RTS / ITS / GL	Ref. DORA	Ziele und wesentliche Inhalte	Status
RTS zur Spezifizierung der Elemente, bei der Untervergabe von kritischen oder wichtigen Funktionen [Link Regupedia] JC 2023 67	Art. 30.5	**Zielsetzung:** Standardisierung und Spezifizierung der Elemente, die ein Finanzunternehmen bei der Vergabe von Unteraufträgen für IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen, bestimmen und bewerten muss. **Inhalt:** • **Bewertung der Komplexität und des Risikos:** Sitz des IKT-Subunternehmers, Ort der Datenverarbeitung und -speicherung, Übertragbarkeit und Wiedereingliederung der IKT-Dienste • **Risikobewertung in der Vorvertragsphase und regelmäßig bei Veränderungen**: Überprüfung der Untervergabe einer IKT-Dienstleistung, die kritische oder wichtige Funktionen unterstützt, einschl. Due-Diligence-Prozess • **Beschreibung von Funktionen und Dienstleistungen**: klare Beschreibungen aller IKT-Funktionen und -Dienstleistungen, u.a. Das von IKT-Unterauftragnehmern einzuhaltende Dienstleistungsniveau und IKT-Sicherheitsstandards • **Regulierung der Untervergabe:** Vertragliche Vereinbarungen müssen Zulässigkeit & Bedingungen für Untervergabe von IKT-Dienstleistungen, insbesondere für kritische Funktionen, regeln. • **Anforderungen an Umsetzung und Überwachung:** vertragliche Vereinbarungen für die Untervergabe von IKT-Dienstleistungen, Überwachung der gesamten Untervergabekette. • **Sonderkündigungsrecht**, bei Verstoß von IKT-Dienstleistern gegen unzulässige Unterbeauftragung	**Entwurf** (27.11.2023) Konsultation Abgeschlossen
RTS zum Inhalt der Meldungen und Berichte über schwerwiegende Vorfälle und erhebliche Cyberbedrohungen sowie Festlegung der Fristen für die Meldung schwerwiegender Vorfälle [Link Regupedia] JC 2023 70	Art. 20.a	**Zielsetzung**: Harmonisierung und Straffung des Meldesystems für IKT-bezogene Vorfälle bei Finanzunternehmen in der EU. **Inhalt:** • **Anpassung an NIS2**: Verfahren und Fristen orientieren sich an der Richtlinie (EU) 2022/2555 (NIS2-Standard). • Anforderungen an Meldungen betreffen: **Erstmeldung, Zwischenbericht und Abschlussbericht** • **Fristen für Meldungen**: Erstmeldung innerhalb von 4 Stunden (spätestens 24 Stunden) nach Feststellung des Vorfalls, Zwischenbericht nach max. 72 Stunden, Abschlussbericht spätestens 1 Monat nach Feststellung des Vorfalls • **Inhalt der Meldungen**: 101 Datenpunkte in Meldungen/Berichten zu schwerwiegenden Vorfällen und Cyber-Bedrohungen (u.a. Auswirkungen, Klassifizierung, Vorfallbehandlung, Ursachen, Präventionsmaßnahmen, etc.) • **Verpflichtende und bedingte Datenfelder**: 46 % Angaben verpflichtend, restliche Datenfelder sind abhängig vom Vorfalltyp und Art der Meldung • **Nutzung sicherer Kanäle** und Benachrichtigung der Behörden abweichenden Kanälen oder Fristen • **Verwendung von Standardformularen** für die Meldung erheblicher Cyber-Bedrohungen	**Entwurf** (27.11.2023) Konsultation Abgeschlossen
ITS zu den Standardformularen, Vorlagen und Verfahren zur Meldung eines schwerwiegenden Vorfalls und zur Meldung eines bedeutenden Cyberangriffs [Link Regupedia] JC 2023 70	Art. 20.b	**Zielsetzung:** Festlegung von Standardformularen, Mustertexte und Verfahren für Finanzinstitute zur Meldung schwerwiegender IKT-Vorfälle und zur Meldung erheblicher Cyber-Bedrohungen. **Inhalte:** • Konkretisierung der Vorgaben zur Einreichung von **Erstmeldung, Zwischen- und Abschlussbericht** • **technologie- und meldungsformatneutrale Vorlage** für Meldungen von schwerwiegenden IKT-Vorfällen und erheblichen Cyberbedrohungen • ANHANG I/II: **Vorlagen und Anweisungen für die Meldung größerer IKT-Vorfälle** • ANHANG III/IV: **Vorlagen und Anweisungen für die Meldungen über erhebliche Cyber-Bedrohungen**	**Entwurf** (27.11.2023) Konsultation Abgeschlossen
