ISSN 2432-6089

法と情報雑誌

The Law and Information Magazine

第 10 巻第 5 号（通巻第 66 号・2025 年 6 月）

法と情報研究会　編

本 号 目 次

規則(EU) 2022/2554
[参考訳]

2025 年 6 月 23 日
明治大学法学部教授
夏 井 高 人

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011（OJ L 333, 27.12.2022, p. 1–79）のテキスト（英語版）に基づき，その和訳を試みた。

規則(EU) 2022/2554 の原文のテキストを入手できるサイトの URL は，下記のとおりである。

http://data.europa.eu/eli/reg/2022/2554/oj
[2025 年 3 月 31 日確認]

この規則(EU) 2022/2554 の参考訳は，あくまでも原文を読む際の参考として提供しているものであり，個人的な見解としての法解釈の結果を「日本語以外の言語で書かれた文書の日本語による翻訳文」というスタイルを用いて表現した文書の一種である。

＊＊＊

この規則(EU) 2022/2554 の参考訳の中には，NIS 指令(EU) 2016/1148（OJ L 194, 19.7.2016, p. 1）の参考訳・再訂版（法と情報雑誌 6 巻 6 号 467～548 頁）を踏まえて作成されている部分が含まれている。
ただし，同参考訳・再訂版を公表した後の研究の進展により，現時点では見解を改めた点もある。そのため，この規則(EU) 2022/2554 の参考訳の中には，NIS 指令(EU) 2016/1148 の参考訳・再訂版における訳文とは異なっている箇所がある。

この規則(EU) 2022/2554 の参考訳の中には，指令(EU) 2022/2555（NIS2 指令）（OJ L 333, 27.12.2022, p. 80-152）の参考訳（法と情報雑誌 8 巻 4 号 1～206 頁）を踏まえて作成されている部分が含まれている。
ただし，同参考訳を公表した後の研究の進展により，現時点では見解を改めた点もある。そのため，この規則(EU) 2022/2554 の参考訳の中には，指令(EU) 2022/2555（NIS2 指令）の参考訳における訳文とは異なっている箇所がある。

この規則(EU) 2022/2554 の参考訳の中には，指令(EU) 2022/2557（OJ L 333, 27.12.2022, p. 164-198）の参考訳（法と情報雑誌 8 巻 4 号 207～303 頁）を踏まえて作成されている部分が含まれている。
ただし，同参考訳を公表した後の研究の進展により，現時点では見解を改めた点もある。そのため，この規則(EU) 2022/2554 の参考訳の中には，指令(EU) 2022/2557 の参考訳における訳文とは異なっている箇所

がある。
特に，指令(EU) 2022/2557 においては「critical」と「essential」の両方を「必須」と訳したが，この規則(EU) 2022/2554 の参考訳においては，「critical」を「不可欠」と訳し，「essential」を「必須」と訳すことに改めた。

この規則(EU) 2022/2554 の参考訳の中には，規則(EU) 2019/881（サイバーセキュリティ法）（OJ L 151, 7.6.2019, p.15-69）の参考訳・改訂版（法と情報雑誌 4 巻 8 号 16～86 頁）を踏まえて作成されている部分が含まれている。
ただし，同参考訳・改訂版を公表した後の研究の進展により，現時点では見解を改めた点もある。そのため，この規則(EU) 2022/2554 の参考訳の中には，規則(EU) 2019/881（サイバーセキュリティ法）の参考訳・改訂版における訳文とは異なっている箇所がある。

この規則(EU) 2022/2554 の参考訳の中には，指令(EU) 2015/2366（PSD2）（OJ L 337, 23.12.2015, p. 35-127）の参考訳（法と情報雑誌 3 巻 2 号 1～115 頁）を踏まえて作成されている部分が含まれている。
ただし，同参考訳を公表した後の研究の進展により，現時点では見解を改めた点もある。そのため，この規則(EU) 2022/2554 の参考訳の中には，指令(EU) 2015/2366（PSD2）の参考訳における訳文とは異なっている箇所がある。

この規則(EU) 2022/2554 の参考訳の中には，指令 2009/110/EC（OJ L 267, 10.10.2009, p. 7-17）の参考訳（法と情報雑誌 2 巻 12 号 1～23 頁）を踏まえて作成されている部分が含まれている。
ただし，同参考訳を公表した後の研究の進展により，現時点では見解を改めた点もある。そのため，この規則(EU) 2022/2554 の参考訳の中には，指令 2009/110/EC の参考訳における訳文とは異なっている箇所がある。

この規則(EU) 2022/2554 の参考訳の中には，指令 2014/65/EU（MiFID II）（OJ L 173, 12.6.2014, p.349-496）の参考訳（法と情報雑誌 3 巻 3 号 1～175 頁）を踏まえて作成されている部分が含まれている。
ただし，同参考訳を公表した後の研究の進展により，現時点では見解を改めた点もある。そのため，この規則(EU) 2022/2554 の参考訳の中には，指令 2014/65/EU（MiFID II）の参考訳における訳文とは異なっている箇所がある。

―解 説―

1. 規則(EU) 2022/2554 について

1. 1 総説

規則(EU) 2022/2554 は，金融サービスの分野に特化して金融機関のデジタル運営管理上のサイバー回復力を定める EU の現行法令である。

規則(EU) 2022/2554 は，2025 年 1 月 17 日から適用される（第 64 条参照）。

規則(EU) 2022/2554 は，EU 域内に拠点をもつ金融機関が，EU 域外に拠点をもつ ICT サードパーティサービスプロバイダ（ICT third-party service providers）から業務（特に，金融機関の不可欠な機能または重要な機能（critical or important functions））を遂行する上で重要な ICT サービスを受けており，そのような ICT サードパーティサービスプロバイダからの ICT サービス提供に伴うリスクの削減または排除を主眼とする様々な方策を定めている。
規則(EU) 2022/2554 に定める ICT サードパーティサービスプロバイダは，主として，米国に拠点をもつ巨大なクラウドサービスプロバイダ等のことを想定するものと考えられるが，米国に拠点をもつ企業だけではなく，例えば，日本国の企業が EU 域内の金融機関に対して何らかのサービスを提供する場合，このような ICT サードパーティサービスプロバイダに該当することがあり得ると解される。
それゆえ，日本国に拠点をもち，ICT サービスを提供する企業は，規則(EU) 2022/2554 が定めている内容を正確に理解している必要性があると考えられる。
規則(EU) 2022/2554 の前文(75)に示されているクラウドコンピューティングサービスに関する欧州委員会による拘束力のないモデル契約条項に関しては，欧州委員会による下記の最終報告書が参考になる。ただし，この最終報告書は，規則(EU) 2022/2554 に基づいて作成されたものではなく，規則(EU) 2023/2854（データ法）（OJ L, 2023/2854, 22.12.2023）の第 41 条に基づくものである。

> Final Report of the Expert Group on B2B data sharing and cloud computing contracts
> the European Commission, 2 April 2025
> https://ec.europa.eu/transparency/expert-groups-register/core/api/front/document/116180/download
> [2025 年 4 月 26 日確認]

規則(EU) 2022/2554 は，監督枠組み（Oversight Framework）を導入している。ただし，この枠組みは，規則(EU) 2022/2554 の目的のために限定的に導入されるものであり，他の分野における法令においても導入される新たなモデルとなるものではないとの位置づけが明確にされている（前文(76)参照）。

規則(EU) 2022/2554 の略称としては，一般に，「DORA」が使用されている。
「DORA」は，「the Digital Operational Resilience Act」の頭文字をとったもの。この略称は，公式の略称ではないのだが，規則(EU) 2022/2554 と関連する解説等のコンテンツを参照する際に使用されることが多い。

1．2 規則(EU) 2022/2554 の採択時には未採択だった関連法令など

1．2．1 規則(EU) 2023/1114

規則(EU) 2022/2554 の第 2 条第 1 項(f)は，暗号資産の市場に関する並びに規則(EU) No 1093/2010，規則(EU) No 1095/2010，指令 2013/36/EU 及び指令(EU) 2019/1937 を改正する欧州議会及び理事会の 2023 年 5 月 31 日の規則（「暗号資産の市場に関する規則」）（Regulation of the European Parliament and of the Council on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (‘the Regulation on markets in crypto-assets’)）を参照している。
この第 2 条第 1 項(f)が参照する規則とは，規則(EU) 2022/2554 の採択時点では未採択の規則提案であった暗号資産の市場に関する及び指令(EU) 2019/1937 を改正する欧州議会及び理事会の規則の提案（Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937）（COM (2020) 593，2020/0265/COD）のことを指す。
規則(EU) 2022/2554 の第 2 条第 1 項(f)の中で示されている略称である「暗号資産の市場に関する規則（the Regulation on markets in crypto-assets）」は，規則(EU) 2022/2554 の第 3 条第 30 号，同条第 55 号，同条第 56 号及び第 46 号(d)において参照されている。

同規則案は，暗号資産の市場に関する並びに，規則(EU) No 1093/2010，規則(EU) No 1095/2010，指令 2013/36/EU 及び指令(EU) 2019/1937 を改正する欧州議会及び理事会の 2023 年 5 月 31 日の規則(EU) 2023/1114（Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937）（OJ L 150, 9.6.2023, p. 40–205）として採択された。
同規則は，同規則の第 149 条第 2 項及び第 3 項に定める条項を除き，2024 年 12 月 30 日から適用されている。

従って，規則(EU) 2022/2554 の第 2 条第 1 項(f)が参照する規則は，欧州議会及び理事会の規則(EU) 2023/1114（OJ L 150, 9.6.2023, p. 40–205）と読み替えられなければならず，そのように読み替えた上で，規則(EU) 2022/2554 の第 2 条第 1 項(f)が適用されなければならない。

1．2．2 規則(EU)2022/2065 及び規則(EU)2022/2065

規則(EU) 2022/2554 の第 32 条第 8 項の中で示されている「クラウドコンピューティングサービスのプロバイダに対して適用可能な監督に関する欧州連合の規定（Union rules on oversight applicable to providers of cloud computing services）」とは，前文(20)の中では「デジタル監督当局を設けている欧州連合の横断的な枠組みが存在してないクラウドコンピューティングサービスプロバイダ（cloud computing service providers in the absence of a Union horizontal framework establishing a digital oversight authority）」として示唆されている EU の法令であって，規則(EU) 2022/2554 が採択された時点ではまだ採択されていなかった法令のことを指す。
ところが，規則(EU) 2022/2554 の中には，採択時以前に採択されていたけれども同規則の中では明示

されていない関連法令として，規則(EU)2022/2065（デジタルサービス法）（(OJ L 277, 27.10.2022, p. 1-102）及び規則(EU)2022/868（データ統治法）（OJ L 152, 3.6.2022, p. 1-44）がある。

規則(EU)2022/2065 は，大規模なプラットフォームサービスのプロバイダも適用対象として定めているが，そのようなプラットフォームサービスは，実際には，ほぼ全てにおいてクラウドコンピューティングサービスとして提供される。
また，規則(EU)2022/2065 に関しては，同規則の第 10 条のデータ媒介サービス（data intermediation services）に含まれるプラットフォームの大部分もまた，実際には，ほぼ全てにおいてクラウドコンピューティングサービスとして提供される。

規則(EU)2022/2065 及び規則(EU)2022/868 は，規則(EU) 2022/2554 の中では明示されてはいないけれども，同規則の第 32 条第 8 項に定めるクラウドコンピューティングサービスのプロバイダに対して適用可能な監督に関する欧州連合の規定の一部であることになる。
規則(EU)2022/2065（デジタルサービス法）及び規則(EU)2022/868（データ統治法）の中で定められている関連条項は，規則(EU) 2022/2554 の条項の解釈・適用においても，必要に応じて参酌されなければならない。

1．3 インシデントの通知及び報告

1．3．1 インシデントの分類

規則(EU) 2022/2554 は，異なる性質をもつ複数のタイプのインシデントが存在するというインシデントの体系的理解を前提にして設計されている。

すなわち，全てのインシデントは，ICT と関連するインシデント（ICT-related incidents）とそれ以外のインシデント（non-ICT-related incidents）とに分類される。

「non-ICT-related incidents」は，更に，金融機関の運営管理と関連するインシデント（operational-related incidents）と安全な決済と関連するインシデント（security payment-related incidents）とに分類される。
金融機関の運営管理と関連するインシデントと安全な決済と関連するインシデントの両者を包摂していることを示す簡略表現または短縮表現は「運営管理または安全な決済と関連するインシデント（operational or security payment-related incidents）」である。従って，運営または安全な決済と関連するインシデントは，「non-ICT-related incidents」の別名（alias or synonym）であることになる。
これらのインシデントの深刻度または影響が大きな場合には「大きな（major）」という形容詞が付される。

incidents	ICT-related incidents	
	operational or security payment-related incidents (=non-ICT-related incidents)	operational-related incidents
		security payment-related incidents

運営管理と関連するインシデント（operational-related incidents）は，ICT と関連するインシデント（ICT-related incidents）の要素を含まないので，例えば，経営陣もしくはその構成員，従業者またはアウトソース先の者による詐欺，横領または背任のような犯罪行為，大規模災害，外国による侵略行為・武力侵攻，内戦または暴動等による当該金融機関の建物や人員の喪失・欠乏のように，金融機関としての経営または運営それ自体を機能不全にするインシデントが想定されていると考えられる。

安全な決済と関連するインシデント（security payment-related incidents）もまた，直接的には，ICT と関連するインシデントの要素を含まないので，例えば，アウトソース先の破産，経営破綻または企業合併等により当該金融機関における決済が実行できなくなる事態が発生する場合などが想定されていると考えられる。
しかし，間接的に ICT と関連するインシデントの要素を含む場合，例えば，金融機関に対して不可欠な機能または重要な機能を提供する ICT サードパーティサービスプロバイダの電子的な処理システムがサイバー攻撃を受け，そのために当該金融機関における決済処理と関連するインシデントが発生しているけれども．当該金融機関は当該 ICT サードパーティサービスプロバイダにおいて発生している ICT と関連するインシデントに対して直接的には対応できないような場合を含むものと考えられる。

1．3．2 インシデントの報告義務

このような規則(EU) 2022/2554 におけるインシデントの体系的な類別の前提とした上で，規則(EU) 2022/2554 の対象事項（subject matter）である金融機関に対して適用可能な要件（requirements applicable to financial entities）の一部として，第 1 条第 1 項(a)(ii)は，職務権限のある当局に対する，ICT と関連する大きなインシデントの報告（reporting of major ICT-related incidents）を定め，同項(a)(iii)は，職務権限のある当局に対する運営管理または決済の安全性と関連する大きなインシデントの報告を定めている。

規則(EU) 2022/2554 の第 19 条第 1 項第 1 副項は，第 1 条第 1 項(a)(ii)に対応する要件を定める条項であり，ICT と関連する大きなインシデントがあったときは，同規則の第 46 条に列挙されている各法令に基づく適格な職務権限のある当局に対し，その ICT と関連する大きなインシデントの最初の通知及び報告しなければならないことを定めている。

加えて，規則(EU) 2022/2554 の第 19 条第 1 項第 6 副項は，同項第 1 副項の職務権限のある当局に加え，各構成国の選択に従い，指令(EU) 2022/2555 に従って指定されまたは設けられた職務権限のある当局またはコンピュータセキュリティインシデント対応チーム（CSIRTs）に対しても ICT と関連する大きなインシデントの最初の通知及び報告を任意で提出できることを付加的に定めることができる旨を定めている。

これに対し，規則(EU) 2022/2554 の第 1 条第 1 項(a)(iii)に定める運営管理または決済の安全性と関連する大きなインシデントの報告の要件に関しては，前文(54)において，その要件を定める条項を設けることが述べられている。
規則(EU) 2022/2554 の第 23 条がそれに該当する条項だと解される。同条により，第 19 条第 1 項に定

める ICT と関連する大きなインシデントのインシデントの報告の要件が運営管理または決済の安全性と関連するインシデント（operational or security payment-related incidents）の報告の要件として適用（実質的には準用して適用）されることになる。
ただし，規則(EU) 2022/2554 の第 1 条第 1 項(a)(iii)は，「職務権限のある当局に対する運営管理または決済の安全性と関連する大きなインシデントの報告」を定めているのにも拘わらず，同規則の第 23 条は，職務権限のある当局に対する運営管理または決済の安全性と関連する「大きなインシデント（major operational or security payment-related incidents）」の報告だけではなく，職務権限のある当局に対する「運営管理または決済の安全性と関連するインシデント（operational or security payment-related incidents）」の報告の両者に対して同規則第 19 条に定める報告義務の要件が適用されることを定めているから，適用対象が拡張されていることになる。

1．3．3 サイバー脅威の報告義務

規則(EU) 2022/2554 の第 19 条第 2 項第 1 副項は，金融機関が大きなサイバー脅威を任意で適格な職務権限のある当局に対して通知でき，また，その任意の通知を受けた当局は，他の職務権限のある当局に対してその通知を送信できることを定め，同条第 2 項第 2 副項は，指令 2013/36/EU の第 4 条に従って指定された適格な職務権限のある国内当局に対し任意で大きなサイバー脅威を報告でき，また，その通知を受けた当局は，ECB に対してその通知を直ちに送信することを定め，同条第 2 項第 3 副項は，各構成国の選択に従い，CSIRTs に対しても大きなサイバー脅威を通知できることを付加的に定めることができる旨を定めている。

1．3．4 エスカレーション

規則(EU) 2022/2554 の第 19 条に定める義務的な通知及び任意の通知の仕組みは，ICT と関連する大きなインシデント及び大きなサイバー脅威の情報の関連当局間における情報セキュリティマネジメントシステムにおけるエスカレーションと情報共有の仕組みを定めるものである。

規則(EU) 2022/2554 は，指令(EU) 2022/2555（NIS2 指令）との関係において特別法（*lex specialis*）となっている（前文(16)参照）。

1．3．5 日本国に拠点をもつ企業等との関係

規則(EU) 2022/2554 は，EU の構成国に本店等の拠点をもつ金融機関だけではなく，EU 域内に支店等を設立して事業活動を営んでいるが EU の域外（第三国内）に本店等の拠点をもつ金融機関に対しても適用がある。そのような第三国に拠点のある金融機関には日本国内に本店等の拠点をもつ金融機関も含まれる。
それゆえ，EU 域内に支店等を設立して事業活動を営んでいる日本国に本店等の拠点をもつ金融

機関は，ICT と関連する大きなインシデントに関し，どの構成国のどの当局に対して規則(EU) 2022/2554 の第 19 条第 1 項第 1 副項の最初の通知及び報告をしなければならないかを正確に知っており，かつ，当該職務権限のある当局に対して迅速に通知及び報告を提出できるようにするための技術上及び組織上の準備をしなければならないというだけではなく，同規則の第 19 条第 1 項第 6 副項との関係において，EUのどの構成国がどのような決定をしているのかを精密に調べた上で，もしそのような追加的な定めがあるときは，当該構成国の CSIRT に対しても迅速に通知及び報告を提出できるようにするための技術上及び組織上の準備しなければならないということに留意すべきである。

同様に，EU 域内に支店等を設立して事業活動を営んでいる日本国に本店等の拠点をもつ金融機関は，大きなサイバー脅威に関し，どの構成国のどの当局に対して規則(EU) 2022/2554 の第 19 条第 2 項に定める任意の通知をできるかを正確に知っており，かつ，任意に通知できるようにするための技術上及び組織上の準備をしなければならないということにも留意すべきである。

なお，規則(EU) 2022/2554 の適用対象となる金融機関とは，同規則第 2 条に定める金融機関のことを指す。EU 法及び EU 法に基づく構成国の国内法が適用される裁判管轄権の適用範囲内にある限り，日本国の一般的な法令及び金融業界の常識・理解や日本国内の関連分野における学説上の通説的な定義とは全く無関係に，規則(EU) 2022/2554 の第 2 条が適用される。国家主権とは，本質的にそのようなものである。

それゆえ，規則(EU) 2022/2554 の適用可能性のある日本国企業は，同規則の第 2 条の定め及び第 3 条に含まれている関連定義条項に関し，正確な理解を得ておく必要性がある。

1．4 ICT サードパーティから提供される AI サービス

金融機関が，契約によって，当該金融機関の業務遂行のために ICT と関連する仕事の一部を第三国のクラウドコンピューティングサービスのプロバイダに委託し，そのプロバイダから提供されるサービスを利用する場合のリスク（ICT third-party risk）のマネジメントに関しては，規則(EU) 2022/2554 の第 V 章の中で定められた条項に従うことになる。

この場合におけるサービスの中には，例えば，第三国の ICT サードパーティから提供される AI チャットボットや AI エージェントのサービスの利用も含まれると解される。

そのような AI チャットボットや AI エージェントが自律性と自己学習能力をもっているために在来の情報セキュリティの方法によってはリスクを評価，管理及び解消できない場合，当該金融機関と ICT サードパーティサービスプロバイダとの間で締結された契約上の取決め（contractual arrangement）だけでは対応できない。
また，AI チャットボットや AI エージェントのような AI サービスと関連する契約が全く存在しないにも拘わらず，金融機関の業務の中で汎用品として AI チャットボットや AI エージェントが利用されておりながら，その利用に関しては当該 AI チャットボットや AI エージェントのサービスを提供する企業や組織

等が一方的に定めた約款に従うしかなく，かつ，その約款の中には完全な免責条項が含まれているような場合もあり得る。

例えば，銀行業務の中で Microsoft Word を使用して業務用の文書が作成される場合には自動的に Copilot が実行され，インターネット上の情報検索を実行する際には Google の AI 機能が自動的に実行されることがある。
このような場合，当該機関の従業者は，規則(EU) 2022/2554 が定める枠組みの外で任意に第三国の ICT サードパーティから提供される AI チャットボットや AI エージェントのような AI サービスを利用していることになり得る。つまり，そのような場合においては，規則(EU) 2022/2554 の適用が事実上反故にされていると言い得る。

そして，これらのような場合に関し，規則(EU) 2022/2554 の中には，金融機関に適用される明確な行動規範等を定める条項が存在しない。例えば，規則(EU) 2022/2554 の第 28 条第 3 項は，ICT サードパーティサービスプロバイダから提供される不可欠な機能または重要な機能を支える ICT サービスの利用に関する契約上の取決めの内容である情報の登録簿（register）を設けることを定めているが，AI チャットボットや AI エージェントのような汎用の AI サービスに関して登録簿それ自体が成立するのかどうかについては，かなり疑問である。
加えて，AI チャットボットや AI エージェントのような汎用の AI サービスがごく限られた数の世界的規模の巨大プラットフォーマーから提供される場合，実質的にみて，規則(EU) 2022/2554 の第 29 条によっては対処できない ICT サービスの集中化リスクが生じていることともなり得る。

このような場合に対応するため，何らかの精密な技術的対応が不可欠かつ重要となるかもしれない。また，AI 技術と関連する法令の適用，特に，何か問題が発生した場合のインシデント報告やリスク管理と関連する条項の適用があり得るのかどうか，そして，適用があると解される場合，規則(EU) 2022/2554 の関連条項の適用との優先劣後関係の法解釈や適格な職務権限のある当局の決定をどうすべきかが事前に十分に検討されている必要がある。
また，組織的な対応として，普通の規模の金融機関にとって導入可能な方策としては，当該機関の組織内の規則や労働協約によって，Copilot の自動実行を防止するため Microsoft の製品の使用を全て禁止し，インターネット上の情報検索を実行する際には Google が提供するサービスの使用を全て禁止し，また，それら以外の類似製品や類似サービスに関しても同様に禁止することが考えられる。

ここで述べているような意味での AI 技術と関連する EU の基本法令としては，規則(EU) 2024/1689（人工知能法）（OJ L, 2024/1689, 12.7.2024）がある。規則(EU) 2022/2554 の関連条項の適用の法解釈に際しては，規則(EU) 2024/1689（人工知能法）の中に含まれている監督及び市場監視と関連する条項の法解釈が検討されなければならない。

EU における今後の立法論を含め，欧州委員会レベルで採択可能な措置として，EU において有効な競争法の関連条項の適用を検討した上で，もし直接的に適用可能な条項が存在しないときは，そのような汎用の AI サービスや AI アプリのバンドリングまたはバンドリングと同じ効果もしくは社会的意味をもつ自動実行を禁止する法令案を提案するということ，あるいは，そのような AI サービスや AI ア

プリを完全にオプトアウトできるようにすることを法定の義務とし、義務違反行為に対しては巨額の制裁金を科すような法令案を提案することは，検討可能な範囲内にある。
また，EU の現行の競争法及び関連法令の中に直接的に適用可能な条項が存在するときは，そのような条項を適用して実行される措置命令と制裁を検討することも，検討可能な範囲内にある。

これらの諸点に関する考え方の一般手益な基本原則は，デジタルの権利及び基本原則に関する欧州宣言（2023/C 23/01）の検討の中から得られる。

1．5 データの保護

一般に，金融機関において処理されるデータには，個人データ（personal data），非個人データ（non-personal data）及び個人データと非個人データの混合データ（mixed data）が含まれる。この点に関しては，EU の構成国においても日本国においても同じである。ただし，日本国の現行法制の下においては，非個人データ及び混合データに対する法適用が明確ではない。

EU において，個人データに関しては，規則(EU) 2016/679（一般データ保護規則）（OJ L 119, 4.5.2016, p. 1），規則(EU) 2018/1725（OJ L 295, 21.11.2018, p. 39）が適用され（前文(34)参照），また，非個人データに関しては，規則(EU)2018/1807（OJ L303, 28.11.2018, p. 59）が適用される。
混合データに対する EU の関連法令の適用関係に関しては，非個人データの支障のない流れの枠組みに関する運用指針 COM/2019/250 final が公表されている。

これらのデータは，金融機関のインハウス（in-house）で処理されることもあるが，外部の ICT サードパーティサービスプロバイダ（ICT third-party service providers）に対する事務委託または下請により，当該 ICT サードパーティサービスプロバイダによって処理されることもあり，更に，当該 ICT サードパーティサービスプロバイダから別の法主体に再下請されることもあり得る。
このような外部者がデータ処理する場合においても，上述の個人データ，非個人データ及び混合データに適用される EU の法令の条項及び構成国の関連国内法の条項が適用される。そして，それらの法令の条項が適正に適用されないときは，規則(EU) 2022/2554 の第 28 条，第 29 条及び第 30 条により，当該 ICT サードパーティサービスプロバイダとの間の ICT サービスの利用に関する契約関係が終了となることがあり得る。この ICT サービスの中には，データの処理業務も含まれる。

日本国に本店等の本拠地をもつ企業が EU の構成国の金融機関との関係において第三国に本拠地をもつ ICT サードパーティサービスプロバイダとして扱われる場合，規則(EU) 2022/2554 の第 28 条及び第 29 条により，当該 ICT サードパーティサービスプロバイダとの間の契約関係が終了となることを避けるためには，上述の個人データ，非個人データ及び混合データに適用される EU の法令の条項及び構成国の関連国内法の条項を遵守しなければならないということに留意すべきである。

1．6 欧州連合の監督権限の第三国内における実行

金融部門における ICT サードパーティリスクと関連する事項に関する行政上の監督は，欧州連合のレベルでは，筆頭監督者（Lead Overseer）によって実行される。

規則(EU) 2022/2554 に基づく筆頭監督者の監督権限は，基本的には，欧州連合の領域内において行使される。

しかし，ICT サードパーティリスクと関係する不可欠な ICT サードパーティサービスプロバイダの拠点が第三国内にある場合，規則(EU) 2022/2554 の第 36 条により，当該第三国との間の行政上の協力協定を法的根拠として，当該第三国内における立入検査の権限の行使を可能とするような仕組みを構築することが予定されている。

日本国は，欧州連合との関係においては第三国であることになるので，規則(EU) 2022/2554 の第 36 条による行政上の協力協定が締結された場合，欧州連合の筆頭監督者による立入検査等が日本国の領土内にあり日本国に拠点のある金融機関の構内（premises）において実行され得ることになる。

このような協力協定が存在しない場合，欧州連合の筆頭監督者が第三国の領土内において立入検査等を実行する法的根拠が存在しないことになるので，その権限の実行が不可能な状態に陥ることになる。
このような場合に関し，規則(EU) 2022/2554 の第 36 条第 3 項第 2 副項は，同規則の第 35 条第 1 項(d)により発される筆頭監督者の勧告の中において第三国内における立入検査が実行不可能であることにより生ずると想定される潜在的な結果を考慮に入れることとされている。
すなわち，欧州連合内に拠点をもつ金融機関に対する勧告において，当該不可欠な ICT サードパーティサービスプロバイダからの ICT サービスの提供を受けてはならないということが勧告され得ることになる。
換言すると，例えば，日本国に拠点をもつ不可欠な ICT サードパーティサービスプロバイダが欧州連合の筆頭監督者の監督権限を無視すれば，欧州連合内の市場から排除される可能性があることは言うまでもないことである。

このことは，不可欠な ICT サードパーティサービスプロバイダ宛ての勧告書の中で特定された ICT サードパーティリスク（the ICT third-party risk the specific risks identified in the recommendations addressed to critical ICT third-party service providers）に対して当該金融機関が適切に対処しない場合，当該金融機関に関して職務権限のある当局が，規則(EU) 2022/2554 の第 42 条第 6 項ないし第 8 項により，当該金融機関と当該不可欠な ICT サードパーティサービスプロバイダとの間のアウトソーシング契約または下請契約を終了させることを命ずる決定等によっても行われ得る。

それゆえ，この点に関しても，日本国の関連企業にとっては，その日本国企業が第三国内に拠点をもつ不可欠な ICT サードパーティサービスプロバイダであって，欧州連合内の金融機関に対して ICT サービスを提供する法主体（entity）に該当すると判断され，そのような判断に基づく行政指導や行政

処分としての決定が行われ得る余地が存在する限り，当該 ICT サービスを提供する金融機関が拠点をもつ欧州連合の構成国において当該金融機関に関して職務権限のある当局がどの当局（行政機関）であるのかを事前に調査し，その職務権限（competence）と職務（tasks）を正確に理解し，相互の連絡と情報交換のための単一連絡場所（single contact point）を設けることが重要である。

1．7 規則(EU) 2022/2554 の今後の適用範囲の拡大

一般に，日本国の関連法学分野において，EU の法令の見直し（review）に関する条項が丁寧に分析・検討される機会は乏しいが，立法者の視座を知るために，規則(EU) 2022/2554 に限らず，EU のどの法令においても，見直し条項を丁寧に読み，関連法令を仔細に調べて理解し，それらの思考作業の中から今後の方向性を推察し，日本国の各部門の政策決定及び法解釈に応用することには大きな実利がある。

規則(EU) 2022/2554 の第 58 条においては，現在では適用対象とはなっていない様々な金融サービス（特にデジタルの金融サービス）に対し，今後，同規則の適用範囲を拡大するという法構成での再検討のための評価を実施すべきことが定められている。その結果がどうなるかは，欧州委員会及び関連機関の裁量と全世界の経済動向等によって大きく左右されることであり，特に，ロシアのウクライナ武力侵攻による世界規模での不安定な状況が与える影響を軽視することは許されない。
しかし，それはそれとして，今後も世界規模でデジタル経済が発展するという前提で一応の想定を検討しておくことには大きな意味があると考えられる。

1．8 より大きな視点の重要性

ここまで述べた諸点との関係において，日本国の銀行，証券会社，保険会社，投資会社，クレジットカード会社，前払式支払手段の発行会社，企業年金運用組織等のような規則(EU) 2022/2554 の適用対象となり得る業種のサイバー脅威及び ICT インシデントに対する回復力の程度，その回復力を維持するための準備態勢やマネジメントシステムの実際に関し，事実を把握することが重要である。客観的な事実を踏まえない空想や単なる予測だけでは正しい政策論を形成できない。

しかし，日本国内において公表されている資料等を読む限り，そのような客観的な事実を把握するための包括的な調査結果は，少なくとも現時点（2025 年 4 月現在）では，（EU の基準によるマイクロ企業のような小さな経営規模の企業を除外した企業だけのものとしても）存在しないようである。

それゆえ，個々の日本企業が自社の準備態勢を相対的に評価するための手段・方法は，かなり限られている。

回復力と関連する技術標準（ISO，JIS の規格等）は幾つか存在しているが，それは，一定の規範を示すのみであり，業界全体の実態を表現するものではあり得ず，個々の企業の取引内容，取引相手，

経営規模や業態の相違に応じた実装の実際を示すものでもあり得ない。

それゆえ，現状の下においては，日本国の関連企業は，自己の能力の範囲内で，または，信頼できる情報セキュリティ関連企業に評価と助言を依頼して，統一性のない対応を進めるしかない。このことは，国際的な対応の面における日本国政府の政策上の一貫性の不存在の原因となるだけではなく，サイバー戦のような大規模なサイバーインシデントに対する関連業界内の統一的かつ一貫性のある対処を不可能とする原因ともなり得る。

そして，それらのことは，日本国のサイバー国防上の実力の劣化にも直結することになるであろうし，また，関連する事柄との関係における国際的な信頼の低下をもたらすものともなるであろう。

国際的な経済政策という観点に限定して考えてみても，現在のアメリカ合衆国のトランプ大統領による国内的及び国際的な経済政策がどのようなものであるにしても，日本国政府は，現実の問題として，情報システムを基礎とする電子的な決済手段が（共産主義や社会主義の国家を含め）世界中のほぼ全ての国家における不可欠のインフラとなっているという現状を直視し，そのことを踏まえた冷静かつ客観的な国家政策をとることが重要である。

一般に，情報社会においては，（国防を含め）国家統治のためのインフラと（国内的及び国際的な）経済運営のためのインフラが同一の情報ネットワークシステムになっているという事実，そして，そのことのために，平時の事柄と戦時の事柄とが常に共存しており，表裏一体の関係となっているという事実を正確に理解することが必要である。

規則(EU) 2022/2554 は，そのような意味での現代の情報社会の根幹部分を正しく理解し，その問題点を克服するための継続的な努力と改善のための EU の基本政策の一部として策定された法令であると言える。

ここで述べているような意味での情報法制の考え方の基本的な骨格に関しては，「情報社会の素描ーEU の関連法令を中心としてー」法律論叢 90 巻 4･5 号 135～181 頁，法律論叢 90 巻 6 号 165～211 頁（2018 年）の中で，一般理論として既に述べたとおりである。

同論文の中で示した具体例としての EU の個々の法令及び条項のような詳細部分に関しては既にアウトオブデートになっている箇所がある。しかし，同論文の中で述べた基本的な一般理論に関しては，現時点においても修正する必要性がない。

同論文は，EU の関連法令を素材としつつも，情報法（Information Law）の一般的な基本構造を述べる論文である。

2. 参考訳作成における基本方針

この参考訳においては，規則(EU)2022/2554の前文及び条文の全文を訳出した。

この参考訳においては対訳方式を採用することにした。ただし，原文を表示することが無意味な部分（特に脚注内）に関しては，原文または訳文の表示を省略した。

この参考訳は，あくまでも規則(EU)2022/2554の私的な和訳である。公式訳でも確定訳でもない。

この参考訳は，現時点における研究成果を反映するものである。将来，更に研究を深めた結果として修正すべき部分を発見したときは，その時点において，改訂版等を作成すべきかどうかを検討する。

この参考訳の訳出に際しては原則として直訳とすることとしたが，直訳のままでは日本語になりにくい箇所に関しては，やむを得ず意訳とした。

原文中にある誤記と疑われる箇所に関しては，赤色字で示すことにした。この原文中の誤記と疑われる箇所は，形式的なミスという意味で誤記であるものと意味的な誤りを含むことになるために誤記であるもの両者を含む。
ただし，原文中に存在する誤記と疑われる箇所の全てが赤色字で表示されているという趣旨ではない。判断を保留した箇所が存在する。
原文中に誤りがあると判断した場合，原則として，そのまま直訳とした。しかし，そのまま直訳にしたのでは正しく法解釈された法規範を適正に示したことにならない場合，合理的に法解釈した結果を反映した訳文とすることにし，その箇所を灰色字で示すことにした。
例えば，第5条第2項(i)の中にある「at corporate level」は，文それ自体としては特におかしくはないけれども，この「corporate」を企業を指すと解するとすれば，私企業ではない金融機関（例：構成国の国内中央銀行）の経営陣は同項(i)に定める伝達の経路を設ける必要がないことになるので，意味的には誤った文である。同じ問題は，前文(61)の中にもある。この「at corporate level」は「at financial entity level」または「at cooperation level」の誤記と解すべきであり，前後の文脈から判断して前者の誤記である可能性の方が高いと法解釈することにした。そこで，この部分の訳文は，合理的な法解釈の結果を踏まえた意訳であり，原文の直訳としては成立し得ない訳文（日本語文）になるので，灰色で表示される。なお，後者の誤記であると解するときは，「協力レベルで」という訳文になる。

この参考訳に訳注はない。参考訳中にある脚注は，全て原注である。

読みやすさを重視し，条文中の号(point)の表記を一部省略した。例えば，「point(a)」は「第(a)号」であるが，「第」と「号」を省略し，「(a)」と表記することにした。

3. 参考訳作成において留意した事項

Critical

この参考訳においては，ICT システムの属性等との関係においては，「critical」を「不可欠」と訳すことにした。

Essential

この参考訳においては，ICT システムの属性等との関係においては，「essential」を「必須」と訳すことにした。

Financial entities

「financial entities」は，金融部門の業務を担当する法主体（entities）のことを意味する。規則(EU) 2022/2554 においては，この「financial entities」は，例えば，各国の中央銀行のような公的機関と民間部門の企業である銀行等の両者を含んでいると解される。

この参考訳においては，このような理解を前提とした上で，「financial entities」を「金融機関」と訳すことにした。

Jurisdictions

規則(EU) 2022/2554 の前文(4)，前文(26) 前文(57)，前文(81)及び第 15 条第 1 副項(e)においては，「jurisdictions」は，欧州連合の構成国の領土の支配権のことを指し，それは，国家主権，主権国家それ自体または主権国家の及ぶ範囲（領土）のことを指す。

このような意味をもつ場合における「jurisdictions」は，個々の裁判所の訴訟法上の管轄権のことではない。
しかし，国際政治学及び国際法の素養がなければ混同を避けることができないと判断したので，この参考訳中の上記のような趣旨で用いられている箇所においては，「jurisdictions」を「主権国家」と訳すことにした。

Otherwise

慣用句的に「or otherwise」が使用されている場合，「または，さもなければ」等と訳すことは可能であるが，日本語表現としては重複的であり，くどすぎるので，この参考訳においては，便宜，「or otherwise」を「あるいは」とまとめて表現することにした。日本語によるより良い表現方法が別に存在するときは，それによるべきである。

Conditions and terms

「conditions and terms」は，文脈により，多義的な語であるが，この参考訳においては，共通に適用されることを想定した「約款」を示すものと解されるので，そのような意味をもつものとして，「約款」と訳すことにした。

Premises, land or property

筆頭監督者による立入検査の権限の対象となる物件（material）としての「premises, land or property」の理解は，関係する法分野の相違によって異なっていることがあり得るが，一般名詞として解釈するのではなく，規則(EU) 2022/2554 の第 39 条の現地における検査（on-site inspection）の目的と関連する範囲内に限定して合理的に解釈すると，ICT サードパーティサービスプロバイダが欧州連合内に拠点をもつ金融機関に対して ICT サービスを提供する事業の用に供するための「施設，土地または財物」を指すと解される。

規則(EU) 2022/2554 の第 39 条にいう「構内（premises）」とは，（例えば，賃貸ビル内に拠点をもつだけであり，そのビルの敷地それ自体を当該金融機関の資産としていない場合のように）建物だけの場合と，建物及びその敷地の両方を含む場合とがあり得る。そのため，「premises」の用法に関し，規則(EU) 2022/2554 において，全体的にやや曖昧な用い方が採用されている。そのような語であるので，現実の具体的な法適用・法解釈の場面に直面した際，合理的かつ柔軟に解釈する必要性がある。

このように解釈すると，規則(EU) 2022/2554 の第 39 条にいう「土地（land）」は，事業用の建物や工作物が全く建設されていない土地，当該構成国において建物とは認められていない通信用の鉄塔等の工作物等が建設されているだけの土地など，事業用の建物が含まれていない土地のことを指すと解されることになる。事業用の建物は，「構内（premises）」に含まれる。ちなみに，完全な裸地であっても，当該 ICT サードパーティサービスプロバイダが証拠隠滅のために重要な記録や機器類等を埋めて隠蔽した土地（land）は立入検査の対象となり得ると解される。また，コンテナのような容易に移動可能な収納物（動産）を置いてあるだけの土地の場合や，そのような移動可能な収納物（動産）を仮設的に設置されているだけであり，それらの収納物（動産）が当該構成国の法令上においては建物として扱われていない場合も同様に解することができる。

以上に述べたことを踏まえた上で，立入検査の対象として示されている場合においては，規則(EU) 2022/2554 の第 39 条にいう「property」を「財物」と訳すことにした。この財物は，日本国の民法学及び刑法学において使用されている「財物」の概念と完全に一致するものではない。この参考訳においては，規則(EU) 2022/2554 における立入検査の対象物として人間（監督の職務担当者）が立入ることができる有体物（tangible material）であることを要し，無体物（intangible object）であるデータや情報を含まないものとして，かつ，上述の「構内（premises）」及び「土地（land）」の概念理解と整合性のあるものとして，「property」の概念を理解し，最も適切な訳語として「財物」を使用することにした。

有体物である土地や施設（facilities）等に物理的に立入ることを要求するのではなく，無体物であるデータや情報それ自体及びデータや情報を記録した文書や書面の提供を要求する必要がある場合，規則(EU) 2022/2554 の筆頭監督者は，同規則の第 39 条の立入検査の要求によるのではなく，第 37 条の情報提供の要求により対処すべきことになる。

Telecommunication operator

規則(EU)2022/2554 においては，「telecommunication operator」は，主として，民間企業である電気通信事業者のことを指すと解されるが，国家機関または公立法人である電気通信組織も含む趣旨であり，また，通信の接続サービスの事業者だけではなく，プラットフォーマやクラウドサービスプロバイダを含め多種多様な事業者を含む趣旨と解される。
この参考訳においては，これら全部を含み得る訳語を選択すべきであると判断し，「telecommunication operator」を「通信業務運用者」と訳すことにしたが，他により適切な訳語が存在するときは，その訳語によるべきである。

Judicial authorities

規則(EU) 2022/2554 においては，「judicial authorities」は，裁判所だけではなく，各構成国の法務省，検察庁及び警察のような法務を担当する国家機関を含む趣旨で用いられていると解される。
日本国憲法第 76 条により，日本国の法律用語としての「司法」及び「司法権」という語は，裁判所のみに限定して使用されるべきであり，法務省，検察庁及び警察のような（裁判所以外の）法務を担当する国家機関に対して「司法」及び「司法権」という語を使用することができない。これは，日本国憲法に定める（予約語としての）法律用語の制限の一部である。特に国家機関及び公務員は，裁判所以外の国家機関に関して「司法」及び「司法権」という語を使用しないという義務（制限）を厳守しなければならない（日本国憲法第 99 条）。
それゆえ，この参考訳においては，裁判所以外の国家機関を含む趣旨で使用されていると解釈され得る限り，「judicial authorities」を「法務当局」と訳すことにした。

なお，欧州連合の構成国の大多数においては，裁判所は，法務省の一部を構成する行政官庁の一種であり，裁判官は法務省の職員の一部を構成する公務員または臨時採用公務員であり，裁判の独立が保障されている点だけが他の通常の公務員とは異なっている。
規則(EU) 2022/2554 は，欧州連合の法令であり，国家主権に基づき多種多様である各構成国の国家制度や裁判所制度を全部包摂して，法務当局との概念を用いている。
例えば，規則(EU) 2022/2554 の第 54 条第 5 項第 2 文の「judicial decision」の「judicial」は，構成国の司法機関である裁判所裁判所を指す場合と構成国の行政機関である行政不服審判所を指す場合など国家主権上の異なる性質をもつ国家機関を全部含む趣旨で用いられていると解釈される。規則(EU) 2022/2554 の中では，例えば，第 56 条第 2 項のように，裁判所に限定する場合には「court」と明示されている。
一般に，日本国憲法のようなタイプの憲法とそれに基づく国家体制・国家制度をもつ主権国家は，世界全体の中では稀である。世界全体の中ではかなり異質な国家制度と法律用語を（数学における公理や定理と同じような意味で）当然の前提として固定的にとらえた上で，世界各国の多種多様な国家制度と法制を理解しようとしてはならない。そのことから，欧州連合の構成国における行政処分に対する不服申立制度は，不服申立てを審理する機関及び手続共に日本国憲法の下における裁判所制度とはかなり異なっていることがあるので，そのことを踏まえた慎重な検討を要する。
そして，そのような慎重な検討を行わずに安易に日本国の法律用語を用いて「judicial authorities」を訳

出することは常に危険なことであり，また，国によってかなり異なっていることがある欧州連合の構成国の国家主権及び国家としての名誉に対して侮辱的な訳文となってしまうリスクがある。
これらの諸点を考慮に入れれば，EU 法の条項に関する限り，「judicial authorities」を「法務当局」と訳すのが最も無難である。

4. 関連参考訳等

指令(EU) 2015/2366（PSD2）の参考訳は，法と情報雑誌 3 巻 2 号 1～115 頁にある。指令 2009/110/EC の参考訳は，法と情報雑誌 2 巻 12 号 1～23 頁にある。指令 2014/65/EU（MiFID II）の参考訳は法と情報雑誌 3 巻 3 号 1～175 頁にある。規則(EU) No 648/2012 の参考訳は，法と情報雑誌 3 巻 8 号 1～96 頁にある。規則(EU) No 600/2014（MiFIR）の参考訳は，法と情報雑誌 3 巻 3 号 1～79 頁にある。
FinTech 通知 COM(2018) 109 final の参考訳は，法と情報雑誌 3 巻 8 号 181～200 頁にある。
規則(EU)2022/2065（デジタルサービス法）の参考訳は，法と情報雑誌 8 巻 2 号 1～299 頁にある。規則(EU)2022/868（データ統治法）の参考訳は，法と情報雑誌 8 巻 3 号 1～130 頁にある。

規則(EU) 2024/1689（人工知能法）の参考訳は，法と情報雑誌 9 巻 3 号 1～130 頁，法と情報雑誌 9 巻 4 号 1～143 頁，法と情報雑誌 9 巻 5 号 1～145 頁にある。欧州評議会人工知能枠組み条約（CETS No. 225）の参考訳は，法と情報雑誌 9 巻 5 号 146～181 頁にある。デジタルの権利及び基本原則に関する欧州宣言の参考訳は，法と情報雑誌 9 巻 1 号 200～229 頁にある。

規則(EU) 2019/881（サイバーセキュリティ法）の参考訳・改訂版は，法と情報雑誌 4 巻 8 号 16～86 頁にある。指令(EU) 2016/1148 の参考訳・再訂版は，法と情報雑誌 6 巻 6 号 467～548 頁にある。指令(EU) 2022/2555（NIS2 指令）の参考訳は，法と情報雑誌 8 巻 4 号 1～206 頁にある。指令(EU) 2022/2557 の参考訳は，法と情報雑誌 8 巻 4 号 207～303 頁にある。

規則(EU) 2016/679（一般データ保護規則）の参考訳・再訂版は，法と情報雑誌 3 巻 5 号 1～114 頁にある。規則(EU) 2018/1725 の参考訳は，法と情報雑誌 4 巻 1 号 1～81 頁にある。非個人データの支障のない流れの枠組みに関する運用指針 COM/2019/250 final の参考訳は，法と情報雑誌 10 巻 4 号 1～51 頁にある。

この参考訳の校正等に関し，唐亀侑久氏（株式会社ラック）の助力を得た。

＊＊＊

金融部門のデジタル運営管理上の回復力に関する並びに規則(EC) No 1060/2009, 規則(EU) No 648/2012, 規則(EU) No 600/2014, 規則(EU) No 909/2014 及び規則(EU) 2016/1011 を改正する欧州議会及び理事会の 2022 年 12 月 14 日の規則(EU) 2022/2554

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011

（EEA に適用される正文）
(Text with EEA relevance)

欧州議会及び欧州連合の理事会は,
欧州連合の機能に関する条約, とりわけ, 同条約の第 114 条に鑑み,
欧州委員会からの提案に鑑み,
立法案を国内議会に送付した後,
欧州中央銀行の意見書に鑑み[1],
欧州経済社会委員会の意見書に鑑み[2],
通常の立法手続に従って審議し[3],

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,
Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,
Having regard to the proposal from the European Commission,
After transmission of the draft legislative act to the national parliaments,
Having regard to the opinion of the European Central Bank (1),
Having regard to the opinion of the European Economic and Social Committee (2),
Acting in accordance with the ordinary legislative procedure (3),

Whereas:

(1) デジタル時代において, 情報通信技術（ICT）は, 日々の活動のために利用される複雑なシステムを支えている。ICT は, 金融部門を含め, 鍵となる諸部門において走っている経済を維持しており, また, 域内市場の稼働を拡大している。増加するデジタル化と相互接続性は, ICT のリスクも増幅しており, サイバー脅威または ICT 破壊に対し, 社会全体及びとりわけ金融システムを, より脆弱なものと

[1] OJ C 343, 26.8.2021, p. 1.
[2] OJ C 155, 30.4.2021, p. 38.
[3] 欧州議会の 2022 年 11 月 10 日付け意見書（官報未搭載）及び理事会の 2022 年 11 月 28 日付け決定。
Position of the European Parliament of 10 November 2022 (not yet published in the Official Journal) and decision of the Council of 28 November 2022.

している。今日，ICT システムのユビキタスな利用及び高度なデジタル化と接続性は，欧州連合の金融機関の諸活動のコア機能となっている一方で，金融機関のデジタル回復力は，まだ，よりよく対処されておらず，また，金融機関のより広い運営管理上の枠組みの中に統合されていない。

In the digital age, information and communication technology (ICT) supports complex systems used for everyday activities. It keeps our economies running in key sectors, including the financial sector, and enhances the functioning of the internal market. Increased digitalisation and interconnectedness also amplify ICT risk, making society as a whole, and the financial system in particular, more vulnerable to cyber threats or ICT disruptions. While the ubiquitous use of ICT systems and high digitalisation and connectivity are today core features of the activities of Union financial entities, their digital resilience has yet to be better addressed and integrated into their broader operational frameworks.

(2) ICT の利用は，過去数十年間にわたり，金融サービスの提供における極めて重要な役割を果たして来たのであり，今日，全ての金融機関の典型的な日常業務の運営において不可欠の重要性を獲得するまでに達している。今日，デジタル化は，例えば，現金と紙ベースの手法からデジタルソリューションの利用へと次第に移行してきている決済，並びに，証券の決済と清算，電子的なアルゴリズム取引，融資業務と資金管理業務，ピアツーピア融資，信用格付け，苦情対応及びバックオフィス業務を包摂している。保険部門もまた，インシュアテクを用いてオンラインで運営管理される当該保険仲介事業者のサービスを提供する保険仲介事業者の出現から，デジタル保険引受まで，ICT の利用によって変容してきた。金融は，全部門を通じて大規模にデジタル化していきているというだけではなく，デジタル化もまた，金融部門内における並びにサードパーティのインフラ及びサービスプロバイダとの間における相互の結びつき及び依存性を深化させてきた。

The use of ICT has in the past decades gained a pivotal role in the provision of financial services, to the point where it has now acquired a critical importance in the operation of typical daily functions of all financial entities. Digitalisation now covers, for instance, payments, which have increasingly moved from cash and paper-based methods to the use of digital solutions, as well as securities clearing and settlement, electronic and algorithmic trading, lending and funding operations, peer-to-peer finance, credit rating, claim management and back-office operations. The insurance sector has also been transformed by the use of ICT, from the emergence of insurance intermediaries offering their services online operating with InsurTech, to digital insurance underwriting. Finance has not only become largely digital throughout the whole sector, but digitalisation has also deepened interconnections and dependencies within the financial sector and with third-party infrastructure and service providers.

(3) 欧州システミックリスク委員会（ESBR）は，システミックなサイバーリスクに対処する 2020 年の報告書の中で，局所的なサイバーインシデントが，地理的な境界に遮られることなく，欧州連合の約 2 万 2000 の金融機関のいずれかから金融システム全体へと急速に拡大し得ることから，金融機関，金融市場及び金融市場インフラを横断する既存の高度の相互接続性，並びに，とりわけ，金融機関，金融市場及び金融市場インフラの ICT システムの相互の依存性がいかにシステミックな脆弱性を組成し得るかを再確認した。金融部門の中で発生する重大な ICT 侵害は，金融機関に対して孤立して起きる影響があるだけではない。その ICT 侵害は，金融上の送信の諸経路にわたって局所的な脆弱性の伝播のための方途を円滑するものでもあり，また，流動性が走ることを発生させること及び金融市場

における信用と信頼の全体的な喪失のような，欧州連合の金融システムの安定性を妨げる負の結果の潜在的な引金である。

The European Systemic Risk Board (ESRB) reaffirmed in a 2020 report addressing systemic cyber risk how the existing high level of interconnectedness across financial entities, financial markets and financial market infrastructures, and particularly the interdependencies of their ICT systems, could constitute a systemic vulnerability because localised cyber incidents could quickly spread from any of the approximately 22 000 Union financial entities to the entire financial system, unhindered by geographical boundaries. Serious ICT breaches that occur in the financial sector do not merely affect financial entities taken in isolation. They also smooth the way for the propagation of localised vulnerabilities across the financial transmission channels and potentially trigger adverse consequences for the stability of the Union's financial system, such as generating liquidity runs and an overall loss of confidence and trust in financial markets.

(4) 近年，ICT のリスクは，デジタル回復力を拡大し，技術標準を策定し及び法制上または監督上の仕事を調整する試みの中で，国際的な，欧州連合の及び国内の政策決定者，法制上の当局及び技術標準策定組織の注目を集めてきた。国際的なレベルでは，銀行の監督に関するバーゼル委員会，決済及び市場のインフラに関する委員会，金融安定性理事会，金融安定性協会並びに G7 及び G20 は，様々な主権国家にわたる職務権限のある当局及び市場運営者に対し，それらの者の金融システムの回復力を強化するためツールを提供することを狙いとしている。その仕事は，高度に相互接続されたグローバルな金融システムという文脈における ICT のリスクを適正に検討する必要性及び適格なベストプラクティスのより大きな一貫性を求める必要性によっても駆動されてきた。

In recent years, ICT risk has attracted the attention of international, Union and national policy makers, regulators and standard-setting bodies in an attempt to enhance digital resilience, set standards and coordinate regulatory or supervisory work. At international level, the Basel Committee on Banking Supervision, the Committee on Payments and Market Infrastructures, the Financial Stability Board, the Financial Stability Institute, as well as the G7 and G20 aim to provide competent authorities and market operators across various jurisdictions with tools to bolster the resilience of their financial systems. That work has also been driven by the need to duly consider ICT risk in the context of a highly interconnected global financial system and to seek more consistency of relevant best practices.

(5) 欧州連合の及び国内の狙いを絞った政策上及び立法上の取組みにも拘わらず，ICT のリスクは，欧州連合の金融システムの運営管理上の回復力，遂行能力及び安定性に対して検討課題を呈し続けている。2008 年の金融危機後の改革は，主として欧州連合の金融部門の金融上の回復力を強化し，また，経済，健全性及び市場行動の各観点から，欧州連合の競争力及び安定性を守ることを狙いとしていた。ICT セキュリティ及びデジタル回復力は運営管理上のリスクの一部ではあるが，それらは，金融危機後の法制対象項目ではより少なく焦点が当てられたものであり，かつ，欧州連合の金融サービスの基本方針及び法制の全体像中の幾つかの分野においてのみ，または，ごく少数の構成国においてのみ，策定されてきた。

Despite Union and national targeted policy and legislative initiatives, ICT risk continues to pose a challenge to the

operational resilience, performance and stability of the Union financial system. The reforms that followed the 2008 financial crisis primarily strengthened the financial resilience of the Union financial sector and aimed to safeguard the competitiveness and stability of the Union from economic, prudential and market conduct perspectives. Although ICT security and digital resilience are part of operational risk, they have been less in the focus of the post-financial crisis regulatory agenda and have developed in only some areas of the Union's financial services policy and regulatory landscape, or in only a few Member States.

(6) 「FinTech 行動計画：より競争力のある先進的な欧州金融部門のために」と題する 2018 年 3 月 8 日の通知の中で，欧州委員会は，欧州連合の金融部門の技術上の安全性及び良好な稼働，欧州の金融部門の ICT 侵害及びインシデントからの迅速な復旧を確保するための運営管理上の視点からのものを含め，欧州連合の金融部門をより回復力のあるものとすること，そして，最終的には，ストレスのある状況下を含め，消費者と市場の信頼及び信用も維持しつつ，欧州連合全体にわたる金融サービスの実効的かつ円滑な提供を実現可能にすることが最重要事項であることを強調した。

In its Communication of 8 March 2018 entitled 'FinTech Action plan: For a more competitive and innovative European financial sector', the Commission highlighted the paramount importance of making the Union financial sector more resilient, including from an operational perspective to ensure its technological safety and good functioning, its quick recovery from ICT breaches and incidents, ultimately enabling the effective and smooth provision of financial services across the whole Union, including under situations of stress, while also preserving consumer and market trust and confidence.

(7) 2019 年 4 月，（「欧州の監督当局」または「ESAs」として集団的に知られている）欧州議会及び理事会の規則(EU) No 1093/2010[4]によって設置された欧州の監督当局（欧州銀行局）（「EBA」），欧州議会及び理事会の規則(EU) No 1094/2010[5]によって設置された欧州の監督当局（欧州保険及び企業年金局）（「EIOPA」）並びに欧州議会及び理事会の規則(EU) No 1095/2010[6]によって設置された欧州の監

[4] 欧州監督局（欧州銀行局）を設置する，決定 No 716/2009/EC を改正する及び委員会決定 2009/78/EC を廃止する欧州議会及び理事会の 2010 年 11 月 24 日の規則(EU) No 1093/2010 (OJ L 331, 15.12.2010, p. 12).
Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC (OJ L 331, 15.12.2010, p. 12).

[5] 欧州の監督当局（欧州保険及び企業年金局）を設置し，決定 No 716/2009/EC を改正し及び委員会決定 2009/79/EC を廃止する欧州議会及び理事会の 2010 年 11 月 24 日の規則(EU) No 1094/2010 (OJ L 331, 15.12.2010, p. 48).
Regulation (EU) No 1094/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Insurance and Occupational Pensions Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/79/EC (OJ L 331, 15.12.2010, p. 48).

[6] 欧州の監督当局（欧州証券及び市場局）を設置し，決定 No 716/2009/EC を改正し及び委員会決定 2009/77/EC を廃止する欧州議会及び理事会の 2010 年 11 月 24 日の規則(EU) No 1095/2010 (OJ L 331, 15.12.2010, p. 84).
Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC (OJ L 331, 15.12.2010, p. 84).

督当局(欧州証券及び市場局)(「ESMA」)は，共同して，金融における ICT のリスクに対する一貫性のあるアプローチを求め，かつ，欧州連合の部門別の取組みを介して金融サービス産業のデジタル運営管理上の回復力を比例的な方法で強化することを勧告する技術上の助言を発した。

In April 2019, the European Supervisory Authority (European Banking Authority), (EBA) established by Regulation (EU) No 1093/2010 of the European Parliament and of the Council [4], the European Supervisory Authority (European Insurance and Occupational Pensions Authority), ('EIOPA') established by Regulation (EU) No 1094/2010 of the European Parliament and of the Council [5] and the European Supervisory Authority (European Securities and Markets Authority), ('ESMA') established by Regulation (EU) No 1095/2010 of the European Parliament and of the Council [6] (known collectively as 'European Supervisory Authorities' or 'ESAs') jointly issued technical advice calling for a coherent approach to ICT risk in finance and recommending to strengthen, in a proportionate way, the digital operational resilience of the financial services industry through a sector-specific initiative of the Union.

(8) 欧州連合の金融部門は，単一ルールブックによって規律され，そして，欧州の金融監督制度によって統治されている。ところが，デジタル運営管理上の回復力がデジタル時代における金融の安定性と市場の完全性を確保するために不可欠になってきており，かつ，例えば，共通の健全性基準または市場行動基準よりも劣らず重要であるのにも拘わらず，デジタル運営管理上の回復力及び ICT セキュリティと取組む諸条項は，全面的または一貫性のあるものとしては，いまだに整合化されていない。それゆえ，域内市場の完全性と効率性を保護しかつ域内市場の秩序ある稼働を促進するため，金融部門における ICT リスクの運営管理を監督できるようにするための職務権限のある当局の権限を強化することにより，デジタル運営管理上の回復力をも包摂するための単一ルールブック及び監督の制度が策定されるべきである。

The Union financial sector is regulated by a Single Rulebook and governed by a European system of financial supervision. Nonetheless, provisions tackling digital operational resilience and ICT security are not yet fully or consistently harmonised, despite digital operational resilience being vital for ensuring financial stability and market integrity in the digital age, and no less important than, for example, common prudential or market conduct standards. The Single Rulebook and system of supervision should therefore be developed to also cover digital operational resilience, by strengthening the mandates of competent authorities to enable them to supervise the management of ICT risk in the financial sector in order to protect the integrity and efficiency of the internal market, and to facilitate its orderly functioning.

(9) ICT のリスクと関連する立法上の格差と不平等な国内法制または監督のアプローチは，金融サービスにおける国内市場の稼働を妨げる障碍の引金となり，国境を越えて運営管理している金融機関の設立の自由及びサービス提供の自由の円滑な実行を妨げることの引金となる。異なる構成国で運営管理している同じタイプの金融機関の間の競争も歪められ得る。とりわけ，デジタル運営管理上の回復力試験のように欧州連合の整合化が限定的であった分野または ICT サードパーティリスクの監視のように欧州連合の整合化が不存在であった分野がその場合に該当する。国内レベルで予定されている開発から派生する格差は，域内市場の稼動を妨げ，市場参加者と金融の安定性に不利益を及ぼす障碍を更に生成し得る。

Legislative disparities and uneven national regulatory or supervisory approaches with regard to ICT risk trigger obstacles to the functioning of the internal market in financial services, impeding the smooth exercise of the freedom of establishment and the provision of services for financial entities operating on a cross-border basis. Competition between the same type of financial entities operating in different Member States could also be distorted. This is the case, in particular, for areas where Union harmonisation has been very limited, such as digital operational resilience testing, or absent, such as the monitoring of ICT third-party risk. Disparities stemming from developments envisaged at national level could generate further obstacles to the functioning of the internal market to the detriment of market participants and financial stability.

(10) 今日，ICT のリスクと関連する条項が欧州連合レベルでは部分的にのみ対処されていることのゆえに，ICT と関連するインシデント報告及びデジタル運営管理上の回復力試験のような重要な諸分野における間隙または重複が存在しており，また，多様な国内ルールが生じつつあることの結果としてのまたは重複しているルールの費用対効果の乏しい適用の結果としての一貫性の欠如が存在している。技術上のリスクは国境をもっておらず，かつ，金融部門は欧州連合の内外において国境を越えて広範にそのサービスを展開しているので，このことは，とりわけ，金融部門のような ICT 集約型の利用者にとって不利益となる。国境を越えて運営管理している金融機関または複数の認可を保有している金融機関（例：1 つの金融機関が，1 または複数の構成国の異なる職務権限のある当局からそれぞれ発行された銀行業の許可，投資企業の許可及び決済機関の許可をもち得る）は，一貫性があり費用対効果のある方法で ICT のリスクに対処し及びその金融機関自身に対する ICT のインシデントの負の影響を緩和する上で，運営管理上の検討課題に直面する。

To date, due to the ICT risk related provisions being only partially addressed at Union level, there are gaps or overlaps in important areas, such as ICT-related incident reporting and digital operational resilience testing, and inconsistencies as a result of emerging divergent national rules or cost-ineffective application of overlapping rules. This is particularly detrimental for an ICT-intensive user such as the financial sector since technology risks have no borders and the financial sector deploys its services on a wide cross-border basis within and outside the Union. Individual financial entities operating on a cross-border basis or holding several authorisations (e.g. one financial entity can have a banking, an investment firm, and a payment institution licence, each issued by a different competent authority in one or several Member States) face operational challenges in addressing ICT risk and mitigating adverse impacts of ICT incidents on their own and in a coherent cost-effective way.

(11) 単一ルールブックは，ICT または運営管理上のリスクの包括的な枠組みを伴ってこなかったので，全ての金融機関のための鍵となるデジタル運営管理上の回復力の要件の更なる整合化が求められている。運営管理上の停止に耐えるという観点から，それらの鍵となる要件を基礎とする，金融機関による ICT 実現能力と全体的な回復力の発展は，欧州連合の金融市場の安定性と完全性を維持することの助けとなり，そして，欧州連合における投資家と消費者の高度の保護を確保することに貢献するだろう。この規則は，域内市場の円滑な稼働に貢献することを狙いとしているので，欧州連合の司法裁判所（「司法裁判所」）の一貫性のある判例法に従って解釈されるものとしての欧州連合の機能に関する条約（TFEU）の第 114 条の条項を基礎とすべきである。

As the Single Rulebook has not been accompanied by a comprehensive ICT or operational risk framework, further harmonisation of key digital operational resilience requirements for all financial entities is required. The development of ICT capabilities and overall resilience by financial entities, based on those key requirements, with a view to withstanding operational outages, would help preserve the stability and integrity of the Union financial markets and thus contribute to ensuring a high level of protection of investors and consumers in the Union. Since this Regulation aims to contribute to the smooth functioning of the internal market, it should be based on the provisions of Article 114 of the Treaty on the Functioning of the European Union (TFEU) as interpreted in accordance with the consistent case law of the Court of Justice of the European Union (Court of Justice).

(12) この規則は，これまでは，様々な欧州連合法の中でばらばらに対処されてきた運営管理上のリスクの要件の一部としての ICT のリスクの要件を統合し，かつ，それをアップグレードすることを狙いとしている。それらの法行為は，金融上のリスク（例：信用リスク，市場リスク，取引相手の信用リスク及び流動性リスク，市場行動リスク）の主要な類型を包摂してはいるが，それらの法行為は，それらの法行為の採択の時点においては，運営管理上の回復力の全ての構成要素と包括的に取り組んでいなかった。それらの欧州連合の法行為の中で別の目的のために策定される場合，運営管理上のリスクの諸規定は，しばしば，ICT と関連するインシデントに抗する能力の防護，検出，封じ込め，復旧及び補修のため，または，報告のため及び能力のデジタル試験のための的を絞った定量的な規定ではなく，リスクへの対処のための在来の定量的アプローチ（すなわち，ICT のリスクを補うための資本要件の設定）を好んだ。それらの法行為は，健全性の監督，市場の完全性または市場行動に関する必須の諸規定を包摂し及びアップデートすることを主に意味していた。ICT のリスクに関する異なる諸規定を統合しかつアップグレードすることにより，金融部門におけるデジタルリスクに対処する全ての条項は，一貫性のある態様で，単一の立法行為の中において，初めて集められるべきである。それゆえ，この規則は，当該法行為の中で使用される用語との関係を含め，従前の幾つかの法行為の中にある間隙を埋め，または，一貫性の欠如を解消し，また，ICT リスクマネジメントの実現能力，インシデント報告，運営管理上の回復力試験及び ICT サードパーティリスクの監視に関する的を絞った規定を介して，ICT のリスクを明示で指示する。そして，この規則は，ICT のリスクの理解も向上させ，また，ICT のインシデント及び運営管理上の回復力の欠如が，金融機関の良好性を危険に晒す可能性をもつということの認識も向上させるべきである。

This Regulation aims to consolidate and upgrade ICT risk requirements as part of the operational risk requirements that have, up to this point, been addressed separately in various Union legal acts. While those acts covered the main categories of financial risk (e.g. credit risk, market risk, counterparty credit risk and liquidity risk, market conduct risk), they did not comprehensively tackle, at the time of their adoption, all components of operational resilience. The operational risk rules, when further developed in those Union legal acts, often favoured a traditional quantitative approach to addressing risk (namely setting a capital requirement to cover ICT risk) rather than targeted qualitative rules for the protection, detection, containment, recovery and repair capabilities against ICT-related incidents, or for reporting and digital testing capabilities. Those acts were primarily meant to cover and update essential rules on prudential supervision, market integrity or conduct. By consolidating and upgrading the different rules on ICT risk, all provisions addressing digital risk in the financial sector should for the first time be brought together in a consistent manner in one single legislative act. Therefore, this Regulation fills in the gaps or remedies inconsistencies in some of the prior legal acts,

including in relation to the terminology used therein, and explicitly refers to ICT risk via targeted rules on ICT risk-management capabilities, incident reporting, operational resilience testing and ICT third-party risk monitoring. This Regulation should thus also raise awareness of ICT risk and acknowledge that ICT incidents and a lack of operational resilience have the possibility to jeopardise the soundness of financial entities.

