraglich festgelegte Klauseln zur Meldung von Sicherheitsereignissen sowie in identifizierte Sicherheitsvorfälle und zugehörigen Incident Reports.	Keine Abweichung festgestellt.
SIM-05	Mechanismen sind vorhanden, um Art und Umfang der Sicherheitsvorfälle messen und überwachen sowie an unterstützende Stellen melden zu können. Die aus der Auswertung gewonnenen Informationen werden dazu verwendet, wiederkehrende oder mit erheblichen Folgen verbundene Vorfälle zu identifizieren und Notwendigkeiten für erweiterte Schutzmaßnahmen festzustellen.	Sicherheitsvorfälle werden nach Identifizierung fortlaufend durch die zuständigen Mitarbeiter des Incident Managements oder des CERT-Teams überwacht und ausgewertet. Sich daraus ergebene Maßnahmen werden dem internen Change bzw. Patch Management zugeführt und umgesetzt.	Befragung von Security Managern hinsichtlich der Überwachungsmaßnahmen und weiteren Bearbeitung von Sicherheitsvorfällen (inkl. Ableitung und Durchführung von erweiterten Schutzmaßnahmen). Einsichtnahme in Auswertungen sowie „Lessons Learned“ und daraus abgeleitete Maßnahmenpläne für zukünftig wiederkehrende Vorfälle.	Keine Abweichung festgestellt.
Die Kontrollen sind zutreffend dargestellt sowie angemessen eingerichtet, um das oben genannte Kontrollziel zu erreichen.				

10. KONTINUITÄT DES GESCHÄFTSBETRIEBS UND NOTFALLMANAGEMENT (BCM)

Referenz BSI C5	Kriterium des BSI C5:2020	Arvato Systems Kontrollbeschreibung	Prüfungshandlung	Ergebnis
BCM: Planen, Implementieren, Aufrechterhalten und Testen von Verfahren und Maßnahmen zur Kontinuität des Geschäftsbetriebs und für das Notfallmanagement.				
BCM-01	Die oberste Leitung des Cloud-Anbieters ist als Prozesseigentümer des Kontinuitäts- und Notfallmanagements benannt und trägt die Verantwortung für die Etablierung des Prozesses im Unternehmen und die Einhaltung der Leitlinien. Sie muss dafür sorgen, dass ausreichende Ressourcen für einen effektiven Prozess bereitgestellt werden. Personen in der Unternehmensleitung und anderen relevanten Führungspositionen demonstrieren Führung und Engagement in Bezug auf dieses Thema, indem sie beispielsweise die Mitarbeiter dazu auffordern beziehungsweise ermutigen, zu der Effektivität des Kontinuitäts- und Notfallmanagements aktiv beizutragen.	Die Geschäftsführung von Arvato Systems hat ein Business Continuity Management (BCM) System sowie eine dazugehörige BCM-Organisation eingerichtet. Das BCM-System wird regelmäßig nach der Norm ISO 22301:2019 auditiert und zertifiziert.	Einsichtnahme in die BCM-Richtlinie im Hinblick auf die Verantwortlichkeit und die Grundhaltung der Unternehmensleitung sowie die Bereitstellung von Ressourcen. Einsichtnahme in das ISO 22301 Zertifikat und dessen Gültigkeit. Einsichtnahme in die Kommunikation der Unternehmensleitung zum Thema BCM.	Keine Abweichung festgestellt.

BCM-02	Richtlinien und Anweisungen zum Ermitteln von Auswirkungen etwaiger Störungen des Cloud-Dienstes oder des Unternehmens sind gemäß SP-01 dokumentiert, kommuniziert und bereitgestellt. Mindestens die folgenden Aspekte werden dabei berücksichtigt: – mögliche Szenarien basierend auf einer Risikoanalyse, – Identifizierung kritischer Produkte und Dienstleistungen, – Identifizierung von Abhängigkeiten, einschließlich der Prozesse (inkl. dafür benötigter Ressourcen), Anwendungen, Geschäftspartner und Dritter, – Erfassung von Bedrohungen gegenüber kritischen Produkten und Dienstleistungen, – Ermittlung von Auswirkungen resultierend aus geplanten und ungeplanten Störungen und die Veränderung im Laufe der Zeit, – Feststellung der maximal vertretbaren Dauer von Störungen, – Feststellung der Prioritäten zur Wiederherstellung, – Feststellung zeitlicher Zielvorgaben zur Wiederaufnahme kritischer Produkte und Dienstleistungen innerhalb des maximal vertretbaren Zeitraums (RTO), – Feststellung zeitlicher Vorgaben zum maximal vertretbaren Zeitraum, in dem Daten verloren und nicht wiederhergestellt werden können (RPO), – Abschätzung der zur Wiederaufnahme benötigten Ressourcen.	Auf Basis der BCM-Richtlinie und den individuellen Kundenvereinbarungen wird regelmäßig eine Business-Impact-Analyse durchgeführt und dokumentiert. Die übergreifende Analyse beinhaltet u.a. eingerichtete Verfahren – zu möglichen Risikoszenarien – zur Identifizierung kritischer Produkte und Dienste sowie Abhängigkeiten zu Prozessen, Anwendungen, Geschäftspartner und Dritten – zur Erfassung von Bedrohungen gegenüber kritischen Produkten und Dienstleistungen – zur Ermittlung von Auswirkungen von geplanten oder ungeplanten Störungen mit Berücksichtigung von Veränderungen im Zeitverlauf – zur Feststellung der maximal vertretbaren Störungsdauer – zur Feststellung von Wiederherstellungsprioritäten und verbundenen Zeitvorgaben zur Wiederaufnahme kritischer Produkte und Dienstleistungen innerhalb des maximal vertretbaren Zeitraums (RTO), – Feststellung zeitlicher Vorgaben zum maximal vertretbaren Zeitraum, in dem Daten verloren und nicht wiederhergestellt werden können (RPO), – Zur Abschätzung der zur Wiederaufnahme benötigten Ressourcen. Der dafür vorgesehene Analyseprozess ist intern definiert und etabliert.	Befragung des BCM-Managers und Einsichtnahme in die BCM-Richtlinie und Kundenvereinbarungen hinsichtlich Aktualität und Vollständigkeit der Inhalte betreffend der im Kriterium genannten Aspekte. Einsichtnahme in eine dokumentierte Business-Impact-Analyse und in die zugehörigen implementierten Verfahren mit Beurteilung, ob die im Kriterium genannten Aspekte eingerichtet, festgehalten und bestimmt wurden.	Keine Abweichung festgestellt.

