Matheson

DORA TOOLKIT

Harmonising ICT risk management for financial entities across the EU

CONTENTS

Introduction

Regulation (EU) 2022/2554 ("**DORA**") is a landmark piece of EU legislation which will harmonise the approach to ICT risk management for financial entities across the EU. DORA will apply to nearly all regulated financial entities in Ireland (and indeed the EU) and will have a significant impact at Board level, on the organisational design of financial entities, and upon in-scope entities' ICT risk management frameworks, supplier contracts and supply chain arrangements.

DORA is likely to constitute the most significant regulatory uplift many financial entities will be required to implement in 2025.

From an enforcement and liability perspective, non-compliance with DORA will constitute a 'prescribed contravention' in respect of which the Central Bank of Ireland (the "**Central Bank**") can take enforcement action, including the imposition of significant fines (up to the greater of €10 million or 10% of annual turnover) under the Central Bank's administrative sanctions procedure. In addition, there is the potential for individual liability for PCF and CF holders under the Fitness and Probity regime. Criminal penalties can also apply under DORA for non-compliance.

It is also conceivable that non-compliance with DORA could result in litigation in a number of ways. Customers of regulated entities who are impacted by a security incident and suffer financial loss could seek to bring claims, including claims pleading breach of statutory duty under DORA. In the context of corporate transactions, warranties given as to the status of an entity's DORA compliance could potentially result in future breach of warranty claims where the level of compliance falls short.

With less than 4 months to go until DORA takes effect (from 17 January 2025) it is essential that in-scope firms understand the obligations applicable to them and take steps to prepare for the commencement date as quickly as possible.

With that in mind, the Matheson DORA toolkit has been designed to give you a concise overview of what DORA means to you, and to explore some of the core concepts existing under DORA.

We hope you find the Matheson DORA toolkit useful and that it becomes your go-to resource for DORA going forward. As an e-book rather than a hard copy, we will from time to time update it as new secondary legislation and guidelines get published. In that way, we will be able to keep it up to date for you.

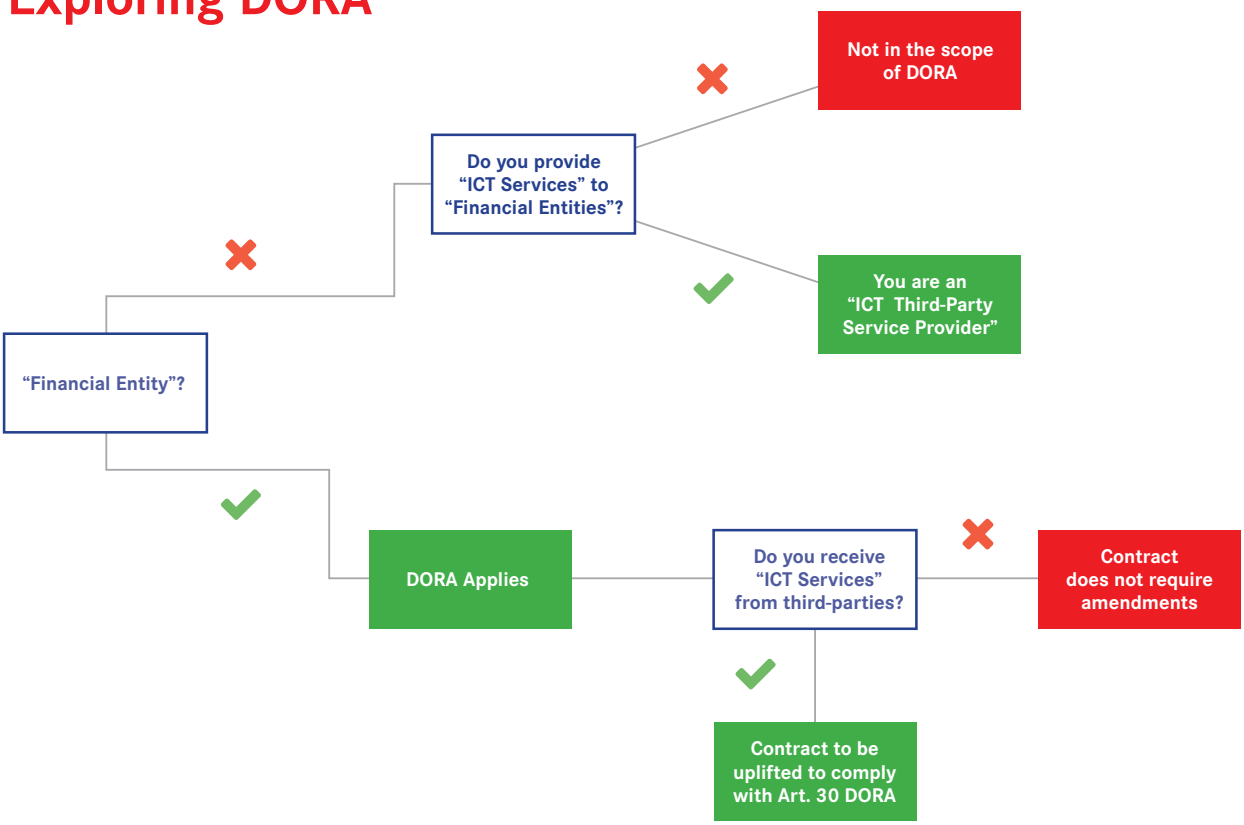
We recommend that this DORA toolkit be reviewed alongside our earlier Operational Resilience Toolkit (available here) and Outsourcing Toolkit (available here).

