

Berichte und Reports

Diese Anlage konkretisiert die Berichtspflichten des Auslagerungsunternehmens.

Die Berichte sind von der vertraglichen Vergütung für die Vertragsleistungen umfasst und sind nicht gesondert zu vergüten. Sofern in dieser Anlage nichts anderes bestimmt ist, sind die Berichte **spätestens innerhalb von 2 Wochen nach dem jeweiligen Monats-, Quartals- bzw. Jahresende** zu liefern.

Folgende Berichte / Reports werden dem Auftraggeber in Bezug auf den ausgelagerten Sachverhalt bereitgestellt:

Berichtsart	Berichtsinhalt und Zweck	Turnus
Service Level-Report	Übersicht über Störungen in Prozessen und Systemen (inkl. Service Level-Verletzungen) unter Angabe des Service Levels und Verursacher der Störung	monatlich
Incident Management	Übersicht der protokollierten, gelösten und offenen Vorfälle; Anzahl der wiedereröffneten Vorfälle und Reaktionszeit bei schwerwiegenden Vorfällen	monatlich
Problem Management	Status der Ursachenanalyse aller geöffneten Probleme	monatlich
Risiken (Abstimmung IKT-Risikomanagement erforderlich)		
Weiterverlagerungen	Übersicht über alle vom Dienstleister eingesetzten Subunternehmen mit Darstellung der weiterverlagerten Aufgaben sowie einer Einstufung der Wesentlichkeit	halbjährlich
Risikobericht	Darstellung von wesentlichen und nicht wesentlichen Risiken (inkl. Risikoveränderungen): a. Gesamtbewertung zur Risikolage	vierteljährlich

Berichtsart	Berichtsinhalt und Zweck	Turnus
	<ul style="list-style-type: none"> b. Wesentliche Änderungen (ggü. Vorbericht) und Vorfälle c. Veränderung der Risikolage ggü. dem Vorbericht d. Risiken: Überblick, Information, ggf. Verteilung der Risiken e. Risikoarten inkl. Quantifizierung nach Schadenshäufigkeit und Eintrittswahrscheinlichkeit sowie Bewertung als wesentlich/ nicht wesentlich f. Informationen zu wesentlichen (ggf. nicht wesentlichen) Einzelrisiken mit Kundenrelevanz g. Beschreibung begleitender Mitigationsmaßnahmen für alle Risiken (wesentlich/ nicht wesentlich) mit besonderem Augenmerk auf der Risikoreduzierung kritischer und hoher Risiken. Maßnahmen zur Risikoreduzierung sollten klare Daten für Mitigationsmaßnahmen enthalten h. Eine aussagekräftige und inhaltlich nachvollziehbare textlich dargestellte Risikobewertungen. Dazu gehört auch die notwendige verbale Ableitung für den Fall einer zur Verfügung gestellten Risikomatrix 	
Änderungsverfahren		
Change-Request-Bericht	Dokumentation des Status der Änderungen, die im vergangenen Monat implementiert wurden, Fragen im Zusammenhang mit den implementierten Änderungen, identifizierte und geplante Änderungen für den kommenden Monat und die tatsächlichen	monatlich

Berichtsart	Berichtsinhalt und Zweck	Turnus
	oder erwarteten Auswirkungen dieser Änderungen auf die Services	
Notfallmanagement (Abstimmung Notfallmanager erforderlich)		
Notfallvorsorgebericht	Sicherstellung der Kontinuität der vertraglich vereinbarten Leistungen, Notfallkonzept, Protokolle der regelmäßigen Notfalltests, Pentests usw.	zeitnah
abgestimmtes Notfallkonzept (sofern vom Auftraggeber gefordert)	aktuelle Fassung / Version des mit dem Auftraggeber abgestimmten Notfallkonzeptes	zeitnah
Prüfberichte Dritter	Prüfberichte Dritter, sofern diese sich auf Notfallvorsorge sowie vorhandene Notfallkonzepte beziehen	zeitnah
Datenschutz (Abstimmung DSB erforderlich)		
Datenschutzbericht	Darstellung der Datenschutzvorkommnisse, durchgeführte Datenschutz- und IT-Sicherheitsmaßnahmen, in der Berichtsperiode durchgeführte Prüfungen zum Datenschutz, Beurteilung des Niveaus der Datenschutzmaßnahmen, geplante Datenschutz und IT-Sicherheitsmaßnahmen für die nächste Periode.	jährlich
Informationssicherheit (Abstimmung IKT-Risikomanagement erforderlich)		
Risikobericht	Darstellung von wesentlichen und nicht wesentlichen Informationssicherheits- und IKT-Risiken (inkl. Risikoveränderungen)	vierteljährlich
Informationssicherheits- risikobericht	Darstellung von:	jährlich