BCM-03	Basierend auf der Business Impact Analyse wird ein einheitliches Rahmenwerk zur Planung der betrieblichen Kontinuität und des Geschäftsplans eingeführt, dokumentiert und angewendet, um sicherzustellen, dass alle Pläne konsistent sind. Die Planung richtet sich nach etablierten Standards, was in einem "Statement of Applicability" nachvollziehbar festgeschrieben ist. Pläne zur betrieblichen Kontinuität und Notfallpläne berücksichtigen dabei folgende Aspekte: – Definierter Zweck und Umfang unter Beachtung der relevanten Abhängigkeiten, – Zugänglichkeit und Verständlichkeit der Pläne für Personen, die danach handeln sollen, – Eigentümerschaft durch mindestens eine benannte Person, die für die Überprüfung, Aktualisierung und Genehmigung zuständig ist, – Festgelegte Kommunikationswege, Rollen und Verantwortlichkeiten einschließlich Benachrichtigung des Kunden, – Wiederherstellungsverfahren, manuelle Übergangslösungen und Referenzinformationen (unter Berücksichtigung der Priorisierung bei der Wiederherstellung von Cloud-Infrastruktur Komponenten und Diensten sowie Ausrichtung an Kunden), – Methoden zur Inkraftsetzung der Pläne, – Kontinuierlicher Verbesserungsprozess der Pläne, – Schnittstellen zum Security Incident Management.	Im Rahmen des Aufbaus von Cloudumgebungen werden in Abstimmung mit dem Kunden Systeme und Applikationen so eingerichtet, dass sie die Anforderungen zur Geschäftsfortführung (z.B. Systembetrieb oder Datensicherungsverfahren in mehreren Regionen) des jeweiligen Kunden erfüllen. Pläne zur betrieblichen Kontinuität und Notfallpläne berücksichtigen dabei – die Definition von Zweck und Umfang unter Beachtung der relevanten Abhängigkeiten – die Festlegung von Rollen und Verantwortlichkeiten sowie Zugänglichkeit und Verständlichkeit der Pläne für beteiligte Mitarbeiter – die Bestimmung von Verantwortlichkeiten für die Überprüfung, Aktualisierung und Genehmigung – die Einrichtung von Kommunikationswegen einschließlich der Kundenbenachrichtigung – Wiederherstellungsverfahren, Übergangslösungen und Referenzinformationen – Verfahren zur Inkraftsetzung der Pläne – kontinuierlicher Verbesserungsprozess der Pläne – Schnittstellen zum Security Incident Management.	Einsichtnahme in das Cloud Adoption Framework und Abstimmungskommunikationen mit Kunden hinsichtlich eines einheitlichen Rahmenwerks zum Aufbau von Cloudumgebungen mit dem Ziel der betrieblichen Kontinuität. Einsichtnahme in Pläne zur betrieblichen Kontinuität und in Notfallpläne hinsichtlich Aktualität, Konsistenz und Vollständigkeit der Inhalte betreffend die im Kriterium genannten Aspekte. Einsichtnahme in die Pläne zum BCM mit Prüfung auf Konsistenz mit den Ergebnissen der Business Impact Analyse.	Keine Abweichung festgestellt.

BCM-04	Die Business Impact Analyse sowie die Pläne zur betrieblichen Kontinuität und Notfallpläne werden regelmäßig (mindestens jährlich) oder nach wesentlichen organisatorischen oder umgebungsbedingten Veränderungen überprüft, aktualisiert und getestet. Tests beziehen betroffene Kunden (Tenants) und relevante Dritte mit ein. Die Tests werden dokumentiert und Ergebnisse werden für zukünftige Maßnahmen der betrieblichen Kontinuität berücksichtigt. Zusatzkriterium Zusätzlich zu den Tests werden auch Übungen durchgeführt, die u.a. Szenarien aus in der Vergangenheit bereits aufgetretenen Sicherheitsvorfällen hervorgegangen sind.	Es finden jährliche BCM-Tests statt, die die Wirksamkeit von Notfallplänen und Wiederherstellungsverfahren prüft (z.B. Übung bereits aufgetretener Vorfälle). Die Ergebnisse der Tests sind Grundlage für notwendige Anpassungen an den bisher definierten Plänen und Verfahren und werden dokumentiert.	Einsichtnahme in die Vorgaben, ob die definierten Notfallpläne mindestens jährlich oder bei relevanten Umfeldänderungen überprüft und aktualisiert werden. Einsichtnahme in die Testvorbereitungen (ggf. unter Einbindung des Kunden) und die Dokumentation der Testverfahren sowie die Ergebnisse.	Hinweis: Arvato Systems führt jährlich verschiedene BCM-Tests durch. Zum Prüfungszeitpunkt beinhalteten diese BCM-Tests noch keine AWS-spezifischen Testhandlungen. Ein entsprechendes AWS-Testmuster wird bis Q1 2025 aufgebaut.
Die Kontrollen sind zutreffend dargestellt sowie angemessen eingerichtet, um das oben genannte Kontrollziel zu erreichen.				