This toolkit does not address each and every aspect of DORA, but rather is intended to focus attention on the key aspects applicable to financial entities, and the resulting critical implementation steps.

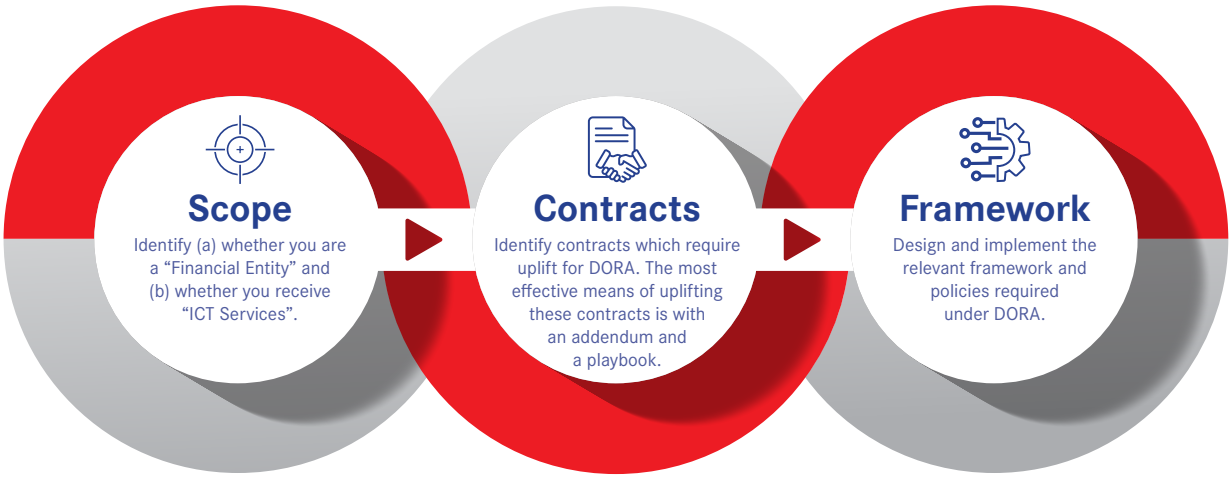
Firms should pay particular attention to the relevant regulatory technical standards, a list of which is available at Schedule 1 below.

Should you have any queries in respect of the materials included in this Toolkit, please do not hesitate to contact your usual Matheson contact, or one of the contacts listed herein.

Exploring DORA



Where Do We Start?



Key Pillars of DORA

Pillar 1: ICT Risk Management

Governance and Organisation (Article 5)

Board and Senior Management Responsibilities

The management body of the financial entity bears the ultimate responsibility for managing the financial entity's ICT risk, for putting relevant ICT risk policies in place and for setting and approving the digital operational resilience strategy of the entity. Some of the key responsibilities of the management body are set out below:

No.	Requirement	Guidance
1.	**Allocation of roles**	Set clear roles and responsibilities for all ICT-related functions and make sure appropriate governance arrangements are in place to ensure effective and timely communication, cooperation and coordination.
2.	**Monitor implementation**	Approve, oversee and periodically review the implementation of the financial entity's ICT business continuity policy and ICT response and recovery plans.
3.	**Review audit plans**	Approve and periodically review the financial entity's ICT internal audit plans, ICT audits and material modifications to them.
4.	**Allocate resources**	Allocate and periodically review the appropriate budget to fulfil the financial entity's digital operational resilience.
5.	**Approve third party ICT service providers**	Approve and periodically review the financial entity's policy on arrangements regarding the use of ICT services provided by ICT third-party service providers.
6.	**Designate responsibility for third party arrangements**	Establish a role in order to monitor the arrangements concluded with ICT third-party providers on the use of ICT services; or designate responsibility to a member of senior management for overseeing the related risk exposure and relevant documentation.
7.	**Keep up to date**	Keep up to date with requisite knowledge and skills to understand and assess ICT risk and its impact of the operations of the financial entity.

