***Hinweis:** Grau hinterlegte Artikel sind für Finanzunternehmen nur indirekt relevant, da sie insb. Anforderungen an die involvierten Behörden spezifizieren.

Übersicht über die DORA-Verordnung		Zusammenfassung	Übersicht über Regulatory Technical Standards (RTS), Implementing Technical Standards (ITS) & Joint Guidelines (JGL).
KAPITEL I - Allgemeine Bestimmungen			
Artikel 1 - 4		Gegenstand, Geltungsbereich, Begriffsbestimmungen, Grundsatz der Verhältnismäßigkeit der DORA-Verordnung	
KAPITEL II - IKT-Risikomanagement			
Artikel 5	Governance und Organisation	Aufgaben, Verantwortung und Anforderungen an die Geschäftsleitung	
Artikel 6	IKT-Risikomanagementrahmen	Mindestanforderungen an die Ausgestaltung und Dokumentation des IKT-Risikomanagementrahmens	
Artikel 7	IKT-Systeme, -Protokolle und -Tools	Anforderungen an IKT-Systeme, -Protokolle und –Tools mit Bezug zu deren Aktualität, Zuverlässigkeit und Resilienz	
Artikel 8	Identifizierung	Anforderungen an die Identifizierung und Dokumentation von Informations- sowie IKT-Assets und IKT-Risiken	
Artikel 9	Schutz und Prävention	Anforderungen an die Überwachung von IKT-Systemen und –Tools sowie Anforderung zur Nutzung von IKT-Sicherheitstools sowie der Erstellung von Sicherheitsrichtlinien und –Verfahren	
Artikel 10	Erkennung	Anforderung zur Nutzung von Tools und Verfahren zur Erkennung von Schwachstellen, anomalen Aktivitäten in Netzwerken und IKT-Incidents	
Artikel 11	Reaktion und Wiederherstellung	Anforderungen an das (IT-) Notfallmanagement, insb. Erstellung, Pflege und Tests von IKT-Geschäftsfortführungsleitlinie, IKT-Reaktions- und Wiederherstellungsplänen sowie Krisenkommunikationsplänen und Beauftragung der ESA zur Erstellung von Leitlinien für die Schätzung der aggregierten jährlichen Kosten und Verluste	**Konkretisierung zu Art. 11.11** DRAFT (2nd wave): JC 2023 68 **JGL** on the estimation of aggregated annual costs and losses caused by major ICT-related incidents
Artikel 12	Richtlinie und Verfahren zum Backup sowie Verfahren und Methoden zur Wiedergewinnung und Wiederherstellung	Anforderungen an die Verfahren zur Datensicherung sowie Wiedergewinnungs- und Wiederherstellungsverfahren	
Artikel 13	Lernprozesse und Weiterentwicklung	Anforderungen an Ursachenanalyse und Verbesserungspotential bei der Bewältigung von schwerwiegenden IKT-Incidents, sowie Schulungs- und Awarenesstrainings	
Artikel 14	Kommunikation	Anforderungen an die Erstellung von Kommunikationsstrategien & -pläne mit Kunden und Öffentlichkeit	
Artikel 15	Weitere Harmonisierung von Tools, Methoden, Prozessen und Richtlinien für IKT-Risikomanagement	Mandatierung der ESA zur Erstellung von technischen Regulierungsstandards zu geforderten Richtlinien, Verfahren, Protokollen und Tools für das IKT-Risikomanagement	**Konkretisierung zu Art. 15 und 16.3** FINAL (1st wave): JC 2023 86 **RTS** to further harmonise ICT risk management tools, methods, processes and policies as mandated under Articles 15 and 16(3)
Artikel 16	Vereinfachter IKT-Risikomanagementrahmen		
KAPITEL III - Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle			
Artikel 17	Prozess für die Behandlung IKT-bezogener Vorfälle	Anforderungen zur Einrichtung eines IKT-Incident Management Prozesses	
Artikel 18	Klassifizierung von IKT-bezogenen Vorfällen und Cyberbedrohungen	Anforderungen an die Klassifikation von IKT-Incidents und Mandatierung der ESA zur Erstellung von technischen Regulierungsstandards zur Festlegung von Klassifikationskriterien	**Konkretisierung zu Art. 18.3** FINAL (1st wave): JC 2023 83 **RTS** specifying the criteria for the classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats
Artikel 19	Meldung schwerwiegender IKT-bezogener Vorfälle und freiwillige Meldung erheblicher Cyberbedrohungen	Anforderungen an die Meldepflichten zu IKT-Incidents	
