Anlage 6: Zusätzliche Anforderungen für Dienstleistercluster „DL06 Cloud-Dienste"

Die folgenden Dienstleistungen sind dem Dienstleistercluster DL06 zugeordnet:

- Cloud-Dienste IaaS
- Cloud-Dienste PaaS
- Cloud-Dienste SaaS

1 Einleitung

Folgende Anforderungen gelten für Dienstleistungsbezüge, sofern im Rahmen des Dienstleistungsbezuges Cloud-Dienste außerhalb der ILB in Anspruch genommen werden.

2 Generelle Sicherheitsthemen

2.1 Informationssicherheitsmanagement

1. Der Dienstleister verpflichtet sich, ein Informationssicherheitsmanagementsystem (ISMS) auf Basis eines anerkannten Standards gemäß AT 7.2 der MaRisk (z. B. ISO 27001 bzw. BSI-Standard 200-1) zu betreiben. Die von der ILB genutzten Dienste, IT-Systeme und Kommunikationsverbindungen sind im ISMS-Geltungsbereich betrachtet. Im Rahmen des ISMS betreibt der Dienstleister ein Informationssicherheitsrisikomanagement (IRM).
2. Der Informationssicherheitsstandard umfasst mindestens Aufgaben der Planung, der Implementierung, des Betriebs, der Überwachung, des Reportings, der Pflege und Durchführung kontinuierlicher Verbesserungen von Maßnahmen, die zur Gewährleistung der Verfügbarkeit, der Vertraulichkeit, der Integrität und der Authentizität der vom Dienstleister sowie dessen Subdienstleistern im Auftrag der ILB verwalteten Informationen/Daten und Ressourcen dienen.
3. Die Anforderungen zur Einhaltung der Informationssicherheit sind in schriftlicher Form beim Dienstleister dokumentiert und es finden regelmäßige Kontrollen über die Einhaltung der Anforderungen durch den Dienstleister statt.

ab Schutzbedarf „hoch“

4. Der Dienstleister muss nachweisen, dass er eine anerkannte ISMS-Zertifizierung (z. B. ISO 27001 oder ISO 27001 auf Basis von IT-Grundschutz) vorweisen kann und sich die von der ILB genutzten Dienste, IT-Systeme und Kommunikationsverbindungen im Geltungsbereich des Zertifikats befinden. Das Zertifikat muss während der Laufzeit des Vertrages gültig sein. Alle Änderungen am Geltungsbereich oder etwaige Änderungen bei der Gültigkeit des Zertifikats sind der ILB zu melden.

2.2 Kontrollrecht

ab Schutzbedarf „hoch“

1. Der Dienstleister informiert den Auftraggeber unverzüglich, mindestens in Textform, über wesentliche Feststellungen bei vertragserheblichen Audits, sowie bei vertragsrelevanten entzogenen Zertifikaten und Testaten.
2. Der Dienstleister hat bei Bekanntwerden von unzureichend erfüllten Sicherheitsanforderungen, zum Beispiel aufgrund von allgemeiner Risikoidentifizierung, veränderter Gefährdungs- oder Gesetzeslage, Nachbesserungen zu vollziehen.
3. Der Dienstleister verpflichtet sich, berechtigten Beschäftigten der ILB oder von der ILB beauftragten Prüfern nach voriger Anmeldung Zutritt zu den relevanten Räumlichkeiten zu gewähren, so dass diese ein Vor-Ort-Audit der vertraglich vereinbarten Sicherheitsmaßnahmen durchführen können.