Practical Steps

- Arrange presentation to the Board on ICT governance arrangements, and business continuity and disaster recovery plans, and arrange for approval by the Board.
- Develop and implement an annual ICT specific training programme to ensure that relevant updates are being communicated and understood by senior management and staff.
- Review and approve ICT related audit plans (if not already standard practice).
- Update Board calendars and agendas to incorporate annual reviews of ICT risk management governance arrangements, business continuity and disaster recovery plans, ICT training and ICT audit plans.
- Update Board calendars and agendas to ensure necessary ad hoc or periodic reports and updates on ICT matters are provided to the Board, including allowing for "NIL" returns.
- Ensure a senior management member is appointed to have responsibility for overseeing ICT related risk exposures.
- Review and update procurement policies and procedures to ensure consistency with the obligations relating to assessment and review of ICT providers under DORA, taking into account applicable outsourcing obligations.

ICT Risk Management Framework (Article 6)

Financial entities must establish a sound, comprehensive and well documented ICT risk management framework in order to address ICT risk quickly and efficiently, ensuring a high level of digital operational resilience.

No.	Requirement	Guidance
1.	**Framework Requirements**	Financial entities must include strategies, policies, procedures, ICT protocols and tools needed to adequately protect all information assets and ICT assets, to ensure they are adequately protected from risks.
2.	**Minimise the impact**	Financial entities must minimise the impact of ICT risk by adopting appropriate strategies, policies, procedures, ICT protocols and tools.
3.	**Assign responsibility for ICT risk**	Financial entities must assign responsibility for managing and overseeing ICT risk to a control function and ensure that there is an adequate level of independence of such a control function, and appropriate segregation and independence of ICT risk management functions, control functions and internal audit functions.
4.	**Review ICT risk management framework**	Financial entities must document and review the ICT risk management framework: ▪ at least annually; ▪ following a major ICT-related incident; and ▪ following supervisory instruction or conclusions derived from testing or audit processes.
5.	**Internal Audit**	Financial entities must subject the framework to ▪ an internal audit by auditors on a regular basis; and ▪ follow-up processes based on the findings of the internal audit review.
6.	**Risk strategy measures**	The strategy must demonstrate how the framework will be implemented and how ICT risks will be addressed by: ▪ explaining how the framework supports the business strategy and objectives; ▪ establishing the risk tolerance level for ICT risk, and the impact tolerance for ICT disruptions; ▪ setting out clear information security objectives; ▪ explaining the ICT reference architecture and any changes needed to achieve specific business objectives; ▪ outlining the different mechanisms in place to detect ICT-related incidents, prevent their impact and provide protection from it; ▪ evidencing the current digital operational resilience situation based on the number of ICT-related incidents reported and the effectiveness of preventative measures; ▪ implementing digital operational resilience testing; and ▪ outlining a communication strategy in the event of ICT-related incidents.

No.	Requirement	Guidance
7.	**ICT Multi-Vendor Strategy**	Financial entities must define a holistic ICT multi-vendor strategy showing key dependencies on ICT third-party service providers and explain the rationale behind the mix of ICT third-party service providers.
8.	**Verification of Compliance**	Financial entities remain fully responsible for the verification of compliance with ICT risk management requirements to intra-group or external undertakings, where such tasks are outsourced.

Practical Steps

- Collate information and ICT asset register, identify group and third party ICT providers, and assess key dependencies and risks associated with assets and / or providers, including in the context of the overall business and strategy of the Financial Entity.
- Ensure associated key dependencies and risks are factored into overall ICT risk management policies and procedures.
- Agree the form and frequency of reviews of the ICT risk management framework and ensure Board calendars and agendas reflect this.
- As part of the ICT audit plan, ensure that the overall ICT risk framework is subject to periodic audit.
- Ensure that the internal audit function has the requisite ICT related knowledge appropriate to the identified ICT risks.
- Implement comprehensive ICT incident management procedures, including procedures for reporting to the Board following major incidents.
- Ensure ICT risk and audit procedures provide for reporting to the Board following ICT related testing, audits and supervisory interactions.
- Ensure that existing outsourcing frameworks are updated (where relevant) to take account of key ICT dependencies and risks, and the DORA requirements in relation to contracts and sub-contracting.
- Periodically assess the independence of the ICT risk control function.

ICT Systems, Protocols and Tools (Article 7)

No.	Requirement	Guidance
1.	**ICT System Requirements**	Financial entities must use and maintain ICT systems, protocols and tools that: ▪ are proportionate to the magnitude of operations supporting the conduct of their activities; ▪ are reliable; ▪ have sufficient capacity to accurately process the data necessary for the performance of activities and the timely provision of services, and to deal with peak volumes; and ▪ are technologically resilient to adequately deal with additional information processing needs as needed under stressed market conditions or other adverse situations.