Leitlinie zur Schätzung der Gesamtkosten und -verluste durch größere IKT-bezogene Vorfälle [Link Regupedia] JC 2023 68	Art. 11.11	**Zielsetzung:** Harmonisierung der Schätzung aggregierter jährlicher Kosten und Verluste durch Finanzinstitute für schwerwiegende IKT-bezogene Vorfälle **Inhalte:** • **Einzelne Schätzung** und **Zusammenfassung** von Bruttokosten und -verluste sowie Nettokosten und -verluste (inkl. Rückflüsse) für alle schwerwiegenden IKT-Vorfälle • **Bruttokosten und -verluste** enthalten u.a. entzogene Gelder oder finanzielle Vermögenswerte; Kosten für den Ersatz oder die Verlagerung von Software; Hardware oder Infrastruktur; Personalkosten, Gebühren aufgrund der Nichteinhaltung vertraglicher Verpflichtungen; Verluste aufgrund von Einnahmeausfällen; Beratungskosten etc. • **Jährliche Meldung** der aggregierten Kosten und Verluste anhand vorgegebener Meldeformulare	**Entwurf** (27.11.2023) Konsultation Abgeschlossen

RTS zu Spezifizierung von Elementen im Zusammenhang mit Penetrationstests [Link Regupedia] JC 2023 72	Art. 26.11	**Zielsetzung:** Definitionen von Aspekten der der fortgeschrittenen Prüfung von IKT-Werkzeugen, -Systemen und -Prozessen auf der Grundlage von TLPT in Übereinstimmung mit dem TIBER-EU-Rahmen. **Inhalte:** • **Definitionen** Kriterien für die Identifizierung von Finanzunternehmen, die bedrohungsorientierte Penetrationstests (TLPT) durchführen müssen • **Festlegung der für TLPT notwendigen Rollen:** TPLP-Cyberteam, Kontrollteam, blaues Team, rotes Team und Anbieter von Bedrohungsdaten • **Erweiterter Rahmen für Testing,** betreffend Szenarien für das gesamte Unternehmen (im Vergleich zu Penetration Tests die sich auf einzelne Systeme beziehen) • **Vorgaben für das Risikomanagement während der gesamten Testphase** • Vorgehen für TLPT-Tests: Vorbereitungsphase, Testphase (mind. 12 Wochen!), Abschlussphase • Einbindung der TLPT-zuständigen Behörde	**Entwurf** (27.11.2023) Konsultation Abgeschlossen
RTS zu Harmonisierung der Bedingungen für die Durchführung der Aufsichtstätigkeiten [Link Regupedia] JC 2023 69	Art. 41	**Zielsetzung:** Klärung der Bedingungen für die harmonisierte Durchführung von Aufsichtstätigkeiten für als kritisch eingestufte IKT-Drittdienstleister (CTPP) . **Inhalte:** • Klärung der Informationen, die ein IKT-Drittdienstleister in seinem Antrag auf Einstufung als kritisch angeben muss. • Festlegung der von IKT-Drittdienstleistern zu übermittelnden Informationen, die für die Erfüllung der Aufgaben des LO (Lead Overseer) erforderlich sind. • Präzisierung der Einzelheiten der Bewertung der von CTPP ergriffenen Maßnahmen durch die zuständigen Behörden auf Grundlage der Empfehlungen des LO. • Konsultationspapier und RTS-Entwurf: Das vorliegende Konsultationspapier und der enthaltene RTS-Entwurf umfassen die technischen Standards für die genannten Bereiche a), b) und d). Punkt c), der sich auf das gemeinsame Prüfungsteam bezieht, wird in einem separaten RTS-Entwurf zu einem späteren Zeitpunkt konsultiert.	**Entwurf** (27.11.2023) Konsultation Abgeschlossen