2.3 IKT-Vorfallmanagement

1. Der Dienstleister etabliert einen internen Prozess zur Identifizierung, Eindämmung, Beseitigung und Bewertung von Sicherheitsvorfällen.
2. Über eine geeignete Meldekette ist sicherzustellen, dass alle erforderlichen Stellen schnellstmöglich in die Behandlung der Sicherheitsvorfälle geeignet eingebunden werden. Die relevanten Rollen sind in einer Kommunikations- und Eskalationsmatrix zu dokumentieren.
3. Alle relevanten Ereignisse, Entscheidungen und Handlungen sind nachvollziehbar zu dokumentieren.
4. Im Nachgang ist zu allen Sicherheitsvorfällen eine Ursachenanalyse zu erstellen. Etwaige Maßnahmen zur Vermeidung zukünftiger Sicherheitsvorfälle oder Verbesserung der Sicherheitsvorfallbehandlung sind nachzuhalten.
5. Durch regelmäßige Übungen stellt der Dienstleister sicher, dass die etablierten Maßnahmen zur Sicherheitsvorfallbehandlung den Erwartungen entsprechend funktionieren.
6. Der Dienstleister informiert die ILB umgehend, sobald potenzielle Sicherheitsvorfälle gemeldet werden, die die Informationssicherheit der ILB beinträchtigen könnten und stellt der ILB alle relevanten Unterlagen zur Verfügung.
7. Der Dienstleister hat standardisierte Protokolle und Berichte zur Meldung von Sicherheitsvorfällen zu etablieren.
8. Für Erst-, Folge- und Erledigungsmeldungen zu Informationssicherheitsvorfällen gelten folgende formalen Anforderungen:
   - Kurzbeschreibung
   - Betroffener Service / Asset
   - Bearbeitungsstatus
   - Detailbeschreibung
   - Betroffenes Schutzziel
   - Ursachenbeschreibung
   - Datenschutzbeurteilung
   - Eingeleitete Sofortmaßnahmen
   - Lessons Learned

ab Schutzbedarf „hoch“

9. Der Dienstleister stellt sicher, dass etwaige Sicherheitsvorfälle zu jeder Zeit identifiziert werden können und dass auch außerhalb der normalen Dienstzeiten sofort mit der Eindämmung und Beseitigung begonnen wird.
10. Der Dienstleister stellt sicher, dass bei einem Verdacht von vorsätzlichen Handlungen oder wenn schwerwiegende Auswirkungen zu erwarten sind, forensische Untersuchungen durch qualifizierte Personen zeitnah durchgeführt werden.

2.4 Personalsicherheit

1. Der Dienstleister verpflichtet seine Mitarbeitende zur Einhaltung der Vertraulichkeitspflichten und zur Bewahrung etwaiger Geschäftsgeheimnisse während und nach der Durchführung von Aufgaben für die ILB.
2. Der Dienstleister muss einen Ansprechpartner benennen, der für alle Fragen der Einbindung bei der ILB aussagefähig ist und bei Bedarf Aktionen zur Sicherstellung der sicheren Einbindung initiieren kann.

3. Die Beschäftigten des Dienstleisters müssen schriftlich verpflichtet werden, einschlägige Gesetze, Vorschriften sowie die Regelungen der ILB einzuhalten.

ab Schutzbedarf „hoch“

4. Der Dienstleister stellt sicher, dass die Beschäftigten geregelt in ihre Aufgaben eingewiesen und über bestehende Regelungen zur Informationssicherheit unterrichtet wurden
5. Der Dienstleister stellt sicher, dass die Vertrauenswürdigkeit des eingesetzten Personals geeignet überprüft wird.

2.5 Berechtigungsmanagement

1. In Abstimmung mit der ILB muss bestimmt werden, welche Berechtigungen durch den Dienstleister und welche durch die ILB vergeben werden. Für alle Berechtigungen, die der Dienstleister selbst vergibt, muss dieser ein Berechtigungskonzept auf der Basis von Rollen erstellen. Für jede Rolle sind die erforderlichen Rechte, eine kurze Beschreibung und etwaige Ausschlüsse mit anderen Rollen zu dokumentieren. Es dürfen nur Berechtigungen auf der Basis dieser Berechtigungskonzepte vergeben werden.
2. Jede durch den Dienstleister vergebene Berechtigung ist zu dokumentieren.
3. Das Berechtigungskonzept des Dienstleisters sowie die vergebenen Berechtigungen sind halbjährlich vom Dienstleister zu prüfen.

ab Schutzbedarf „hoch“

4. Für besonders schutzbedürftige Informationen erfolgt eine Vergabe einer Berechtigung nur nach Freigabe durch die ILB.
5. Die Gültigkeit der Berechtigungen ist monatlich vom Dienstleister zu prüfen.