Practical Steps

- Ensure governance procedures allow for reassessment and consideration of the ICT risk management framework in the context of any material change to the size and complexity of the Financial Entity's operations and / or data processing, including in the context of any proposed outsourcings.
- Determine parameters for stress testing of ICT systems, protocols and tools.

Identification (Article 8)

Financial entities must be able to 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.

No.	Requirement	Guidance
1.	**Adequacy**	Financial entities must review the adequacy of each classification on at least an annual basis.
2.	**Annual Review**	Financial entities should identify and review all risk sources and assess cyber threats and ICT vulnerabilities relevant to their ICT supported business functions, information assets and ICT assets at least annually.
3.	**Risk Assessments**	Financial entities should perform a risk assessment on each major change in the network and information system infrastructure, the processes or procedures affecting their ICT supported business functions, information assets or ICT assets.
4.	**Map information and ICT assets**	Financial entities should identify all information assets and ICT assets including those on remote sites, network resources and hardware equipment and map those considered critical.
5.	**ICT Third Party Service Providers**	Financial entities should identify and document all processes that are dependent on ICT third-party service providers and the interconnections with ICT third-party providers that provide services that support critical or important functions.
6.	**Inventories**	Financial entities should maintain relevant inventories and update them periodically and when a major change occurs.
7.	**ICT Risk Assessment**	Financial entities should conduct on at least an annual basis a specific ICT risk assessment on all legacy ICT systems.

Practical Steps

- Develop classification of ICT business functions, roles and responsibilities, and document links to and dependencies on information and ICT asset register, group and third party ICT providers, and other relevant risk sources. Reassess adequacy of classifications on at least an annual basis.
- Identify legacy ICT systems, reassess list on an annual basis, and ensure annual risk review of identified legacy systems.
- Periodically undertake project specific ICT risk assessments and undertake data protection impact assessments (DPIAs) alongside ICT risk assessments, as necessary.
- Maintain centralised records of group and third party ICT providers, in parallel with and not just where these constitute outsourcings, and ensure connections between these and ICT supported business functions are considered and recorded. The Central Bank has developed a template for recording all relevant outsourcing arrangements and for reporting purposes which can be accessed **here**.

Protection and Prevention (Article 9)

In order to adequately protect ICT systems, financial entities must continuously monitor and control the security and functioning of ICT systems and tools, and minimise the impact of ICT risk on ICT systems.

No.	Requirement	Guidance
1.	**ICT Systems and Data**	Financial entities should sign, procure and implement ICT security policies, procedures, protocols and tools to ensure the resilience, continuity and availability of ICT systems, and maintain high standards of availability, authenticity, integrity and confidentiality of data.
2.	**ICT Processes and Solutions**	Financial entities should use ICT solutions and processes which: ▪ ensure the security of the means of transfer of data; ▪ minimise the risk of corruption or loss of data, unauthorised access and technical flaws that may hinder business activity; ▪ prevent the lack of availability, the impairment of the authenticity and integrity, the breaches of confidentiality and the loss of data; and ▪ ensure that data is protected from risks arising from data management including poor administration, processing-related risks and human error.
3.	**Policies and Protocols**	As part of the ICT risk management framework, financial entities should ensure: ▪ the development and documentation of an information security policy defining rules to protect the availability, authenticity, integrity and confidentiality of data, information assets and ICT assets; ▪ following a risk-based approach, establishing a sound network and infrastructure management using appropriate techniques, methods and protocols that may include implementing automated mechanisms to isolate affected information assets in the event of cyber-attacks; ▪ 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 a set of policies, procedures and controls that address access rights and ensure a sound administration; ▪ implement policies and protocols for strong authentication mechanisms and protection measures of cryptographic keys; ▪ implement documented policies, procedures and controls for ICT change management, that are based on a risk assessment approach and are an integral part of the financial entity's overall change management process to ensure that all changes to ICT systems are recorded, assessed, approved, implemented and verified in a controlled manner; and ▪ have appropriate and comprehensive documented policies for patches and updates.

Practical Steps

- Identify risks and threats to data security and availability, and implement appropriate technical, operational and contractual security measures to protect same.
- Assess and update information security policies and procedures, including employee use policies and access protocols.
- Ensure access protocols are properly implemented and enforced.
- Consider extent to which GDPR related policies, procedures and tools can be leveraged to protect data more broadly.

Detection (Article 10)

Financial entities should have mechanisms in place to detect anomalous activities.