(13) 金融機関は，ICT のリスクに対処する際，その金融機関の規模と全体的なリスクプロファイル並びにその金融機関のサービス，活動及び運営管理の性質，規模及び複雑性を考慮に入れた上で，同一のアプローチと同一の基本原則を基礎とするルールに従うべきである。増加するデジタルリスクを伴っている ICT システム，プラットフォーム及びインフラに対して高度に依拠する時代においては特に，一貫性は，その金融機関への信頼を拡大すること及びその金融機関の安定性を維持することに貢献する。基本的なサイバー衛生を尊重することは，ICT の混乱の影響及び費用をミニマム化することによって，経済に対して重い費用負担を課すことも避けるべきである。

Financial entities should follow the same approach and the same principle-based rules when addressing ICT risk taking into account their size and overall risk profile, and the nature, scale and complexity of their services, activities and operations. Consistency contributes to enhancing confidence in the financial system and preserving its stability especially in times of high reliance on ICT systems, platforms and infrastructures, which entails increased digital risk. Observing basic cyber hygiene should also avoid imposing heavy costs on the economy by minimising the impact and costs of ICT disruptions.

(14) 規則は，法制上の複雑性の削減を助け，監督上の収斂を育成し及び法的確実性を増加させ，かつ，特に国境を越えて運営管理している金融機関にとって，法令遵守の費用を押さえること及び競争の歪みを削減することにも貢献する。それゆえ，金融機関のデジタル運営管理上の回復力のための共通の枠組みを確立するため，規則という法形式を選択することは，欧州連合の金融部門による ICT のリスクマネジメントの全ての構成要素の均質かつ一貫性のある適用を保証するための最も適切な方法である。

A Regulation helps reduce regulatory complexity, fosters supervisory convergence and increases legal certainty, and also contributes to limiting compliance costs, especially for financial entities operating across borders, and to reducing competitive distortions. Therefore, the choice of a Regulation for the establishment of a common framework for the digital operational resilience of financial entities is the most appropriate way to guarantee a homogenous and coherent application of all components of ICT risk management by the Union financial sector.

(15) 欧州議会及び理事会の指令(EU) 2016/1148[7]は，3 つのタイプの金融機関，すなわち，与信機関，取引場所及び中央清算機関にも適用される，欧州連合レベルで制定された最初の横断的なサイバー

[7] 欧州連合全域にわたるネットワーク及び情報システムの共通の高いレベルの安全性のための措置に関する欧州議会及び理事会の 2016 年 7 月 6 日の指令(EU) 2016/1148 (OJ L 194, 19.7.2016, p. 1).
Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).

セキュリティの枠組みであった。ただし，指令(EU) 2016/1148 は，必須サービスの運営者の国内レベルにおける識別の仕組みを定めているので，実務上においては，構成国によって識別された一定の与信機関，取引場所及び中央清算機関のみがその適用範囲内に入れられてきたのであり，また，それゆえに，同指令の中で定められた ICT のセキュリティの要件及びインシデント通知の要件を遵守することが要求されてきた。欧州議会及び理事会の指令(EU) 2022/2555[8]は，同指令の適用範囲における 3 つのタイプの金融機関も維持しつつ，同指令の適用範囲内にある法主体を決定するための統一的な基準（規模上限規定）を定めている。

Directive (EU) 2016/1148 of the European Parliament and of the Council [7] was the first horizontal cybersecurity framework enacted at Union level, applying also to three types of financial entities, namely credit institutions, trading venues and central counterparties. However, since Directive (EU) 2016/1148 set out a mechanism of identification at national level of operators of essential services, only certain credit institutions, trading venues and central counterparties that were identified by the Member States, have been brought into its scope in practice, and hence required to comply with the ICT security and incident notification requirements laid down in it. Directive (EU) 2022/2555 of the European Parliament and of the Council [8] sets a uniform criterion to determine the entities falling within its scope of application (size-cap rule) while also keeping the three types of financial entities in its scope.

(16) しかしながら，この規則は，欧州連合の現行の金融サービス法の中で定められている諸要件と比較してより厳格な，ICT リスクマネジメント及び ICT と関連するインシデント報告に関する諸要件を導入することによって，デジタル回復力の様々な構成要素の整合化のレベルを増加させているので，この高いレベルは，指令(EU) 2022/2555 の中で定められている諸要件と比較しても増加された整合化となっている。その結果として，この規則は，指令(EU) 2022/2555 との関係において*特別法*となっている。それと同時に，金融部門と，構成国によって採択されるサイバーセキュリティ戦略の一貫性を確保するため，及び，金融監督当局が，同指令によって包摂されている別の部門に対して影響を与えるサイバーインシデントに気づくことができるようにするために，現在では指令(EU) 2022/2555 の中で定められている欧州連合の横断的なサイバーセキュリティの枠組みとの間の強力な関係を維持することが重要である。

However, as this Regulation increases the level of harmonisation of the various digital resilience components, by introducing requirements on ICT risk management and ICT-related incident reporting that are more stringent in comparison to those laid down in the current Union financial services law, this higher level constitutes an increased harmonisation also in comparison with the requirements laid down in Directive (EU) 2022/2555. Consequently, this Regulation constitutes *lex specialis* with regard to Directive (EU) 2022/2555. At the same time, it is crucial to maintain a

[8] 欧州全域の共通の高いレベルのサイバーセキュリティのための措置に関する，規則(EU) No 910/2014 及び指令(EU) 2018/1972 を改正し並びに指令(EU) 2016/1148 を廃止する欧州議会及び理事会の 2022 年 12 月 14 日の指令(EU) 2022/2555（NIS2 指令）（この官報の 80 頁参照）.
Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (see page 80 of this Official Journal).

strong relationship between the financial sector and the Union horizontal cybersecurity framework as currently laid out in Directive (EU) 2022/2555 to ensure consistency with the cyber security strategies adopted by Member States and to allow financial supervisors to be made aware of cyber incidents affecting other sectors covered by that Directive.

(17) 欧州連合条約の第 4 条第 2 項に従い，かつ，司法裁判所による司法上の見直しを妨げることなく，この規則は，例えば，国家安全保障の安全確保に反するような情報の供給と関係して，公共の保安，国防及び国家安全保障の安全確保と関係する国家の必須機能と関連する構成国の責務に対して影響を与えてはならない。

In accordance with Article 4(2) of the Treaty on European Union and without prejudice to the judicial review by the Court of Justice, this Regulation should not affect the responsibility of Member States with regard to essential State functions concerning public security, defence and the safeguarding of national security, for example concerning the supply of information which would be contrary to the safeguarding of national security.

(18) 部門間の学習を実現可能にするため及びサイバー脅威を取扱う際に別の部門の経験を実効的に活かすため，指令(EU) 2022/2555 に示す金融機関は，同指令の「エコシステム」の一部（例えば，協力グループ及びコンピュータセキュリティインシデント対応チーム（CSIRTs））であることを維持すべきである。ESA 及び職務権限のある国内当局は，同指令の下における戦略上の政策の討議と協力グループの技術的な作業に参加できるべきであり，また，同指令に従って指定または設置された単一連絡部局との間で情報を交換し及び更に協力できるべきである。この規則の下にある職務権限のある当局は，CSIRTs との間においても意見聴取し及び協力すべきである。職務権限のある当局は，指令(EU) 2022/2555 に従って指定または設置された職務権限のある当局からの技術上の助言を求めることもでき，また，実効的かつ迅速に対応する調整の仕組みを確保することを狙いとする協力覚書の締結もできるべきである。

To enable cross-sector learning and to effectively draw on experiences of other sectors in dealing with cyber threats, the financial entities referred to in Directive (EU) 2022/2555 should remain part of the 'ecosystem' of that Directive (for example, Cooperation Group and computer security incident response teams (CSIRTs)).The ESAs and national competent authorities should be able to participate in the strategic policy discussions and the technical workings of the Cooperation Group under that Directive, and to exchange information and further cooperate with the single points of contact designated or established in accordance with that Directive. The competent authorities under this Regulation should also consult and cooperate with the CSIRTs. The competent authorities should also be able to request technical advice from the competent authorities designated or established in accordance with Directive (EU) 2022/2555 and establish cooperation arrangements that aim to ensure effective and fast-response coordination mechanisms.

(19) 金融機関のデジタル回復力と物理的な回復力との間の強力な相互の牽連性に鑑み，この規則並びに欧州議会及び理事会の指令(EU) 2022/2557[9]においては，不可欠法主体の回復力に関する一

[9] 不可欠法主体の回復力に関する及び理事会指令 2008/114/EC を廃止する欧州議会及び理事会の 2022 年 12 月 14 日の指令(EU)2022/2557（この官報の 164 頁参照）。

貫性のあるアプローチが必要である。金融機関の物理的な回復力が，この規則によって包摂されている ICT リスクマネジメント及び報告義務によって包括的な態様で対処されていることに鑑み，指令(EU) 2022/2557 の第 III 章及び第 IV 章の中で定められた義務は，同指令の適用範囲内にある金融機関に対して適用してはならない。

Given the strong interlinkages between the digital resilience and the physical resilience of financial entities, a coherent approach with regard to the resilience of critical entities is necessary in this Regulation and Directive (EU) 2022/2557 of the European Parliament and the Council [9]. Given that the physical resilience of financial entities is addressed in a comprehensive manner by the ICT risk management and reporting obligations covered by this Regulation, the obligations laid down in Chapters III and IV of Directive (EU) 2022/2557 should not apply to financial entities falling within the scope of that Directive.

(20) クラウドコンピューティングサービスのプロバイダは，指令(EU) 2022/2555 によって包摂されているデジタルインフラの一類型である。この規則によって設けられる欧州連合の監督枠組み（「監督枠組み」）は，金融機関に対して ICT サービスを提供しているクラウドコンピューティングサービスのプロバイダを含め，全ての不可欠 ICT サードパーティサービスプロバイダに対して適用され，かつ，指令(EU) 2022/2555 によって実施される監督を補完するものと判断されるべきである。更に，この規則によって設けられる監督枠組みは，デジタル監督当局を設けている欧州連合の横断的な枠組みが存在してない クラウドコンピューティングサービスプロバイダを包摂すべきである。

Cloud computing service providers are one category of digital infrastructure covered by Directive (EU) 2022/2555. The Union Oversight Framework ('Oversight Framework') established by this Regulation applies to all critical ICT third-party service providers, including cloud computing service providers providing ICT services to financial entities, and should be considered complementary to the supervision carried out pursuant to Directive (EU) 2022/2555. Moreover, the Oversight Framework established by this Regulation should cover cloud computing service providers in the absence of a Union horizontal framework establishing a digital oversight authority.

(21) ICT のリスクに対する全面的な管理を維持するため，金融機関は，強力かつ実効性のある ICT リスクマネジメント，並びに，ICT と関連する全てのインシデントを取扱うため及び ICT と関連する大きなインシデントを報告するための個別の仕組み及び基本方針を実現可能にするための包括的な実現能力をもつ必要がある。同様に，金融機関は，ICT システムの試験，管理策及び処理のため並びに ICT サードパーティリスクを取扱うための基本方針をもつべきである。金融機関のためのデジタル運営管理上の回復力の基線は，一定の金融機関，とりわけマイクロ企業及び簡素化された ICT リスクマネジメント枠組みに服する金融機関に対する諸要件の比例的な適用も認めつつ，増加されるべきである。職務権限のある当局にかかる行政上の負担を軽減する必要性に比例的でありかつその必要性に対処している職域退職者給付機関の効率的な監督を容易にするため，そのような金融機関

Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (see page 164 of this Official Journal).

との関係における適格な国内監督上の手立ては，欧州議会及び理事会の指令(EU) 2016/2341[10]の第 5 条の中で定められている適格な閾値を超過している場合であっても，その金融機関の規模及び全体的なリスクプロファイル，その金融機関のサービス，活動及び運営管理の性質，規模及び複雑性，を考慮に入れるべきである。とりわけ，監督活動は，主として，特定の法主体の ICT リスクマネジメントと関係する重大なリスクに対処する必要性に焦点を当てるべきである。

In order to maintain full control over ICT risk, financial entities need to have comprehensive capabilities to enable a strong and effective ICT risk management, as well as specific mechanisms and policies for handling all ICT-related incidents and for reporting major ICT-related incidents. Likewise, financial entities should have policies in place for the testing of ICT systems, controls and processes, as well as for managing ICT third-party risk. The digital operational resilience baseline for financial entities should be increased while also allowing for a proportionate application of requirements for certain financial entities, particularly microenterprises, as well as financial entities subject to a simplified ICT risk management framework. To facilitate an efficient supervision of institutions for occupational retirement provision that is proportionate and addresses the need to reduce administrative burdens on the competent authorities, the relevant national supervisory arrangements in respect of such financial entities should take into account their size and overall risk profile, and the nature, scale and complexity of their services, activities and operations even when the relevant thresholds established in Article 5 of Directive (EU) 2016/2341 of the European Parliament and of the Council [(10)] are exceeded. In particular, supervisory activities should focus primarily on the need to address serious risks associated with the ICT risk management of a particular entity.

職務権限のある当局は，指令(EU) 2016/2341 の第 31 条に従って，資産管理，保険数理計算，会計及びデータ管理のような，同基金のコアとなる事業の大部分をサービスプロバイダにアウトソースする職域退職給付機関の監督との関係において，慎重かつ比例的なアプローチも維持すべきである。

Competent authorities should also maintain a vigilant but proportionate approach in relation to the supervision of institutions for occupational retirement provision which, in accordance with Article 31 of Directive (EU) 2016/2341, outsource a significant part of their core business, such as asset management, actuarial calculations, accounting and data management, to service providers.

(22) ICT と関連するインシデント報告の閾値及び分類法は，国内レベルにおいて大きく異なっている。共通点は，欧州議会及び理事会の規則(EU) 2019/881[11]によって設置された欧州連合サイバーセキュリ

---

[10] 職域年金給付機関（IORPs）の活動及び監督に関する欧州議会及び理事会の 2016 年 12 月 14 日の指令(EU) 2016/2341 (OJ L 354, 23.12.2016, p. 37).

Directive (EU) 2016/2341 of the European Parliament and of the Council of 14 December 2016 on the activities and supervision of institutions for occupational retirement provision (IORPs) (OJ L 354, 23.12.2016, p. 37).

[11] ENISA（欧州連合サイバーセキュリティ局）に関する及び情報通信技術のサイバーセキュリティ認証に関する並びに規則(EU)No 526/2013 を廃止する欧州議会及び理事会の 2019 年 4 月 17 日の規則(EU)2019/881（サイバーセキュリティ法） (OJ L 151, 7.6.2019, p. 15).

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing

ティ局（ENISA）及び指令(EU) 2022/2555 の下にある協力グループによって実施される適格な作業を通じて到達され得るが，閾値の設定及び分類法の利用に関する多様なアプローチが依然として存在しており，または，残りの金融機関に関して発生し得る。それらの多様性のゆえに，特に複数の構成国にわたって運営管理する場合または金融グループの一部となっている場合において金融機関が遵守しなければならない多重の要件が存在している。更に，そのような多様性は，報告のプロセスを加速し，かつ，潜在的にシステミックな結果をもたらす大規模攻撃の際における ICT のリスクに対処するために重要な職務権限のある当局の間の迅速かつ円滑な情報交換を支える，より統一化または集中化された欧州連合の仕組みの創設を妨げる可能性がある。

ICT-related incident reporting thresholds and taxonomies vary significantly at national level. While common ground may be achieved through the relevant work undertaken by the European Union Agency for Cybersecurity (ENISA) established by Regulation (EU) 2019/881 of the European Parliament and of the Council [(11)] and the Cooperation Group under Directive (EU) 2022/2555, divergent approaches on setting the thresholds and use of taxonomies still exist, or can emerge, for the remainder of financial entities. Due to those divergences, there are multiple requirements that financial entities must comply with, especially when operating across several Member States and when part of a financial group. Moreover, such divergences have the potential to hinder the creation of further uniform or centralised Union mechanisms that speed up the reporting process and support a quick and smooth exchange of information between competent authorities, which is crucial for addressing ICT risk in the event of large-scale attacks with potentially systemic consequences.

(23) 行政上の負担及び一定の金融機関の潜在的に重複する報告義務を削減するため，欧州議会及び理事会の指令(EU) 2015/2366[12]によるインシデント報告に関する要件は，この規則の適用範囲内にある決済サービスプロバイダに対しては適用を終えるべきである。その結果，同指令の第 33 条第 1 項に示す与信機関，電子マネー機関，決済機関及び口座情報サービスプロバイダは，この規則の適用の日から，この規則により，そのようなインシデントが ICT と関連するか否かに拘わらず，従前は同指令により報告された運営管理または決済の安全性と関連する全てのインシデントを報告すべきである。

To reduce the administrative burden and potentially duplicative reporting obligations for certain financial entities, the requirement for the incident reporting pursuant to Directive (EU) 2015/2366 of the European Parliament and of the Council [(12)] should cease to apply to payment service providers that fall within the scope of this Regulation. Consequently, credit institutions, e-money institutions, payment institutions and account information service providers, as referred to in Article 33(1) of that Directive, should, from the date of application of this Regulation, report pursuant to

---

Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15).

12 域内市場における決済サービスに関する並びに指令 2002/65/EC，指令 2009/110/EC，指令 2013/36/EU 及び規則(EU)No 1093/2010 を改正し，指令 2007/64/EC を廃止する欧州議会及び理事会の 2015 年 11 月 25 日の指令(EU) 2015/2366 (OJ L 337, 23.12.2015, p. 35).

Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337, 23.12.2015, p. 35).

this Regulation, all operational or security payment-related incidents which have been previously reported pursuant to that Directive, irrespective of whether such incidents are ICT-related.

(24) 職務権限のある当局が，ICT と関連するインシデントの性質，頻度，大きさ及び影響の完全な概況を獲得することによって監督の役割を満たすことができるようにするため，及び，法執行機関及び破綻処理当局を含め，適格な行政機関との間の情報交換を拡大できるようにするため，この規則は，ICT と関連するインシデントの堅牢な報告体制を定め，それによって，金融サービス法の中にある現在の間隙に対して適格な要件が対処し，費用を軽減するために既存の重複を除去すべきである。この規則に定める単一の揃えられた枠組みを介して当該金融機関の職務権限のある当局に対して報告することを全ての金融機関に対して要求することにより，ICT と関連するインシデント報告体制を整合化することが必須である。加えて，ESAs は，分類法，時間枠，データセット，雛型及び適用可能な閾値のような，ICT と関連するインシデント報告の枠組みのための適格な要素をより細目的に指定する権限を与えられるべきである。指令(EU) 2022/2555 との全面的な一貫性を確保するため，金融機関は，そのサイバー脅威が金融システム，サービス利用者または顧客と関係する脅威であるとその金融機関が判断するときは，任意で，適格な職務権限のある当局に対して大きなサイバー脅威を通知できるべきである。

To enable competent authorities to fulfil supervisory roles by acquiring a complete overview of the nature, frequency, significance and impact of ICT-related incidents and to enhance the exchange of information between relevant public authorities, including law enforcement authorities and resolution authorities, this Regulation should lay down a robust ICT-related incident reporting regime whereby the relevant requirements address current gaps in financial services law, and remove existing overlaps and duplications to alleviate costs. It is essential to harmonise the ICT-related incident reporting regime by requiring all financial entities to report to their competent authorities through a single streamlined framework as set out in this Regulation. In addition, the ESAs should be empowered to further specify relevant elements for the ICT-related incident reporting framework, such as taxonomy, timeframes, data sets, templates and applicable thresholds. To ensure full consistency with Directive (EU) 2022/2555, financial entities should be allowed, on a voluntary basis, to notify significant cyber threats to the relevant competent authority, when they consider that the cyber threat is of relevance to the financial system, service users or clients.

(25) デジタル運営管理上の回復力試験の要件は，全面的に揃えられているとは限らない枠組みを定めている一定の金融副部門において策定されてきた。このことは，国境を越える金融機関にとっての費用の潜在的な重複を導き，また，デジタル運営管理上の回復力試験の結果の相互承認を複雑にする。そのことは，次第に，域内市場を断片化させ得る。

Digital operational resilience testing requirements have been developed in certain financial subsectors setting out frameworks that are not always fully aligned. This leads to a potential duplication of costs for cross-border financial entities and makes the mutual recognition of the results of digital operational resilience testing complex which, in turn, can fragment the internal market.

(26) 加えて，いかなる ICT 試験も要求されない場合，脆弱性が検出されないままであり，金融機関が ICT

のリスクに晒されることを帰結し，そして，最終的には，金融部門の安定性と完全性を妨げる高度のリスクをつくり出す。欧州連合の介入がなければ，デジタル運営管理上の回復力試験は，一貫性を欠き続けるだろうし，また，異なる主権国家にわたる ICT 試験の結果の相互承認のシステムを欠くことになるだろう。加えて，他の金融副部門は有意な規模の試験制度を採択しそうにないので，それらの副部門は，ICT の脆弱性とリスクを明らかにすること，防御上の実現能力と事業継続性を試験することという面において，試験の枠組みの，顧客，供給者及び事業上のパートナーの信頼を向上させることに貢献するという潜在的な受益を失うことだろう。それらの重複，多様性及び間隙を解消するため，調整された試験体制のための規定を定める必要があり，そして，それによって，この規則の中で定められた基準に適合する金融機関のための高度な試験の相互承認を促進する必要がある。

In addition, where no ICT testing is required, vulnerabilities remain undetected and result in exposing a financial entity to ICT risk and ultimately create a higher risk to the stability and integrity of the financial sector. Without Union intervention, digital operational resilience testing would continue to be inconsistent and would lack a system of mutual recognition of ICT testing results across different jurisdictions. In addition, as it is unlikely that other financial subsectors would adopt testing schemes on a meaningful scale, they would miss out on the potential benefits of a testing framework, in terms of revealing ICT vulnerabilities and risks, and testing defence capabilities and business continuity, which contributes to increasing the trust of customers, suppliers and business partners. To remedy those overlaps, divergences and gaps, it is necessary to lay down rules for a coordinated testing regime and thereby facilitate the mutual recognition of advanced testing for financial entities meeting the criteria set out in this Regulation.

(27) ICT サービスの利用に対する金融機関の依拠は，部分的には，それらの金融機関の，競争的なデジタルグローバル経済の出現に適応し，事業の効率性を加速し及び消費者の求めに応ずる必要性によって駆動されている。そのような依拠の性質及び範囲は，近年において進化し続けており，金融の仲介における費用の削減を導いており，複雑な内部処理を取扱うための幅広い ICT ツールを提供しつつ，金融活動の配置における事業の拡大と拡張性を実現可能にしてきた。

Financial entities' reliance on the use of ICT services is partly driven by their need to adapt to an emerging competitive digital global economy, to boost their business efficiency and to meet consumer demand. The nature and extent of such reliance has been continuously evolving in recent years, driving cost reduction in financial intermediation, enabling business expansion and scalability in the deployment of financial activities while offering a wide range of ICT tools to manage complex internal processes.

(28) ICT サービスの広範な利用は，複雑な契約条項によって証明される。そのことにより，金融機関は，しばしば，当該金融機関が服している健全性の基準またはそれ以外の法制上の要件に個別対応する契約条件の交渉における困難と直面し，あるいは，当該金融機関の契約条項中に当該権利が掲げられている場合においてさえ，アクセスの権利や監査の権利のような，個々の権利の行使における困難と直面する。更に，それらの契約条項の多くは，下請契約の過程を完全に監視できるようにする十分な安全確保を定めておらず，そのことは，金融機関から，関連するリスクを評価するためのその金融機関の能力を奪っている。加えて，ICT サードパーティサービスプロバイダは，しばしば，異なるタイプの顧客に対して標準化されたサービスを提供するので，そのような契約条項は，金融業の

関係者の個々の需要または個別の需要に対して必ずしも適切に対応しているわけではない。

The extensive use of ICT services is evidenced by complex contractual arrangements, whereby financial entities often encounter difficulties in negotiating contractual terms that are tailored to the prudential standards or other regulatory requirements to which they are subject, or otherwise in enforcing specific rights, such as access or audit rights, even when the latter are enshrined in their contractual arrangements. Moreover, many of those contractual arrangements do not provide for sufficient safeguards allowing for the fully-fledged monitoring of subcontracting processes, thus depriving the financial entity of its ability to assess the associated risks. In addition, as ICT third-party service providers often provide standardised services to different types of clients, such contractual arrangements do not always cater adequately for the individual or specific needs of financial industry actors.

(29) 欧州連合の金融サービス法は，アウトソーシングに関する一定の一般的な規定を含んでいるとはいえ，契約の局面の監視が欧州連合法の中で全面的に定められているわけではない。ICT のサードパーティサービスプロバイダとの間で締結される契約条項に適用される欧州連合の明確かつ個別対応の基準が存在しなければ，ICT のリスクの外部発生源は，包括的に対処されない。そのため，金融機関の ICT サードパーティリスクの管理の指針となる一定の鍵となる基本原則を定める必要がある。当該金融機関の不可欠な機能または重要な機能を支えるために，金融機関が ICT サードパーティサービスプロバイダに頼る場合，その基本原則は，とりわけ重要性をもつものである。それらの基本原則は，ICT サードパーティサービスプロバイダの側で生じている全ての ICT リスクを実効的に監視するための金融機関の能力を強化するため，一定のミニマムの安全確保を提供するという観点から，契約条項の効力及び有効期間における幾つかの要素との関係において，コアとなる契約上の権利のセットを伴うべきである。それらの基本原則は，アウトソーシングに適用可能な部門別の法律を補完する。

Even though Union financial services law contains certain general rules on outsourcing, monitoring of the contractual dimension is not fully anchored into Union law. In the absence of clear and bespoke Union standards applying to the contractual arrangements concluded with ICT third-party service providers, the external source of ICT risk is not comprehensively addressed. Consequently, it is necessary to set out certain key principles to guide financial entities' management of ICT third-party risk, which are of particular importance when financial entities resort to ICT third-party service providers to support their critical or important functions. Those principles should be accompanied by a set of core contractual rights in relation to several elements in the performance and termination of contractual arrangements with a view to providing certain minimum safeguards in order to strengthen financial entities' ability to effectively monitor all ICT risk emerging at the level of third-party service providers. Those principles are complementary to the sectoral law applicable to outsourcing.

(30) 今日，ICT サードパーティリスクの監視及び ICT サードパーティ依存性と関連する均一性と収斂の一定の欠如が明らかである。2019 年のアウトソーシングに関する EBA 運用指針及び 2021 年のクラウドサービスプロバイダへのアウトソーシングに関する ESMA 運用指針のような，アウトソーシングに対処するための努力にも拘わらず，ごく限られた数の不可欠な ICT サードパーティサービスプロバイダに対して金融部門が晒されていることが引金となりかもしれない反作用的なシステミックリスクというより

広範な問題は，欧州連合法によっては十分に対処されていない。欧州連合レベルの規定の欠如は，金融監督当局が ICT サードパーティ依存性の良い理解を獲得できるようにし，また，ICT サードパーティ依存の集中から生ずるリスクを適切に監視できるようにするための権限及びツールに関する国内規定の欠如によって複合化されている。

A certain lack of homogeneity and convergence regarding the monitoring of ICT third-party risk and ICT third-party dependencies is evident today. Despite efforts to address outsourcing, such as EBA Guidelines on outsourcing of 2019 and ESMA Guidelines on outsourcing to cloud service providers of 2021 the broader issue of counteracting systemic risk which may be triggered by the financial sector's exposure to a limited number of critical ICT third-party service providers is not sufficiently addressed by Union law. The lack of rules at Union level is compounded by the absence of national rules on mandates and tools that allow financial supervisors to acquire a good understanding of ICT third-party dependencies and to monitor adequately risks arising from the concentration of ICT third-party dependencies.

(31) アウトソーシングの実務の増加に伴う及び ICT サードパーティの集中に伴う潜在的なシステミックリスクを考慮に入れた上で，かつ，不可欠 ICT サードパーティサービスプロバイダにおいて発生する ICT リスクの結果として生ずることを定量評価し，定性評価し及び解消するための適切なツールを金融監督当局に提供することにおける国内の仕組みが不十分であることに留意した上で，金融機関以外の顧客の機密性と安全性が守られることを確保しつつ，金融機関向けの不可欠 ICT サードパーティサービスプロバイダである ICT サードパーティサービスプロバイダの活動を継続的に監視できるようにする適切な監督枠組みを設ける必要がある。ICT サービスのグループ内提供は個別のリスクと利益を伴うが，それは，金融グループの外にあるプロバイダからの ICT サービスの提供よりもリスクが低いと自動的に判断されてはならず，また，それゆえ，同じ法制上の枠組みに服するべきである。ただし，同一の金融グループ内から ICT サービスが提供される場合，金融機関は，グループ内プロバイダに対するより高いレベルの管理をもち得る。それは，全体的なリスク評価の中で考慮に入れられるべきである。

Taking into account the potential systemic risk entailed by increased outsourcing practices and by the ICT third-party concentration, and mindful of the insufficiency of national mechanisms in providing financial supervisors with adequate tools to quantify, qualify and redress the consequences of ICT risk occurring at critical ICT third-party service providers, it is necessary to establish an appropriate Oversight Framework allowing for a continuous monitoring of the activities of ICT third-party service providers that are critical ICT third-party service providers to financial entities, while ensuring that the confidentiality and security of customers other than financial entities is preserved. While intra-group provision of ICT services entails specific risks and benefits, it should not be automatically considered less risky than the provision of ICT services by providers outside of a financial group and should therefore be subject to the same regulatory framework. However, when ICT services are provided from within the same financial group, financial entities might have a higher level of control over intra-group providers, which ought to be taken into account in the overall risk assessment.

(32) ICT のリスクがますます複雑で巧妙になってきていることから，ICT のリスクの検出及び防止のための良い手段は，金融機関の間における脅威と脆弱性の知識の定期的な共有に大きな範囲で依存している。情報共有は，サイバー脅威の認識の増加をつくり出すことに貢献する。更に，そのことは，サ

イバー脅威が現実の ICT と関連するインシデントになることを防止するための金融機関の能力を拡大し，また，金融機関が，ICT と関連するインシデントの影響をより実効的に抑え込み，かつ，より迅速に復旧できるようにする。欧州連合レベルの運用指針がないので，幾つかの要因，とりわけ，その知識共有とデータ保護，独占禁止及び法的責任の諸規定との間の互換性に関する不確実性が，そのような知識の共有を阻害しているように思われる。

With ICT risk becoming more and more complex and sophisticated, good measures for the detection and prevention of ICT risk depend to a great extent on the regular sharing between financial entities of threat and vulnerability intelligence. Information sharing contributes to creating increased awareness of cyber threats. In turn, this enhances the capacity of financial entities to prevent cyber threats from becoming real ICT-related incidents and enables financial entities to more effectively contain the impact of ICT-related incidents and to recover faster. In the absence of guidance at Union level, several factors seem to have inhibited such intelligence sharing, in particular uncertainty about its compatibility with data protection, anti-trust and liability rules.

(33) 加えて，他の市場の参加者との間において，または，（分析上の入力ための ENISA のような，または，法執行目的のための Europol のような）非監督の機関との間において共有され得る情報のタイプに関する疑問は，有用な情報が隠蔽されることを導く。それゆえ，現在のところ，情報共有の範囲及び質は，限定的でありかつ断片化されたままであって，適格な交換は主として（国内的な取組みにより）地域的に行われており，また，統合された金融システムの需要に個別対応する欧州連合全体の情報共有協定との一貫性がない。それゆえ，それらの通信経路を強化することが重要である。

In addition, doubts about the type of information that can be shared with other market participants, or with non-supervisory authorities (such as ENISA, for analytical input, or Europol, for law enforcement purposes) lead to useful information being withheld. Therefore, the extent and quality of information sharing currently remains limited and fragmented, with relevant exchanges mostly being local (by way of national initiatives) and with no consistent Union-wide information-sharing arrangements tailored to the needs of an integrated financial system. It is therefore important to strengthen those communication channels.

(34) 金融機関は，情報共有協定に参加することにより，適切に，サイバー脅威を評価し，監視し，それに抗して防御しかつそれに対応するための金融機関の実現能力を拡大するという観点から，金融機関の間においてサイバー脅威の情報と知識を交換すること，及び，戦略レベル，戦術レベル及び運用レベルにおける金融機関の個々の知識と実務上の経験を集団的に梃入れすることに努めるべきである。それゆえ，任意の情報共有協定のための仕組みの欧州連合レベルでの出現を実現可能にする必要がある。その情報共有協定は，信頼できる環境において締結されるときは，ICT のリスクの拡散を迅速に抑制することによって及び金融の経路全部を通じて潜在的な伝播を抑止することによって，サイバー脅威を防止し及び集団的に対応するために，金融産業のコミュニティを助けるだろう。それらの仕組みは，「横断的な協力協定に対する欧州連合の機能に関する条約の第 101 条の適用可能性に関する運用指針」と題する 2011 年 1 月 14 日の委員会通知の中で定められた欧州連合の適用可能な競争法上の諸規定，及び，欧州連合のデータ保護規定，とりわけ，欧州議会及び理事会の規則(EU) 2016/679[13]を遵守すべきである。それらの仕組みは，同規則の第 6 条第 1 項(f)に示す，

管理者によってまたはサードパーティによって求められる適正な利益の目的のために必要となる個人データの処理の過程におけるような，並びに，同規則の第 6 条第 1 項の(c)及び(e)にそれぞれ示す，管理者が服する法律上の義務の遵守のために必要となる，または，公共の利益においてもしくは管理者に属する公的権限の行使において行われる職務の遂行のために必要となる個人データの処理の過程におけるような，同規則の第 6 条の中で定められている 1 または複数の法的根拠を基礎として運用すべきである。

Financial entities should be encouraged to exchange among themselves cyber threat information and intelligence, and to collectively leverage their individual knowledge and practical experience at strategic, tactical and operational levels with a view to enhancing their capabilities to adequately assess, monitor, defend against, and respond to cyber threats, by participating in information sharing arrangements. It is therefore necessary to enable the emergence at Union level of mechanisms for voluntary information-sharing arrangements which, when conducted in trusted environments, would help the community of the financial industry to prevent and collectively respond to cyber threats by quickly limiting the spread of ICT risk and impeding potential contagion throughout the financial channels. Those mechanisms should comply with the applicable competition law rules of the Union set out in the Communication from the Commission of 14 January 2011 entitled 'Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal cooperation agreements', as well as with Union data protection rules, in particular Regulation (EU) 2016/679 of the European Parliament and of the Council [13]. They should operate based on the use of one or more of the legal bases that are laid down in Article 6 of that Regulation, such as in the context of the processing of personal data that is necessary for the purposes of the legitimate interest pursued by the controller or by a third party, as referred to in Article 6(1), point (f), of that Regulation, as well as in the context of the processing of personal data necessary for compliance with a legal obligation to which the controller is subject, necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, as referred to in Article 6(1), points (c) and (e), respectively, of that Regulation.

(35) 金融部門全体のための高度のデジタル運営管理上の回復力を維持するため，及び，それと同時に，技術の発展のペースを保つために，この規則は，全てのタイプの ICT サービスから派生するリスクに対応すべきである。その目的のために，この規則の文脈における ICT サービスの定義は，ICT システムを通じて，1 または複数の内部利用者または外部利用者に対して継続的に提供されるデジタルサービスとデータサービスを包含する広い態様で理解されるべきである。その定義は，例えば，いわゆる「オーバーザトップ」サービスを含めるべきである。それは，電気通信サービスの類型の中にある。公衆電話交換ネットワーク（PSTN）サービス，地上線電話サービス，旧型単純電話サービス（POTS）または固定線電話サービスとして分類される在来型のアナログ電話サービスという限定された類型

13 個人データの処理と関連する自然人の保護及びそのようなデータの支障のない移動に関する並びに指令 95/46/EC を廃止する欧州議会及び理事会の 2016 年 4 月 27 日の規則(EU) 2016/679（一般データ保護規則）(OJ L 119, 4.5.2016, p. 1).
Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

のみが除外されるべきである。

In order to maintain a high level of digital operational resilience for the whole financial sector, and at the same time to keep pace with technological developments, this Regulation should address risk stemming from all types of ICT services. To that end, the definition of ICT services in the context of this Regulation should be understood in a broad manner, encompassing digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis. That definition should, for instance, include so called 'over the top' services, which fall within the category of electronic communications services. It should exclude only the limited category of traditional analogue telephone services qualifying as Public Switched Telephone Network (PSTN) services, landline services, Plain Old Telephone Service (POTS), or fixed-line telephone services.

(36) この規則によって想定されている広範な包摂範囲に拘わらず，デジタル運営管理上の回復力の規定の適用は，その規模の面における金融機関間の大きな相違及び全体的なリスクプロファイルを考慮に入れるべきである。一般原則として，ICT リスクマネジメント枠組みの実装のために資源及び実現能力を分配する際，金融機関は，その金融機関の規模及び全体的なリスクプロファイルに見合ったその金融機関の ICT 関連の必要性と，その金融機関のサービス，活動及び運営管理の性質，規模及び複雑性との間の適正なバランスをとるべきであり，他方において，職務権限のある当局は，そのような分配のアプローチを評価し及び見直し続けるべきである。

Notwithstanding the broad coverage envisaged by this Regulation, the application of the digital operational resilience rules should take into account the significant differences between financial entities in terms of their size and overall risk profile. As a general principle, when distributing resources and capabilities for the implementation of the ICT risk management framework, financial entities should duly balance their ICT-related needs to their size and overall risk profile, and the nature, scale and complexity of their services, activities and operations, while competent authorities should continue to assess and review the approach of such distribution.

(37) 指令(EU) 2015/2366 の第 33 条第 1 項に示す口座情報サービスプロバイダは，当該プロバイダの活動の特性及びその活動から生ずるリスクを考慮に入れ，明示で，この規則の適用範囲に含められる。加えて，欧州議会及び理事会の指令 2009/110/EC[14]の第 9 条第 1 項及び指令(EU) 2015/2366 の第 32 条第 1 項により適用除外とされている電子マネー機関及び決済機関は，それらの機関が指令 2009/110/EC に従って電子マネーを発行するための承認を与えられていない場合であっても，また，それらの機関が指令(EU) 2015/2366 に従って決済サービスを提供及び実行するための承認を与えられていない場合であっても，この規則の適用範囲に含められる。ただし，欧州議会及び理事会の指

[14] 電子マネー機関の事業の開始，遂行及び健全性監督に関する，指令 2005/60/EC 及び 2006/48/EC を改正し並びに指令 2000/46/EC を廃止する欧州議会及び理事会の 2009 年 9 月 16 日の指令 2009/110/EC (OJ L 267, 10.10. 2009, p. 7).
Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC (OJ L 267, 10.10.2009, p. 7).

令 2013/36/EU[15]の第 2 条第 5 項第 3 号に示す郵便振替取扱機関は，この規則の適用範囲から除外される。指令(EU) 2015/2366 により適用除外された決済機関，指令 2009/110/EC により適用除外された電子マネー機関及び指令(EU) 2015/2366 の第 33 条第 1 項に示す口座情報サービスプロバイダの職務権限のある当局は，指令(EU) 2015/2366 の第 22 条に従って指定された職務権限のある当局であるべきである。

Account information service providers, referred to in Article 33(1) of Directive (EU) 2015/2366, are explicitly included in the scope of this Regulation, taking into account the specific nature of their activities and the risks arising therefrom. In addition, electronic money institutions and payment institutions exempted pursuant to Article 9(1) of Directive 2009/110/EC of the European Parliament and of the Council (14) and Article 32(1) of Directive (EU) 2015/2366 are included in the scope of this Regulation even if they have not been granted authorisation in accordance Directive 2009/110/EC to issue electronic money, or if they have not been granted authorisation in accordance with Directive (EU) 2015/2366 to provide and execute payment services. However, post office giro institutions, referred to in Article 2(5), point (3), of Directive 2013/36/EU of the European Parliament and of the Council (15), are excluded from the scope of this Regulation. The competent authority for payment institutions exempted pursuant to Directive (EU) 2015/2366, electronic money institutions exempted pursuant to Directive 2009/110/EC and account information service providers as referred to in Article 33(1) of Directive (EU) 2015/2366, should be the competent authority designated in accordance with Article 22 of Directive (EU) 2015/2366.

(38) より大きな金融機関は，より広範な資源を利用できるかもしれず，また，統治構造を開発するための資金を迅速に分配でき，かつ，様々な運営管理戦略を定めることができるので，この規則の意味におけるマイクロ企業ではない金融機関のみが，より複雑な統治の手立てを設けることを要求されるべきである。そのような金融機関は，とりわけ，ICT サードパーティサービスプロバイダとの間の監督の手立てに関するもしくは危機管理の取扱いに関する専用のマネジメント機能を設けるため，3 つの防御線モデルに従って当該金融機関の ICT リスクマネジメントを組織化するため，または，内部リスクマネジメント管理モデルを設けるため，並びに，内部監査に対してその金融機関の ICT リスクマネジメント枠組みに服するための能力をより良く具備している。

As larger financial entities might enjoy wider resources and can swiftly deploy funds to develop governance structures and set up various corporate strategies, only financial entities that are not microenterprises in the sense of this Regulation should be required to establish more complex governance arrangements. Such entities are better equipped in particular to set up dedicated management functions for supervising arrangements with ICT third-party service providers or for dealing with crisis management, to organise their ICT risk management according to the three lines of defence model,

---

15 与信機関の活動へのアクセス及び与信機関の健全性監督に関する，指令 2002/87/EC を改正する並びに指令 2006/48/EC 及び指令 2006/49/EC を廃止する欧州議会及び理事会の 2013 年 6 月 26 日の指令 2013/36/EU (OJ L 176, 27.6.2013, p. 338).

Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (OJ L 176, 27.6.2013, p. 338).

or to set up an internal risk management and control model, and to submit their ICT risk management framework to internal audits.

(39) 幾つかの金融機関は，適用除外から受益しており，または，適格な部門別の欧州連合法の下にある非常に軽い法制枠組みに服している。そのような金融機関は，欧州議会及び理事会の指令 2011/61/EU[16]の第 3 条第 2 項に示すオルタナティブ投資ファンド運用者，欧州議会及び理事会の指令 2009/138/EC[17]の第 4 条に示す保険事業者及び再保険事業者，合計で 15 名を超えない加入者を集めた年金制度を運用している職域退職給付機関を含む。それらの適用除外に照らし，そのような金融機関をこの規則の適用範囲内に含めることは，比例的ではないだろう。加えて，この規則は，マイクロ企業または小企業もしくは中規模企業として分類される保険仲介事業者，再保険仲介事業者及び補助的な保険仲介事業者がこの規則に服してはならないということを帰結する保険仲介市場の構造の特性を認めている。

Some financial entities benefit from exemptions or are subject to a very light regulatory framework under the relevant sector-specific Union law. Such financial entities include managers of alternative investment funds referred to in Article 3(2) of Directive 2011/61/EU of the European Parliament and of the Council (16), insurance and reinsurance undertakings referred to in Article 4 of Directive 2009/138/EC of the European Parliament and of the Council (17), and institutions for occupational retirement provision which operate pension schemes which together do not have more than 15 members in total. In light of those exemptions it would not be proportionate to include such financial entities in the scope of this Regulation. In addition, this Regulation acknowledges the specificities of the insurance intermediation market structure, with the result that insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries qualifying as microenterprises or as small or medium-sized enterprises should not be subject to this Regulation.

(40) 指令 2013/36/EU の第 2 条第 5 項第 4 号ないし第 23 号に示す法主体は同指令の適用範囲から除外されるので，その結果として，構成国は，それらの構成国それぞれの領土内に所在しているそのような法主体をこの規則の適用から除外することを選択できるべきである。

Since the entities referred to in Article 2(5), points (4) to (23), of Directive 2013/36/EU are excluded from the scope of that Directive, Member States should consequently be able to choose to exempt from the application of this Regulation

---

16 オルタナティブ投資ファンド管理者に関する並びに指令 2003/41/EC 及び指令 2009/65/EC 並びに規則(EC) No 1060/ 2009 及び規則(EU) No 1095/2010 を改正する欧州議会及び理事会の 2011 年 6 月 8 日の指令 2011/61/EU (OJ L 174, 1.7.2011, p. 1).

Directive 2011/61/EU of the European Parliament and of the Council of 8 June 2011 on Alternative Investment Fund Managers and amending Directives 2003/41/EC and 2009/65/EC and Regulations (EC) No 1060/2009 and (EU) No 1095/2010 (OJ L 174, 1.7.2011, p. 1).

17 保険及び再保険の事業の開始及び遂行に関する欧州議会及び理事会の 2009 年 11 月 25 日の指令 2009/138/EC（Solvency II） (OJ L 335, 17.12.2009, p. 1).

Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II) (OJ L 335, 17.12.2009, p. 1).

such entities located within their respective territories.

(41) 同様に，欧州議会及び理事会の指令 2014/65/EU[18]の適用範囲にこの規則を揃えるため，指令 2014/65/EU の下における認可を受けることを要せずして投資サービスを提供することが認められている同指令の第 2 条及び第 3 条に示す自然人及び法人をこの規則の適用範囲から除外することも適切である。ただし，指令 2014/65/EU の第 2 条もまた，証券集中保管機関，投資信託事業者または保険事業者及び再保険事業者のような，この規則の目的のために金融機関として分類される法主体を同指令の適用範囲から除外している。同指令の第 2 条及び第 3 条に示す個人及び法主体のこの規則の適用範囲からの適用除外は，それらの証券集中保管機関，投資信託事業者または保険事業者及び再保険事業者を包含してはならない。

Similarly, in order to align this Regulation to the scope of Directive 2014/65/EU of the European Parliament and of the Council [(18)], it is also appropriate to exclude from the scope of this Regulation natural and legal persons referred in Articles 2 and 3 of that Directive which are allowed to provide investment services without having to obtain an authorisation under Directive 2014/65/EU. However, Article 2 of Directive 2014/65/EU also excludes from the scope of that Directive entities which qualify as financial entities for the purposes of this Regulation such as, central securities depositories, collective investment undertakings or insurance and reinsurance undertakings. The exclusion from the scope of this Regulation of the persons and entities referred to in Articles 2 and 3 of that Directive should not encompass those central securities depositories, collective investment undertakings or insurance and reinsurance undertakings.

(42) 部門別の欧州連合法の下において，幾つかの金融機関は，その金融機関の規模またはその金融機関が提供するサービスと関係する理由により，より軽い要件または適用除外に服している。その類型の金融機関は，小規模で相互結合のない投資企業，関係する構成国によって指令(EU) 2016/2341 の第 5 条の中で定められた条件の下で同指令の適用範囲から適用除外されることができ，かつ，合計で 100 名を超えない加入者を集めた年金制度を運用している小規模な職域退職給付機関，並びに，指令 2013/36/EU によって適用除外された機関を含む。それゆえ，比例性の原則に従い，かつ，部門別の欧州連合法の精神を保持するため，それらの金融機関をこの規則の下にある簡素化された ICT リスクマネジメント枠組みに服させることも適切である。それらの金融機関に適用される ICT リスクマネジメント枠組みの比例的な性格は，ESAs によって策定される法制上の技術標準によって変えられてはならない。更に，比例性の原則に従い，欧州連合の当該法行為を国内法化する国内法に従って適用除外された指令(EU) 2015/2366 の第 32 条第 1 項に示す決済機関及び指令 2009/110/EC の第 9 条に示す電子マネー機関をこの規則の下にある簡素化された ICT リスクマネジメント枠組みに服させることも適切であるものの，部門別の欧州連合法を国内法化するそれぞれの国内法に従って適用除外されなかった決済機関及び電子マネー機関は，この規則によって定められた一般的な枠組みを遵守すべきである。

---

[18] 金融商品市場に関する並びに指令 2002/92/EC 及び指令 2011/61/EU を改正する欧州議会及び理事会の 2014 年 5 月 15 日の指令 2014/65/EU (OJ L 173, 12.6.2014, p. 349).

Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (OJ L 173, 12.6.2014, p. 349).

Under sector-specific Union law, some financial entities are subject to lighter requirements or exemptions for reasons associated with their size or the services they provide. That category of financial entities includes small and non-interconnected investment firms, small institutions for occupational retirement provision which may be excluded from the scope of Directive (EU) 2016/2341 under the conditions laid down in Article 5 of that Directive by the Member State concerned and operate pension schemes which together do not have more than 100 members in total, as well as institutions exempted pursuant to Directive 2013/36/EU. Therefore, in accordance with the principle of proportionality and to preserve the spirit of sector-specific Union law, it is also appropriate to subject those financial entities to a simplified ICT risk management framework under this Regulation. The proportionate character of the ICT risk management framework covering those financial entities should not be altered by the regulatory technical standards that are to be developed by the ESAs. Moreover, in accordance with the principle of proportionality, it is appropriate to also subject payment institutions referred to in Article 32(1) of Directive (EU) 2015/2366 and electronic money institutions referred to in Article 9 of Directive 2009/110/EC exempted in accordance with national law transposing those Union legal acts to a simplified ICT risk management framework under this Regulation, while payment institutions and electronic money institutions which have not been exempted in accordance with their respective national law transposing sectoral Union law should comply with the general framework laid down by this Regulation.

(43) 同様に，マイクロ企業として分類される金融機関またはこの規則の下における簡素化された ICT リスクマネジメント枠組みに服している金融機関は，ICT サービスの利用に関して ICT サードパーティサービスプロバイダとの間で締結したその金融機関の約定を監督するための担当部署を設けること，または，関連するリスクエクスポージャー及び適格な文書化を監視する職責を負う上級管理職の者を指名すること;利益相反を防止するため，管理機能に対する ICT リスクを取扱うこと及び監督することに職責を負う者を任命すること及びそのような管理機能の適切なレベルの独立性を確保すること;ICT リスクマネジメント枠組みを文書化しかつ少なくとも年 1 度見直すこと;ICT リスクマネジメント枠組みを定期的に内部監査に服させること;その金融機関のネットワーク及び情報システムのインフラ及びプロセスの大きな変更の後に詳細な評価を遂行すること;旧式の ICT システムに対して定期的なリスク分析を実施すること;ICT 対応計画及び ICT 復旧計画の実装を独立の内部監査による見直しに服させること;危機管理機能をもつこと;主たる ICT インフラと冗長施設間の切替えのシナリオを把握することに，事業継続並びに対応及び復旧計画の試験を拡大すること;職務権限のある当局の要請に応じて，ICT と関連する大きなインシデントによって生じた年費用及び損失の合計推計額を職務権限のある当局に対して報告すること;冗長な ICT 能力を維持管理すること;職務権限のある国内当局に対し，ICT と関連するインシデントの事後評価に従って実装された変更を伝達すること;適格な技術上の発展を継続して監視すること;この規則の中で定められている ICT リスクマネジメント枠組みと一体となるものとして，包括的なデジタル運営管理上の回復力の試験計画を定めること;または，ICT サードパーティリスクに関する戦略を採択しかつ定期的に見直すことを要求されてはならない。加えて，マイクロ企業は，そのような当該マイクロ企業の全体的なリスクプロファイルを基礎とする冗長な ICT 能力を維持することの要否を評価することのみを要求されるべきである。マイクロ企業は，デジタル運営管理上の回復力の試験計画に関し，より柔軟な制度から受益すべきである。遂行されるべき試験のタイプ及び頻度を検討する際，マイクロ企業は，高度のデジタル運営管理上の回復力を維持するという目的，利用可能な資源及び当該マイクロ企業のリスクプロファイルを適正にバランスさせるべきである。この規則の下における簡素化された ICT リスクマネジメント枠組みに服するマイクロ企

業及び金融機関は，この規則の中で定められた基準に適合している金融機関のみがそのような試験を実施することを要求されるべきであるので，脅威ベースのペネトレーション試験（TLPT）を基礎とする ICT ツール，システム及びプロセスの高度な試験を実行する要件から適用除外されるべきである。マイクロ企業の限定的な実現能力に照らし，当該金融機関が，当該 ICT サードパーティサービスプロバイダの遂行能力に関する全ての適格な情報及び保証をいつでもそれぞれの独立のサードパーティに対して要求できることを条件として，マイクロ企業は，当該 ICT サードパーティサービスプロバイダから指定された独立のサードパーティへの，金融機関のアクセスの権利，検査の権利及び監査の権利を委任することを ICT サードパーティサービスプロバイダとの間で合意できるべきである。

Similarly, financial entities which qualify as microenterprises or are subject to the simplified ICT risk management framework under this Regulation should not be required to establish a role to monitor their arrangements concluded with ICT third-party service providers on the use of ICT services; or to designate a member of senior management to be responsible for overseeing the related risk exposure and relevant documentation; to assign the responsibility for managing and overseeing ICT risk to a control function and ensure an appropriate level of independence of such control function in order to avoid conflicts of interest; to document and review at least once a year the ICT risk management framework; to subject to internal audit on a regular basis the ICT risk management framework; to perform in-depth assessments after major changes in their network and information system infrastructures and processes; to regularly conduct risk analyses on legacy ICT systems; to subject the implementation of the ICT Response and Recovery plans to independent internal audit reviews; to have a crisis management function, to expand the testing of business continuity and response and recovery plans to capture switchover scenarios between primary ICT infrastructure and redundant facilities; to report to competent authorities, upon their request, an estimation of aggregated annual costs and losses caused by major ICT-related incidents, to maintain redundant ICT capacities; to communicate to national competent authorities implemented changes following post ICT-related incident reviews; to monitor on a continuous basis relevant technological developments, to establish a comprehensive digital operational resilience testing programme as an integral part of the ICT risk management framework provided for in this Regulation, or to adopt and regularly review a strategy on ICT third-party risk. In addition, microenterprises should only be required to assess the need to maintain such redundant ICT capacities based on their risk profile. Microenterprises should benefit from a more flexible regime as regards digital operational resilience testing programmes. When considering the type and frequency of testing to be performed, they should properly balance the objective of maintaining a high digital operational resilience, the available resources and their overall risk profile. Microenterprises and financial entities subject to the simplified ICT risk management framework under this Regulation should be exempted from the requirement to perform advanced testing of ICT tools, systems and processes based on threat-led penetration testing (TLPT), as only financial entities meeting the criteria set out in this Regulation should be required to carry out such testing. In light of their limited capabilities, microenterprises should be able to agree with the ICT third-party service provider to delegate the financial entity's rights of access, inspection and audit to an independent third-party, to be appointed by the ICT third-party service provider, provided that the financial entity is able to request, at any time, all relevant information and assurance on the ICT third-party service provider's performance from the respective independent third-party.

(44) 高度なデジタル回復力試験の目的のために識別された金融機関のみが脅威ベースのペネトレーション試験を実施することを要求されるべきであるので，そのような試験の遂行に伴う運営プロセス及び

資金上の費用は，小さな割合の金融機関によって負わされるべきである。

As only those financial entities identified for the purposes of the advanced digital resilience testing should be required to conduct threat-led penetration tests, the administrative processes and financial costs entailed in the performance of such tests should be borne by a small percentage of financial entities.

(45) 一方における金融機関の事業上の戦略と他方における ICT リスクマネジメントの実行との間の全面的な均一性及び全体的な一貫性を確保するため，金融機関の経営陣は，ICT リスクマネジメント枠組み及びデジタル運営管理上の回復力の全体的な戦略の舵取り及び適応において，重要かつ能動的な役割を維持することを要求されるべきである。経営陣によって採られるアプローチは，ICT システムの回復力を確保する手段に焦点を当てるべきであるだけではなく，企業の個々のレイヤにおいて，全ての担当従業者に対し，サイバーリスクに関して強い認識の感覚を涵養し，かつ，全てのレベルにおいて厳格なサイバー衛生を遵守することに寄与する基本方針のセットにより，人々及びプロセスを包摂するものでもあるべきである。金融機関の ICT リスクを取扱うことにおいて経営陣が最終的な責任を負うことは，ICT リスクマネジメントの監視の管理における経営陣の継続的な関与の中へと更に翻訳された当該包括的なアプローチの包摂的な基本原則の一つであるべきである。

To ensure full alignment and overall consistency between financial entities' business strategies, on the one hand, and the conduct of ICT risk management, on the other hand, the financial entities' management bodies should be required to maintain a pivotal and active role in steering and adapting the ICT risk management framework and the overall digital operational resilience strategy. The approach to be taken by management bodies should not only focus on the means of ensuring the resilience of the ICT systems, but should also cover people and processes through a set of policies which cultivate, at each corporate layer, and for all staff, a strong sense of awareness about cyber risks and a commitment to observe a strict cyber hygiene at all levels. The ultimate responsibility of the management body in managing a financial entity's ICT risk should be an overarching principle of that comprehensive approach, further translated into the continuous engagement of the management body in the control of the monitoring of the ICT risk management.

(46) 更に，金融機関の ICT リスクのマネジメントに関して経営陣が全面的かつ最終的な責任を負うという基本原則は，その金融機関が高度のデジタル運営管理上の回復力を達成することを実現可能にするような，その金融機関のための平等な ICT 関連投資及び全体的な予算を守る必要性と連携して進められる。

Moreover, the principle of the management body's full and ultimate responsibility for the management of the ICT risk of the financial entity goes hand in hand with the need to secure a level of ICT-related investments and an overall budget for the financial entity that would enable the financial entity to achieve a high level of digital operational resilience.

(47) サイバーリスクの運営管理のための国際的な，国内の及び産業界の適格なベストプラクティス，運用指針，推奨事項及びアプローチから触発され，この規則は，ICT リスクマネジメントの全体構造を構成する基本原則のセットを促進する。その結果，この規則の中で定められている ICT リスクマネジメントの様々な機能（識別，防護及び防止，検出，対応及び復旧，学習及び進化並びに伝達）に対応す

るために金融機関が設けた主たる実現能力に沿って，金融機関は，異なって枠組み構成されまたは分類されている ICT リスクマネジメントモデルを用いることが自由なままであるべきである。

Inspired by relevant international, national and industry best practices, guidelines, recommendations and approaches to the management of cyber risk, this Regulation promotes a set of principles that facilitate the overall structure of ICT risk management. Consequently, as long as the main capabilities which financial entities put in place address the various functions in the ICT risk management (identification, protection and prevention, detection, response and recovery, learning and evolving and communication) set out in this Regulation, financial entities should remain free to use ICT risk management models that are differently framed or categorised.

(48) サイバー脅威の全体像の進化と速度を合わせるため，金融機関は，その金融機関のサービスに対して要求されるデータの処理を保証するためだけではなく，ストレスのかかった市場条件またはそれ以外の負の状況のゆえの付加的な処理の需要をその金融機関が適切に取扱うことができるようにするための十分な技術上の回復力を確保するためにも，信頼性がありかつ利用可能な最新の ICT システムを維持管理すべきである。

To keep pace with an evolving cyber threat landscape, financial entities should maintain updated ICT systems that are reliable and capable, not only for guaranteeing the processing of data required for their services, but also for ensuring sufficient technological resilience to allow them to deal adequately with additional processing needs due to stressed market conditions or other adverse situations.

(49) 損害を抑制することにより，及び，当該金融機関のバックアップ基本方針に従って活動再開及び復旧活動に対する優先権を与えることにより，金融機関が，ICT と関連するインシデント，とりわけサイバー攻撃を率先してかつ迅速に解決できるようにするため，実効性のある事業継続性及び復旧計画が必要である。ただし，そのような再開は，いかなる方法においても，ネットワーク及び情報システムの完全性と安全性またはデータの可用性，真正性，完全性もしくは機密性を危険に晒してはならない。

Efficient business continuity and recovery plans are necessary to allow financial entities to promptly and quickly resolve ICT-related incidents, in particular cyber-attacks, by limiting damage and giving priority to the resumption of activities and recovery actions in accordance with their back-up policies. However, such resumption should in no way jeopardise the integrity and security of the network and information systems or the availability, authenticity, integrity or confidentiality of data.

(50) この規則は，当該金融機関の復旧時間目標及び復旧時点目標を金融機関が柔軟な態様で決定することを認めており，また，それゆえ，適格な機能の性質及び不可欠性並びに個別の事業上の必要性を全面的に考慮に入れることによって，そのような目標を定めることを認めているが，それでもなお，この規則は，当該金融機関に対し，そのような目標を決定する際，市場の効率性に対する潜在的な全体的影響の評価を実行することを要求すべきである。

While this Regulation allows financial entities to determine their recovery time and recovery point objectives in a flexible manner and hence to set such objectives by fully taking into account the nature and the criticality of the relevant functions and any specific business needs, it should nevertheless require them to carry out an assessment of the potential overall impact on market efficiency when determining such objectives.

(51) サイバー攻撃を広める者は，その発生源において金銭的利益を追求しようとする傾向があり，それは，金融機関を重大な結果に晒している。ICT システムが完全性を喪失することまたは利用不可能になることを阻止するため，また，それゆえ，データ侵害及び物理的な ICT インフラの毀損を避けるため，金融機関からの ICT と関連する大きなインシデントの報告は，大きく改善され，かつ，揃えられるべきである。ICT と関連するインシデントの報告は，全ての金融機関に関し，その金融機関の適格な職務権限のある当局に対して直接に報告する要件の導入を介して，整合化されるべきである。金融機関が複数の職務権限のある国内当局の監督に服するときは，構成国は，そのような報告の名宛人として，単一の職務権限のある当局を指定すべきである。理事会規則(EU) No 1024/2013[19]の第 6 条第 4 項に従って大きいと分類された与信機関は，職務権限のある国内当局に対してそのような報告を提出すべきであり，それを受けた後，当該当局は，欧州中央銀行（ECB）に対してその報告を送信すべきである。

The propagators of cyber-attacks tend to pursue financial gains directly at the source, thus exposing financial entities to significant consequences. To prevent ICT systems from losing integrity or becoming unavailable, and hence to avoid data breaches and damage to physical ICT infrastructure, the reporting of major ICT-related incidents by financial entities should be significantly improved and streamlined. ICT-related incident reporting should be harmonised through the introduction of a requirement for all financial entities to report directly to their relevant competent authorities. Where a financial entity is subject to supervision by more than one national competent authority, Member States should designate a single competent authority as the addressee of such reporting. Credit institutions classified as significant in accordance with Article 6(4) of Council Regulation (EU) No 1024/2013 (19) should submit such reporting to the national competent authorities, which should subsequently transmit the report to the European Central Bank (ECB).

(52) 直接の報告は，金融監督当局が，ICT と関連する大きなインシデントに関する情報への迅速なアクセスをもつことができるようにすべきである。次いで，金融監督当局は，金融監督当局ではない行政機関に対してそのようなインシデントの認識を拡大するため，また，CSIRTs の場合には，金融機関に対して与えられ得る迅速な補助をしかるべく促進するため，（指令(EU) 2022/2555 の下にある職務権限のある当局及び単一連絡部局，国内データ保護当局のような）金融監督当局ではない行政機関及び刑事上の性質をもつ ICT と関連する大きなインシデントに関する法執行機関に対し，適切に，ICT と関連する大きなインシデントの詳細情報を渡すべきである。加えて，構成国は，金融機関が，自ら，金融サービスの分野外の行政機関に対してそのような情報を提供すべきことを決定できるべき

[19] 与信機関の健全性監督と関連する政策と関係する特別の仕事を欧州中央銀行に対して与える 2013 年 10 月 15 日の理事会規則(EU) No 1024/2013 (OJ L 287, 29.10.2013, p. 63).
Council Regulation (EU) No 1024/2013 of 15 October 2013 conferring specific tasks on the European Central Bank concerning policies relating to the prudential supervision of credit institutions (OJ L 287, 29.10.2013, p. 63).

である。それらの情報の流れは，金融機関が，そのような行政機関による適格な技術上の入力，解消に関する助言及びその後の事後対応から速やかに受益できるようにすべきである。ICT と関連する大きなインシデントに関する情報伝達は，相互に経路が設けられるべきである：ESAs は，より広い集団的な防衛を支援するため，インシデントと関係するサイバー脅威及び脆弱性に関する匿名化されたデータを共有すべきであるが，金融監督当局は，金融機関に対し，必要な全てのフィードバックまたは運用指針を提供すべきである。

The direct reporting should enable financial supervisors to have immediate access to information about major ICT-related incidents. Financial supervisors should in turn pass on details of major ICT-related incidents to public non-financial authorities (such as competent authorities and single points of contact under Directive (EU) 2022/2555, national data protection authorities, and to law enforcement authorities for major ICT-related incidents of a criminal nature) in order to enhance such authorities awareness of such incidents and, in the case of CSIRTs, to facilitate prompt assistance that may be given to financial entities, as appropriate. Member States should, in addition, be able to determine that financial entities themselves should provide such information to public authorities outside the financial services area. Those information flows should allow financial entities to swiftly benefit from any relevant technical input, advice about remedies, and subsequent follow-up from such authorities. The information on major ICT-related incidents should be mutually channelled: financial supervisors should provide all necessary feedback or guidance to the financial entity, while the ESAs should share anonymised data on cyber threats and vulnerabilities relating to an incident, to aid wider collective defence.

(53) 全ての金融機関がインシデント報告を実行することを要求されるべきであるが，同要件は，全ての金融機関に対して同じ態様で影響を及ぼすとは想定されていない。無論，適格な具現性の閾値及び報告の行程は，ICT と関連する大きなインシデントのみを包摂するという観点から，ESAs によって策定される法制上の技術標準を基礎とする委任される行為の過程において，適正に補正されるべきである。加えて，報告義務の行程を設定する際には，金融機関の特性が考慮に入れられるべきである。

While all financial entities should be required to carry out incident reporting, that requirement is not expected to affect all of them in the same manner. Indeed, relevant materiality thresholds, as well as reporting timelines, should be duly adjusted, in the context of delegated acts based on the regulatory technical standards to be developed by the ESAs, with a view to covering only major ICT-related incidents. In addition, the specificities of financial entities should be taken into account when setting timelines for reporting obligations.

(54) この規則は，与信機関，決済機関，口座情報サービスプロバイダ及び電子マネー機関に対し，そのインシデントが ICT と関連するインシデントという性質をもつか否かとは無関係に（従来は指令(EU) 2015/2366 の下において報告されていた）運営管理または決済の安全性と関連する全てのインシデントを報告することを要求すべきである。

This Regulation should require credit institutions, payment institutions, account information service providers and electronic money institutions to report all operational or security payment-related incidents – previously reported under Directive (EU) 2015/2366 – irrespective of the ICT nature of the incident.