2.6 Mandantentrennung

1. Der Dienstleister muss durch Mandantentrennung sicherstellen, dass die Daten und Verarbeitungskontexte der ILB ausreichend sicher von anderen Mandanten getrennt sind.
2. Der Dienstleister hat dies in einem Mandantentrennungskonzept zu dokumentieren.
3. Das Mandantentrennungskonzept muss zwischen mandantenabhängigen und mandantenübergreifenden Daten und Objekten unterscheiden und darlegen, mit welchen Mechanismen der Dienstleister diese trennt.

ab Schutzbedarf „hoch“

4. Die Dienste für die ILB werden auf gesonderten Instanzen bereitgestellt. Der Netzverkehr wird durch eine geeignete Netzsegmentierung von anderen Kunden getrennt.

2.7 Ordnungsgemäße IT-Administration

1. Der IT-Betrieb des Dienstleisters erfolgt auf der Basis von dokumentierten IT-Betriebsprozessen. Alle Entscheidungen und Handlungen im Rahmen dieser Prozesse müssen nachvollziehbar dokumentiert werden.
2. Alle Änderungen an den Anwendungen, IT-Systemen und Kommunikationsverbindungen, die Einfluss auf die Bereitstellung der Dienst für die ILB haben könnten, sind im Rahmen eines Änderungsmanagements (Change-Managements) zu planen, zu testen, freizugeben und umzusetzen. Für jede Änderung müssen geeignete Maßnahmen zur Wiederherstellung des vorigen Zustands dokumentiert werden (Fallback-Lösung). Alle Störungen und sonstigen Vorfälle müssen im Rahmen eines Vorfalls-Management (Incident Management) dokumentiert, bewertet und behandelt werden.

ab Schutzbedarf „hoch“

3. Der Dienstleister etabliert einen Betriebsprozess zu langfristigen Lösungen von Problemen (Problem Management).

4. Die Dokumentation der einzelnen IT-Prozesse erfolgt in geeigneten Softwarelösungen (z. B. Ticket-Systemen).
5. Die IT-Komponenten werden in einer CMDB verwaltet.

2.8 Schwachstellenmanagement

1. Der Dienstleister stellt für alle Komponenten, die für die Bereitstellung der Dienste für die ILB notwendig sind, sicher, dass Quellen zur Beschaffung von Informationen über Schwachstellen dokumentiert sind (z. B. Herstellerseiten, CERTs, Newsletter, Nachrichtenseiten etc.) und regelmäßig bzw. anlassbezogen in Bezug auf Schwachstellen ausgewertet werden.
2. Alle gemeldeten Schwachstellen werden durch den Dienstleister dokumentiert und im Hinblick auf ihre potenziellen Auswirkungen bewertet. Der Dienstleister leitet bei Bedarf Gegenmaßnahmen ein.
3. Der Dienstleister informiert die ILB umgehend über die gemeldeten Schwachstellen und seine Einschätzung über die Auswirkungen.

ab Schutzbedarf „hoch“

4. Der Dienstleister führt mindestens einmal monatlich automatisierte Schwachstellenscans gegen die für die Bereitstellung der Dienste der ILB notwendigen IT-Systeme und Anwendungen durch.
5. Der Dienstleister führt mindestens einmal jährlich einen Penetrationstest gegen die für die Bereitstellung der Dienste der ILB notwendigen IT-Systeme und Anwendungen in Abstimmung mit der ILB durch.

2.9 Patchmanagement

1. Der Dienstleister etabliert einen Prozess zur Ermittlung von Updates für alle eingesetzten Anwendungen, Betriebssysteme und Firmwares. Er bewertet alle gemeldeten Updates im Hinblick auf etwaige Auswirkungen auf die Sicherheit und den Betrieb der Dienste für die ILB. Auf Basis dieser Einstufung entscheidet er, wie diese Updates eingespielt werden sollen.
2. Alle Patches sind im Rahmen des Änderungsmanagements auf getrennten Systemen umfassend zu testen, bevor sie auf Produktivsystemen aufgespielt werden.
3. Im Falle unmittelbarer Gefahren für die betroffenen Anwendungen, Betriebssysteme und Firmwares ist ein Verfahren für ein sicheres beschleunigtes Einspielen der Patches zu definieren.
4. Die ILB ist über alle getroffenen Entscheidungen zum Umgang mit Patches umgehend zu informieren. Die ILB kann bei Bedarf Einfluss auf den Zeitpunkt des Einspielens nehmen.

ab Schutzbedarf „hoch“

5. In Abhängigkeit des Betriebsmodells müssen alle Entscheidungen über das Einspielen von Patches mit der ILB abgestimmt werden.

