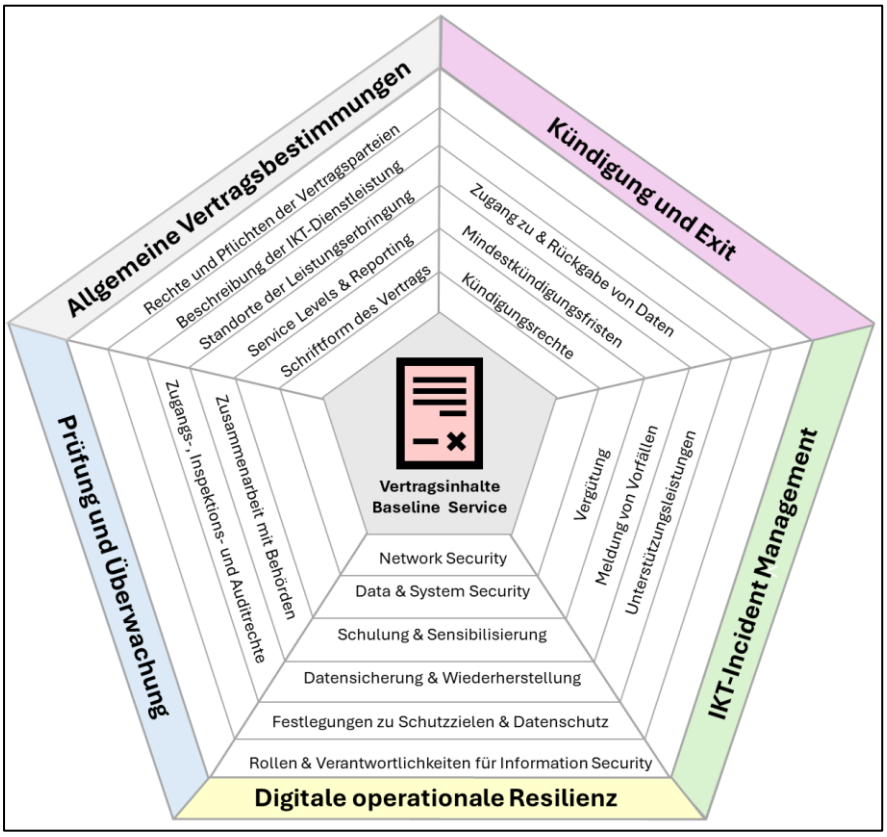
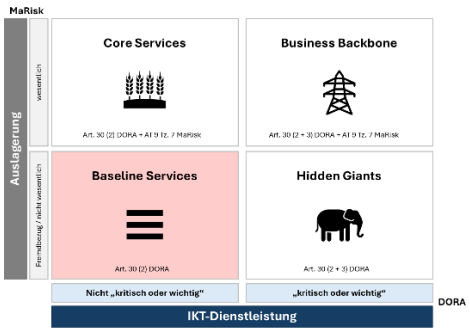
DORA-Mindestvertragsinhalte für Baseline Services

- Ein Cheatsheet aus der DORA-Werkstatt -

DISCLAIMER: Das Cheatsheet dient als Orientierungshilfe für die erste Einschätzung, welche Mindestvertragsinhalte gemäß DORA-Verordnung in einen IKT-Vertrag aufgenommen werden müssen. Das Cheatsheet ist nicht rechtsverbindlich und ersetzt keine juristische Prüfung.





Baseline Services: Verträge in diesem Quadranten betreffen IKT-Dienstleistungen, die weder für die Finanzstabilität noch für die tägliche Funktionsfähigkeit des Unternehmsens von zentraler Bedeutung sind. Sie werden weder als wesentliche Auslagerungen gemäß MaRisk betrachtet noch haben sie eine Relevanz für kritische oder wichtige Funktionen nach DORA. Die Risiken, die mit solchen IKT-Verträgen verbunden sind, sind vergleichsweise gering, weshalb auch die Anforderungen an die Verträge weniger anspruchsvoll sind.