11. COMPLIANCE (COM)

Referenz BSI C5	Kriterium des BSI C5:2020	Arvato Systems Kontrollbeschreibung	Prüfungshandlung	Ergebnis
COM: Vermeiden von Verstößen gegen gesetzliche, regulatorische, selbstauferlegte oder vertragliche Anforderungen zur Informationssicherheit und Überprüfen der Einhaltung.				
COM-01	Die für die Informationssicherheit des Cloud-Dienstes relevanten gesetzlichen, regulatorischen, selbstauferlegten und vertraglichen Anforderungen sowie die Verfahren des Cloud-Anbieters zur Einhaltung dieser Anforderungen sind ausdrücklich definiert und dokumentiert.	Für die Beurteilung von Compliance-Anforderungen (z.B. auf Basis von Gesetzen, Regularien oder Verträgen) und deren Einhaltung im Hinblick auf die Informationssicherheit des angebotenen Cloud-Service wird regelmäßig ein Assessment mit Kunden und Providern anhand von Compliance-Fragebögen durchgeführt und dokumentiert. Die Ergebnisse des Assessments bilden die Basis für den jeweiligen Cloud-Betrieb.	Befragung des Compliance-Managers hinsichtlich der Überprüfung und Einhaltung von Anforderungen zur Informationssicherheit (u.a. auf Basis von Assessments mit Kunden und Providern). Einsichtnahme in Vorgaben und Richtlinien, ob die für die Cloud-Dienste relevanten gesetzlichen, regulatorischen, selbstauferlegten und vertraglichen Anforderungen in Bezug auf die Informationssicherheit vollständig definiert und dokumentiert sind. Einsichtnahme in ein dokumentiertes Assessment sowie in einen Compliance-Fragebogen und Beurteilung, ob Compliance-Anforderungen ermittelt und geprüft werden.	Keine Abweichung festgestellt.

COM-02	Richtlinien und Anweisungen mit Vorgaben für die Planung und Durchführung von Audits sind gemäß SP-01 dokumentiert, kommuniziert und bereitgestellt und adressieren folgende Aspekte: – Beschränkung auf Lesezugriff für Systemkomponenten gemäß der vereinbarten Prüfungsplanung und wie es für die Durchführung der Aktivitäten notwendig ist, – Aktivitäten, die zu Störungen des Cloud-Dienstes oder Verstößen gegen vertragliche Anforderungen führen können, werden während der planmäßigen Wartungsfester oder außerhalb der Zeiten von Lastspitzen durchgeführt, – Protokollierung und Überwachung der Aktivitäten. <u>Zusatzkriterium</u> Der Cloud-Anbieter gewährt seinen Cloud-Kunden vertraglich zugesicherte Informations- und Prüfrechte.	Es existiert eine dokumentierte Audit-Richtlinie, die Vorgaben zur Planung und Durchführung von internen und externen Audits definiert. Die Inhalte und Prozessschritte der Richtlinie sind an die zuständigen Audit-Mitarbeiter kommuniziert.	Einsichtnahme in die Audit-Richtlinie und Beurteilung, ob Verfahrensanweisungen zur Planung und Durchführung von internen und externen Audits definiert und an die zuständigen Mitarbeiter kommuniziert sind. Einsichtnahme in einen Kundenvertrag hinsichtlich vertraglich zugesicherter Informations- und Prüfrechte.	Keine Abweichung festgestellt.
COM-03	Qualifiziertes Personal überprüft in regelmäßigen Abständen, mindestens jährlich, in internen Audits die Compliance des Informationssicherheits-managementsystems mit den relevanten und anwendbaren gesetzlichen, regulatorischen, selbstauferlegten oder vertraglichen Anforderungen (vgl. COM-01) sowie die Einhaltung der Richtlinien und Arbeitsanweisungen (vgl. SP-01) in dessen Geltungsbereich (vgl. OIS-01). Identifizierte Schwachstellen und Abweichungen werden gemäß dem Verfahren zum Umgang mit Risiken (vgl. OIS-06) einer Risikobeurteilung	Das ISMS von Arvato Systems wird auf Basis der Audit-Richtline einem jährlichen internen Audit unterzogenen. Gemäß eines PDCA-Zyklus werden anhand der Ergebnisse des Audits (z.B. identifizierte Schwachstellen) notwendige Maßnahmen abgeleitet und zur Umsetzung an die zuständigen Organisationsbereiche kommuniziert. Je Quartal erfolgen weitere ISMS Management Audits unter Einbindung der Geschäftsführung hinsichtlich Effektivität und	Einsichtnahme in die Planung von internen Audits und Beurteilung, ob die Compliance des Informationssicherheits-managementsystems mit den relevanten und anwendbaren Anforderungen sowie die Einhaltung mindestens jährlich überprüft wird (einschließlich der Dokumentation der identifizierten Abweichungen und der Ableitung von Maßnahmen, sofern notwendig).	Keine Abweichung festgestellt.