2.10 Systemhärtung

1. Alle IT-Systeme müssen so konfiguriert werden, dass keine nicht benötigten Dienste oder Anwendungen laufen.

ab Schutzbedarf „sehr hoch“

2. Auf jedem Server darf nur ein Dienst betrieben werden.

2.11 Schutz vor Schadprogrammen

1. Der Dienstleister stellt auf allen Systemen, bei denen es eine realistische Chance für einen Befall durch Schadsoftware gibt oder die Daten mit verwundbaren Systemen austauschen, einen Schutz vor Schadsoftware sicher. Dieser Schutz bietet Virenschutz auf allen Systemen, die angreifbar für Schadsoftware sind oder Daten mit angreifbaren Systemen austauschen.
2. Jede Datei, die auf dieses System übertragen wird, muss durch einen On-Access-Scanner sofort untersucht werden.
3. Zusätzlich sind regelmäßig bzw. mindestens wöchentlich Scans aller gespeicherten Daten durchzuführen.
4. Die Muster für die Schadprogrammerkennung sind nach den Vorgaben des Herstellers zu aktualisieren.

ab Schutzbedarf „hoch“

5. Der für die ILB relevante Netzverkehr muss auf Schadsoftware hin untersucht werden.
6. Alle Meldungen über erkannte Schadsoftware sind an die ILB zu übermitteln.

2.12 Protokollierung

1. Der Dienstleister dokumentiert für jedes System eine Übersicht der zu protokollierenden Daten und definiert Schwellenwerte, ab denen eine Alarmierung und ggf. weitere Maßnahmen notwendig werden.
2. Der Dienstleister überwacht während der vereinbarten Zeiten die Protokolldaten auf Anomalien sowie Alarme und leitet bei Bedarf die weiteren Maßnahmen ein.
3. Das Protokollierungskonzept wird mindestens jährlich oder anlassbezogen überprüft und aktualisiert. Zudem muss ein Prozess existieren, welcher die Überwachungs- und Protokollierungstools regelmäßig validiert und überprüft hinsichtlich Einhaltung der Funktionalität und Reaktionsmuster im vorgegebenen Zeitraum.
4. Der Dienstleister vereinbart mit der ILB, unter welchen Umständen eine Benachrichtigung der ILB notwendig ist und welche Daten in Berichten zusammengefasst werden sollen. Der Dienstleister stellt sicher, dass die Benachrichtigung und Berichte zu den vereinbarten Zeiten an die ILB übermittelt werden sollen.
5. Der Dienstleister bestimmt zusammen mit der ILB, wie lange die Protokolldateien aufbewahrt werden müssen. Der Dienstleister verpflichtet sich, die Protokolldaten für den vereinbarten Zeitraum aufzubewahren.
6. Der Dienstleister stellt sicher, dass die Systemzeit von IT-Systemen gleich ist und automatisierte Dienste zur Zeitsynchronisation auf allen IT-Systemen aktiviert sind.

ab Schutzbedarf „hoch“

7. Der Dienstleister protokolliert alle privilegierten Handlungen an seinen Systemen und Anwendungen.
8. Der Dienstleister sammelt die Protokolldaten auf zentralen Systemen und stellt durch geeignete technische Mittel sicher, dass diese nicht manipuliert werden können.
9. Der Dienstleister stellt die Überwachung und eine angemessene Reaktion rund um die Uhr (24/7) sicher.
10. Der Dienstleister stellt sicher, dass in angemessener Regelmäßigkeit Datensicherungen der Protokolldaten erstellt werden, damit die Verfügbarkeit der Protokolldaten bei Datenverlusten und Systemausfällen gewährleistet ist. Die Effektivität der Datensicherungsmechanismen sowie die Wiederherstellungsprozesse sind jährlich zu testen. Für die Datensicherung von Protokolldaten muss ebenfalls sichergestellt werden, dass diese vergleichbar vor Zugriff und Änderung der Daten geschützt werden wie die Originaldaten.