No.	Requirement	Guidance
1.	**Anomalous Activities**	Financial entities should have mechanisms in place to: ▪ identify potential material single points of failure; ▪ ensure that such mechanisms enable multiple layers of control, define alert thresholds and criteria to trigger and initiate ICT-related incident response processes; and ▪ devote sufficient resources and capabilities to monitor user activity, the occurrence of ICT anomalies and ICT-related incidents.

Practical Steps

- Document single points of failure identified as part of risk assessment and the control mechanisms implemented to monitor and mitigate such risks, including escalation and incident reporting mechanisms.

Pillar 2: ICT Third-Party Risk Management

General Principles (Article 28)

Management of third-party risk by a financial institution is considered an "integral component of ICT risk within their ICT risk management framework". The management of third-party ICT risk should be incorporated into the ICT risk management framework of financial entities. Before entering into agreements with ICT third party service providers, financial entities should assess the relevant risks and perform due diligence on any potential providers. Financial entities should also keep and maintain a register of all contractual arrangements with third party providers. All arrangements with providers should also comply with security standards; have verified auditors carry out audits and assessments; and include exit strategies and contingency measures.

No.	Requirement	Guidance
1.	**Proportionality**	Assess third-party ICT risk, accounting for: ▪ the complexity, nature and importance of the ICT-related service; ▪ risks stemming from contractual arrangements with TPP in view of the criticality, functionality and impact of services provided.
2.	**ICT Third Party Risk Strategy**	Develop regular reviews of their ICT third-party risk strategy; with reference to the financial entity's policy on the use of ICT service for critically important functions. Such reviews should be benchmarked against the overall complexity, risk profile and scale of the service being provided.
3.	**Maintain Register of Contractual Arrangements in Respect of ICT Services**	Ensure that the register contains all contractual arrangements on the use of ICT services rendered by TPP. Including: ▪ those arrangements that cover critical and important functions and those that do not; and ▪ annual reports to the competent authority on the category use and type of contractual arrangements with TPP. Further ensuring the availability of the full register upon request by the competent authority, informing them of any changes to same in a timely manner.
4.	**Contractual Assessment**	Financial entities should assess prospective contractual arrangements on the use of ICT services with reference to the following: ▪ do the arrangements cover critical/important functions? ▪ are Supervisory conditions for contracting met? ▪ identifying and categorising all risk in relation to the arrangement; ▪ the suitability of the TPP; and ▪ the potential for a conflict of interest stemming from the arrangement.
5.	**Compliance with Information Security Standards**	Ensure that any and all contractual arrangements entered into with a TPP employ the latest in Information Security Standards.

No.	Requirement	Guidance
6.	**Audit Requirements**	Set internal and external audits and assessments; where contractual arrangements are concluded with a TPP, and such agreements concern the use of ICT services of high technical complexity. Financial entities must ensure that such assessments are carried out by auditors of appropriate skills and knowledge.
7.	**Termination Requirements**	Develop arrangements for the termination of ICT services in the following circumstances: ▪ breaches by TPP of applicable laws, regulations and contractual terms; ▪ occurrences which are deemed capable of altering the performance of the contract, including material changes to the TPP; ▪ evidence of weakness in the TPP's overall ICT risk management; regarding the availability, authenticity, integrity and confidentiality of relevant data; and ▪ where the conditions/circumstances of the arrangement preclude the competent authority from its supervisory function.
8.	**Formulation of Exit Strategy**	Develop exit strategies for ICT services supporting critical/important functions in the following circumstances: ▪ disruption to the financial entity's business activities; ▪ limited compliance of TPP with regulatory requirements; and ▪ detrimental impact on the continuity and quality of service to clients.

Practical Steps

- Undertake periodic review of ICT third party risks and ICT risk strategy, and identify any existing arrangements which are outliers. Consider remediation strategy for those arrangements, including applicable rights under contracts.
- Consider proposed ICT contracts against ICT risk strategy and undertake third party risk assessment of the provider, taking into account the criticality of the ICT services and location risk.
- Review and update template ICT related agreements to reflect DORA contractual and sub-contracting requirements.
- Identify on centralised records of group and third party ICT providers which ones support critical and important functions, and assess contracts for compliance with DORA contract requirements.
- Ensure ongoing reviews of third-party ICT services against service level requirements in contracts.
- Ensure audit plans and procedures address relevant ICT provider and services audits.
- Establish clear policies and procedures in relation to critical or important functions provided by ICT third-party service providers and ensure those policies and procedures are subject to ongoing review by the management body.