	unterzogen und Maßnahmen zur Behandlung definiert und nachverfolgt (vgl. OPS-18). Zusatzkriterium Interne Audits werden durch Verfahren zur automatischen Überwachung anwendbarer Vorgaben aus Richtlinien und Arbeitsanweisungen hinsichtlich der folgenden Aspekte ergänzt: • Konfiguration von Systemkomponenten zur Bereitstellung des Cloud-Dienstes im Verantwortungsbereich des Cloud-Anbieters, • Leistung und Verfügbarkeit dieser Systemkomponenten, • Reaktionszeit bei Störungen und Sicherheitsvorfällen, • Wiederherstellungszeit (Zeitraum bis zum Abschluss der Störungsbeseitigung). Identifizierte Schwachstellen und Abweichungen werden automatisch an das dafür zuständige Personal oder die dafür zuständigen Systemkomponenten des Cloud-Anbieters berichtet, um diese umgehend einer Beurteilung zu unterziehen und erforderliche Maßnahmen einzuleiten. Die Einhaltung ausgewählter vertraglicher Anforderungen kann durch die Cloud-Kunden in Echtzeit eingesehen werden.	Verbesserungspotenzial der ISMS Kontrollumgebung. Verfahren zur automatisierten Überwachung von Vorgaben aus Richtlinien und Arbeitsanweisungen zu Konfiguration, Leistung und Verfügbarkeit, Reaktionszeiten bei Störung und Sicherheitsvorfällen sowie Wiederherstellungszeiten sind eingerichtet. Die Einhaltung vertraglicher Anforderungen kann durch den Kunden im bereitgestellten Customer Service Reporting in Echtzeit und über Power BI-Reports eingesehen werden.	Einsichtnahme in die Dokumentation, dass die in internen Audits identifizierten Schwachstellen und Abweichungen gemäß der Richtlinie für den Umgang mit Risiken (vgl. OIS-06) bewertet und in einen Maßnahmenplan überführt wurden. Einsichtnahme in automatisierte Überwachungssysteme und Beurteilung, ob diese gemäß den Anforderungen des Zusatzkriteriums eingerichtet sind und deren Ergebnisse im Customer Service Reporting und in Form von Power Bi-Reports bereitgestellt werden.	
COM-04	Die oberste Leitung des Cloud-Anbieters wird in regelmäßigen Abständen über die Informationssicherheitsleistung im Anwendungsbereich des ISMS informiert, um dessen fortdauernde Eignung, Angemessenheit und Wirksamkeit sicherzustellen. Die Informationen fließen mindestens jährlich in die Managementbewertung des ISMS ein.	Die Ergebnisse von internen und externen Audits des Informationssicherheits-managementsystems werden mindestens jährlich an die Geschäftsleitung von Arvato Systems kommuniziert.	Einsichtnahme in das ISMS Management-Reporting und Beurteilung, ob die Geschäftsleitung mindestens jährlich über die Eignung, Angemessenheit und Wirksamkeit des ISMS informiert wird.	Keine Abweichung festgestellt.
Die Kontrollen sind zutreffend dargestellt sowie angemessen eingerichtet, um das oben genannte Kontrollziel zu erreichen.				

12. UMGANG MIT ERMITTLUNGSFRAGEN STAATLICHER STELLEN (INQ)

Referenz BSI C5	Kriterium des BSI C5:2020	Arvato Systems Kontrollbeschreibung	Prüfungshandlung	Ergebnis
INQ: Gewährleisten eines angemessenen Umgangs mit Ermittlungsanfragen staatlicher Stellen hinsichtlich juristischer Überprüfung, Information der Cloud-Kunden und Begrenzung des Zugriffs auf oder der Offenlegung von Daten.				
INQ-01	Ermittlungsanfragen staatlicher Stellen werden einer juristischen Beurteilung durch qualifiziertes Personal des Cloud-Anbieters unterzogen. Im Rahmen der Beurteilung wird festgestellt, ob sich die staatliche Stelle auf eine anwendbare sowie rechtsgültige Rechtsgrundlage stützt und welche weiteren Schritte einzuleiten sind.	Ermittlungsanfragen staatlicher Stellen werden der juristischen Beurteilung durch die Rechtsabteilung von Arvato Systems unterzogen. Die Arvato Systems berät zu den notwendigen Folgeschritten.	Befragung des Legal-Manager hinsichtlich staatlich durchgeführter Ermittlungsanfragen. Befragung des Legal-Manager hinsichtlich des Umgangs und der Behandlung von Ermittlungsanfragen staatlicher Behörden. Einsichtnahme in Richtlinie zum Umgang mit Ermittlungsanfragen staatlicher Stellen, ob diese durch qualifiziertes Personal des Cloud-Anbieters juristisch beurteilt werden.	Keine Abweichung festgestellt. Hinweis: Auf Basis unserer Befragung lagen zum Prüfungszeitpunkt keine konkreten Fälle von staatlichen Ermittlungsanfragen vor.
INQ-02	Der Cloud-Anbieter informiert den oder die betroffenen Cloud-Kunden nach Eingang einer Ermittlungsanfrage einer staatlichen Stelle unverzüglich, soweit die anwendbare Rechtsgrundlage, auf die sich die staatliche Stelle stützt, dies nicht untersagt oder eindeutige Hinweise auf rechtswidrige Handlungen im Zusammenhang mit der Nutzung des Cloud-Dienstes vorliegen.	Arvato Systems informiert den oder die betroffenen Cloud-Kunden nach Eingang einer Ermittlungsanfrage einer staatlichen Stelle unverzüglich, soweit die anwendbare Rechtsgrundlage, auf die sich die staatliche Stelle stützt, dies nicht untersagt oder eindeutige Hinweise auf rechtswidrige Handlungen im Zusammenhang mit der Nutzung des Cloud-Dienstes vorliegen.	Einsichtnahme in Richtlinie zur Behandlung von Ermittlungsanfragen staatlicher Stellen und Beurteilung, ob betroffene Cloud-Kunden informiert werden, soweit dem nicht rechtliche Gründe entgegenstehen.	Keine Abweichung festgestellt.