2.13 Datensicherung

1. Der Dienstleister dokumentiert für jedes System die Rahmenbedingungen für die jeweiligen Datensicherungen (mindestens Zeiträume, Datensicherungsart, Medien).
2. Der Dienstleister stellt sicher, dass alle Datensicherungen den Vorgaben entsprechend durchgeführt werden.
3. Der Dienstleister stellt sicher, dass keine Unbefugten Zugriff auf die Daten erlangen können.

ab Schutzbedarf „hoch“

4. Der Dienstleister führt regelmäßig Wiederherstellungsübungen der gesicherten Daten durch.
5. Der Dienstleister erstellt regelmäßig einen Bericht über die durchgeführten und fehlgeschlagenen Datensicherungen und Wiederherstellungsübungen.
6. Der Dienstleister stellt sicher, dass die Sicherungsmedien durch kryptographische Verfahren vor unbefugten Zugriff geschützt werden. Er stellt sicher, dass die Schlüssel zu diesen Archiven getrennt und angemessen geschützt aufbewahrt werden.

2.14 Archivierung

1. Der Dienstleister dokumentiert für jedes System die Rahmenbedingungen für die jeweiligen Archivdaten (mindestens Zeiträume, Sicherungsart, Medien, Aufbewahrungsfristen, Löschfristen).
2. Der Dienstleister stellt sicher, dass alle Daten den Vorgaben entsprechend archiviert werden.
3. Der Dienstleister stellt sicher, dass Unbefugte keinen Zugriff auf die Daten erlangen können.
4. Der Dienstleister stellt sicher, dass nach Eintreten der Löschfrist die Daten sicher gelöscht werden.

ab Schutzbedarf „hoch“

5. Der Dienstleister führt regelmäßig oder nach Änderungen an den Komponenten des Archivsystems Wiederherstellungsübungen der archivierten Daten durch.
6. Der Dienstleister erstellt regelmäßig einen Bericht über die durchgeführten und fehlgeschlagenen Archivierungen und Wiederherstellungsübungen.
7. Der Dienstleister stellt sicher, dass die Sicherungsmedien durch kryptographische Verfahren vor unbefugten Zugriff geschützt werden. Er stellt sicher, dass die Schlüssel zu diesen Archiven getrennt und angemessen geschützt aufbewahrt werden.

2.15 Kryptokonzept

1. Der Dienstleister führt für jedes IT-System eine Dokumentation aller verwendeten kryptografischen Verfahren.
2. Er stellt mindestens einmal jährlich oder ggf. bei neuen Erkenntnissen zu den kryptografischen Verfahren sicher, dass die verwendeten Verfahren und Schlüssellängen den offiziellen Empfehlungen gemäß BSI TR-02102-1 entsprechen.
3. Alle eingesetzten kryptografischen Verfahren, die nicht den offiziellen Empfehlungen entsprechen sind an die ILB zu melden.
4. Der Dienstleister stellt sicher, dass die Vorgaben zur sicheren Erzeugung, Übermittlung, Speicherung, Wechsel und Vernichtung von kryptografischen Schlüsseln definiert und umgesetzt werden.

2.16 Löschung und Vernichtung

1. Es muss festgelegt werden, wie alle Informationen, Daten und ggf. Hardware der ILB vom Dienstleister zurückgegeben werden.
2. Im Falle einer Beendigung des Vertrages muss der Dienstleister sicherstellen, dass alle Daten der ILB vernichtet oder an die ILB zurückgegeben werden. Hierbei sind gesetzliche Vorgaben zur Aufbewahrung von Daten zu beachten.

ab Schutzbedarf „hoch“

3. Alle Datenträger, die Daten der ILB enthalten und nicht mehr benötigt werden oder defekt sind, sind durch den Dienstleister angemessen zu vernichten. Die ILB erhält entsprechende Nachweise der Vernichtung.