Preliminary Assessment of ICT Risk (Article 29)

There are a number of considerations that financial entities should consider when identifying and assessing the risks associated with using ICT services supporting critical and important function, including contracting with a provider that is not easily substitutable, and having multiple contracts with closely connected ICT third party service providers. Financial entities must also consider the implications of subcontracting, and carry out a cost benefit analysis of alternative solutions.

No.	Requirement	Guidance
1.	**Cost Benefit Analysis**	Financial entities must conduct an analysis of the impact the proposed arrangement would have on critical or important functions, in particular: ▪ the substitutability of the ICT service being contracted into; ▪ the potential for overlapping contractual arrangements in place for ICT services.
2.	**Subcontracting Analysis**	Financial entities must conduct a risk analysis where there is a possibility that critical or important functions undertaken by a TPP could be subcontracted. With particular attention to be paid to potential subcontracting in third countries.
3.	**Insolvency Requirements**	Ensure that all contractual arrangements concerning ICT services of critical or important functions, consider: ▪ implications of TPP bankruptcy on the provision of service; and ▪ the recovery of the financial entity's data in the event of such insolvency.
4.	**Third Country Requirements**	Ensure that where the service provider is from a third country: ▪ compliance with the criteria at 2 (above) concerning the analysis of subcontracting agreements; and ▪ compliance with EU data protection rules and the effective enforcement of such laws in third countries.
5.	**Subcontracting Complexity**	Assess the length and complexity of any subcontracting agreement between the TPP and a subcontractor servicing critical or important functions. Ensuring the agreement does not impinge on either their, or the competent authorities', ability to supervise financial entities.

Practical Steps

- Ensure a pre-contractual due diligence review is conducted into any proposed arrangement, objectively weighing the benefits of the proposal against the risks to the provision of Financial Entity's services.
- Assess service location risks, including data and GDPR risks.
- Assess whether third party should be required to participate in the Financial Entity's training programme and reflect in written contract as appropriate.
- Where the provision of the ICT services also constitutes an outsouring, undertake an analysis of the impact of with reference also to the **Central Bank Cross-Industry Guidance on Outsourcing.**.
- Consider the potential impact of any sub-contracting by the ICT provider, and include a 'flow down' provision in TPP contracts passing on appropriate terms to any subcontract (or otherwise to ensure compliance by the subcontractor with such requirements).
- Review existing ICT arrangements against the above DORA requirements and consider remediation strategies for those arrangements which are not compliant, including change provisions and other applicable rights under contracts.
- Ensure ICT risk management strategies and business continuity plans take into account transitions between ICT providers and contingencies in the event of ICT contract terminations, including data recovery.

General Requirements for Contractual Provisions for ICT Service Providers (Article 30(2))

The below requirements are general ones, to be included in all contracts with all CTPP/TPP; regardless of the criticality or the importance of the function. Specific requirements for those contracts that cover critical and important functions are outlined in the checklist (Contractual Requirements for Critical and Important Functions) (**below**).

No.	Requirement	Guidance
1.	**Clear Descriptors**	Ensure that any third-party service provision is allocated and set out in writing. Written agreements should clearly set out out all functions, rights and obligations of the parties.
2.	**Location of Contract**	Set out the physical locations in which the services are to be carried out; including data processing, storage locations and any change in these locations, for the duration of the agreement.
3.	**Data Protection Requirements & Insolvency**	Ensure that service agreements with TPP contain provisions on the availability, authenticity, integrity and confidentiality of data, including personal data.
4.	**Service Level Descriptors**	Outline the expected level of service to be provided, as well as any updates/modifications expected to occur and appropriate corrective action in the event of service disruption.
5.	**ICT Service Provider Obligations**	Establish a clear obligation on the TPP to assist the financial entity for either no cost, or a cost that has been pre-determined.
6.	**Termination & Minimum Notice Period**	Ensure the agreement contains: ▪ termination rights; and ▪ minimum notice periods.
7.	**Digital Operational Resilience Requirements**	Detail any requirements upon the TPP to participate in the financial entity's digital security and awareness training programmes.
8.	**Standard Clauses**	When drafting the agreement, financial entities should consider the use of standard contractual clauses developed by public authorities for ICT services.

Practical Steps

- Implement procurement policies and procedures to ensure that all ICT agreements are formalised written arrangements, containing appropriate contractual terms, outlining the expectations, obligations and requirements of all parties, and written in clear and practical language to the greatest extent possible.
- Implement procedures to ensure all relevant ICT contracts are recorded on the centralised information and ICT asset register, and on the outsourcing contracts egister as appropriate.
- Review and update template ICT related agreements to reflect DORA contractual and sub-contracting requirements.
- Review existing ICT contracts against above DORA contract and sub-contracting requirements, and consider remediation strategies for those arrangements which are not compliant, including contract amendments, change provisions and other applicable rights under contracts.