INQ-03	Der Zugriff auf oder die Offenlegung von Daten der Cloud-Kunden im Rahmen von Ermittlungsanfragen staatlicher Stellen erfolgt nur unter der Voraussetzung, dass die juristische Beurteilung des Cloud-Anbieters ergab, dass eine anwendbare und rechtsgültige Rechtsgrundlage vorliegt und der Ermittlungsanfrage auf dieser Grundlage stattgegeben werden muss.	Der Zugriff auf oder die Offenlegung von Daten der Cloud-Kunden im Rahmen von Ermittlungsanfragen staatlicher Stellen erfolgt nur unter der Voraussetzung, dass die juristische Beurteilung von Arvato Systems ergab, dass eine anwendbare und rechtsgültige Rechtsgrundlage vorliegt und der Ermittlungsanfrage auf dieser Grundlage stattgegeben werden muss.	Einsichtnahme in Richtlinie zur Behandlung von Ermittlungsanfragen staatlicher Stellen und Beurteilung, ob ein Zugriff auf oder die Offenlegung von Daten der Cloud-Kunden nur auf Basis einer juristischen Prüfung stattfindet.	Keine Abweichung festgestellt.
INQ-04	Die Verfahren des Cloud-Anbieters für das Einrichten des Zugriffs auf oder das Offenlegen von Daten der Cloud-Kunden im Rahmen von Ermittlungsanfragen staatlicher Stellen gewährleisten, dass diese nur Zugriff auf oder Einsicht in diejenigen Daten erhalten, die Gegenstand der Ermittlungsanfrage sind. Soweit keine klare Eingrenzung der Daten möglich ist, anonymisiert oder pseudonymisiert der Cloud-Anbieter die Daten, so dass staatliche Stellen diese nur solchen Cloud-Kunden zuordnen können, die Gegenstand der Ermittlungsanfrage sind.	Die Verfahren von Arvato Systems für das Einrichten des Zugriffs auf oder das Offenlegen von Daten der Cloud-Kunden im Rahmen von Ermittlungsanfragen staatlicher Stellen gewährleisten, dass diese nur Zugriff auf oder Einsicht in diejenigen Daten erhalten, die Gegenstand der Ermittlungsanfrage sind. Soweit keine klare Eingrenzung der Daten möglich ist, anonymisiert oder pseudonymisiert Arvato Systems die Daten, so dass staatliche Stellen diese nur solchen Cloud-Kunden zuordnen können, die Gegenstand der Ermittlungsanfrage sind.	Einsichtnahme in Richtlinie zur Behandlung von Ermittlungsanfragen staatlicher Stellen und Beurteilung, ob nur die Daten herausgegeben werden, die Gegenstand der Ermittlungsanfrage sind. Einsichtnahme in Richtlinie und Beurteilung, ob nicht klar abgrenzbare Daten anonymisiert oder pseudonymisiert werden.	Keine Abweichung festgestellt.
Die Kontrollen sind zutreffend dargestellt sowie angemessen eingerichtet, um das oben genannte Kontrollziel zu erreichen.				

ANLAGE 3

ALLGEMEINE AUFTRAGSBEDINGUNGEN

Allgemeine Auftragsbedingungen

für die

Dr. Stückmann und Partner mbB
Wirtschaftsprüfungsgesellschaft Steuerberatungsgesellschaft

vom 1. Januar 2024

1. Geltungsbereich

(1) Die Auftragsbedingungen gelten für Verträge zwischen der Dr. Stückmann und Partner mbB Wirtschaftsprüfungsgesellschaft (im Nachstehenden „Wirtschaftsprüfer" genannt) und ihren Auftraggebern über Prüfungen, Steuerberatung, Beratungen in wirtschaftlichen Angelegenheiten und sonstige Aufträge, soweit nicht etwas anderes ausdrücklich in Textform vereinbart oder gesetzlich zwingend vorgeschrieben ist.

(2) Dritte können nur dann Ansprüche aus dem Vertrag zwischen Wirtschaftsprüfer und Auftraggeber herleiten, wenn dies vereinbart ist oder sich aus zwingenden gesetzlichen Regelungen ergibt. Im Hinblick auf solche Ansprüche gelten diese Auftragsbedingungen auch diesen Dritten gegenüber. Einreden und Einwendungen aus dem Vertragsverhältnis mit dem Auftraggeber stehen dem Wirtschaftsprüfer auch gegenüber Dritten zu.

2. Umfang und Ausführung des Auftrags

(1) Gegenstand des Auftrags ist die vereinbarte Leistung, nicht ein bestimmter wirtschaftlicher Erfolg. Der Auftrag wird nach den Grundsätzen ordnungsmäßiger Berufsausübung ausgeführt. Der Wirtschaftsprüfer übernimmt im Zusammenhang mit seinen Leistungen keine Aufgaben der Geschäftsführung. Der Wirtschaftsprüfer ist für die Nutzung oder Umsetzung der Ergebnisse seiner Leistungen nicht verantwortlich. Der Wirtschaftsprüfer ist berechtigt, sich zur Durchführung des Auftrags sachverständiger Personen zu bedienen.

(2) Die Berücksichtigung ausländischen Rechts bedarf – außer bei betriebswirtschaftlichen Prüfungen – der ausdrücklichen Vereinbarung in Textform.

(3) Ändert sich die Sach- oder Rechtslage nach Abgabe der abschließenden beruflichen Äußerung, so ist der Wirtschaftsprüfer nicht verpflichtet, den Auftraggeber auf Änderungen oder sich daraus ergebende Folgerungen hinzuweisen.