(55) ESAs は，欧州連合レベルにおける ICT と関連するインシデントの報告の集中化の実現可能性と条件を評価する職務を与えられるべきである。そのような集中化は，適格な報告を直接に受領しかつ職務権限のある国内当局に対して自動的に通知し，または，職務権限のある国内当局から転送された適格な報告を集中化して調整の役割を満たすだけの，ICT と関連する大きなインシデントの報告のための単一の EU ハブによって組成され得る。ESAs は，ECB 及び ENISA からの意見聴取を経た上で，単一 EU ハブを設置することの実現可能性を検討する共同報告書を準備する職務を与えられるべきである。

The ESAs should be tasked with assessing the feasibility and conditions for a possible centralisation of ICT-related incident reports at Union level. Such centralisation could consist of a single EU Hub for major ICT-related incident reporting either directly receiving relevant reports and automatically notifying national competent authorities, or merely centralising relevant reports forwarded by the national competent authorities and thus fulfilling a coordination role. The ESAs should be tasked with preparing, in consultation with the ECB and ENISA, a joint report exploring the feasibility of setting up a single EU Hub.

(56) 高度のデジタル運営管理上の回復力を達成するため，かつ，適格な国際的な技術標準（例：G7 の脅威ベースのペネトレーション試験の基本要素）及び TIBER-EU のような欧州連合内において適用される枠組みに沿って，金融機関は，潜在的な ICT の脆弱性を明らかにし及びそれに対処するためのその金融機関の ICT システム及び ICT と関連する職責をもつ担当従業者の防止能力，検出能力，対応能力及び復旧能力の実効性に関し，それらの ICT システム及び担当従業者を定期的に試験すべきである。金融機関のサイバーセキュリティ上の準備態勢のレベルに関する様々な金融副部門全体にわたって存在する相違及びその副部門の中に存在する相違を反映するため，試験は，基本的な要件の評価（例：脆弱性評価及び脆弱性スキャン，オープンソース分析，ネットワークセキュリティ評価，ギャップ分析，物理的なセキュリティの見直し，アンケート及びスキャニングのソフトウェアソリューション，それが実施可能なときはソースコードの見直し，シナリオベースの試験，互換性の試験，遂行能力の試験またはエンドツーエンドの試験）から TLPT によるより高度な試験に至るまでの多種多様なツール及び行為を含むべきである。そのような高度な試験は，合理的にそれを実行するために ICT の観点から十分に熟達している金融機関のみに要求されるべきである。そして，この規則によって要求されるデジタル運営管理上の回復力の試験は，この規則の中で定められた基準に適合する金融機関（例えば，大規模であり，システミックでありかつ ICT に熟達した与信機関，株式交換所，証券集中保管機関及び中央清算機関）に関しては，それ以外の金融機関よりも多く求められるべきである。それと同時に，TLPT によるデジタル運営管理上の回復力の試験は，コアとなる金融サービス副部門（例えば，支払，銀行及び清算と決済）において運営管理している金融機関及びシステミックな役割を演じている金融機関に関してはより多く適格であり，かつ，それ以外の副部門（例えば，資産管理及び与信格付機関）に関してはより少なく適格であるべきである。

In order to achieve a high level of digital operational resilience, and in line with both the relevant international standards (e.g. the G7 Fundamental Elements for Threat-Led Penetration Testing) and with the frameworks applied in the Union, such as the TIBER-EU, financial entities should regularly test their ICT systems and staff having ICT-related responsibilities with regard to the effectiveness of their preventive, detection, response and recovery capabilities, to

uncover and address potential ICT vulnerabilities. To reflect differences that exist across, and within, the various financial subsectors as regards financial entities' level of cybersecurity preparedness, testing should include a wide variety of tools and actions, ranging from the assessment of basic requirements (e.g. vulnerability assessments and scans, open source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews where feasible, scenario-based tests, compatibility testing, performance testing or end-to-end testing) to more advanced testing by means of TLPT. Such advanced testing should be required only of financial entities that are mature enough from an ICT perspective to reasonably carry it out. The digital operational resilience testing required by this Regulation should thus be more demanding for those financial entities meeting the criteria set out in this Regulation (for example, large, systemic and ICT-mature credit institutions, stock exchanges, central securities depositories and central counterparties) than for other financial entities. At the same time, the digital operational resilience testing by means of TLPT should be more relevant for financial entities operating in core financial services subsectors and playing a systemic role (for example, payments, banking, and clearing and settlement), and less relevant for other subsectors (for example, asset managers and credit rating agencies).

(57) 国境を越える活動に関与しており，かつ，設立の自由を行使しまたは欧州連合内におけるサービス提供の自由を行使している金融機関は，その金融機関の本国である構成国における単一のセットの高度な試験の要件（すなわち，TLPT）を遵守すべきである。その単一のセットの要件は，国境を越える金融グループが欧州連合内において業務遂行している全ての主権国家内の ICT インフラを含むべきであり，そして，そのような国境を越える金融グループが，1 つの主権国家のみにおいて，関連する ICT 試験の費用を負担することができるようにすべきである。

Financial entities involved in cross-border activities and exercising the freedoms of establishment, or of provision of services within the Union, should comply with a single set of advanced testing requirements (i.e. TLPT) in their home Member State, which should include the ICT infrastructures in all jurisdictions where the cross-border financial group operates within the Union, thus allowing such cross-border financial groups to incur related ICT testing costs in one jurisdiction only.

(58) とりわけ，TIBER-EU の枠組みの実装と関連して，一定の職務権限のある当局によって既に獲得された専門知識を活かすため，この規則は，構成国が，TLPT の全ての事項に関して国内レベルで金融部門に職責を負う単一の行政機関を指定することを認め，または，そのような指定がないときは，職務権限のある当局が，他の金融上の職務権限のある国内機関に対して TLPT と関連する職務の実施を委任することを認めるべきである。

To draw on the expertise already acquired by certain competent authorities, in particular with regard to implementing the TIBER-EU framework, this Regulation should allow Member States to designate a single public authority as responsible in the financial sector, at national level, for all TLPT matters, or competent authorities, to delegate, in the absence of such designation, the exercise of TLPT related tasks to another national financial competent authority.

(59) この規則は，金融機関に対し，単一の脅威ベースのペネトレーション試験の中に全ての不可欠な機能または重要な機能を包摂することを要求していないので，金融機関は，どの不可欠な機能または

重要な機能が及びいかなる回数でそのような試験の適用範囲内に含められるべきかを判断することが自由であるべきである。
Since this Regulation does not require financial entities to cover all critical or important functions in one single threat-led penetration test, financial entities should be free to determine which and how many critical or important functions should be included in the scope of such a test.

(60) （1 つの TLPT に複数の金融機関が参加し，かつ，その TLPT に関して ICT サードパーティサービスプロバイダが外部の試験担当者との間で直接に契約上の取決めを締結できるものを含め）この規則の意味におけるプールされた試験は，この規則の適用範囲外にある顧客に対して当該 ICT サードパーティサービスプロバイダから供給されるサービスの品質もしくは安全性またはそのようなサービスと関連するデータの機密性が悪影響を受けることが合理的に予測される場合に限り，認められるべきである。プールされた試験は，包摂される金融機関に対するこの規則による TLPT の目的に適合する堅牢な試験の実施を確保するため，安全確保（指定された 1 つの金融機関による指示，参加する金融機関の数の調整）に服するべきである。

Pooled testing within the meaning of this Regulation – involving the participation of several financial entities in a TLPT and for which an ICT third-party service provider can directly enter into contractual arrangements with an external tester – should be allowed only where the quality or security of services delivered by the ICT third-party service provider to customers that are entities falling outside the scope of this Regulation, or the confidentiality of the data related to such services, are reasonably expected to be adversely impacted. Pooled testing should also be subject to safeguards (direction by one designated financial entity, calibration of the number of participating financial entities) to ensure a rigorous testing exercise for the financial entities involved which meet the objectives of the TLPT pursuant to this Regulation.

(61) 金融機関レベルで利用可能な内部資源を活用するため，監督機関の承認が存在すること，利益相反がないこと及び定期的に（3 回毎に）内部の試験担当者の利用と外部の試験担当者の利用とが切り替わることを条件として，また，当該 TLPT 内の脅威情報提供者が当該金融機関に対して常に外部者であることも要求されつつ，この規則は，TLPT を実行する目的のための内部の試験担当者の利用を認めるべきである。TLPT を実施することの責任は，全面的に，金融機関にあるままであるべきである。当局から提供される証明書は，相互承認の目的のためのみとすべきであり，また，その金融機関が晒されている ICT リスクに対処するために必要となる事後的な活動を排除してはならず，かつ，その証明書は，金融機関の ICT リスクのマネジメント能力及び緩和能力の監督機関の承認とみなされてはならない。

In order to take advantage of internal resources available at corporate level, this Regulation should allow the use of internal testers for the purposes of carrying out TLPT, provided there is supervisory approval, no conflicts of interest, and periodical alternation of the use of internal and external testers (every three tests), while also requiring the provider of the threat intelligence in the TLPT to always be external to the financial entity. The responsibility for conducting TLPT should remain fully with the financial entity. Attestations provided by authorities should be solely for the purpose of mutual recognition and should not preclude any follow-up action needed to address the ICT risk to which the financial

entity is exposed, nor should they be seen as a supervisory endorsement of a financial entity's ICT risk management and mitigation capabilities.

(62) 金融部門における ICT サードパーティリスクの良好な監視を確保するため，とりわけ，不可欠な機能または重要な機能を支える ICT サービスに関し，ICT サードパーティサービスプロバイダに対してアウトソースされる機能という文脈において，また，より一般的には，全ての ICT サードパーティ依存性という文脈において監視のリスクが生じているときは，金融機関をガイドするための基本原則ベースの規定のセットを定めることが必要である。

To ensure a sound monitoring of ICT third-party risk in the financial sector, it is necessary to lay down a set of principle-based rules to guide financial entities' when monitoring risk arising in the context of functions outsourced to ICT third-party service providers, particularly for ICT services supporting critical or important functions, as well as more generally in the context of all ICT third-party dependencies.

(63) 金融サービスの円滑な提供を実現可能にする技術ソリューションのプロバイダの趨勢及び多様性を考慮に入れつつ，ICTリスクの様々な発生源の複雑性に対処するため，この規則は，クラウドコンピューティングサービス，ソフトウェア，データ分析サービスのプロバイダ及びデータセンターサービスのプロバイダを含め，幅広い ICT サードパーティサービスプロバイダを包摂すべきである。同様に，金融機関は，金融グループ内において調達される ICT サービスの過程における場合を含め，全てのタイプのリスクを，実効的かつ一貫性をもって特定し及び取扱うべきであるので，1 つの金融グループの一部となっており，かつ，主として当該事業者の親事業者に対してまたは当該事業者の親事業者の子事業者もしくは支店に対して ICT サービスを提供する事業者並びに他の金融機関に対してICTサービスを提供する金融機関もまた，この規則の下においてはICTサードパーティサービスプロバイダとして判断されるべきであるということが明確にされるべきである。最後に，進化しつつある決済サービス市場が複雑な技術ソリューションに次第に依存するようになっていることに照らし，かつ，新たなタイプの決済サービスと決済関連ソリューションが登場していることを考慮し，決済システムまたは証券清算システムを運用管理している際の中央銀行及び国家の権能を満たす過程において ICT 関連サービスを提供している際の行政機関を除き，決済処理活動を提供しておりまたは決済インフラを運用管理している，決済サービスのエコシステムの参加者もまた，この規則の下においてはICTサードパーティサービスプロバイダとして判断されるべきである。

To address the complexity of the various sources of ICT risk, while taking into account the multitude and diversity of providers of technological solutions which enable a smooth provision of financial services, this Regulation should cover a wide range of ICT third-party service providers, including providers of cloud computing services, software, data analytics services and providers of data centre services. Similarly, since financial entities should effectively and coherently identify and manage all types of risk, including in the context of ICT services procured within a financial group, it should be clarified that undertakings which are part of a financial group and provide ICT services predominantly to their parent undertaking, or to subsidiaries or branches of their parent undertaking, as well as financial entities providing ICT services to other financial entities, should also be considered as ICT third-party service providers under this Regulation. Lastly, in light of the evolving payment services market becoming increasingly dependent on

complex technical solutions, and in view of emerging types of payment services and payment-related solutions, participants in the payment services ecosystem, providing payment-processing activities, or operating payment infrastructures, should also be considered to be ICT third-party service providers under this Regulation, with the exception of central banks when operating payment or securities settlement systems, and public authorities when providing ICT related services in the context of fulfilling State functions.

(64) 金融機関は，常時，この規則の中で定められた金融機関の義務を遵守することに関し，全面的に責任を負うままであるべきである。金融機関は，その金融機関の ICT と関連する依存性の性質，規模，複雑性及び重要性，契約上の取決めに服するサービス，プロセスまたは機能の不可欠性または重要性を適正に判断することにより，並びに，その推移次第では，個々の及びグループレベルの金融サービスの継続性及び品質に対する潜在的な影響の注意深い評価を適切に基礎として，ICT サードパーティサービスプロバイダの側で生じているリスクの監視に対し，比例的なアプローチを適用すべきである。

A financial entity should at all times remain fully responsible for complying with its obligations set out in this Regulation. Financial entities should apply a proportionate approach to the monitoring of risks emerging at the level of the ICT third-party service providers, by duly considering the nature, scale, complexity and importance of their ICT-related dependencies, the criticality or importance of the services, processes or functions subject to the contractual arrangements and, ultimately, on the basis of a careful assessment of any potential impact on the continuity and quality of financial services at individual and at group level, as appropriate.

(65) そのような監視の実行は，全ての ICT サードパーティ依存性の継続的な審査に根をもつ特化された ICT サードパーティリスク戦略がその金融機関の経営陣によって採択されることを介して公式のものとされる ICT サードパーティリスクに対する戦略的なアプローチに服するべきである。ICT サードパーティ依存性の監督上の認識を拡大するため，かつ，この規則によって設けられた監督枠組みの過程における仕事を更に支援するという観点から，全ての金融機関は，ICT サードパーティサービスプロバイダから提供される ICT サービスの利用に関する全ての契約上の取決めの情報の登録簿を維持管理することを要求されるべきである。金融監督当局は，登録簿全部の提出を要求しまたは登録簿の特定の箇所の提出を求めることもでき，また，金融機関の ICT 依存性のより広い理解を獲得するための必須の情報を入手することもできるべきである。

The conduct of such monitoring should follow a strategic approach to ICT third-party risk formalised through the adoption by the financial entity's management body of a dedicated ICT third-party risk strategy, rooted in a continuous screening of all ICT third-party dependencies. To enhance supervisory awareness of ICT third-party dependencies, and with a view to further supporting the work in the context of the Oversight Framework established by this Regulation, all financial entities should be required to maintain a register of information with all contractual arrangements about the use of ICT services provided by ICT third-party service providers. Financial supervisors should be able to request the full register, or to ask for specific sections thereof, and thus to obtain essential information for acquiring a broader understanding of the ICT dependencies of financial entities.

(66) とりわけ，予定されている ICT 契約によって支えられるサービスの不可欠性または重要性，必要的な監督機関の承認またはそれ以外の条件，それに伴う潜在的な集中のリスクのような諸要素に焦点を当てることによって，また，ICT サードパーティサービスプロバイダの選定及び評価のプロセスにおいてデューデリジェンスに努めること並びに利益相反を評価することによって，緻密な事前合意の分析が契約上の取決めの公式の締結を支えるべきであり，かつ，その締結に先立って行われるべきである。不可欠な機能または重要な機能と関係する契約上の取決めに関し，金融機関は，ICT サードパーティサービスプロバイダによる最新かつ最高度の情報セキュリティ基準の利用を考慮に入れるべきである。一連の状況，とりわけ，法律上もしくは契約上の条件の重大な違反，契約上の取決めの中で定められた機能の遂行能力の潜在的な変更を明らかにしている状況，ICT サードパーティサービスプロバイダの全体的な ICT リスクマネジメントの中にある当該サービスプロバイダの弱点の証拠，または，当該金融機関を実効的に監督するための適格な職務権限のある当局の不能を示す状況が，その ICT サードパーティサービスプロバイダのレベルにおける不足を示していることによって，少なくとも，契約上の取決めの終了が促進され得る。

A thorough pre-contracting analysis should underpin and precede the formal conclusion of contractual arrangements, in particular by focusing on elements such as the criticality or importance of the services supported by the envisaged ICT contract, the necessary supervisory approvals or other conditions, the possible concentration risk entailed, as well as applying due diligence in the process of selection and assessment of ICT third-party service providers and assessing potential conflicts of interest. For contractual arrangements concerning critical or important functions, financial entities should take into consideration the use by ICT third-party service providers of the most up-to-date and highest information security standards. Termination of contractual arrangements could be prompted at least by a series of circumstances showing shortfalls at the ICT third-party service provider level, in particular significant breaches of laws or contractual terms, circumstances revealing a potential alteration of the performance of the functions provided for in the contractual arrangements, evidence of weaknesses of the ICT third-party service provider in its overall ICT risk management, or circumstances indicating the inability of the relevant competent authority to effectively supervise the financial entity.

(67) ICT サードパーティの集中のリスクのシステミックな影響に対処するため，硬直的な上限または厳格な制限を加えることが事業者の行為を阻害し得るものであり，また，契約上の自由を抑制し得るものであることから，この規則は，そのような集中のリスクに対して柔軟かつ段階的なアプローチを講ずる方法により，バランスのとれた解決を促進する。金融機関は，とりわけ，第三国内に拠点をもつ ICT サードパーティサービスプロバイダとの間で締結されるときは，下請契約上の取決めの詳細な分析による場合を含め，そのようなリスクが生じていることの蓋然性を発見するため，その金融機関の予定されている契約上の取決めを緻密に評価すべきである。この段階において，かつ，契約上の自由を維持する必要性と金融の安定性を保証する必要性との間の公正なバランスをとるという観点から，ICT サードパーティのエクスポージャーに対する厳格な上限及び制限に関する規定を定めることは適切であるとは判断されない。監督枠組みの文脈においては，この規則によって任命される筆頭監督者は，不可欠な ICT サードパーティサービスプロバイダとの関係において，相互依存の影響度を全面的に理解すること，欧州連合内における不可欠の ICT サードパーティサービスプロバイダの高度の集中が欧州連合の金融システムの安定性及び完全性に対して負荷を加えているような個別の

場合を発見すること，そして，特定のリスクが特定された場合において，不可欠な ICT サードパーティサービスプロバイダとの間で対話することに特に注意を払うべきである。

To address the systemic impact of ICT third-party concentration risk, this Regulation promotes a balanced solution by means of taking a flexible and gradual approach to such concentration risk since the imposition of any rigid caps or strict limitations might hinder the conduct of business and restrain the contractual freedom. Financial entities should thoroughly assess their envisaged contractual arrangements to identify the likelihood of such risk emerging, including by means of in-depth analyses of subcontracting arrangements, in particular when concluded with ICT third-party service providers established in a third country. At this stage, and with a view to striking a fair balance between the imperative of preserving contractual freedom and that of guaranteeing financial stability, it is not considered appropriate to set out rules on strict caps and limits to ICT third-party exposures. In the context of the Oversight Framework, a Lead Overseer, appointed pursuant to this Regulation, should, in respect to critical ICT third-party service providers, pay particular attention to fully grasp the magnitude of interdependences, discover specific instances where a high degree of concentration of critical ICT third-party service providers in the Union is likely to put a strain on the Union financial system's stability and integrity and maintain a dialogue with critical ICT third-party service providers where that specific risk is identified.

(68) ICT サードパーティサービスプロバイダが，金融機関のデジタル運営管理上の回復力に対して負の影響を与えることなく，金融機関に対して安全にサービスを提供するための能力を定期的に査定及び監視するため，ICT サードパーティサービスプロバイダとの間の複数の鍵となる契約要素が整合化されるべきである。金融機関のデジタル回復力は金融機関が受ける ICT サービスの安定性，機能性，可用性及び安全性に深く依存していることから，金融機関のデジタル回復力を安全にすることの金融機関の必要性という観点から，そのような整合化は，ICT サードパーティサービスプロバイダから生じ得るリスクの金融機関による全面的な監視を可能とすることにとって重要なミニマムな分野を包摂すべきである。

To evaluate and monitor on a regular basis the ability of an ICT third party service provider to securely provide services to a financial entity without adverse effects on a financial entity's digital operational resilience, several key contractual elements with ICT third-party service providers should be harmonised. Such harmonisation should cover minimum areas which are crucial for enabling a full monitoring by the financial entity of the risks that could emerge from the ICT third-party service provider, from the perspective of a financial entity's need to secure its digital resilience because it is deeply dependent on the stability, functionality, availability and security of the ICT services received.

(69) この規則の要件と揃えることを求めるために契約上の取決めを再交渉する際，金融機関と ICT サードパーティサービスプロバイダは，この規則に定める鍵となる契約条項を包摂することを確保すべきである。

When renegotiating contractual arrangements to seek alignment with the requirements of this Regulation, financial entities and ICT third-party service providers should ensure the coverage of the key contractual provisions as provided for in this Regulation.

(70) この規則の中で定められている「不可欠な機能または重要な機能」の定義は，欧州議会及び理事会の指令 2024/59/EU[20]の第 2 条第 1 項第 35 号に定義する「不可欠な機能」を包含している。従って，指令 2014/59/EU によって不可欠であると判断される機能は，この規則の意味における不可欠な機能の定義の中に含められている。

The definition of 'critical or important function' provided for in this Regulation encompasses the 'critical functions' as defined in Article 2(1), point (35), of Directive 2014/59/EU of the European Parliament and of the Council[20]. Accordingly, functions deemed to be critical pursuant to Directive 2014/59/EU are included in the definition of critical functions within the meaning of this Regulation.

(71) ICT サービスによって支えられている機能の不可欠性または重要性の有無に拘わらず，契約上の取決めは，とりわけ，機能及びサービス，そのような機能が提供される場所及びデータが処理される場所の完全な記述の仕様並びにサービスレベルの記述の表示を定めるべきである。それら以外の，ICT サードパーティリスクの金融機関による監視を実現可能にするための必須の要素は，以下のとおりである：すなわち，個人データのアクセシビリティ，可用性，完全性，セキュリティ及び保護が ICT サードパーティサービスプロバイダによってどのように確保されるかの細目を定める契約条項；ICT サードパーティサービスプロバイダの破産，経営破綻または事業運営の継続不能の場合において，データのアクセス，復旧及び返還を実現可能にするための適格な保証を定める契約条項；及び，提供されるサービスと関係する ICT インシデントの場合において，付加的な費用負担なくまたは*事前に*定められた費用負担で，ICT サードパーティサービスプロバイダに対して補助を提供することを要求する契約条項；ICT サードパーティサービスプロバイダの，職務権限のある当局及び金融機関の破綻処理当局と全面的に協力する義務に関する契約条項；並びに，職務権限のある当局及び破綻処理当局の期待水準に従い，終了の権利及び契約上の取決めの終了のための関連するミニマムの通知期限に関する契約条項。

Irrespective of the criticality or importance of the function supported by the ICT services, contractual arrangements should, in particular, provide for a specification of the complete descriptions of functions and services, of the locations where such functions are provided and where data is to be processed, as well as an indication of service level descriptions. Other essential elements to enable a financial entity's monitoring of ICT third party risk are: contractual provisions specifying how the accessibility, availability, integrity, security and protection of personal data are ensured by the ICT third-party service provider, provisions laying down the relevant guarantees for enabling the access, recovery and return of data in the case of insolvency, resolution or discontinuation of the business operations of the ICT third-party

---

[20] 与信機関及び投資企業の再生及び破綻処理のための枠組みを定める，並びに，理事会指令 82/891/EEC，欧州議会及び理事会の指令 2001/24/EC，指令 2002/47/EC，指令 2004/25/EC，指令 2005/56/EC，指令 2007/36/EC，指令 2011/35/EU，指令 2012/30/EU 及び指令 2013/36/EU 並びに規則(EU) No 1093/2010 及び規則(EU) No 648/2012 を改正する欧州議会及び理事会の 2014 年 5 月 15 日の指令 2024/59/EU (OJ L 173, 12.6.2014, p. 190).

Directive 2014/59/EU of the European Parliament and of the Council of 15 May 2014 establishing a framework for the recovery and resolution of credit institutions and investment firms and amending Council Directive 82/891/EEC, and Directives 2001/24/EC, 2002/47/EC, 2004/25/EC, 2005/56/EC, 2007/36/EC, 2011/35/EU, 2012/30/EU and 2013/36/EU, and Regulations (EU) No 1093/2010 and (EU) No 648/2012, of the European Parliament and of the Council (OJ L 173, 12.6.2014, p. 190).

service provider, as well as provisions requiring the ICT third-party service provider to provide assistance in case of ICT incidents in connection with the services provided, at no additional cost or at a cost determined *ex-ante*; provisions on the obligation of the ICT third-party service provider to fully cooperate with the competent authorities and resolution authorities of the financial entity; and provisions on termination rights and related minimum notice periods for the termination of the contractual arrangements, in accordance with the expectations of competent authorities and resolution authorities.

(72) そのような契約条項に加え，かつ，金融機関の ICT セキュリティを阻害し得るサードパーティの側で生ずる全ての進展の全面的な監督を金融機関が維持することを確保するという観点から，不可欠な機能または重要な機能を支える ICT サービスの提供のための契約は，以下のことも定めるべきである：すなわち，合意されたサービスレベルに適合していない場合において不適正な遅滞なく適切な解消の活動をできるようにするための，詳密な定量的及び定性的な遂行能力の目標をもつ，サービスレベル全体の記述の仕様；当該 ICT サードパーティサービスプロバイダのそれぞれの ICT サービスを実効的に提供するための当該 ICT サードパーティサービスプロバイダの能力に対して潜在的で物理的な影響をもつ事態の場合における，ICT サードパーティサービスプロバイダの適格な通知期限及び報告義務；事業上の緊急事態対応計画を実装し及び試験し，並びに，サービスの安全な提供ができるようにする ICT セキュリティの方策，ツール及び基本方針をもち，また，当該金融機関によって実施される TLPT に参加しかつ全面的に協力すべき当該 ICT サードパーティサービスプロバイダの要件。

In addition to such contractual provisions, and with a view to ensuring that financial entities remain in full control of all developments occurring at third-party level which may impair their ICT security, the contracts for the provision of ICT services supporting critical or important functions should also provide for the following: the specification of the full service level descriptions, with precise quantitative and qualitative performance targets, to enable without undue delay appropriate corrective actions when the agreed service levels are not met; the relevant notice periods and reporting obligations of the ICT third-party service provider in the event of developments with a potential material impact on the ICT third-party service provider's ability to effectively provide their respective ICT services; a requirement upon the ICT third-party service provider to implement and test business contingency plans and have ICT security measures, tools and policies allowing for the secure provision of services, and to participate and fully cooperate in the TLPT carried out by the financial entity.

(73) 不可欠な機能または重要な機能を支える ICT サービスの提供に関する契約は，金融機関または指定されたサードパーティによるアクセスの権利，検査の権利及び監査の権利，並びに，検査の間における当該サービスプロバイダの全面的な協力と組み合わされたその ICT サードパーティサービスプロバイダの遂行能力の金融機関による監視の進行中における重要な道具として，コピーをとる権利を実現可能にする条項も含めるべきである。同様に，金融機関の職務権限のある当局は，通知に基づき，機密情報の保護に服して，ICT サードパーティサービスプロバイダを検査及び監査する権利をもつべきである。

Contracts for the provision of ICT services supporting critical or important functions should also contain provisions

enabling the rights of access, inspection and audit by the financial entity, or an appointed third party, and the right to take copies as crucial instruments in the financial entities' ongoing monitoring of the ICT third-party service provider's performance, coupled with the service provider's full cooperation during inspections. Similarly, the competent authority of the financial entity should have the right, based on notices, to inspect and audit the ICT third-party service provider, subject to the protection of confidential information.

(74) そのような契約上の取決めは，とりわけ，金融機関の側における混乱のリスクを削減するという観点から，その期間内は ICT サードパーティサービスプロバイダが適格なサービスを提供することを継続すべき強制的な移行期間を可能にするため，金融機関が，実効的に，他の ICT サードパーティサービスプロバイダの利用へと切替えることができるようにするため，または，代替的に，提供されるサービスの複雑性に合致するインハウスのソリューションに変更できるようにするための専用の出口戦略も定めるべきである。更に，指令 2014/59/EU の適用範囲内にある金融機関は，ICT サービスに関する適格な契約が，当該金融機関の破綻処理の際において堅牢かつ全面的に執行可能であることを確保すべきである。それゆえ，破綻処理当局の期待水準に沿って，それらの金融機関は，ICT サービスに関する適格な契約が破綻回復力をもつことを確保すべきである。それらの金融機関がそれらの金融機関の決済義務に適合し続けている限り，それらの金融機関は，他の諸要件の中でも，ICT サービスに関する適格な契約が，再建処理または破綻処理を理由として終了しないこと，停止しないこと及び変更しないことのための条項を含むことを確保すべきである。

Such contractual arrangements should also provide for dedicated exit strategies to enable, in particular, mandatory transition periods during which ICT third-party service providers should continue providing the relevant services with a view to reducing the risk of disruptions at the level of the financial entity, or to allow the latter effectively to switch to the use of other ICT third-party service providers or, alternatively, to change to in-house solutions, consistent with the complexity of the provided ICT service. Moreover, financial entities within the scope of Directive 2014/59/EU should ensure that the relevant contracts for ICT services are robust and fully enforceable in the event of resolution of those financial entities. Therefore, in line with the expectations of the resolution authorities, those financial entities should ensure that the relevant contracts for ICT services are resolution resilient. As long as they continue meeting their payment obligations, those financial entities should ensure, among other requirements, that the relevant contracts for ICT services contain clauses for non-termination, non-suspension and non-modification on grounds of restructuring or resolution.

(75) 更に，行政機関または欧州連合の機関によって策定された標準契約条項の任意の利用，とりわけ，クラウドコンピューティングサービスに関して欧州委員会によって策定される契約条項の利用は，欧州連合の金融サービス法によって定められた要件及び期待水準に全面的に揃えられて，金融部門におけるクラウドコンピューティングサービスの利用と関連する金融機関と ICT サードパーティサービスプロバイダの側における法的確実性を拡大することにより，金融機関と ICT サードパーティサービスプロバイダに対し，更なる快適さを提供し得る。措置を基礎とする標準契約条項の策定は，金融機関によってアウトソースされるクラウドコンピューティングサービスの利用に関する標準契約条項の策定を推進及び促進する欧州委員会の意図をアナウンスした 2018 年のフィンテック行動計画の中で既に予定されていた。それは，部門横断的なクラウドコンピューティングサービスの利用者の努力に基づいており，欧州委員会は，金融部門の関与という助けにより促進した。

Moreover, the voluntary use of standard contractual clauses developed by public authorities or Union institutions, in particular the use of contractual clauses developed by the Commission for cloud computing services could provide further comfort to the financial entities and ICT third-party service providers, by enhancing their level of legal certainty regarding the use of cloud computing services in the financial sector, in full alignment with the requirements and expectations set out by the Union financial services law. The development of standard contractual clauses builds on measures already envisaged in the 2018 Fintech Action Plan that announced the Commission's intention to encourage and facilitate the development of standard contractual clauses for the use of cloud computing services outsourcing by financial entities, drawing on cross-sectorial cloud computing services stakeholders' efforts, which the Commission has facilitated with the help of the financial sector's involvement.

(76) 金融部門における ICT サードパーティリスクに対処する際における監督上のアプローチとの関係における収束と効率を促進するため，また，金融サービスの供給を支える ICT サービスの提供のために不可欠な ICT サードパーティサービスプロバイダに依拠する金融機関のデジタル運営管理上の回復力を強化するため，そして，それによって，欧州連合の金融システムの安定性及び金融サービスのための域内市場の完全性の保全に貢献するため，不可欠な ICT サードパーティサービスプロバイダは，欧州連合の監督枠組みに服するべきである。監督枠組みの設置は，欧州連合レベルで行動をとることの付加価値によって及び金融サービスの提供における ICT サービスの利用の固有の役割と特性の効果によって正当化されるのであるが，それと同時に，金融部門におけるデジタル運営管理上の回復力を特に取扱うこの規則の文脈においてのみ，この解決策が適切であると思われることが想起されるべきである。ただし，そのような監督枠組みは，他の分野の金融サービス及び活動における欧州連合の監督のための新たなモデルとして考えられてはならない。

With a view to promoting convergence and efficiency in relation to supervisory approaches when addressing ICT third-party risk in the financial sector, as well as to strengthening the digital operational resilience of financial entities which rely on critical ICT third-party service providers for the provision of ICT services that support the supply of financial services, and thereby to contributing to the preservation of the Union's financial system stability and the integrity of the internal market for financial services, critical ICT third-party service providers should be subject to a Union Oversight Framework. While the set-up of the Oversight Framework is justified by the added value of taking action at Union level and by virtue of the inherent role and specificities of the use of ICT services in the provision of financial services, it should be recalled, at the same time, that this solution appears suitable only in the context of this Regulation specifically dealing with digital operational resilience in the financial sector. However, such Oversight Framework should not be regarded as a new model for Union supervision in other areas of financial services and activities.

(77) 監督枠組みは，不可欠な ICT サードパーティサービスプロバイダのみに対して，適用されるべきである。それゆえ，そのような ICT サードパーティサービスプロバイダに対する当該金融部門の依拠の局面及び性質を考慮に入れるための指定の仕組みが存在すべきである。その仕組みは，監督枠組みへの包摂のための基礎としての不可欠性のパラメータを定めるための定量的及び定性的な基準のセットを含むべきである。その評価の正確性を確保するため，かつ，ICT サードパーティサービスプロバイダの企業構造の別に拘わらず，ICT サードパーティサービスプロバイダがより広範なグループの一部となっている場合においては，そのような基準は，その ICT サードパーティサービスプロバイダ

のグループ全体の構造を考慮に入れるべきである。一方において，それらの基準の適用の効力によって自動的に指定されるのではない不可欠な ICT サードパーティサービスプロバイダは，任意で監督枠組みの中に入ることの可能性をもつべきであるが，他方において，TFEU の第 127 条第 2 項に示す欧州中央銀行制度の仕事を満たすことを支える監督の仕組みの枠組みに既に服している ICT サードパーティサービスプロバイダは，適用除外されるべきである。

The Oversight Framework should apply only to critical ICT third-party service providers. There should therefore be a designation mechanism to take into account the dimension and nature of the financial sector's reliance on such ICT third-party service providers. That mechanism should involve a set of quantitative and qualitative criteria to set the criticality parameters as a basis for inclusion in the Oversight Framework. In order to ensure the accuracy of that assessment, and regardless of the corporate structure of the ICT third-party service provider, such criteria should, in the case of a ICT third-party service provider that is part of a wider group, take into consideration the entire ICT third-party service provider's group structure. On the one hand, critical ICT third-party service providers, which are not automatically designated by virtue of the application of those criteria, should have the possibility to opt in to the Oversight Framework on a voluntary basis, on the other hand, ICT third-party service providers, that are already subject to oversight mechanism frameworks supporting the fulfilment of the tasks of the European System of Central Banks as referred to in Article 127(2) TFEU, should be exempted.

(78) 同様に，他の金融機関に対して ICT サービスを提供する金融機関もまた，この規則の下における ICT サードパーティサービスプロバイダの類型に属するが，それらの金融機関が欧州連合の適格な金融サービス法によって設けられた監督の仕組みに既に服していることから，監督枠組みから適用除外されるべきである。それが適用可能なときは，職務権限のある当局は，当該当局の監督活動の過程において，ICT サービスを提供している金融機関によって金融機関に対して呈されている ICT リスクを考慮に入れるべきである。同様に，グループレベルのリスク監視の仕組みが存在することから，主として当該 ICT サードパーティサービスプロバイダ自身のグループの法主体に対してサービスを供給している ICT サードパーティサービスプロバイダに関しては，同じ適用除外が導入されるべきである。1 つの構成国内のみにおいて，当該構成国内のみで能動的な金融機関に対して ICT サービスを提供している ICT サードパーティサービスプロバイダもまた，当該金融機関の限定された活動であること及び国境を越える影響が欠けていることのゆえに，指定の仕組みから適用除外されるべきである。

Similarly, financial entities providing ICT services to other financial entities, while belonging to the category of ICT third-party service providers under this Regulation, should also be exempted from the Oversight Framework since they are already subject to supervisory mechanisms established by the relevant Union financial services law. Where applicable, competent authorities should take into account, in the context of their supervisory activities, the ICT risk posed to financial entities by financial entities providing ICT services. Likewise, due to the existing risk monitoring mechanisms at group level, the same exemption should be introduced for ICT third-party service providers delivering services predominantly to the entities of their own group. ICT third-party service providers providing ICT services solely in one Member State to financial entities that are active only in that Member State should also be exempted from the designation mechanism because of their limited activities and lack of cross-border impact.

(79) 金融サービスにおいて経験されたデジタル変革は，かつてないレベルの ICT サービスの利用とそれに対する依拠をもたらした。クラウドコンピューティングサービス，ソフトウェアソリューション及びデータ関連サービスの利用なしに金融サービスを提供することが考えられなくなってしまったので，欧州連合の金融のエコシステムは，必然的に，ICT サービスの供給される一定の ICT サービスに共に依存するものとなった。それらの供給者，ICT ベースの技術を開発し及び適用する技術開発者の幾つかは，金融サービスの供給において大きな役割を果たしており，または，金融サービスの価値連鎖の中に統合されるようになった。そして，それらは，欧州連合の金融システムの安定性及び完全性によって不可欠になった。不可欠な ICT サードパーティサービスプロバイダが運営管理上の混乱または大きなサイバーインシデントによって影響を受けるときは，不可欠な ICT サードパーティサービスプロバイダから供給されるサービスに対するこの広範な依拠は，様々な市場運営者の情報システムの相互依存と結合されて，欧州連合の金融サービスシステムに対する及び金融サービスの供給の継続性に対する直接的かつ潜在的に重大なリスクをつくり出す。サイバーインシデントは，金融部門において監視される他のタイプのリスクよりもはるかに速いペースで金融システム全体に増殖及び繁殖するための特有の能力をもっており，また，部門を超えてかつ地理的国境を越えて拡大し得る。サイバーインシデントは，実体経済を支える機能の混乱によりまたは金融上の大きな損失により，金融システムに対する信頼が損なわれ，金融システムが存立できないレベルに達する場合または強力な緩衝措置の配置を要求するレベルに達する場合には，システミックな危機に進化する潜在力をもつ。それらのシナリオが生ずること避け，かつ，欧州連合の金融の安定性と完全性が損なわれることを避けるため，とりわけ，不可欠な ICT サードパーティサービスプロバイダの欧州連合の監督を実現可能にする新たな規定を通じて，金融における ICT サードパーティリスクと関連する監督実務の収斂を提供することが必須である。

The digital transformation experienced in financial services has brought about an unprecedented level of use of, and reliance upon, ICT services. Since it has become inconceivable to provide financial services without the use of cloud computing services, software solutions and data-related services, the Union financial ecosystem has become intrinsically co-dependent on certain ICT services provided by ICT service suppliers. Some of those suppliers, innovators in developing and applying ICT-based technologies, play a significant role in the delivery of financial services, or have become integrated into the financial services value chain. They have thus become critical to the stability and integrity of the Union financial system. This widespread reliance on services supplied by critical ICT third-party service providers, combined with the interdependence of the information systems of various market operators, create a direct, and potentially severe, risk to the Union financial services system and to the continuity of delivery of financial services if critical ICT third-party service providers were to be affected by operational disruptions or major cyber incidents. Cyber incidents have a distinctive ability to multiply and propagate throughout the financial system at a considerably faster pace than other types of risk monitored in the financial sector and can extend across sectors and beyond geographical borders. They have the potential to evolve into a systemic crisis, where trust in the financial system has been eroded due to the disruption of functions supporting the real economy, or to substantial financial losses, reaching a level which the financial system is unable to withstand, or which requires the deployment of heavy shock absorption measures. To prevent these scenarios from taking place and thereby endangering the financial stability and integrity of the Union, it is essential to provide the convergence of supervisory practices relating to ICT third-party risk in finance, in particular through new rules enabling the Union oversight of critical ICT third-party service providers.

(80) 監督枠組みは，筆頭監督者と，金融サービスの供給に影響を与えるサービスを金融機関に対して供給している不可欠な ICT サードパーティサービスプロバイダとの間の共働の程度に大きく依存している。監督の成功は，就中，不可欠な ICT サードパーティサービスプロバイダによって利用される諸原則，管理策及び処理を評価するため並びに金融の安定性及び金融システムの完全性に対する当該 ICT サードパーティサービスプロバイダの活動の潜在的に累積的な影響を評価するための監視の任務と検査を実効的に実施するための筆頭監督者の能力にかかっている。それと同時に，不可欠な ICT サードパーティサービスプロバイダが，筆頭監督者の勧告書に従うこと及び筆頭監督者の関心事に対処することが重要である。不可欠な ICT サードパーティサービスプロバイダの構内へのアクセスを認めることまたは情報を送信することを拒否する場合のように，金融サービスの供給に影響を与えるサービスを提供している不可欠な ICT サードパーティサービスプロバイダによる協力が欠けると，その推移次第では，ICT サードパーティのリスクの評価において筆頭監督者の必須のツールを筆頭監督者から奪うことになり，また，金融の安定性及び金融システムの完全性に対して負の影響を与え得るので，相応の制裁の体制を定めることも必要である。

The Oversight Framework largely depends on the degree of collaboration between the Lead Overseer and the critical ICT third-party service provider delivering to financial entities services affecting the supply of financial services. Successful oversight is predicated, inter alia, upon the ability of the Lead Overseer to effectively conduct monitoring missions and inspections to assess the rules, controls and processes used by the critical ICT third-party service providers, as well as to assess the potential cumulative impact of their activities on financial stability and the integrity of the financial system. At the same time, it is crucial that critical ICT third-party service providers follow the Lead Overseer's recommendations and address its concerns. Since a lack of cooperation by a critical ICT third-party service provider providing services that affect the supply of financial services, such as the refusal to grant access to its premises or to submit information, would ultimately deprive the Lead Overseer of its essential tools in appraising ICT third-party risk, and could adversely impact the financial stability and the integrity of the financial system, it is necessary to also provide for a commensurate sanctioning regime.

(81) この背景事情に抗して，この規則の中で定められた透明性の義務及びアクセスと関連する義務を遵守することを不可欠な ICT サードパーティサービスプロバイダに対して強制するために，筆頭監督者が制裁金を科す必要性は，第三国内に拠点をもつ不可欠な ICT サードパーティサービスプロバイダとの関係におけるそれらの制裁金の執行から生ずる困難によって危険に晒されてはならない。そのような制裁の執行可能性を確保するため，そして，指定の仕組み及び勧告書を発する過程における不可欠な ICT サードパーティサービスプロバイダの防御の権利を支える手続を迅速に準備できるようにするため，金融サービスの供給に影響を与えるサービスを金融機関に対して提供しているそれらの不可欠な ICT サードパーティサービスプロバイダは，欧州連合内において十分な事業活動を維持管理することを要求されるべきである。その監督の性質のゆえに，また，他の主権国家内において同等の手立てが存在しないことのゆえに，第三国内に拠点をもつ不可欠な ICT サードパーティサービスプロバイダとして分類される ICT サードパーティサービスプロバイダによって呈されるデジタル運営管理上のリスクの影響の監視との関係において，第三国内において金融監督当局との間で実効的に共働するという方法により，この目的の達成を確保する適切な代替の仕組みは存在しない。それゆえ，欧州連合内の金融機関に対して当該 ICT サードパーティサービスプロバイダの ICT サー

ビスの提供を継続するためには，この規則に従って不可欠として指定された第三国内に拠点をもつ ICT サードパーティサービスプロバイダは，その指定から 12 か月以内に，欧州連合の*法*に定義する支店，すなわち，欧州議会及び理事会の指令 2013/34/EU[21]に定義する子事業者を設立することにより，欧州連合内における当該 ICT サードパーティサービスプロバイダの設立を確保するための全ての必要な手立てを実施すべきである。

Against this background, the need of the Lead Overseer to impose penalty payments to compel critical ICT third-party service providers to comply with the transparency and access-related obligations set out in this Regulation should not be jeopardised by difficulties raised by the enforcement of those penalty payments in relation to critical ICT third-party service providers established in third countries. In order to ensure the enforceability of such penalties, and to allow a swift roll out of procedures upholding the critical ICT third-party service providers' rights of defence in the context of the designation mechanism and the issuance of recommendations, those critical ICT third-party service providers, providing services to financial entities that affect the supply of financial services, should be required to maintain an adequate business presence in the Union. Due to the nature of the oversight, and the absence of comparable arrangements in other jurisdictions, there are no suitable alternative mechanisms ensuring this objective by way of effective cooperation with financial supervisors in third countries in relation to the monitoring of the impact of digital operational risks posed by systemic ICT third-party service providers, qualifying as critical ICT third-party service providers established in third countries. Therefore, in order to continue its provision of ICT services to financial entities in the Union, an ICT third-party service provider established in a third country which has been designated as critical in accordance with this Regulation should undertake, within 12 months of such designation, all necessary arrangements to ensure its incorporation within the Union, by means of establishing a subsidiary, as defined throughout the Union *acquis*, namely in Directive 2013/34/EU of the European Parliament and of the Council[(21)].

(82) 欧州連合内に子事業者を設置する要件は，不可欠な ICT サードパーティサービスプロバイダが，欧州連合の外に所在する施設及びインフラから ICT サービス及び関連する技術サポートのサービスを供給することを妨げてはならない。この規則は，データの記録保存または処理が欧州連合内において実施されることをこの規則が要求していないので，データローカライゼーションの義務を課さない。

The requirement to set up a subsidiary in the Union should not prevent the critical ICT third-party service provider from supplying ICT services and related technical support from facilities and infrastructure located outside the Union. This Regulation does not impose a data localisation obligation as it does not require data storage or processing to be undertaken in the Union.

---

[21] 一定のタイプの事業者の年次財務諸表，連結財務諸表及び関連報告書に関する，欧州議会及び理事会の指令 2006/43/EC を改正する，並びに，理事会指令 78/660/EEC 及び理事会指令 83/349/EEC を廃止する欧州議会及び理事会の 2013 年 6 月 26 日の指令 2013/34/EU (OJ L 182, 29.6.2013, p. 19).

Directive 2013/34/EU of the European Parliament and of the Council of 26 June 2013 on the annual financial statements, consolidated financial statements and related reports of certain types of undertakings, amending Directive 2006/43/EC of the European Parliament and of the Council and repealing Council Directives 78/660/EEC and 83/349/EEC (OJ L 182, 29.6.2013, p. 19).

(83) 不可欠な ICT サードパーティサービスプロバイダは，欧州連合内に所在する構内から提供する必要なく，または，欧州連合内に所在する構内のみから提供するのではなく，世界中のどこからでも ICT サービスを提供できるべきである。監督活動は，この規則により不可欠な ICT サードパーティサービスプロバイダによって設立された子事業者を含め，欧州連合内に所在する施設において，かつ，欧州連合内に所在する法主体とのやりとりによって，まず実行されるべきである。ただし，そのような欧州連合内における活動は，この規則の下にある筆頭監督者がその義務を完全かつ実効的に遂行できるようにするためには，不十分かもしれない。それゆえ，筆頭監督者は，第三国内においても，筆頭監督者の適格な監督権限を行使できるべきである。第三国内におけるその権限の行使は，筆頭監督者が，不可欠な ICT サードパーティサービスプロバイダによって ICT サービスまたは技術サポートのサービスが実際に提供されまたは取扱われる施設を調査できるようにすべきであり，また，筆頭監督者に対し，その不可欠な ICT サードパーティサービスプロバイダの ICT リスクマネジメントの包括的かつ運用上の理解を与えるべきである。筆頭監督者が，欧州連合の部局として，欧州連合の領域の外において権限を行使し得ることは，適格な諸条件によって，とりわけ，関係する不可欠な ICT サードパーティサービスプロバイダの同意によって，適正に枠付けられるべきである。同様に，第三国の適格な当局は，筆頭監督者の活動の当該第三国の領土上における実行について連絡を受けているべきであり，かつ，それに対して異議を唱えていないべきである。ただし，効率的な実装を確保するため，かつ，欧州連合の機関及び構成国のそれぞれの職務権限を妨げることなく，そのような権限は，関係する第三国の適格な当局との間における行政協力協定の締結においても，全面的に定められている必要がある。それゆえ，この規則は，ESAs が，第三国の適格な当局との間において行政協力協定を締結できるようにすべきであるが，その協定は，欧州連合及びその構成国との関係において，それ以外の法律上の義務をつくり出してはならない。

Critical ICT third-party service providers should be able to provide ICT services from anywhere in the world, not necessarily or not only from premises located in the Union. Oversight activities should be first conducted on premises located in the Union and by interacting with entities located in the Union, including the subsidiaries established by critical ICT third-party service providers pursuant to this Regulation. However, such actions within the Union might be insufficient to allow the Lead Overseer to fully and effectively perform its duties under this Regulation. The Lead Overseer should therefore also be able to exercise its relevant oversight powers in third countries. Exercising those powers in third countries should allow the Lead Overseer to examine the facilities from which the ICT services or the technical support services are actually provided or managed by the critical ICT third-party service provider, and should give the Lead Overseer a comprehensive and operational understanding of the ICT risk management of the critical ICT third-party service provider. The possibility for the Lead Overseer, as a Union agency, to exercise powers outside the territory of the Union should be duly framed by relevant conditions, in particular the consent of the critical ICT third-party service provider concerned. Similarly, the relevant authorities of the third country should be informed of, and not have objected to, the exercise on their own territory of the activities of the Lead Overseer. However, in order to ensure efficient implementation, and without prejudice to the respective competences of the Union institutions and the Member States, such powers also need to be fully anchored in the conclusion of administrative cooperation arrangements with the relevant authorities of the third country concerned. This Regulation should therefore enable the ESAs to conclude administrative cooperation arrangements with the relevant authorities of third countries, which should not otherwise create legal obligations in respect of the Union and its Member States.

(84) 筆頭監督者との間の通信を容易にするため及び適切な代理を確保するため，グループの一部となっている不可欠な ICT サードパーティサービスプロバイダは，当該 ICT サードパーティサービスプロバイダの調整場所として，1 つの法人を指定すべきである。

To facilitate communication with the Lead Overseer and to ensure adequate representation, critical ICT third-party service providers which are part of a group should designate one legal person as their coordination point.

(85) 監督枠組みは，この規則の下においては不可欠として指定されていないが，国内レベルでは重要だと考えられている ICT サードパーティサービスプロバイダとの関係において，当該構成国自身の監督または監視の任務を実行する構成国の職務権限を妨げてはならない。

The Oversight Framework should be without prejudice to Member States' competence to conduct their own oversight or monitoring missions in respect to ICT third-party service providers which are not designated as critical under this Regulation, but which are regarded as important at national level.

(86) 金融サービスの分野における多層の組織アーキテクチャを梃入れするため，ESAs の共同委員会は，サイバーセキュリティに関する同委員会の職務に従い，ICT リスクと関連する全ての事項との関係において全ての部門を横断する調整を確保することを続けるべきである。同委員会は，不可欠な ICT サードパーティサービスプロバイダに宛てられた個々の決定，並びに，とりわけ，不可欠な ICT サードパーティサービスプロバイダに対する監督計画の指標化との関係において，集団的な勧告を発すること，及び，ICT 集中化リスクという問題に対処するためのベストプラクティスを発見することの両者のための準備作業を実行する新たな小委員会（「監督フォーラム」）によって支えられるべきである。

To leverage the multi-layered institutional architecture in the financial services area, the Joint Committee of the ESAs should continue to ensure overall cross-sectoral coordination in relation to all matters pertaining to ICT risk, in accordance with its tasks on cybersecurity. It should be supported by a new Subcommittee (the 'Oversight Forum') carrying out preparatory work both for the individual decisions addressed to critical ICT third-party service providers, and for the issuing of collective recommendations, in particular in relation to benchmarking the oversight programmes for critical ICT third-party service providers, and identifying best practices for addressing ICT concentration risk issues.

(87) 不可欠な ICT サードパーティサービスプロバイダが欧州連合レベルで適切かつ実効的に監督されることを確保するため，この規則は，3 つの ESAs 中のいずれかが筆頭監督者として指定され得ることを定めている。3 つの ESAs の 1 つへの不可欠な ICT サードパーティサービスプロバイダの個々の割当ては，当該 ESA が職責を負う金融部門において運営管理している金融機関の優位性の評価から帰結すべきである。このアプローチは，監督機能の実行の過程において，3 つの ESAs の間におけるバランスのとれた職務と職責の割当てを導くべきであり，また，3 つの ESAs のそれぞれにおいて利用可能な人的資源及び技術上の専門知識の最善の利用をつくり出すべきである。

To ensure that critical ICT third-party service providers are appropriately and effectively overseen on a Union level, this Regulation provides that any of the three ESAs could be designated as a Lead Overseer. The individual assignment of a

critical ICT third-party service provider to one of the three ESAs should result from an assessment of the preponderance of financial entities operating in the financial sectors for which that ESA has responsibilities. This approach should lead to a balanced allocation of tasks and responsibilities between the three ESAs, in the context of exercising the oversight functions, and should make the best use of the human resources and technical expertise available in each of the three ESAs.

(88) 筆頭監督者は，調査を実行するため，不可欠な ICT サードパーティサービスプロバイダの構内及び所在地の内外における検査を実施するため，並びに，完全かつアップデートされた情報を入手するために必要となる権限を与えられるべきである。それらの権限は，金融機関に対して及びその推移次第では欧州連合の金融システムに対して呈された ICT サードパーティリスクのタイプ，局面及び影響の実際の知見を筆頭監督者が獲得することを実現可能にすべきである。ESAs に対して筆頭監督の役割が任されることは，金融における ICT リスクのシステミックな局面の理解及び対応のための前提条件である。欧州連合の金融部門に対する不可欠な ICT サードパーティサービスプロバイダの影響及び ICT 集中化リスクに伴って生ずる潜在的な検討課題は，欧州連合レベルの集団的なアプローチをとることを求めている。不可欠な ICT サードパーティサービスプロバイダが多数の監視と検査の要求に服する場合には，不可欠な ICT サードパーティサービスプロバイダにとって，冗長性，負担及び複雑性をつくり出すことにもなるのであるが，多数の職務権限のある当局によって，それらの当局間においてあまり調整されずまたは全く調整されずに個別に遂行される多重の監査とアクセスの権利の同時の実施は，金融監督当局が，欧州連合における ICT サードパーティリスクの完全かつ包括的な概況を獲得することを妨げることだろう。

Lead Overseers should be granted the necessary powers to conduct investigations, to carry out onsite and offsite inspections at the premises and locations of critical ICT third-party service providers and to obtain complete and updated information. Those powers should enable the Lead Overseer to acquire real insight into the type, dimension and impact of the ICT third-party risk posed to financial entities and ultimately to the Union's financial system. Entrusting the ESAs with the lead oversight role is a prerequisite for understanding and addressing the systemic dimension of ICT risk in finance. The impact of critical ICT third-party service providers on the Union financial sector and the potential issues caused by the ICT concentration risk entailed call for taking a collective approach at Union level. The simultaneous carrying out of multiple audits and access rights, performed separately by numerous competent authorities, with little or no coordination among them, would prevent financial supervisors from obtaining a complete and comprehensive overview of ICT third-party risk in the Union, while also creating redundancy, burden and complexity for critical ICT third-party service providers if they were subject to numerous monitoring and inspection requests.

(89) 不可欠として指定されることの大きな影響のゆえに，この規則は，不可欠な ICT サードパーティサービスプロバイダの諸権利が監督枠組みの実装の全体を通じて尊重されることを確保すべきである。不可欠として指定される前に，そのようなプロバイダは，例えば，筆頭監督者に対し，当該プロバイダの指定と関連する評価の目的のための適格な情報を含む理由を付した陳述書を提出する権利をもつべきである。筆頭監督者は，その推移次第では金融機関または金融システムの安定性を害する一定の契約上の取決めに反対する権限を含む，ICT リスク上の事柄及びそれらの事柄の適切な解消策に関する勧告書を提出する権限を与えられるべきであるので，不可欠な ICT サードパーティサ

ービスプロバイダもまた，それらの勧告書の完成の前に，その勧告書の中に掲げられているソリューションの，この規則の適用範囲外にある法主体である顧客に対する予想される影響に関する説明書を提出する機会及びリスクを緩和するためのソリューションを形成する機会を与えられるべきである。勧告書に同意しない不可欠な ICT サードパーティサービスプロバイダは，その勧告書に賛成しないつもりであるという当該不可欠な ICT サードパーティサービスプロバイダの理由を付した説明書を提出すべきである。そのような理由を付した説明書が提出されない場合，または，不十分であると判断される場合，筆頭監督者は，不遵守事項の要旨を示す告示を発するべきである。

Due to the significant impact of being designated as critical, this Regulation should ensure that the rights of critical ICT third-party service providers are observed throughout the implementation of the Oversight Framework. Prior to being designated as critical, such providers should, for example, have the right to submit to the Lead Overseer a reasoned statement containing any relevant information for the purposes of the assessment related to their designation. Since the Lead Overseer should be empowered to submit recommendations on ICT risk matters and suitable remedies thereto, which include the power to oppose certain contractual arrangements ultimately affecting the stability of the financial entity or the financial system, critical ICT third-party service providers should also be given the opportunity to provide, prior to the finalisation of those recommendations, explanations regarding the expected impact of the solutions, envisaged in the recommendations, on customers that are entities falling outside the scope of this Regulation and to formulate solutions to mitigate risks. Critical ICT third-party service providers disagreeing with the recommendations should submit a reasoned explanation of their intention not to endorse the recommendation. Where such reasoned explanation is not submitted or where it is considered to be insufficient, the Lead Overseer should issue a public notice summarily describing the matter of non-compliance.

(90) 職務権限のある当局は，金融機関の健全性監督と関連する当該当局の権能内において，筆頭監督者から発された勧告書の実質的な遵守を検証する職務を適正に含めるべきである。職務権限のある当局は，金融機関に対し，筆頭監督者の勧告書の中で特定されたリスクに対処するための付加的な方策をとることを要求できるべきであり，かつ，しかるべく，その旨の通知を発するべきである。指令(EU) 2022/2555 の下において監督を受ける不可欠な ICT サードパーティサービスプロバイダに対して筆頭監督者が勧告書を発出するときは，当の不可欠な ICT サードパーティサービスプロバイダを取扱うための調整されたアプローチを育成するため，職務権限のある当局は，任意にかつ付加的な方策を採択する前に，同指令の下にある職務権限のある当局から意見聴取できるべきである。

Competent authorities should duly include the task of verifying substantive compliance with recommendations issued by the Lead Overseer in their functions with regard to prudential supervision of financial entities. Competent authorities should be able to require financial entities to take additional measures to address the risks identified in the Lead Overseer's recommendations, and should, in due course, issue notifications to that effect. Where the Lead Overseer addresses recommendations to critical ICT third-party service providers that are supervised under Directive (EU) 2022/2555, the competent authorities should be able, on a voluntary basis and before adopting additional measures, to consult the competent authorities under that Directive in order to foster a coordinated approach to dealing with the critical ICT third-party service providers in question.

(91) 監督の実行は，以下のことを確保することを求めている 3 つの運営管理上の基本原則によってガイドされるべきである：すなわち，(a) 共同監督ネットワーク（JON）を介する，ESAs の筆頭監督者の役割における ESAs 間の緊密な調整，(b)（不可欠な ICT サードパーティサービスプロバイダに対して向けられた措置の重複を避けるための指令(EU) 2022/2555 の下における諸組織の任意の意見聴取を介する）同指令によって設けられた枠組みとの一貫性，並びに，(c) この規則の適用範囲外にある法主体である顧客に対する不可欠な ICT サードパーティサービスプロバイダから提供されるサービスの混乱という潜在的なリスクをミニマム化することに努めることである。

The exercise of the oversight should be guided by three operational principles seeking to ensure: (a) close coordination among the ESAs in their Lead Overseer roles, through a joint oversight network (JON), (b) consistency with the framework established by Directive (EU) 2022/2555 (through a voluntary consultation of bodies under that Directive to avoid duplication of measures directed at critical ICT third-party service providers), and (c) applying diligence to minimise the potential risk of disruption to services provided by the critical ICT third-party service providers to customers that are entities falling outside the scope of this Regulation.

(92) 監督枠組みは，不可欠な ICT サードパーティサービスプロバイダとの間で締結された契約上の取決めの継続的な監視を維持すべき当該金融機関の義務を含め，ICT サードパーティサービスプロバイダの利用に伴うリスクを当該金融機関自身が取扱うという金融機関の要件を置換えてはならず，または，いかなる方途においても，もしくは，いかなる部分においても別のものに代えてはならない。同様に，監督枠組みは，この規則及び適格な金融サービス法の中で定められた全ての法律上の義務を遵守することに関する及びそれを履行することに関する金融機関の全面的な職責に影響を与えてはならない。

The Oversight Framework should not replace, or in any way or for any part substitute for, the requirement for financial entities to manage themselves the risks entailed by the use of ICT third-party service providers, including their obligation to maintain an ongoing monitoring of contractual arrangements concluded with critical ICT third-party service providers. Similarly, the Oversight Framework should not affect the full responsibility of financial entities for complying with, and discharging, all the legal obligations laid down in this Regulation and in the relevant financial services law.

(93) 重複と重用を避けるため，職務権限のある当局は，不可欠な ICT サードパーティサービスプロバイダのリスクを監視することを狙いとする措置を個別に講ずることを控えるべきであり，また，この点に関しては，適格な筆頭監督者の評価に依拠すべきである。措置は，監督枠組みにおける職務の実行の過程においては，いかなる場合においても筆頭監督者が優越して調整され合意されるべきである。

To avoid duplications and overlaps, competent authorities should refrain from taking individually any measures aiming to monitor the critical ICT third-party service provider's risks and should, in that respect, rely on the relevant Lead Overseer's assessment. Any measures should in any case be coordinated and agreed in advance with the Lead Overseer in the context of the exercise of tasks in the Oversight Framework.

(94) ICT サードパーティサービスプロバイダのデジタルリスクマネジメントの見直し及び監視におけるベス

トプラクティスの利用に関する国際的なレベルの収斂を促進するため，ESAs は，適格な監督上及び法制上の第三国の当局との間で協力協定を締結することが推奨されるべきである。

To promote convergence at international level as regards the use of best practices in the review and monitoring of ICT third-party service providers' digital risk-management, the ESAs should be encouraged to conclude cooperation arrangements with relevant supervisory and regulatory third-country authorities.

(95) 職務権限のある当局，3 つの ESAs 及び任意ベースで指令(EU) 2022/2555 の下における職務権限のある当局の中における運営管理上及び ICT のリスクに特化している職員の個別の能力，技術上の技能及び専門知識を梃入れするため，筆頭監督者は，国内の監督の能力と知識を活かすべきであり，また，不可欠な ICT サードパーティサービスプロバイダの一般的な調査及び検査を含め，監督活動の準備及び実行を支える学際的なチームをプールする，個々の不可欠な ICT サードパーティサービスプロバイダに関する並びにそれらの監督活動の必要な事後対応に関する専門検討チームを設けるべきである。

To leverage the specific competences, technical skills and expertise of staff specialising in operational and ICT risk within the competent authorities, the three ESAs and, on a voluntary basis, the competent authorities under Directive (EU) 2022/2555, the Lead Overseer should draw on national supervisory capabilities and knowledge and set up dedicated examination teams for each critical ICT third-party service provider, pooling multidisciplinary teams in support of the preparation and execution of oversight activities, including general investigations and inspections of critical ICT third-party service providers, as well as for any necessary follow-up thereto.

(96) 監督の職務からもたらされる費用は，不可欠な ICT サードパーティサービスプロバイダに対して課される手数料から全額資金付けられるだろうが，しかしながら，専用の ICT システムが開発されかつ予め設置されている必要があるので，監督枠組みの開始の前に，来るべき監督を支える専用の ICT システムの実装のための費用が ESAs にかかりそうである。それゆえ，この規則は，ハイブリッドな資金モデルを定める。そのモデルによって，ESAs の ICT システムの開発が欧州連合及び職務権限のある国内当局の拠出から資金付けられるようにしつつ，監督枠組みは，そのように全額が手数料で資金付けられるだろう。

Whereas costs resulting from oversight tasks would be fully funded from fees levied on critical ICT third-party service providers, the ESAs are. however, likely to incur, before the start of the Oversight Framework, costs for the implementation of dedicated ICT systems supporting the upcoming oversight, since dedicated ICT systems would need to be developed and deployed beforehand. This Regulation therefore provides for a hybrid funding model, whereby the Oversight Framework would, as such, be fully fee-funded, while the development of the ESAs' ICT systems would be funded from Union and national competent authorities' contributions.

(97) 職務権限のある当局は，この規則の下における職務権限のある当局の責務の適正な履行を確保するために要求される監督権限，調査権限及び制裁権限の全てをもつべきである。職務権限のある当局は，原則として，当該職務権限のある当局が課した行政制裁の通知を公表すべきである。金融機

関及び ICT サードパーティサービスプロバイダは，異なる構成国において設立され得るのであり，かつ，異なる職務権限のある当局により監督され得るので，この規則の適用は，一方において，理事会規則(EU) No 1024/2013 によって ECB に対して与えられた特別の職務との関連において ECB を含め，適格な職務権限のある当局の間における緊密な共働によって，また，他方において，適格な監督活動の過程における情報の相互交換と補助の提供を介する ESAs からの意見聴取により，容易にされるべきである。

Competent authorities should have all required supervisory, investigative and sanctioning powers to ensure the proper exercise of their duties under this Regulation. They should, in principle, publish notices of the administrative penalties they impose. Since financial entities and ICT third-party service providers can be established in different Member States and supervised by different competent authorities, the application of this Regulation should be facilitated by, on the one hand, close cooperation among relevant competent authorities, including the ECB with regard to specific tasks conferred on it by Council Regulation (EU) No 1024/2013, and, on the other hand, by consultation with the ESAs through the mutual exchange of information and the provision of assistance in the context of relevant supervisory activities.