	Vertragsinhalt	Auszug aus dem Rechtstext
Allgemeine Vertragsbestimmungen	Schriftform des Vertrags	Die Rechte und Pflichten des Finanzunternehmens und des IKT-Drittdienstleisters werden eindeutig zugewiesen und schriftlich dargelegt. Der vollständige Vertrag umfasst die Vereinbarung über die Dienstleistungsgüte und wird in einem schriftlichen Dokument, das den Parteien in Papierform zur Verfügung steht, oder in einem Dokument in einem anderen herunterladbaren, dauerhaften und zugänglichen Format dokumentiert (Art. 30 Abs. 1 DORA)
	Beschreibung der IKT-Dienstleistung	eine klare und vollständige Beschreibung aller Funktionen und IKT-Dienstleistungen, die der IKT-Drittdienstleister bereitzustellen hat, [...] (Art. 30 Abs. 2 lit. a DORA)
	Rechte und Pflichten der Vertragsparteien	eine klare und vollständige Beschreibung aller Funktionen und IKT-Dienstleistungen, die der IKT-Drittdienstleister bereitzustellen hat, [...] (Art. 30 Abs. 2 lit. a DORA)
	Standorte der Leistungserbringung	die Standorte — das heißt die Regionen oder Länder —, an denen die vertraglich vereinbarten oder an Unterauftragnehmer vergebenen Funktionen und IKT-Dienstleistungen bereitzustellen sind und an denen Daten verarbeitet werden sollen, einschließlich des Speicherorts, sowie die Auflage für den IKT-Drittdienstleister, das Finanzunternehmen vorab zu benachrichtigen, wenn er eine Änderung dieser Standorte beabsichtigt (Art. 30 Abs. 2 lit. b DORA)
	Service Levels und Reporting	Beschreibungen der Dienstleistungsgüte, einschließlich Aktualisierungen und Überarbeitungen (Art. 30 Abs. 2 lit. e DORA)
Kündigung und Exit	Kündigungsfristen	Kündigungsrechte und damit zusammenhängende Mindestkündigungsfristen für die Beendigung der vertraglichen Vereinbarungen entsprechend den Erwartungen der zuständigen Behörden und der Abwicklungsbehörden (Art. 30 Abs. 2 lit. h DORA)
	Datenzugang zu und Rückgabe von Daten	Bestimmungen über die Sicherstellung des Zugangs zu personenbezogenen und nicht personenbezogenen Daten, die von dem Finanzunternehmen im Fall einer Insolvenz, Abwicklung, Einstellung der Geschäftstätigkeit des IKT-Drittdienstleisters oder einer Beendigung der vertraglichen Vereinbarungen verarbeitet werden, sowie über die Wiederherstellung und Rückgabe dieser Daten in einem leicht zugänglichen Format (Art. 30 Abs. 2 lit. d DORA)
	Kündigungsrechte	Finanzunternehmen stellen sicher, dass vertragliche Vereinbarungen über die Nutzung von IKT-Dienstleistungen gekündigt werden können, wenn einer der folgenden Umstände vorliegt: • ein erheblicher Verstoß des IKT-Drittdienstleisters gegen geltende Gesetze, sonstige Vorschriften oder Vertragsbedingungen; • Umstände, die im Laufe der Überwachung des IKT-Drittparteienrisikos festgestellt wurden