2.17 Physische Sicherheit

1. Der Dienstleister stellt durch Zutrittsbeschränkungen sicher, dass keine Unbefugten Zutritt zu den IT-Systemen, worauf Daten der ILB verarbeitet bzw. gespeichert werden, erhalten können.
2. Wände, Türen und Fenster der Gebäudeaußenhaut sind grundsätzlich analog der Widerstandsklasse RC2 N auszuführen.
3. Die IT-Systeme müssen so betrieben werden, dass sie mit ausreichend Energie versorgt werden und das gesamte Jahr über eine geeignete Klimatisierung sichergestellt wird.
4. Es muss durch den Dienstleister sichergestellt werden, dass durch Spannungsschwankungen oder kurze Stromausfälle keine Auswirkungen auf die IT-Systeme und deren Kommunikationsverbindungen entstehen.
5. Die für die ILB relevanten IT-Systeme müssen in brand- und rauchgeschützten Räumen betrieben werden. Bei etwaigen Bränden im Umfeld der IT-Systeme ist eine umgehende Alarmierung der Feuerwehr notwendig. Eine angemessene Löschung im Umfeld der IT-Systeme ist im Vorfeld durch den Dienstleister mit der Feuerwehr abzustimmen.
6. Zur Vermeidung von Wasserschäden sind folgende Aspekte zu berücksichtigen:
   - Gebäudebereiche, die einer besonderen Gefährdung durch Wassereinbrüche ausgesetzt sind (z. B. Kellerbereiche).
   - Flüssigkeitsführende Leitungen (z. B. Wasserleitungen) innerhalb von Räumen.

ab Schutzbedarf „hoch“

7. Standorte bzw. Gebäude sind in Sicherheitszonen (z. B. Außenbereich, kontrollierter Innenbereich, interner Bereich, Sicherheitsbereich) zu unterteilen und zu dokumentieren.
8. Außentüren und -fenster von Gebäuden, die öffentlich zugänglich bzw. erhöhten Einbruchrisiken ausgesetzt sind (z. B. Fenster im Erdgeschossbereich) und in denen Sicherheitszonen mit hohem Schutzbedarf oder höher untergebracht sind, müssen grundsätzlich gemäß der Widerstandsklasse RC3 ausgeführt werden. Sofern die betreffenden Türen und Fenster mittels Gefahrenmeldeanlage überwacht werden, ist die Ausführung gemäß der Widerstandsklasse RC2 N ausreichend
9. IT-Räume des Dienstleisters, in denen die für die ILB relevanten IT-Systeme aufbewahrt werden, haben Löschanlagen, die bei einem Brand das Feuer bekämpfen können.
10. Der Dienstleister stellt sicher, dass auch bei längerfristigen Stromausfällen keine Ausfälle der für die ILB relevanten IT-Systeme und Kommunikationsverbindungen auftreten (z.B. Netzersatzanlage, zweite Stromeinspeisung).
11. Alle für die Aufrechterhaltung der Stromversorgung und Klimatisierung notwendigen Geräte sind redundant ausgelegt, so dass der Ausfall einzelner Geräte keine Auswirkungen auf die für die ILB relevanten IT-Systeme haben.

ab Schutzbedarf „sehr hoch“

12. Sicherheitszonen, die IKT-Infrastruktur beherbergen (bspw. Serverräume oder Rechenzentren) dürfen keine Fenster besitzen, die aus öffentlich zugänglichen Bereichen erreichbar sind.
13. Diese Zonen sollten grundsätzlich nicht in Gebäudebereichen liegen, die einer besonderen Gefährdung durch Wassereinbrüche ausgesetzt sind (z. B. Kellerbereiche).
14. In diesen Zonen dürfen keine flüssigkeitsführenden Leitungen (z. B. Wasserleitungen) innerhalb des Raums vorhanden sein.