3. Mitwirkungspflichten des Auftraggebers

(1) Der Auftraggeber hat dafür zu sorgen, dass dem Wirtschaftsprüfer alle für die Ausführung des Auftrags notwendigen Unterlagen und weiteren Informationen rechtzeitig übermittelt werden und ihm von allen Vorgängen und Umständen Kenntnis gegeben wird, die für die Ausführung des Auftrags von Bedeutung sein können. Dies gilt auch für die Unterlagen und weiteren Informationen, Vorgänge und Umstände, die erst während der Tätigkeit des Wirtschaftsprüfers bekannt werden. Der Auftraggeber wird dem Wirtschaftsprüfer geeignete Auskunftspersonen benennen.

(2) Auf Verlangen des Wirtschaftsprüfers hat der Auftraggeber die Vollständigkeit der vorgelegten Unterlagen und der weiteren Informationen sowie der gegebenen Auskünfte und Erklärungen in einer vom Wirtschaftsprüfer formulierten Erklärung in gesetzlicher Schriftform oder einer sonstigen vom Wirtschaftsprüfer bestimmten Form zu bestätigen.

4. Sicherung der Unabhängigkeit

(1) Der Auftraggeber hat alles zu unterlassen, was die Unabhängigkeit der Mitarbeiter des Wirtschaftsprüfers gefährdet. Dies gilt für die Dauer des Auftragsverhältnisses insbesondere für Angebote auf Anstellung oder Übernahme von Organfunktionen und für Angebote, Aufträge auf eigene Rechnung zu übernehmen.

(2) Sollte die Durchführung des Auftrags die Unabhängigkeit des Wirtschaftsprüfers, die der mit ihm verbundenen Unternehmen, seiner Netzwerkunternehmen oder solcher mit ihm assoziierten Unternehmen, auf die die Unabhängigkeitsvorschriften in gleicher Weise Anwendung finden wie auf den Wirtschaftsprüfer, in anderen Auftragsverhältnissen beeinträchtigen, ist der Wirtschaftsprüfer zur außerordentlichen Kündigung des Auftrags berechtigt.

5. Berichterstattung und mündliche Auskünfte

Soweit der Wirtschaftsprüfer Ergebnisse im Rahmen der Bearbeitung des Auftrags in gesetzlicher Schriftform oder Textform darzustellen hat, ist allein diese Darstellung maßgebend. Entwürfe solcher Darstellungen sind unverbindlich. Sofern nicht anders gesetzlich vorgesehen oder vertraglich vereinbart, sind mündliche Erklärungen und Auskünfte des Wirtschaftsprüfers nur dann verbindlich, wenn sie in Textform bestätigt werden. Erklärungen und Auskünfte des Wirtschaftsprüfers außerhalb des erteilten Auftrags sind stets unverbindlich.

6. Weitergabe einer beruflichen Äußerung des Wirtschaftsprüfers

(1) Die Weitergabe beruflicher Äußerungen des Wirtschaftsprüfers (Arbeitsergebnisse oder Auszüge von Arbeitsergebnissen – sei es im Entwurf oder in der Endfassung) oder die Information über das Tätigwerden des Wirtschaftsprüfers für den Auftraggeber an einen Dritten bedarf der in Textform erteilten Zustimmung des Wirtschaftsprüfers, es sei denn, der Auftraggeber ist zur Weitergabe oder Information aufgrund eines Gesetzes oder einer behördlichen Anordnung verpflichtet.

(2) Die Verwendung beruflicher Äußerungen des Wirtschaftsprüfers und die Information über das Tätigwerden des Wirtschaftsprüfers für den Auftraggeber zu Werbezwecken durch den Auftraggeber sind unzulässig.

7. Mängelbeseitigung

(1) Bei etwaigen Mängeln hat der Auftraggeber Anspruch auf Nacherfüllung durch den Wirtschaftsprüfer. Nur bei Fehlschlagen, Unterlassen bzw. unberechtigter Verweigerung, Unzumutbarkeit oder Unmöglichkeit der Nacherfüllung kann er die Vergütung mindern oder vom Vertrag zurücktreten; ist der Auftrag nicht von einem Verbraucher erteilt worden, so kann der Auftraggeber wegen eines Mangels nur dann vom Vertrag zurücktreten, wenn die erbrachte Leistung wegen Fehlschlagens, Unterlassung, Unzumutbarkeit oder Unmöglichkeit der Nacherfüllung für ihn ohne Interesse ist. Soweit darüber hinaus Schadensersatzansprüche bestehen, gilt Nr. 9.

(2) Ein Nacherfüllungsanspruch aus Abs. 1 muss vom Auftraggeber unverzüglich in Textform geltend gemacht werden. Nacherfüllungsansprüche nach Abs. 1, die nicht auf einer vorsätzlichen Handlung beruhen, verjähren nach Ablauf eines Jahres ab dem gesetzlichen Verjährungsbeginn.

(3) Offenbare Unrichtigkeiten, wie z.B. Schreibfehler, Rechenfehler und formelle Mängel, die in einer beruflichen Äußerung (Bericht, Gutachten und dgl.) des Wirtschaftsprüfers enthalten sind, können jederzeit vom Wirtschaftsprüfer auch Dritten gegenüber berichtigt werden. Unrichtigkeiten, die geeignet sind, in der beruflichen Äußerung des Wirtschaftsprüfers enthaltene Ergebnisse infrage zu stellen, berechtigen diesen, die Äußerung auch Dritten gegenüber zurückzunehmen. In den vorgenannten Fällen ist der Auftraggeber vom Wirtschaftsprüfer tunlichst vorher zu hören.