(98) ICT サードパーティサービスプロバイダの不可欠としての指定のための基準を更に定量化及び定性化するため，また，監督費用を整合化するため，TFEU の第 290 条に従い，当該 ICT サードパーティサービスプロバイダが ICT サービスを提供する金融機関に対して ICT サードパーティサービスプロバイダの不履行または運用停止がもち得るシステミックな影響，当の ICT サードパーティサービスプロバイダに依拠するグローバルなシステミック上で重要な機関（G-SIIs）またはそれ以外のシステミック上で重要な機関（O-SIIs）の数，所与の市場において能動的な ICT サードパーティサービスプロバイダの数，他の ICT サードパーティサービスプロバイダに対してデータ及び ICT 作業を移植する費用，並びに，監督の費用の額及びその費用が支払われる方法を更に細目的に定めることによってこの規則を補完するための法行為を採択する権限は，欧州委員会に対して委任されるべきである。欧州委員会が，その準備作業の間，専門家レベルのものを含め，適切な意見聴取を実施すること，そして，その意見聴取がより良い立法に関する 2016 年 4 月 13 日の機関間合意[22]の中で定められた基本原則に従って実行されることは，とりわけ重要である。とりわけ，委任される行為の準備への平等な参加を確保するため，欧州議会及び理事会は，構成国の専門家と同時に全ての文書を受領すべきであり，かつ，構成国の専門家は，委任される行為の準備を取扱う欧州委員会の専門家グループの会合へのアクセスを自動的にもつべきである。

In order to further quantify and qualify the criteria for the designation of ICT third-party service providers as critical and to harmonise oversight fees, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission to supplement this Regulation by further specifying the systemic impact that a failure or operational outage of an ICT third-party service provider could have on the financial entities it provides ICT services to, the number of global systemically important institutions (G-SIIs), or other systemically important institutions (O-SIIs), that rely on the ICT third-party service provider in question, the number of ICT third-party service providers active on a given market,

[22] OJ L 123, 12.5.2016, p. 1.

the costs of migrating data and ICT workloads to other ICT third-party service providers, as well as the amount of the oversight fees and the way in which they are to be paid. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making[22]. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council should receive all documents at the same time as Member States' experts, and their experts should systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

(99) 法制上の技術標準は，この規則の中で定められた要件の一貫性のある整合化を確保すべきである。高度に特化された専門知識を具有する組織としての ESAs の役割の中で，ESAs は，欧州委員会に対して提出するため，基本方針上の選択肢を含まない法制上の技術標準案を策定すべきである。法制上の技術標準は，ICT リスクマネジメント，ICT と関連する大きなインシデントの報告，試験の分野において，及び，ICT サードパーティリスクの良好な監視のための鍵となる要件との関係において策定されるべきである。欧州委員会及び ESAs は，それらの技術標準及び要件が，当該金融機関の規模及び全体的なリスクプロファイル並びに当該金融機関のサービス，活動及び運営管理の性質，規模及び複雑性と比例的な態様で，全ての金融機関によって適用され得ることを確保すべきである。欧州委員会は，TFEU の第 290 条による委任される行為という方法により，かつ，規則(EU) No 1093/2010，規則(EU) No 1094/2010 及び規則(EU) No 1095/2010 の各第 10 条ないし第 14 条に従って，それらの法制上の技術標準を採択する権限を与えられるべきである。

Regulatory technical standards should ensure the consistent harmonisation of the requirements laid down in this Regulation. In their roles as bodies endowed with highly specialised expertise, the ESAs should develop draft regulatory technical standards which do not involve policy choices, for submission to the Commission. Regulatory technical standards should be developed in the areas of ICT risk management, major ICT-related incident reporting, testing, as well as in relation to key requirements for a sound monitoring of ICT third-party risk. The Commission and the ESAs should ensure that those standards and requirements can be applied by all financial entities in a manner that is proportionate to their size and overall risk profile, and the nature, scale and complexity of their services, activities and operations. The Commission should be empowered to adopt those regulatory technical standards by means of delegated acts pursuant to Article 290 TFEU and in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.

(100) ICT と関連する大きなインシデント，運営管理または決済の安全性と関連する大きなインシデントに関する報告の比較可能性を促進するため，及び，ICT サードパーティサービスプロバイダから提供される ICT サービスの利用に関する契約上の取決めに関して透明性を確保するため，ESAs は，ICT と関連する大きなインシデント及び運営管理または決済の安全性と関連する大きなインシデントを金融機関が報告するための標準化された雛型，書式及び手続，並びに，情報の登録簿のための標準化された雛型を定める実装技術標準案を策定すべきである。それらの技術標準を策定する際，ESAs は，金融機関の規模及び全体的なリスクプロファイル並びに当該金融機関のサービス，活動及び運営管理の性質，規模及び複雑性を考慮に入れるべきである。欧州委員会は，TFEU の第 291 条による実装行為という方法により，かつ，規則(EU) No 1093/2010，規則(EU) No 1094/2010 及び規

則(EU) No 1095/2010の各第 15 条に従って，それらの実装技術標準を採択する権限を与えられるべきである。

To facilitate the comparability of reports on major ICT-related incidents and major operational or security payment-related incidents, as well as to ensure transparency regarding contractual arrangements for the use of ICT services provided by ICT third-party service providers, the ESAs should develop draft implementing technical standards establishing standardised templates, forms and procedures for financial entities to report a major ICT-related incident and a major operational or security payment-related incident, as well as standardised templates for the register of information. When developing those standards, the ESAs should take into account the size and the overall risk profile of the financial entity, and the nature, scale and complexity of its services, activities and operations. The Commission should be empowered to adopt those implementing technical standards by means of implementing acts pursuant to Article 291 TFEU and in accordance with Article 15 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.

(101) 欧州議会及び理事会の規則(EC) No 1060/2009[23]，規則(EU) No 648/2012[24]，規則(EU) No 600/2014[25]及び規則 (EU) No 909/2014[26]の中で法制上の技術標準及び実装技術標準を基礎とする委任される行為及び実装行為により，別の要件が既に細目的に定められているので，ESAs に対し，それぞれ単独でまたは共同委員会を介して共同で，既存の ICT リスクマネジメントの規定を維持し及びアップデートする委任される行為及び実装行為の採択のために法制上の技術標準及び実装技術標準を欧州委員会に対して提出することを命ずるのが適切である。

Since further requirements have already been specified through delegated and implementing acts based on technical regulatory and implementing technical standards in Regulations (EC) No 1060/2009[(23)], (EU) No 648/2012[(24)], (EU) No 600/2014[(25)] and (EU) No 909/2014[(26)] of the European Parliament and of the Council, it is appropriate to mandate

---

[23] 信用格付け部局に関する欧州議会及び理事会の 2009 年 9 月 16 日の規則(EC) No 1060/2009 (OJ L 302, 17.11.2009, p. 1).
Regulation (EC) No 1060/2009 of the European Parliament and of the Council of 16 September 2009 on credit rating agencies (OJ L 302, 17.11.2009, p. 1).

[24] OTC デリバティブ，中央清算機関及び取引情報蓄積機関に関する欧州議会及び理事会の 2012 年 7 月 4 日の規則(EU) No 648/2012 (OJ L 201, 27.7.2012, p. 1).
Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC Derivatives, central counterparties and trade repositories (OJ L 201, 27.7.2012, p. 1).

[25] 金融商品市場に関する及び規則(EU) No 648/2012 を改正する欧州議会及び理事会の 2014 年 5 月 15 日の規則(EU) No 600/2014 (OJ L 173, 12.6.2014, p. 84).
Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/2012 (OJ L 173, 12.6.2014, p. 84).

[26] 欧州連合における証券清算の改善に関する及び証券集中保管機関に関する並びに指令 98/26/EC，指令 2014/65/EU 及び規則(EU) No 236/2012 を改正する欧州議会及び理事会の 2014 年 7 月 23 日の規則(EU) No 909/2014 (OJ L 257, 28.8.2014, p. 1).
Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012 (OJ L 257, 28.8.2014, p. 1).

the ESAs, either individually or jointly through the Joint Committee, to submit regulatory and implementing technical standards to the Commission for adoption of delegated and implementing acts carrying over and updating existing ICT risk management rules.

(102) この規則は，欧州議会及び理事会の指令(EU) 2022/2556[27]と共に，全面的な一貫性を確保するために，規則(EC) No 1060/2009，規則(EU) No 648/2012，規則(EU) No 600/2014 及び規則(EU) No 909/2014 並びに欧州議会及び理事会の規則(EU) 2016/1011[28]を含め，欧州連合の金融サービス法令の多重の規則及び指令を横断する ICT リスクマネジメント条項の統合を伴っているので，それらの規則は，適用可能な ICT リスク関連条項がこの規則の中で定められていることを明確化するために改正されるべきである。

Since this Regulation, together with Directive (EU) 2022/2556 of the European Parliament and of the Council[(27)], entails a consolidation of the ICT risk management provisions across multiple regulations and directives of the Union's financial services *acquis*, including Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014, and Regulation (EU) 2016/1011 of the European Parliament and of the Council[(28)], in order to ensure full consistency, those Regulations should be amended to clarify that the applicable ICT risk-related provisions are laid down in this Regulation.

(103) その結果として，規則(EC) No 1060/2009，規則(EU) No 648/2012，規則(EU) No 600/2014，規則(EU) No 909/2014 及び規則(EU) 2016/1011 の中で定められた権限に基づき，委任される行為及び実装行為の採択が命じられていたときは，現時点では当該各規則の一部であるデジタル運営管理上の回復力の側面を包摂する全ての条項をこの規則の中で引き継ぐという観点から，運営管理上のリスクと関連する適格な諸条項の適用範囲は，狭められるべきである。

Consequently, the scope of the relevant articles related to operational risk, upon which empowerments laid down in Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014, and (EU) 2016/1011 had mandated the adoption of delegated and implementing acts, should be narrowed down with a view to carry over into this Regulation all provisions covering the digital operational resilience aspects which today are part of those

---

[27] 金融部門のデジタル運営管理上の回復力と関連して指令 2009/65/EC，指令 2009/138/EC，指令 2011/61/EU，指令 2013/36/EU，指令 2014/59/EU，指令 2014/65/EU，指令(EU) 2015/2366 及び指令(EU) 2016/2341 を改正する欧州議会及び理事会の 2022 年 12 月 14 日の指令(EU) 2022/2556（この官報の 153 頁参照）.
Directive (EU) 2022/2556 of the European Parliament and of the Council of 14 December 2022 amending Directives 2009/65/EC, 2009/138/EC, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 and (EU) 2016/2341 as regards digital operational resilience for the financial sector (see page 153 of this Official Journal).

[28] 金融商品及び金融契約において指標として使用されまたは投資資金の効果を測定するために使用される指数に関する並びに指令 2008/48/EC，指令 2014/17/EU 及び規則(EU) No 596/2014 を改正する欧州議会及び理事会の 2016 年 6 月 8 日の規則(EU) 2016/1011 (OJ L 171, 29.6.2016, p. 1).
Regulation (EU) 2016/1011 of the European Parliament and of the Council of 8 June 2016 on indices used as benchmarks in financial instruments and financial contracts or to measure the performance of investment funds and amending Directives 2008/48/EC and 2014/17/EU and Regulation (EU) No 596/2014 (OJ L 171, 29.6.2016, p. 1).

Regulations.

(104) 決済システムの運営管理及び決済処理活動の提供を実現可能にする ICT インフラの利用と関係する潜在的にシステミックなサイバーリスクは，整合化されたデジタル回復力規定を介して，欧州連合レベルで適正に対処されるべきである。その点に関し，欧州委員会は，そのような見直しを指令(EU) 2015/2366 の下において予定されている包括的な見直しの結果と揃えつつ，この規則の適用の範囲の見直しの必要性の有無を迅速に評価すべきである。過去 10 年間にわたる多数の大規模攻撃は，決済システムがいかにサイバー脅威に晒されるようになってきたかを明らかにしている。決済サービスの連鎖のコアの場所にあり，かつ，金融システム全体との間の強力な相互の結びつきを示して，決済システム及び決済処理活動は，欧州連合の金融市場の稼動によって不可欠の重要性を獲得した。そのようなシステムに対するサイバー攻撃は，決済の促進のような鍵となる経済機能に対する直接の打撃と関連する経済プロセスに対する間接的な影響をもつ運営管理事業上の深刻な混乱を発生させ得る。整合化された法体制及び決済システム及び処理法主体の運営者の監督が欧州連合レベルで設けられるまでの間，構成国は，それらの構成国自身の国家主権の下において監督を受ける決済システム及び処理法主体の運営者に対して諸規定を適用する際，類似の市場実務を適用するため，この規則によって定められたデジタル運営管理上の回復力要件から着想を得ることができる。

The potential systemic cyber risk associated with the use of ICT infrastructures that enable the operation of payment systems and the provision of payment processing activities should be duly addressed at Union level through harmonised digital resilience rules. To that effect, the Commission should swiftly assess the need for reviewing the scope of this Regulation while aligning such review with the outcome of the comprehensive review envisaged under Directive (EU) 2015/2366. Numerous large-scale attacks over the past decade demonstrate how payment systems have become exposed to cyber threats. Placed at the core of the payment services chain and showing strong interconnections with the overall financial system, payment systems and payment processing activities acquired a critical significance for the functioning of the Union financial markets. Cyber-attacks on such systems can cause severe operational business disruptions with direct repercussions on key economic functions, such as the facilitation of payments, and indirect effects on related economic processes. Until a harmonised regime and the supervision of operators of payment systems and processing entities are put in place at Union level, Member States may, with a view to applying similar market practices, draw inspiration from the digital operational resilience requirements laid down by this Regulation, when applying rules to operators of payment systems and processing entities supervised under their own jurisdictions.

(105) この規則の目的，すなわち，法制の下にある金融法主体の高度のデジタル運営管理上の回復力を達成することは，欧州連合法及び国内法にある多種多様な異なる諸規定の整合化を要することから，構成国によっては十分に達成さえ得ず，その規模及び影響のゆえに欧州連合レベルでより良く達成され得るので，欧州連合は，欧州連合条約の第 5 条に定める補完性の原則に従って措置を採択できる。同条に定める比例性の原則に従い，この規則は，その目的を達成するために必要なところを越えることがない。

Since the objective of this Regulation, namely to achieve a high level of digital operational resilience for regulated

financial entities, cannot be sufficiently achieved by the Member States because it requires harmonisation of various different rules in Union and national law, but can rather, by reason of its scale and effects, be better achieved at Union level, the Union may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

(106) 欧州データ保護監督官は，欧州議会及び理事会の規則(EU) 2018/1725[29]の第 42 条第 1 項に従って意見聴取を受け，2021 年 5 月 10 日に意見[30]を伝達した，

The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council[29] and delivered an opinion on 10 May 2021[30],

HAVE ADOPTED THIS REGULATION:

以上のとおりであるので，この規則を採択する:

[29] 欧州連合の機関，組織，事務局及び部局による個人データの処理と関連する自然人の保護及びそのデータの支障のない移動に関する並びに規則(EC) No 45/2001 及び決定 No 1247/2002/EC を廃止する欧州議会及び理事会の 2018 年 10 月 23 日の規則(EU) 2018/1725 (OJ L 295, 21.11.2018, p. 39).
Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

[30] OJ C 229, 15.6.2021, p. 16.

第 I 章 総則的な条項
CHAPTER I **General provisions**

第 1 条 対象事項
Article 1 **Subject matter**

1. 高度に共通のレベルのデジタル運営管理上の回復力を達成するため，この規則は，金融機関の業務プロセスを支えるネットワーク及び情報システムの安全性に関する統一的な要件を以下のとおり定める：

In order to achieve a high common level of digital operational resilience, this Regulation lays down uniform requirements concerning the security of network and information systems supporting the business processes of financial entities as follows:

(a) 以下の事項との関係において金融機関に対して適用可能な要件：

requirements applicable to financial entities in relation to:

(i) 情報通信技術（ICT）のリスクマネジメント；

information and communication technology (ICT) risk management;

(ii) 職務権限のある当局に対する，ICT と関連する大きなインシデントの報告及び大きなサイバー脅威の任意の通知；

reporting of major ICT-related incidents and notifying, on a voluntary basis, significant cyber threats to the competent authorities;

(iii) 第 2 条第 1 項(a)ないし(d)に示す金融機関による職務権限のある当局に対する運営管理または決済の安全性と関連する大きなインシデントの報告；

reporting of major operational or security payment-related incidents to the competent authorities by financial entities referred to in Article 2(1), points (a) to (d);

(iv) デジタル運営管理上の回復力の試験；

digital operational resilience testing;

(v) サイバー脅威及び脆弱性との関係における情報と知識の共有；

information and intelligence sharing in relation to cyber threats and vulnerabilities;

(vi) ICT サードパーティリスクの良好な管理のための方策；

measures for the sound management of ICT third-party risk;

(b) ICT サードパーティサービスプロバイダと金融機関との間で締結された契約上の取決めとの関係における要件；

requirements in relation to the contractual arrangements concluded between ICT third-party service providers and financial entities;

(c) 金融機関に対してサービスを提供する際における不可欠な ICT サードパーティサービスプロバイダの監督枠組みの設置及び行動に関する規定；

rules for the establishment and conduct of the Oversight Framework for critical ICT third-party service providers when providing services to financial entities;

(d) この規則によって包摂される全ての事項との関係において，職務権限のある当局間の協力に関する規定並びに職務権限のある当局による監督及び執行に関する規定。

rules on cooperation among competent authorities, and rules on supervision and enforcement by competent authorities in relation to all matters covered by this Regulation.

2. 指令(EU) 2022/2555 の第 3 条を国内法化する国内規定により必須法主体または重要法主体として識別された金融機関との関係において，この規則は，同指令の第 4 条の目的のために欧州連合の部門別の法行為として判断される。

In relation to financial entities identified as essential or important entities pursuant to national rules transposing Article 3 of Directive (EU) 2022/2555, this Regulation shall be considered a sector-specific Union legal act for the purposes of Article 4 of that Directive.

3. この規則は，欧州連合法に従った公共の保安，国防及び国家安全保障と関係する国家の必須の機能と関連する構成国の職責を妨げない。

This Regulation is without prejudice to the responsibility of Member States' regarding essential State functions concerning public security, defence and national security in accordance with Union law.

第 2 条 適用範囲

Article 2 **Scope**

1. 第 3 項及び第 4 項を妨げることなく, この規則は, 以下の法主体に対して適用される:

Without prejudice to paragraphs 3 and 4, this Regulation applies to the following entities:

(a) 与信機関;

credit institutions;

(b) 指令(EU) 2015/2366 により適用除外される決済機関を含め, 決済機関;

payment institutions, including payment institutions exempted pursuant to Directive (EU) 2015/2366;

(c) 口座情報サービスプロバイダ;

account information service providers;

(d) 指令 2009/110/EC により適用除外される電子マネー機関を含め, 電子マネー機関;

electronic money institutions, including electronic money institutions exempted pursuant to Directive 2009/110/EC;

(e) 投資企業;

investment firms;

(f) 暗号資産の市場に関する並びに規則(EU) No 1093/2010, 規則(EU) No 1095/2010, 指令 2013/36/EU 及び指令(EU) 2019/1937 を改正する欧州議会及び理事会の規則(「暗号資産の市場に関する規則」)の下において認可を受けた暗号資産サービスプロバイダ及び資産参照トークンの発行者;

crypto-asset service providers as authorised under a Regulation of the European Parliament and of the Council on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 ('the Regulation on markets in crypto-assets') and issuers of asset-referenced tokens

(g) 証券集中保管機関;

central securities depositories;

(h) 中央清算機関;

central counterparties;

(i) 取引場所;

trading venues;

(j) 取引情報蓄積機関;

trade repositories;

(k) オルタナティブ投資ファンド管理者;

managers of alternative investment funds;

(l) 資産管理会社;

management companies;

(m) データ報告サービスプロバイダ;

data reporting service providers;

(n) 保険事業者及び再保険事業者;

insurance and reinsurance undertakings;

(o) 保険仲介事業者，再保険仲介事業者及び補助的な保険仲介事業者;

insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries;

(p) 職域年金給付機関;

institutions for occupational retirement provision;

(q) 与信格付機関;

credit rating agencies;

(r) 不可欠指標の管理者；

administrators of critical benchmarks;

(s) クラウドファンディングサービスプロバイダ；

crowdfunding service providers;

(t) 証券化情報蓄積機関；

securitisation repositories;

(u) ICT サードパーティサービスプロバイダ。

ICT third-party service providers.

2. この規則の目的のために，第 1 項(a)ないし(t)に示す法主体は，「金融機関」として集合的に参照される。

For the purposes of this Regulation, entities referred to in paragraph 1, points (a) to (t), shall collectively be referred to as 'financial entities'.

3. この規則は，以下の者に対しては適用されない：

This Regulation does not apply to:

(a) 指令 2011/61/EU の第 3 条第 2 項に示すオルタナティブ投資ファンド管理者；

managers of alternative investment funds as referred to in Article 3(2) of Directive 2011/61/EU;

(b) 指令 2009/138/EC の第 4 条に示す保険事業者及び再保険事業者；

insurance and reinsurance undertakings as referred to in Article 4 of Directive 2009/138/EC;

(c) 合計で 15 名を超えない加入者を集めた年金制度を運用している職域退職給付機関；

institutions for occupational retirement provision which operate pension schemes which together do not have more than 15 members in total;

(d) 指令 2014/65/EU の第 2 条及び第 3 条により適用除外される自然人または法人；

natural or legal persons exempted pursuant to Articles 2 and 3 of Directive 2014/65/EU;

(e) マイクロ企業または小企業もしくは中規模企業である保険仲介事業者，再保険仲介事業者及び補助的な保険仲介事業者；

insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries which are microenterprises or small or medium-sized enterprises;

(f) 指令 2013/36/EU の第 2 条第 5 項第 3 号に示す郵便振替取扱機関。

post office giro institutions as referred to in Article 2(5), point (3), of Directive 2013/36/EU.

4. 構成国は，構成国それぞれの領土内に所在している指令 2013/36/EU の第 2 条第 5 項第 4 号ないし第 23 号に示す法主体を，この規則の適用範囲から除外できる。構成国がそのような選択肢を用いるときは，その構成国は，欧州委員会に対し，その利用及びその後のその利用の変更を連絡する。欧州委員会は，Web サイト上においてまたは他の容易にアクセス可能な手段により，その情報を公表する。

Member States may exclude from the scope of this Regulation entities referred to in Article 2(5), points (4) to (23), of Directive 2013/36/EU that are located within their respective territories. Where a Member State makes use of such option, it shall inform the Commission thereof as well as of any subsequent changes thereto. The Commission shall make that information publicly available on its website or other easily accessible means.

第 3 条 定義

Article 3 **Definitions**

この規則の目的のために，以下の定義が適用される：

For the purposes of this Regulation, the following definitions shall apply:

(1) 「デジタル運営管理上の回復力」とは，直接にまたは ICT サードパーティサービスプロバイダから提供されるサービスの利用を介して間接に，金融機関が使用するネットワーク及び情報システム及び金融サービスの継続的な提供及びその品質を支えるネットワーク及び情報システムの安全性に対処するために必要な，混乱中の場合を含め，全般に及ぶ ICT 関連の実現能力を確保することにより，その金融機関の運営管理上の完全性及び信頼性を構築し，保証し及び見直すための金融機関の能力のことを意味し；

‘digital operational resilience’ means the ability of a financial entity to build, assure and review its operational integrity and reliability by ensuring, either directly or indirectly through the use of services provided by ICT third-party service providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity uses, and which support the continued provision of financial services and their quality, including throughout disruptions;

(2) 「ネットワーク及び情報システム」とは，指令(EU) 2022/2555 の第 6 条第 1 号に定義するネットワーク及び情報システムのことを意味し；

‘network and information system’ means a network and information system as defined in Article 6, point 1, of Directive (EU) 2022/2555;

(3) 「旧式の ICT システム」とは，ライフサイクルの終点（寿命）に達しており，技術的な理由もしくは商業上の理由によりアップグレードもしくは補修に適しておらず，または，当該システムの供給者からもしくは ICT サードパーティサービスプロバイダからサポートを受けなくなっているけれども，なお利用されておりかつ金融機関の機能を支える ICT システムのことを意味し；

‘legacy ICT system’ means an ICT system that has reached the end of its lifecycle (end-of-life), that is not suitable for upgrades or fixes, for technological or commercial reasons, or is no longer supported by its supplier or by an ICT third-party service provider, but that is still in use and supports the functions of the financial entity;

(4) 「ネットワーク及び情報システムの安全性」とは，指令(EU) 2022/2555 の第 6 条第 2 号に定義するネットワーク及び情報システムの安全性のことを意味し；

‘security of network and information systems’ means security of network and information systems as defined in Article 6, point 2, of Directive (EU) 2022/2555;

(5) 「ICT リスク」とは，ネットワーク及び情報システムの利用との関係において合理的に特定可能な状況であって，それが現実化すると，デジタルまたは物理的な環境において負の影響をつくり出すことによって，ネットワーク及び情報システムの安全性，技術的に依存するツールもしくはプロセスの安全性，運用及び処理の安全性またはサービス提供の安全性を混乱させ得るもののことを意味し；

‘ICT risk’ means any reasonably identifiable circumstance in relation to the use of network and information systems which, if materialised, may compromise the security of the network and information systems, of any technology dependent tool or process, of operations and processes, or of the provision of services by producing adverse effects in the digital or physical environment;

(6) 「情報資産」とは，有形または無形の，防護に値する情報の集合のことを意味し；

‘information asset’ means a collection of information, either tangible or intangible, that is worth protecting;

(7) 「ICT 資産」とは，金融機関によって用いられるネットワーク及び情報システム内のソフトウェア資産またはハードウェア資産のことを意味し；

‘ICT asset’ means a software or hardware asset in the network and information systems used by the financial entity;

(8) 「ICT と関連するインシデント」とは，ネットワーク及び情報システムの安全性を混乱させ，かつ，データの可用性，真正性，完全性もしくは機密性に対するまたは金融機関から提供されるサービスに対する負の影響をもつ，当該金融機関によって計画されていない単一の出来事または一連の牽連する出来事のことを意味し；

‘ICT-related incident’ means a single event or a series of linked events unplanned by the financial entity that compromises the security of the network and information systems, and have an adverse impact on the availability, authenticity, integrity or confidentiality of data, or on the services provided by the financial entity;

(9) 「運営管理または決済の安全性と関連するインシデント」とは，ICT と関連するインシデントであるか否かを問わず，決済と関連するデータの可用性，真正性，完全性もしくは機密性に対するまたは金融機関から提供される決済と関連するサービスに対する負の影響をもつ，第 2 条第 1 項(a)ないし(d)に示す金融機関によって計画されていない単一の出来事または一連の牽連する出来事のことを意味し；

‘operational or security payment-related incident’ means a single event or a series of linked events unplanned by the financial entities referred to in Article 2(1), points (a) to (d), whether ICT-related or not, that has an adverse impact on the availability, authenticity, integrity or confidentiality of payment-related data, or on the payment-related services provided by the financial entity;

(10) 「ICT と関連する大きなインシデント」とは，金融機関の不可欠な機能または重要な機能を支えるネットワーク及び情報システムに対する高度の負の影響をもつ ICT と関連するインシデントのことを意味し；

‘major ICT-related incident’ means an ICT-related incident that has a high adverse impact on the network and information systems that support critical or important functions of the financial entity;

(11) 「運営管理または決済の安全性と関連する大きなインシデント」とは，提供される決済と関連するサービスに対する高度の負の影響をもつ運営管理または決済の安全性と関連するインシデントのことを意味し；

‘major operational or security payment-related incident’ means an operational or security payment-related

incident that has a high adverse impact on the payment-related services provided;

(12) 「サイバー脅威」とは，規則(EU) 2019/881 の第 2 条第 8 号に定義する「サイバー脅威」のことを意味し；

‘cyber threat’ means ‘cyber threat’ as defined in Article 2, point (8), of Regulation (EU) 2019/881;

(13) 「大きなサイバー脅威」とは，そのサイバー脅威の技術上の特性が，ICT と関連する大きなインシデントまたは運営管理もしくは決済の安全性と関連する大きなインシデントを帰結する潜在性をもち得るということを示しているサイバー脅威のことを意味し；

‘significant cyber threat’ means a cyber threat the technical characteristics of which indicate that it could have the potential to result in a major ICT-related incident or a major operational or security payment-related incident;

(14) 「サイバー攻撃」とは，資産を破壊し，危険に晒し，改変し，利用不能にし，盗み，または，資産への無権限のアクセスを獲得しもしくは資産の無権限の利用を行うために，脅威の行為者によって行われた試みにより生じた ICT と関連する悪意あるインシデントのことを意味し；

‘cyber-attack’ means a malicious ICT-related incident caused by means of an attempt perpetrated by any threat actor to destroy, expose, alter, disable, steal or gain unauthorised access to, or make unauthorised use of, an asset;

(15) 「脅威情報」とは，意思決定のための必要な文脈を提供するために，並びに，サイバー攻撃の技術上の詳細，その攻撃に責任を負う者及び当該の者の*手口*と動機を含め，ICT と関連するインシデントまたはサイバー脅威の影響を緩和するための適格かつ十分な理解を可能にするために，要約され，変形され，分析され，解釈されまたは充実化された情報のことを意味し；

‘threat intelligence’ means information that has been aggregated, transformed, analysed, interpreted or enriched to provide the necessary context for decision-making and to enable relevant and sufficient understanding in order to mitigate the impact of an ICT-related incident or of a cyber threat, including the technical details of a cyber-attack, those responsible for the attack and their *modus operandi* and motivations;

(16) 「脆弱性」とは，資産，システム，プロセスまたは管理の，悪用され得る弱点，被感染性または欠点のことを意味し；

‘vulnerability’ means a weakness, susceptibility or flaw of an asset, system, process or control that can be exploited;

(17) 「脅威ベースのペネトレーション試験（TLPT）」とは，真のサイバー脅威を呈していると認識されている現実世界の脅威行為者の戦術，技法及び手順を模倣する枠組みであって，金融機関の不可欠なライブプロダクションシステムの，管理され，個別対応の，脅威情報主導型（レッド

チーム）の試験を提供するもののことを意味し；

‘threat-led penetration testing (TLPT)’ means a framework that mimics the tactics, techniques and procedures of real-life threat actors perceived as posing a genuine cyber threat, that delivers a controlled, bespoke, intelligence-led (red team) test of the financial entity’s critical live production systems;

(18) 「ICT サードパーティリスク」とは，アウトソーシングの取決めを介する場合を含め，ICT サードパーティサービスプロバイダからまたはその下請契約者から提供される ICT サービスの金融機関による利用との関係において金融機関に生じ得る ICT リスクのことを意味し；

‘ICT third-party risk’ means an ICT risk that may arise for a financial entity in relation to its use of ICT services provided by ICT third-party service providers or by subcontractors of the latter, including through outsourcing arrangements;

(19) 「ICT サードパーティサービスプロバイダ」とは，ICT サービスを提供している事業者のことを意味し；

‘ICT third-party service provider’ means an undertaking providing ICT services;

(20) 「ICT グループ内サービスプロバイダ」とは，金融グループの一部となっており，かつ，主として，当該事業者の親事業者，子事業者，支店またはそれら以外の共通の保有もしくは支配の下にある法主体を含め，同一のグループ内の金融機関に対してまたは同一の組織的な防護のスキームに属する金融機関に対して ICT サービスを提供する事業者のことを意味し；

‘ICT intra-group service provider’ means an undertaking that is part of a financial group and that provides predominantly ICT services to financial entities within the same group or to financial entities belonging to the same institutional protection scheme, including to their parent undertakings, subsidiaries, branches or other entities that are under common ownership or control;

(21) 「ICT サービス」とは，ハードウェアの提供者からのソフトウェアまたはファームウェアのアップデートを介する技術サポートの提供を含んでいるハードウェアアズアサービス及びハードウェアサービスを含め，在来型のアナログ電話サービスを除き，1 または複数の内部利用者または外部利用者に対して ICT システムを介して継続的に提供されるデジタルサービス及びデータサービスのことを意味し；

‘ICT services’ means digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis, including hardware as a service and hardware services which includes the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone services;

(22) 「不可欠な機能または重要な機能」とは，当該機能の破壊が，金融機関の金融上の遂行能力，その金融機関のサービス及び活動の良好性もしくは継続性を実質的に阻害するような機能，または，当該機能の継続不能，不完全な遂行もしくは不遂行が，その金融機関の認可の条件及び義務もしくはそれ以外の適用可能な金融サービス法の下にある金融機関の義務の金融機関による遵守の継続を実質的に阻害するような機能のことを意味し；

‘critical or important function’ means a function, the disruption of which would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law;

(23) 「不可欠な ICT サードパーティサービスプロバイダ」とは，第 31 条に従って不可欠として指定された ICT サードパーティサービスプロバイダのことを意味し；

‘critical ICT third-party service provider’ means an ICT third-party service provider designated as critical in accordance with Article 31;

(24) 「第三国内に拠点をもつ ICT サードパーティサービスプロバイダ」とは，第三国内に拠点をもつ法人であり，かつ，金融機関との間で ICT サービスの提供に関する契約上の取決めを締結した ICT サードパーティサービスプロバイダのことを意味し；

‘ICT third-party service provider established in a third country’ means an ICT third-party service provider that is a legal person established in a third-country and that has entered into a contractual arrangement with a financial entity for the provision of ICT services;

(25) 「子事業者」とは，指令 2013/34/EU の第 2 条第 10 号及び第 22 条の意味における子事業者のことを意味し；

‘subsidiary’ means a subsidiary undertaking within the meaning of Article 2, point (10), and Article 22 of Directive 2013/34/EU;

(26) 「グループ」とは，指令 2013/34/EU の第 2 条第 11 号に定義するグループのことを意味し；

‘group’ means a group as defined in Article 2, point (11), of Directive 2013/34/EU;

(27) 「親事業者」とは，指令 2013/34/EU の第 2 条第 9 号及び第 22 条の意味における親事業者のことを意味し；

‘parent undertaking’ means a parent undertaking within the meaning of Article 2, point (9), and Article 22 of

Directive 2013/34/EU;

(28) 「第三国内に拠点をもつ ICT 下請契約者」とは，第三国内に拠点をもつ法人であり，かつ，ICT サードパーティサービスプロバイダとの間または第三国内に拠点をもつ ICT サードパーティサービスプロバイダとの間で契約上の取決めを締結した ICT 下請契約者のことを意味し；

‘ICT subcontractor established in a third country’ means an ICT subcontractor that is a legal person established in a third-country and that has entered into a contractual arrangement either with an ICT third-party service provider, or with an ICT third-party service provider established in a third country;

(29) 「ICT 集中化リスク」とは，個々または多重の関連する ICT サードパーティサービスプロバイダに対するそのようなプロバイダへのある程度の依存性をつくり出すエクスポージャーであって，それによって，そのようなプロバイダの不可用性，不履行もしくはそれ以外のタイプの欠点が，不可欠な機能もしくは重要な機能を供給する金融機関の能力を潜在的な危険に晒し得るもの，または，巨額の損失を含め，それ以外のタイプの不の影響を金融機関に対して及ぼすことを生じさせ得るもの，または，欧州連合全体の金融の安定性を危険に晒し得るもののことを意味し；

‘ICT concentration risk’ means an exposure to individual or multiple related critical ICT third-party service providers creating a degree of dependency on such providers so that the unavailability, failure or other type of shortfall of such provider may potentially endanger the ability of a financial entity to deliver critical or important functions, or cause it to suffer other types of adverse effects, including large losses, or endanger the financial stability of the Union as a whole;

(30) 「経営陣」とは，指令 2014/65/EU の第 4 条第 1 項第 36 号，指令 2013/36/EU の第 3 条第 1 項第 7 号，欧州議会及び理事会の指令 2009/65/EC[31]の第 2 条第 1 項(s)，規則(EU) No 909/2014 の第 2 条第 1 項第 45 号，規則(EU) 2016/1011 の第 3 条第 1 項第 20 号並びに暗号資産の市場に関する規則の適格な条項に定義する経営陣，または，それらと均等の者であって，適格な欧州連合法もしくは国内法に従って当該法主体を実効的に運営している者もしくは鍵となる権能をもつ者のことを意味し；

‘management body’ means a management body as defined in Article 4(1), point (36), of Directive 2014/65/EU, Article 3(1), point (7), of Directive 2013/36/EU, Article 2(1), point (s), of Directive 2009/65/EC of the European Parliament and of the Council[31], Article 2(1), point (45), of Regulation (EU) No 909/2014, Article 3(1), point

[31] 譲渡可能証券の投資信託事業者と関連する法律，規則及び行政上の条項の調整に関する欧州議会及び理事会の 2009 年 7 月 13 日の指令 2009/65/EC (UCITS) (OJ L 302, 17.11.2009, p. 32).
Directive 2009/65/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities (UCITS) (OJ L 302, 17.11.2009, p. 32).

(20), of Regulation (EU) 2016/1011, and in the relevant provision of the Regulation on markets in crypto-assets, or the equivalent persons who effectively run the entity or have key functions in accordance with relevant Union or national law;

(31) 「与信機関」とは，欧州議会及び理事会の規則(EU) No 575/2013[32]の第 4 条第 1 項第 1 号に定義する与信機関のことを意味し；

'credit institution' means a credit institution as defined in Article 4(1), point (1), of Regulation (EU) No 575/2013 of the European Parliament and of the Council[(32)];

(32) 「指令 2013/36/EU により適用除外される機関」とは，指令 2013/36/EU の第 2 条第 5 項第 4 号ないし第 23 号に示す法主体のことを意味し；

'institution exempted pursuant to Directive 2013/36/EU' means an entity as referred to in Article 2(5), points (4) to (23), of Directive 2013/36/EU;

(33) 「投資企業」とは，指令 2014/65/EU の第 4 条第 1 項第 1 号に定義する投資企業のことを意味し；

'investment firm' means an investment firm as defined in Article 4(1), point (1), of Directive 2014/65/EU;

(34) 「小規模で相互結合のない投資企業」とは，欧州議会及び理事会の規則(EU) 2019/2033[33]の第 12 条第 1 項の中で定められた条件に適合する投資企業のことを意味し；

'small and non-interconnected investment firm' means an investment firm that meets the conditions laid out in Article 12(1) of Regulation (EU) 2019/2033 of the European Parliament and of the Council[(33)];

(35) 「決済機関」とは，指令(EU) 2015/2366 の第 4 条第 4 号に定義する決済機関のことを意味し；

'payment institution' means a payment institution as defined in Article 4, point (4), of Directive (EU) 2015/2366;

---

[32] 与信機関の健全性要件に関する及び規則(EU) No 648/2012 を改正する欧州議会及び理事会の 2013 年 6 月 26 日の規則(EU) No 575/2013 (OJ L 176, 27.6.2013, p. 1).
Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1).

[33] 投資企業の健全性要件に関する並びに規則(EU) No 1093/2010, 規則(EU) No 575/2013, 規則(EU) No 600/2014 及び規則 (EU) No 806/2014 を改正する欧州議会及び理事会の 2019 年 11 月 27 日の規則(EU) 2019/2033 (OJ L 314, 5.12.2019, p. 1).
Regulation (EU) 2019/2033 of the European Parliament and of the Council of 27 November 2019 on the prudential requirements of investment firms and amending Regulations (EU) No 1093/2010, (EU) No 575/2013, (EU) No 600/2014 and (EU) No 806/2014 (OJ L 314, 5.12.2019, p. 1).

(36) 「指令(EU) 2015/2366 により適用除外される決済機関」とは，指令(EU) 2015/2366 の第 32 条第 1 項により適用除外される決済機関のことを意味し；

‘payment institution exempted pursuant to Directive (EU) 2015/2366’ means a payment institution exempted pursuant to Article 32(1) of Directive (EU) 2015/2366;

(37) 「口座情報サービスプロバイダ」とは，指令(EU) 2015/2366 の第 33 条第 1 項に示す口座情報サービスプロバイダのことを意味し；

‘account information service provider’ means an account information service provider as referred to in Article 33(1) of Directive (EU) 2015/2366;

(38) 「電子マネー機関」とは，欧州議会及び理事会の指令 2009/110/EC の第 2 条第 1 号に定義する電子マネー機関のことを意味し；

‘electronic money institution’ means an electronic money institution as defined in Article 2, point (1), of Directive 2009/110/EC of the European Parliament and of the Council;

(39) 「指令 2009/110/EC により適用除外される電子マネー機関」とは，指令 2009/110/EC の第 9 条第 1 項に示す免除から受益している電子マネー機関のことを意味し；

‘electronic money institution exempted pursuant to Directive 2009/110/EC’ means an electronic money institution benefitting from a waiver as referred to in Article 9(1) of Directive 2009/110/EC;

(40) 「中央清算機関」とは，規則(EU) No 648/2012 の第 2 条第 1 号に定義する中央清算機関のことを意味し；

‘central counterparty’ means a central counterparty as defined in Article 2, point (1), of Regulation (EU) No 648/2012;

(41) 「取引情報蓄積機関」とは，規則(EU) No 648/2012 の第 2 条第 2 号に定義する取引情報蓄積機関のことを意味し；

‘trade repository’ means a trade repository as defined in Article 2, point (2), of Regulation (EU) No 648/2012;

(42) 「証券集中保管機関」とは，規則(EU) No 909/2014 の第 2 条第 1 項第 1 号に定義する証券集中保管機関のことを意味し；

‘central securities depository’ means a central securities depository as defined in Article 2(1), point (1), of Regulation (EU) No 909/2014;

(43) 「取引場所」とは，指令 2014/65/EU の第 4 条第 1 項第 24 号に定義する取引場所のことを意味し；

‘trading venue’ means a trading venue as defined in Article 4(1), point (24), of Directive 2014/65/EU;

(44) 「オルタナティブ投資ファンド管理者」とは，指令 2011/61/EU の第 4 条第 1 項(b)に定義するオルタナティブ投資ファンド管理者のことを意味し；

‘manager of alternative investment funds’ means a manager of alternative investment funds as defined in Article 4(1), point (b), of Directive 2011/61/EU;

(45) 「資産管理会社」とは，指令 2009/65/EC の第 2 条第 1 項(b)に定義する資産管理会社のことを意味し；

‘management company’ means a management company as defined in Article 2(1), point (b), of Directive 2009/65/EC;

(46) 「データ報告サービスプロバイダ」とは，規則(EU) No 600/2014 の第 2 条第 1 項第 34 号ないし第 36 号に示す，同規則の意味におけるデータ報告サービスプロバイダのことを意味し；

‘data reporting service provider’ means a data reporting service provider within the meaning of Regulation (EU) No 600/2014, as referred to in Article 2(1), points (34) to (36) thereof;

(47) 「保険事業者」とは，指令 2009/138/EC の第 13 条第 1 号に定義する保険事業者のことを意味し；

‘insurance undertaking’ means an insurance undertaking as defined in Article 13, point (1), of Directive 2009/138/EC;

(48) 「再保険事業者」とは，指令 2009/138/EC の第 13 条第 4 号に定義する再保険事業者のことを意味し；

‘reinsurance undertaking’ means a reinsurance undertaking as defined in Article 13, point (4), of Directive 2009/138/EC;

(49) 「保険仲介事業者」とは，欧州議会及び理事会の指令(EU) 2016/97[34]の第 2 条第 1 項第 3 号に定義する保険仲介事業者のことを意味し；

[34] 保険の流通に関する欧州議会及び理事会の 2016 年 1 月 20 日の指令(EU) 2016/97 (OJ L 26, 2.2.2016, p. 19).
Directive (EU) 2016/97 of the European Parliament and of the Council of 20 January 2016 on insurance distribution (OJ L 26,

‘insurance intermediary’ means an insurance intermediary as defined in Article 2(1), point (3), of Directive (EU) 2016/97 of the European Parliament and of the Council[34];

(50) 「補助的な保険仲介事業者」とは，指令(EU) 2016/97 の第 2 条第 1 項第 4 号に定義する補助的な保険仲介事業者のことを意味し；

‘ancillary insurance intermediary’ means an ancillary insurance intermediary as defined in Article 2(1), point (4), of Directive (EU) 2016/97;

(51) 「再保険仲介事業者」とは，指令(EU) 2016/97 の第 2 条第 1 項第 5 号に定義する再保険仲介事業者のことを意味し；

‘reinsurance intermediary’ means a reinsurance intermediary as defined in Article 2(1), point (5), of Directive (EU) 2016/97;

(52) 「職域退職給付機関」とは，指令(EU) 2016/2341 の第 6 条第 1 号に定義する職域退職給付機関のことを意味し；

‘institution for occupational retirement provision’ means an institution for occupational retirement provision as defined in Article 6, point (1), of Directive (EU) 2016/2341;

(53) 「小規模な職域退職給付機関」とは，合計で 100 名を超えない加入者を集めた年金制度を運用している職域退職給付機関のことを意味し；

‘small institution for occupational retirement provision’ means an institution for occupational retirement provision which operates pension schemes which together have less than 100 members in total;

(54) 「与信格付機関」とは，規則(EC) No 1060/2009 の第 3 条第 1 項(b)に定義する与信格付機関のことを意味し；

‘credit rating agency’ means a credit rating agency as defined in Article 3(1), point (b), of Regulation (EC) No 1060/2009;

(55) 「暗号資産サービスプロバイダ」とは，暗号資産の市場に関する規則の適格な条項に定義する暗号資産サービスプロバイダのことを意味し；

‘crypto-asset service provider’ means a crypto-asset service provider as defined in the relevant provision of the Regulation on markets in crypto-assets;

2.2.2016, p. 19).

(56) 「資産参照トークンの発行者」とは，暗号資産の市場に関する規則の適格な条項に定義する資産参照トークンの発行者のことを意味し；

‘issuer of asset-referenced tokens’ means an issuer of asset-referenced tokens as defined in the relevant provision of the Regulation on markets in crypto-assets;

(57) 「不可欠指標の管理者」とは，規則(EU) 2016/1011 の第 3 条第 1 項第 25 号に定義する「不可欠指標」の管理者のことを意味し；

‘administrator of critical benchmarks’ means an administrator of ‘critical benchmarks’ as defined in Article 3(1), point (25), of Regulation (EU) 2016/1011;

(58) 「クラウドファンディングサービスプロバイダ」とは，欧州議会及び理事会の規則(EU) 2020/1503[35] の第 2 条第 1 項(e)に定義するクラウドファンディングサービスプロバイダのことを意味し；

‘crowdfunding service provider’ means a crowdfunding service provider as defined in Article 2(1), point (e), of Regulation (EU) 2020/1503 of the European Parliament and of the Council[(35)];

(59) 「証券化情報蓄積機関」とは，欧州議会及び理事会の規則(EU) 2017/2402[36]の第 2 条第 23 号に定義する証券化情報蓄積機関のことを意味し；

‘securitisation repository’ means a securitisation repository as defined in Article 2, point (23), of Regulation (EU) 2017/2402 of the European Parliament and of the Council[(36)];

(60) 「マイクロ企業」とは，取引場所，中央清算機関，取引情報蓄積機関または証券集中保管機関以外の金融機関であって，10 名未満の者を雇用し，かつ，200 万ユーロ未満の年次総売上及びまたは年次貸借対照表合計をもつ金融機関のことを意味し；

---

[35] 企業向けの欧州クラウドファンディングサービスプロバイダに関する並びに規則(EU) 2017/1129 及び指令(EU) 2019/1937 を改正する欧州議会及び理事会の 2020 年 10 月 7 日の規則(EU) 2020/1503 (OJ L 347, 20.10.2020, p. 1).
Regulation (EU) 2020/1503 of the European Parliament and of the Council of 7 October 2020 on European crowdfunding service providers for business, and amending Regulation (EU) 2017/1129 and Directive (EU) 2019/1937 (OJ L 347, 20.10.2020, p. 1).

[36] 証券化のための一般的な枠組みを定め及び簡素化され，透明性がありかつ標準化された証券化のための特別の枠組みを創設する並びに指令 2009/65/EC，指令 2009/138/EC 及び指令 2011/61/EU 並びに規則(EC) No 1060/2009 及び規則(EU) No 648/2012 を改正する欧州議会及び理事会の 2017 年 12 月 12 日の規則(EU) 2017/2402 (OJ L 347, 28.12.2017, p. 35).
Regulation (EU) 2017/2402 of the European Parliament and of the Council of 12 December 2017 laying down a general framework for securitisation and creating a specific framework for simple, transparent and standardised securitisation, and amending Directives 2009/65/EC, 2009/138/EC and 2011/61/EU and Regulations (EC) No 1060/2009 and (EU) No 648/2012 (OJ L 347, 28.12.2017, p. 35).

‘microenterprise’ means a financial entity, other than a trading venue, a central counterparty, a trade repository or a central securities depository, which employs fewer than 10 persons and has an annual turnover and/or annual balance sheet total that does not exceed EUR 2 million;

(61) 「筆頭監督者」とは，この規則の第 31 条第 1 項(b)に従って任命された欧州の監督当局のことを意味し；

‘Lead Overseer’ means the European Supervisory Authority appointed in accordance with Article 31(1), point (b) of this Regulation;

(62) 「共同委員会」とは，規則(EU) No 1093/2010，規則(EU) No 1094/2010 及び規則(EU) No 1095/2010 の各第 54 条に示す委員会のことを意味し；

‘Joint Committee’ means the committee referred to in Article 54 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010;

(63) 「小企業」とは，10 名以上 50 名未満の者を雇用し，かつ，200 万ユーロを超え 1000 万ユーロ未満の年次総売上及びまたは年次貸借対照表合計をもつ金融機関のことを意味し；

‘small enterprise’ means a financial entity that employs 10 or more persons, but fewer than 50 persons, and has an annual turnover and/or annual balance sheet total that exceeds EUR 2 million, but does not exceed EUR 10 million;

(64) 「中規模企業」とは，小企業ではなく，かつ，250 名未満の者を雇用し，かつ，5000 万ユーロ未満の年次総売上及びまたは 4300 万ユーロ未満の年次貸借対照表をもつ金融機関のことを意味し；

‘medium-sized enterprise’ means a financial entity that is not a small enterprise and employs fewer than 250 persons and has an annual turnover that does not exceed EUR 50 million and/or an annual balance sheet that does not exceed EUR 43 million;

(65) 「行政機関」とは，国内中央銀行を含め，政府またはそれ以外の公行政の法主体のことを意味する。

‘public authority’ means any government or other public administration entity, including national central banks.

第 4 条 比例性の原則

Article 4 **Proportionality principle**

1. 金融機関は，その金融機関の規模と全体的なリスクプロファイル並びにその金融機関のサービス，活動及び運営管理の性質，規模及び複雑性を考慮に入れた上で，比例性の原則に従って第 II 章の中で定められた規定を実装する。

   Financial entities shall implement the rules laid down in Chapter II in accordance with the principle of proportionality, taking into account their size and overall risk profile, and the nature, scale and complexity of their services, activities and operations.

2. 加えて，金融機関による第 III 章，第 IV 章及び第 V 章第 I 節の適用は，それらの章の適格な規定の中で個別に定められているとおり，その金融機関の規模と全体的なリスクプロファイル並びにその金融機関のサービス，活動及び運営管理の性質，規模及び複雑性と比例するものとする。

   In addition, the application by financial entities of Chapters III, IV and V, Section I, shall be proportionate to their size and overall risk profile, and to the nature, scale and complexity of their services, activities and operations, as specifically provided for in the relevant rules of those Chapters.

3. 職務権限のある当局は，第 6 条第 5 項及び第 16 条第 2 項による職務権限のある当局の要求に応じて提出された報告書を基礎として，ICT リスクマネジメント枠組みの一貫性を評価する際，金融機関による比例性の原則の適用を判断する。

   The competent authorities shall consider the application of the proportionality principle by financial entities when reviewing the consistency of the ICT risk management framework on the basis of the reports submitted upon the request of competent authorities pursuant to Article 6(5) and Article 16(2).

第 II 章 ICT リスクマネジメント
CHAPTER II ICT risk management

第 I 節
Section I

第 5 条 統治と組織
Article 5 Governance and organisation

1. 金融機関は，高度のデジタル運営管理上の回復力を達成するため，第 6 条第 4 項に従い，ICT リスクの実効的かつ健全なマネジメントを確保する内部の統治と管理の枠組みを設ける。

Financial entities shall have in place an internal governance and control framework that ensures an effective and prudent management of ICT risk, in accordance with Article 6(4), in order to achieve a high level of digital operational resilience.

2. 金融機関の経営陣は，第 6 条第 1 項に示す ICT リスクマネジメント枠組みと関連する全ての手立ての実装を定義し，承認し，監督し，かつ，その実装に関して責任を負う。

The management body of the financial entity shall define, approve, oversee and be responsible for the implementation of all arrangements related to the ICT risk management framework referred to in Article 6(1).

第 1 副項の目的のために，経営陣は:

For the purposes of the first subparagraph, the management body shall:

(a) 当該金融機関の ICT リスクを取扱うことに関する最終的な責任を負い;

bear the ultimate responsibility for managing the financial entity's ICT risk;

(b) 高度な水準のデータの可用性，真正性，完全性及び機密性を維持することを確保することを狙いとする基本方針を設け;

put in place policies that aim to ensure the maintenance of high standards of availability, authenticity, integrity and confidentiality, of data;

(c) ICT と関連する権能をもつ全ての者の明確な役割及び職責を設け，かつ，当該権能をもつ者の間における実効的かつ適時の伝達，協力及び調整を確保するための適切な統治上の取決めを定め;

set clear roles and responsibilities for all ICT-related functions and establish appropriate governance arrangements

to ensure effective and timely communication, cooperation and coordination among those functions;

(d) 第 6 条第 8 項(b)に示す金融機関の ICT リスクの適切なリスク許容レベルの決定を含め，第 6 条第 8 項に示すデジタル運営管理上の回復力戦略を設けること及び承認することに関する全体的な職責を負い；

bear the overall responsibility for setting and approving the digital operational resilience strategy as referred to in Article 6(8), including the determination of the appropriate risk tolerance level of ICT risk of the financial entity, as referred to in Article 6(8), point (b);

(e) 当該金融機関の全体的な事業継続性基本方針並びに対応計画及び回復計画の不可欠な部分を形成する専用の個別の基本方針として採択され得る第 11 条第 1 項及び第 3 項にそれぞれ示す当該金融機関の ICT 事業継続性基本方針並びに ICT 対応計画及び ICT 復旧計画の実装を承認し，監督し及び定期的に見直し；

approve, oversee and periodically review the implementation of the financial entity's ICT business continuity policy and ICT response and recovery plans, referred to, respectively, in Article 11(1) and (3), which may be adopted as a dedicated specific policy forming an integral part of the financial entity's overall business continuity policy and response and recovery plan;

(f) 当該金融機関の ICT 内部監査計画，ICT 監査及びそれらに対する実質的な変更を承認し及び定期的に見直し；

approve and periodically review the financial entity's ICT internal audit plans, ICT audits and material modifications to them;

(g) 第 13 条第 6 項に示す適格な ICT セキュリティ認識向上計画とデジタル運営管理上の回復力訓練及び全ての従業者の ICT 技能を含め，全てのタイプの資源との関係において，当該金融機関のデジタル運営管理上の回復力の必要性を満たすための適切な予算を割当て及び定期的に見直し；

allocate and periodically review the appropriate budget to fulfil the financial entity's digital operational resilience needs in respect of all types of resources, including relevant ICT security awareness programmes and digital operational resilience training referred to in Article 13(6), and ICT skills for all staff;

(h) ICT サードパーティサービスプロバイダから提供される ICT サービスの利用と関連する取決めに関する当該金融機関の基本方針を承認し及び定期的に見直し；

approve and periodically review the financial entity's policy on arrangements regarding the use of ICT services provided by ICT third-party service providers;

(i) 金融機関レベルで，以下の事項が適正に情報伝達されることを実現可能にする報告の経路を設ける:

put in place, at corporate level, reporting channels enabling it to be duly informed of the following:

(i) ICT サービスの利用に関して ICT サードパーティサービスプロバイダとの間で締結した取決め，

arrangements concluded with ICT third-party service providers on the use of ICT services,

(ii) ICT サードパーティサービスプロバイダに関して適格に計画された実質的な変更，

any relevant planned material changes regarding the ICT third-party service providers,

(iii) 当該変更の影響及び少なくとも ICT と関連する大きなインシデント及びその影響並びに対応，復旧及び是正の方策を評価するためのリスク分析の要約を含め，当該取決めに服する不可欠な機能または重要な機能に関するそのような変更の潜在的な影響。

the potential impact of such changes on the critical or important functions subject to those arrangements, including a risk analysis summary to assess the impact of those changes, and at least major ICT-related incidents and their impact, as well as response, recovery and corrective measures.

3. マイクロ企業以外の金融機関は，ICT サービスの利用に関して ICT サードパーティサービスプロバイダとの間で締結した取決めを監視するための担当部署を設け，または，関連するリスクエクスポージャー及び適格な文書化を監視する職責を負う上級管理職の者を指定する。

Financial entities, other than microenterprises, shall establish a role in order to monitor the arrangements concluded with ICT third-party service providers on the use of ICT services, or shall designate a member of senior management as responsible for overseeing the related risk exposure and relevant documentation.

4. 金融機関の経営陣の構成員は，定期的に個別の訓練を受けることによる場合を含め，ICT リスク及び当該金融機関の運営管理に対するその ICT リスクの影響を理解し及び評価するための，取扱われる ICT リスクに見合った十分な知識及び技能を，積極的に最新のものに保つ。

Members of the management body of the financial entity shall actively keep up to date with sufficient knowledge and skills to understand and assess ICT risk and its impact on the operations of the financial entity, including by following specific training on a regular basis, commensurate to the ICT risk being managed.

第 II 節
Section II

第 6 条 ICT リスクマネジメント枠組み
Article 6 **ICT risk management framework**

1. 金融機関は，当該金融機関の全体的なリスクマネジメントシステムの一部として，良好であり，包括的かつ十分に文書化され，ICT リスクに対して当該金融機関が迅速，効率的かつ包括的に対処できるようにし，かつ，高度のデジタル運営管理上の回復力を確保できるようにする ICT リスクマネジメント枠組みをもつ。

   Financial entities shall have a sound, comprehensive and well-documented ICT risk management framework as part of their overall risk management system, which enables them to address ICT risk quickly, efficiently and comprehensively and to ensure a high level of digital operational resilience.

2. 全ての情報資産及び ICT 資産が，毀損及び無権限のアクセスまたは利用を含むリスクから適切に防護されることを確保するため，ICT リスクマネジメント枠組みは，少なくとも，コンピュータソフトウェア，ハードウェア，サーバを含め，全ての情報資産及び ICT 資産を適正かつ適切に防護するために必要となる，並びに，構内，データセンター及び機微と指定された区域のような，全ての適格な物理的コンポーネント及びインフラを防護するために必要となる戦略，基本方針，手続，ICT 手順及びツールを含める。

   The ICT risk management framework shall include at least strategies, policies, procedures, ICT protocols and tools that are necessary to duly and adequately protect all information assets and ICT assets, including computer software, hardware, servers, as well as to protect all relevant physical components and infrastructures, such as premises, data centres and sensitive designated areas, to ensure that all information assets and ICT assets are adequately protected from risks including damage and unauthorised access or usage.

3. 当該金融機関の ICT リスクマネジメント枠組みに従い，金融機関は，適切な戦略，基本方針，手続，ICT 手順及びツールを設けることにより，ICT リスクの影響をミニマム化する。金融機関は，職務権限のある当局の要求に応じて，職務権限のある当局に対し，ICT リスクに関する及び当該金融機関の ICT リスクマネジメント枠組みに関する完全かつアップデートされた情報を提供する。

   In accordance with their ICT risk management framework, financial entities shall minimise the impact of ICT risk by deploying appropriate strategies, policies, procedures, ICT protocols and tools. They shall provide complete and updated information on ICT risk and on their ICT risk management framework to the competent authorities upon their request.

4. マイクロ企業以外の金融機関は，利益相反を防止するため，管理機能に対する ICT リスクを取扱うこと及び監督することに職責を負う者を任命し，かつ，そのような管理機能の適切なレベルの独立性を確保する。金融機関は，3 つの防衛線モデルに従い， ICT リスクマネジメント機能，管理機能及び内

部監査機能の適切な分離と独立を確保し，または，内部リスクマネジメント管理モデルを確保する。

Financial entities, other than microenterprises, shall assign the responsibility for managing and overseeing ICT risk to a control function and ensure an appropriate level of independence of such control function in order to avoid conflicts of interest. Financial entities shall ensure appropriate segregation and independence of ICT risk management functions, control functions, and internal audit functions, according to the three lines of defence model, or an internal risk management and control model.

5. ICT リスクマネジメント枠組みは，文書化され，かつ，少なくとも年 1 回，または，マイクロ企業の場合においては定期的に及び ICT と関連する大きなインシデントの発生に応じて，かつ，適格なデジタル運営管理上の回復力試験または監査プロセスからもたらされる監督上の指示または判断結果に従って，見直される。ICT リスクマネジメント枠組みは，実装及び監視からもたらされる教訓を基礎として，継続的に改善される。ICTリスクマネジメント枠組みの見直しに関する報告書は，職務権限のある当局の要求に応じて，職務権限のある当局に対して提出される。

The ICT risk management framework shall be documented and reviewed at least once a year, or periodically in the case of microenterprises, as well as upon the occurrence of major ICT-related incidents, and following supervisory instructions or conclusions derived from relevant digital operational resilience testing or audit processes. It shall be continuously improved on the basis of lessons derived from implementation and monitoring. A report on the review of the ICT risk management framework shall be submitted to the competent authority upon its request.

6. マイクロ企業以外の金融機関の ICT リスクマネジメント枠組みは，当該金融機関の監査計画に沿って定期的に，監査担当者による内部監査に服する。それらの監査担当者は，ICT リスクにおける十分な知識，技能及び経験並びに適切な独立性をもつ。ICT 監査の頻度及び対象は，当該金融機関の ICTリスクと見合ったものとする。

The ICT risk management framework of financial entities, other than microenterprises, shall be subject to internal audit by auditors on a regular basis in line with the financial entities' audit plan. Those auditors shall possess sufficient knowledge, skills and expertise in ICT risk, as well as appropriate independence. The frequency and focus of ICT audits shall be commensurate to the ICT risk of the financial entity.

7. 内部監査による見直しからの判断結果を基礎として，金融機関は，ICT 監査の重要な判断結果の適時の検証と解消のための規定を含め，公式の事後対応プロセスを設ける。

Based on the conclusions from the internal audit review, financial entities shall establish a formal follow-up process, including rules for the timely verification and remediation of critical ICT audit findings.

8. ICT リスクマネジメント枠組みは，その枠組みがどのように実装されるのかを定めるデジタル運営管理上の回復力戦略を含める。その目的のために，デジタル運営管理上の回復力戦略は，以下のことによって，ICTリスクに対処し及び個別の ICT 目標を達成するための手法を含める：

The ICT risk management framework shall include a digital operational resilience strategy setting out how the framework shall be implemented. To that end, the digital operational resilience strategy shall include methods to address ICT risk and attain specific ICT objectives, by:

(a) ICT リスクマネジメント枠組みが，当該金融機関の事業戦略及び事業目標をどのように支えるかを説明すること；

explaining how the ICT risk management framework supports the financial entity's business strategy and objectives;

(b) 当該金融機関のリスク選好に従って ICT リスクのリスク許容レベルを設定すること，及び，ICT の混乱の許容の影響を分析すること；

establishing the risk tolerance level for ICT risk, in accordance with the risk appetite of the financial entity, and analysing the impact tolerance for ICT disruptions;

(c) 鍵となる遂行能力指標及び鍵となるリスク指標を含め，情報セキュリティ上の明確な目標を設定すること；

setting out clear information security objectives, including key performance indicators and key risk metrics;

(d) ICT 参照アーキテクチャ及び個別の事業目標を達成するために必要となる修正を説明すること；

explaining the ICT reference architecture and any changes needed to reach specific business objectives;

(e) ICT と関連するインデントを検出し，その影響を防止し及びその影響からの防護を提供するために設けられた異なる仕組みの概要を示すこと；

outlining the different mechanisms put in place to detect ICT-related incidents, prevent their impact and provide protection from it;

(f) 報告された ICT と関連する大きなインシデントの数及び防止方策の実効性を基礎として，現在のデジタル運営管理上の回復力の状況を根拠づけること；

evidencing the current digital operational resilience situation on the basis of the number of major ICT-related incidents reported and the effectiveness of preventive measures;

(g) この規則の第 IV 章に従い，デジタル運営管理上の回復力試験を実装すること；

implementing digital operational resilience testing, in accordance with Chapter IV of this Regulation;

(h) 第 14 条に従ってそのインシデントの開示が要求されている ICT と関連するインシデントの際における伝達戦略の概要を示すこと。

outlining a communication strategy in the event of ICT-related incidents the disclosure of which is required in accordance with Article 14.

9. 金融機関は，第 8 項に示すデジタル運営管理上の回復力戦略の過程において，グループレベルまたは法主体レベルで，ICT サードパーティサービスプロバイダへの鍵となる依存性を示し，かつ，ICT サードパーティサービスプロバイダの調達構成の背後にある合理性を説明する全体的な ICT マルチベンダ戦略を定義できる。

Financial entities may, in the context of the digital operational resilience strategy referred to in paragraph 8, define a holistic ICT multi-vendor strategy, at group or entity level, showing key dependencies on ICT third-party service providers and explaining the rationale behind the procurement mix of ICT third-party service providers.

10. 金融機関は，部門別の欧州連合法及び国内法に従い，ICT リスクマネジメントの要件の遵守を検証する仕事を，グループ内事業者または外部事業者に対してアウトソースできる。そのようなアウトソースをする場合，当該金融機関は，ICT リスクマネジメントの要件の遵守の検証に関し，全面的に責任を負い続ける。

Financial entities may, in accordance with Union and national sectoral law, outsource the tasks of verifying compliance with ICT risk management requirements to intra-group or external undertakings. In case of such outsourcing, the financial entity remains fully responsible for the verification of compliance with the ICT risk management requirements.

第 7 条 ICT システム，手順及びツール

Article 7 **ICT systems, protocols and tools**

ICT リスクに対処し及びそれを取扱うため，金融機関は，以下のような，最新の ICT システム，手順及びツールを使用し及び維持する：

In order to address and manage ICT risk, financial entities shall use and maintain updated ICT systems, protocols and tools that are:

(a) 第 4 条に示す比例性の原則に従い，当該金融機関の活動の遂行を支える運営管理の影響度に照らして適切であり；

appropriate to the magnitude of operations supporting the conduct of their activities, in accordance with the

proportionality principle as referred to in Article 4;

(b) 信頼性があり;

reliable;

(c) 活動の遂行と適時のサービス提供のために必要となるデータを正確に処理するため，及び，新たな技術が導入される際を含め，必要に応じて，ピーク時の注文，メッセージまたはトランザクションの分量を取扱うために十分な能力を具備しており;

equipped with sufficient capacity to accurately process the data necessary for the performance of activities and the timely provision of services, and to deal with peak orders, message or transaction volumes, as needed, including where new technology is introduced;

(d) ストレスのかかった市場条件またはそれ以外の負の状況の下において要求される付加的な情報処理の需要を適切に取扱うことができるようにするための技術上の回復力がある。

technologically resilient in order to adequately deal with additional information processing needs as required under stressed market conditions or other adverse situations.

第 8 条 識別

Article 8 **Identification**

1. 第 6 条第 1 項に示す ICT リスクマネジメント枠組みの一部として，金融機関は，ICT によって支えられた事業上の機能，役割及び職責，それらの機能を支える情報資産及び ICT 資産並びに ICT リスクとの関係におけるそれらの役割及び依存性の全てを識別し，分類し及び適切に文書化する。金融機関は，必要に応じて，かつ，少なくとも年次で，この分類の適切性及び適格な文書の適切性を見直す。

As part of the ICT risk management framework referred to in Article 6(1), financial entities shall identify, classify and adequately document all ICT supported business functions, roles and responsibilities, the information assets and ICT assets supporting those functions, and their roles and dependencies in relation to ICT risk. Financial entities shall review as needed, and at least yearly, the adequacy of this classification and of any relevant documentation.

2. 金融機関は，継続的に，全ての ICT リスクの発生源，とりわけ，他の金融機関に対する及び他の金融機関からのリスクエクスポージャーを識別し，かつ，当該金融機関の ICT によって支えられた事業上の機能，情報資産及び ICT 資産と関係するサイバー脅威及び ICT 脆弱性を評価する。金融機関は，定期的にかつ少なくとも年次で，当該金融機関に影響を与えるリスクシナリオを見直す。

Financial entities shall, on a continuous basis, identify all sources of ICT risk, in particular the risk exposure to and from other financial entities, and assess cyber threats and ICT vulnerabilities relevant to their ICT supported business functions, information assets and ICT assets. Financial entities shall review on a regular basis, and at least yearly, the risk scenarios impacting them.

3. マイクロ企業以外の金融機関は，ネットワーク及び情報システムのインフラにおける大きな変更，当該金融機関の ICT によって支えられた事業上の機能，情報資産または ICT 資産に影響を与えるプロセスまたは手続の大きな変更があれば，リスク評価を遂行する。

Financial entities, other than microenterprises, shall perform a risk assessment upon each major change in the network and information system infrastructure, in the processes or procedures affecting their ICT supported business functions, information assets or ICT assets.