2.18 Berücksichtigung der Gefährdungs- und Gesetzeslage

ab Schutzbedarf „hoch“

1. Die vereinbarten Sicherheitsanforderungen müssen bei Änderung der Gefährdungslage für die Technik sowie bei Änderung der Gesetzeslage für die erbrachte Dienstleistung durch den Dienstleister nachgebessert werden.

2.19 Risiko- und Informationssicherheitsberichte

1. Der Dienstleister stellt der ILB jährlich einen Risikobericht zur Verfügung (ggf. Risikoberichterstattung gemäß AT 9 der MaRisk). Der Risikobericht enthält mindestens Auskunft über die folgenden Punkte:
   - Wie die Informationssicherheit für die Dienstleistung gewährleistet wird.
   - Wie die vereinbarten Regelungen aus dieser Anlage umgesetzt werden.
   - Ob Kontrollen für die vereinbarten Regelungen aus dieser Anlage effektiv sind.
   - Identifizierte Informationssicherheitsrisiken und deren Behandlung
   - Welche Informationssicherheitsvorfälle mit Bezug zur ILB seit dem letzten Risikobericht aufgetreten sind.
   - Eine Bewertung der aktuellen Risikosituation für die Dienstleistung.

(vierteljährlicher Risikobericht bei kritischen wichtigen Funktionen oder wesentlichen Auslagerungen)

ab Schutzbedarf „hoch“

1. Wenn Risikoanalysen notwendig sind, sind Vereinbarungen zu treffen, wie die Risikoanalyse geprüft und gegebenenfalls in das eigene Risikomanagement überführt werden kann.
2. Der Dienstleister ist verpflichtet, dem Auftraggeber mindestens einmal pro Kalenderjahr einen Informationssicherheitsbericht zur Verfügung zu stellen, der in Bezug auf die Leistungserbringung mindestens die folgenden Informationen zu sicherheitsrelevanten Themen enthält:
   - Angemessenheit der Aufbau- und Ablauforganisation sowie der Personal- und Ressourcenausstattung im ISMS
   - Aktualität der Informationssicherheitsdokumentation (Strategie, Leitlinien/Richtlinien, Informationssicherheitsprozess etc.)
   - Die grundsätzliche Einhaltung der vertraglich vereinbarten Sicherheitsmaßnahmen
   - Sachstand und Entwicklung zu Informationssicherheitsvorfällen
   - Gesamtübersicht zu durchgeführten Schwachstellenscans und deren Ergebnisse
   - Gesamtübersicht zu durchgeführten Penetrationstests und deren Ergebnisse
   - Ergebnisse aus durchgeführten Sicherheitsaudits der ISMS-Organisation

- Durchgeführte Security Awareness Maßnahmen und
- Relevante Ergebnisse der Internen Revision und Drittprüfer (z. B. Wirtschaftsprüfer) mit Bezug zum ISMS des Auftragsnehmers sowie sicherheitsrelevante Feststellungen im Zusammenhang mit der ausgelagerten Leistungserbringung (z. B. verwendete IT-Systeme, Gebäudesicherheitssysteme).

3 Sicherheit von Cloud-Diensten

3.1 Festlegung von Verantwortungsbereichen und Schnittstellen

1. Für die bereitgestellten Cloud-Dienste muss der Dienstleister alle relevanten Schnittstellen zur ILB und Verantwortlichkeiten für die Cloud-Nutzung identifizieren und dokumentieren. Dies müssen mindestens die folgenden Punkte beinhalten:
   - Schnittstellen,
   - Netzanbindung,
   - Administrationsmodell sowie
   - Datenmanagementmodell.
2. Bei Anpassung der Schnittstellen des durch die ILB bezogenen Cloud-Dienstes durch den Dienstleister muss dieser eine Mitteilung über die Anpassung an die ILB bereitstellen.
3. Der Dienstleister muss in einer Dokumentation klar erkennbar machen, wie die Verantwortungsbereiche zwischen Cloud-Dienst und der ILB voneinander abgegrenzt sind.