8. Schweigepflicht gegenüber Dritten, Datenschutz

(1) Der Wirtschaftsprüfer ist nach Maßgabe der Gesetze (§ 323 Abs. 1 HGB, § 43 WPO, § 203 StGB) verpflichtet, über Tatsachen und Umstände, die ihm bei seiner Berufstätigkeit anvertraut oder bekannt werden, Stillschweigen zu bewahren, es sei denn, dass der Auftraggeber ihn von dieser Schweigepflicht entbindet.

(2) Der Wirtschaftsprüfer wird bei der Verarbeitung von personenbezogenen Daten die nationalen und europarechtlichen Regelungen zum Datenschutz beachten.

9. Haftung

(1) Für gesetzlich vorgeschriebene Leistungen des Wirtschaftsprüfers, insbesondere Prüfungen, gelten die jeweils anzuwendenden gesetzlichen Haftungsbeschränkungen, insbesondere die Haftungsbeschränkung des § 323 Abs. 2 HGB.

(2) Sofern weder eine gesetzliche Haftungsbeschränkung Anwendung findet noch eine einzelvertragliche Haftungsbeschränkung besteht, ist der Anspruch des Auftraggebers aus dem zwischen ihm und dem Wirtschaftsprüfer bestehenden Vertragsverhältnis auf Ersatz eines fahrlässig verursachten Schadens, mit Ausnahme von Schäden aus der Verletzung von Leben, Körper und Gesundheit sowie von Schäden, die eine Ersatzpflicht des Herstellers nach § 1 ProdHaftG begründen, gemäß § 54a Abs. 1 Nr. 2 WPO auf 4 Mio. € beschränkt. Gleiches gilt für Ansprüche, die Dritte aus oder im Zusammenhang mit dem Vertragsverhältnis gegenüber dem Wirtschaftsprüfer geltend machen.

(3) Leiten mehrere Anspruchsteller aus dem mit dem Wirtschaftsprüfer bestehenden Vertragsverhältnis Ansprüche aus einer fahrlässigen Pflichtverletzung des Wirtschaftsprüfers her, gilt der in Abs. 2 genannte Höchstbetrag für die betreffenden Ansprüche aller Anspruchsteller insgesamt.

(4) Der Höchstbetrag nach Abs. 2 bezieht sich auf einen einzelnen Schadensfall. Ein einzelner Schadensfall ist auch bezüglich eines aus mehreren Pflichtverletzungen stammenden einheitlichen Schadens gegeben. Der einzelne Schadensfall umfasst sämtliche Folgen einer Pflichtverletzung ohne Rücksicht darauf, ob Schäden in einem oder in mehreren aufeinanderfolgenden Jahren entstanden sind. Dabei gilt mehrfaches auf gleicher oder gleichartiger Fehlerquelle beruhendes Tun oder Unterlassen als einheitliche Pflichtverletzung, wenn die betreffenden Angelegenheiten miteinander in rechtlichem oder wirtschaftlichem Zusammenhang stehen. In diesem Fall kann der Wirtschaftsprüfer nur bis zur Höhe von 5 Mio. € in Anspruch genommen werden.

(5) Ein Schadensersatzanspruch erlischt, wenn nicht innerhalb von sechs Monaten nach der in Textform erklärten Ablehnung der Ersatzleistung Klage erhoben wird und der Auftraggeber auf diese Folge hingewiesen wurde. Dies gilt nicht für Schadensersatzansprüche, die auf vorsätzliches Verhalten zurückzuführen sind, sowie bei einer schuldhaften Verletzung von Leben, Körper oder Gesundheit sowie bei Schäden, die eine Ersatzpflicht des Herstellers nach § 1 ProdHaftG begründen. Das Recht, die Einrede der Verjährung geltend zu machen, bleibt unberührt.

(6) § 323 HGB bleibt von den Regelungen in Abs. 2 bis 5 unberührt.

10. Ergänzende Bestimmungen für Prüfungsaufträge

(1) Ändert der Auftraggeber nachträglich den durch den Wirtschaftsprüfer geprüften und mit einem Bestätigungsvermerk versehenen Abschluss oder Lagebericht, darf er diesen Bestätigungsvermerk nicht weiterverwenden.

Hat der Wirtschaftsprüfer einen Bestätigungsvermerk nicht erteilt, so ist ein Hinweis auf die durch den Wirtschaftsprüfer durchgeführte Prüfung im Lagebericht oder an anderer für die Öffentlichkeit bestimmter Stelle nur mit in gesetzlicher Schriftform erteilter Einwilligung des Wirtschaftsprüfers und mit dem von ihm genehmigten Wortlaut zulässig.

(2) Widerruft der Wirtschaftsprüfer den Bestätigungsvermerk, so darf der Bestätigungsvermerk nicht weiterverwendet werden. Hat der Auftraggeber den Bestätigungsvermerk bereits verwendet, so hat er auf Verlangen des Wirtschaftsprüfers den Widerruf bekanntzugeben.

(3) Der Auftraggeber hat Anspruch auf fünf Berichtsausfertigungen. Weitere Ausfertigungen werden besonders in Rechnung gestellt.

11. Ergänzende Bestimmungen für Hilfeleistung in Steuersachen

(1) Der Wirtschaftsprüfer ist berechtigt, sowohl bei der Beratung in steuerlichen Einzelfragen als auch im Falle der Dauerberatung die vom Auftraggeber genannten Tatsachen, insbesondere Zahlenangaben, als richtig und vollständig zugrunde zu legen; dies gilt auch für Buchführungsaufträge. Er hat jedoch den Auftraggeber auf von ihm festgestellte wesentliche Unrichtigkeiten hinzuweisen.