4. 金融機関は，リモートサイト上にある情報資産及び ICT 資産，ネットワーク上の資源及びハードウェア装置を含め，全ての情報資産及び ICT 資産を識別し，かつ，当該金融機関が不可欠であると判断するものをマップする。当該金融機関は，その情報資産及び ICT 資産の構成並びに異なる情報資産及び ICT 資産の間における結びつき及び相互の依存性をマップする。

Financial entities shall identify all information assets and ICT assets, including those on remote sites, network resources and hardware equipment, and shall map those considered critical. They shall map the configuration of the information assets and ICT assets and the links and interdependencies between the different information assets and ICT assets.

5. 金融機関は，ICT サードパーティサービスプロバイダに依存している全てのプロセスを識別及び文書化し，かつ，不可欠な機能または重要な機能を支えるサービスを提供する ICT サードパーティサービスプロバイダとの間の相互の結びつきを識別する。

Financial entities shall identify and document all processes that are dependent on ICT third-party service providers, and shall identify interconnections with ICT third-party service providers that provide services that support critical or important functions.

6. 第 1 項，第 4 項及び第 5 項の目的のために，金融機関は，適格な資産目録を維持管理し，かつ，定期的に，及び，第 3 項に示す大きな変更が発生するときは常に，アップデートする。

For the purposes of paragraphs 1, 4 and 5, financial entities shall maintain relevant inventories and update them periodically and every time any major change as referred to in paragraph 3 occurs.

7. マイクロ企業以外の金融機関は，定期的に，かつ，少なくとも年次で，及び，技術，アプリケーションまたはシステムの接続の前後の場合において，全ての旧式の ICT システムに対する個別の ICT リスク評価を実施する。

Financial entities, other than microenterprises, shall on a regular basis, and at least yearly, conduct a specific ICT risk assessment on all legacy ICT systems and, in any case before and after connecting technologies, applications or systems.

第 9 条 防護と防止

Article 9 **Protection and prevention**

1. ICT システムを適切に防護する目的のために，及び，対応の方策を準備するという観点から，金融機関は，ICT システム及びツールの安全性及び稼働を継続的に監視及び管理し，かつ，適切な ICT セキュリティのツール，基本方針及び手続の配置を介して，ICT システムに対する ICT リスクの影響をミニマム化する。

   For the purposes of adequately protecting ICT systems and with a view to organising response measures, financial entities shall continuously monitor and control the security and functioning of ICT systems and tools and shall minimise the impact of ICT risk on ICT systems through the deployment of appropriate ICT security tools, policies and procedures.

2. 金融機関は，とりわけ，不可欠な機能または重要な機能を支える ICT システムに関し，ICT システムの回復力，継続性及び可用性を確保することを狙いとし，また，休止中，使用中または移動中の別を問わず，データの高度な水準の可用性，真正性，完全性及び機密性を維持することを狙いとする ICT セキュリティの基本方針，手続，手順及びツールを設計し，調達し及び実装する。

   Financial entities shall design, procure and implement ICT security policies, procedures, protocols and tools that aim to ensure the resilience, continuity and availability of ICT systems, in particular for those supporting critical or important functions, and to maintain high standards of availability, authenticity, integrity and confidentiality of data, whether at rest, in use or in transit.

3. 第 2 項に示す目的を達成するため，金融機関は，第 4 条に従い，適切な ICT ソリューション及びプロセスを用いる。それらの ICT ソリューション及びプロセスは：

   In order to achieve the objectives referred to in paragraph 2, financial entities shall use ICT solutions and processes that are appropriate in accordance with Article 4. Those ICT solutions and processes shall:

   (a) データの移転手段の安全性を確保し；

   ensure the security of the means of transfer of data;

   (b) 事業活動を妨げるかもしれないデータの破損または喪失，無権限アクセス及び技術上の欠陥のリスクをミニマム化し；

minimise the risk of corruption or loss of data, unauthorised access and technical flaws that may hinder business activity;

(c) 可用性の欠如，真正性と完全性の毀損，機密性の侵害及びデータの喪失を防止し；
prevent the lack of availability, the impairment of the authenticity and integrity, the breaches of confidentiality and the loss of data;

(d) 貧弱な運用管理，処理と関連するリスク及びヒューマンエラーを含め，データのマネジメントから生ずるリスクからデータが防護されることを確保する。

ensure that data is protected from risks arising from data management, including poor administration, processing-related risks and human error.

4. 第 6 条第 1 項に示す ICT リスクマネジメント枠組みの一部として，金融機関は：

As part of the ICT risk management framework referred to in Article 6(1), financial entities shall:

(a) それが適用可能なときは，金融機関の顧客のデータ，情報資産及び ICT 資産を含め，データ，情報資産及び ICT 資産の可用性，真正性，完全性及び機密性を防護するための諸原則を定義する情報セキュリティの基本方針を策定し及び文書化し；

develop and document an information security policy defining rules to protect the availability, authenticity, integrity and confidentiality of data, information assets and ICT assets, including those of their customers, where applicable;

(b) リスクベースのアプローチに従い，サイバー攻撃の場合において影響を受ける情報資産を分離するための自動化された仕組みを実装することを含めることができる適切な技術，手法及び手順を用いている良好なネットワーク及びインフラのマネジメント構造を構築し；

following a risk-based approach, establish a sound network and infrastructure management structure using appropriate techniques, methods and protocols that may include implementing automated mechanisms to isolate affected information assets in the event of cyber-attacks;

(c) 情報資産及び ICT 資産に対する物理的なアクセスまたは論理的なアクセスを，正当かつ承認された機能及び活動の範囲内のみに限定する基本方針を実装し，また，その目的のために，アクセスの権利に対応する基本方針，手続及び管理策のセットを定め，かつ，その良好な運用を確保し；

implement policies that limit the physical or logical access to information assets and ICT assets to what is required for legitimate and approved functions and activities only, and establish to that end a set of policies, procedures and

controls that address access rights and ensure a sound administration thereof;

(d) 適格な技術標準及び専用の管理システムを基礎とする強力な認証の仕組みのための基本方針及び手順，並びに，承認されたデータ分類及び ICT リスク評価プロセスの結果を基礎とし，それによってデータが暗号化される暗号化鍵という防護方策を実装し；

implement policies and protocols for strong authentication mechanisms, based on relevant standards and dedicated control systems, and protection measures of cryptographic keys whereby data is encrypted based on results of approved data classification and ICT risk assessment processes;

(e) ICT システムに対する全ての変更が，管理された態様で記録され，試験され，評価され，承認され，実装され，検証されることを確保するため，ソフトウェア，ハードウェア，ファームウェアのコンポーネント，システムまたはセキュリティのパラメータの変更を含め，リスク評価のアプローチを基礎とし，当該金融機関の全体的な変更マネジメントのプロセスの不可欠の部分である ICT の変更マネジメントに関する文書化された基本方針，手続及び管理策を実装し；

implement documented policies, procedures and controls for ICT change management, including changes to software, hardware, firmware components, systems or security parameters, that are based on a risk assessment approach and are an integral part of the financial entity's overall change management process, in order to ensure that all changes to ICT systems are recorded, tested, assessed, approved, implemented and verified in a controlled manner;

(f) パッチ及びアップデートに関する適切かつ包括的な文書化された基本方針をもつ。

have appropriate and comprehensive documented policies for patches and updates.

第 1 副項(b)の目的のために，金融機関は，特に相互に結び付けられた金融プロセスにおける伝播をミニマム化しかつ防止するために直ちに切断されまたは分離されるようにすることのできる方法により，ネットワーク接続のインフラを設計する。

For the purposes of the first subparagraph, point (b), financial entities shall design the network connection infrastructure in a way that allows it to be instantaneously severed or segmented in order to minimise and prevent contagion, especially for interconnected financial processes.

第 1 副項(e)の目的のために，ICT 変更マネジメントのプロセスは，経営陣の適切なラインによって承認され，かつ，個別の手順を設ける。

For the purposes of the first subparagraph, point (e), the ICT change management process shall be approved by appropriate lines of management and shall have specific protocols in place.

第 10 条 検出

Article 10 **Detection**

1. 金融機関は，ICT ネットワークの遂行能力上の問題及び ICT と関連するインシデントを含め，第 17 条に従って異常な活動を直ちに検出するため，並びに，潜在的な実質的な単一障害点を特定するための仕組みを設ける。

   Financial entities shall have in place mechanisms to promptly detect anomalous activities, in accordance with Article 17, including ICT network performance issues and ICT-related incidents, and to identify potential material single points of failure.

   第 1 副項に示す全ての検出の仕組みは，第 25 条に従い，定期的に試験される。

   All detection mechanisms referred to in the first subparagraph shall be regularly tested in accordance with Article 25.

2. 第 1 項に示す検出の仕組みは，多重のレイヤの管理を可能なものとし，かつ，ICT と関連するインシデント対応に従事する適格な従業者に対する自動化された警報の仕組みを含め，ICT と関連するインシデント対応のプロセスの引金となり及びそれを開始するための警告の閾値及び基準を定義する。

   The detection mechanisms referred to in paragraph 1 shall enable multiple layers of control, define alert thresholds and criteria to trigger and initiate ICT-related incident response processes, including automatic alert mechanisms for relevant staff in charge of ICT-related incident response.

3. 金融機関は，利用者の活動，ICT の異常及び ICT と関連するインシデントの発生，とりわけサイバー攻撃を監視するための十分な資源と実現能力を投入する。

   Financial entities shall devote sufficient resources and capabilities to monitor user activity, the occurrence of ICT anomalies and ICT-related incidents, in particular cyber-attacks.

4. それに加えて，データ報告サービスプロバイダは，完全性に関して取引報告を実効的に点検でき，欠落と明白なエラーを識別し，かつ，当該報告の再送を要求できるシステムを設ける。

   Data reporting service providers shall, in addition, have in place systems that can effectively check trade reports for completeness, identify omissions and obvious errors, and request re-transmission of those reports.

第 11 条 対応及び復旧

Article 11 **Response and recovery**

1. 第 6 条第 1 項に示す ICT リスクマネジメント枠組みの一部として，かつ，第 8 条の中で定められた識

別の要件を基礎として，金融機関は，包括的な ICT 事業継続性基本方針を設ける。その基本方針は，当該金融機関の全体的な事業継続性基本方針の不可欠な部分を形成する専用の個別の基本方針として採択され得る。

As part of the ICT risk management framework referred to in Article 6(1) and based on the identification requirements set out in Article 8, financial entities shall put in place a comprehensive ICT business continuity policy, which may be adopted as a dedicated specific policy, forming an integral part of the overall business continuity policy of the financial entity.

2. 金融機関は，以下のことを狙いとする専用の，適切かつ文書化された取決め，計画，手続及び仕組みを介して，ICT 事業継続性基本方針を実装する：

Financial entities shall implement the ICT business continuity policy through dedicated, appropriate and documented arrangements, plans, procedures and mechanisms aiming to:

(a) 当該金融機関の不可欠な機能または重要な機能の継続性を確保すること；

ensure the continuity of the financial entity's critical or important functions;

(b) ICT と関連する全てのインシデントに対して，損害を抑制しかつ活動の再開と復旧活動を優先とする方法で，迅速に，適切かつ実効的に対応し，かつ，それを解決すること；

quickly, appropriately and effectively respond to, and resolve, all ICT-related incidents in a way that limits damage and prioritises the resumption of activities and recovery actions;

(c) 個々のタイプの ICT と関連するインシデントに適した封じ込めの仕組み，プロセス及び技術を実現可能にし，更なる損害を防止する専用の計画並びに第 12 条に従って定められた個別対応の対応手続及び復旧手続を，遅滞なく能動化すること；

activate, without delay, dedicated plans that enable containment measures, processes and technologies suited to each type of ICT-related incident and prevent further damage, as well as tailored response and recovery procedures established in accordance with Article 12;

(d) 予測される影響，損害及び損失を推定すること；

estimate preliminary impacts, damages and losses;

(e) 第 14 条に従って全ての適格な内部従業者及び外部の利害関係者に対してアップデートされた情報が送信されることを確保する伝達と危機管理の活動を定めること，並びに，第 19 条に従って職務権限のある当局に対して報告すること。

set out communication and crisis management actions that ensure that updated information is transmitted to all relevant internal staff and external stakeholders in accordance with Article 14, and report to the competent authorities in accordance with Article 19.

3. 第 6 条第 1 項に示す ICT リスクマネジメント枠組みの一部として，金融機関は，マイクロ企業以外の金融機関の場合においては独立の内部監査による見直しに服する関連する ICT 対応計画及び ICT 復旧計画を実装する。

As part of the ICT risk management framework referred to in Article 6(1), financial entities shall implement associated ICT response and recovery plans which, in the case of financial entities other than microenterprises, shall be subject to independent internal audit reviews.

4. 金融機関は，特に，ICT サードパーティサービスプロバイダとの間の取決めを介してアウトソースされまたは契約される不可欠な機能または重要な機能との関連において，適切な ICT 事業継続性計画を設け，維持管理し及び定期的に試験する。

Financial entities shall put in place, maintain and periodically test appropriate ICT business continuity plans, notably with regard to critical or important functions outsourced or contracted through arrangements with ICT third-party service providers.

5. 全体的な事業継続性の基本方針の一部として，金融機関は，当該金融機関が深刻な事業中断に晒されることの事業影響分析（BIA）を実施する。BIA の下において，金融機関は，適切に，内部データと外部データ及びシナリオ分析を用い，定量的基準及び定性的基準により，深刻な事業中断の潜在的な影響を評価する。BIA は，識別され及びマップされた事業上の機能，支えるプロセス，サードパーティの依存性及び情報資産並びにそれらの相互依存性を考察する。金融機関は，ICT 資産と ICT サービスが，とりわけ，全ての不可欠なコンポーネントの冗長性を適切に確保することに関して，BIA と全面的に揃えられて設計され及び利用されることを確保する。

As part of the overall business continuity policy, financial entities shall conduct a business impact analysis (BIA) of their exposures to severe business disruptions. Under the BIA, financial entities shall assess the potential impact of severe business disruptions by means of quantitative and qualitative criteria, using internal and external data and scenario analysis, as appropriate. The BIA shall consider the criticality of identified and mapped business functions, support processes, third-party dependencies and information assets, and their interdependencies. Financial entities shall ensure that ICT assets and ICT services are designed and used in full alignment with the BIA, in particular with regard to adequately ensuring the redundancy of all critical components.

6. 当該金融機関の包括的な ICT リスクマネジメントの一部として，金融機関は：

As part of their comprehensive ICT risk management, financial entities shall:

(a) 全ての機能を支える ICT システムとの関係において，少なくとも年次で，かつ，不可欠な機能または重要な機能を支える ICT システムに対する大きな変更がある場合，ICT 事業継続性計画並びに ICT 対応計画及び ICT 復旧計画を試験し；

test the ICT business continuity plans and the ICT response and recovery plans in relation to ICT systems supporting all functions at least yearly, as well as in the event of any substantive changes to ICT systems supporting critical or important functions;

(b) 第 14 条に従って設けられる危機伝達計画を試験する。

test the crisis communication plans established in accordance with Article 14.

第 1 副項(a)の目的のために，マイクロ企業以外の金融機関は，その試験計画の中にサイバー攻撃のシナリオ並びに第 12 条の中で定められた義務に適合するために必要となる主たる ICT インフラと冗長能力，バックアップ及び冗長施設との間の切替えのシナリオを含める。

For the purposes of the first subparagraph, point (a), financial entities, other than microenterprises, shall include in the testing plans scenarios of cyber-attacks and switchovers between the primary ICT infrastructure and the redundant capacity, backups and redundant facilities necessary to meet the obligations set out in Article 12.

金融機関は，第 1 副項に従って実施された試験の結果及び監査の点検または監督の報告書から派生する推奨事項を考慮に入れた上で，当該金融機関の ICT 事業継続性の基本方針並びに ICT 対応計画及び ICT 復旧計画を定期的に見直す。

Financial entities shall regularly review their ICT business continuity policy and ICT response and recovery plans, taking into account the results of tests carried out in accordance with the first subparagraph and recommendations stemming from audit checks or supervisory reviews.

7. マイクロ企業以外の金融機関は，危機管理の機能をもつ。その機能は，当該金融機関の ICT 事業継続性計画並びに ICT 対応計画及び ICT 復旧計画の能動化の場合において，就中，第 14 条に従って内部及び外部の危機の伝達を運営管理する明確な手続を定める。

Financial entities, other than microenterprises, shall have a crisis management function, which, in the event of activation of their ICT business continuity plans or ICT response and recovery plans, shall, inter alia, set out clear procedures to manage internal and external crisis communications in accordance with Article 14.

8. 金融機関は，当該金融機関の ICT 事業継続性計画並びに ICT 対応計画及び ICT 復旧計画が能動化する場合において，混乱の出来事の前及びその最中の活動の容易にアクセス可能な記録を保管する。

Financial entities shall keep readily accessible records of activities before and during disruption events when their ICT business continuity plans and ICT response and recovery plans are activated.

9. 証券集中保管機関は，職務権限のある当局に対し，ICT 事業継続性の試験の結果または類似の演習の結果の複製物を提供する。

Central securities depositories shall provide the competent authorities with copies of the results of the ICT business continuity tests, or of similar exercises.

10. マイクロ企業以外の金融機関は，職務権限のある当局の要求に応じて，当該当局に対し，ICT と関連する大きなインシデントにより生じた集約された年次の費用及び損失の推計を報告する。

Financial entities, other than microenterprises, shall report to the competent authorities, upon their request, an estimation of aggregated annual costs and losses caused by major ICT-related incidents.

11. 規則(EU) No 1093/2010，規則(EU) No 1094/2010 及び規則(EU) No 1095/2010 の各第 16 条に従い，ESAs は，共同委員会を介して，2024 年 7 月 17 日までに，第 10 項に示す集約された年次の費用及び損失の推計に関する共通運用指針を策定する。

In accordance with Article 16 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, the ESAs, through the Joint Committee, shall by 17 July 2024 develop common guidelines on the estimation of aggregated annual costs and losses referred to in paragraph 10.

第 12 条 バックアップの基本方針及び手続．修復と復旧の手続及び手法

Article 12 **Backup policies and procedures, restoration and recovery procedures and methods**

1. ミニマムの停止時間，限定的な混乱と喪失により ICT システム及びデータの修復を確保する目的のために，当該金融機関の ICT リスクマネジメント枠組みの一部として，金融機関は，以下のことを策定及び文書化する:

For the purpose of ensuring the restoration of ICT systems and data with minimum downtime, limited disruption and loss, as part of their ICT risk management framework, financial entities shall develop and document:

(a) 情報の不可欠性またはデータの機密性レベルを基礎として，バックアップに服するデータの適用範囲及びバックアップのミニマムの頻度の細目を定めるバックアップの基本方針及び手続；

backup policies and procedures specifying the scope of the data that is subject to the backup and the minimum frequency of the backup, based on the criticality of information or the confidentiality level of the data;

(b) 修復及び復旧の手続及び手法。

restoration and recovery procedures and methods.

2. 金融機関は，バックアップの基本方針及び手続並びに修復及び復旧の手続及び手法に従って能動化され得るバックアップシステムを設置する。バックアップシステムの能動化は，ネットワーク及び情報システムの安全性またはデータの可用性，真正性，完全性もしくは機密性を危険に晒してはならない。定期的に，バックアップの手続並びに修復及び復旧の手続及び手法の試験が実施される。

Financial entities shall set up backup systems that can be activated in accordance with the backup policies and procedures, as well as restoration and recovery procedures and methods. The activation of backup systems shall not jeopardise the security of the network and information systems or the availability, authenticity, integrity or confidentiality of data. Testing of the backup procedures and restoration and recovery procedures and methods shall be undertaken periodically.

3. 自身のシステムを用いてバックアップデータを修復する場合，金融機関は，元の ICT システムから物理的及び論理的に分離された ICT システムを用いる。その ICT システムは，無権限のアクセスまたは ICT 汚染から安全に防護され，かつ，必要に応じてデータとシステムのバックアップを利用できるようにするサービスの適時の修復が可能なものとする。

When restoring backup data using own systems, financial entities shall use ICT systems that are physically and logically segregated from the source ICT system. The ICT systems shall be securely protected from any unauthorised access or ICT corruption and allow for the timely restoration of services making use of data and system backups as necessary.

中央清算機関に関しては，復旧計画は，当該中央清算機関が確実性のある運用を継続できるようにするため及び予定日に清算を完了できるようにするため，破綻の時点における全ての取引の復旧を実現可能なものとする。

For central counterparties, the recovery plans shall enable the recovery of all transactions at the time of disruption to allow the central counterparty to continue to operate with certainty and to complete settlement on the scheduled date.

データ報告サービスプロバイダは，それに加えて，当該プロバイダのサービスを常時提供し及び維持管理するため，適切な資源を維持し及びバックアップと修復施設を設ける。

Data reporting service providers shall additionally maintain adequate resources and have back-up and restoration facilities in place in order to offer and maintain their services at all times.

4. マイクロ企業以外の金融機関は，事業上の必要性を満たすために適切な資源，能力及び機能を具備する冗長性のある ICT 能力を維持する。マイクロ企業は，当該マイクロ企業のリスクプロファイルを基礎として，そのような冗長性のある ICT 能力を維持する必要性を評価する。

Financial entities, other than microenterprises, shall maintain redundant ICT capacities equipped with resources, capabilities and functions that are adequate to ensure business needs. Microenterprises shall assess the need to maintain such redundant ICT capacities based on their risk profile.

5. 証券集中保管機関は，事業上の必要性を満たすために適切な資源，能力，機能及び従業者の手立てを満たす少なくとも 1 つの従たる処理場所を維持する。

Central securities depositories shall maintain at least one secondary processing site endowed with adequate resources, capabilities, functions and staffing arrangements to ensure business needs.

従たる処理場所は：

The secondary processing site shall be:

(a) 区別されたリスクプロファイルに対応することを確保するため及び主たる処理場所に対して影響を与えた出来事からの影響を従たる処理場所が受けることを防止するため，主たる処理場所から地理的に離れた場所に所在し；

located at a geographical distance from the primary processing site to ensure that it bears a distinct risk profile and to prevent it from being affected by the event which has affected the primary site;

(b) 主たる処理場所と同様の不可欠な機能もしくは重要な機能の継続性を確保することができ，または，復旧の目的の範囲内において当該金融機関の不可欠な運用管理を当該金融機関が遂行することを確保するために必要となるサービスのレベルを提供することができ；

capable of ensuring the continuity of critical or important functions identically to the primary site, or providing the level of services necessary to ensure that the financial entity performs its critical operations within the recovery objectives;

(c) 主たる処理場所が利用できなくなった場合において，不可欠な機能または重要な機能の継続性を確保するため，当該金融機関の従業者に対して即時にアクセスできるものとする。

immediately accessible to the financial entity's staff to ensure continuity of critical or important functions in the event that the primary processing site has become unavailable.

6. 個々の機能の復旧時間目標及び復旧時点目標を決定する際，金融機関は，その機能が不可欠な機能または重要な機能であるかどうか，及び，市場の効率性に対する潜在的な全体的影響を考慮に入れる。そのような復旧時間目標は，極限状態のシナリオでは，合意されたサービスレベルに適合していることを確保する。

In determining the recovery time and recovery point objectives for each function, financial entities shall take into account whether it is a critical or important function and the potential overall impact on market efficiency. Such time objectives shall ensure that, in extreme scenarios, the agreed service levels are met.

7. ICT と関連するインシデントから復旧する際，金融機関は，最高度のデータの完全性が維持されることを確保するため，多重の点検と照合を含め，必要な点検を遂行する。システム間において全てのデータが一貫していることを確保するため，外部の利害関係者からのデータを再構築する際においても，それらの点検が遂行される。

When recovering from an ICT-related incident, financial entities shall perform necessary checks, including any multiple checks and reconciliations, in order to ensure that the highest level of data integrity is maintained. These checks shall also be performed when reconstructing data from external stakeholders, in order to ensure that all data is consistent between systems.

第 13 条 学習すること及び進化すること

Article 13 **Learning and evolving**

1. 金融機関は，脆弱性とサイバー脅威，ICT と関連するインシデント，とりわけ，サイバー攻撃に関する情報を収集するための能力と従業者を設け，かつ，それらが当該金融機関のデジタル運営管理上の回復力に対してもつ見込みのある影響を分析する。

Financial entities shall have in place capabilities and staff to gather information on vulnerabilities and cyber threats, ICT-related incidents, in particular cyber-attacks, and analyse the impact they are likely to have on their digital operational resilience.

2. 金融機関は，混乱の原因を分析し，かつ，ICT の運用に対するまたは第 11 条に示す ICT 事業継続性基本方針の範囲内における必要な改善を識別する，当該金融機関のコア活動を混乱させる ICT と関連する大きなインシデントの後の ICT と関連するインシデントの事後評価を設ける。

Financial entities shall put in place post ICT-related incident reviews after a major ICT-related incident disrupts their core activities, analysing the causes of disruption and identifying required improvements to the ICT operations or within the ICT business continuity policy referred to in Article 11.

マイクロ企業以外の金融機関は，要請に応じて，職務権限のある当局に対し，第 1 副項に示す ICT と関連するインシデントの事後評価に従って実装された変更を伝達する。

Financial entities, other than microenterprises, shall, upon request, communicate to the competent authorities, the changes that were implemented following post ICT-related incident reviews as referred to in the first subparagraph.

第 1 副項に示す ICT と関連するインシデントの事後評価は，以下のことと関係する場合を含め，設けられた手続が従われたかどうか，及び，行われた活動が実効的だったかどうかを判定する：

The post ICT-related incident reviews referred to in the first subparagraph shall determine whether the established procedures were followed and the actions taken were effective, including in relation to the following:

(a) セキュリティ警告に対する対応する際及び ICT と関連するインシデントの影響とその深刻さの判断の際の迅速性；

the promptness in responding to security alerts and determining the impact of ICT-related incidents and their severity;

(b) それが適切だと判断するときは，フォレンジック分析の遂行の品質と速度；

the quality and speed of performing a forensic analysis, where deemed appropriate;

(c) 当該金融機関内におけるインシデントのエスカレーションの実効性；

the effectiveness of incident escalation within the financial entity;

(d) 内部及び外部の伝達の実効性。

the effectiveness of internal and external communication.

3. 第 26 条及び第 27 条に従って実施されたデジタル運営管理上の回復力試験からもたらされた教訓，並びに，ICT 事業継続性計画並びに ICT 対応計画及び ICT 復旧計画の能動化により直面した検討課題に沿って，現実の ICT と関連するインシデント，とりわけ，サイバー攻撃からもたらされた教訓は，取引相手との間で交換されかつ監督上の見直しの間に評価された適格な情報と共に，継続的に，ICT リスク評価プロセスの中に適正に組込まれる。それらの判断結果は，第 6 条第 1 項に示す ICT リスクマネジメント枠組みの適格な構成要素の適切な見直しの基礎を形成する。

Lessons derived from the digital operational resilience testing carried out in accordance with Articles 26 and 27 and from real life ICT-related incidents, in particular cyber-attacks, along with challenges faced upon the activation of ICT business continuity plans and ICT response and recovery plans, together with relevant information exchanged with counterparts and assessed during supervisory reviews, shall be duly incorporated on a continuous basis into the ICT risk assessment process. Those findings shall form the basis for appropriate reviews of relevant components of the ICT risk management framework referred to in Article 6(1).

4. 金融機関は，第 6 条第 8 項の中で定められた当該金融機関のデジタル運営管理上の回復力戦略の実装の実効性を監視する。金融機関は，ICT リスクの時間の経過に伴う進化をマップし，ICT リスク

のエクスポージャーのレベルを理解するという観点から，とりわけ，不可欠な機能または重要な機能との関係において，ICT と関連するインシデント，とりわけ，サイバー攻撃とそのパターンの頻度，タイプ，影響度及び進化を分析し，かつ，当該金融機関のサイバー成熟度と準備態勢を拡大させる。

Financial entities shall monitor the effectiveness of the implementation of their digital operational resilience strategy set out in Article 6(8). They shall map the evolution of ICT risk over time, analyse the frequency, types, magnitude and evolution of ICT-related incidents, in particular cyber-attacks and their patterns, with a view to understanding the level of ICT risk exposure, in particular in relation to critical or important functions, and enhance the cyber maturity and preparedness of the financial entity.

5. 上級 ICT 従業者は，少なくとも年次で，経営陣に対し，第 3 項に示す判断結果を報告し，かつ，推奨事項を提案する。

Senior ICT staff shall report at least yearly to the management body on the findings referred to in paragraph 3 and put forward recommendations.

6. 金融機関は，当該金融機関の職員訓練スキーム中の義務的なモジュールとして，ICT セキュリティ認識向上計画とデジタル運営管理上の回復力訓練を策定する。それらの計画及び訓練は，全ての従業者及び上級管理職者に対して提供可能なものとし，かつ，それぞれの職種の権能に相応の複雑さのレベルをもつ。それが適切なときは，金融機関は，第 30 条第 2 項(i)に従い，当該金融機関の適格な訓練スキームの中に ICT サードパーティサービスプロバイダも含める。

Financial entities shall develop ICT security awareness programmes and digital operational resilience training as compulsory modules in their staff training schemes. Those programmes and training shall be applicable to all employees and to senior management staff, and shall have a level of complexity commensurate to the remit of their functions. Where appropriate, financial entities shall also include ICT third-party service providers in their relevant training schemes in accordance with Article 30(2), point (i).

7. マイクロ企業以外の金融機関は，ICT の安全性要件及びデジタル運営管理上の回復力に対するそのような新技術の配置のあり得る影響を理解するという観点からも，定期的に，適格な技術上の発展を監視する。当該金融機関は，現在のサイバー攻撃または新たな形態のサイバー攻撃と実効的に闘うため，最新の ICT リスクマネジメントプロセスにより，最新の状態を保つ。

Financial entities, other than microenterprises, shall monitor relevant technological developments on a continuous basis, also with a view to understanding the possible impact of the deployment of such new technologies on ICT security requirements and digital operational resilience. They shall keep up-to-date with the latest ICT risk management processes, in order to effectively combat current or new forms of cyber-attacks.

第 14 条 伝達

Article 14 **Communication**

1. 第 6 条第 1 項に示す ICT リスクマネジメント枠組みの一部として，金融機関は，顧客及び取引相手に対し並びに公衆に対し，少なくとも，ICT と関連する大きなインシデントまたは脆弱性を，責任をもって適切に開示することを実現可能にする危機伝達計画を設ける。

As part of the ICT risk management framework referred to in Article 6(1), financial entities shall have in place crisis communication plans enabling a responsible disclosure of, at least, major ICT-related incidents or vulnerabilities to clients and counterparts as well as to the public, as appropriate.

2. ICT リスクマネジメント枠組みの一部として，金融機関は，内部従業者向け及び外部利害関係者向けの伝達基本方針を実装する。従業者向けの伝達基本方針は，ICT リスクマネジメントに関与する従業者の間において，とりわけ，対応と復旧に関する職責を負う従業者と情報提供を受ける必要のある従業者との間において区別を設ける必要性を考慮に入れる。

As part of the ICT risk management framework, financial entities shall implement communication policies for internal staff and for external stakeholders. Communication policies for staff shall take into account the need to differentiate between staff involved in ICT risk management, in particular the staff responsible for response and recovery, and staff that needs to be informed.

3. 金融機関内の少なくとも 1 名の者は，ICT と関連するインシデントの伝達戦略を実装する職務を与えられ，かつ，その目的のために，広報及び報道対応の権能を満たすものとする。

At least one person in the financial entity shall be tasked with implementing the communication strategy for ICT-related incidents and fulfil the public and media function for that purpose.

第 15 条 ICT リスクマネジメントのツール，手法，プロセス及び基本方針の更なる整合化

Article 15 **Further harmonisation of ICT risk management tools, methods, processes and policies**

ESAs は，共同委員会を介して，欧州連合サイバーセキュリティ局（ENISA）からの意見聴取を経た上で，以下のことのための，共通の法制上の技術標準案を策定する：

The ESAs shall, through the Joint Committee, in consultation with the European Union Agency on Cybersecurity (ENISA), develop common draft regulatory technical standards in order to:

(a) ネットワークの安全性を確保するという観点から，第 9 条第 2 項に示す ICT セキュリティの基本方針，手続，手順及びツールの中に含められる諸要素の細目を別途定めるため，侵入とデータ悪用に抗する適切な安全確保を実現可能にするため，暗号技術を含め，データの可用性，

真正性，完全性及び機密性を維持するため，並びに，大きな混乱及び不適正な遅滞のない正確かつ迅速なデータ送信を保証するため；

specify further elements to be included in the ICT security policies, procedures, protocols and tools referred to in Article 9(2), with a view to ensuring the security of networks, enable adequate safeguards against intrusions and data misuse, preserve the availability, authenticity, integrity and confidentiality of data, including cryptographic techniques, and guarantee an accurate and prompt data transmission without major disruptions and undue delays;

(b) 第 9 条第 4 項(c)に示すアクセスマネジメントの権利の管理策の構成要素を別途策定し，並びに，アクセスの権利，権利の付与及び取消の手続，ネットワーク利用のパターン，時間，IT 活動及び知らない機器を含め，ICT リスクとの関係における異常な行動を適切な指標により監視することの細目を定める関係する人的資源の基本方針を別途策定するため；

develop further components of the controls of access management rights referred to in Article 9(4), point (c), and associated human resource policy specifying access rights, procedures for granting and revoking rights, monitoring anomalous behaviour in relation to ICT risk through appropriate indicators, including for network use patterns, hours, IT activity and unknown devices;

(c) 異常な活動の迅速な検出を可能にする第 10 条第 1 項の中で細目が定められた仕組み及び ICT と関連するインシデントの検出の引金となる第 10 条第 2 項の中で定められた基準並びに対応のプロセスを別途策定するため；

develop further the mechanisms specified in Article 10(1) enabling a prompt detection of anomalous activities and the criteria set out in Article 10(2) triggering ICT-related incident detection and response processes;

(d) 第 11 条第 1 項に示す ICT 事業継続の基本方針の構成要素の細目を別途定めるため；

specify further the components of the ICT business continuity policy referred to in Article 11(1);

(e) そのような試験が，許容できないレベルまたは失敗まで不可欠な機能または重要な機能の提供の品質を劣化させるシナリオを適正に考慮に入れること，また，適格な ICT サードパーティサービスプロバイダの破産またはそれ以外の失敗の潜在的な影響，及び，それが適格なときは，それぞれのプロバイダの主権国家における政治的リスクを適正に判断することを確保するために，第 11 条第 6 項に示す ICT 事業継続計画の試験の細目を別途定めるため；

specify further the testing of ICT business continuity plans referred to in Article 11(6) to ensure that such testing duly takes into account scenarios in which the quality of the provision of a critical or important function deteriorates to an unacceptable level or fails, and duly considers the potential impact of the insolvency, or other failures, of any relevant ICT third-party service provider and, where relevant, the political risks in the respective

providers' jurisdictions;

(f) 第 11 条第 3 項に示す ICT 対応計画及び ICT 復旧計画の構成要素の細目を別途定めるため;

specify further the components of the ICT response and recovery plans referred to in Article 11(3);

(g) 第 6 条第 5 項に示す ICT リスクマネジメント枠組みの見直しに関する報告書の内容及び書式の細目を別途定めるため。

specifying further the content and format of the report on the review of the ICT risk management framework referred to in Article 6(5);

それらの法制上の技術標準案を策定する際, ESAs は, 異なる金融サービス部門にわたる活動の異なる性質から生ずる特性を適正に考慮に入れつつ, 金融機関の規模及び全体的なリスクプロファイル, 並びに, 当該金融機関のサービス, 活動及び運営管理の性質, 規模及び複雑性を考慮に入れる。

When developing those draft regulatory technical standards, the ESAs shall take into account the size and the overall risk profile of the financial entity, and the nature, scale and complexity of its services, activities and operations, while duly taking into consideration any specific feature arising from the distinct nature of activities across different financial services sectors.

ESAs は, 欧州委員会に対し, 2024 年 1 月 17 日までに, それらの法制上の技術標準案を提出する。

The ESAs shall submit those draft regulatory technical standards to the Commission by 17 January 2024.

規則(EU) No 1093/2010, 規則(EU) No 1094/2010 及び規則(EU) No 1095/2010 の各第 10 条ないし第 14 条に従って第 1 副項に示す法制上の技術標準を採択することによってこの規則を補遺するための権限は, 欧州委員会に対して与えられる。

Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in the first paragraph in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.

第 16 条 簡素化された ICT リスクマネジメント枠組み

Article 16 **Simplified ICT risk management framework**

1. この規則の第 5 条ないし第 15 条は, 小規模で相互結合のない投資企業, 指令(EU) 2015/2366 により

適用除外された決済機関;この規則の第 2 条第 4 項に示す選択肢を適用しないことを決定した構成国との関係においては指令 2013/36/EU によって適用除外された機関;指令 2009/110/EC によって適用除外された電子マネー機関;並びに，小規模な職域退職給付機関に対して適用してはならない。

Articles 5 to 15 of this Regulation shall not apply to small and non-interconnected investment firms, payment institutions exempted pursuant to Directive (EU) 2015/2366; institutions exempted pursuant to Directive 2013/36/EU in respect of which Member States have decided not to apply the option referred to in Article 2(4) of this Regulation; electronic money institutions exempted pursuant to Directive 2009/110/EC; and small institutions for occupational retirement provision.

第 1 副項を妨げることなく，第 1 副項の中で列挙された法主体は:

Without prejudice to the first subparagraph, the entities listed in the first subparagraph shall:

(a) 適格な物理的コンポーネント及びインフラの防護に関するものを含め，ICT リスクの迅速，効率的かつ包括的なマネジメントを狙いとする仕組み及び方策の詳細を定める良好かつ文書化された ICT リスクマネジメント枠組みを設けかつ維持し;

put in place and maintain a sound and documented ICT risk management framework that details the mechanisms and measures aimed at a quick, efficient and comprehensive management of ICT risk, including for the protection of relevant physical components and infrastructures;

(b) 全ての ICT システムの安全性及び稼働を継続的に監視し;

continuously monitor the security and functioning of all ICT systems;

(c) 当該法主体の活動及びサービス提供の遂行を支えるために適切な，良好で，回復力がありかつ最新の ICT のシステム，手順及びツールの利用により，ICT リスクの影響をミニマム化し，かつ，ネットワーク及び情報システムの中にあるデータの可用性，真正性，完全性及び機密性を適切に防護し;

minimise the impact of ICT risk through the use of sound, resilient and updated ICT systems, protocols and tools which are appropriate to support the performance of their activities and the provision of services and adequately protect availability, authenticity, integrity and confidentiality of data in the network and information systems;

(d) ネットワーク及び情報システム内の ICT リスク及び異常活動の発生源が直ちに特定されかつ検出され得るようにし，かつ，ICT と関連するインシデントが迅速に取扱われ得るようにし;

allow sources of ICT risk and anomalies in the network and information systems to be promptly identified and

detected and ICT-related incidents to be swiftly handled;

(e) ICT サードパーティサービスプロバイダへの鍵となる依存性を識別し；

identify key dependencies on ICT third-party service providers;

(f) 少なくともバックアップの方策及び修復の方策を含め，事業継続計画並びに対応の方策及び復旧の方策により，不可欠な機能または重要な機能の継続性を確保し；

ensure the continuity of critical or important functions, through business continuity plans and response and recovery measures, which include, at least, back-up and restoration measures;

(g) (f)に示す計画及び方策並びに(a)及び(c)に従って実装された管理策の実効性を定期的に試験し；

test, on a regular basis, the plans and measures referred to in point (f), as well as the effectiveness of the controls implemented in accordance with points (a) and (c);

(h) (g)に示す試験から及びインシデントの事後分析からもたらされる適格な運営管理上の判断を ICT リスク評価プロセスの中に適切に実装し，かつ，必要性及び ICT リスクプロファイルに従って，ICT セキュリティ認識向上計画及び従業者と経営陣のためのデジタル運営管理上の回復力試験を策定する。

implement, as appropriate, relevant operational conclusions resulting from the tests referred to in point (g) and from post-incident analysis into the ICT risk assessment process and develop, according to needs and ICT risk profile, ICT security awareness programmes and digital operational resilience training for staff and management.

2. 第 1 項第 2 副項(a)に示す ICT リスクマネジメント枠組みは，定期的に，及び，ICT と関連する大きなインシデントの発生に応じて，監督上の指示を遵守して，文書化され及び見直される。その枠組みは，実装及び監視から派生する教訓を基礎として，継続的に改善される。ICT リスクマネジメント枠組みの見直しに関する報告書は，職務権限のある当局の要求に応じて，職務権限のある当局に対して提出される。

The ICT risk management framework referred to in paragraph 1, second subparagraph, point (a), shall be documented and reviewed periodically and upon the occurrence of major ICT-related incidents in compliance with supervisory instructions. It shall be continuously improved on the basis of lessons derived from implementation and monitoring. A report on the review of the ICT risk management framework shall be submitted to the competent authority upon its request.

3. ESAs は，共同委員会を介して，ENISA からの意見聴取を経た上で，以下のことのために，共通の法

制上の技術標準案を策定する:

The ESAs shall, through the Joint Committee, in consultation with the ENISA, develop common draft regulatory technical standards in order to:

(a) 第 1 項第 2 副項(a)に示す ICT リスクマネジメント枠組みの中に含められる諸要素の細目を別途定めるため;

specify further the elements to be included in the ICT risk management framework referred to in paragraph 1, second subparagraph, point (a);

(b) ネットワークの安全性を確保し, 侵入とデータ悪用に抗する適切な安全確保を実現可能にし並びにデータの可用性, 真正性, 完全性及び機密性を維持するという観点から, 第 1 項第 2 副項(c)に示す ICT リスクの影響をミニマム化するためのシステム, 手順及びツールとの関係において, 構成要素の細目を別途定めるため;

specify further the elements in relation to systems, protocols and tools to minimise the impact of ICT risk referred to in paragraph 1, second subparagraph, point (c), with a view to ensuring the security of networks, enabling adequate safeguards against intrusions and data misuse and preserving the availability, authenticity, integrity and confidentiality of data;

(c) 第 1 項第 2 副項(f)に示す ICT 事業継続性計画の構成要素の細目を別途定めるため;

specify further the components of the ICT business continuity plans referred to in paragraph 1, second subparagraph, point (f);

(d) 事業継続性計画の試験に関する規定の細目を別途定め, かつ, 第 1 項第 2 副項(g)に示す管理策の実効性を確保し, 及び, そのような試験が, 許容できないレベルまたは失敗まで不可欠な機能または重要な機能の提供の品質を劣化させるシナリオを適正に考慮に入れることを確保するため;

specify further the rules on the testing of business continuity plans and ensure the effectiveness of the controls referred to in paragraph 1, second subparagraph, point (g) and ensure that such testing duly takes into account scenarios in which the quality of the provision of a critical or important function deteriorates to an unacceptable level or fails;

(e) 第 2 項に示す ICT リスクマネジメント枠組みの見直しに関する報告書の内容及び書式の細目を別途定めるため。

specify further the content and format of the report on the review of the ICT risk management framework

referred to in paragraph 2.

それらの法制上の技術標準案を策定する際，ESAs は，金融機関の規模及び全体的なリスクプロファイル，並びに，当該金融機関のサービス，活動及び運営管理の性質，規模及び複雑性を考慮に入れる。

When developing those draft regulatory technical standards, the ESAs shall take into account the size and the overall risk profile of the financial entity, and the nature, scale and complexity of its services, activities and operations.

ESAs は，欧州委員会に対し，2024 年 1 月 17 日までに，それらの法制上の技術標準案を提出する。

The ESAs shall submit those draft regulatory technical standards to the Commission by 17 January 2024.

規則(EU) No 1093/2010，規則(EU) No 1094/2010 及び規則(EU) No 1095/2010 の各第 10 条ないし第 14 条に従って第 1 副項に示す法制上の技術標準を採択することによってこの規則を補遺するための権限は，欧州委員会に対して与えられる。

Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in the first subparagraph in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.

第 III 章　ICT と関連するインシデントのマネジメント，分類及び報告
CHAPTER III ICT-related incident management, classification and reporting

第 17 条　ICT と関連するインシデントのマネジメントプロセス
Article 17 ICT-related incident management process

1. 金融機関は，ICT と関連するインシデントを検出し，取扱い及び通知するための ICT と関連するインシデントのマネジメントプロセスを定義し，設け及び実装する。

   Financial entities shall define, establish and implement an ICT-related incident management process to detect, manage and notify ICT-related incidents.

2. 金融機関は，全ての ICT と関連するインシデント及び大きなサイバー脅威を記録する。金融機関は，ICT と関連するインシデントの一貫性がありかつ統合された監視，取扱い及び事後対応を確保するため，そのようなインシデントの発生を防止するために根本原因が特定され，文書化され及び対処されることを確保するための適切な手続及びプロセスを定める。

   Financial entities shall record all ICT-related incidents and significant cyber threats. Financial entities shall establish appropriate procedures and processes to ensure a consistent and integrated monitoring, handling and follow-up of ICT-related incidents, to ensure that root causes are identified, documented and addressed in order to prevent the occurrence of such incidents.

3. 第 1 項に示す ICT と関連するインシデントのマネジメントプロセスは:

   The ICT-related incident management process referred to in paragraph 1 shall:

   (a) 早期警戒の指標を設け;

   put in place early warning indicators;

   (b) 当該インシデントの優先度及び深刻度により，及び，第 18 条第 1 項の中で定められた基準に従い，影響を受けるサービスの不可欠性により，ICT と関連するインシデントを識別し，追跡し，履歴を記録し，区分し及び分類するための手続を設け;

   establish procedures to identify, track, log, categorise and classify ICT-related incidents according to their priority and severity and according to the criticality of the services impacted, in accordance with the criteria set out in Article 18(1);

   (c) 異なる ICT と関連するインシデントのタイプ及びシナリオに対して能動化される必要のある役割及び職責を割当て;

assign roles and responsibilities that need to be activated for different ICT-related incident types and scenarios;

(d) 第 14 条に従った従業者，外部の利害関係者及び報道機関に対する伝達の計画及び顧客に対する通知の計画，ICT と関連する顧客の苦情を含め，内部のエスカレーション手続の計画，並びに，取引相手として行動する金融機関に対する情報の提供の計画を適切に設け；

set out plans for communication to staff, external stakeholders and media in accordance with Article 14 and for notification to clients, for internal escalation procedures, including ICT-related customer complaints, as well as for the provision of information to financial entities that act as counterparts, as appropriate;

(e) 少なくとも ICT と関連する大きなインシデントが適格な上級管理職に対して報告されること，及び，経営陣に対して少なくとも ICT と関連する大きなインシデントが，影響，対応及びそのような ICT と関連するインシデントの結果として設けられる付加的な管理策を説明して情報提供されることを確保し；

ensure that at least major ICT-related incidents are reported to relevant senior management and inform the management body of at least major ICT-related incidents, explaining the impact, response and additional controls to be established as a result of such ICT-related incidents;

(f) 影響を緩和するための ICT と関連するインシデントの対応手続を設け，また，サービスが，適時の態様で，運用可能かつ安全になることを確保する。

establish ICT-related incident response procedures to mitigate impacts and ensure that services become operational and secure in a timely manner.

第 18 条 ICT と関連するインシデント及びサイバー脅威の分類

Article 18 **Classification of ICT-related incidents and cyber threats**

1. 金融機関は，ICT と関連するインシデントを分類し，かつ，以下の基準を基礎として当該インシデントの影響を判断する：

Financial entities shall classify ICT-related incidents and shall determine their impact based on the following criteria:

(a) 影響を受けた顧客または金融上の取引相手の数及びまたは適格性，並びに，それが適用可能なときは，当該 ICT と関連するインシデントによって影響を受けたやりとりの額または数，及び，当該 ICT と関連するインシデントが評判上の影響を生じさせたか否か；

the number and/or relevance of clients or financial counterparts affected and, where applicable, the amount or number of transactions affected by the ICT-related incident, and whether the ICT-related incident has caused

reputational impact;

(b) サービス停止時を含め，ICT と関連するインシデントの持続期間；

the duration of the ICT-related incident, including the service downtime;

(c) とりわけ，そのインシデントが複数の構成国に影響を与えているときは，当該 ICT と関連するインシデントによって影響を受けた地域に関する地理的な広がり；

the geographical spread with regard to the areas affected by the ICT-related incident, particularly if it affects more than two Member States;

(d) データの可用性，真正性，完全性または機密性との関係において，当該 ICT と関連するインシデントに伴うデータの喪失；

the data losses that the ICT-related incident entails, in relation to availability, authenticity, integrity or confidentiality of data;

(e) 当該金融機関のやりとり及び運営管理を含め，影響を受けたサービスの不可欠性；

the criticality of the services affected, including the financial entity's transactions and operations;

(f) 絶対的にも相対的にも，当該 ICT と関連するインシデントの経済的影響，とりわけ，直接及び間接の費用及び損失。

the economic impact, in particular direct and indirect costs and losses, of the ICT-related incident in both absolute and relative terms.

2. 金融機関は，当該金融機関のやりとり及び運営管理を含め，リスクに直面しているサービスの不可欠性，狙いとされた顧客または金融上の取引相手の数及びまたは適格性並びにリスクに直面している地域の地理的な広がりを基礎として，サイバー脅威を大きなものと分類する。

Financial entities shall classify cyber threats as significant based on the criticality of the services at risk, including the financial entity's transactions and operations, number and/or relevance of clients or financial counterparts targeted and the geographical spread of the areas at risk.

3. ESAs は，共同委員会を介して，かつ，ECB 及び ENISA からの意見聴取を経た上で，以下の事柄の細目を別途定める共通の法制上の技術標準案を策定する：

The ESAs shall, through the Joint Committee and in consultation with the ECB and ENISA, develop common draft

regulatory technical standards further specifying the following:

(a) ICT と関連する大きなインシデント，または，しかるべく，運営管理もしくは決済の安全性と関連する大きなインシデントであって，第 19 条第 1 項の中で定められた報告義務に服するものを判定するための具現性の閾値を含め，第 1 項の中で定められた基準；

the criteria set out in paragraph 1, including materiality thresholds for determining major ICT-related incidents or, as applicable, major operational or security payment-related incidents, that are subject to the reporting obligation laid down in Article 19(1);

(b) ICT と関連する大きなインシデント，または，しかるべく，運営管理または決済の安全性と関連する大きなインシデントの適格性を評価する目的のために，職務権限のある当局によって他の構成国の適格な職務権限のある当局に対して適用される基準，並びに，第 19 条第 6 項及び第 7 項により他の職務権限のある当局との間で共有される ICT と関連する大きなインシデントの詳細情報，または，しかるべく，運営管理もしくは決済の安全性と関連する大きなインシデントの詳細情報；

the criteria to be applied by competent authorities for the purpose of assessing the relevance of major ICT-related incidents or, as applicable, major operational or security payment-related incidents, to relevant competent authorities in other Member States', and the details of reports of major ICT-related incidents or, as applicable, major operational or security payment-related incidents, to be shared with other competent authorities pursuant to Article 19(6) and (7);

(c) 大きなサイバー脅威を判定するための高い具現性の閾値を含め，本条第 2 項の中で定められた基準。

the criteria set out in paragraph 2 of this Article, including high materiality thresholds for determining significant cyber threats.

4. 本条第 3 項に示す共通の法制上の技術標準案を策定する際，ESAs は，第 4 条第 2 項の中で定められた基準，並びに，国際的な技術標準，それが適切なときは，他の経済部門のための仕様を含め，ENISA によって策定及び公表された運用指針及び仕様を考慮に入れる。第 4 条第 2 項の中で定められた基準を適用する目的のために，ESAs は，ICT と関連するインシデントが迅速に取扱われることを確保するために十分な資源と実現能力を移転可能にすることのマイクロ企業並びに小企業及び中規模企業の需要を適正に判断する。

When developing the common draft regulatory technical standards referred to in paragraph 3 of this Article, the ESAs shall take into account the criteria set out in Article 4(2), as well as international standards, guidance and specifications developed and published by ENISA, including, where appropriate, specifications for other economic sectors. For the purposes of applying the criteria set out in Article 4(2), the ESAs shall duly consider the need for microenterprises and

small and medium-sized enterprises to mobilise sufficient resources and capabilities to ensure that ICT-related incidents are managed swiftly.

ESAs は，欧州委員会に対し，2024 年 1 月 17 日までに，それらの共通の法制上の技術標準案を提出する。

The ESAs shall submit those common draft regulatory technical standards to the Commission by 17 January 2024.

規則(EU) No 1093/2010，規則(EU) No 1094/2010 及び規則(EU) No 1095/2010 の各第 10 条ないし第 14 条に従って第 3 項に示す法制上の技術標準を採択することによってこの規則を補遺するための権限は，欧州委員会に対して与えられる。

Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in paragraph 3 in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.

第 19 条　ICT と関連する大きなインシデントの報告及び大きなサイバー脅威の任意の通知

Article 19 **Reporting of major ICT-related incidents and voluntary notification of significant cyber threats**

1. 金融機関は，本条第 4 項に従って，第 46 条に示す適格な職務権限のある当局に対し，ICT と関連する大きなインシデントを報告する。

Financial entities shall report major ICT-related incidents to the relevant competent authority as referred to in Article 46 in accordance with paragraph 4 of this Article.

金融機関が，第 46 条に示す複数の職務権限のある国内当局による監督に服している場合，構成国は，本条の中で定められた権能及び義務を実行する職責を負う適格な職務権限のある当局として，単一の職務権限のある当局を指定する。

Where a financial entity is subject to supervision by more than one national competent authority referred to in Article 46, Member States shall designate a single competent authority as the relevant competent authority responsible for carrying out the functions and duties provided for in this Article.

規則(EU) No 1024/2013 の第 6 条第 4 項に従って大きいと分類された与信機関は，指令 2013/36/EU の第 4 条に従って指定された適格な職務権限のある国内当局に対し，ICT と関連する大きなインシデントを報告する。その当局は，直ちに，ECB に対し，当該報告を送信する。

Credit institutions classified as significant, in accordance with Article 6(4) of Regulation (EU) No 1024/2013, shall report major ICT-related incidents to the relevant national competent authority designated in accordance with Article 4

of Directive 2013/36/EU, which shall immediately transmit that report to the ECB.

第 1 副項の目的のために，金融機関は，全ての適格な情報を収集及び分析した後，第 20 条に示す雛型を用いて本条第 4 項に示す最初の通知及び報告書を作成し，かつ，職務権限のある当局に対し，それらを提出する。技術的に不可能であることが雛型を用いる最初の通知の提出を妨げている場合，金融機関は，代替的な手段を介して，職務権限のある当局に対し，通知する。

For the purpose of the first subparagraph, financial entities shall produce, after collecting and analysing all relevant information, the initial notification and reports referred to in paragraph 4 of this Article using the templates referred to in Article 20 and submit them to the competent authority. In the event that a technical impossibility prevents the submission of the initial notification using the template, financial entities shall notify the competent authority about it via alternative means.

第 4 項に示す最初の通知及び報告書は，ICT と関連する大きなインシデントの大きさを判断し，かつ，国境を超える影響があり得ることを評価するために職務権限のある当局にとって必要となる全ての情報を含める。

The initial notification and reports referred to in paragraph 4 shall include all information necessary for the competent authority to determine the significance of the major ICT-related incident and assess possible cross-border impacts.

金融機関から適格な職務権限のある当局に対する第 1 副項による報告を妨げることなく，構成国は，幾つかの金融機関または全ての金融機関が，指令(EU) 2022/2555 に従って指定されまたは設けられた職務権限のある当局またはコンピュータセキュリティインシデント対応チーム（CSIRTs）に対しても，第 20 条に示す雛型を用いて本条第 4 項に示す最初の通知及び各報告を提供することを付加的に決定できる。

Without prejudice to the reporting pursuant to the first subparagraph by the financial entity to the relevant competent authority, Member States may additionally determine that some or all financial entities shall also provide the initial notification and each report referred to in paragraph 4 of this Article using the templates referred to in Article 20 to the competent authorities or the computer security incident response teams (CSIRTs) designated or established in accordance with Directive (EU) 2022/2555.

2. 金融機関は，その脅威が金融システム，サービス利用者または顧客と関係する脅威であるとその金融機関が判断するときは，任意で，適格な職務権限のある当局に対して大きなサイバー脅威を通知できる。適格な職務権限のある当局は，第 6 項に示す他の適格な当局に対し，そのような情報を提供できる。

Financial entities may, on a voluntary basis, notify significant cyber threats to the relevant competent authority when they deem the threat to be of relevance to the financial system, service users or clients. The relevant competent authority may provide such information to other relevant authorities referred to in paragraph 6.

規則(EU) No 1024/2013 の第 6 条第 4 項に従って大きいと分類された与信機関は，指令 2013/36/EU の第 4 条に従って指定された適格な職務権限のある国内当局に対し，任意で，大きなサイバー脅威を通知できる。その当局は，直ちに，ECB に対し，当該通知を送信する。

Credit institutions classified as significant, in accordance with Article 6(4) of Regulation (EU) No 1024/2013, may, on a voluntary basis, notify significant cyber threats to relevant national competent authority, designated in accordance with Article 4 of Directive 2013/36/EU, which shall immediately transmit the notification to the ECB.

構成国は，第 1 副項に従って任意で通知する金融機関が，指令(EU) 2022/2555 に従って指定されまたは設けられた CSIRTs に対しても，同通知を送信できることを決定できる。

Member States may determine that those financial entities that on a voluntary basis notify in accordance with the first subparagraph may also transmit that notification to the CSIRTs designated or established in accordance with Directive (EU) 2022/2555.

3. ICT と関連する大きなインシデントが発生し，かつ，顧客の金融上の利益に対する影響をもつときは，金融機関は，不適切な遅滞なく，当該金融機関がそのインシデントに気づいたならば直ちに，当該金融機関の顧客に対し，その ICT と関連する大きなインシデントに関し及びそのようなインシデントの負の影響を緩和するためにとられた方策に関し，連絡する。

Where a major ICT-related incident occurs and has an impact on the financial interests of clients, financial entities shall, without undue delay as soon as they become aware of it, inform their clients about the major ICT-related incident and about the measures that have been taken to mitigate the adverse effects of such incident.

大きなサイバー脅威の場合においては，金融機関は，それが適用可能なときは，当該金融機関の影響を受け得る顧客に対し，その顧客がとることを検討できる適切な防護の方策を連絡する。

In the case of a significant cyber threat, financial entities shall, where applicable, inform their clients that are potentially affected of any appropriate protection measures which the latter may consider taking.

4. 金融機関は，適格な職務権限のある当局に対し，第 20 条第 1 項(a)(ii)に従って定められる期限内に，以下のものを提出する：

Financial entities shall, within the time limits to be laid down in accordance with Article 20, first paragraph, point (a), point (ii), submit the following to the relevant competent authority:

(a) 最初の通知；

an initial notification;

(b) 当初のインシデントの状態が大きく変化したときまたは利用可能な新たな情報を基礎としてICT と関連する大きなインシデントの取扱いが変更されたときは直ちに，適格な状況のアップデートが利用可能なときは常に，または，職務権限のある当局の個別の要求があるときは，アップデートされた通知を適切に伴って，(a)に示す最初の通知の後の中間報告書；

an intermediate report after the initial notification referred to in point (a), as soon as the status of the original incident has changed significantly or the handling of the major ICT-related incident has changed based on new information available, followed, as appropriate, by updated notifications every time a relevant status update is available, as well as upon a specific request of the competent authority;

(c) 緩和の方策が既に実装されたか否かを問わず，根本原因の分析が完了したときは，及び，実際の影響の数値が推定値を置換えるために利用可能なときは，最終報告書。

a final report, when the root cause analysis has been completed, regardless of whether mitigation measures have already been implemented, and when the actual impact figures are available to replace estimates.

5. 金融機関は，欧州連合法及び部門別の国内法に従い，本条の下にある報告義務をサードパーティサービスプロバイダに対してアウトソースできる。そのようなアウトソースをする場合，当該金融機関は，インシデント報告の要件を満たすことに関し，全面的に責任を負い続ける。

Financial entities may outsource, in accordance with Union and national sectoral law, the reporting obligations under this Article to a third-party service provider. In case of such outsourcing, the financial entity remains fully responsible for the fulfilment of the incident reporting requirements.

6. 第 4 項に示す最初の通知を受領したとき及び各報告を受領したときは，職務権限のある当局は，当該受領者それぞれの職務権限をしかるべく基礎として，以下の受領者に対し，適時の態様で，ICT と関連する大きなインシデントの詳細情報を提供する：

Upon receipt of the initial notification and of each report referred to in paragraph 4, the competent authority shall, in a timely manner, provide details of the major ICT-related incident to the following recipients based, as applicable, on their respective competences:

(a) EBA，ESMA または EIOPA；

EBA, ESMA or EIOPA;

(b) 第 2 条第 1 項(a)，(b)及び(d)に示す金融機関の場合，ECB；

the ECB, in the case of financial entities referred to in Article 2(1), points (a), (b) and (d);

(c) 職務権限のある当局，指令(EU) 2022/2555 に従って指定されまたは設けられた単一連絡部局またはCSIRTs；

the competent authorities, single points of contact or CSIRTs designated or established in accordance with Directive (EU) 2022/2555;

(d) 欧州議会及び理事会の規則(EU) No 806/2014[37]の第 7 条第 2 項に示す法主体との関係においては，また，そのような詳細情報が指令 2014/59/EU の第 2 条第 1 項第 35 号の意味における不可欠な機能を確保することに対するリスクを呈するインシデントと関係するものであるときは，規則(EU) No 806/2014 の第 7 条第 4 項(b)及び第 5 項に示す法主体及びグループとの関係においては，指令 2014/59/EU の第 3 条に示す破綻処理当局及び単一破綻処理委員会（SRB）；並びに

the resolution authorities, as referred to in Article 3 of Directive 2014/59/EU, and the Single Resolution Board (SRB) with respect to entities referred to in Article 7(2) of Regulation (EU) No 806/2014 of the European Parliament and of the Council[37], and with respect to entities and groups referred to in Article 7(4)(b) and (5) of Regulation (EU) No 806/2014 if such details concern incidents that pose a risk to ensuring critical functions within the meaning of Article 2(1), point (35), of Directive 2014/59/EU; and

(e) それら以外の，国内法の下にある適格な行政機関。

other relevant public authorities under national law.

7. 第 6 項に従った情報の受領の後，EBA，ESMA または EIOPA 及び ECB は，ENISA からの意見聴取を経た上で，かつ，適格な職務権限のある当局と協力して，その ICT と関連する大きなインシデントが他の構成国の職務権限のある当局にとって適格であるか否かを評価する。その評価の後，EBA，ESMA または EIOPA は，可能な限り速やかに，他の構成国の適格な職務権限のある当局に対し，しかるべく通知する。ECB は，欧州中央銀行制度の構成員に対し，決済システムと関係する問題を通知する。その通知があったときは，職務権限のある当局は，しかるべく，金融システムの即時の安定性を保護するために必要となる全ての措置を講ずる。

Following receipt of information in accordance with paragraph 6, EBA, ESMA or EIOPA and the ECB, in consultation with ENISA and in cooperation with the relevant competent authority, shall assess whether the major ICT-

[37] 単一破綻処理の仕組み及び単一破綻処理基金の枠組み内において与信機関及び一定の投資会社の破綻処理のための統一的な規定及び統一的な手続を設ける並びに規則(EU) No 1093/2010 を改正する欧州議会及び理事会の 2014 年 7 月 15 日の規則(EU) No 806/2014 (OJ L 225, 30.7.2014, p. 1).
Regulation (EU) No 806/2014 of the European Parliament and of the Council of 15 July 2014 establishing uniform rules and a uniform procedure for the resolution of credit institutions and certain investment firms in the framework of a Single Resolution Mechanism and a Single Resolution Fund and amending Regulation (EU) No 1093/2010 (OJ L 225, 30.7.2014, p. 1).

related incident is relevant for competent authorities in other Member States. Following that assessment, EBA, ESMA or EIOPA shall, as soon as possible, notify relevant competent authorities in other Member States accordingly. The ECB shall notify the members of the European System of Central Banks on issues relevant to the payment system. Based on that notification, the competent authorities shall, where appropriate, take all of the necessary measures to protect the immediate stability of the financial system.

8. 証券集中保管機関がホスト構成国内において国境を越える大きな活動をもっている場合，ICT と関連する大きなインシデントがホスト構成国の金融市場にとって深刻な結果を生じさせ得る場合及び金融機関の監督と関連する職務権限のある当局間の協力協定が存在する場合においては，本条第 7 項による ESMA によって行われる通知は，ホスト構成国の適格な当局に対して ICT と関連する大きなインシデントの詳細情報を緊急に送信する職務権限のある当局の職責を妨げてはならない。

The notification to be done by ESMA pursuant to paragraph 7 of this Article shall be without prejudice to the responsibility of the competent authority to urgently transmit the details of the major ICT-related incident to the relevant authority in the host Member State, where a central securities depository has significant cross-border activity in the host Member State, the major ICT-related incident is likely to have severe consequences for the financial markets of the host Member State and where there are cooperation arrangements among competent authorities related to the supervision of financial entities.

第 20 条 報告の内容及び雛型の整合化

Article 20 **Harmonisation of reporting content and templates**

ESAs は，共同委員会を介して，かつ，ENISA 及び ECB からの意見聴取を経た上で，以下のものを策定する：

The ESAs, through the Joint Committee, and in consultation with ENISA and the ECB, shall develop:

(a) 以下のための共通の法制上の技術標準案：

common draft regulatory technical standards in order to:

(i) 第 18 条第 1 項の中で定められた基準を反映するため，及び，他の構成国に対する報告の適格性及び当該インシデントが運営管理または決済の安全性と関連する大きなインシデントを組成するか否かを判定するための細目事項のような別の構成要素を組込むため，ICT と関連する大きなインシデントの報告書の内容を定めること；

establish the content of the reports for major ICT-related incidents in order to reflect the criteria laid down in Article 18(1) and incorporate further elements, such as details for establishing the relevance of the reporting for other Member States and whether it constitutes a major operational or security payment-related

incident or not;

(ii) 最初の通知及び第 19 条第 4 項に示す各報告の期限を決定すること;

determine the time limits for the initial notification and for each report referred to in Article 19(4);

(iii) 大きなサイバー脅威に関する通知の内容を定めること。

establish the content of the notification for significant cyber threats.

それらの法制上の技術標準案を策定する際, ESAs は, 金融機関の規模及び全体的なリスクプロファイル, 並びに, 当該金融機関のサービス, 活動及び運営管理の性質, 規模及び複雑性を考慮に入れ, また, とりわけ, 本副項(a)(ii)の目的のために, 異なる期限が適切に反映され得ることを確保するという観点から, この規則及び指令(EU) 2022/2555 による ICT と関連するインシデントの報告への一貫性のあるアプローチを維持することを妨げることなく, 金融部門の特性を考慮に入れる。ESAs は, 同指令の文脈においてとられるアプローチから逸れる場合においては, しかるべく, その正当化事由を提供する。

When developing those draft regulatory technical standards, the ESAs shall take into account the size and the overall risk profile of the financial entity, and the nature, scale and complexity of its services, activities and operations, and in particular, with a view to ensuring that, for the purposes of this paragraph, point (a), point (ii), different time limits may reflect, as appropriate, specificities of financial sectors, without prejudice to maintaining a consistent approach to ICT-related incident reporting pursuant to this Regulation and to Directive (EU) 2022/2555. The ESAs shall, as applicable, provide justification when deviating from the approaches taken in the context of that Directive;

(b) ICT と関連する大きなインシデントを報告し及び大きなサイバー脅威を通知するための金融機関のための標準的な方式, 雛型及び手続を定めるための共通の実装技術標準案。

common draft implementing technical standards in order to establish the standard forms, templates and procedures for financial entities to report a major ICT-related incident and to notify a significant cyber threat.