Berichtsart	Berichtsinhalt und Zweck	Turnus
	<ul style="list-style-type: none"> a. Angemessenheit der Aufbau- und Ablauforganisation sowie der Personal- und Ressourcenausstattung im ISMS; b. Aktualität der Informationssicherheitsdokumentation (Strategie, Leitlinien/Policies, Richtlinien, Informationssicherheitsprozess etc.); c. Die grundsätzliche Einhaltung der vertraglich vereinbarten Sicherheitsmaßnahmen; d. Identifizierte Informationssicherheitsrisiken (ggf. durch separate Risikoberichterstattung gemäß AT 9 der MaRisk zu ersetzen); e. Sachstand und Entwicklung zu Informationssicherheitsvorfällen; f. Gesamtübersicht zu durchgeführten Schwachstellenscans und deren Ergebnisse; g. Gesamtübersicht zu durchgeführten Penetrationstests und deren Ergebnisse; h. Ergebnisse aus durchgeführten Sicherheitsaudits der ISMS-Organisation; i. Durchgeführte Security Awareness Maßnahmen 	
Nachhaltigkeit		
CSR- oder Lagerbericht	Darstellung der gesellschaftlichen Anforderungen im Hinblick auf Umweltschonung, Arbeitnehmerschutz, Achtung der Menschenrechte, Korruptionsbekämpfung, Diversität usw.	Bei Vertragsschluss und danach jährlich
ESG-Fragebogen für Lieferanten	Bestätigung der Beachtung der Nachhaltigkeitsstandards in den Bereichen „Umwelt“ (Environment), „Soziales“ (Social) und „Unternehmensführung“ (Governance)	Beim Vertragsschluss und danach jährlich

Berichtsart	Berichtsinhalt und Zweck	Turnus
Prüfberichte		
Jahresabschlussprüfer Interne Revision Sonstige Prüfberichte	Auszüge der Prüfberichte, sofern diese in Zusammenhang mit der erbrachten Dienstleistung des Auslagerungsunternehmens stehen. Prüffeld-Übersichten (Audit universe) und den Prüfungsplan der Internen Revision des Auslagerungsunternehmens	jährlich
Ergebnisse der Prüfungen der Internen Revision des Auslagerungsunternehmens	Vollständiger Revisionsbericht inklusive der Einzelfeststellungen; die Berichterstattung muss auch Prüfungsergebnisse zu Nebenpflichten (z. B. Datenschutz, BCM, IKS, Informationssicherheit, Personal, ISMS) und Basisleistungen (Infrastruktur, Gebäude, Clouddienste) enthalten. Die Interne Revision des Auslagerungsunternehmens wird insbesondere auch unverzüglich und unaufgefordert über ihre Erkenntnisse berichten, soweit die Ordnungsmäßigkeit, Sicherheit und Verfügbarkeit der Leistungserbringung durch das Auslagerungsunternehmen maßgeblich berührt sind.	Mindestens quartalsweise zu den Stichtagen 31. März., 30. Juni, 30. September und 31. Dezember
Prüfungsbericht unabhängigen anerkannten Prüfungsunternehmens	Prüfungsbericht unabhängigen anerkannten Prüfungsunternehmens z.B. gemäß SOC 2 Type 2; IDW PS 951 Typ 2 oder ISAE 3402 (in ihrer jeweils gültigen Fassung)	jährlich
Ad hoc-Berichterstattung	Ad hoc-Berichterstattung von Prüfungen mit mindestens als „wesentlich“ eingestuften Feststellungen	Unverzüglich
Berichterstattung über den Status sämtlicher Feststellungen	Berichterstattung über den Status sämtlicher Feststellungen und die im jeweiligen Quartal geschlossenen Feststellungen	Mindestens quartalsweise zu den Stichtagen

Berichtsart	Berichtsinhalt und Zweck	Turnus
		31.3., 30.6., 30.9. und 31.12.
Erledigungsnachweise	Erledigungsnachweise für aus Sicht des auslagernden Instituts mindestens als „wesentlich“ eingestuften Feststellungen, wobei das auslagernde Institut das Auslagerungsunternehmen über die aus seiner Sicht mindestens als „wesentlich“ eingestuften Feststellungen informieren wird und berechtigt ist, stichprobenartig Erledigungsnachweise für weitere, von ihm bestimmte Feststellungen anzufordern	jährlich
Ergebnisse aufsichtsrechtlicher Prüfungen	Ergebnisse aufsichtsrechtlicher Prüfungen (z. B. nach Art. 12 der EU-Verordnung 1024/2013 oder § 44 Abs. 1 KWG) mit Relevanz für den ausgelagerten Bereich oder die Interne Revision des Auslagerungsunternehmens	Unverzüglich nach Veröffentlichung
Ergebnisse externer Quality Assessments	Ergebnisse externer Quality Assessments der Internen Revision des Auslagerungsunternehmens, welche das Auslagerungsunternehmen mindestens gem. den Empfehlungen des Institute of Internal Auditors (IIA) durchführt	Unverzüglich nach Veröffentlichung (mind. alle 5 Jahre)
Berichterstattung über die Abarbeitung von Feststellungen in externen Prüfungsberichten	Berichterstattung über die Abarbeitung von Feststellungen in externen Prüfungsberichten, soweit eine Relevanz für den ausgelagerten Bereich oder die Interne Revision des Auslagerungsunternehmens besteht	Mindestens jährlich
Versicherung(en)		
Versicherungsnachweise	Nachweis einer gültigen Versicherungspolice zur Abdeckung von Risiken, welche mit dem Auslagerungsgegenstand korrelieren	jährlich