3.2 Vertragsgestaltung mit dem Cloud-Dienstanbieter

1. Der Dienstleister stellt der ILB für die bezogenen Cloud-Dienste die folgenden Informationen zur Verfügung:
   - Standort der Leistungserbringung der Cloud-Dienste.
   - Es sind entsprechende Eskalationsstufen und Kommunikationswege zu definieren, zu dokumentieren und dem Vertrag beizufügen sind.
   - Der Dienstleister verpflichtet seine Mitarbeitende, beobachtete oder vermutete Vorfälle im Bereich der Informationssicherheit und anomale Verhaltensweisen rechtzeitig zu melden. Die mit der ILB vereinbarten Meldemechanismen sind zu kennen und einzuhalten.
   - Es muss festgelegt werden, wie alle Informationen, Daten und ggf. Hardware der ILB vom Dienstleister zurückgegeben werden. Hierbei sind gesetzliche Vorgaben zur Aufbewahrung von Daten zu beachten.
   - Alle Subunternehmenden des Dienstleisters, die für die Bereitstellung der durch die ILB bezogenen Cloud-Dienste benötigt werden.

3.3 Erstellung eines Notfallkonzeptes für einen Cloud-Dienst

1. Für die genutzten Cloud-Dienste muss der Dienstleister in Abstimmung mit der ILB ein Notfallkonzept erstellen.
2. Das Notfallkonzept muss alle notwendigen Angaben zu Zuständigkeiten und Ansprechpersonen enthalten.
3. Es müssen detaillierte Regelungen hinsichtlich der Datensicherung getroffen werden.
4. Vorgaben zu Redundanzen (z. B. Management-Tools, Schnittstellensysteme) müssen im Notfallkonzept enthalten sein.

3.4 Aufrechterhaltung der Informationssicherheit im laufenden Cloud-Nutzungs-Betrieb

1. Der Dienstleister muss regelmäßige, mindestens jedoch jährliche, Abstimmungstermine mit der ILB bzgl. der Aufrechterhaltung der Informationssicherheit im laufenden Cloud-Nutzungs-Betrieb durchführen.
2. Die Reaktion auf Systemausfälle muss durch den Dienstleister dokumentiert, geplant und geübt werden.

3.5 Verschlüsselung

1. Die Kommunikation mit der Cloud-Umgebung und innerhalb der Cloud-Infrastruktur muss über verschlüsselte Kanäle nach dem Stand der Technik erfolgen
2. Cloud Dienstleister müssen sicherstellen, dass die Daten der ILB zu jedem Zeitpunkt ausreichend durch Verschlüsselung vor fremden Zugriff geschützt sind.

3.6 Nachweis einer ausreichenden Informationssicherheit bei der Cloud-Nutzung

ab Schutzbedarf „hoch“

1. Der Dienstleister weist die Informationssicherheit für die Cloud-Dienste anhand eines Zertifikats nach, das auf einem international anerkannten Regelwerk basiert (z. B. ISO 27001 Zertifizierung auf Basis von IT-Grundschutz, ISO/IEC 27001, Anforderungskatalog Cloud-Computing (C5) Testat Typ-1 bzw. Typ-2, Cloud Controls Matrix der Cloud Security Alliance).
2. Nutzt der Dienstleister Subunternehmende, um die Cloud-Dienste zu erbringen, muss der ILB jährlich und anlassbezogen nachgewiesen werden, dass diese die notwendigen Audits durchführen.
3. Der Dienstleister ist verpflichtet, alle Schutzbedarfsanforderungen auch bei seinen Subunternehmen, die mit der Erbringung der Dienstleistung befasst sind, durchzusetzen. Es muss sichergestellt sein, dass die Anforderungen der ILB von allen mit dem Service befassten Subunternehmern eingehalten werden.

3.7 Sicherstellung der Portabilität von Cloud-Diensten

1. Die ILB muss jederzeit in der Lage sein, auf die in der Cloud gespeicherten Daten zuzugreifen und diese auch bei Bedarf zurückführen können.

ab Schutzbedarf „hoch“

2. Der Dienstleister muss für die durch die ILB bezogenen Cloud-Dienste definieren, welche Daten wie zu sichern sind und wie Wiederherstellungstests erfolgen.
3. Diese Datensicherung und Wiederherstellungstest müssen anlassbezogen und regelmäßig, jedoch mindestens jährlich, erfolgen.