ESAs は, 欧州委員会に対し, 2024 年 7 月 17 日までに, 第 1 副項(a)に示す共通の法制上の技術標準案及び第 1 副項(b)に示す共通の共通の実装技術標準案を提出する。

The ESAs shall submit the common draft regulatory technical standards referred to in the first paragraph, point (a), and the common draft implementing technical standards referred to in the first paragraph, point (b), to the Commission by 17 July 2024.

規則(EU) No 1093/2010, 規則(EU) No 1094/2010 及び規則(EU) No 1095/2010 の各第 10 条ないし第 14

条に従って第 1 項(a)に示す法制上の技術標準を採択することによってこの規則を補遺するための権限は，欧州委員会に対して与えられる。

Power is delegated to the Commission to supplement this Regulation by adopting the common regulatory technical standards referred to in the first paragraph, point (a), in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.

規則(EU) No 1093/2010，規則(EU) No 1094/2010 及び規則(EU) No 1095/2010 の各第 15 条に従って第 1 項(b)に示す共通の実装技術標準を採択するための権限は，欧州委員会に対して与えられる。

Power is conferred on the Commission to adopt the common implementing technical standards referred to in the first paragraph, point (b), in accordance with Article 15 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.

第 21 条 ICT と関連する大きなインシデントの報告の集中化

Article 21 **Centralisation of reporting of major ICT-related incidents**

1. ESAs は，共同委員会を介して，かつ，ECB 及び ENISA から意見聴取した上で，金融機関からの ICT と関連する大きなインシデントの報告のための単一 EU ハブの設置によりインシデント報告の更なる集中化の実現可能性を評価する共同報告書を準備する。その共同報告書は，ICT と関連するインシデントの報告の流れを促進し，関係する費用を削減し，かつ，監督上の収斂を拡大するという観点からテーマ別の分析を支えるための方途を拓くものとする。

The ESAs, through the Joint Committee, and in consultation with the ECB and ENISA, shall prepare a joint report assessing the feasibility of further centralisation of incident reporting through the establishment of a single EU Hub for major ICT-related incident reporting by financial entities. The joint report shall explore ways to facilitate the flow of ICT-related incident reporting, reduce associated costs and underpin thematic analyses with a view to enhancing supervisory convergence.

2. 第 1 項に示す共同報告書は，少なくとも，以下の構成要素を包含する:

The joint report referred to in paragraph 1 shall comprise at least the following elements:

(a) 単一 EU ハブの設置の前提条件;

prerequisites for the establishment of a single EU Hub;

(b) 機微の情報の高度の集中化と関係するリスクを含め，受益，制限及びリスク;

benefits, limitations and risks, including risks associated with the high concentration of sensitive information;

(c) 他の適格な報告制度と関連する相互運用性を確保するために必要となる実現能力；

the necessary capability to ensure interoperability with regard to other relevant reporting schemes;

(d) 運営管理上のマネジメントの諸要素；

elements of operational management;

(e) 構成員となる条件；

conditions of membership;

(f) 単一 EU ハブにアクセスするための，金融機関及び職務権限のある国内機関のための技術上の手立て；

technical arrangements for financial entities and national competent authorities to access the single EU Hub;

(g) 必要な専門知識を含め，単一 EU ハブを支える運営管理プラットフォームの設置によってかかる費用額の事前評価。

a preliminary assessment of financial costs incurred by setting-up the operational platform supporting the single EU Hub, including the requisite expertise.

3. ESAs は，欧州議会，理事会及び欧州委員会に対し，2025 年 1 月 17 日までに，第 1 項に示す報告書を提出する。

The ESAs shall submit the report referred to in paragraph 1 to the European Parliament, to the Council and to the Commission by 17 January 2025.

第 22 条 監督上のフィードバック

Article 22 **Supervisory feedback**

1. 適用可能なときは，国内法に従って，指令(EU) 2022/2555 の下にある CSIRTs から提供され得る技術的な入力，助言または解消策及びその後の事後対応を妨げることなく，職務権限のある当局は，第 19 条第 4 項に示す最初の通知を受領したとき及び各報告を受領したときは，その受領を連絡し，かつ，それが実現可能なときは，とりわけ，類似の脅威に関する適格で匿名化された情報と知識を利用できるようにすることによって，当該金融機関に対し，適時の態様で，適格かつ比例的なフィードバックまたは高度な運用指針を提供でき，また，当該金融機関の側で適用される解消策及び金融部門にわたる負の影響をミニマム化し及び緩和するための方法を討議できる。受領した監督上のフ

ィードバックを妨げることなく，金融機関は，第 19 条第 1 項により報告された ICT と関連するインシデントの取扱いに関し及びその結果として生ずることに関し，全面的に責任を負い続ける。

Without prejudice to the technical input, advice or remedies and subsequent follow-up which may be provided, where applicable, in accordance with national law, by the CSIRTs under Directive (EU) 2022/2555, the competent authority shall, upon receipt of the initial notification and of each report as referred to in Article 19(4), acknowledge receipt and may, where feasible, provide in a timely manner relevant and proportionate feedback or high-level guidance to the financial entity, in particular by making available any relevant anonymised information and intelligence on similar threats, and may discuss remedies applied at the level of the financial entity and ways to minimise and mitigate adverse impact across the financial sector. Without prejudice to the supervisory feedback received, financial entities shall remain fully responsible for the handling and for consequences of the ICT-related incidents reported pursuant to Article 19(1).

2. ESAs は，共同委員会を介して，匿名化及び集約化ベースで，年次で，ICT と関連する大きなインシデントに関して報告する。その報告書の詳細内容は，少なくとも，ICT と関連する大きなインシデントの数，そのインシデントの性質及び金融機関の運営管理または顧客に対するそのインシデントの影響，講じられた是正の活動及びかかった費用を列挙して，第 19 条第 6 項に従って，職務権限のある当局から提供される。

The ESAs shall, through the Joint Committee, on an anonymised and aggregated basis, report yearly on major ICT-related incidents, the details of which shall be provided by competent authorities in accordance with Article 19(6), setting out at least the number of major ICT-related incidents, their nature and their impact on the operations of financial entities or clients, remedial actions taken and costs incurred.

ESAs は，警告を発し，また，ICT の脅威と脆弱性の分析を支えるための高度の統計を作成する。

The ESAs shall issue warnings and produce high-level statistics to support ICT threat and vulnerability assessments.

第 23 条　与信機関，決済機関，口座情報サービスプロバイダ及び電子マネー機関と関係する運営管理または決済の安全性と関連するインシデント

Article 23　**Operational or security payment-related incidents concerning credit institutions, payment institutions, account information service providers, and electronic money institutions**

本章の中で定められた要件は，当該インシデントが与信機関，決済機関，口座情報サービスプロバイダ及び電子マネー機関と関係するときは，運営管理または決済の安全性と関連するインシデントに対しても及び運営管理または決済の安全性と関連する大きなインシデントに対しても適用される。

The requirements laid down in this Chapter shall also apply to operational or security payment-related incidents and to major operational or security payment-related incidents, where they concern credit institutions, payment institutions, account information service providers, and electronic money institutions.

第 IV 章　デジタル運営管理上の回復力試験
CHAPTER IV **Digital operational resilience testing**

第 24 条　デジタル運営管理上の回復力試験の遂行に関する総則的な要件
Article 24 **General requirements for the performance of digital operational resilience testing**

1. ICT と関連するインシデントを取扱うための準備態勢を評価する目的，デジタル運営管理上の回復力における弱点，欠陥及び間隙を識別する目的並びに是正の方策を迅速に実装する目的のために，マイクロ企業以外の金融機関は，第 4 条第 2 項の中で定められた基準を考慮に入れ，かつ，第 6 条に示す ICT リスクマネジメント枠組みの不可欠な部分として，良好かつ包括的なデジタル運営管理上の回復力試験計画を策定し，維持し及び見直す。

   For the purpose of assessing preparedness for handling ICT-related incidents, of identifying weaknesses, deficiencies and gaps in digital operational resilience, and of promptly implementing corrective measures, financial entities, other than microenterprises, shall, taking into account the criteria set out in Article 4(2), establish, maintain and review a sound and comprehensive digital operational resilience testing programme as an integral part of the ICT risk-management framework referred to in Article 6.

2. デジタル運営管理上の回復力試験計画は，第 25 条及び第 26 条に従って適用される範囲内の評価，試験，手法，実務及びツールを含める。

   The digital operational resilience testing programme shall include a range of assessments, tests, methodologies, practices and tools to be applied in accordance with Articles 25 and 26.

3. 本条第 1 項に示すデジタル運営管理上の回復力試験計画を実行する際，マイクロ企業以外の金融機関は，第 4 条第 2 項の中で定められた基準を考慮に入れ，ICT リスクの進化しつつある全体像，関係する金融機関が晒されているまたは晒されたかもしれない特定のリスク，情報資産の不可欠性及び提供されるサービスの不可欠性並びに当該金融機関が適切であると考えるその他の要因を適正に判断するリスクベースのアプローチに従う。

   When conducting the digital operational resilience testing programme referred to in paragraph 1 of this Article, financial entities, other than microenterprises, shall follow a risk-based approach taking into account the criteria set out in Article 4(2) duly considering the evolving landscape of ICT risk, any specific risks to which the financial entity concerned is or might be exposed, the criticality of information assets and of services provided, as well as any other factor the financial entity deems appropriate.

4. マイクロ企業以外の金融機関は，内部者であるか外部者であるかに拘わらず，試験が独立の関与者によって実施されることを確保する。試験が内部の試験担当者によって実施される場合，金融機関は，十分な資源を投入し，かつ，試験の設計段階及び実行段階を通じて，利益相反が避けられることを確保する。

Financial entities, other than microenterprises, shall ensure that tests are undertaken by independent parties, whether internal or external. Where tests are undertaken by an internal tester, financial entities shall dedicate sufficient resources and ensure that conflicts of interest are avoided throughout the design and execution phases of the test.

5. マイクロ企業以外の金融機関は，試験の遂行を通じて明らかにされた全ての問題の優先度を決め，それを分類し及び解消する手続及び基本方針を定め，かつ，特定された全ての弱点，欠陥または間隙が全面的に対処されていることを確認するための内部の検証手法を定める。

Financial entities, other than microenterprises, shall establish procedures and policies to prioritise, classify and remedy all issues revealed throughout the performance of the tests and shall establish internal validation methodologies to ascertain that all identified weaknesses, deficiencies or gaps are fully addressed.

6. マイクロ企業以外の金融機関は，少なくとも年次で，不可欠な機能または重要な機能を支える全ての ICT システム及びアプリケーションに関し，適切な試験が実行されることを確保する。

Financial entities, other than microenterprises, shall ensure, at least yearly, that appropriate tests are conducted on all ICT systems and applications supporting critical or important functions.

第 25 条 ICT のツール及びシステムの試験

Article 25 **Testing of ICT tools and systems**

1. 第 24 条に示すデジタル運営管理上の回復力試験計画は，脆弱性評価及び脆弱性スキャン，オープンソース分析，ネットワークセキュリティ評価，ギャップ分析，物理的なセキュリティの見直し，アンケート及びスキャニングのソフトウェアソリューション，それが実施可能なときはソースコードの見直し，シナリオベースの試験，互換性の試験，遂行能力の試験，エンドツーエンドの試験並びにペネトレーション試験のような，適切な試験の実行を，第 4 条第 2 項の中で定められた基準に従って定める。

The digital operational resilience testing programme referred to in Article 24 shall provide, in accordance with the criteria set out in Article 4(2), for the execution of appropriate tests, such as vulnerability assessments and scans, open source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews where feasible, scenario-based tests, compatibility testing, performance testing, end-to-end testing and penetration testing.

2. 証券集中保管機関及び中央清算機関は，金融機関の不可欠な機能または重要な機能を支える新たなまたは既存のアプリケーションとインフラコンポーネント及び ICT サービスの配置または再配置の前に，脆弱性評価を遂行する。

Central securities depositories and central counterparties shall perform vulnerability assessments before any deployment or redeployment of new or existing applications and infrastructure components, and ICT services supporting critical or

important functions of the financial entity.

3. マイクロ企業は，リスクベースのアプローチを ICT 試験の戦略的な計画に結びつけることによって，一方における，本条の中で定められた ICT 試験のために割当てられる資源の規模及び時間と，他方における，緊急性，リスクのタイプ，情報資産の不可欠性及び提供されるサービスの不可欠性，並びに，その金融機関の計算されたリスクをとる能力を含め，その他の適格な要因との間のバランスのとれたアプローチを維持する必要性を適正に判断することによって，第 1 項に示す試験を遂行する。

Microenterprises shall perform the tests referred to in paragraph 1 by combining a risk-based approach with a strategic planning of ICT testing, by duly considering the need to maintain a balanced approach between the scale of resources and the time to be allocated to the ICT testing provided for in this Article, on the one hand, and the urgency, type of risk, criticality of information assets and of services provided, as well as any other relevant factor, including the financial entity's ability to take calculated risks, on the other hand.

第 26 条　TLPT を基礎とする ICT のツール，システム及びプロセスの高度な試験

Article 26　**Advanced testing of ICT tools, systems and processes based on TLPT**

1. 第 16 条第 1 項第 1 副項に示す法主体以外の金融機関及び本条第 8 項第 3 副項に従って識別されるマイクロ企業以外の金融機関は，少なくとも 3 年毎に，TLPT による高度な試験を実行する。当該金融機関のリスクプロファイルを基礎として，かつ，運営管理上の状況を考慮に入れた上で，職務権限のある当局は，それが必要なときは，金融機関に対し，その頻度を減らしまたは増やすことを要求できる。

Financial entities, other than entities referred to in Article 16(1), first subparagraph, and other than microenterprises, which are identified in accordance with paragraph 8, third subparagraph, of this Article, shall carry out at least every 3 years advanced testing by means of TLPT. Based on the risk profile of the financial entity and taking into account operational circumstances, the competent authority may, where necessary, request the financial entity to reduce or increase this frequency.

2. 個々の脅威ベースのペネトレーション試験は，金融機関の幾つかのまたは全ての不可欠な機能または重要な機能を包摂するものとし，かつ，そのような機能を支えるライブプロダクションシステム上で遂行される。

Each threat-led penetration test shall cover several or all critical or important functions of a financial entity, and shall be performed on live production systems supporting such functions.

金融機関は，ICT サードパーティサービスプロバイダに対してアウトソースされまたは ICT サードパーティサービスプロバイダとの間で契約された不可欠な機能または重要な機能を支える ICT のシステ

ム，手続及び技術を含め，不可欠な機能または重要な機能及び ICT サービスを支える全ての適格な基盤となる ICT のシステム，手続及び技術を識別する。

Financial entities shall identify all relevant underlying ICT systems, processes and technologies supporting critical or important functions and ICT services, including those supporting the critical or important functions which have been outsourced or contracted to ICT third-party service providers.

金融機関は，どの不可欠な機能または重要な機能が TLPT に包摂される必要があるかを評価する。その評価結果は，TLPT の細密な適用範囲を定め，かつ，職務権限のある当局によって検証される。

Financial entities shall assess which critical or important functions need to be covered by the TLPT. The result of this assessment shall determine the precise scope of TLPT and shall be validated by the competent authorities.

3. ICT サードパーティサービスプロバイダが TLPT の適用範囲に含まれている場合，当該金融機関は，その TLPT へのそのような ICT サードパーティサービスプロバイダの参加を確保するために必要となる方策及び安全確保をとり，かつ，常時，この規則の遵守を確保することの全面的な責任を保持する。

Where ICT third-party service providers are included in the scope of TLPT, the financial entity shall take the necessary measures and safeguards to ensure the participation of such ICT third-party service providers in the TLPT and shall retain at all times full responsibility for ensuring compliance with this Regulation.

4. 第 2 項第 1 副項及び第 2 副項を妨げることなく，第 3 項に示す TLPT への ICT サードパーティサービスプロバイダの参加が当該 ICT サードパーティサービスプロバイダからこの規則の適用範囲外にある法主体である顧客に対して供給されるサービスの品質もしくは安全性に対する負の影響またはそのようなサービスと関連するデータの機密性に対する負の影響をもつと合理的に予測されるときは，当該金融機関及び当該 ICT サードパーティサービスプロバイダは，当該 ICT サードパーティサービスプロバイダが，指定された 1 つの金融機関の指揮の下で，ICT サービスを提供している複数の金融機関が関与するプールされた TLPT（プールされた試験）を実行する目的のために，当該 ICT サードパーティサービスプロバイダが外部の試験担当者との間で直接に契約上の取決めに入ることを書面により合意できる。

Without prejudice to paragraph 2, first and second subparagraphs, where the participation of an ICT third-party service provider in the TLPT, referred to in paragraph 3, is reasonably expected to have an adverse impact on the quality or security of services delivered by the ICT third-party service provider to customers that are entities falling outside the scope of this Regulation, or on the confidentiality of the data related to such services, the financial entity and the ICT third-party service provider may agree in writing that the ICT third-party service provider directly enters into contractual arrangements with an external tester, for the purpose of conducting, under the direction of one designated financial entity, a pooled TLPT involving several financial entities (pooled testing) to which the ICT third-party service provider provides ICT services.

そのプールされた試験は，当該金融機関によってそれぞれの ICT サードパーティサービスプロバイダとの間で契約した不可欠な機能または重要な機能を支える適格な範囲内の ICT サービスを包摂する。プールされた試験は，そのプールされた試験に参加している金融機関によって実行された TLPT であると判断される。

That pooled testing shall cover the relevant range of ICT services supporting critical or important functions contracted to the respective ICT third-party service provider by the financial entities. The pooled testing shall be considered TLPT carried out by the financial entities participating in the pooled testing.

プールされた試験に参加している金融機関の数は，包摂されているサービスの複雑性とタイプを考慮に入れた上で，適正に算定される。

The number of financial entities participating in the pooled testing shall be duly calibrated taking into account the complexity and types of services involved.

5. 金融機関は，ICT サードパーティサービスプロバイダ及び試験担当者を含めるが職務権限のある当局は除外したその他の関与者と協力して，データに対する潜在的な影響のリスク，資産に対する毀損のリスク，不可欠な機能または重要な機能，サービスまたは運営管理に対する混乱のリスクを緩和するため，当該金融機関自身，当該金融機関の取引相手の側で，または，金融部門に対して，実効的なリスクマネジメントの管理策を適用する。

Financial entities shall, with the cooperation of ICT third-party service providers and other parties involved, including the testers but excluding the competent authorities, apply effective risk management controls to mitigate the risks of any potential impact on data, damage to assets, and disruption to critical or important functions, services or operations at the financial entity itself, its counterparts or to the financial sector.

6. 試験の最後において，報告書及び解消計画書が合意された後，金融機関，及び，それが適用可能なときは，外部の試験担当者は，第 9 項または第 10 項に従って指定された当局に対し，適格な判断結果の要旨，解消計画書及び諸要件に従って TLPT が実行されたことを示す文書を提供する。

At the end of the testing, after reports and remediation plans have been agreed, the financial entity and, where applicable, the external testers shall provide to the authority, designated in accordance with paragraph 9 or 10, a summary of the relevant findings, the remediation plans and the documentation demonstrating that the TLPT has been conducted in accordance with the requirements.

7. 当局は，職務権限のある当局の間において脅威ベースのペネトレーション試験の相互承認ができるようにするため，金融機関に対し，文書で証拠化されるものとして，諸要件に従ってその試験が遂行されたことを確認する証明書を提供する。金融機関は，適格な職務権限のある当局に対し，その証明書，適格な判断結果の要旨及び解消計画書を通知する。

Authorities shall provide financial entities with an attestation confirming that the test was performed in accordance with the requirements as evidenced in the documentation in order to allow for mutual recognition of threat led penetration tests between competent authorities. The financial entity shall notify the relevant competent authority of the attestation, the summary of the relevant findings and the remediation plans.

そのような証明書を妨げることなく，金融機関は，常時，第 4 項に示す試験の影響に関し全面的な責任を負い続ける。

Without prejudice to such attestation, financial entities shall remain at all times fully responsible for the impact of the tests referred to in paragraph 4.

8. 金融機関は，第 27 条に従って TLPT を実施する目的のために，試験担当者と契約する。TLPT を実施する目的のために金融機関が内部の試験担当者を用いる場合，当該金融機関は，3 回の試験毎に外部の試験担当者と契約する。

Financial entities shall contract testers for the purposes of undertaking TLPT in accordance with Article 27. When financial entities use internal testers for the purposes of undertaking TLPT, they shall contract external testers every three tests.

規則(EU) No 1024/2013 の第 6 条第 4 項に従って大きいと分類されている与信機関は，第 27 条第 1 項(a)ないし(e)に従って，外部の試験のみを用いる。

Credit institutions that are classified as significant in accordance with Article 6(4) of Regulation (EU) No 1024/2013, shall only use external testers in accordance with Article 27(1), points (a) to (e).

職務権限のある当局は，以下の評価を基礎として，第 4 条第 2 項の中で定められた基準を考慮に入れた上で TLPT を遂行することが要求される金融機関を識別する:

Competent authorities shall identify financial entities that are required to perform TLPT taking into account the criteria set out in Article 4(2), based on an assessment of the following:

(a) 影響と関連する要因，とりわけ，提供されるサービス及び当該金融機関によって行われる活動が金融部門に影響する範囲;

impact-related factors, in particular the extent to which the services provided and activities undertaken by the financial entity impact the financial sector;

(b) しかるべく，欧州連合レベルまたは国内レベルにおける当該金融機関のシステミックな性格を含め，あり得る金融の安定上の懸念;

possible financial stability concerns, including the systemic character of the financial entity at Union or national level, as applicable;

(c) 個別の ICT リスクプロファイル，当該金融機関の ICT 成熟度のレベルまたは関与する技術上の特性。

specific ICT risk profile, level of ICT maturity of the financial entity or technology features involved.

9. 構成国は，国内レベルの金融部門において TLPT と関連する事項に関して職責を負う金融部門の単一の行政機関を指定し，かつ，その行政機関に対し，その点に関する全ての職務権限及び職務を委任できる。

Member States may designate a single public authority in the financial sector to be responsible for TLPT-related matters in the financial sector at national level and shall entrust it with all competences and tasks to that effect.

10. 本条第 9 項に従った指定がない場合において，かつ，TLPT を遂行することが要求される金融機関を識別する権限を妨げることなく，職務権限のある当局は，本条及び第 27 条に示す職務の一部または全部の実行を，金融部門の別の国内当局に委任できる。

In the absence of a designation in accordance with paragraph 9 of this Article, and without prejudice to the power to identify the financial entities that are required to perform TLPT, a competent authority may delegate the exercise of some or all of the tasks referred to in this Article and Article 27 to another national authority in the financial sector.

11. ESAs は，ECB と合意した上で，以下のことの細目を別途定めるため，TIBER-EU 枠組みに従って，共同の法制上の技術標準案を策定する：

The ESAs shall, in agreement with the ECB, develop joint draft regulatory technical standards in accordance with the TIBER-EU framework in order to specify further:

(a) 第 8 項第 2 副項の適用の目的のために用いられる基準；

the criteria used for the purpose of the application of paragraph 8, second subparagraph;

(b) 内部の試験担当者の利用を規律する要件及び技術標準；

the requirements and standards governing the use of internal testers;

(c) 以下のこととの関係における要件；

the requirements in relation to:

(i) 第 2 項に示す TLPT の適用範囲;

the scope of TLPT referred to in paragraph 2;

(ii) 試験プロセスの個々の特定のフェーズが依るべき試験の手法及びアプローチ;

the testing methodology and approach to be followed for each specific phase of the testing process;

(iii) 試験の結果, 終了及び解消の各段階;

the results, closure and remediation stages of the testing;

(d) 複数の構成国内で運営管理する金融機関という文脈において, 金融副部門または地域金融市場の特性に対応するための適切なレベルの監督上の包摂と柔軟な実装ができるようにするための, 監督のタイプ及びそれ以外の TLPT の実装のため及び同試験の相互承認の促進のために必要となる適格な協力のタイプ。

the type of supervisory and other relevant cooperation which are needed for the implementation of TLPT, and for the facilitation of mutual recognition of that testing, in the context of financial entities that operate in more than one Member State, to allow an appropriate level of supervisory involvement and a flexible implementation to cater for specificities of financial sub-sectors or local financial markets.

それらの法制上の技術標準案を策定する際, ESAs は, 異なる金融サービス諸部門にわたる活動の独特の性質から生ずる特性を適正に考慮に入れる。

When developing those draft regulatory technical standards, the ESAs shall give due consideration to any specific feature arising from the distinct nature of activities across different financial services sectors.

ESAs は, 欧州委員会に対し, 2024 年 7 月 17 日までに, それらの法制上の技術標準案を提出する。

The ESAs shall submit those draft regulatory technical standards to the Commission by 17 July 2024.

規則(EU) No 1093/2010, 規則(EU) No 1094/2010 及び規則(EU) No 1095/2010 の各第 10 条ないし第 14 条に従って第 1 副項に示す法制上の技術標準を採択することによってこの規則を補遺するための権限は, 欧州委員会に対して与えられる。

Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in the first subparagraph in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.

第 27 条 TLPT の実行のための試験担当者の要件

Article 27 **Requirements for testers for the carrying out of TLPT**

1. 金融機関は，TLPT を実行するために，以下のとおりの試験担当者のみを用いる：

Financial entities shall only use testers for the carrying out of TLPT, that:

(a) 最高度の適合性と良い評判をもつ者であり；

are of the highest suitability and reputability;

(b) 技術上及び組織上の能力を保有しており，かつ，脅威情報，ペネトレーション試験及びレッドチーム試験における個別の専門知識があることを示しており；

possess technical and organisational capabilities and demonstrate specific expertise in threat intelligence, penetration testing and red team testing;

(c) 構成国の認証組織から認証を受けており，または，公式の行動準則もしくは倫理枠組みを遵守しており；

are certified by an accreditation body in a Member State or adhere to formal codes of conduct or ethical frameworks;

(d) 当該金融機関の機密情報の適正な保護及び当該金融機関の事業遂行上のリスクの解消を含め，TLPT を実行することと関連するリスクの良好なマネジメントとの関係において，独立性の保証または監査報告書を提供しており；

provide an independent assurance, or an audit report, in relation to the sound management of risks associated with the carrying out of TLPT, including the due protection of the financial entity's confidential information and redress for the business risks of the financial entity;

(e) 不正行為及び過失行為のリスクに対するものを含め，適格な専門家損害賠償保険の適正かつ全面的な適用対象となっていること。

are duly and fully covered by relevant professional indemnity insurances, including against risks of misconduct and negligence.

2. 内部の試験担当者を用いる場合，金融機関は，第 1 項の要件に加え，以下の条件に適合していることを確保する。

When using internal testers, financial entities shall ensure that, in addition to the requirements in paragraph 1, the following conditions are met:

(a) 適格な職務権限のある当局によってまたは第 26 条第 9 項及び第 10 項に従って指定された単一の行政機関によって，そのように用いることが承認されたこと；

such use has been approved by the relevant competent authority or by the single public authority designated in accordance with Article 26(9) and (10);

(b) 当該金融機関が十分な専用の資源をもっていること及び当該試験の設計段階及び実行段階を通じて利益相反が避けられていることが確保されていることを，適格な職務権限のある当局が確認したこと；かつ

the relevant competent authority has verified that the financial entity has sufficient dedicated resources and ensured that conflicts of interest are avoided throughout the design and execution phases of the test; and

(c) 脅威情報の提供者が当該金融機関との関係で外部者であること。

the threat intelligence provider is external to the financial entity.

3. 金融機関は，外部の試験担当者との間で締結される契約が TLPT の結果の良好なマネジメントを要求していることを確保し，かつ，生成，記録保存，集約，作成，報告，通信または破壊を含め，その TLPT の結果を処理するデータが当該金融機関に対してリスクをつくり出さないことを確保する。

Financial entities shall ensure that contracts concluded with external testers require a sound management of the TLPT results and that any data processing thereof, including any generation, store, aggregation, draft, report, communication or destruction, do not create risks to the financial entity.

第 V 章 ICT サードパーティリスクの取扱い
CHAPTER V Managing of ICT third-party risk

第 I 節 ICT サードパーティリスクの良好なマネジメントのための鍵となる基本原則
Section I Key principles for a sound management of ICT third-party risk

第 28 条 総則的な基本原則
Article 28 General principles

1. 金融機関は，第 6 条第 1 項に示す当該金融機関の ICT リスクマネジメント枠組み内にある ICT リスクの不可欠なコンポーネントとして，かつ，以下の基本原則に従って，ICT サードパーティリスクを取扱う:

Financial entities shall manage ICT third-party risk as an integral component of ICT risk within their ICT risk management framework as referred to in Article 6(1), and in accordance with the following principles:

(a) 当該金融機関の事業上の運営管理を走らせるために ICT サービスの利用のための契約上の取決めを設けている金融機関は，常時，この規則及び適用可能な金融サービス法の下にある全ての義務の遵守及びその履行に関し，全面的に責任を負い続ける;

financial entities that have in place contractual arrangements for the use of ICT services to run their business operations shall, at all times, remain fully responsible for compliance with, and the discharge of, all obligations under this Regulation and applicable financial services law;

(b) 金融機関の ICT サードパーティリスクのマネジメントは，以下のことを考慮に入れた上で，比例性の原則に照らして実装される:

financial entities' management of ICT third-party risk shall be implemented in light of the principle of proportionality, taking into account:

(i) ICT と関連する依存性の性質，規模，複雑性及び重要性;

the nature, scale, complexity and importance of ICT-related dependencies,

(ii) 当該それぞれのサービス，プロセスまたは機能の不可欠性または重要性，並びに，個々の及びグループレベルの金融サービス及び金融活動の継続性及び可用性に対する潜在的な影響を考慮に入れた上で，ICT サードパーティサービスプロバイダとの間で締結された ICT サービスの利用に関する契約上の取決めから生ずるリスク。

the risks arising from contractual arrangements on the use of ICT services concluded with ICT third-party

service providers, taking into account the criticality or importance of the respective service, process or function, and the potential impact on the continuity and availability of financial services and activities, at individual and at group level.

2. 当該金融機関の ICT リスクマネジメント枠組みの一部として，第 16 条第 1 項第 1 副項に示す法主体以外の金融機関及びマイクロ企業以外の金融機関は，それが適用可能なときは，第 6 条第 9 項に示すマルチベンダ戦略を考慮に入れた上で，ICT サードパーティリスクに関する戦略を採択しかつ定期的に見直す。ICT サードパーティリスクに関する戦略は，ICT サードパーティサービスプロバイダから提供される不可欠な機能または重要な機能を支える ICT サービスの利用に関する基本方針を含めるものとし，かつ，個別ベースで，また，それが適格なときは，サブ連結ベース及び連結ベースで適用される。経営陣は，金融機関の全体的なリスクプロファイル並びに事業上のサービスの規模及び複雑性の評価を基礎として，定期的に，不可欠な機能または重要な機能を支える ICT サービスの利用に関する契約上の取決めとの関係において特定されたリスクを見直す。

As part of their ICT risk management framework, financial entities, other than entities referred to in Article 16(1), first subparagraph, and other than microenterprises, shall adopt, and regularly review, a strategy on ICT third-party risk, taking into account the multi-vendor strategy referred to in Article 6(9), where applicable. The strategy on ICT third-party risk shall include a policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers and shall apply on an individual basis and, where relevant, on a sub-consolidated and consolidated basis. The management body shall, on the basis of an assessment of the overall risk profile of the financial entity and the scale and complexity of the business services, regularly review the risks identified in respect to contractual arrangements on the use of ICT services supporting critical or important functions.

3. 当該金融機関の ICT リスクマネジメント枠組みの一部として，金融機関は，法主体レベルで並びにサブ連結レベル及び連結レベルで，ICT サードパーティサービスプロバイダから提供される ICT サービスの利用に関する全ての契約上の取決めとの関係において，情報の登録簿を維持管理しかつアップデートする。

As part of their ICT risk management framework, financial entities shall maintain and update at entity level, and at sub-consolidated and consolidated levels, a register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers.

第 1 副項に示す契約上の取決めは，不可欠な機能または重要な機能を支える ICT サービスの利用に適用されるものとそうではないものとを区別して，適切に文書化される。

The contractual arrangements referred to in the first subparagraph shall be appropriately documented, distinguishing between those that cover ICT services supporting critical or important functions and those that do not.

金融機関は，少なくとも年次で，職務権限のある当局に対し，ICT サービスの利用に関する新たな取決めの数，ICT サードパーティサービスプロバイダの類型，契約上の取決めのタイプ並びに提供さ

れている ICT サービス及び機能に関し，報告する。

Financial entities shall report at least yearly to the competent authorities on the number of new arrangements on the use of ICT services, the categories of ICT third-party service providers, the type of contractual arrangements and the ICT services and functions which are being provided.

金融機関は，職務権限のある当局の要求に応じて，職務権限のある当局に対し，金融機関の実効的な監督を実現可能にするために必要であると考えられる情報に沿って，情報の登録簿全部を利用できるようにし，または，要求に応じて，登録簿の特定の箇所を利用できるようにする。

Financial entities shall make available to the competent authority, upon its request, the full register of information or, as requested, specified sections thereof, along with any information deemed necessary to enable the effective supervision of the financial entity.

金融機関は，職務権限のある当局に対し，不可欠な機能または重要な機能を支える ICT サービスの利用に関する計画中の契約上の取決めに関し，及び，ある機能が不可欠または重要となった場合において，適時の態様で連絡する。

Financial entities shall inform the competent authority in a timely manner about any planned contractual arrangement on the use of ICT services supporting critical or important functions as well as when a function has become critical or important.

4. ICT サービスの利用に関する契約上の取決めを締結する前に，金融機関は:

Before entering into a contractual arrangement on the use of ICT services, financial entities shall:

(a) 当該契約上の取決めが不可欠な機能または重要な機能を支える ICT サービスの利用を包摂しているか否かを評価し;

assess whether the contractual arrangement covers the use of ICT services supporting a critical or important function;

(b) 契約締結のための監督上の条件に適合しているか否かを評価し;

assess if supervisory conditions for contracting are met;

(c) そのような契約上の取決めが第 29 条に示す ICT 集中化リスクを増強することに貢献するかもしれないという可能性を含め，当該契約上の取決めとの関係において，全ての適格なリスクを特定しかつ評価し;

identify and assess all relevant risks in relation to the contractual arrangement, including the possibility that such contractual arrangement may contribute to reinforcing ICT concentration risk as referred to in Article 29;

(d) 予定している ICT サードパーティサービスプロバイダに関する全てのデューデリジェンスを尽くし，かつ，その選定及び評価の過程を通じて，当該 ICT サードパーティサービスプロバイダが適切であることを確保し；

undertake all due diligence on prospective ICT third-party service providers and ensure throughout the selection and assessment processes that the ICT third-party service provider is suitable;

(e) 当該契約上の取決めが生じさせるかもしれない利益相反を識別し及び評価する。

identify and assess conflicts of interest that the contractual arrangement may cause.

5. 金融機関は，適切な情報セキュリティ上の技術標準を遵守する ICT サードパーティサービスプロバイダとの間においてのみ，契約上の取決めを締結できる。当該契約上の取決めが不可欠な機能または重要な機能に関するものであるときは，金融機関は，当該取決めを締結する前に，最新でありかつ最高度の品質の情報セキュリティ上の技術標準を ICT サードパーティサービスプロバイダによって使用されていることを適切に判断する。

Financial entities may only enter into contractual arrangements with ICT third-party service providers that comply with appropriate information security standards. When those contractual arrangements concern critical or important functions, financial entities shall, prior to concluding the arrangements, take due consideration of the use, by ICT third-party service providers, of the most up-to-date and highest quality information security standards.

6. ICT サードパーティサービスプロバイダに対するアクセスの権利，検査の権利及び監査の権利を行使する前に，金融機関は，リスクベースのアプローチを基礎として，そのような監査基準の使用と導入に関する監督上の指示に沿って，共通に承認された監査基準に依ることを通じて，監査と検査の頻度及び監査される分野を事前に決定する。

In exercising access, inspection and audit rights over the ICT third-party service provider, financial entities shall, on the basis of a risk-based approach, pre-determine the frequency of audits and inspections as well as the areas to be audited through adhering to commonly accepted audit standards in line with any supervisory instruction on the use and incorporation of such audit standards.

ICT サービスの利用に関して ICT サードパーティサービスプロバイダとの間で締結された契約上の取決めが高度の技術上の複雑性を伴うときは，金融機関は，内部であるか外部であるかを問わず，監査者または監査者のプールが，適格な監査及び評価を実効的に遂行するための適切な技能及び知識を保有していることを確認する。

Where contractual arrangements concluded with ICT third-party service providers on the use of ICT services entail high technical complexity, the financial entity shall verify that auditors, whether internal or external, or a pool of auditors, possess appropriate skills and knowledge to effectively perform the relevant audits and assessments.

7. 金融機関は，ICT サービスの利用に関する契約上の取決めが，以下のいずれかの状況の下においては終了となり得ることを確保する：

Financial entities shall ensure that contractual arrangements on the use of ICT services may be terminated in any of the following circumstances:

(a) 当該 ICT サードパーティサービスプロバイダによる適用可能な法律，規則または契約条件の重大な違反；

significant breach by the ICT third-party service provider of applicable laws, regulations or contractual terms;

(b) 当該取決めに対しまたは当該 ICT サードパーティサービスプロバイダの状況に対して影響を与える実質的な変更を含め，ICT サードパーティリスクの監視を通じて識別された，契約上の取決めを介して提供される機能の遂行能力を変えることが可能であると判断される状況；

circumstances identified throughout the monitoring of ICT third-party risk that are deemed capable of altering the performance of the functions provided through the contractual arrangement, including material changes that affect the arrangement or the situation of the ICT third-party service provider;

(c) 証拠によって確認された，当該 ICT サードパーティサービスプロバイダの全体的な ICT リスクマネジメントと関係し，かつ，とりわけ，個人データであるかもしくはそれ以外の機微のデータであるかまたは非個人データであるかを問わず，データの可用性，真正性，完全性及び機密性をその ICT サードパーティサービスプロバイダが確保する方法における，ICT サードパーティサービスプロバイダの弱点；

ICT third-party service provider's evidenced weaknesses pertaining to its overall ICT risk management and in particular in the way it ensures the availability, authenticity, integrity and, confidentiality, of data, whether personal or otherwise sensitive data, or non-personal data;

(d) それぞれの契約上の取決めと関連する条件または状況の結果として，職務権限のある当局が当該金融機関を実効的に監督できなくなった場合。

where the competent authority can no longer effectively supervise the financial entity as a result of the conditions of, or circumstances related to, the respective contractual arrangement.

8. 不可欠な機能または重要な機能を支える ICT サービスに関し，金融機関は，出口戦略を設ける。そ

の出口戦略は，ICT サードパーティサービスプロバイダの側において生ずるかもしれないリスク，とりわけ，その ICT サードパーティサービスプロバイダの側においてあり得る失敗，提供される ICT サービスの品質の低下，ICT サービスの不適切な提供もしくは不提供による事業上の混乱またはそれぞれの ICT サービスの適切かつ継続的な配置との関係において生ずる実質的なリスク，または，第 7 項の中で列挙されたいずれかの状況の下における ICT サードパーティサービスプロバイダとの間の契約上の取決めの終了を考慮に入れる。

For ICT services supporting critical or important functions, financial entities shall put in place exit strategies. The exit strategies shall take into account risks that may emerge at the level of ICT third-party service providers, in particular a possible failure on their part, a deterioration of the quality of the ICT services provided, any business disruption due to inappropriate or failed provision of ICT services or any material risk arising in relation to the appropriate and continuous deployment of the respective ICT service, or the termination of contractual arrangements with ICT third-party service providers under any of the circumstances listed in paragraph 7.

金融機関は，以下のことがなく，契約上の取決めを終了させることができることを確保する：

Financial entities shall ensure that they are able to exit contractual arrangements without:

(a) 当該金融機関の事業活動の混乱，

disruption to their business activities,

(b) 法制上の要件の遵守を制限すること，

limiting compliance with regulatory requirements,

(c) 顧客に対して提供されるサービスの継続性及び品質の低下。

detriment to the continuity and quality of services provided to clients.

出口計画は，包括的であり，文書化され，かつ，第 4 条第 2 項の中で定められた基準に従って，十分に試験されかつ定期的に見直される。

Exit plans shall be comprehensive, documented and, in accordance with the criteria set out in Article 4(2), shall be sufficiently tested and reviewed periodically.

金融機関は，代替的なソリューションを識別し，かつ，締約された ICT サービスと適格なデータを当該 ICT サードパーティサービスプロバイダから除去すること，及び，それらの ICT サービスと適格なデータを代替的なプロバイダに対して安全かつ一体として移転しもしくはそれらの ICT サービスと適格なデータをインハウスに再組込みすることを当該金融機関ができるようにする移行計画を策定す

る。

Financial entities shall identify alternative solutions and develop transition plans enabling them to remove the contracted ICT services and the relevant data from the ICT third-party service provider and to securely and integrally transfer them to alternative providers or reincorporate them in-house.

金融機関は，第 1 副項に示す状況が発生した場合における事業継続性を維持するため，適切な緊急事態対応策を設ける。

Financial entities shall have appropriate contingency measures in place to maintain business continuity in the event of the circumstances referred to in the first subparagraph.

9. ESAs は，共同委員会を介して，ICT サービスの利用に関する全ての契約上の取決めに共通の情報を含め，第 3 項に示す情報の登録簿の目的のための標準雛型を定めるための実装技術標準案を策定する。ESAs は，欧州委員会に対し，2024 年 1 月 17 日までに，それらの実装技術標準案を提出する。

The ESAs shall, through the Joint Committee, develop draft implementing technical standards to establish the standard templates for the purposes of the register of information referred to in paragraph 3, including information that is common to all contractual arrangements on the use of ICT services. The ESAs shall submit those draft implementing technical standards to the Commission by 17 January 2024.

規則(EU) No 1093/2010，規則(EU) No 1094/2010 及び規則(EU) No 1095/2010 の各第 15 条に従って第 1 副項に示す実装技術標準を採択するための権限は，欧州委員会に対して与えられる。

Power is conferred on the Commission to adopt the implementing technical standards referred to in the first subparagraph in accordance with Article 15 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.

10. ESAs は，共同委員会を介して，ICT サードパーティサービスプロバイダから提供される不可欠な機能または重要な機能を支える ICT サービスの利用に関する契約上の取決めとの関係において，第 2 項に示す基本方針の詳細内容の細目を別途定めるため，法制上の技術標準案を策定する。

The ESAs shall, through the Joint Committee, develop draft regulatory technical standards to further specify the detailed content of the policy referred to in paragraph 2 in relation to the contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers.

それらの法制上の技術標準案を策定する際，ESAs は，金融機関の規模及び全体的なリスクプロファイル，並びに，当該金融機関のサービス，活動及び運営管理の性質，規模及び複雑性を考慮に入れる。ESAs は，欧州委員会に対し，2024 年 1 月 17 日までに，それらの法制上の技術標準案を提

出する。

When developing those draft regulatory technical standards, the ESAs shall take into account the size and the overall risk profile of the financial entity, and the nature, scale and complexity of its services, activities and operations. The ESAs shall submit those draft regulatory technical standards to the Commission by 17 January 2024.

規則(EU) No 1093/2010, 規則(EU) No 1094/2010 及び規則(EU) No 1095/2010 の各第 10 条ないし第 14 条に従って第 1 副項に示す法制上の技術標準を採択することによってこの規則を補遺するための権限は, 欧州委員会に対して与えられる。

Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in the first subparagraph in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.

第 29 条 法主体の側における ICT 集中化リスクの事前評価

Article 29 **Preliminary assessment of ICT concentration risk at entity level**

1. 第 28 条第 4 項(c)に示すリスクの特定及び評価を遂行する際, 金融機関は, 不可欠な機能または重要な機能を支える ICT サービスとの関係における契約上の取決めの予定されている締結が, 以下のいずれかのことを導くようであるか否かも考慮に入れる:

When performing the identification and assessment of risks referred to in Article 28(4), point (c), financial entities shall also take into account whether the envisaged conclusion of a contractual arrangement in relation to ICT services supporting critical or important functions would lead to any of the following:

(a) 容易に代替可能ではない ICT サードパーティサービスプロバイダとの間で契約すること;または

contracting an ICT third-party service provider that is not easily substitutable; or

(b) 同一の ICT サードパーティサービスプロバイダとの間でもしくは緊密に相互結合された ICT サードパーティサービスプロバイダとの間で不可欠な機能または重要な機能を支える ICT サービスの提供との関係において多重の契約上の取決めを設けること。

having in place multiple contractual arrangements in relation to the provision of ICT services supporting critical or important functions with the same ICT third-party service provider or with closely connected ICT third-party service providers.

金融機関は, 予定されているソリューションが, 当該金融機関のデジタル回復力戦略の中で定めら

れた事業上の必要性及び目的に合致しているかどうか及びどのように合致しているかを考慮に入れた上で，異なる ICT サードパーティサービスプロバイダの利用のような，代替的なソリューションの受益と費用を考量する。

Financial entities shall weigh the benefits and costs of alternative solutions, such as the use of different ICT third-party service providers, taking into account if and how envisaged solutions match the business needs and objectives set out in their digital resilience strategy.

2. 不可欠な機能または重要な機能を支える ICT サービスの利用に関する契約上の取決めが，ICT サードパーティサービスプロバイダが別の ICT サードパーティサービスプロバイダに対して不可欠な機能または重要な機能を支える ICT サービスを更に下請契約する可能性を含んでいるときは，金融機関は，受益と，そのような下請契約と関係して生ずるかもしれないリスク，とりわけ，第三国内に拠点をもつ ICT 下請契約者の場合のリスクを考量する。

Where the contractual arrangements on the use of ICT services supporting critical or important functions include the possibility that an ICT third-party service provider further subcontracts ICT services supporting a critical or important function to other ICT third-party service providers, financial entities shall weigh benefits and risks that may arise in connection with such subcontracting, in particular in the case of an ICT subcontractor established in a third-country.

契約上の取決めが不可欠な機能または重要な機能を支える ICT サービスと関係するときは，金融機関は，ICT サードパーティサービスプロバイダの破産の場合において適用され得る破産法の条項及び当該金融機関のデータの緊急の復旧との関係において生ずるかもしれない制約を適正に検討する。

Where contractual arrangements concern ICT services supporting critical or important functions, financial entities shall duly consider the insolvency law provisions that would apply in the event of the ICT third-party service provider's bankruptcy as well as any constraint that may arise in respect to the urgent recovery of the financial entity's data.

不可欠な機能または重要な機能を支える ICT サービスの利用に関する契約上の取決めが，第三国内に拠点をもつ ICT サードパーティサービスプロバイダとの間で締結されるときは，金融機関は，第 2 副項に示す検討に加え，欧州連合のデータ保護規定の遵守及び当該第三国における法律の実効的な執行も検討する。

Where contractual arrangements on the use of ICT services supporting critical or important functions are concluded with an ICT third-party service provider established in a third country, financial entities shall, in addition to the considerations referred to in the second subparagraph, also consider the compliance with Union data protection rules and the effective enforcement of the law in that third country.

不可欠な機能または重要な機能を支える ICT サービスの利用に関する契約上の取決めが下請契約を定めているときは，金融機関は，契約された機能を全面的に監視するための当該金融機関の

能力及びこの点に関して当該金融機関を実効的に監視するための職務権限のある当局の能力に対し，潜在的に長くまたは複雑な下請契約の連鎖が影響を与え得るか否か及びどのように影響を与え得るかを評価する。

Where the contractual arrangements on the use of ICT services supporting critical or important functions provide for subcontracting, financial entities shall assess whether and how potentially long or complex chains of subcontracting may impact their ability to fully monitor the contracted functions and the ability of the competent authority to effectively supervise the financial entity in that respect.

第 30 条 鍵となる契約条項

Article 30 **Key contractual provisions**

1. 金融機関の権利及び義務並びに ICT サードパーティサービスプロバイダの権利及び義務は，明確に配分され，かつ，書面により定められる。契約全体は，サービスレベル合意を含めるものとし，かつ，紙で，または，ダウンロード可能であり，耐久性がありかつアクセス可能な別のフォーマットによる文書の中で当事者が利用可能な 1 つの書面の中で，文書化される。

The rights and obligations of the financial entity and of the ICT third-party service provider shall be clearly allocated and set out in writing. The full contract shall include the service level agreements and be documented in one written document which shall be available to the parties on paper, or in a document with another downloadable, durable and accessible format.

2. ICT サービスの利用に関する契約上の取決めは，少なくとも，以下の諸要素を含める：

The contractual arrangements on the use of ICT services shall include at least the following elements:

(a) 不可欠な機能または重要な機能を支える ICT サービスまたはその実質的な一部の下請契約が許容されているか否か，また，その場合に該当するときは，そのような下請契約に対して適用される条件を示す，ICT サードパーティサービスプロバイダから提供される全ての機能及び ICT サービスの明確かつ完全な記述；

a clear and complete description of all functions and ICT services to be provided by the ICT third-party service provider, indicating whether subcontracting of an ICT service supporting a critical or important function, or material parts thereof, is permitted and, when that is the case, the conditions applying to such subcontracting;

(b) 契約されまたは下請契約された機能と ICT サービスが提供される場所，及び，記録保存の場所を含め，データが処理される場所，すなわち，地域または国，並びに，そのような場所を変更することを ICT サードパーティサービスプロバイダが予定するときは，当該金融機関に対して事前に通知すべき当該 ICT サードパーティサービスプロバイダの要件；

the locations, namely the regions or countries, where the contracted or subcontracted functions and ICT services are to be provided and where data is to be processed, including the storage location, and the requirement for the ICT third-party service provider to notify the financial entity in advance if it envisages changing such locations;

(c) 個人データを含め，データの保護との関係における可用性，真正性，完全性及び機密性に関する条項；

provisions on availability, authenticity, integrity and confidentiality in relation to the protection of data, including personal data;

(d) ICT サードパーティサービスプロバイダの破産，経営破綻もしくは事業運営の継続不能の場合において，または，契約上の取決めが終了する場合において，当該金融機関によって処理される個人データ及び非個人データのアクセス，復旧及び容易にアクセス可能なフォーマットによる返還を確保することに関する条項；

provisions on ensuring access, recovery and return in an easily accessible format of personal and non-personal data processed by the financial entity in the event of the insolvency, resolution or discontinuation of the business operations of the ICT third-party service provider, or in the event of the termination of the contractual arrangements;

(e) そのアップデート及び改訂を含め，サービスレベルの記述；

service level descriptions, including updates and revisions thereof;

(f) 金融機関に対して提供される ICT サービスと関連する ICT インシデントが発生する場合において，付加的な費用負担なくまたは*事前に*定められた費用負担で，当該金融機関に対して補助を提供すべき ICT サードパーティサービスプロバイダの義務；

the obligation of the ICT third-party service provider to provide assistance to the financial entity at no additional cost, or at a cost that is determined *ex-ante*, when an ICT incident that is related to the ICT service provided to the financial entity occurs;

(g) 当該職務権限のある当局から指定された者を含め，職務権限のある当局及び金融機関の破綻処理当局に全面的に協力すべき ICT サードパーティサービスプロバイダの義務；

the obligation of the ICT third-party service provider to fully cooperate with the competent authorities and the resolution authorities of the financial entity, including persons appointed by them;

(h) 職務権限のある当局及び破綻処理当局の所期するところに従い，契約上の取決めの終了の権利及びその終了のための関連するミニマムの通知期限；

termination rights and related minimum notice periods for the termination of the contractual arrangements, in accordance with the expectations of competent authorities and resolution authorities;

(i) 第 13 条第 6 項に従って当該金融機関の ICT セキュリティ認識向上計画とデジタル運営管理上の回復力訓練への ICT サードパーティサービスプロバイダの参加に関する条件。

the conditions for the participation of ICT third-party service providers in the financial entities' ICT security awareness programmes and digital operational resilience training in accordance with Article 13(6).

3. 不可欠な機能または重要な機能を支える ICT サービスの利用に関する契約上の取決めは，第 2 項に示す諸要素に加え，少なくとも，以下のことを含める：

The contractual arrangements on the use of ICT services supporting critical or important functions shall include, in addition to the elements referred to in paragraph 2, at least the following:

(a) 当該金融機関による ICT サービスの実効的な監視をできるようにし，かつ，合意されたサービスレベルに適合していない場合において不適正な遅滞なく適切な解消の活動をできるようにするための，合意されたサービスレベル内における詳密な定量的及び定性的な遂行能力の目標を付して，そのアップデート及び改訂を含め，サービスレベルの完全な記述；

full service level descriptions, including updates and revisions thereof with precise quantitative and qualitative performance targets within the agreed service levels to allow effective monitoring by the financial entity of ICT services and enable appropriate corrective actions to be taken, without undue delay, when agreed service levels are not met;

(b) 合意されたサービスレベルに沿って，不可欠な機能または重要な機能を支える ICT サービスを実効的に提供するための当該 ICT サードパーティサービスプロバイダの能力に対して実質的な影響をもち得る発展の通知を含め，ICT サードパーティサービスプロバイダの通知期限及び当該金融機関に対する報告義務；

notice periods and reporting obligations of the ICT third-party service provider to the financial entity, including notification of any development that might have a material impact on the ICT third-party service provider's ability to effectively provide the ICT services supporting critical or important functions in line with agreed service levels;

(c) 事業上の緊急事態対応計画を実装し及び試験し，並びに，当該金融機関の法制上の枠組みに沿って，当該金融機関からのサービスの提供にとって適切なレベルの安全性を提供する ICT セキュリティの方策，ツール及び基本方針をもつべき当該 ICT サードパーティサービスプロバイダの要件；

requirements for the ICT third-party service provider to implement and test business contingency plans and to have in place ICT security measures, tools and policies that provide an appropriate level of security for the provision of services by the financial entity in line with its regulatory framework;

(d) 第 26 条及び第 27 条に示す当該金融機関の TLPT に参加しかつ全面的に協力すべき当該 ICT サードパーティサービスプロバイダの義務；

the obligation of the ICT third-party service provider to participate and fully cooperate in the financial entity's TLPT as referred to in Articles 26 and 27;

(e) ICT サードパーティサービスプロバイダの遂行能力を継続的に監視する権利であって，以下の権利及び義務を伴うもの：

the right to monitor, on an ongoing basis, the ICT third-party service provider's performance, which entails the following:

(i) 当該金融機関によるもしくは指定されたサードパーティによるまたは職務権限のある当局による制約のないアクセスの権利，検査の権利及び監査の権利，並びに，当該文書が当該 ICT サードパーティサービスプロバイダの運営管理のために不可欠であるときは，その権利の行使が他の契約上の取決めまたは実装の基本方針によって妨げられまたは制限されることのない，現場において適格な文書の複製を入手する権利；

unrestricted rights of access, inspection and audit by the financial entity, or an appointed third party, and by the competent authority, and the right to take copies of relevant documentation on-site if they are critical to the operations of the ICT third-party service provider, the effective exercise of which is not impeded or limited by other contractual arrangements or implementation policies;

(ii) 他の顧客の権利が影響を受けるときは，代替的な保証レベルに関して合意する権利；

the right to agree on alternative assurance levels if other clients' rights are affected;

(iii) 職務権限のある当局，筆頭監督者，金融機関または指定されたサードパーティによって遂行される現場における検査及び監査の間，全面的に協力すべき当該 ICT サードパーティサービスプロバイダの義務；並びに

the obligation of the ICT third-party service provider to fully cooperate during the onsite inspections and audits performed by the competent authorities, the Lead Overseer, financial entity or an appointed third party; and

(iv) そのような検査及び監査の範囲，従うべき手続及び頻度に関して詳細内容を提供すべ

き義務；

the obligation to provide details on the scope, procedures to be followed and frequency of such inspections and audits;

(f) 出口戦略，とりわけ，以下のような義務的な適切な移行期間の設定：
exit strategies, in particular the establishment of a mandatory adequate transition period:

(i) 当該金融機関の側における混乱のリスクを削減するという観点から，または，当該金融機関の実効的な破綻処理及び再建を確保するという観点から，その期間内は，当該 ICT サードパーティサービスプロバイダは，それぞれの機能または ICT サービスを提供し続けることになり；

during which the ICT third-party service provider will continue providing the respective functions, or ICT services, with a view to reducing the risk of disruption at the financial entity or to ensure its effective resolution and restructuring;

(ii) 当該金融機関が，他の ICT サードパーティサービスプロバイダに移行できるようにするため，または，提供されるサービスの複雑性に合致するインハウスのソリューションに変更できるようにする。

allowing the financial entity to migrate to another ICT third-party service provider or change to in-house solutions consistent with the complexity of the service provided.

(e)からの特例により，ICT サードパーティサービスプロバイダとマイクロ企業である金融機関は，当該金融機関のアクセスの権利，検査の権利及び監査の権利が当該 ICT サードパーティサービスプロバイダによって指定された独立のサードパーティに対して委任され得ること，並びに，当該金融機関が，いつでも，当該サードパーティから，当該 ICT サードパーティサービスプロバイダの遂行能力に関する情報及び保証を要求できることを合意できる。

By way of derogation from point (e), the ICT third-party service provider and the financial entity that is a microenterprise may agree that the financial entity's rights of access, inspection and audit can be delegated to an independent third party, appointed by the ICT third-party service provider, and that the financial entity is able to request information and assurance on the ICT third-party service provider's performance from the third party at any time.

4. 契約上の取決めを交渉する際，金融機関と ICT サードパーティサービスプロバイダは，特定のサービスのために行政機関によって策定された標準契約条項の利用を検討する。

When negotiating contractual arrangements, financial entities and ICT third-party service providers shall consider the use of standard contractual clauses developed by public authorities for specific services.

5. ESAs は，共同委員会を介して，不可欠な機能または重要な機能を支える ICT サービスを下請契約する場合における金融機関が判定及び評価する必要のある第 2 項(a)に示す要素の詳細内容の細目を別途定めるため，法制上の技術標準案を策定する。

The ESAs shall, through the Joint Committee, develop draft regulatory technical standards to specify further the elements referred to in paragraph 2, point (a), which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions.

それらの法制上の技術標準案を策定する際，ESAs は，金融機関の規模と全体的なリスクプロファイル並びにその金融機関のサービス，活動及び運営管理の性質，規模及び複雑性を考慮に入れる。

When developing those draft regulatory technical standards, the ESAs shall take into consideration the size and overall risk profile of the financial entity, and the nature, scale and complexity of its services, activities and operations.

ESAs は，欧州委員会に対し，2024 年 7 月 17 日までに，それらの法制上の技術標準案を提出する。

The ESAs shall submit those draft regulatory technical standards to the Commission by 17 July 2024.

規則(EU) No 1093/2010，規則(EU) No 1094/2010 及び規則(EU) No 1095/2010 の各第 10 条ないし第 14 条に従って第 1 副項に示す法制上の技術標準を採択することによってこの規則を補遺するための権限は，欧州委員会に対して与えられる。

Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in the first subparagraph in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.

第 II 節　不可欠な ICT サードパーティサービスプロバイダの監督枠組み
Section II　Oversight Framework of critical ICT third-party service providers

第 31 条　不可欠な ICT サードパーティサービスプロバイダの指定
Article 31　Designation of critical ICT third-party service providers

1. ESAs は，共同委員会を介して，かつ，第 32 条第 1 項により設けられる監督フォーラムからの勧告に応じて：

The ESAs, through the Joint Committee and upon recommendation from the Oversight Forum established pursuant to Article 32(1), shall:

(a) 第 2 項の中で細目が定められた基準を考慮に入れる評価の後，金融機関にとって不可欠な ICT サードパーティサービスプロバイダを指定し；

designate the ICT third-party service providers that are critical for financial entities, following an assessment that takes into account the criteria specified in paragraph 2;

(b) 個々の不可欠な ICT サードパーティサービスプロバイダの筆頭監督者として，規則(EU) No 1093/2010，規則(EU) No 1094/2010 及び規則(EU) No 1095/2010 に従って，当該金融機関の個別の貸借対照表の合計額によって証明されるものとしての，適格な不可欠な ICT サードパーティサービスプロバイダのサービスを用いる全金融機関の総資産の価額中の最大割合の総資産を占める金融機関に関する職責を負う ESA を任命する。

appoint as Lead Overseer for each critical ICT third-party service provider the ESA that is responsible, in accordance with Regulations (EU) No 1093/2010, (EU) No 1094/2010 or (EU) No 1095/2010, for the financial entities having together the largest share of total assets out of the value of total assets of all financial entities using the services of the relevant critical ICT third-party service provider, as evidenced by the sum of the individual balance sheets of those financial entities.

2. 第 1 項(a)に示す指定は，ICT サードパーティサービスプロバイダから提供される ICT サービスとの関係において，以下の全ての基準を基礎とする：

The designation referred to in paragraph 1, point (a), shall be based on all of the following criteria in relation to ICT services provided by the ICT third-party service provider:

(a) 適格な ICT サードパーティサービスプロバイダがサービスを提供している金融機関の数及び資産総額を考慮に入れた上で，適格な ICT サードパーティサービスプロバイダがそのサービスの提供の大規模な運営管理上の失敗に直面するというようなことが発生する際における金融サービスの提供の安定性，継続性または品質に対するシステミックな影響；

the systemic impact on the stability, continuity or quality of the provision of financial services in the event that the relevant ICT third-party service provider would face a large scale operational failure to provide its services, taking into account the number of financial entities and the total value of assets of financial entities to which the relevant ICT third-party service provider provides services;

(b) 以下のパラメータに従って評価された，適格な ICT サードパーティサービスプロバイダに依拠する金融機関のシステミックな性質または重要性：

the systemic character or importance of the financial entities that rely on the relevant ICT third-party service provider, assessed in accordance with the following parameters:

(i) ICT サードパーティサービスプロバイダにそれぞれ依拠するグローバルなシステミックな影響上の重要性をもつ機関（G-SIIs）の数またはそれ以外のシステミックな影響上の重要性をもつ機関（O-SIIs）の数；

the number of global systemically important institutions (G-SIIs) or other systemically important institutions (O-SIIs) that rely on the respective ICT third-party service provider;

(ii) G-SIIs または O-SIIs がそれら以外の金融機関に対して金融上のインフラサービスを提供する状況を含め，(i)に示す G-SIIs または O-SIIs とそれら以外の金融機関との間の相互依存性；

the interdependence between the G-SIIs or O-SIIs referred to in point (i) and other financial entities, including situations where the G-SIIs or O-SIIs provide financial infrastructure services to other financial entities;

(c) 金融機関が当該サービスに対して直接に依拠するかまたは下請契約上の取決めを介して間接に依拠するかの別を問わず，金融機関の，究極的には同じ ICT サードパーティサービスプロバイダが関与する不可欠な機能または重要な機能との関係において，適格な ICT サードパーティサービスプロバイダから提供されるサービスに対する金融機関の依拠；

the reliance of financial entities on the services provided by the relevant ICT third-party service provider in relation to critical or important functions of financial entities that ultimately involve the same ICT third-party service provider, irrespective of whether financial entities rely on those services directly or indirectly, through subcontracting arrangements;

(d) 以下のパラメータを考慮に入れた上で，当該 ICT サードパーティサービスプロバイダの代替可能性の程度：

the degree of substitutability of the ICT third-party service provider, taking into account the following parameters:

(i) 特定の市場における ICT サードパーティサービスプロバイダの限定された数もしくは適格な ICT サードパーティサービスプロバイダの市場支配のゆえの，または，専有的技術との関係を含め，技術上の複雑性もしくはそれに含まれている洗練性のゆえの，または，ICT サードパーティサービスプロバイダの組織もしくは活動の特性のゆえの，部分的にせよ，実際の代替の欠如；

the lack of real alternatives, even partial, due to the limited number of ICT third-party service providers active on a specific market, or the market share of the relevant ICT third-party service provider, or the technical complexity or sophistication involved, including in relation to any proprietary technology, or the specific features of the ICT third-party service provider's organisation or activity;

(ii) 移植のプロセスに伴い得る大きな費用，時間もしくはそれ以外の資源による，または，そのような移植を通じて当該金融機関が晒されるかもしれない ICT リスクもしくはそれ以外の運営管理上のリスクの増加による，適格な ICT サードパーティサービスプロバイダから別の ICT サードパーティサービスプロバイダに対する適格なデータ及び作業を部分的または全面的に移植することとの関係における困難。

difficulties in relation to partially or fully migrating the relevant data and workloads from the relevant ICT third-party service provider to another ICT third-party service provider, due either to significant financial costs, time or other resources that the migration process may entail, or to increased ICT risk or other operational risks to which the financial entity may be exposed through such migration.

3. ICT サードパーティサービスプロバイダがグループに属する場合，第 2 項に示す基準は，全体としてのグループから提供される ICT サービスとの関係において判断される。

Where the ICT third-party service provider belongs to a group, the criteria referred to in paragraph 2 shall be considered in relation to the ICT services provided by the group as a whole.

4. グループの一部となっている不可欠な ICT サードパーティサービスプロバイダは，筆頭監督者との間の適切な代理及び通信を確保するための調整点として，1 つの法人を指定する。

Critical ICT third-party service providers which are part of a group shall designate one legal person as a coordination point to ensure adequate representation and communication with the Lead Overseer.

5. 筆頭監督者は，ICT サードパーティサービスプロバイダに対し，第 1 項(a)に示す指定を導いている評価の結果を通知する。その通知の日から 6 週間以内に，当該 ICT サードパーティサービスプロバイダは，筆頭監督者に対し，評価の目的のための適格な情報をもつ理由を付した陳述書を提出できる。筆頭監督者は，理由を付した陳述書を判断し，かつ，そのような陳述書の受領の日から 30 暦日以内に，付加的な情報が提出されることを要求できる。

The Lead Overseer shall notify the ICT third-party service provider of the outcome of the assessment leading to the designation referred in paragraph 1, point (a). Within 6 weeks from the date of the notification, the ICT third-party service provider may submit to the Lead Overseer a reasoned statement with any relevant information for the purposes of the assessment. The Lead Overseer shall consider the reasoned statement and may request additional information to be submitted within 30 calendar days of the receipt of such statement.

ICT サードパーティサービスプロバイダの不可欠としての指定の後，ESAs は，共同委員会を介して，当該 ICT サードパーティサービスプロバイダに対し，そのような指定及び当該 ICT サードパーティサービスプロバイダが監督活動に実効的に服することになる開始日を通知する。その開始日は，通知後 1 か月以内とする。当該 ICT サードパーティサービスプロバイダは，当該 ICT サードパーティサービスプロバイダがサービスを提供する金融機関に対し，ICT サードパーティサービスプロバイダの不可欠としての指定を通知する。

After designating an ICT third-party service provider as critical, the ESAs, through the Joint Committee, shall notify the ICT third-party service provider of such designation and the starting date as from which they will effectively be subject to oversight activities. That starting date shall be no later than one month after the notification. The ICT third-party service provider shall notify the financial entities to which they provide services of their designation as critical.

6. 欧州委員会は，2024 年 7 月 17 日までに本条第 2 項に示す基準の細目を別途定めることによってこの規則を補遺するため，第 57 条に従って委任される行為を採択する権限を与えられる。

The Commission is empowered to adopt a delegated act in accordance with Article 57 to supplement this Regulation by specifying further the criteria referred to in paragraph 2 of this Article, by 17 July 2024.

7. 第 1 項(a)に示す指定は，第 6 項に従って欧州委員会が委任される行為を採択するまでは，使用されてはならない。

The designation referred to in paragraph 1, point (a), shall not be used until the Commission has adopted a delegated act in accordance with paragraph 6.