Contractual Requirements For Critical And Important Functions (Article 30(3))

Where the service agreement covers critical or important functions, the below requirements are required to be included into such contractual arrangements, in addition to those outlined in the checklist (General Requirement for Contractual Provisions for ICT Service Provider) (**above**).

No.	Requirement	Guidance
1.	**Full Service Level Descriptors**	Management must ensure that the service agreement entered into contains precise quantitative and qualitative performance targets, ensuring: ▪ effective monitoring; and ▪ corrective action in the event of service disruption.
2.	**Notice Periods & Reporting Obligations**	The service agreement entered into must contain precise: ▪ notice periods; and ▪ reporting obligations. Ensuring that any development, which could have a material impact on the provision of critical or important functions, by the CTPP, is notifiable.
3.	**Third-Party Provider Obligations**	Agreements concerning CTPP and critical or important functions must contain: ▪ a business contingency plan tested and implemented by the TPP; ▪ an obligation on the third-party provider to participate fully in the financial entity's TLPT; and ▪ an obligation to fully cooperate with regulatory inspections and audits.
4.	**Monitoring Requirements**	The agreement must allow financial entities to monitor on an ongoing basis the CTPP performance, entailing: ▪ unrestricted access and auditory rights of all documentation critical to the provision of service; ▪ right to vary assurance levels in the event of interference with the financial entity's rights; and ▪ detail the scope and frequency of onsite inspections and audits of the third-party provider.
5.	**Exit Strategies**	The agreement must detail the establishment of exit strategies and transitionary periods, whereby: ▪ the TPP will continue to provide the service with a view to minimising disruption and risk to the financial entity during the transitional period; and ▪ the TPP will enable the financial entity to migrate to another provider or to transfer the critical or important function in-house.

Practical Steps

- Review and update template ICT related agreements related to critical and important functions to reflect DORA contractual and sub-contracting requirements.
- Review existing ICT contracts against DORA contract and sub-contracting requirements supporting critical and important functions, and consider remediation strategies for those arrangements which are not compliant, including contract amendments, change provisions and other applicable rights under contracts.

Pillar 3: Incident Reporting

Classification of ICT-related Incidents and Cyber Threats (Article 18)

Financial entities must define, establish and implement an ICT-related incident management process to detect, manage and notify ICT-related incidents.

No.	Requirement	Guidance
1.	**ICT Incident Reporting**	The ICT-related incident management process must: ▪ put in place early warning indicators; ▪ implement 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 per **Article 18(1)**; ▪ assign roles and responsibilities for different ICT-related incident types and scenarios; ▪ set out notification requirements to external stakeholders and media per **Article 14** and for notification to clients, internal escalation procedures, customer complaint procedures and provision of information to financial entities that act as counterparts, as appropriate; ▪ ensure that major ICT-related incidents are reported to relevant senior management and inform the management body of any major ICT-related incidents, explaining the impact, response and additional controls to be established; and ▪ establish ICT-related incident response procedures to mitigate impacts and ensure the resumption of security and services.
2.	**ICT Incidents Impact Classification Criteria**	Financial entities must classify ICT-related incidents, determining their impact based on the following criteria: ▪ clients or financial counterparts affected, the amount or number of transactions affected, and reputational damage; ▪ the duration of the ICT-related incident, including the service down-time; ▪ the geographical spread affected by the ICT-related incident, if it affects more than two Member States; ▪ the data losses that the ICT-related incident entails, in relation to availability, authenticity, integrity and confidentiality; ▪ the criticality of the services affected, including the financial entity's transactions and operations; and ▪ the economic impact of the ICT-related incident in both absolute and relative terms.

Harmonisation of Reporting Content and Templates

(Article 20)

Financial entities must record all ICT-related incidents and significant cyber threats, establishing appropriate procedures and processes to ensure a consistent and integrated monitoring, handling and follow-up of ICT related incidents to ensure that the root causes are identified, documented and addressed, in order to prevent the reoccurrence of such ICT related incidents