(2) Der Steuerberatungsauftrag umfasst nicht die zur Wahrung von Fristen erforderlichen Handlungen, es sei denn, dass der Wirtschaftsprüfer hierzu ausdrücklich den Auftrag übernommen hat. In diesem Fall hat der Auftraggeber dem Wirtschaftsprüfer alle für die Wahrung von Fristen wesentlichen Unterlagen, insbesondere Steuerbescheide, so rechtzeitig vorzulegen, dass dem Wirtschaftsprüfer eine angemessene Bearbeitungszeit zur Verfügung steht.

(3) Mangels einer anderweitigen Vereinbarung in Textform umfasst die laufende Steuerberatung folgende, in die Vertragsdauer fallenden Tätigkeiten:

a) Ausarbeitung und elektronische Übermittlung der Jahressteuererklärungen, einschließlich E-Bilanzen, für die Einkommensteuer, Körperschaftsteuer und Gewerbesteuer, und zwar auf Grund der vom Auftraggeber vorzulegenden Jahresabschlüsse und sonstiger für die Besteuerung erforderlichen Aufstellungen und Nachweise
b) Nachprüfung von Steuerbescheiden zu den unter a) genannten Steuern
c) Verhandlungen mit den Finanzbehörden im Zusammenhang mit den unter a) und b) genannten Erklärungen und Bescheiden
d) Mitwirkung bei Betriebsprüfungen und Auswertung der Ergebnisse von Betriebsprüfungen hinsichtlich der unter a) genannten Steuern
e) Mitwirkung in Einspruchs- und Beschwerdeverfahren hinsichtlich der unter a) genannten Steuern.

Der Wirtschaftsprüfer berücksichtigt bei den vorgenannten Aufgaben das Gesetz, die veröffentlichte höchstrichterliche Rechtsprechung, die finanzgerichtliche Rechtsprechung der Instanzgerichte in solchen Gebieten, die sich erkennbar in der Entwicklung befinden, und die Verwaltungsauffassung.

(4) Erhält der Wirtschaftsprüfer für die laufende Steuerberatung ein Pauschalhonorar, so sind mangels anderweitiger Vereinbarungen in Textform die unter Abs. 3 Buchst. d) und e) genannten Tätigkeiten gesondert zu honorieren.

(5) Sofern der Wirtschaftsprüfer auch Steuerberater ist und die Steuerberatervergütungsverordnung für die Bemessung der Vergütung anzuwenden ist, kann eine höhere oder niedrigere als die gesetzliche Vergütung in Textform vereinbart werden.

(6) Die Bearbeitung besonderer Einzelfragen der Einkommensteuer, Körperschaftsteuer, Gewerbesteuer und Einheitsbewertung sowie aller Fragen der Umsatzsteuer, Lohnsteuer, sonstigen Steuern und Abgaben erfolgt auf Grund eines besonderen Auftrags. Dies gilt auch für

a) die Bearbeitung einmalig anfallender Steuerangelegenheiten, z.B. auf dem Gebiet der Erbschaftsteuer und Grunderwerbsteuer,
b) die Mitwirkung und Vertretung in Verfahren vor den Gerichten der Finanz- und der Verwaltungsgerichtsbarkeit sowie in Steuerstrafsachen,
c) die beratende und gutachtliche Tätigkeit im Zusammenhang mit Umwandlungen, Kapitalerhöhung und -herabsetzung, Sanierung, Eintritt und Ausscheiden eines Gesellschafters, Betriebsveräußerung, Liquidation und dergleichen und
d) die Unterstützung bei der Erfüllung von Anzeige- und Dokumentationspflichten.

(7) Soweit auch die Ausarbeitung der Umsatzsteuerjahreserklärung als zusätzliche Tätigkeit übernommen wird, gehört dazu nicht die Überprüfung etwaiger besonderer buchmäßiger Voraussetzungen sowie die Frage, ob alle in Betracht kommenden umsatzsteuerrechtlichen Vergünstigungen wahrgenommen worden sind. Eine Gewähr für die vollständige Erfassung der Unterlagen zur Geltendmachung des Vorsteuerabzugs wird nicht übernommen.

12. Elektronische Kommunikation

Die Kommunikation zwischen dem Wirtschaftsprüfer und dem Auftraggeber kann auch per E-Mail erfolgen. Soweit der Auftraggeber eine Kommunikation per E-Mail nicht wünscht oder besondere Sicherheitsanforderungen stellt, wie etwa die Verschlüsselung von E-Mails, wird der Auftraggeber den Wirtschaftsprüfer entsprechend in Textform informieren.

13. Vergütung

(1) Der Wirtschaftsprüfer hat neben seiner Gebühren- oder Honorarforderung Anspruch auf Erstattung seiner Auslagen; die Umsatzsteuer wird zusätzlich berechnet. Er kann angemessene Vorschüsse auf Vergütung und Auslagenersatz verlangen und die Auslieferung seiner Leistung von der vollen Befriedigung seiner Ansprüche abhängig machen. Mehrere Auftraggeber haften als Gesamtschuldner.

(2) Ist der Auftraggeber kein Verbraucher, so ist eine Aufrechnung gegen Forderungen des Wirtschaftsprüfers auf Vergütung und Auslagenersatz nur mit unbestrittenen oder rechtskräftig festgestellten Forderungen zulässig.

14. Streitschlichtungen

Der Wirtschaftsprüfer ist nicht bereit, an Streitbeilegungsverfahren vor einer Verbraucherschlichtungsstelle im Sinne des § 2 des Verbraucherstreitbeilegungsgesetzes teilzunehmen.

15. Anzuwendendes Recht

Für den Auftrag, seine Durchführung und die sich hieraus ergebenden Ansprüche gilt nur deutsches Recht.