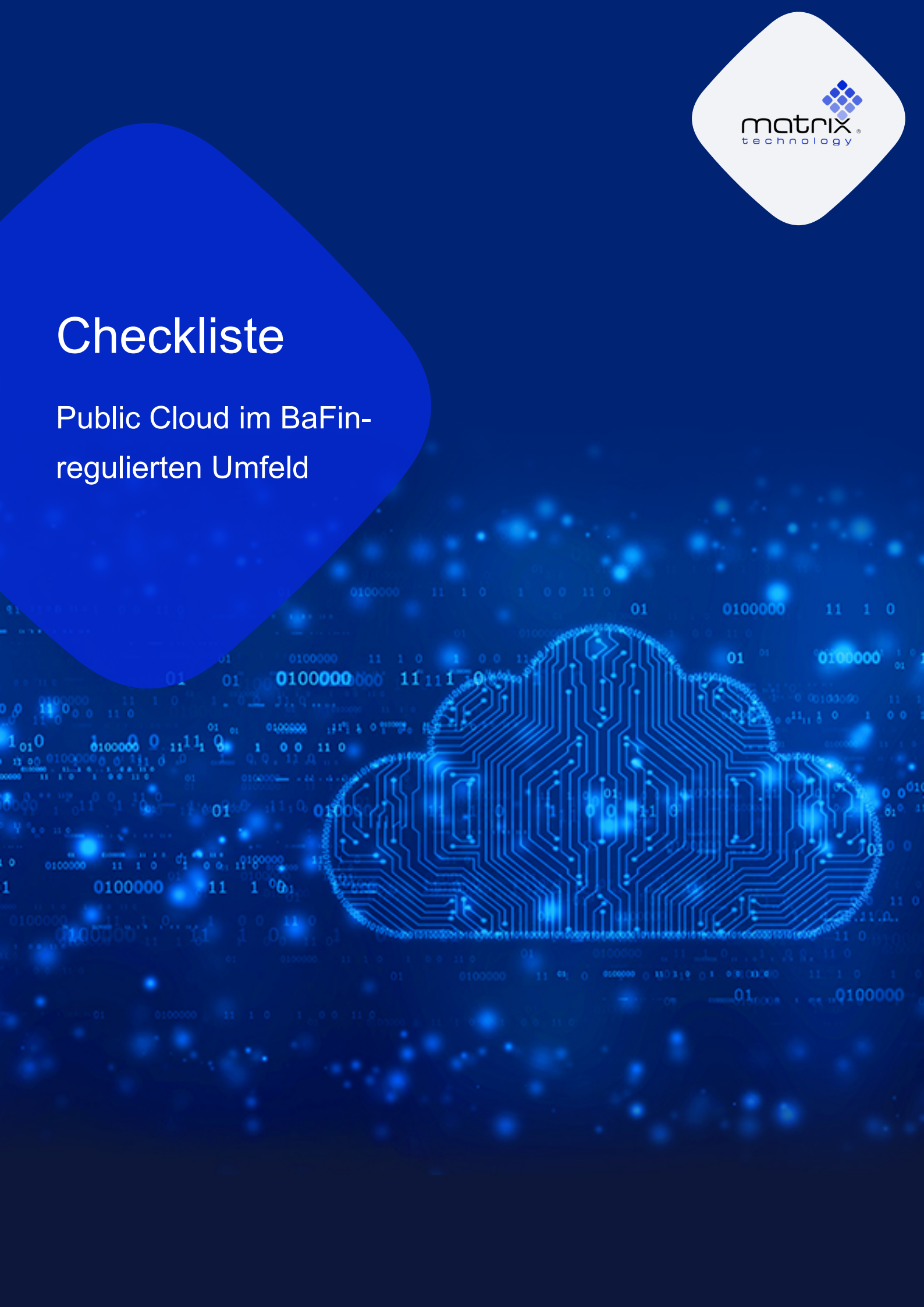
Checkliste

Public Cloud im BaFin-regulierten Umfeld



„Public Cloud im regulierten Umfeld – Das geht nicht!“ Wie oft haben wir diese Aussage nicht schon gelesen oder gehört. Dem ist jedoch nicht so: Vielmehr kann das Cloud Computing als Schlüsseltechnologie bei der Digitalisierung der Finanzbranche gesehen werden. Wenn man dabei auf eine standardisierte Public Cloud-Plattform zurückgreift, kann die Umsetzung regulatorischer Anforderungen sogar deutlich vereinfacht werden. Regulatorik verhindert keinen Cloud-Einsatz. Vielmehr zwingt sie Institute dazu, das Cloud-Computing strategisch, risikoorientiert und effizient anzugehen und umzusetzen.

Diese Checkliste unterstützt Sie bei der Evaluation Ihres Cloud Computing Vorhabens. Basis der Checkliste sind sowohl die Empfehlungen der BaFin im Merkblatt „Orientierungshilfe zu Auslagerungen an Cloud-Anbieter“ als auch die Anforderungen, die in den BAITs bzw. VAITs sowie dem C5-Katalog des BSI niedergeschrieben sind.

1. Organisation der Informationssicherheit – Cloud Readiness

In der Neuauflage des C5-Standards von 2020 wird explizit herausgehoben, dass es nicht reicht, wenn ein Institut einen Anbieter auswählt, der die C5-Kriterien erfüllt. Vielmehr muss das Institut sicherstellen, dass es selbst die C5-Kriterien bei sich umgesetzt hat.