8. 第 1 項(a)に示す指定は，以下の者に対して適用してはならない：

The designation referred to in paragraph 1, point (a), shall not apply to the following:

(i) 他の金融機関に対して ICT サービスを提供する金融機関；

financial entities providing ICT services to other financial entities;

(ii) 欧州連合の機能に関する条約の第 127 条第 2 項に示す職務を支えるために設けられた監督枠組みに服する ICT サードパーティサービスプロバイダ；

ICT third-party service providers that are subject to oversight frameworks established for the purposes of supporting the tasks referred to in Article 127(2) of the Treaty on the Functioning of the European Union;

(iii) ICT グループ内サービスプロバイダ；

ICT intra-group service providers;

(iv) 1 つの構成国内のみにおいて，当該構成国内のみで能動的な金融機関に対して ICT サービスを提供する ICT サードパーティサービスプロバイダ。

ICT third-party service providers providing ICT services solely in one Member State to financial entities that are only active in that Member State.

9. ESAs は，共同委員会を介して，年次で，欧州連合レベルにおける不可欠な ICT サードパーティサービスプロバイダのリストを作成し，公表し及びアップデートする。

The ESAs, through the Joint Committee, shall establish, publish and update yearly the list of critical ICT third-party service providers at Union level.

10. 第 1 項(a)の目的のために，職務権限のある当局は，年次でかつ集約ベースで，第 32 条により設けられる監督フォーラムに対し，第 28 条第 3 項第 3 副項に示す報告書を送付する。監督フォーラムは，職務権限のある当局から受領した情報を基礎として，金融機関の ICT サードパーティ依存を評価する。

For the purposes of paragraph 1, point (a), competent authorities shall, on a yearly and aggregated basis, transmit the reports referred to in Article 28(3), third subparagraph, to the Oversight Forum established pursuant to Article 32. The Oversight Forum shall assess the ICT third-party dependencies of financial entities based on the information received from the competent authorities.

11. 第 9 項に示すリストの中に含まれていない ICT サードパーティサービスプロバイダは，第 1 項(a)に従い，不可欠として指定されることを求め得る。

The ICT third-party service providers that are not included in the list referred to in paragraph 9 may request to be designated as critical in accordance with paragraph 1, point (a).

第 1 副項の目的のために，ICT サードパーティサービスプロバイダは，EBA，ESMA または EIOPA に対し，理由を付した申請書を提出する。EBA，ESMA または EIOPA は，共同委員会を介して，第 1 項(a)に従い，当該 ICT サードパーティサービスプロバイダを不可欠として指定するかどうかを決定する。

For the purpose of the first subparagraph, the ICT third-party service provider shall submit a reasoned application to EBA, ESMA or EIOPA, which, through the Joint Committee, shall decide whether to designate that ICT third-party service provider as critical in accordance with paragraph 1, point (a).

第 2 副項に示す決定は，その申請書の受領から 6 か月以内に，採択されかつ当該 ICT サードパーティサービスプロバイダに対して通知される。

The decision referred to in the second subparagraph shall be adopted and notified to the ICT third-party service provider within 6 months of receipt of the application.

12. 金融機関は，当該 ICT サードパーティサービスプロバイダが，その指定後 12 か月以内に欧州連合内に支店を設置した場合に限り，第三国内に拠点をもちかつ第 1 項(a)に従って不可欠として指定された ICT サードパーティサービスプロバイダのサービスを利用する。

Financial entities shall only make use of the services of an ICT third-party service provider established in a third country and which has been designated as critical in accordance with paragraph 1, point (a), if the latter has established a subsidiary in the Union within the 12 months following the designation.

13. 第 12 項に示す不可欠な ICT サードパーティサービスプロバイダは，筆頭監督者に対し，欧州連合内で設置された支店の経営の構造に対する変更を通知する。

The critical ICT third-party service provider referred to in paragraph 12 shall notify the Lead Overseer of any changes to the structure of the management of the subsidiary established in the Union.

第 32 条 監督枠組みの構造

Article 32 **Structure of the Oversight Framework**

1. 共同委員会は，規則(EU) No 1093/2010，規則(EU) No 1094/2010 及び規則(EU) No 1095/2010 の各第 57 条第 1 項に従い，金融部門全部にわたる ICT サードパーティリスクの分野において共同委員会の仕事及び第 31 条第 1 項(b)に示す筆頭監督者の仕事を支える目的のための小委員会として，監督フォーラムを設ける。監督フォーラムは，当該分野における共同委員会の共同意見書案及び共通行為案を準備する。

The Joint Committee, in accordance with Article 57(1) of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, shall establish the Oversight Forum as a sub-committee for the purposes of supporting the work of the Joint Committee and of the Lead Overseer referred to in Article 31(1), point (b), in the area of ICT third-party risk across financial sectors. The Oversight Forum shall prepare the draft joint positions and the draft common acts of the Joint Committee in that area.

監督フォーラムは，定期的に，ICT リスク及び脆弱性に関する適格な進展を討議し，欧州連合レベルの ICT サードパーティリスクの監視における一貫性のあるアプローチを促進する。

The Oversight Forum shall regularly discuss relevant developments on ICT risk and vulnerabilities and promote a consistent approach in the monitoring of ICT third-party risk at Union level.

2. 監督フォーラムは，年次で，全ての不可欠な ICT サードパーティサービスプロバイダに関して行われた監督活動の結果及び判断の集団的な評価を実施し，また，金融機関のデジタル運営管理上の回復力を向上させるための調整措置を促進し，ICT 集中化リスクへの対処に関するベストプラクティスを育成し，及び，部門間にわたるリスク移転に対する緩和策を開拓する。

The Oversight Forum shall, on a yearly basis, undertake a collective assessment of the results and findings of the oversight activities conducted for all critical ICT third-party service providers and promote coordination measures to increase the digital operational resilience of financial entities, foster best practices on addressing ICT concentration risk and explore mitigants for cross-sector risk transfers.

3. 監督フォーラムは，規則(EU) No 1093/2010，規則(EU) No 1094/2010 及び規則(EU) No 1095/2010 の各第 56 条第 1 項に従い，ESAs の共同意見書として共同委員会によって採択されるため，不可欠な ICT サードパーティサービスプロバイダに関する包括的な指標を提出する。

The Oversight Forum shall submit comprehensive benchmarks for critical ICT third-party service providers to be adopted by the Joint Committee as joint positions of the ESAs in accordance with Article 56(1) of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.

4. 監督フォーラムは，以下の者によって構成される：

The Oversight Forum shall be composed of:

(a) ESAs の各議長；

the Chairpersons of the ESAs;

(b) 各構成国から，第 46 条に示す適格な職務権限のある当局の現在の職員中の 1 名の上級代表者；

one high-level representative from the current staff of the relevant competent authority referred to in Article 46 from each Member State;

(c) オブザーバーとして，各 ESAs の執行役員及び欧州委員会，ESRB，ECB 及び ENISA から 1 名の代表者；

the Executive Directors of each ESA and one representative from the Commission, from the ESRB, from ECB and from ENISA as observers;

(d) それが適切なときは，オブザーバーとして，各構成国から，第 46 条に示す職務権限のある当局の 1 名の付加的な代表者；

where appropriate, one additional representative of a competent authority referred to in Article 46 from each Member State as observer;

(e) それが適用可能なときは，オブザーバーとして，指令(EU) 2022/2555 に服する必須法主体または重要法主体であって，不可欠な ICT サードパーティサービスプロバイダとして指定された法主体の監督に関して職責を負う同指令に従って指定されまたは設けられた職務権限のある当局の 1 名の代表者。

where applicable, one representative of the competent authorities designated or established in accordance with Directive (EU) 2022/2555 responsible for the supervision of an essential or important entity subject to that Directive, which has been designated as a critical ICT third-party service provider, as observer.

監督フォーラムは，それが適切なときは，第 6 項に従って任命された独立の専門家の助言を求めることができる。

The Oversight Forum may, where appropriate, seek the advice of independent experts appointed in accordance with paragraph 6.

5. 各構成国は，その職員が第 4 項第 1 副項(b)に示す上級代表者である適格な職務権限のある当局を指定し，かつ，筆頭監督者に対し，そのことを連絡する。

Each Member State shall designate the relevant competent authority whose staff member shall be the high-level representative referred in paragraph 4, first subparagraph, point (b), and shall inform the Lead Overseer thereof.

ESAs は，構成国から指定された適格な職務権限のある当局の現在の職員からの上級代表者のリストを ESAs の Web サイト上で公表する。

The ESAs shall publish on their website the list of high-level representatives from the current staff of the relevant competent authority designated by Member States.

6. 第 4 項第 2 副項に示す独立の専門家は，公開かつ透明性のある申請過程の後に選抜された専門家のプールから，監督フォーラムによって任命される。

The independent experts referred to in paragraph 4, second subparagraph, shall be appointed by the Oversight Forum

from a pool of experts selected following a public and transparent application process.

独立の専門家は，金融の安定性，デジタル運営管理上の回復力及び ICT のセキュリティ上の事項における当該の者の専門知識を基礎として，任命される。独立の専門家は，全体としての欧州連合の利益においてのみ，独立にかつ客観的に行動し，また，欧州連合の機関もしくは組織から，構成国のいかなる政府から，または，それら以外の公的もしくは私的な組織から指示を求めてはならず，かつ，指示を受けてはならない。

The independent experts shall be appointed on the basis of their expertise in financial stability, digital operational resilience and ICT security matters. They shall act independently and objectively in the sole interest of the Union as a whole and shall neither seek nor take instructions from Union institutions or bodies, from any government of a Member State or from any other public or private body.

7. 規則(EU) No 1093/2010，規則(EU) No 1094/2010 及び規則(EU) No 1095/2010 の各第 16 条に従い，ESAs は，本節の目的のために，2024 年 7 月 17 日までに，職務権限のある当局と ESAs との間の職務の分配及び執行に関する詳細な手続及び条件，並びに，第 35 条第 1 項(d)による勧告の事後対応を確保するために職務権限のある当局にとって必要となる情報の交換の詳細を包摂する，不可欠な ICT サードパーティサービスプロバイダに宛の，ESAs と職務権限のある当局との間の協力に関する運用指針を発行する。

In accordance with Article 16 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, the ESAs shall by 17 July 2024 issue, for the purposes of this Section, guidelines on the cooperation between the ESAs and the competent authorities covering the detailed procedures and conditions for the allocation and execution of tasks between competent authorities and the ESAs and the details on the exchanges of information which are necessary for competent authorities to ensure the follow-up of recommendations pursuant to Article 35(1), point (d), addressed to critical ICT third-party service providers.

8. 本節の中で定められた要件は，指令(EU) 2022/2555 の適用及び同規則以外のクラウドコンピューティングサービスのプロバイダに対して適用可能な監督に関する欧州連合の規定の適用を妨げてはならない。

The requirements set out in this Section shall be without prejudice to the application of Directive (EU) 2022/2555 and of other Union rules on oversight applicable to providers of cloud computing services.

9. ESAs は，共同委員会を介して，かつ，監督フォーラムによって実行された準備作業を基礎として，欧州議会，理事会及び欧州委員会に対し，年次で，本節の適用に関する報告書を提出する。

The ESAs, through the Joint Committee and based on preparatory work conducted by the Oversight Forum, shall, on yearly basis, submit a report on the application of this Section to the European Parliament, the Council and the Commission.

第 33 条 筆頭監督者の職務

Article 33 **Tasks of the Lead Overseer**

1. 第 31 条第 1 項(b)に従って任命された筆頭監督者は，所管する不可欠な ICT サードパーティサービスプロバイダの監督を実行し，かつ，その監督と関連する全ての事項の目的のために，それらの不可欠な ICT サードパーティサービスプロバイダのための主たる連絡先となる。

The Lead Overseer, appointed in accordance with Article 31(1), point (b), shall conduct the oversight of the assigned critical ICT third-party service providers and shall be, for the purposes of all matters related to the oversight, the primary point of contact for those critical ICT third-party service providers.

2. 第 1 項の目的のために，筆頭監督者は，金融機関に対して当該不可欠な ICT サードパーティサービスプロバイダが示し得る ICT リスクを取扱うための包括的であり，良好でありかつ実効的な規定，手続，仕組み及び取決めを個々の不可欠な ICT サードパーティサービスプロバイダが設けているか否か評価する。

For the purposes of paragraph 1, the Lead Overseer shall assess whether each critical ICT third-party service provider has in place comprehensive, sound and effective rules, procedures, mechanisms and arrangements to manage the ICT risk which it may pose to financial entities.

第 1 副項に示す評価は，主として，不可欠な ICT サードパーティサービスプロバイダから提供され，金融機関の不可欠な機能または重要な機能を支える ICT サービスに焦点を当てる。全ての適格なリスクに対処するために必要なときは，その評価は，不可欠な機能または重要な機能以外の機能を支える ICT サービスに拡大される。

The assessment referred to in the first subparagraph shall focus mainly on ICT services provided by the critical ICT third-party service provider supporting the critical or important functions of financial entities. Where necessary to address all relevant risks, that assessment shall extend to ICT services supporting functions other than those that are critical or important.

3. 第 2 項に示す評価は，以下の事柄を包摂する:

The assessment referred to in paragraph 2 shall cover:

(a) とりわけ，不可欠な ICT サードパーティサービスプロバイダが金融機関に対して提供するサービスの安全性，可用性，継続性，拡張性及び品質を確保するため，並びに，常時，データの高度な水準の可用性，真正性，完全性または機密性を維持するための能力を確保するための ICT 要件;

ICT requirements to ensure, in particular, the security, availability, continuity, scalability and quality of services

which the critical ICT third-party service provider provides to financial entities, as well as the ability to maintain at all times high standards of availability, authenticity, integrity or confidentiality of data;

(b) 構内，施設，データセンターのセキュリティを含め，ICT のセキュリティを確保することに貢献する物理的なセキュリティ；

the physical security contributing to ensuring the ICT security, including the security of premises, facilities, data centres;

(c) ICT リスクマネジメントの基本方針，ICT 事業継続性基本方針並びに ICT 対応計画及び ICT 復旧計画を含め，リスクマネジメントプロセス；

the risk management processes, including ICT risk management policies, ICT business continuity policy and ICT response and recovery plans;

(d) 明確であり，透明性がありかつ一貫性のある責任ライン及び実効性のある ICT リスクマネジメントを実現可能にする説明責任の規定をもつ組織構造を含め，統治の手配；

the governance arrangements, including an organisational structure with clear, transparent and consistent lines of responsibility and accountability rules enabling effective ICT risk management;

(e) 金融機関に対する実質的な ICT と関連するインシデントの特定，監視及び迅速な報告，それらのインシデントの，とりわけ，サイバー攻撃の取扱い及び解消；

the identification, monitoring and prompt reporting of material ICT-related incidents to financial entities, the management and resolution of those incidents, in particular cyber-attacks;

(f) 金融機関による終了の権利の実効的な行使を確保する，データのポータビリティ，アプリケーションのポータビリティ及び相互運用性のための仕組み；

the mechanisms for data portability, application portability and interoperability, which ensure an effective exercise of termination rights by the financial entities;

(g) ICT システム，インフラ及び管理策の試験；

the testing of ICT systems, infrastructure and controls;

(h) ICT 監査；

the ICT audits;

(i) 金融機関に対する不可欠な ICT サードパーティサービスプロバイダの ICT サービスの提供に対して適用可能な適格な国内技術標準及び国際的な技術標準の利用。

the use of relevant national and international standards applicable to the provision of its ICT services to the financial entities.

4. 第 2 項に示す評価を基礎として，かつ，第 34 条第 1 項に示す共同監督ネットワーク（JON）と調整した上で，筆頭監督者は，個々の不可欠な ICT サードパーティサービスプロバイダに関して計画された年次の監督目標及び主要な監督活動を記述している，明確であり，詳細でありかつ理由を付した個々の監督計画を採択する。同計画は，年次で，当該不可欠な ICT サードパーティサービスプロバイダに対して伝達される。

Based on the assessment referred to in paragraph 2, and in coordination with the Joint Oversight Network (JON) referred to in Article 34(1), the Lead Overseer shall adopt a clear, detailed and reasoned individual oversight plan describing the annual oversight objectives and the main oversight actions planned for each critical ICT third-party service provider. That plan shall be communicated yearly to the critical ICT third-party service provider.

監督計画を採択する前に，筆頭監督者は，不可欠な ICT サードパーティサービスプロバイダに対し，監督計画案を伝達する。

Prior to the adoption of the oversight plan, the Lead Overseer shall communicate the draft oversight plan to the critical ICT third-party service provider.

監督計画案を受領したときは，不可欠な ICT サードパーティサービスプロバイダは，15 暦日以内に，この規則の適用範囲外にある法主体である顧客に対する予想される影響を根拠づけ，かつ，それが適切なときは，リスクを緩和するための解決策を明確に述べる理由を付した陳述書を提出できる。

Upon receipt of the draft oversight plan, the critical ICT third-party service provider may submit a reasoned statement within 15 calendar days evidencing the expected impact on customers which are entities falling outside of the scope of this Regulation and where appropriate, formulating solutions to mitigate risks.

5. 第 4 項に示す年次監督計画が採択され，かつ，不可欠な ICT サードパーティサービスプロバイダに対して通知された後においては，職務権限のある当局は，筆頭監督者の同意がある場合に限り，そのような不可欠な ICT サードパーティサービスプロバイダと関係する措置を講ずることができる。

Once the annual oversight plans referred to in paragraph 4 have been adopted and notified to the critical ICT third-party service providers, competent authorities may take measures concerning such critical ICT third-party service providers only in agreement with the Lead Overseer.

第 34 条 筆頭監督者間の運営管理上の調整

Article 34 **Operational coordination between Lead Overseers**

1. 監督活動への一貫性のあるアプローチを確保するため，かつ，調整された一般的な監督戦略及び結束的な業務運用上のアプローチと作業手法を実現可能にするという観点から，第 31 条第 1 項(b)に従って任命される 3 つの筆頭監督者は，準備段階におけるそれらの筆頭監督者間の調整のため，それらの筆頭監督者それぞれの監督対象である不可欠な ICT サードパーティサービスプロバイダに対する監督活動の実行を調整するため，及び，第 42 条によって必要となり得る活動の過程において，JON を設ける。

   To ensure a consistent approach to oversight activities and with a view to enabling coordinated general oversight strategies and cohesive operational approaches and work methodologies, the three Lead Overseers appointed in accordance with Article 31(1), point (b), shall set up a JON to coordinate among themselves in the preparatory stages and to coordinate the conduct of oversight activities over their respective overseen critical ICT third-party service providers, as well as in the course of any action that may be needed pursuant to Article 42.

2. 第 1 項の目的のために，筆頭監督者は，日々の調整を実行するため及び迅速な意見交換と対応活動を確保するために従うべき詳細手続の細目を定める共通監督手順を策定する。その手順は，運営管理上の必要性，とりわけ，実務上の監督の取決めの進化を反映させるため，定期的に改訂される。

   For the purposes of paragraph 1, the Lead Overseers shall draw up a common oversight protocol specifying the detailed procedures to be followed for carrying out the day-to-day coordination and for ensuring swift exchanges and reactions. The protocol shall be periodically revised to reflect operational needs, in particular the evolution of practical oversight arrangements.

3. 筆頭監督者は，アドホックに，ECB 及び ENISA に対し，技術上の助言を提供すること，実務上の経験を共有することまたは JON の個別の調整会合に加わることを求めることができる。

   The Lead Overseers may, on an ad-hoc basis, call on the ECB and ENISA to provide technical advice, share hands-on experience or join specific coordination meetings of the JON.

第 35 条 筆頭監督者の権限

Article 35 **Powers of the Lead Overseer**

1. 本節の中で定められた義務を実行する目的のために，筆頭監督者は，不可欠な ICT サードパーティサービスプロバイダとの関係において，以下のための権限をもつ：

   For the purposes of carrying out the duties laid down in this Section, the Lead Overseer shall have the following powers

in respect of the critical ICT third-party service providers:

(a) 第 37 条に従い，全ての適格な情報及び文書を要求するため；

to request all relevant information and documentation in accordance with Article 37;

(b) 第 38 条及び第 39 条それぞれに従い，一般的な調査及び検査を実行するため；

to conduct general investigations and inspections in accordance with Articles 38 and 39, respectively;

(c) 監督活動の完了の後，本項の(d)に示す勧告との関係において，不可欠な ICT サードパーティサービスプロバイダによってとられた活動または実装された解消策の細目を示す報告書を要求するため；

to request, after the completion of the oversight activities, reports specifying the actions that have been taken or the remedies that have been implemented by the critical ICT third-party service providers in relation to the recommendations referred to in point (d) of this paragraph;

(d) とりわけ，以下の事柄と関係して，第 33 条第 3 項に示す分野における勧告書を発するため：

to issue recommendations on the areas referred to in Article 33(3), in particular concerning the following:

(i) とりわけ，金融機関に対して提供されるサービスの ICT セキュリティを確保するために適格であると筆頭監督者が考えるパッチ，アップデート，暗号化及びそれら以外のセキュリティ上の方策を準備することとの関係において，特定の ICT セキュリティ要件及び品質要件または手続の利用；

the use of specific ICT security and quality requirements or processes, in particular in relation to the roll-out of patches, updates, encryption and other security measures which the Lead Overseer deems relevant for ensuring the ICT security of services provided to financial entities;

(ii) 当該約款の下において不可欠な ICT サードパーティサービスプロバイダが金融機関に対して ICT サービスを提供するものであって，単一障害点の生成，その増幅を防止するため，または，ICT 集中化リスクの場合における欧州連合の金融部門にわたってあり得るシステミックな影響をミニマム化するために適格であると筆頭監督者が考える，当該約款の技術上の実装を含め，約款の利用；

the use of conditions and terms, including their technical implementation, under which the critical ICT third-party service providers provide ICT services to financial entities, which the Lead Overseer deems relevant for preventing the generation of single points of failure, the amplification thereof, or for

minimising the possible systemic impact across the Union's financial sector in the event of ICT concentration risk;

(iii) 不可欠な ICT サードパーティサービスプロバイダが ICT サードパーティサービスプロバイダとの間または第三国内に拠点をもつ ICT 下請契約者との間において締結することを計画している下請契約上の取決めを含め，別の下請契約が当該金融機関によるサービスの提供に対するリスクまたは金融の安定性に対するリスクの引金となり得ると筆頭監督者が第 37 条及び第 38 条に従って収集された情報の検討を基礎として考えるときは，計画された下請契約；

any planned subcontracting, where the Lead Overseer deems that further subcontracting, including subcontracting arrangements which the critical ICT third-party service providers plan to enter into with ICT third-party service providers or with ICT subcontractors established in a third country, may trigger risks for the provision of services by the financial entity, or risks to the financial stability, based on the examination of the information gathered in accordance with Articles 37 and 38;

(iv) 以下の累積的な条件に合致するときは，別の下請契約上の取決めを締結することを控えること:

refraining from entering into a further subcontracting arrangement, where the following cumulative conditions are met:

- 予定されている下請契約者が第三国内に拠点をもつ ICT サードパーティサービスプロバイダまたは ICT 下請契約者である；

  the envisaged subcontractor is an ICT third-party service provider or an ICT subcontractor established in a third country;

- その下請契約が，当該金融機関の不可欠な機能または重要な機能と関係している;かつ

  the subcontracting concerns critical or important functions of the financial entity; and

- そのような下請契約の利用が，監督上の要件を遵守するための金融機関の能力に対するものを含め，欧州連合の金融の安定性に対するまたは金融機関に対する明確かつ重大なリスクを呈していると筆頭監督者が考える。

  the Lead Overseer deems that the use of such subcontracting poses a clear and serious risk to the financial stability of the Union or to financial entities, including to the ability of financial entities to comply with supervisory requirements.

本号の(iv)の目的のために，当該不可欠な ICT サードパーティサービスプロバイダは，第 41 条第 1 項(b)に示す雛型を用いて，筆頭監督者に対し，下請契約に関する情報を送付する。

For the purpose of point (iv) of this point, ICT third-party service providers shall, using the template referred to in Article 41(1), point (b), transmit the information regarding subcontracting to the Lead Overseer.

2. 本条に示す権限を行使する際，筆頭監督者は:

When exercising the powers referred to in this Article, the Lead Overseer shall:

(a) JON 内における定期的な調整を確保し，かつ，とりわけ，不可欠な ICT サードパーティサービスプロバイダの監督に関し，しかるべく，一貫性のあるアプローチを求め；

ensure regular coordination within the JON, and in particular shall seek consistent approaches, as appropriate, with regard to the oversight of critical ICT third-party service providers;

(b) 指令(EU) 2022/2555 によって設けられた枠組みを適正に考慮に入れ，かつ，それが必要なときは，同指令によって不可欠な ICT サードパーティサービスプロバイダに対して適用され得る技術上及び組織上の措置の重複を避けるため，同指令に従って指定されまたは設けられた適格な職務権限のある当局から意見聴取し；

take due account of the framework established by Directive (EU) 2022/2555 and, where necessary, consult the relevant competent authorities designated or established in accordance with that Directive, in order to avoid duplication of technical and organisational measures that might apply to critical ICT third-party service providers pursuant to that Directive;

(c) 可能な範囲内において，不可欠な ICT サードパーティサービスプロバイダからこの規則の適用範囲外にある法主体である顧客に対して提供されるサービスの混乱というリスクをミニマム化することを求める。

seek to minimise, to the extent possible, the risk of disruption to services provided by critical ICT third-party service providers to customers that are entities falling outside the scope of this Regulation.

3. 筆頭監督者は，第 1 項に示す権限を行使する前に，監督フォーラムから意見を聴取する。

The Lead Overseer shall consult the Oversight Forum before exercising the powers referred to in paragraph 1.

第 1 項(d)に従って勧告書を発する前に，筆頭監督者は，当該不可欠な ICT サードパーティサービスプロバイダに対し，この規則の適用範囲外にある法主体である顧客に対する予想される影響を根拠づけ，また，それが適切なときは，リスクを緩和するための解決策を明確に述べる適格な情報を 30

暦日以内に提供する機会を与える。

Before issuing recommendations in accordance with paragraph 1, point (d), the Lead Overseer shall give the opportunity to the ICT third-party service provider to provide, within 30 calendar days, relevant information evidencing the expected impact on customers that are entities falling outside the scope of this Regulation and, where appropriate, formulating solutions to mitigate risks.

4. 筆頭監督者は，JON に対し，第 1 項(a)及び(b)に示す権限の行使の結果を連絡する。筆頭監督者は，不適切な遅滞なく，JON に対し及び当該不可欠な ICT サードパーティサービスプロバイダの ICT サービスを利用している金融機関の職務権限のある当局に対し，第 1 項(c)に示す報告書を送付する。

The Lead Overseer shall inform the JON of the outcome of the exercise of the powers referred to in paragraph 1, points (a) and (b). The Lead Overseer shall, without undue delay, transmit the reports referred to in paragraph 1, point (c), to the JON and to the competent authorities of the financial entities using the ICT services of that critical ICT third-party service provider.

5. 不可欠な ICT サードパーティサービスプロバイダは，筆頭監督者と誠実に協力し，かつ，筆頭監督者の職務を満たすことの上で筆頭監督者を補助する。

Critical ICT third-party service providers shall cooperate in good faith with the Lead Overseer, and assist it in the fulfilment of its tasks.

6. 第 1 項(a)，(b)及び(c)の下における権限の行使によって講じられることが要求されている措置の全部または一部の不遵守の場合においては，かつ，それぞれの措置の通知を当該不可欠な ICT サードパーティサービスプロバイダが受領した日から少なくとも 30 暦日の期限の経過後において，筆頭監督者は，当該不可欠な ICT サードパーティサービスプロバイダに対して当該措置の遵守を強いるための定期制裁金を科す決定を採択する。

In the event of whole or partial non-compliance with the measures required to be taken pursuant to the exercise of the powers under paragraph 1, points (a), (b) and (c), and after the expiry of a period of at least 30 calendar days from the date on which the critical ICT third-party service provider received notification of the respective measures, the Lead Overseer shall adopt a decision imposing a periodic penalty payment to compel the critical ICT third-party service provider to comply with those measures.

7. 第 6 項に示す定期制裁金は，遵守が達成されるまで日単位で，かつ，当該不可欠な ICT サードパーティサービスプロバイダに対して定期制裁金を科す決定の通知後 6 か月の機関を超えない期間，科される。

The periodic penalty payment referred to in paragraph 6 shall be imposed on a daily basis until compliance is achieved and for no more than a period of six months following the notification of the decision to impose a periodic penalty

payment to the critical ICT third-party service provider.

8. 定期制裁金を科す決定の中で定められた日から起算される定期制裁金の額は，前事業年における当該不可欠な ICT サードパーティサービスプロバイダの全世界の平均日売上額の 1%までとする。制裁金の額を決定する際，筆頭監督者は，第 6 項に示す措置の不遵守と関連する以下の基準を考慮に入れる：

The amount of the periodic penalty payment, calculated from the date stipulated in the decision imposing the periodic penalty payment, shall be up to 1 % of the average daily worldwide turnover of the critical ICT third-party service provider in the preceding business year. When determining the amount of the penalty payment, the Lead Overseer shall take into account the following criteria regarding non-compliance with the measures referred to in paragraph 6:

(a) 不遵守の重大性及び継続期間；

the gravity and the duration of non-compliance;

(b) 不遵守が意図的に実行されたか過失によるものか；

whether non-compliance has been committed intentionally or negligently;

(c) 当該不可欠な ICT サードパーティサービスプロバイダの筆頭監督者との間の協力のレベル。

the level of cooperation of the ICT third-party service provider with the Lead Overseer.

第 1 副項の目的のために，一貫性のあるアプローチを確保するため，筆頭監督者は，JON 内において意見聴取を行う。

For the purposes of the first subparagraph, in order to ensure a consistent approach, the Lead Overseer shall engage in consultation within the JON.

9. 制裁金は，行政制裁金という性質をもつものとし，かつ，執行され得るものとする。執行は，その領土上において検査及びアクセスが実行される構成国において有効な民事手続の規定によって規律される。関係する構成国の裁判所は，不規則な執行の実行と関連する不服申立ての裁判管轄権をもつ。制裁金の額は，欧州連合の一般予算に入れられる。

Penalty payments shall be of an administrative nature and shall be enforceable. Enforcement shall be governed by the rules of civil procedure in force in the Member State on the territory of which inspections and access shall be carried out. Courts of the Member State concerned shall have jurisdiction over complaints related to irregular conduct of enforcement. The amounts of the penalty payments shall be allocated to the general budget of the European Union.

10. 筆頭監督者は，そのような開示が金融市場を深刻に危険に晒すような場合または関係する当事者に対して比例的ではない損害を生じさせるような場合を除き，科された全ての定期制裁金を公衆に対して開示する。

The Lead Overseer shall disclose to the public every periodic penalty payment that has been imposed, unless such disclosure would seriously jeopardise the financial markets or cause disproportionate damage to the parties involved.

11. 第 6 項の下における定期制裁金を科す前に，筆頭監督者は，審理手続に服する不可欠な ICT サードパーティサービスプロバイダの代表者に対し，審理上で聴聞を受ける機会を与え，かつ，審理手続に服する不可欠な ICT サードパーティサービスプロバイダが意見を陳述する機会をもった審理結果のみを筆頭監督者の決定の基礎とする。

Before imposing a periodic penalty payment under paragraph 6, the Lead Overseer shall give the representatives of the critical ICT third-party service provider subject to the proceedings the opportunity to be heard on the findings and shall base its decisions only on findings on which the critical ICT third-party service provider subject to the proceedings has had an opportunity to comment.

審理手続に服する者の防御の権利は，その審理手続において全面的に尊重される。審理手続に服する不可欠な ICT サードパーティサービスプロバイダは，他の者の事業活動上の秘密の保護における他の者の正当な利益に服して，記録へのアクセスをもつ権利を与えられる。記録へのアクセスの権利は，機密情報に対して，または，筆頭監督者の内部的な準備文書に対しては，拡張されてはならない。

The rights of the defence of the persons subject to the proceedings shall be fully respected in the proceedings. The critical ICT third-party service provider subject to the proceedings shall be entitled to have access to the file, subject to the legitimate interest of other persons in the protection of their business secrets. The right of access to the file shall not extend to confidential information or to the Lead Overseer's internal preparatory documents.

第 36 条 欧州連合の外における筆頭監督者の権限の行使

Article 36 **Exercise of the powers of the Lead Overseer outside the Union**

1. 第 31 条第 12 項の目的のために設けられた支店とのやりとりによっては，または，欧州連合内に所在する構内における監督活動の実行によっては監督の目的が達成され得ないときは，筆頭監督者は，不可欠な ICT サードパーティサービスプロバイダによって欧州連合の金融機関に対してサービスを提供する目的のために，欧州連合の金融機関の事業上の運営管理，機能またはサービスとの関係において保有されまたは何らかの方法で使用されている，経営，事業遂行または運営管理の事務所，構内，土地，建物またはその他の財産を含め，第三国内に所在する構内において，以下の諸条項に示す権限を行使できる:

When oversight objectives cannot be attained by means of interacting with the subsidiary set up for the purpose of Article 31(12), or by exercising oversight activities on premises located in the Union, the Lead Overseer may exercise the powers, referred to in the following provisions, on any premises located in a third-country which is owned, or used in any way, for the purposes of providing services to Union financial entities, by a critical ICT third-party service provider, in connection with its business operations, functions or services, including any administrative, business or operational offices, premises, lands, buildings or other properties:

(a) 第 35 条第 1 項(a);及び

in Article 35(1), point (a); and

(b) 第 38 条第 2 項(a), (b)及び(d)に従って第 35 条第 1 項(b), 並びに, 第 39 条第 1 項及び第 2 項(b)。

in Article 35(1), point (b), in accordance with Article 38(2), points (a), (b) and (d), and in Article 39(1) and (2), point (a).

第 1 副項に示す権限は, 以下の全ての条件に服して行使され得る:

The powers referred to in the first subparagraph may be exercised subject to all of the following conditions:

(i) この規則の下にある筆頭監督者の義務を全面的かつ実効的に遂行することができるようにするためには第三国内における検査の実行が必要であると筆頭監督者によって考えられている;

the conduct of an inspection in a third-country is deemed necessary by the Lead Overseer to allow it to fully and effectively perform its duties under this Regulation;

(ii) 第三国内における検査が, 欧州連合内の金融機関に対する ICT サービスの提供と直接に関連している;

the inspection in a third-country is directly related to the provision of ICT services to financial entities in the Union;

(iii) 関係する不可欠な ICT サードパーティサービスプロバイダが, 第三国内における検査の実行に同意している;かつ

the critical ICT third-party service provider concerned consents to the conduct of an inspection in a third-country; and

(iv) 関係する第三国の適格な当局が, 筆頭監督者から公式に通知を受け, かつ, その通知に対し

て異議を唱えなかった。

the relevant authority of the third-country concerned has been officially notified by the Lead Overseer and raised no objection thereto.

2. 欧州連合の機関及び構成国それぞれの職務権限を妨げることなく，第 1 項の目的のために，EBA，ESMA または EIOPA は，筆頭監督者及び当該第三国内における筆頭監督者の任務のためのその指定チームによる関係する第三国内における検査の円滑な実行を可能にするための第三国の適格な当局との間における行政協力協定を締結する。その協力協定は，欧州連合及びその構成国との関係において法律上の義務をつくり出してはならず，かつ，その協力協定は，構成国及び構成国の職務権限のある当局が当該第三国及びその第三国の適格な当局との間で二国間または多国間の協定を締結することを妨げてはならない。

Without prejudice to the respective competences of the Union institutions and of Member States, for the purposes of paragraph 1, EBA, ESMA or EIOPA shall conclude administrative cooperation arrangements with the relevant authority of the third country in order to enable the smooth conduct of inspections in the third country concerned by the Lead Overseer and its designated team for its mission in that third country. Those cooperation arrangements shall not create legal obligations in respect of the Union and its Member States nor shall they prevent Member States and their competent authorities from concluding bilateral or multilateral arrangements with those third countries and their relevant authorities.

これらの協力協定は，少なくとも，以下の要素の細目を定める：

Those cooperation arrangements shall specify at least the following elements:

(a) 関係する第三国の国家主権の下にある領土上における第 1 項第 1 副項に示す一般的な調査及び現場における検査が筆頭監督者及びその指定チームによる実行を可能とするための関係する第三国の適格な当局の同意の送付に関する細目を含め，この規則の下において実行される監督活動と，関係する第三国の適格な当局によって実行される金融部門における ICT サードパーティリスクの類似の監視との調整のための手続；

the procedures for the coordination of oversight activities carried out under this Regulation and any analogous monitoring of ICT third-party risk in the financial sector exercised by the relevant authority of the third country concerned, including details for transmitting the agreement of the latter to allow the conduct, by the Lead Overseer and its designated team, of general investigations and on-site inspections as referred to in paragraph 1, first subparagraph, on the territory under its jurisdiction;

(b) とりわけ，第 37 条により筆頭監督者から要求され得る情報との関係において，EBA，ESMA または EIOPA と関係する第三国の適格な当局との間の適格な情報の送付のための仕組み；

the mechanism for the transmission of any relevant information between EBA, ESMA or EIOPA and the relevant authority of the third country concerned, in particular in connection with information that may be requested by the Lead Overseer pursuant to Article 37;

(c) 第三国内に拠点をもちかつ第 31 条第 1 項(a)に従って不可欠として指定された ICT サードパーティサービスプロバイダが，当該第三国内の金融機関に対してサービスを提供する際，関係する第三国の適用可能な法律により依るべきことが強制されている要件に違反したと考えられている案件並びに適用された解消策及び制裁について，関係する第三国の適格な当局から EBA，ESMA または EIOPA に対する通知を促進するための仕組み；

the mechanisms for the prompt notification by the relevant authority of the third-country concerned to EBA, ESMA or EIOPA of cases where an ICT third-party service provider established in a third country and designated as critical in accordance with Article 31(1), point (a), is deemed to have infringed the requirements to which it is obliged to adhere pursuant to the applicable law of the third country concerned when providing services to financial institutions in that third country, as well as the remedies and penalties applied;

(d) 関係する第三国内の金融機関の ICT サードパーティリスクの監視に関する法制上または監督上の進展に関するアップデートの定期的な送付；

the regular transmission of updates on regulatory or supervisory developments on the monitoring of ICT third-party risk of financial institutions in the third country concerned;

(e) それが必要なときは，筆頭監督者及びその指定チームによって実行される検査への，適格な第三国の当局の 1 名の代表の参加を認めるための細目。

the details for allowing, if needed, the participation of one representative of the relevant third-country authority in the inspections conducted by the Lead Overseer and the designated team.

3. 筆頭監督者が第 1 項及び第 2 項に示す欧州連合外における監督活動を実行できないときは，筆頭監督者は:

When the Lead Overseer is not able to conduct oversight activities outside the Union, referred to in paragraphs 1 and 2, the Lead Overseer shall:

(a) 筆頭監督者にとって利用可能な全ての事実及び文書を基礎として，第 35 条の下における筆頭監督者の権限を行使し；

exercise its powers under Article 35 on the basis of all facts and documents available to it;

(b) 本条に示す予定された監督活動を筆頭監督者が実行できないことの結果を文書化しかつ説

明する。

document and explain any consequence of its inability to conduct the envisaged oversight activities as referred to in this Article.

本項(b)に示す結果として潜在的に生ずることは，第 35 条第 1 項(d)により発される筆頭監督者の勧告の中において考慮に入れられる。

The potential consequences referred to in point (b) of this paragraph shall be taken into consideration in the Lead Overseer's recommendations issued pursuant to Article 35(1), point (d).

第 37 条 情報提供の要求

Article 37 **Request for information**

1. 筆頭監督者は，簡易な要求によりまたは決定により，不可欠な ICT サードパーティサービスプロバイダに対し，全ての適格な事業遂行上または運営管理上の文書，契約，基本方針，関連文書，ICT セキュリティ監査報告書，ICT と関連するインシデント報告書，並びに，当該不可欠な ICT サードパーティサービスプロバイダが運営管理上の機能または活動をアウトソースした者と関連する情報を含め，この規則の下にある筆頭監督者の義務を遂行するために筆頭監督者にとって必要となる全ての情報を提供することを要求できる。

The Lead Overseer may, by simple request or by decision, require critical ICT third-party service providers to provide all information that is necessary for the Lead Overseer to carry out its duties under this Regulation, including all relevant business or operational documents, contracts, policies, documentation, ICT security audit reports, ICT-related incident reports, as well as any information relating to parties to whom the critical ICT third-party service provider has outsourced operational functions or activities.

2. 第 1 項の下において情報提供を求める簡易な要求を送付する際，筆頭監督者は:

When sending a simple request for information under paragraph 1, the Lead Overseer shall:

(a) その要求の法律上の根拠として，本条を示し;

refer to this Article as the legal basis of the request;

(b) その要求の目的を述べ;

state the purpose of the request;

(c) どの情報が要求されているかの細目を示し；

specify what information is required;

(d) その情報が提供されるべき期限を設定し；

set a time limit within which the information is to be provided;

(e) その情報が要求されている不可欠な ICT サードパーティサービスプロバイダの代表者に対し，彼または彼女は情報を提供することを強いられないが，要求に対して任意に返答する場合には，提供される情報は不正確または誤解を招くものであってはならないということを連絡する。

inform the representative of the critical ICT third-party service provider from whom the information is requested that he or she is not obliged to provide the information, but in the event of a voluntary reply to the request the information provided must not be incorrect or misleading.

3. 第 1 項の下において情報を供給することを決定により要求する場合，筆頭監督者は：

When requiring by decision to supply information under paragraph 1, the Lead Overseer shall:

(a) その要求の法律上の根拠として，本条を示し；

refer to this Article as the legal basis of the request;

(b) その要求の目的を述べ；

state the purpose of the request;

(c) どの情報が要求されているかの細目を示し；

specify what information is required;

(d) その情報が提供されるべき期限を設定し；

set a time limit within which the information is to be provided;

(e) 要求された情報の作成が完了しない場合またはそのような情報が本項(d)に示す期限内に提供されない場合の第 35 条第 6 項の中で定められている定期制裁金を表示し；

indicate the periodic penalty payments provided for in Article 35(6) where the production of the required

information is incomplete or when such information is not provided within the time limit referred to in point (d) of this paragraph;

(f) 規則(EU) No 1093/2010, 規則(EU) No 1094/2010 及び規則(EU) No 1095/2010 の各第 60 条及び各第 61 条に従い, ESA の不服審理委員会において当該決定に対して不服申立てする権利及び欧州連合司法裁判所（司法裁判所）において当該決定を見直しさせる権利を表示する。

indicate the right to appeal the decision to ESA's Board of Appeal and to have the decision reviewed by the Court of Justice of the European Union (Court of Justice) in accordance with Articles 60 and 61 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.

4. 不可欠な ICT サードパーティサービスプロバイダの代表者は, 要求された情報を供給する。適正に訴訟行為を授権された法律家は, 当該顧客の代わりに情報を供給できる。供給された情報が不完全, 不正確または誤解を招くものであるときは, 不可欠な ICT サードパーティサービスプロバイダは, 全面的に責任を負い続ける。

The representatives of the critical ICT third-party service providers shall supply the information requested. Lawyers duly authorised to act may supply the information on behalf of their clients. The critical ICT third-party service provider shall remain fully responsible if the information supplied is incomplete, incorrect or misleading.

5. 筆頭監督者は, 遅滞なく, 適格な不可欠な ICT サードパーティサービスプロバイダのサービスを利用する金融機関の職務権限のある当局に対し及び JON に対し, 情報を供給するため, 決定書のコピーを送付する。

The Lead Overseer shall, without delay, transmit a copy of the decision to supply information to the competent authorities of the financial entities using the services of the relevant critical ICT third-party service providers and to the JON.

第 38 条 一般的な調査

Article 38 **General investigations**

1. この規則の下にある筆頭監督者の義務を遂行するため, 筆頭監督者は, 第 40 条第 1 項に示す共同検討チームによる補佐を受け, それが必要なときは, 不可欠な ICT サードパーティサービスプロバイダの調査を実行できる。

In order to carry out its duties under this Regulation, the Lead Overseer, assisted by the joint examination team referred to in Article 40(1), may, where necessary, conduct investigations of critical ICT third-party service providers.

2. 筆頭監督者は, 以下のための権限をもつ:

The Lead Overseer shall have the power to:

(a) それが記録保存されている媒体の別を問わず，筆頭監督者の職務の実行にとって適格な記録，データ，手続及びそれら以外の物件を検討するため；

examine records, data, procedures and any other material relevant to the execution of its tasks, irrespective of the medium on which they are stored;

(b) そのような記録，データ，文書化された手続及びそれら以外の物件の認証されたコピーまたは抜粋を取得または入手するため；

take or obtain certified copies of, or extracts from, such records, data, documented procedures and any other material;

(c) 調査の対象事項及び目的と関連する事実または文書に関して口頭または書面による説明を求め，不可欠な ICT サードパーティサービスプロバイダの代表者を審問するため，並びに，その回答を記録するため；

summon representatives of the critical ICT third-party service provider for oral or written explanations on facts or documents relating to the subject matter and purpose of the investigation and to record the answers;

(d) それ以外の，調査の対象事項と関連する情報を収集する目的のために，質問を受けることに同意した自然人または法人に対して質問するため；

interview any other natural or legal person who consents to be interviewed for the purpose of collecting information relating to the subject matter of an investigation;

(e) 電話及びデータ送受信の記録を要求するため。

request records of telephone and data traffic.

3. 第 1 項に示す調査の目的のために筆頭監督者から権限を授与された官吏及びそれ以外の者は，調査の対象事項及び目的の細目を示す書面による許可証の作成に関し，それらの者の権限を行使する。

The officials and other persons authorised by the Lead Overseer for the purposes of the investigation referred to in paragraph 1 shall exercise their powers upon production of a written authorisation specifying the subject matter and purpose of the investigation.

同許可証は，要求された記録，データ，文書化された手続もしくはそれら以外の物件が作成されず

もしくは不完全である場合または不可欠な ICT サードパーティサービスプロバイダの代表者に対して問われた質問に対する回答が提供されずもしくは不完全な場合における第 35 条第 6 項の中で定められた定期制裁金も表示する。

That authorisation shall also indicate the periodic penalty payments provided for in Article 35(6) where the production of the required records, data, documented procedures or any other material, or the answers to questions asked to representatives of the ICT third-party service provider are not provided or are incomplete.

4. 不可欠な ICT サードパーティサービスプロバイダの代表者は，筆頭監督者の決定書に基く調査を受入れることを要求される。その決定書は，調査の対象事項及び目的，第 35 条第 6 項の中で定められた定期制裁金，規則(EU) No 1093/2010，規則(EU) No 1094/2010 及び規則(EU) No 1095/2010 の下において利用可能な法律上の救済並びに司法裁判所によって決定を見直させる権利の細目を示す。

The representatives of the critical ICT third-party service providers are required to submit to the investigations on the basis of a decision of the Lead Overseer. The decision shall specify the subject matter and purpose of the investigation, the periodic penalty payments provided for in Article 35(6), the legal remedies available under Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, and the right to have the decision reviewed by the Court of Justice.

5. 調査を開始する前の適時において，筆頭監督者は，当該不可欠な ICT サードパーティサービスプロバイダの ICT サービスを利用する金融機関の職務権限のある当局に対し，予定されている調査及び権限を授与された者の識別名を連絡する。

In good time before the start of the investigation, the Lead Overseer shall inform competent authorities of the financial entities using the ICT services of that critical ICT third-party service provider of the envisaged investigation and of the identity of the authorised persons.

筆頭監督者は，JON に対し，第 1 副項によって送付された全ての情報を伝達する。

The Lead Overseer shall communicate to the JON all information transmitted pursuant to the first subparagraph.

第 39 条 検査

Article 39 **Inspections**

1. この規則の下にある筆頭監督者の義務を遂行するため，筆頭監督者は，第 40 条第 1 項に示す共同検討チームによる補佐を受け，本店事務所，運営センター，二次的な構内のような，不可欠な ICT サードパーティサービスプロバイダの事業用の構内，土地または財物に対し，必要となる全ての現場における検査に入ることができ及び実行でき，並びに，現場の外における検査を実行できる。

In order to carry out its duties under this Regulation, the Lead Overseer, assisted by the joint examination teams referred to in Article 40(1), may enter in, and conduct all necessary onsite inspections on, any business premises, land or property of the ICT third-party service providers, such as head offices, operation centres, secondary premises, as well as to conduct off-site inspections.

第 1 副項に示す権限の行使の目的のために，筆頭監督者は，JON から意見聴取する。

For the purposes of exercising the powers referred to in the first subparagraph, the Lead Overseer shall consult the JON.

2. 現場における検査を実行するために筆頭監督者から権限を授与された官吏及びそれ以外の者は，以下のための権限をもつ：

The officials and other persons authorised by the Lead Overseer to conduct an on-site inspection shall have the power to:

(a) そのような事業用の構内，土地または財物に入るため；並びに

enter any such business premises, land or property; and

(b) 検査の期間内で，かつ，検査のために必要な範囲内で，そのような事業用の構内，冊子または記録を封印するため。

seal any such business premises, books or records, for the period of, and to the extent necessary for, the inspection.

関係する不可欠な ICT サードパーティサービスプロバイダの代表者が検査を受入れないときは，筆頭監督者から権限を授与された官吏及びそれ以外の者は，検査の対象事項及び目的並びに第 35 条第 6 項の中で定められた定期制裁金の細目を示す書面による許可証の作成に基づく当該官吏及びそれ以外の者の権限を行使する。

The officials and other persons authorised by the Lead Overseer shall exercise their powers upon production of a written authorisation specifying the subject matter and the purpose of the inspection, and the periodic penalty payments provided for in Article 35(6) where the representatives of the critical ICT third-party service providers concerned do not submit to the inspection.

3. 検査を開始する前の適時において，筆頭監督者は，当該不可欠な ICT サードパーティサービスプロバイダの ICT サービスを利用する金融機関の職務権限のある当局に対し，連絡する。

In good time before the start of the inspection, the Lead Overseer shall inform the competent authorities of the financial entities using that ICT third-party service provider.

4. 検査は，金融機関に対する ICT サービスの提供のために利用されまたはそれに貢献する全ての範

囲の適格な ICT システム，ネットワーク，機器，情報及びデータを包摂する。

Inspections shall cover the full range of relevant ICT systems, networks, devices, information and data either used for, or contributing to, the provision of ICT services to financial entities.

5. そのような通知が緊急もしくは危機的な状況のゆえに不可能な場合またはその検査もしくは監査が実効的ではなくなってしまう状況を導き得る場合を除き，筆頭監督者は，計画された現場における検査の前に，当該不可欠な ICT サードパーティサービスプロバイダに対し，合理的な通知を与える。

Before any planned on-site inspection, the Lead Overseer shall give reasonable notice to the critical ICT third-party service providers, unless such notice is not possible due to an emergency or crisis situation, or if it would lead to a situation where the inspection or audit would no longer be effective.

6. 不可欠な ICT サードパーティサービスプロバイダは，筆頭監督者の決定書によって命ぜられた現場における検査を受入れる。その決定書は，検査の対象事項及び目的の細目を示し，その検査が開始される日を確定し，かつ，第 35 条第 6 項の中で定められた定期制裁金，規則(EU) No 1093/2010，規則(EU) No 1094/2010 及び規則(EU) No 1095/2010 の下において利用可能な法律上の救済並びに司法裁判所によって決定を見直させる権利を表示する。

The critical ICT third-party service provider shall submit to on-site inspections ordered by decision of the Lead Overseer. The decision shall specify the subject matter and purpose of the inspection, fix the date on which the inspection shall begin and shall indicate the periodic penalty payments provided for in Article 35(6), the legal remedies available under Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, as well as the right to have the decision reviewed by the Court of Justice.

7. 筆頭監督者から権限を授与された官吏及びそれ以外の者が，不可欠な ICT サードパーティサービスプロバイダが本条によって命ぜられた検査に反対していると判断するときは，筆頭監督者は，当該不可欠な ICT サードパーティサービスプロバイダに対し，適格な金融機関の職務権限のある当局が，当該不可欠な ICT サードパーティサービスプロバイダとの間で締結された契約上の取決めを終了させることを金融機関に対して要求する可能性を含め，そのような反対の結果として生ずることを連絡する。

Where the officials and other persons authorised by the Lead Overseer find that a critical ICT third-party service provider opposes an inspection ordered pursuant to this Article, the Lead Overseer shall inform the critical ICT third-party service provider of the consequences of such opposition, including the possibility for competent authorities of the relevant financial entities to require financial entities to terminate the contractual arrangements concluded with that critical ICT third-party service provider.

第 40 条 継続的な監督

Article 40 **Ongoing oversight**

1. 監督活動，とりわけ，一般的な調査または検査を実行する際，筆頭監督者は，個々の不可欠な ICT サードパーティサービスプロバイダ毎に設けられる共同検討チームによる補佐を受ける。

When conducting oversight activities, in particular general investigations or inspections, the Lead Overseer shall be assisted by a joint examination team established for each critical ICT third-party service provider.

2. 第 1 項に示す共同検討チームは，以下の組織の職員によって構成される：

The joint examination team referred to in paragraph 1 shall be composed of staff members from:

(a) ESAs；

the ESAs;

(b) 当該不可欠な ICT サードパーティサービスプロバイダが ICT サービスを提供している金融機関を監督する適格な職務権限のある当局；

the relevant competent authorities supervising the financial entities to which the critical ICT third-party service provider provides ICT services;

(c) 任意で，第 32 条第 4 項(e)に示す職務権限のある国内当局；

the national competent authority referred to in Article 32(4), point (e), on a voluntary basis;

(d) 任意で，当該不可欠な ICT サードパーティサービスプロバイダが拠点をもつ構成国の 1 つの職務権限のある国内当局。

one national competent authority from the Member State where the critical ICT third-party service provider is established, on a voluntary basis.

共同検討チームの構成員は，ICT の事項の専門知識及び運営管理上のリスクの専門知識をもつものとする。共同検討チームは，指定された筆頭監督者の職員（「筆頭監督者調整担当者」）の調整の下において作業する。

Members of the joint examination team shall have expertise in ICT matters and in operational risk. The joint examination team shall work under the coordination of a designated Lead Overseer staff member (the 'Lead Overseer coordinator').

3. 調査または検査の完了から 3 か月以内に，筆頭監督者は，監督フォーラムから意見聴取した後，第 35 条に示す権限によって不可欠な ICT サードパーティサービスプロバイダに宛てられた勧告書を採択する。
Within 3 months of the completion of an investigation or inspection, the Lead Overseer, after consulting the Oversight Forum, shall adopt recommendations to be addressed to the critical ICT third-party service provider pursuant to the powers referred to in Article 35.

4. 第 3 項に示す勧告書は，直ちに，不可欠な ICT サードパーティサービスプロバイダに対し及び当該不可欠な ICT サードパーティサービスプロバイダが ICT サービスを提供している金融機関の職務権限のある当局に対し，伝達される。

The recommendations referred to in paragraph 3 shall be immediately communicated to the critical ICT third-party service provider and to the competent authorities of the financial entities to which it provides ICT services.

監督活動を満たす目的のために，筆頭監督者は，適格な第三者認証書及び当該不可欠な ICT サードパーティサービスプロバイダによって利用できるようにされた ICT サードパーティの内部監査報告書または外部監査報告書を考慮に入れることができる。

For the purposes of fulfilling the oversight activities, the Lead Overseer may take into consideration any relevant third-party certifications and ICT third-party internal or external audit reports made available by the critical ICT third-party service provider.

第 41 条 監督活動の実行を可能とする条件の整合化

Article 41 **Harmonisation of conditions enabling the conduct of the oversight activities**

1. ESAs は，共同委員会を介して，以下の事項の細目を定める法制上の技術標準案を策定する:

The ESAs shall, through the Joint Committee, develop draft regulatory technical standards to specify:

(a) 第 31 条第 11 項の下において不可欠として指定されることの任意の求めのための申請書の中で ICT サードパーティサービスプロバイダから提供されるべき情報；

the information to be provided by an ICT third-party service provider in the application for a voluntary request to be designated as critical under Article 31(11);

(b) 下請契約上の取決めに関する情報を提供するための雛型を含め，第 35 条第 1 項によって不可欠な ICT サードパーティサービスプロバイダから提出され，開示されまたは報告される情報の内容，構造及び書式；

the content, structure and format of the information to be submitted, disclosed or reported by the ICT third-party service providers pursuant to Article 35(1), including the template for providing information on subcontracting arrangements;

(c) ESAs の職員と適格な職務権限のある当局の職員のバランスのとれた参加を確保する共同検討チームの構成，その職員の任命，職務及び作業覚書を決定するための基準；

the criteria for determining the composition of the joint examination team ensuring a balanced participation of staff members from the ESAs and from the relevant competent authorities, their designation, tasks, and working arrangements.

(d) 第 42 条第 3 項による筆頭監督者の勧告書を基礎とする，不可欠な ICT サードパーティサービスプロバイダによってとられた方策の職務権限のある当局の評価の細目。

the details of the competent authorities' assessment of the measures taken by critical ICT third-party service providers based on the recommendations of the Lead Overseer pursuant to Article 42(3).

2. ESAs は，欧州委員会に対し，2024 年 7 月 17 日までに，それらの法制上の技術標準案を提出する。

The ESAs shall submit those draft regulatory technical standards to the Commission by 17 July 2024.

規則(EU) No 1093/2010，規則(EU) No 1094/2010 及び規則(EU) No 1095/2010 の各第 10 条ないし第 14 条の中で定められた手続に従って第 1 項に示す法制上の技術標準を採択することによってこの規則を補遺するための権限は，欧州委員会に対して与えられる。

Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in paragraph 1 in accordance with the procedure laid down in Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.

第 42 条 職務権限のある当局による事後対応

Article 42 **Follow-up by competent authorities**

1. 第 35 条第 1 項(d)により筆頭監督者から発された勧告書の受領から 60 暦日以内に，不可欠な ICT サードパーティサービスプロバイダは，勧告書に従うという当該不可欠な ICT サードパーティサービスプロバイダの意図を筆頭監督者に対して通知し，または，そのような勧告書に従わないことに関する理由を付した説明を提供する。筆頭監督者は，直ちに，関係する金融機関の職務権限のある当局に対し，この情報を送付する。

Within 60 calendar days of the receipt of the recommendations issued by the Lead Overseer pursuant to Article 35(1),

point (d), critical ICT third-party service providers shall either notify the Lead Overseer of their intention to follow the recommendations or provide a reasoned explanation for not following such recommendations. The Lead Overseer shall immediately transmit this information to the competent authorities of the financial entities concerned.

2. 筆頭監督者は，不可欠な ICT サードパーティサービスプロバイダが第 1 項に従って筆頭監督者に対して通知しない場合，または，不可欠な ICT サードパーティサービスプロバイダから提供された説明が不十分であると考えられる場合，公開で開示する。公開される情報は，当該不可欠な ICT サードパーティサービスプロバイダの識別名並びに不遵守のタイプ及び性質に関する情報を開示する。そのような情報は，そのような公開が，関係する当事者に対して比例的ではない損害を生じさせるような場合，または，金融市場が正常に機能すること及び金融市場の完全性または欧州連合の金融システムの全部もしくは一部の安定性を深刻に危険に晒し得る場合を除き，公衆の認識の向上を確保する目的のために適格かつ比例的なところに限定される。

The Lead Overseer shall publicly disclose where a critical ICT third-party service provider fails to notify the Lead Overseer in accordance with paragraph 1 or where the explanation provided by the critical ICT third-party service provider is not deemed sufficient. The information published shall disclose the identity of the critical ICT third-party service provider as well as information on the type and nature of the non-compliance. Such information shall be limited to what is relevant and proportionate for the purpose of ensuring public awareness, unless such publication would cause disproportionate damage to the parties involved or could seriously jeopardise the orderly functioning and integrity of financial markets or the stability of the whole or part of the financial system of the Union.

筆頭監督者は，当該不可欠な ICT サードパーティサービスプロバイダに対し，当該公開の開示を通知する。

The Lead Overseer shall notify the ICT third-party service provider of that public disclosure.

3. 職務権限のある当局は，適格な金融機関に対し，第 35 条第 1 項(d)に従って不可欠な ICT サードパーティサービスプロバイダに宛てられた勧告書の中で特定されたリスクを連絡する。

Competent authorities shall inform the relevant financial entities of the risks identified in the recommendations addressed to critical ICT third-party service providers in accordance with Article 35(1), point (d).

ICT サードパーティリスクを取扱う際，金融機関は，第 1 副項に示すリスクを考慮に入れる。

When managing ICT third-party risk, financial entities shall take into account the risks referred to in the first subparagraph.

4. 金融機関が勧告書の中で特定された特定のリスクをその金融機関の ICT サードパーティリスクのマネジメントの範囲内で考慮に入れていないまたは十分に対処していないと職務権限のある当局が考えるときは，その職務権限のある当局は，当該金融機関に対し，そのようなリスクに対処することを狙

いとする適切な契約上の取決めがない場合，そのような通知の受領から 60 暦日以内に，本条第 6 項により，決定が行われる可能性があることを通知する。

Where a competent authority deems that a financial entity fails to take into account or to sufficiently address within its management of ICT third-party risk the specific risks identified in the recommendations, it shall notify the financial entity of the possibility of a decision being taken, within 60 calendar days of the receipt of such notification, pursuant to paragraph 6, in the absence of appropriate contractual arrangements aiming to address such risks.

5. 第 35 条第 1 項(c)に示す報告書の受領の後，かつ，本条第 6 項に示す決定を行う前に，職務権限のある当局は，任意に，指令(EU) 2022/2555 に服する必須法主体または重要法主体であって，不可欠な ICT サードパーティサービスプロバイダとして指定された法主体の監督に関する職責を負う同指令に従って指定されまたは設けられた職務権限のある当局から意見聴取できる。

Upon receiving the reports referred to in Article 35(1), point (c), and prior to taking a decision as referred to in paragraph 6 of this Article, competent authorities may, on a voluntary basis, consult the competent authorities designated or established in accordance with Directive (EU) 2022/2555 responsible for the supervision of an essential or important entity subject to that Directive, which has been designated as a critical ICT third-party service provider.

6. 職務権限のある当局は，最後の手段として，通知の後，かつ，それが適切なときは，本条第 4 項及び第 5 項に定める意見聴取の後，第 50 条に従い，不可欠な ICT サードパーティサービスプロバイダに宛てられた勧告書の中で特定されたリスクが対処されるまで，金融機関に対し，当該不可欠な ICT サードパーティサービスプロバイダから提供されるサービスの利用または配置を，その全部または一部において一時的に停止することを要求する決定を行うことができる。それが必要なときは，職務権限のある当局は，金融機関に対し，不可欠な ICT サードパーティサービスプロバイダとの間で締結された適格な契約上の取決めの全部または一部を終了させることを要求できる。

Competent authorities may, as a measure of last resort, following the notification and, if appropriate, the consultation as set out in paragraph 4 and 5 of this Article, in accordance with Article 50, take a decision requiring financial entities to temporarily suspend, either in part or completely, the use or deployment of a service provided by the critical ICT third-party service provider until the risks identified in the recommendations addressed to critical ICT third-party service providers have been addressed. Where necessary, they may require financial entities to terminate, in part or completely, the relevant contractual arrangements concluded with the critical ICT third-party service providers.

7. 不可欠な ICT サードパーティサービスプロバイダが，筆頭監督者から助言されたアプローチとは異なるアプローチを根拠として勧告書に依ることを拒否しており，かつ，そのような異なるアプローチが，多数の金融機関に対してまたは金融部門の大きな部分に対して負の影響を与えるかもしれず，かつ，職務権限のある当局から発された個別の警告が金融の安定性に対する潜在的なリスクを緩和する一貫性のあるアプローチを帰結しなかったときは，筆頭監督者は，監督フォーラムから意見聴取した上で，一貫性がありかつ収斂性のある監督上の事後対応を促進するため，職務権限のある当局に対し，しかるべく，拘束力がなくかつ非公開の意見書を発することができる。

Where a critical ICT third-party service provider refuses to endorse recommendations, based on a divergent approach from the one advised by the Lead Overseer, and such a divergent approach may adversely impact a large number of financial entities, or a significant part of the financial sector, and individual warnings issued by competent authorities have not resulted in consistent approaches mitigating the potential risk to financial stability, the Lead Overseer may, after consulting the Oversight Forum, issue non-binding and non-public opinions to competent authorities, in order to promote consistent and convergent supervisory follow-up measures, as appropriate.

8. 第 35 条第 1 項(c)に示す報告書の受領の後，職務権限のある当局は，本条第 6 項に示す決定を行う際，以下の諸基準に鑑み，当該不可欠な ICT サードパーティサービスプロバイダによって対処されていないリスクのタイプ及び影響度並びに不遵守の深刻度を考慮に入れる：

Upon receiving the reports referred to in Article 35(1), point (c), competent authorities, when taking a decision as referred to in paragraph 6 of this Article, shall take into account the type and magnitude of risk that is not addressed by the critical ICT third-party service provider, as well as the seriousness of the non-compliance, having regard to the following criteria:

(a) 不遵守の重大性及び継続期間；

the gravity and the duration of the non-compliance;

(b) その不遵守が，当該不可欠な ICT サードパーティサービスプロバイダの手続，マネジメントシステム，リスクマネジメント及び内部管理策における重大な弱点を明らかにしたかどうか；

whether the non-compliance has revealed serious weaknesses in the critical ICT third-party service provider's procedures, management systems, risk management and internal controls;

(c) 金融犯罪が容易にされたか，金融犯罪の機会を与えたか，また，それら以外に，その不遵守が金融犯罪の原因となったか否か；

whether a financial crime was facilitated, occasioned or is otherwise attributable to the non-compliance;

(d) 不遵守が意図的に実行されたか過失によるものか；

whether the non-compliance has been intentional or negligent;

(e) 当該契約上の取決めの停止または終了が，当該金融機関のサービスの提供における混乱を避けるための金融機関の努力に拘わらず，当該金融機関の事業上の運営管理の継続性に対するリスクを導入するどうか；

whether the suspension or termination of the contractual arrangements introduces a risk for continuity of the

financial entity's business operations notwithstanding the financial entity's efforts to avoid disruption in the provision of its services;

(f) それが適用可能なときは，指令(EU) 2022/2555 に服する必須法主体または重要法主体であって，不可欠な ICT サードパーティサービスプロバイダとして指定された法主体の監督に関する職責を負う同指令に従って指定されまたは設けられた職務権限のある当局の，本条第 5 項に従って任意に求められた意見；

where applicable, the opinion of the competent authorities designated or established in accordance with Directive (EU) 2022/2555 responsible for the supervision of an essential or important entity subject to that Directive, which has been designated as a critical ICT third-party service provider, requested on a voluntary basis in accordance with paragraph 5 of this Article.

金融機関のデジタル運営管理上の回復力に対する悪影響を避けるため，及び，第 28 条に示す出口戦略及び移行計画を金融機関が配置できるようにするため，職務権限のある当局は，金融機関に対し，不可欠な ICT サードパーティサービスプロバイダとの間の契約上の取決めを当該金融機関が補正できるようにするために必要な期間を与える。

Competent authorities shall grant financial entities the necessary period of time to enable them to adjust the contractual arrangements with critical ICT third-party service providers in order to avoid detrimental effects on their digital operational resilience and to allow them to deploy exit strategies and transition plans as referred to in Article 28.

9. 本条第 6 項に示す決定は，第 32 条第 4 項(a), (b)及び(c)に示す監督フォーラムの構成員に対し並びに JON に対し，通知される。

The decision referred to in paragraph 6 of this Article shall be notified to the members of the Oversight Forum referred to in Article 32(4), points (a), (b) and (c), and to the JON.

本条第 6 項の中で定められた決定による影響を受ける不可欠な ICT サードパーティサービスプロバイダは，とりわけ，当該不可欠な ICT サードパーティサービスプロバイダの契約上の取決めの停止または終了の過程という文脈において，影響を受ける金融機関と全面的に協力する。

The critical ICT third-party service providers affected by the decisions provided for in paragraph 6 shall fully cooperate with the financial entities impacted, in particular in the context of the process of suspension or termination of their contractual arrangements.