Leitlinien für die Zusammenarbeit zwischen ESAs und zuständigen Behörden [Link Regupedia] JC 2023 71	Art. 32.7	**Zielsetzung**: Definition von Verfahren und Bedingungen für die Zuweisung und Ausführung von Aufgaben zwischen den zuständigen Behörden und den ESA sowie Einzelheiten zum Informationsaustausch **Inhalte:** • **Neue Rollen und Verantwortlichkeiten:** ESAs und zuständige Behörden (CAs) erhalten neue Rollen und Verantwortlichkeiten im Rahmen des Aufsichtsrahmens. • **LO-Funktion der ESA:** ESAs fungieren als federführende Aufsichtsbehörde (Lead Overseer - LO) für CTPPs, übernehmen Aufsicht, geben Empfehlungen und verfolgen diese nach. • Benennung **kritischer IKT-Drittdienstleister** auf Basis der Auswertung von Informationsregistern der Institute • Definition eines **jährlicher Aufsichtsplans**, Durchführung von Untersuchungen und Prüfungen • **Zusammenarbeit und Informationsaustausch**: Enge Zusammenarbeit und Informationsaustausch zwischen ESAs und CAs sind entscheidend für kohärentes Aufsichtskonzept und gleiche Wettbewerbsbedingungen	**Entwurf** (27.11.2023) Konsultation Abgeschlossen

Regulierung	DORA	Auswirkungen	Status
RTS zum Rahmen für das IKT-Risikomanagement und RTS zum vereinfachten Rahmen für das IKT-**Risikomanagement** [Link Regupedia] JC 2023 39	Art. 15 Art. 16.3	Konkretisierungen der Anforderungen, Methoden & Prozesse zum IKT-Risikomanagement, u.a.: • Technologieneutralität, sektorübergreifend und Verhältnismäßigkeit, • IKT-Sicherheitsstrategien, -verfahren, -protokolle und -werkzeuge, • Managementregeln, • IKT-Risikomanagement, • IKT-Assetmanagement, • Verschlüsselung und Kryptografie, • Sicherheit des IKT-Betriebs und Sicherheit von Netzwerken.	**Entwurf** (13.06.2023) Konsultation Abgeschlossen
RTS zu Kriterien für die Klassifizierung von IKT-Vorfällen [Link Regupedia] JC 2023 34	Art. 18.3	Konkretisierung von Kriterien für einheitliche Methoden zur Klassifizierung von Vorfällen, um Schweregrad und die Dringlichkeit von Vorfällen besser einzuschätzen und geeignete Maßnahmen zu deren Bewältigung zu ergreifen, u.a.: • Kriterien und Signifikanzschwellen für die Bestimmung erheblicher Cyber-Bedrohungen, • Kriterien für die zuständigen Behörden zur Beurteilung der Relevanz von Vorfällen, • Kunden, finanzielle Gegenparteien und betroffene Transaktionen.	**Entwurf** (13.06.2023) Konsultation Abgeschlossen
ITS zur Erstellung von Vorlagen für das Informationsregister [Link Regupedia] JC 2023 36	Art. 28.9	Konkretisierung der Vorgaben für das Informationsregister zur Dokumentation und Aufbewahrung relevanter Informationen, z.B. über IT-Systeme, kritische Dienstleistungen und Outsourcing-Vereinbarungen, u.a: • Anwendungsbereich in Bezug auf den Verträgen des Informationsregisters, • Struktur des Informationsregisters, • Vertragsstruktur und Dokumentation, • Vorlagen als Flache Tabelle oder in einer Relationalen Struktur entwickeln, • Verwendung des LEI-Codes zur Identifizierung von Finanzunternehmen.	**Entwurf** (13.06.2023) Konsultation Abgeschlossen
RTS zum Umgang mit IKT-Diensten, die von IKT-Drittdienstleistern bereitgestellt werden [Link Regupedia] JC 2023 35	Art. 28.10	Konkretisierung der Regelungen zur Nutzung von IKT-Dienstleistungen und Anforderungen an das Risikomanagement, die Sicherheit, die Überwachung und die Kontrolle von IKT-Drittanbietern, u. a: • Verhältnismäßigkeitsprinzip, • Überwachung der Vertraglichen Vereinbarungen über die Nutzung von IKT-Diensten zu Unterstützung Kritische oder wichtige Funktionen, • Vertragsklauseln, • Quellen von Interessentenkonflikten, • Grad der Sicherheit im Due-Diligence-Verfahren.	**Entwurf** (13.06.2023) Konsultation Abgeschlossen