- Die Organisation der Informationssicherheit wurde umgesetzt, wird aufrechterhalten und kontinuierlich verbessert.
- Die Nutzung von Cloud-Diensten wurde beim Institut hinreichend im Rahmen der IT-Strategie betrachtet. Die damit verbundenen Risiken wurden erfasst, bewertet und können im Rahmen einer Auslagerung gemanaged und beherrscht werden.
- Es wurde ein Prozess definiert, der alle wichtigen Schritte der Cloud Auslagerung – von der Strategie über die Transformation bis zur Exit-Strategie – umfasst.
- Es fand eine Prüfung der internen Prozesse hinsichtlich der Cloud Readiness des Instituts statt, mit dem Ergebnis, dass es bereit für die Cloud ist.

2. Sicherheitsrichtlinien

- Rollen- und Rechtekonzept, Richtlinie zur Verwaltung von Zugangs- und Zutrittsberechtigungen, Passwortrichtlinie und weitere Richtlinien im Kontext der Informationssicherheit wurden sowohl beim Institut als auch beim Cloud Provider ausgearbeitet und schriftlich festgehalten.
- Die zugehörigen Abläufe werden gelebt, regelmäßig geprüft und kontinuierlich verbessert.

3. Anforderungen an das Personal

- Das mit der Cloudnutzung betraute Personal wurde angemessen ausgebildet und ausreichend dimensioniert.
- Das Personal kennt seine Aufgaben im Rahmen der Informationssicherheit und nimmt sie zuverlässig wahr.

4. Asset Management | Physische Sicherheit

- Die Assets des Institutes sind bekannt und klassifiziert, damit sie angemessen geschützt werden können.
- Der Zutritt bzw. Zugang zu den genutzten Räumlichkeiten ist so organisiert, dass die Assets geschützt sind.

5. Identitäts- und Berechtigungsmanagement

- Zugangsberechtigungen werden eindeutig und nachvollziehbar in einem formalen Verfahren erteilt.
- Zugriffsberechtigung erfolgt nach dem „Need-to-Know“-Prinzip.
- Zugriffsberechtigungen werden mindestens jährlich überprüft.
- Einsatz von vertrauenswürdigen Verfahren zur Identitätsprüfung.
- Zwei-Faktor-Authentifizierung kommt bei der Identitätsprüfung von Administratoren zum Einsatz.
- Unberechtigte Zugriffe werden verhindert.

6. Kryptographie | Kommunikationssicherheit

- Kryptografische Verfahren sind vorhanden und beschrieben, um den Schutz der Vertraulichkeit, Authentizität und Integrität der Daten sicher zu stellen.
- Für den Schutz der Informationen im Netz wurden ausreichende Vorkehrungen getroffen worden.

7. Business Continuity

- Die Kontinuität des Geschäftsbetriebes ist durch angemessene Maßnahmen sichergestellt.
- Notfallpläne wurden implementiert und werden regelmäßig getestet und verbessert.

8. Steuerung und Überwachung von Dienstleistern

- Informations- und Prüfungsrechte sowie umfassende Kontrollmöglichkeiten sind vertraglich vereinbart und nicht eingeschränkt.
- Das auslagernde Institut hat die Möglichkeit, Vor-Ort Prüfungen beim Cloud-Anbieter durchzuführen bzw. durchführen zu lassen.
- Vereinbarte Leistungen werden überwacht und regelmäßig geprüft.
- Uneingeschränkter Zugriff auf Informationen, Daten sowie den Ort der Leistungserbringung (Büroräume des Cloud-Dienstleisters, Begehung der Rechenzentren) ist möglich.

Anmerkung: Unter Erfüllung bestimmter Voraussetzungen kann Ihre Bank auf individuelle Prüfungen beim Cloud-Anbieter verzichten und stattdessen:

- Die interne Revision des Cloud-Anbieters prüfen und reporten lassen
- An einer Sammelprüfung teilnehmen
- Einen vom Cloud-Anbieter oder vom auslagernden Institut beauftragten Dritten prüfen lassen.

Hinzu kommt, dass ein Institut auf Nachweise bzw. Zertifikate gängiger Standards oder auf Prüfberichte Dritter bzw. des Cloud-Anbieters mit entsprechender Detailtiefe zurückgreifen darf.

9. Compliance | Datenschutz

Verstöße gegen gesetzliche, regulatorische, selbstauferlegte oder vertragliche Anforderungen zur Informationssicherheit sowie Anforderungen des Datenschutzes werden durch angemessene Maßnahmen verhindert.

Durchführung einer ausführlichen, schriftlich dokumentierten und nachvollziehbaren Risikoanalyse als Basis für die Entscheidung der Wesentlichkeit.

Berücksichtigung wichtiger Aspekte wie Kritikalität der auszulagernden Leistung, Bewertung der finanziellen, operationellen und rechtlichen Risiken sowie Reputationsrisiken, Eignung des Cloud-Anbieters.

Über den Autor

Jürgen Brombacher
Head of Cloud Consulting

Jürgen Brombacher ist seit 2019 bei der matrix technology tätig und seit 2021 in seiner Position als Head of Cloud Consulting. Als Informatiker beschäftigt er sich seit 30 Jahren mit zahlreichen IT-Themen wie Server- und Datenbankmanagement, ITIL, Anwendungs- und Systemarchitekturen, Rechenzentrum und IT-Outsourcing.

Seit 2017 liegt sein Schwerpunkt in den Bereichen Cyber-Security, Regulatorik und Compliance. So hat er die Ergebnistypen im Bereich Security Operations verantwortet, die nach einer EZB-Prüfung von vier Großbanken bei einem IT-Dienstleister umzusetzen waren, an zahlreichen Prüfungsterminen beratend teilgenommen und ein Security Operation Center aufgebaut und geleitet.

Kontakt

Finsurance IT-Services

(Eine Marke der matrix technology GmbH)

Telefon +49 89 589395-600

Telefax +49 89 589395-711

Web: finsurance-it-services.de

E-Mail: finsurance@matrix.ag