10. 職務権限のある当局は，筆頭監督者に対し，定期的に，金融機関との関係における当該職務権限のある当局の監督の職務においてとられたアプローチ及び措置に関し，並びに，筆頭監督者から当該不可欠な ICT サードパーティサービスプロバイダに宛てられた勧告書の全部または一部に不可欠な ICT サードパーティサービスプロバイダが依らない場合において金融機関によって締結された

契約上の取決めに関し，連絡する。

Competent authorities shall regularly inform the Lead Overseer on the approaches and measures taken in their supervisory tasks in relation to financial entities as well as on the contractual arrangements concluded by financial entities where critical ICT third-party service providers have not endorsed in part or entirely recommendations addressed to them by the Lead Overseer.

11. 筆頭監督者は，求めに応じて，事後対応措置に関して職務権限のある当局を導くために発された勧告書に関し，更に明確な説明を提供できる。

The Lead Overseer may, upon request, provide further clarifications on the recommendations issued to guide the competent authorities on the follow-up measures.

第 43 条 監督の手数料

Article 43 **Oversight fees**

1. 筆頭監督者は，本条第 2 項に示す委任される行為に従い，不可欠な ICT サードパーティサービスプロバイダに対し，第 40 条に示す共同検討チームによって実行された仕事の結果として負担され得る費用の弁償並びに直接的な監督活動の権限の下にある事柄との関係における第 32 条第 4 条第 2 副項に示す独立の専門家から提供される助言の費用の弁償を含め，この規則による監督の職務の実行との関係における筆頭監督者の必要的な支出の全部をまかなう手数料を課金する。

The Lead Overseer shall, in accordance with the delegated act referred to in paragraph 2 of this Article, charge critical ICT third-party service providers fees that fully cover the Lead Overseer's necessary expenditure in relation to the conduct of oversight tasks pursuant to this Regulation, including the reimbursement of any costs which may be incurred as a result of work carried out by the joint examination team referred to in Article 40, as well as the costs of advice provided by the independent experts as referred to in Article 32(4), second subparagraph, in relation to matters falling under the remit of direct oversight activities.

不可欠な ICT サードパーティサービスプロバイダに対して課金される手数料の額は，本節の中で定められた義務の遂行から生ずる全ての費用をまかなうものとし，かつ，当該不可欠な ICT サードパーティサービスプロバイダの総売上額と比例的なものとする。

The amount of a fee charged to a critical ICT third-party service provider shall cover all costs derived from the execution of the duties set out in this Section and shall be proportionate to its turnover.

2. 欧州委員会は，2024 年 7 月 17 日までに手数料の額及びその手数料が支払われる方法を決定することによってこの規則を補遺するため，第 57 条に従って委任される行為を採択する権限を与えられる。

The Commission is empowered to adopt a delegated act in accordance with Article 57 to supplement this Regulation by determining the amount of the fees and the way in which they are to be paid by 17 July 2024.

第 44 条 国際的な協力

Article 44 **International cooperation**

1. 第 36 条を妨げることなく，EBA，ESMA 及び EIOPA は，規則(EU) No 1093/2010，規則(EU) No 1095/2010 及び規則(EU) No 1094/2010 の各 33 条にそれぞれ従い，第三国の法制上の当局及び監督上の当局との間で，とりわけ，ICT リスクマネジメントの実務と管理策，緩和方策及びインシデント対応の見直しのためのベストプラクティスを策定することによって，異なる金融部門にわたる ICT サードパーティリスクに関する国際的な協力を育成するための行政協定を締結できる。

Without prejudice to Article 36, EBA, ESMA and EIOPA may, in accordance with Article 33 of Regulations (EU) No 1093/2010, (EU) No 1095/2010 and (EU) No 1094/2010, respectively, conclude administrative arrangements with third-country regulatory and supervisory authorities to foster international cooperation on ICT third-party risk across different financial sectors, in particular by developing best practices for the review of ICT risk management practices and controls, mitigation measures and incident responses.

2. ESAs は，共同委員会を介して，5 年毎に，欧州議会，理事会及び欧州委員会に対し，第 1 項に示す第三国の当局との間でもたれた適格な討議の結論を要約し，ICT サードパーティリスクの進化と，金融の安定性，市場の完全性，投資家の保護及び域内市場の稼動に対してもつ意味に焦点を当てる共同の秘密報告書を提出する。

The ESAs shall, through the Joint Committee, submit every five years a joint confidential report to the European Parliament, to the Council and to the Commission, summarising the findings of relevant discussions held with the third countries' authorities referred to in paragraph 1, focusing on the evolution of ICT third-party risk and the implications for financial stability, market integrity, investor protection and the functioning of the internal market.

第 VI 章 情報共有の取決め
CHAPTER VI **Information-sharing arrangements**

第 45 条 サイバー脅威の情報及び知識に関する情報共有の取決め
Article 45 **Information-sharing arrangements on cyber threat information and intelligence**

1. 金融機関は，金融機関間において，以下のような情報と知識の共有の範囲内で，混乱の指標，戦術，技法及び手続，サイバーセキュリティ警報及び設定ツールを含め，サイバー脅威の情報及び知識を交換できる:

Financial entities may exchange amongst themselves cyber threat information and intelligence, including indicators of compromise, tactics, techniques, and procedures, cyber security alerts and configuration tools, to the extent that such information and intelligence sharing:

(a) とりわけ，サイバー脅威との関係における認識を向上させること，サイバー脅威の拡大する能力を抑制または抑止すること，防御能力，脅威検出技法，緩和戦略または対応と修復の段階を支えることにより，金融機関のデジタル運営管理上の回復力を拡大することを狙いとし;

aims to enhance the digital operational resilience of financial entities, in particular through raising awareness in relation to cyber threats, limiting or impeding the cyber threats' ability to spread, supporting defence capabilities, threat detection techniques, mitigation strategies or response and recovery stages;

(b) 金融機関の信頼できるコミュニティ内に設けられ;

takes places within trusted communities of financial entities;

(c) 共有される情報の潜在的に機微な性質を保護し，かつ，事業活動上の機密性，規則(EU) 2016/679 に従った個人データの保護及び競争政策に関する運用指針を全面的に尊重する行動準則によって規律される情報共有覚書によって実装される。

is implemented through information-sharing arrangements that protect the potentially sensitive nature of the information shared, and that are governed by rules of conduct in full respect of business confidentiality, protection of personal data in accordance with Regulation (EU) 2016/679 and guidelines on competition policy.

2. 第 1 項(c)の目的のために，情報共有覚書は，参加の条件を定義し，かつ，それが適切なときは，行政機関の関与と行政機関が情報共有覚書に参加できる資格に関する細目，ICT サードパーティサービスプロバイダの関与に関する細目及び専用の IT プラットフォームの利用を含め，運用管理上の諸要素に関する細目を定める。

For the purpose of paragraph 1, point (c), the information-sharing arrangements shall define the conditions for

participation and, where appropriate, shall set out the details on the involvement of public authorities and the capacity in which they may be associated to the information-sharing arrangements, on the involvement of ICT third-party service providers, and on operational elements, including the use of dedicated IT platforms.

3. 金融機関は，職務権限のある当局に対し，当該金融機関の構成員資格が有効となった後，第 1 項に示す情報共有覚書への当該金融機関の参加を通知し，または，有効となっている当該金融機関の構成員資格の終了をしかるべく通知する。

Financial entities shall notify competent authorities of their participation in the information-sharing arrangements referred to in paragraph 1, upon validation of their membership, or, as applicable, of the cessation of their membership, once it takes effect.

第 VII 章 職務権限のある当局
CHAPTER VII **Competent authorities**

第 46 条 職務権限のある当局
Article 46 Competent authorities

この規則の第 V 章第 II 節に示す不可欠な ICT サードパーティサービスプロバイダの監督枠組みに関する条項を妨げることなく，この規則の遵守は，それぞれの法行為によって与えられた権限に従い，以下の職務権限のある当局によって確保される:

Without prejudice to the provisions on the Oversight Framework for critical ICT third-party service providers referred to in Chapter V, Section II, of this Regulation, compliance with this Regulation shall be ensured by the following competent authorities in accordance with the powers granted by the respective legal acts:

(a) 与信機関に関して及び指令 2013/36/EU によって適用除外となる機関に関しては，同指令の第 4 条に従って指定された職務権限のある当局，並びに，規則(EU) No 1024/2013 の第 6 条第 4 項に従って大きいと分類されている与信機関に関しては，同規則によって与えられた権限及び職務に従って ECB；

for credit institutions and for institutions exempted pursuant to Directive 2013/36/EU, the competent authority designated in accordance with Article 4 of that Directive, and for credit institutions classified as significant in accordance with Article 6(4) of Regulation (EU) No 1024/2013, the ECB in accordance with the powers and tasks conferred by that Regulation;

(b) 指令(EU) 2015/2366 により適用除外された決済機関を含め，決済機関，指令 2009/110/EC によって適用除外された電子マネー機関を含め，電子マネー機関及び指令(EU) 2015/2366 の第 33 条第 1 項に示す口座情報サービスプロバイダに関しては，指令(EU) 2015/2366 の第 22 条に従って指定された職務権限のある当局；

for payment institutions, including payment institutions exempted pursuant to Directive (EU) 2015/2366, electronic money institutions, including those exempted pursuant to Directive 2009/110/EC, and account information service providers as referred to in Article 33(1) of Directive (EU) 2015/2366, the competent authority designated in accordance with Article 22 of Directive (EU) 2015/2366;

(c) 投資企業に関しては，欧州議会及び理事会の指令(EU) 2019/2034[38]の第 4 条に従って指定された職務権限のある当局；

[38] 投資企業の健全性監督に関する並びに指令 2002/87/EC，指令 2009/65/EC，指令 2011/61/EU，指令 2013/36/EU，指令 2014/59/EU 及び指令 2014/65/EU を改正する欧州議会及び理事会の 2019 年 11 月 27 日の指令(EU) 2019/2034 (OJ L 314, 5.12.2019, p. 64).

for investment firms, the competent authority designated in accordance with Article 4 of Directive (EU) 2019/2034 of the European Parliament and of the Council[38];

(d) 暗号資産の市場に関する規則の下において認可された暗号資産サービスプロバイダ及び資産参照トークンの発行者に関しては，同規則の適格な条項に従って指定された職務権限のある当局；

for crypto-asset service providers as authorised under the Regulation on markets in crypto-assets and issuers of asset-referenced tokens, the competent authority designated in accordance with the relevant provision of that Regulation;

(e) 証券集中保管機関に関しては，規則(EU) No 909/2014 の第 11 条に従って指定された職務権限のある当局；

for central securities depositories, the competent authority designated in accordance with Article 11 of Regulation (EU) No 909/2014;

(f) 中央清算機関に関しては，規則(EU) No 648/2012 の第 22 条に従って指定された職務権限のある当局；

for central counterparties, the competent authority designated in accordance with Article 22 of Regulation (EU) No 648/2012;

(g) 取引場所及びデータ報告サービスプロバイダに関しては，指令 2014/65/EU の第 67 条に従って指定された職務権限のある当局及び規則(EU) No 600/2014 の第 2 条第 1 項第 18 号の中で定義された職務権限のある当局；

for trading venues and data reporting service providers, the competent authority designated in accordance with Article 67 of Directive 2014/65/EU, and the competent authority as defined in Article 2(1), point (18), of Regulation (EU) No 600/2014;

(h) 取引情報蓄積機関に関しては，規則(EU) No 648/2012 の第 22 条に従って指定された職務権限のある当局；

for trade repositories, the competent authority designated in accordance with Article 22 of Regulation (EU) No 648/2012;

Directive (EU) 2019/2034 of the European Parliament and of the Council of 27 November 2019 on the prudential supervision of investment firms and amending Directives 2002/87/EC, 2009/65/EC, 2011/61/EU, 2013/36/EU, 2014/59/EU and 2014/65/EU (OJ L 314, 5.12.2019, p. 64).

(i) オルタナティブ投資ファンド管理者に関しては，指令 2011/61/EU の第 44 条に従って指定された職務権限のある当局；

for managers of alternative investment funds, the competent authority designated in accordance with Article 44 of Directive 2011/61/EU;

(j) 資産管理会社に関しては，指令 2009/65/EC の第 97 条に従って指定された職務権限のある当局；

for management companies, the competent authority designated in accordance with Article 97 of Directive 2009/65/EC;

(k) 保険事業者及び再保険事業者に関しては，指令 2009/138/EC の第 30 条に従って指定された職務権限のある当局；

for insurance and reinsurance undertakings, the competent authority designated in accordance with Article 30 of Directive 2009/138/EC;

(l) 保険仲介事業者，再保険仲介事業者及び補助的な保険仲介事業者に関しては，指令(EU) 2016/97 の第 12 条に従って指定された職務権限のある当局；

for insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries, the competent authority designated in accordance with Article 12 of Directive (EU) 2016/97;

(m) 職域退職給付機関に関しては，指令(EU) 2016/2341 の第 47 条に従って指定された職務権限のある当局；

for institutions for occupational retirement provision, the competent authority designated in accordance with Article 47 of Directive (EU) 2016/2341;

(n) 与信格付機関に関しては，規則(EC) No 1060/2009 の第 21 条に従って指定された職務権限のある当局；

for credit rating agencies, the competent authority designated in accordance with Article 21 of Regulation (EC) No 1060/2009;

(o) 不可欠指標の管理者に関しては，規則(EU) 2016/1011 の第 40 条及び第 41 条に従って指定された職務権限のある当局；

for administrators of critical benchmarks, the competent authority designated in accordance with Articles 40 and

41 of Regulation (EU) 2016/1011;

(p) クラウドファンディングサービスプロバイダに関しては，規則(EU) 2020/1503 の第 29 条に従って指定された職務権限のある当局；

for crowdfunding service providers, the competent authority designated in accordance with Article 29 of Regulation (EU) 2020/1503;

(q) 証券化情報蓄積機関に関しては，規則(EU) 2017/2402 の第 10 条及び第 14 条第 1 項に従って指定された職務権限のある当局。

for securitisation repositories, the competent authority designated in accordance with Articles 10 and 14(1) of Regulation (EU) 2017/2402.

第 47 条　指令(EU) 2022/2555 により設けられた構造及び当局との間の協力

Article 47　**Cooperation with structures and authorities established by Directive (EU) 2022/2555**

1. この指令の下において指定された職務権限のある当局と指令(EU) 2022/2555 の第 14 条によって設けられた協力グループとの間の協力を育成し及び監督上の情報交換を実現可能にするため，ESAs 及び職務権限のある当局は，金融機関との関係における ESAs 及び職務権限のある当局の監督活動と関係する事柄に関し，協力グループの活動に参加できる。ESAs 及び職務権限のある当局は，この規則の第 31 条により不可欠な ICT サードパーティサービスプロバイダとしても指定された指令(EU) 2022/2555 に服する必須法主体または重要法主体との関係における事柄に関し，協力グループの活動への参加を招請されることを要求できる。

To foster cooperation and enable supervisory exchanges between the competent authorities designated under this Regulation and the Cooperation Group established by Article 14 of Directive (EU) 2022/2555, the ESAs and the competent authorities may participate in the activities of the Cooperation Group for matters that concern their supervisory activities in relation to financial entities. The ESAs and the competent authorities may request to be invited to participate in the activities of the Cooperation Group for matters in relation to essential or important entities subject to Directive (EU) 2022/2555 that have also been designated as critical ICT third-party service providers pursuant to Article 31 of this Regulation.

2. それが適切なときは，職務権限のある当局は，指令(EU) 2022/2555 に従って指定されまたは設けられた単一連絡部局または CSIRTs との間で意見聴取し及び情報共有できる。

Where appropriate, competent authorities may consult and share information with the single points of contact and the CSIRTs designated or established in accordance with Directive (EU) 2022/2555.

3. それが適切なときは，職務権限のある当局は，指令(EU) 2022/2555 に従って指定されまたは設けられた職務権限のある当局に対し，適格な技術上の助言と補助を求めることができ，かつ，実効的かつ迅速に対応する調整の仕組みが設置され得るようにするための協力覚書を結び得る。

Where appropriate, competent authorities may request any relevant technical advice and assistance from the competent authorities designated or established in accordance with Directive (EU) 2022/2555 and establish cooperation arrangements to allow effective and fast-response coordination mechanisms to be set up.

4. 本条第 3 項に示す覚書は，就中，調査及び現場における検査の国内法に従った実行のための手続，指令(EU) 2022/2555 に従って指定されまたは設けられた職務権限のある当局から求められた情報へのアクセスを含むこの指令の下における職務権限のある当局と同指令に従って指定されまたは設けられた職務権限のある当局との間の情報の交換に関する仕組みのための手続を含め，この規則の第 31 条により不可欠な ICT サードパーティサービスプロバイダとして指定された指令(EU) 2022/2555 に服する必須法主体または重要法主体との関係における監督活動及び監視活動の調整のための手続の細目を定めることができる。

The arrangements referred to in paragraph 3 of this Article may, inter alia, specify the procedures for the coordination of supervisory and oversight activities in relation to essential or important entities subject to Directive (EU) 2022/2555 that have been designated as critical ICT third-party service providers pursuant to Article 31 of this Regulation, including for the conduct, in accordance with national law, of investigations and on-site inspections, as well as for mechanisms for the exchange of information between the competent authorities under this Regulation and the competent authorities designated or established in accordance with that Directive which includes access to information requested by the latter authorities.

第 48 条 当局間の協力

Article 48 **Cooperation between authorities**

1. 職務権限のある当局は，当局間において緊密に協力し，かつ，それが適用可能なときは，筆頭監督者と協力する。

Competent authorities shall cooperate closely among themselves and, where applicable, with the Lead Overseer.

2. 職務権限のある当局と筆頭監督者は，適時の態様で，不可欠な ICT サードパーティサービスプロバイダと関係する情報であって，とりわけ，特定されたリスク，アプローチ及び筆頭監督者の監督の職務の一部として講じられた措置との関係において，この規則の下における職務権限のある当局と筆頭監督者それぞれの義務を遂行するための職務権限のある当局と筆頭監督者にとって必要となる全ての適格な情報を相互に交換する。

Competent authorities and the Lead Overseer shall, in a timely manner, mutually exchange all relevant information

concerning critical ICT third-party service providers which is necessary for them to carry out their respective duties under this Regulation, in particular in relation to identified risks, approaches and measures taken as part of the Lead Overseer's oversight tasks.

第 49 条　金融分野横断の演習，伝達及び協力

Article 49　**Financial cross-sector exercises, communication and cooperation**

1. ESAs は，共同委員会を介して，かつ，職務権限のある当局，指令 2014/59/EU の第 3 条に示す破綻処理当局，ECB，規則(EU) No 806/2014 の適用範囲内にある法主体と関連する情報に関しては単一破綻処理委員会，ESRB 及び ENISA としかるべく共働して，状況認識を拡大し及び諸部門にわたる共通のサイバー脆弱性とリスクを識別するための諸金融部門にわたる実効的な実務の共有を実現可能にする仕組みを設けることができる。

The ESAs, through the Joint Committee and in collaboration with competent authorities, resolution authorities as referred to in Article 3 of Directive 2014/59/EU, the ECB, the Single Resolution Board as regards information relating to entities falling under the scope of Regulation (EU) No 806/2014, the ESRB and ENISA, as appropriate, may establish mechanisms to enable the sharing of effective practices across financial sectors to enhance situational awareness and identify common cyber vulnerabilities and risks across sectors.

ESAs は，伝達経路を開発するという観点から及び欧州連合の金融部門全体に対してシステミックな影響をもつ国境を越える大きな ICT と関連するインシデントまたは ICT と関連する脅威が発生する場合における欧州連合レベルの実効的で調整された対応を段階的に実現可能にするという観点から，サイバー攻撃のシナリオを包摂する危機管理演習及び緊急事態対応演習を策定できる。

They may develop crisis management and contingency exercises involving cyber-attack scenarios with a view to developing communication channels and gradually enabling an effective coordinated response at Union level in the event of a major cross-border ICT-related incident or related threat having a systemic impact on the Union's financial sector as a whole.

それらの演習は，しかるべく，他の経済部門における金融機関の依存性も試験できる。

Those exercises may, as appropriate, also test the financial sector's dependencies on other economic sectors.

2. 職務権限のある当局，ESAs 及び ECB は，第 47 条ないし第 54 条による義務を遂行するため，相互に緊密に協力し，かつ，情報を交換する。職務権限のある当局，ESAs 及び ECB は，この規則の違反行為を発見及び解消するためのそれらの当局の監督を緊密に調整し，ベストプラクティスを開発及び促進し，共働を容易にし，解釈の一貫性を育成し，かつ，不同意が発生する場合においては国家主権横断的な評価を提供する。

Competent authorities, ESAs and the ECB shall cooperate closely with each other and exchange information to carry out their duties pursuant to Articles 47 to 54. They shall closely coordinate their supervision in order to identify and remedy breaches of this Regulation, develop and promote best practices, facilitate collaboration, foster consistency of interpretation and provide cross-jurisdictional assessments in the event of any disagreements.

第 50 条 行政制裁金及び是正措置

Article 50 Administrative penalties and remedial measures

1. 職務権限のある当局は，この規則の下にある職務権限のある当局の義務を満たすために必要となる全ての監督権限，調査権限及び制裁権限をもつ。

Competent authorities shall have all supervisory, investigatory and sanctioning powers necessary to fulfil their duties under this Regulation.

2. 第 1 項に示す権限は，少なくとも，以下のための権限を含む：

The powers referred to in paragraph 1 shall include at least the following powers to:

(a) 職務権限のある当局がその義務の遂行のために適格であると判断する全ての形態の文書またはデータへのアクセスをもち，及び，それを受領しまたはそのコピーを入手するため；

have access to any document or data held in any form that the competent authority considers relevant for the performance of its duties and receive or take a copy of it;

(b) 現場における検査または調査を実行するため，その検査または調査は，以下のものを含むがそれらに限定されない；

carry out on-site inspections or investigations, which shall include but shall not be limited to;

(i) 調査の対象事項及び目的と関連する事実または文書に関して口頭または書面による説明を求め，金融機関の代表者を審問するため，並びに，その回答を記録するため；

summoning representatives of the financial entities for oral or written explanations on facts or documents relating to the subject matter and purpose of the investigation and to record the answers;

(ii) それ以外の，調査の対象事項と関連する情報を収集する目的のために質問を受けることに同意した自然人または法人に対して質問するため；

interviewing any other natural or legal person who consents to be interviewed for the purpose of collecting

information relating to the subject matter of an investigation;

(c) この規則の要件の違反行為に対する訂正措置及び是正措置を要求するため。

require corrective and remedial measures for breaches of the requirements of this Regulation.

3. 第 52 条に従って刑事制裁を科す構成国の権利を妨げることなく，構成国は，この規則の違反行為に対する適切な行政制裁及び是正措置を定める規定を定め，かつ，それらの規定の実効的な実装を確保する。

Without prejudice to the right of Member States to impose criminal penalties in accordance with Article 52, Member States shall lay down rules establishing appropriate administrative penalties and remedial measures for breaches of this Regulation and shall ensure their effective implementation.

それらの制裁及び措置は，実効的であり，比例的でありかつ抑止力のあるものとする。

Those penalties and measures shall be effective, proportionate and dissuasive.

4. 構成国は，職務権限のある当局に対し，この規則の違反行為に対し，少なくとも，以下のことのための行政制裁または是正措置を適用する権限を与える：

Member States shall confer on competent authorities the power to apply at least the following administrative penalties or remedial measures for breaches of this Regulation:

(a) 自然人または法人に対し，この規則に違反する行為を終了すること及び当該行為の反復をしないことを要求する命令を発する；

issue an order requiring the natural or legal person to cease conduct that is in breach of this Regulation and to desist from a repetition of that conduct;

(b) この規則の条項に反すると職務権限のある当局が判断する実務または行為の一時的または恒久的な終了及び当該実務または行為の反復を防止することを要求すること；

require the temporary or permanent cessation of any practice or conduct that the competent authority considers to be contrary to the provisions of this Regulation and prevent repetition of that practice or conduct;

(c) 金銭的な性質の措置を含め，金融機関が法律上の要件を遵守し続けることを確保するための何らかのタイプの措置を採択すること；

adopt any type of measure, including of pecuniary nature, to ensure that financial entities continue to comply with

legal requirements;

(d) この規則の違反行為の合理的な疑いが存在する場合であり，かつ，この規則の違反行為の調査のためそのような記録が適格であり得る場合，国内法によって許容される限りにおいて，通信業務運用者によって保有されている既存のデータトラフィック記録を要求すること；並びに

require, insofar as permitted by national law, existing data traffic records held by a telecommunication operator, where there is a reasonable suspicion of a breach of this Regulation and where such records may be relevant to an investigation into breaches of this Regulation; and

(e) 当該自然人または法人の識別名及び違反行為の性質を表示する公的声明を含め，公的通知を発すること。

issue public notices, including public statements indicating the identity of the natural or legal person and the nature of the breach.

5. 第 2 項(c)及び第 4 項が法人に対して適用される場合，構成国は，職務権限のある当局に対し，国内法の中で定められた条件に服して，経営陣の構成員に対し，及び，それ以外の，国内法の下において当該違反行為に関して責任を負う個人に対し，行政制裁及び是正措置を適用するための権限を与える。

Where paragraph 2, point (c), and paragraph 4 apply to legal persons, Member States shall confer on competent authorities the power to apply the administrative penalties and remedial measures, subject to the conditions provided for in national law, to members of the management body, and to other individuals who under national law are responsible for the breach.

6. 構成国は，第 2 項(c)の中で定められた行政制裁または是正措置を加える決定が適正に理由に付すものであり，かつ，不服申立ての権利に服することを確保する。

Member States shall ensure that any decision imposing administrative penalties or remedial measures set out in paragraph 2, point (c), is properly reasoned and is subject to a right of appeal.

第 51 条　行政制裁及び是正措置を加える権限の行使

Article 51 **Exercise of the power to impose administrative penalties and remedial measures**

1. 職務権限のある当局は，しかるべく，以下のとおりに，当該職務権限のある当局の国内法上の枠組みに従って第 50 条に示す行政制裁及び是正措置を加える権限を行使する：

Competent authorities shall exercise the powers to impose administrative penalties and remedial measures referred to in

Article 50 in accordance with their national legal frameworks, where appropriate, as follows:

(a) 直接に;

directly;

(b) 他の当局と共働して;

in collaboration with other authorities;

(c) 他の当局に対する委任により，当該職務権限のある当局の責任の下において;または

under their responsibility by delegation to other authorities; or

(d) 職務権限のある法務当局に対する申立てにより。

by application to the competent judicial authorities.

2. 職務権限のある当局は，第 50 条の下において加えられ得る行政制裁または是正措置のタイプ及び程度を決定する際，その違反行為が意図的であるかまたは過失からの帰結であるかの範囲，及び，しかるべく，以下の事項を含め，他の適格な全ての事情を考慮に入れる:

Competent authorities, when determining the type and level of an administrative penalty or remedial measure to be imposed under Article 50, shall take into account the extent to which the breach is intentional or results from negligence, and all other relevant circumstances, including the following, where appropriate:

(a) その違反行為の具現性，重大性及び持続期間;

the materiality, gravity and the duration of the breach;

(b) その違反行為に責任を負う自然人または法人の責任の程度;

the degree of responsibility of the natural or legal person responsible for the breach;

(c) 責任を負う自然人または法人の財力;

the financial strength of the responsible natural or legal person;

(d) それが確定され得る限り，責任を負う自然人または法人によって獲得された利益または回避された損失の重要性;

the importance of profits gained or losses avoided by the responsible natural or legal person, insofar as they can be determined;

(e) それが確定され得る限り，その違反行為によって生じた第三者の損失；

the losses for third parties caused by the breach, insofar as they can be determined;

(f) 当該自然人または法人によって獲得された利益または回避された損失を吐き出させることを確保する必要性を妨げることなく，責任を負う自然人または法人と職務権限のある当局との間の協力のレベル；

the level of cooperation of the responsible natural or legal person with the competent authority, without prejudice to the need to ensure disgorgement of profits gained or losses avoided by that natural or legal person;

(g) 責任を負う自然人または法人の既往の違反行為。

previous breaches by the responsible natural or legal person.

第 52 条 刑事制裁

Article 52 **Criminal penalties**

1. 構成国は，当該構成国の国内法の下にある刑事制裁に服する違反行為に関し，行政制裁または是正措置に関する規定を定めないことを決定できる。

Member States may decide not to lay down rules for administrative penalties or remedial measures for breaches that are subject to criminal penalties under their national law.

2. 構成国が，この規則の違反行為に関する刑事制裁を定めることを選択したときは，当該構成国は，この規則の違反行為に関して開始された犯罪捜査または刑事手続と関連する個別の情報を受領するために当該職務権限のある当局の国家主権の範囲内にある法務当局，訴追当局または刑事法務当局と連絡をとるために必要となる全ての権限並びにこの規則の目的のために協力すべき当該職務権限のある当局の義務を満たすために当局の他の当局に対し及び EBA，ESMA または EIOPA に対し同じ情報を提供するために必要となる全ての権限を職務権限のある当局がもつようにするための適切な措置が設けられることを確保する。

Where Member States have chosen to lay down criminal penalties for breaches of this Regulation, they shall ensure that appropriate measures are in place so that competent authorities have all the necessary powers to liaise with judicial, prosecuting, or criminal justice authorities within their jurisdiction to receive specific information related to criminal investigations or proceedings commenced for breaches of this Regulation, and to provide the same information to other

competent authorities, as well as EBA, ESMA or EIOPA to fulfil their obligations to cooperate for the purposes of this Regulation.

第 53 条 通知義務

Article 53 **Notification duties**

構成国は，2025 年 1 月 17 日までに，欧州委員会，ESMA，EBA 及び EIOPA に対し，適格な刑事法の条項を含め，本章を実装する法律，規則及び行政条項を通知する。構成国は，不適切な遅滞なく，欧州委員会，ESMA，EBA 及び EIOPA に対し，それらの法律，規則及び行政条項のその後の改正を通知する。

Member States shall notify the laws, regulations and administrative provisions implementing this Chapter, including any relevant criminal law provisions, to the Commission, ESMA, the EBA and EIOPA by 17 January 2025. Member States shall notify the Commission, ESMA, the EBA and EIOPA without undue delay of any subsequent amendments thereto.

第 54 条 行政制裁の公表

Article 54 **Publication of administrative penalties**

1. 職務権限のある当局は，不適切な遅滞なく，当該決定が当該制裁の名宛人に対して通知された後に当該制裁を不服とする不服申立てが存在しない行政制裁を科す決定を，当該職務権限のある当局の公式の Web サイト上で公表する。

   Competent authorities shall publish on their official websites, without undue delay, any decision imposing an administrative penalty against which there is no appeal after the addressee of the penalty has been notified of that decision.

2. 第 1 項に示す公表は，違反行為のタイプ及び性質，責任を負う者の識別名並びに科された制裁に関する情報を含める。

   The publication referred to in paragraph 1 shall include information on the type and nature of the breach, the identity of the persons responsible and the penalties imposed.

3. ケースバイケースの評価の後，職務権限のある当局が，法人の場合には識別名の公表もしくは自然人の場合には識別名と個人データの公表が比例的ではないようだ，個人データの保護との関係におけるリスクを含んでいるようだ，金融市場の安定性または現在進行中の捜査の遂行を危険に晒すようだ，または，それが確定され得る限り，関与する者に対して比例的ではない損害を与えるようだと判断するときは，その職務権限のある当局は，行政制裁を科す決定との関係において，以下の解決策中の 1 つを採択する：

Where the competent authority, following a case-by-case assessment, considers that the publication of the identity, in the case of legal persons, or of the identity and personal data, in the case of natural persons, would be disproportionate, including risks in relation to the protection of personal data, jeopardise the stability of financial markets or the pursuit of an ongoing criminal investigation, or cause, insofar as these can be determined, disproportionate damages to the person involved, it shall adopt one of the following solutions in respect of the decision imposing an administrative penalty:

(a) 公表しないこととする全ての理由が消滅するまで，行政制裁の公表を延期する；

defer its publication until all reasons for non-publication cease to exist;

(b) 国内法に従い，匿名ベースで行政制裁を公表する；または

publish it on an anonymous basis, in accordance with national law; or

(c) (a)及び(b)の中で定められた選択肢が金融市場の安定性に対する危険がないことを保証するためには十分ではないと考えられるとき，または，そのような公表が科される制裁の寛大さと比例的ではないときは，行政制裁を公表することを控える。

refrain from publishing it, where the options set out in points (a) and (b) are deemed either insufficient to guarantee a lack of any danger for the stability of financial markets, or where such a publication would not be proportionate to the leniency of the imposed penalty.

4. 第 3 項(b)に従って匿名ベースで行政制裁を公表するための決定の場合，関連データの公表は，延期され得る。

In the case of a decision to publish an administrative penalty on an anonymous basis in accordance with paragraph 3, point (b), the publication of the relevant data may be postponed.

5. 適格な法務当局における当該制裁を不服とする不服申立てが存在する行政制裁を科す決定を職務権限のある当局が公表している場合，各職務権限のある当局は，当該職務権限のある当局の公式の Web サイト上に当該情報を直ちに付加し，また，後の段階において，そのような不服申立ての結果に関するその後の関連情報を付加する。行政制裁を科す決定を無効にする法務上の決定もまた公表される。

Where a competent authority publishes a decision imposing an administrative penalty against which there is an appeal before the relevant judicial authorities, competent authorities shall immediately add on their official website that information and, at later stages, any subsequent related information on the outcome of such appeal. Any judicial decision annulling a decision imposing an administrative penalty shall also be published.

6. 職務権限のある当局は，第 1 項ないし第 4 項に示す公表が，本条を有効にするために必要となる

期間だけ当該職務権限のある当局の公式の Web サイト上に残されることを確保する。この期間は，その決定の公表から 5 年を超えてはならない。

Competent authorities shall ensure that any publication referred to in paragraphs 1 to 4 shall remain on their official website only for the period which is necessary to bring forth this Article. This period shall not exceed five years after its publication.

第 55 条 職業上の秘密

Article 55 **Professional secrecy**

1. この規則によって受領され，交換されまたは送信された機密の情報は，第 2 項の中で定められた職業上の秘密の条件に服する。

   Any confidential information received, exchanged or transmitted pursuant to this Regulation shall be subject to the conditions of professional secrecy laid down in paragraph 2.

2. 職業上の秘密の義務は，この規則による職務権限のある当局のために，または，監査人及び監査人によって契約締結された専門家を含め，当該の者に対してそれらの職務権限のある当局が当該職務権限のある当局の権限を委任した当局または市場の事業者または自然人もしくは法人のために働いている全ての者または働いていた全ての者に対して適用される。

   The obligation of professional secrecy applies to all persons who work, or who have worked, for the competent authorities pursuant to this Regulation, or for any authority or market undertaking or natural or legal person to whom those competent authorities have delegated their powers, including auditors and experts contracted by them.

3. この規則の下にある職務権限のある当局及び指令(EU) 2022/2555 に従って指定されまたは設けられた職務権限のある当局の間における情報交換を含め，職業上の秘密の適用のある情報は，欧州連合法または国内法によって定められた条項の効力による場合を除き，他の者または当局に対して開示されてはならない。

   Information covered by professional secrecy, including the exchange of information among competent authorities under this Regulation and competent authorities designated or established in accordance with Directive (EU) 2022/2555, shall not be disclosed to any other person or authority except by virtue of provisions laid down by Union or national law;

4. この規則によって職務権限のある当局の間で交換される事業上の条件または運営管理上の条件及びそれ以外の経済的事柄または個人的事柄と関係する全ての情報は，機密であると判断され，かつ，その伝達の時点において，当該職務権限のある当局が，そのような情報が開示され得ると述べている場合または法律上の手続のためにそのような開示が必要となる場合を除き，職業上の秘密の

要件に服する。

All information exchanged between the competent authorities pursuant to this Regulation that concerns business or operational conditions and other economic or personal affairs shall be considered confidential and shall be subject to the requirements of professional secrecy, except where the competent authority states, at the time of communication, that such information may be disclosed or where such disclosure is necessary for legal proceedings.

第 56 条 データ保護

Article 56 **Data Protection**

1. ESAs と職務権限のある当局は，この規則による当該職務権限のある当局それぞれの義務を実行することの目的のために必要となる場合，とりわけ，調査，検査，情報提供の要求，伝達，公表，査定，検証，評価及び監督計画の起草のために必要となる場合に限り，個人データを処理することが認められる。個人データは，それが適用可能であるときは常に，規則(EU) 2016/679 または規則(EU) 2018/1725 に従って処理される。

The ESAs and the competent authorities shall be allowed to process personal data only where necessary for the purpose of carrying out their respective obligations and duties pursuant to this Regulation, in particular for investigation, inspection, request for information, communication, publication, evaluation, verification, assessment and drafting of oversight plans. The personal data shall be processed in accordance with Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, whichever is applicable.

2. 他の部門の法行為の中で別異に定められている場合を除き，第 1 項に示す個人データは，そのようなデータを更に保持することを要する裁判所の手続が係属中である場合を除き，適用可能な監督上の義務が果たされるまで，かつ，いかなる場合においても，最長 15 年まで，保持される。

Except where otherwise provided in other sectoral acts, the personal data referred to in paragraph 1 shall be retained until the discharge of the applicable supervisory duties and in any case for a maximum period of 15 years, except in the event of pending court proceedings requiring further retention of such data.

第 VIII 章　委任される行為
CHAPTER VIII **Delegated acts**

第 57 条　委任の実行
Article 57 **Exercise of the delegation**

1. 委任される行為を採択する権限は，本条に定める条件に服して，欧州委員会に対して与えられる。

   The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. 第 31 条第 6 項及び第 43 条第 2 項に示す委任される行為を採択する権限は，2024 年 1 月 17 日から 5 年の期間，欧州委員会に対して与えられる。欧州委員会は，その 5 年の期間の最終日よりも前の遅くとも 9 か月以内に，その権限の委任に関する報告書を作成する。権限の委任は，欧州議会または理事会が各期間の最終日よりも前の遅くとも 3 か月以内にそのような延長に反対しない限り，同一の期間で，黙示で延長される。

   The power to adopt delegated acts referred to in Articles 31(6) and 43(2) shall be conferred on the Commission for a period of five years from 17 January 2024. The Commission shall draw up a report in respect of the delegation of power not later than nine months before the end of the five-year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period.

3. 第 31 条第 6 項及び第 43 条第 2 項に示す権限の委任は，いつでも，欧州議会または理事会によって取消され得る。取消しの決定は，同決定の中で指示される権限の委任を終了させる。その決定は，EU 官報上におけるその決定の公示の翌日に発効し，または，その決定の中で指定された後の日に発効する。その決定は，既に発効している委任される行為の有効性に影響を与えてはならない。

   The delegation of power referred to in Articles 31(6) and 43(2) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. 委任される行為を採択する前に，欧州委員会は，より良い立法に関する 2016 年 4 月 13 日の機関間合意の中で定められた基本原則に従い，各構成国によって指定された専門家から意見聴取する。

   Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the interinstitutional Agreement of 13 April 2016 on Better Law-Making.

5. 委員会が委任される行為を採択したときは直ちに，欧州委員会は，欧州議会及び理事会に対し，同時に，そのことを通知する。

As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

6. 第 31 条第 6 項及び第 43 条第 2 項によって採択された委任される行為は，欧州議会及び理事会に対する当該行為の通知から 3 か月以内に欧州議会もしくは理事会のいずれからも異議が表明されないとき，または，その期間が満了する前に，欧州議会及び理事会の両者が欧州委員会に対して異議を述べない旨を連絡したときに限り発効する。その期間は，欧州議会の発意または理事会の発意により，3か月まで延長される。

A delegated act adopted pursuant to Articles 31(6) and 43(2) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of three months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by three months at the initiative of the European Parliament or of the Council.

第 IX 章 経過措置条項及び最終条項
CHAPTER IX **Transitional and final provisions**

第 I 節
Section I

第 58 条 見直し条項
Article 58 **Review clause**

1. 2028 年 1 月 17 日までに，欧州委員会は，ESAs 及び ESRB からの意見聴取を経た上で，しかるべく，見直しを実行し，かつ，欧州議会及び理事会に対し，それが適切なときは立法提案を添えて，報告書を提出する。その見直しは，少なくとも，以下の事項を含める:

By 17 January 2028, the Commission shall, after consulting the ESAs and the ESRB, as appropriate, carry out a review and submit a report to the European Parliament and the Council, accompanied, where appropriate, by a legislative proposal. The review shall include at least the following:

(a) 第 31 条第 2 項に従った不可欠な ICT サードパーティサービスプロバイダの指定のための基準;

the criteria for the designation of critical ICT third-party service providers in accordance with Article 31(2);

(b) 第 19 条に示す大きなサイバー脅威の通知の任意という性質;

the voluntary nature of the notification of significant cyber threats referred to in Article 19;

(c) 第三国内に拠点をもつ不可欠な ICT サードパーティサービスプロバイダの実効的な監督を確保することと関連するそれらの条項の実効性及び欧州連合内に支店を設ける必要性を査定するという観点から，第 31 条第 12 項に示す制度及び第 35 条第 1 項(d)(iv)第 1 段の中で定められた筆頭監督者の権限;

the regime referred to in Article 31(12) and the powers of the Lead Overseer provided for in Article 35(1), point (d), point (iv), first indent, with a view to evaluating the effectiveness of those provisions with regard to ensuring effective oversight of critical ICT third-party service providers established in a third country, and the necessity to establish a subsidiary in the Union.

本号第 1 段落の目的のために，その見直しは，第三国からのサービスへの欧州連合の金融機関のアクセス及び欧州連合の市場におけるそのようなサービスの可用性という側面を含め，第 31 条第 12 項に示す制度の分析を含めるものとし，また，その見直しは，この規則によって包摂されるサービスのための市場における更なる進展，同制度の申請及びそれぞれの監督と

関連する金融機関と金融監督者の実務経験，並びに，国際的なレベルで起きている適格な法制上の進展及び監督上の進展を考慮に入れる。

For the purposes of the first subparagraph of this point, the review shall include an analysis of the regime referred to in Article 31(12), including in terms of access for Union financial entities to services from third countries and availability of such services on the Union market and it shall take into account further developments in the markets for the services covered by this Regulation, the practical experience of financial entities and financial supervisors with regard to the application and, respectively, supervision of that regime, and any relevant regulatory and supervisory developments taking place at international level.

(d) そのようなシステムの利用に関する将来の市場の発展に照らし，自動化された販売システムを活用している第 2 条第 3 項(e)に示す金融機関をこの規則の適用範囲内に含めることの適切性；

the appropriateness of including in the scope of this Regulation financial entities referred to in Article 2(3), point (e), making use of automated sales systems, in light of future market developments on the use of such systems;

(e) 監督枠組み内における監督の一貫性及び情報交換の効率性を支える上での JON の稼動及び実効性。

the functioning and effectiveness of the JON in supporting the consistency of the oversight and the efficiency of the exchange of information within the Oversight Framework.

2. 指令(EU) 2015/2366 の見直しの過程において，欧州委員会は，決済システム及び決済処理活動のサイバー回復力を増加させる必要性，並びに，決済システムの運用者及び決済処理活動に関与する法主体に対してこの規則の適用範囲を拡大することの適切性を評価する。この評価に照らし，欧州委員会は，2023 年 7 月 17 日以前に，指令(EU) 2015/2366 の評価の一部として，欧州議会及び理事会に対し，報告書を提出する。

In the context of the review of Directive (EU) 2015/2366, the Commission shall assess the need for increased cyber resilience of payment systems and payment-processing activities and the appropriateness of extending the scope of this Regulation to operators of payment systems and entities involved in payment-processing activities. In light of this assessment, the Commission shall submit, as part of the review of Directive (EU) 2015/2366, a report to the European Parliament and the Council no later than 17 July 2023.

同見直しの報告書を基礎として，かつ，ESAs，ECB 及び ESRB からの意見聴取を経た上で，欧州委員会は，それが適切なときは，かつ，指令(EU) 2015/2366 の第 108 条第 2 項により欧州委員会が採択できる立法提案の一部として，中央銀行の現行の監督を考慮に入れつつ，全ての決済システムの運用者及び決済処理活動に関与する法主体が適切な監督に服することを確保するための提案書を提出できる。

Based on that review report, and after consulting ESAs, ECB and the ESRB, the Commission may submit, where appropriate and as part of the legislative proposal that it may adopt pursuant to Article 108, second paragraph, of Directive (EU) 2015/2366, a proposal to ensure that all operators of payment systems and entities involved in payment-processing activities are subject to an appropriate oversight, while taking into account existing oversight by the central bank.

3. 2026 年 1 月 17 日までに，欧州委員会は，ESAs 及び欧州監査監督機関委員会からの意見聴取を経た上で，見直しを実行し，かつ，欧州議会及び理事会に対し，それが適切なときは，この規則の適用範囲内に法定の監査人及び監査法人を包摂することにより，及び，欧州議会及び理事会の指令 2006/43/EC[39]の改正により，デジタル運営管理上の回復力と関連する法定の監査人及び監査法人に対する強化された要件の適切性に関する立法提案を添えて，報告書を提出する。

By 17 January 2026, the Commission shall, after consulting the ESAs and the Committee of European Auditing Oversight Bodies, carry out a review and submit a report to the European Parliament and the Council, accompanied, where appropriate, by a legislative proposal, on the appropriateness of strengthened requirements for statutory auditors and audit firms as regards digital operational resilience, by means of the inclusion of statutory auditors and audit firms into the scope of this Regulation or by means of amendments to Directive 2006/43/EC of the European Parliament and of the Council[39].

[39] 年次決算書及び連結決算書の法定監査に関する，理事会指令 78/660/EEC 及び理事会指令 83/349/EEC を改正する並びに理事会指令 84/253/EEC を廃止する欧州議会及び理事会の 2006 年 5 月 17 日の指令 2006/43/EC (OJ L 157, 9.6.2006, p. 87).

Directive 2006/43/EC of the European Parliament and of the Council of 17 May 2006 on statutory audits of annual accounts and consolidated accounts, amending Council Directives 78/660/EEC and 83/349/EEC and repealing Council Directive 84/253/EEC (OJ L 157, 9.6.2006, p. 87).

第 II 節 改正
Section II Amendments

第 59 条 規則(EC) No 1060/2009 の改正
Article 59 Amendments to Regulation (EC) No 1060/2009

規則(EC) No 1060/2009 は，以下のとおり，改正される：

Regulation (EC) No 1060/2009 is amended as follows:

(1) 別紙 I のセクション A の第 4 号の第 1 段落は，以下の文によって置き換えられる：

in Annex I, Section A, point 4, the first subparagraph is replaced by the following:

「与信格付機関は，欧州議会及び理事会の規則(EU) 2022/2554(*)に従った良好な管理上及び会計上の手続，内部管理の仕組み，リスク評価のための実効的な手続，ICT システムを取扱うための実効的な管理及び安全確保の手立てをもつ。

‘A credit rating agency shall have sound administrative and accounting procedures, internal control mechanisms, effective procedures for risk assessment, and effective control and safeguard arrangements for managing ICT systems in accordance with Regulation (EU) 2022/2554 of the European Parliament and of the Council(*).

(*) 金融部門のデジタル運営管理上の回復力に関する並びに規則(EC) No 1060/2009, 規則(EU) No 648/2012, 規則(EU) No 600/2014, 規則(EU) No 909/2014 及び規則(EU) 2016/1011 を改正する欧州議会及び理事会の 2022 年 12 月 14 日の規則(EU) 2022/2554 (OJ L 333, 27.12.2022, p. 1).」；

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L 333, 27.12.2022, p. 1).’;

(2) 別紙 III の第 12 号は，以下の文によって置き換えられる：

in Annex III, point 12 is replaced by the following:

「12. 規則(EU) 2022/2554 に従った良好な経営上及び会計上の手続，内部管理の仕組み，リスク評価のための実効的な手続，ICT システムを取扱うための実効的な管理もしくは安全確保の手立てをもたないことによって；または，別紙 I のセクション A の第 4 号によって要求される意思決定手続もしくは組織構造を実装しないこともしくは維持しないことによって，同号と重畳的に第 6 条第 2 項に違反している与信格付機関」。

‘12. The credit rating agency infringes Article 6(2), in conjunction with point 4 of Section A of Annex I, by not

having sound administrative or accounting procedures, internal control mechanisms, effective procedures for risk assessment, or effective control or safeguard arrangements for managing ICT systems in accordance with Regulation (EU) 2022/2554; or by not implementing or maintaining decision-making procedures or organisational structures as required by that point.'.

第 60 条 規則(EC) No 648/2012 の改正

Article 60 **Amendments to Regulation (EU) No 648/2012**

規則(EC) No 648/2012 は，以下のとおり，改正される：

Regulation (EU) No 648/2012 is amended as follows:

(1) 第 26 条は，以下のとおり改正される：

Article 26 is amended as follows:

(a) 第 3 項は，以下の文によって置き換えられる：

paragraph 3 is replaced by the following:

「CCP は，CCP のサービス及び活動の遂行における継続性及び正常な稼働を確保する組織構造を維持管理及び運営管理する。CCP は，欧州議会及び理事会の規則(EU) 2022/2554 (*)に従って管理運営される ICT システムを含め，適切でありかつ比例的なシステム，資源及び手続を使用する。

'3. A CCP shall maintain and operate an organisational structure that ensures continuity and orderly functioning in the performance of its services and activities. It shall employ appropriate and proportionate systems, resources and procedures, including ICT systems managed in accordance with Regulation (EU) 2022/2554 of the European Parliament and of the Council(*).

(*) 金融部門のデジタル運営管理上の回復力に関する並びに規則(EC) No 1060/2009，規則(EU) No 648/2012，規則(EU) No 600/2014，規則(EU) No 909/2014 及び規則(EU) 2016/1011 を改正する欧州議会及び理事会の 2022 年 12 月 14 日の規則(EU) 2022/2554 (OJ L 333, 27.12.2022, p. 1).」；

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L 333, 27.12.2022, p. 1).';

(b) 第 6 項は，削除される；

paragraph 6 is deleted;

(2) 第 34 条は，以下のとおり改正される:

Article 34 is amended as follows:

(a) 第 1 項は，以下の文によって置き換えられる:

paragraph 1 is replaced by the following:

「1. CCP は，CCP の機能の保全，適時の運用の修復及び CCP の義務を満たすことを確保することを狙いとする適切な事業継続性の基本方針及び災害復旧計画を設け，実装しかつ維持管理し，その計画は，規則(EU) 2022/2554 に従って設けられかつ実装される ICT 事業継続性計画並びに ICT 対応計画及び ICT 復旧計画を含めるものとする。」;

‘1. A CCP shall establish, implement and maintain an adequate business continuity policy and disaster recovery plan, which shall include ICT business continuity policy and ICT response and recovery plans put in place and implemented in accordance with Regulation (EU) 2022/2554, aiming to ensure the preservation of its functions, the timely recovery of operations and the fulfilment of the CCP’s obligations.’;

(b) 第 3 項において，第 1 副項は，以下の文によって置き換えられる:

in paragraph 3, the first subparagraph is replaced by the following:

「3. 本条の一貫性のある適用を確保するため，ESMA は，ESCB の構成員からの意見聴取を経た上で，ICT 事業継続性計画及び災害復旧計画を除き，事業継続性計画及び災害復旧計画のミニマムの内容と要件の細目を定める法制上の技術標準案を策定する。」;

‘3. In order to ensure consistent application of this Article, ESMA shall, after consulting the members of the ESCB, develop draft regulatory technical standards specifying the minimum content and requirements of the business continuity policy and of the disaster recovery plan, excluding ICT business continuity policy and disaster recovery plans.’;

(3) 第 56 条第 3 項において，第 1 副項は，以下の文によって置き換えられる:

in Article 56(3), the first subparagraph is replaced by the following:

「3.　本条の一貫性のある適用を確保するため，ESMA は，ICT リスクマネジメントと関連する要件以外の，第 1 項に示す登録のための申請書の細目を定める法制上の技術標準案を策定する。」;

‘3. In order to ensure consistent application of this Article, ESMA shall develop draft regulatory technical standards specifying the details, other than for requirements related to ICT risk management, of the application for registration referred to in paragraph 1.’;

(4)　第 79 条において，第 1 項及び第 2 項は，以下の文によって置き換えられる:

in Article 79, paragraphs 1 and 2 are replaced by the following:

「1. 取引情報蓄積機関は，規則(EU)2022/2554 に従って管理運営される ICT システムを含め，適切なシステム，管理策及び手続を開発することによっても，運営管理上のリスクの発生源を特定しかつそれをミニマム化する。

‘1. A trade repository shall identify sources of operational risk and minimise them also through the development of appropriate systems, controls and procedures, including ICT systems managed in accordance with Regulation (EU)2022/2554.

2. 取引情報蓄積機関は，規則(EU) 2022/2554 に従って設けられる ICT 事業継続性計画並びに ICT 対応計画及び ICT 復旧計画を含め，取引情報蓄積機関の機能の維持管理，適時の運用の修復及び取引情報蓄積機関の義務を満たすことを確保することを狙いとする適切な事業継続性基本方針及び災害復旧計画を設け，実装しかつ維持管理する。」;

2. A trade repository shall establish, implement and maintain an adequate business continuity policy and disaster recovery plan including ICT business continuity policy and ICT response and recovery plans established in accordance with Regulation (EU) 2022/2554, aiming to ensure the maintenance of its functions, the timely recovery of operations and the fulfilment of the trade repository’s obligations.’;

(5)　第 80 条第 1 項は，削除される。

in Article 80, paragraph 1 is deleted.

(6)　別紙 I において，セクション II は，以下のとおり改正される:

in Annex I, Section II is amended as follows:

(a)　(a)及び(b)は，以下の文によって置き換えられる:

points (a) and (b) are replaced by the following:

「(a)　規則(EU)2022/2554 に従って管理運営される ICT システムを含め，適切なシステム，管理策及び手続を開発することによって，運営管理上のリスクの発生源を特定しないことによって，または，それらのリスクをミニマム化しないことによって第 79 条第 1 項に違反する取引情報蓄積機関；

‘(a) a trade repository infringes Article 79(1) by not identifying sources of operational risk or by not minimising those risks through the development of appropriate systems, controls and procedures including ICT systems managed in accordance with Regulation (EU) 2022/2554;

(b)　取引情報蓄積機関の機能の維持管理，適時の運用の修復及び取引情報蓄積機関の義務を満たすことを確保することを狙いとして規則(EU) 2022/2554 に従って設けられる適切な事業継続性基本方針及び災害復旧計画を定めないことによって，実装しないことによってまたは維持管理しないことによって第 79 条第 1 項に違反する取引情報蓄積機関；」；

(b) a trade repository infringes Article 79(2) by not establishing, implementing or maintaining an adequate business continuity policy and disaster recovery plan established in accordance with Regulation (EU) 2022/2554, aiming to ensure the maintenance of its functions, the timely recovery of operations and the fulfilment of the trade repository's obligations;';

(b)　(c)は，削除される。

point (c) is deleted.

(7)　別紙 III は，以下のとおり改正される：

Annex III is amended as follows:

(a)　セクション II は，以下のとおり改正される：

Section II is amended as follows:

(i)　(c)は，以下の文によって置き換えられる：

point (c) is replaced by the following:

「(c)　当該 Tier 2 CCP のサービス及び活動の遂行における継続性及び正常な稼働を確保する組織構造を維持管理しないことによってもしくは運営管理しないことによ

って，または，規則(EU)2022/2554 に従って管理運営される ICT システムを含め，適切かつ比例的なシステム，資源及び手続を使用しないことによって第 26 条第 3 項に違反する Tier 2 CCP；」；

‘(c) a Tier 2 CCP infringes Article 26(3) by not maintaining or operating an organisational structure that ensures continuity and orderly functioning in the performance of its services and activities or by not employing appropriate and proportionate systems, resources or procedures including ICT systems managed in accordance with Regulation (EU) 2022/2554;’;

(ii) (f)は，削除される。

point (f) is deleted.

(b) セクション III において，(a)は，以下の文によって置き換えられる：

in Section III, point (a) is replaced by the following:

「(a) 取引情報蓄積機関の機能の保全，適時の運用の修復及び当該 CCP の義務を満たすことを確保することを狙いとして規則(EU) 2022/2554 に従って設けられる適切な事業継続性基本方針並びに対応計画及び復旧計画であって，少なくとも，当該 CCP が確実性のある運用を継続できるようにするため及び予定日に清算を完了できるようにするため，破綻の時点において，全てのやりとりの復旧ができるようにするものを定めないことによって，実装しないことによってまたは維持管理しないことによって第 34 条第 1 項に違反する Tier 2 CCP；」。

‘(a) a Tier 2 CCP infringes Article 34(1) by not establishing, implementing or maintaining an adequate business continuity policy and response and recovery plan set up in accordance with Regulation (EU) 2022/2554, aiming to ensure the preservation of its functions, the timely recovery of operations and the fulfilment of the CCP’s obligations, which at least allows for the recovery of all transactions at the time of disruption to allow the CCP to continue to operate with certainty and to complete settlement on the scheduled date;’.

第 61 条 規則(EU) No 909/2014 の改正

Article 61 **Amendments to Regulation (EU) No 909/2014**

規則(EU) No 909/2014 の第 45 条は，以下のとおり改正される：

Article 45 of Regulation (EU) No 909/2014 is amended as follows:

(1) 第 1 項は，以下の文によって置き換えられる:

paragraph 1 is replaced by the following:

「1. CDS は，内部及び外部の運営管理上のリスクの発生源を特定し，かつ，欧州議会及び理事会の規則(EU) 2022/2554(*)に従って定められ及び運営管理される適切な ICT ツール，プロセス及び基本方針によることによっても，また，当該 CSD が運用している全ての証券清算システムを含め，他のタイプの運営管理上のリスクに関する他の適格な適切なツール，管理策及び手続によって，当該運営管理上のリスクの影響をミニマム化する。

‘1. A CSD shall identify sources of operational risk, both internal and external, and minimise their impact also through the deployment of appropriate ICT tools, processes and policies set up and managed in accordance with Regulation (EU) 2022/2554 of the European Parliament and of the Council (*), as well as through any other relevant appropriate tools, controls and procedures for other types of operational risk, including for all the securities settlement systems it operates.

———————————

(*) 金融部門のデジタル運営管理上の回復力に関する並びに規則(EC) No 1060/2009，規則(EU) No 648/2012，規則(EU) No 600/2014，規則(EU) No 909/2014 及び規則(EU) 2016/1011 を改正する欧州議会及び理事会の 2022 年 12 月 14 日の規則(EU) 2022/2554 (OJ L 333, 27.12.2022, p. 1).」;

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L 333, 27.12.2022, p. 1).’;

(2) 第 2 項は，削除される。

paragraph 2 is deleted;

(3) 第 3 項及び第 4 項は，以下の文によって置き換えられる:

paragraphs 3 and 4 are replaced by the following:

「3. 当該 CSD が提供するサービスに関しては及び当該 CSD が運用する個々の証券清算システムに関しては，CSD は，規則(EU) 2022/2554 に従って設けられる ICT 事業継続性計画並びに ICT 対応計画及び ICT 復旧計画を含め，運営管理の混乱の大きなリスクを示す出来事の場合において，当該 CSD のサービスの保全，適時の運用の修復及び CSD の義務を満たすことを確保するための適切な事業継続性基本方針及び災害復旧計画を設け，実装しかつ維持管理する。

‘3. For services that it provides as well as for each securities settlement system that it operates, a CSD shall establish, implement and maintain an adequate business continuity policy and disaster recovery plan, including

ICT business continuity policy and ICT response and recovery plans established in accordance with Regulation (EU) 2022/2554, to ensure the preservation of its services, the timely recovery of operations and the fulfilment of the CSD's obligations in the case of events that pose a significant risk to disrupting operations.

4. 第 3 項に示す計画は，規則(EU) 2022/2554 の第 12 条第 5 項及び第 7 項の中で定められた破綻の時点から，不可欠な IT システムが運用を再開できることを確保することによる場合を含め，CSD の参加者が確実性のある運用を継続できるようにするため及び予定日に清算を完了できるようにするため，破綻の時点における全てのやりとりと参加者のポジションの復旧を定める。」；

4. The plan referred to in paragraph 3 shall provide for the recovery of all transactions and participants' positions at the time of disruption to allow the participants of a CSD to continue to operate with certainty and to complete settlement on the scheduled date, including by ensuring that critical IT systems can resume operations from the time of disruption as provided for in Article 12(5) and (7) of Regulation (EU) 2022/2554.';

(4) 第 6 項は，以下の文によって置き換えられる：

paragraph 6 is replaced by the following:

「6. CSD は，当該 CSD が運用する証券清算システムの主要な参加者，並びに，サービスプロバイダ及びユーティリティプロバイダ及び他の CSDs または他の市場インフラが当該 CSD の運用に対して呈しているかもしれないリスクを特定し，監視し及び取扱う。CSD は，要請に応じて，職務権限のある当局及び適格な当局に対し，そのような特定されたリスクに関する情報を提供する。CSD は，職務権限のある当局及び適格な当局に対し，遅滞なく，ICT リスクと関係するもの以外の，そのようなリスクから帰結する運営管理上のインシデントも連絡する。」；

'6. A CSD shall identify, monitor and manage the risks that key participants in the securities settlement systems it operates, as well as service and utility providers, and other CSDs or other market infrastructures might pose to its operations. It shall, upon request, provide competent and relevant authorities with information on any such risk identified. It shall also inform the competent authority and relevant authorities without delay of any operational incidents, other than in relation to ICT risk, resulting from such risks.';

(5) 第 7 項において，第 1 副項は，以下の文によって置き換えられる：

in paragraph 7, the first subparagraph is replaced by the following:

「7. ESMA は，ESCB の構成員と緊密に協力して，ICT リスク以外の第 1 項及び第 6 項に示す運用管理上のリスクの細目を定めるため，並びに，第 3 項及び第 4 項に示す事業継続性基本方針及び災害復旧計画とそれらの評価手法を含め，それらのリスクを試験するため，それらのリスクに対処するためまたはそれらのリスクをミニマム化するための手法の細目を定めるための

法制上の技術標準案を策定する。」。

‘7. ESMA shall, in close cooperation with the members of the ESCB, develop draft regulatory technical standards to specify the operational risks referred to in paragraphs 1 and 6, other than ICT risk, and the methods to test, to address or to minimise those risks, including the business continuity policies and disaster recovery plans referred to in paragraphs 3 and 4 and the methods of assessment thereof.’.

第 62 条 規則(EU) No 600/2014 の改正

Article 62 **Amendments to Regulation (EU) No 600/2014**

規則(EU) No 600/2014 は，以下のとおり改正される:

Regulation (EU) No 600/2014 is amended as follows:

(1) 第 27 条 g は，以下のとおり改正される:

Article 27g is amended as follows:

(a) 第 4 項は，以下の文によって置き換えられる:

paragraph 4 is replaced by the following:

「4. APA は，欧州議会及び理事会の規則(EU) 2022/2554(*)の中で定められたネットワーク及び情報システムのセキュリティと関係する要件を遵守する。

‘4. An APA shall comply with the requirements concerning the security of network and information systems set out in Regulation (EU) 2022/2554 of the European Parliament and of the Council(*).

(*) 金融部門のデジタル運営管理上の回復力に関する並びに規則(EC) No 1060/2009, 規則(EU) No 648/2012, 規則(EU) No 600/2014, 規則(EU) No 909/2014 及び規則(EU) 2016/1011 を改正する欧州議会及び理事会の 2022 年 12 月 14 日の規則(EU) 2022/2554 (OJ L 333, 27.12.2022, p. 1).」;

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L 333, 27.12.2022, p. 1).’;

(b) 第 8 項において，(c)は，以下の文によって置き換えられる:

in paragraph 8, point (c) is replaced by the following:

「(c) 第 3 項及び第 5 項の中で定められた具体的な組織上の要件。」;

‘(c) the concrete organisational requirements laid down in paragraphs 3 and 5.’;

(2) 第 27 条 h は, 以下のとおり改正される:

Article 27h is amended as follows:

(a) 第 5 項は, 以下の文によって置き換えられる:

paragraph 5 is replaced by the following:

「5. CTP は, 規則(EU) 2022/2554 の中で定められたネットワーク及び情報システムのセキュリティと関係する要件を遵守する。」;

‘5. A CTP shall comply with the requirements concerning the security of network and information systems set out in Regulation (EU) 2022/2554.’.

(b) 第 8 項において, (e)は, 以下の文によって置き換えられる:

in paragraph 8, point (e) is replaced by the following:

「(e) 第 4 項の中で定められた具体的な組織上の要件。」;

‘(e) the concrete organisational requirements laid down in paragraph 4.’;

(3) 第 27 条 i は, 以下のとおり改正される:

Article 27i is amended as follows:

(a) 第 3 項は, 以下の文によって置き換えられる;

paragraph 3 is replaced by the following:

「3. ARM は, 規則(EU) 2022/2554 の中で定められたネットワーク及び情報システムのセキュリティと関係する要件を遵守する。」

‘3. An ARM shall comply with the requirements concerning the security of network and information systems set out in Regulation (EU) 2022/2554.’;

(b)　第 5 項において，(b)は，以下の文によって置き換えられる:

in paragraph 5, point (b) is replaced by the following:

「(b)　第 2 項及び第 4 項の中で定められた具体的な組織上の要件。」。

‘(b) the concrete organisational requirements laid down in paragraphs 2 and 4.’.

第 63 条　規則(EU) 2016/1011 の改正

Article 63　**Amendment to Regulation (EU) 2016/1011**

規則(EU) 2016/1011 の第 6 条において，以下の項が付加される:

In Article 6 of Regulation (EU) 2016/1011, the following paragraph is added:

「6.　不可欠指標に関しては，管理者は，欧州議会及び理事会の規則(EU) 2022/2554(*)に従った良好な管理上及び会計上の手続，内部管理の仕組み，リスク評価のための実効的な手続，ICT システムを取扱うための実効的な管理及び安全確保の手立てをもつ。

‘6. For critical benchmarks, an administrator shall have sound administrative and accounting procedures, internal control mechanisms, effective procedures for risk assessment, and effective control and safeguard arrangements for managing ICT systems in accordance with Regulation (EU) 2022/2554 of the European Parliament and of the Council (*).

(*) 金融部門のデジタル運営管理上の回復力に関する並びに規則(EC) No 1060/2009，規則(EU) No 648/2012，規則(EU) No 600/2014，規則(EU) No 909/2014 及び規則(EU) 2016/1011 を改正する欧州議会及び理事会の 2022 年 12 月 14 日の規則(EU) 2022/2554 (OJ L 333, 27.12.2022, p. 1).」。

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L 333, 27.12.2022, p. 1).’.

第 64 条　発効及び適用

Article 64　**Entry into force and application**

この規則は，EU 官報上におけるその公示の 20 日後に発効する。

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

この規則は，2025 年 1 月 17 日から適用される。

It shall apply from 17 January 2025

この規則は，その全体について拘束力があり，かつ，全ての構成国において直接に適用可能である。

This Regulation shall be binding in its entirety and directly applicable in all Member States.

2022 年 12 月 14 日にストラスブールにおいて行われた。

Done at Strasbourg, 14 December 2022.

欧州議会として	理事会として
長　R. METSOLA	長　M. BEK
For the European Parliament	For the Council
The President　R. METSOLA	The President　M. BEK

2025 Printed in Japan
ISSN 2432-6089
法と情報雑誌　第 10 巻第 5 号（通巻第 66 号）
The Law and Information Magazine vol.10 no.5 (consecutive no.66)

2025 年 6 月 23 日発行
発行者　夏井高人
発行所　法と情報研究会（代表 夏井高人）
東京都千代田区神田駿河台 1－1
学校法人明治大学研究棟
（非売品）