		und die als geeignet eingeschätzt werden, die Wahrnehmung der im Rahmen der vertraglichen Vereinbarung vorgesehenen Funktionen zu beeinträchtigen, einschließlich wesentlicher Änderungen, die sich auf die Vereinbarung oder die Verhältnisse des IKT-Drittdienstleisters auswirken; • nachweisliche Schwächen des IKT-Drittdienstleisters in Bezug auf sein allgemeines IKT-Risikomanagement und insbesondere bei der Art und Weise, in der er die Verfügbarkeit, Authentizität, Sicherheit und Vertraulichkeit von Daten gewährleistet, unabhängig davon, ob es sich um personenbezogene oder anderweitig sensible Daten oder nicht personenbezogene Daten handelt; • die zuständige Behörde kann das Finanzunternehmen infolge der Bedingungen der jeweiligen vertraglichen Vereinbarung oder der mit dieser Vereinbarung verbundenen Umstände nicht mehr wirksam beaufsichtigen. (Art. 28 Abs. 7 DORA)
Digitale operationale Resilienz	Festlegungen zu Schutzzielen & Datenschutz	Bestimmungen über Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit in Bezug auf den Datenschutz, einschließlich des Schutzes personenbezogener Daten (Art. 30 Abs. 2 lit. c DORA)
	Schulung & Sensibilisierung	Bedingungen für die Teilnahme von IKT-Drittdienstleistern an den von den Finanzunternehmen angebotenen Programmen zur Sensibilisierung für IKT-Sicherheit und Schulungen zur digitalen operationalen Resilienz [...] (Art. 30 Abs. 2 lit. i DORA
	Data & System Security	Das [...] Verfahren für die Daten- und Systemsicherheit umfasst [...]: • [...] für IKT-Assets oder -Dienstleistungen, die von einem IKT- Drittdienstleister betrieben werden, die Ermittlung und Umsetzung von Anforderungen an die Aufrechterhaltung der digitalen operationalen Resilienz im Einklang mit den Ergebnissen der Datenklassifizierung und der IKT-Risikobewertung. • Für die Zwecke von Buchstabe k berücksichtigen Finanzunternehmen Folgendes: die Implementierung der vom Anbieter empfohlenen Einstellungen für Komponenten, die vom Finanzunternehmen betrieben werden (Art. 11 (2k) RTS RMF)
	Rollen & Verantwortlichkeiten für Information Security	Für die Zwecke von Buchstabe k berücksichtigen Finanzunternehmen Folgendes: • [...] b) eine klare Aufteilung der die Informationssicherheit betreffenden Aufgaben und Verantwortlichkeiten zwischen dem Finanzunternehmen und dem IKT-Drittdienstleister im Einklang mit dem in Artikel 28 Absatz 1 Buchstabe a der Verordnung (EU) 2022/2554 genannten Grundsatz der vollen Verantwortlichkeit des Finanzunternehmens für seinen IKT-Drittdienstleister und für Finanzunternehmen nach Artikel 28 Absatz 2 der genannten Verordnung sowie im Einklang mit der Richtlinie des Finanzunternehmens für die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen (Art. 11 (2k, b) RTS RMF)
	Datensicherung & Wiederherstellung	Bei der Festlegung der Vorgaben für die Wiederherstellungszeit und die Wiederherstellungspunkte jeder Funktion berücksichtigen die Finanzunternehmen, ob es sich um eine kritische oder wichtige Funktion handelt, sowie die potenziellen Gesamtauswirkungen auf die Markteffizienz. Mit diesen Zeitvorgaben ist sichergestellt, dass die vereinbarte Dienstleistungsgüte in Extremszenarien erreicht werden. (Art. 12 Abs. 6 DORA)
	Network Security	Die Finanzunternehmen entwickeln, dokumentieren und implementieren [...] für Vereinbarungen über Netzwerkdienstleistungen: • i) die Ermittlung und Spezifikation von IKT- und Informationssicherheitsmaßnahmen, der Dienstleistungsgüte und von Managementanforderungen für alle Netzwerkdienste; • ii) die Feststellung, ob diese Dienstleistungen von einem gruppeninternen IKT-Dienstleister oder von IKT- Drittdienstleistern erbracht werden. (Art. 13 (m) RTS RMF)
IKT-Incident Managemnent	Unterstützungsleistungen	die Verpflichtung des IKT-Drittdienstleisters, dem Finanzunternehmen bei einem IKT-Vorfall, der mit dem für das Finanzunternehmen bereitgestellten IKT-Dienst in Verbindung steht, [...] Unterstützung zu leisten (Art. 30 Abs. 2 lit. f DORA)
	Vergütung	die Verpflichtung des IKT-Drittdienstleisters [...] ohne zusätzliche Kosten oder zu vorab festzusetzenden Kosten Unterstützung zu leisten (Art. 30 Abs. 2 lit. f DORA)
	Meldung von Vorfällen	• ii) Meldung schwerwiegender IKT-bezogener Vorfälle und — auf freiwilliger Basis — erheblicher Cyberbedrohungen an die zuständigen Behörden; • iii) Meldung schwerwiegender zahlungsbezogener Betriebs- oder Sicherheitsvorfälle durch in Artikel 2 Absatz 1 Buchstaben a bis d aufgeführte Finanzunternehmen an die zuständigen Behörden; (Art. 1 Abs. 1 lit. a) Ziffer (ii + iii) DORA
Prüfung und Überwachung	Zusammenarbeit mit Behörden	die Verpflichtung des IKT-Drittdienstleisters, vollumfänglich mit den für das Finanzunternehmen zuständigen Behörden und Abwicklungsbehörden zusammenzuarbeiten, einschließlich der von diesen benannten Personen (Art. 30 Abs. 2 lit. g DORA)
	Zugangs-, Inspektions- und Auditrechte	Bei der Ausübung der Zugangs-, Inspektions- und Auditrechte in Bezug auf den IKT-Drittdienstleister bestimmen Finanzunternehmen auf der Grundlage eines risikobasierten Ansatzes vorab die Häufigkeit von Audits und Inspektionen sowie die zu prüfenden Bereiche, [...] (Art. 28 Abs. 6 DORA)