Artikel 20	Harmonisierung von Inhalt und Vorlagen von Meldungen	Mandatierung der ESA zur Erstellung von technischen Regulierungsstandards zu Inhalten und Fristen für die IKT-Incident Meldungen sowie Beauftragung der ESA zur Erstellung von ITS zur Festlegung von Standardformularen, Vorlagen und Verfahren zur Meldung eines schwerwiegenden IKT Incidents	**Konkretisierung zu Art. 20.a** DRAFT (2nd wave): **RTS** on the content of the notification and reports for major incidents and significant cyber threats and determining the time limits for reporting major incidents **Konkretisierung zu Art. 20.b** DRAFT (2nd wave): **ITS** on the standard forms, templates and procedures for financial entities to report a major incident and to notify a significant cyber threat
*Artikel 21**	*Zentralisierung der Berichterstattung über schwerwiegende IKT-bezogene Vorfälle*	*Anforderungen an die ESA zur Erstellung von gemeldeten IKT-Incidents*	
*Artikel 22**	*Rückmeldungen von Aufsichtsbehörden*	*Anforderungen an die Aufsichtsbehörden zur Rückmeldung und Unterstützung der Finanzunternehmen bei IKT-Incidents*	
Artikel 23	Zahlungsbezogene Betriebs- oder Sicherheitsvorfälle, die Kreditinstitute, Zahlungsinstitute, Kontoinformations-dienstleister und E-Geld-Institute betreffen	Anwendbarkeit der Anforderungen aus Kapitel III für zahlungsbezogene Betriebs- oder Sicherheitsvorfälle	
KAPITEL IV - Testen der digitalen operationalen Resilienz			
Artikel 24	Allgemeine Anforderungen für das Testen der digitalen operationalen Resilienz	Anforderungen an die Festlegung eines Programms für Tests zur digitalen operationalen Resilienz durch unabhängige interne oder externe Tester	
Artikel 25	Testen von IKT-Tools und -Systemen	Konkretisierung der Testanforderungen, insb. Zur Durchführung von Schwachstellen-bewertung und -scans, Open-Source-Analysen, Netzwerksicherheitsbewertungen, Lückenanalysen, Überprüfungen der physischen Sicherheit, Fragebögen und Scans von Softwarelösungen, Quellcodeprüfungen, szenariobasierte Tests, Kompatibilitätstests, Leistungstests, End-to-End-Tests und Penetrationstests	
Artikel 26	Erweiterte Tests von IKT-Tools, -Systemen und -Prozessen auf Basis von TLPT	Anforderungen an die Durchführung von Threat-Led-Penetration-Testing (TLPT) alle 3 Jahre für kritische oder wichtige Funktionen sowie zugrunde liegenden IKT-Systeme, -Prozesse und –Technologien sowie Mandatierung der ESA zur Erstellung von technischen Regulierungsstandards zur Konkretisierung der TLPT-Anforderungen	**Konkretisierung zu Art. 26.11** DRAFT (2nd wave): JC 2023 72 **RTS** specifying elements related to threat led penetration tests
Artikel 27	Anforderungen an Tester bezüglich der Durchführung von TLPT	Anforderungen an die TLPT-Tester und deren Genehmigung durch die Aufsichtsbehörde	
KAPITEL V - Management des IKT-Drittparteienrisikos			
Abschnitt I: Schlüsselprinzipien für ein solides Management des IKT-Drittparteienrisikos			
Artikel 28	Allgemeine Prinzipien	Anforderungen an die Erstellung einer Strategie für das IKT-Drittparteirisiko-management, eine Leitlinie für die Nutzung von IKT-Dienstleistungen, die Erstellung eines Informationsregisters, die vertraglichen Regelungen mit IKT-Dienstleistern, Prüfungspflichten; die Durchführung von Risikoanalysen, die Vereinbarung von Kündigungsrechten, die Erstellung von Exitstrategien sowie die Mandatierung der ESA zur Erstellung von ITS mit Standardvorlagen des Informationsregisters sowie RTS zu Inhalten der Leitlinie für die Nutzung von IKT-Dienstleistungen	**Konkretisierung zu Art. 28.9** FINAL (1st wave): JC 2023 85 **ITS** on the standard templates for the purposes of the register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers **Konkretisierung zu Art. 28.10** FINAL (1st wave): JC 2023 84 **RTS** to specify the detailed content of the policy in relation to the contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers
Artikel 29	Vorläufige Bewertung des IKT-Konzentrationsrisikos auf Unternehmensebene	Anforderungen an die Ermittlung von Konzentrationsrisiken durch die Nutzung von IKT-Dienstleistungen von IKT-Dienstleistern	
Artikel 30	Wesentliche Vertragsbestimmungen	Anforderungen an die Vertragsinhalte bei IKT-Verträgen sowie Mandatierung der ESA zur Ausarbeitung von RTS zur Konkretisierung von Anforderungen an die Beauftragtung von IKT-Unterauftranehmern	**Konkretisierung zu Art. 30.5** DRAFT (2nd wave): JC 2023 67 **RTS** to specify the elements which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions
Abschnitt II: Überwachungsrahmen für kritische I KT-Drittdienstleister			
Artikel 31	Einstufung kritischer IKT-Drittdienstleister	Anforderungen an die ESA zur Einstufung von kritischen IKT-Dienstleistern	
*Artikel 32**	*Struktur des Überwachungsrahmens*	*Anforderungen an die Einrichtung und Aufgaben eines Überwachungsforums durch die Überwachungsbehörden*	*Konkretisierung zu Art. 32.7* *DRAFT (2nd wave): JC 2023 71 JGL on the oversight cooperation and information exchange between the ESAs and the competent authorities*
*Artikel 33 – Artikel 40**		*Aufgaben, Verantwortlichkeiten, Zusammenarbeit und Befugnisse der Überwachungsbehörde bei der Überwachung von IKT-Dienstleistern, Vorgaben zu Zwangsgeldern, Verpflichtung zur Informationsbereitstellung*	
*Artikel 41**	*Harmonisierung der Voraussetzungen für die Durchführung der Überwachungstätigkeiten*	*Mandatierung der ESA zur Erstellung von RTS zu Informationsinhalten und -Formaten, die durch IKT-Dienstleister für die Überwachung durch die Behörden bereitzustellen sind.*	*Konkretisierung zu Art. 41* *DRAFT (2nd wave): JC 2023 69 RTS on the harmonisation of conditions enabling the conduct of the oversight activities*
Artikel 42	Folgemaßnahmen zuständiger Behörden	Information der Finanzunternehmen durch die Behörden über die Risiken, die beim IKT-Dienstleister festgestellt wurden, Umgang mit den identifizierten Risiken auf Seiten des Finanzunternehmens (z.B. Aussetzung der Nutzung der IKT-Services, Vertragsanpassung, bis hin zur Vertragskündigung)	
*Artikel 43**	*Überwachungsgebühren*	*Gebühren der Überwachung beim IKT-Dienstleister*	
*Artikel 44**	*Internationale Zusammenarbeit*	*Zusammenarbeit der Behörden auf internationaler Ebene*	
KAPITEL VI - Vereinbarungen über den Austausch von Informationen			
Artikel 45	Vereinbarungen über den Austausch von Informationen und Erkenntnissen zu Cyberbedrohungen	Möglichkeiten der Zusammenarbeit zwischen Finanzunternehmen, insb. den Austausch von Informationen zu Cyberbedrohungen	
KAPITEL VII - Zuständige Behörden			
Artikel 46	Zuständige Behörden	Festlegung der Überwachungszuständigkeiten der Einhaltung/ Umsetzung der DORA-Verordnung	
*Artikel 47 – 49**		*Zusammenarbeit auf Behördenebene*	
*Artikel 50 – 56**		*Befugnisse, Informationspflichten, Informations- und Datenschutz der Überwachungsbehörden*	
KAPITEL VIII - Delegierte Rechtsakte			
*Artikel 57**	*Ausübung der Befugnisübertragung*	*Befugnisse zum Erlass delegierter Rechtsakte*	
KAPITEL IX - Übergangs- und Schlussbestimmungen			
*Artikel 58**	*Überprüfungsklausel*	*Überprüfung der DORA-Verordnung bis 17. Januar 2028 der Kommission*	
*Artikel 59 – 63**		*Änderungen der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 909/2014, (EU) Nr. 600/2014, (EU) 2016/1011 zur Herstellung der Konsistenz zur DORA-Verordnung*	
Artikel 64	Inkrafttreten und Anwendung	Die DORA-Verordnung gilt ab 17. Januar 2025	