No.	Requirement	Guidance
1.	**Major ICT-Incidents Notification & Reporting**	Financial entities must produce the initial notification and reports using templates referred to in **Article 20**; ▪ The initial notification and reports must include all necessary information in relation to the ICT-related incident that will allow the competent authority to determine the significance of the major ICT-related incident; ▪ If technical difficulties prevent submission using the template, alternative means to notify the competent authority are available; and ▪ Member states may additionally determine that some or all financial entities must provide the initial notification and reports to the competent authorities or to the computer security incident response teams established in accordance with Directive (EU) 2022/2555 (NIS 2 Directive).
2.	**Voluntary Notification of Significant Cyber Threats.**	Financial entities may report when they deem a threat to be of relevance to: ▪ the financial system; and ▪ service users or clients.
3.	**ICT-Incident Client. Notification Requirements**	Where an ICT incident impacts clients, financial entities must without undue delay: ▪ inform clients of it; and ▪ the measures taken to mitigate the adverse effects of the incident. If there is a significant cyber threat, financial entities must inform any potential affected clients any appropriate protection measures under consideration by the financial entity.
4.	**Major ICT-Incident Obligations.**	Financial entities must in accordance with **Article 20** submit to the relevant competent authority: ▪ an initial notification; ▪ an intermediate report a soon as the status of the original incident has changed significantly, or its handling has changed based on new available information; ▪ updated notifications every time a relevant status update is available or upon specific request by the competent authority; and ▪ a final report when impact figures and the root cause analysis has been completed, and regardless of whether mitigation measures have been implemented.

No.	Requirement	Guidance
5.	**Outsourcing Reporting Requirements**	Financial entities may outsource the reporting obligations to a third-party service provider but remain fully responsible for the fulfilment of the incident reporting requirements.

Practical Steps

- Consider existing ICT incident management procedures and update to reflect DORA requirements and timelines.
- Document reporting thresholds, including if and when voluntary notifications may be made, and communicate these to appropriate personnel.
- Ensure procedures are in place for timely reporting of ICT incidents to the Board.
- Create a centralised register of Article 20 templates, including both internal and external communications, and establish procedures detailing all notification methods and reporting obligations to all relevant regulatory authorities.
- Implement a procedure to consider and ensure notification to customers where necessary.
- Ensure appropriate implementation of GPDR reporting procedures in parallel to ensure consistency.
- Maintain comprehensive records to ICT incidents.
- Implement and test a 'playbook' for incident notification which covers all regulatory notification requirements. This will likely include multiple regulators (such as the Central Bank and Data Protection Commission).
- Ensure staff training on ICT risks addresses recognition of security incidents and escalation and internal notification steps.

Pillar 4: Digital Operational Resilience testing

General Requirements for the Performance of Digital Operational Resilience Testing (Article 24)

Financial entities must establish, maintain and review a sound and comprehensive digital operational resilience testing programme. The purpose of this is to assess the financial entity's ability to identify weaknesses and gaps in its digital operational resilience and how well positioned it is to implement measures to address any deficiencies that were identified.

No.	Requirement	Guidance
1.	**Proportionality**	Financial entities should follow a proportionate, risk based approach when testing the performance of the financial entity's digital operational resilience, with particular focus on the entity's specific risk exposure and the provision of critical services.
2.	**Independence**	Financial entities must ensure that there is a requisite level of independence by the parties carrying out the testing, regardless of whether they are internal or external.
3.	**Policies and Procedures**	Financial entities must develop policies and procedures which prioritise, classify and remedy any issues identified in the tests. They must also establish validation methodologies to ensure that such deficiencies are fully addressed.
4.	**Frequency**	Financial entities must ensure that all ICT systems that support critical or important functions are tested annually.

Advanced Testing of ICT Tools, Systems and Processes based on TLPT (Article 26)

No.	Requirement	Guidance
1.	**Advanced Testing of ICT Tools Scope**	The most significant financial entities (as specifically designated by the relevant competent authority) must carry out advanced testing by means of TLPT at least every 3 years. Based on the risk profile of the financial entity, they may be required to reduce or increase this frequency. Advanced tests of ICT tools must cover several or all critical functions of a financial entity and be performed on live production systems supporting these functions. Assessing which critical or important functions need to be covered by the TLPT. Financial entities in scope of TLPT must ensure service providers comply with any such TLPT testing requirements.
2.	**External Risk Management by Financial Entities**	If the participation of an ICT third-party service provider is expected to have a negative impact on the quality or security of services a financial entity in scope of TLPT, the financial entity may directly enter into contractual agreements with an external tester on a pooled basis, provided that: ▪ pooled testing must be considered to be carried out by the financial entities participating in the pooled testing; ▪ the number of financial entities participating in the pooled testing must be calibrated taking into account the complexity and types of services involved; and ▪ financial entities must apply effective risk management controls to mitigate the risk of any potential impact on data, damage to assets and others.
3.	**Advanced Testing Summary**	At the end of the testing, the financial entity in scope of the TLPT requirements and external testers (where applicable) must provide a summary of the relevant findings, the remediation plans, and the documentation demonstrating that the TLPT has been conducted in accordance with the requirements.
4.	**Attestation and Notification Requirements**	Upon completion of the TLPT test, financial entities will be provided with an attestation from the competent authority.

Practical Steps

- Design and implement a comprehensive digital operational resiliency testing programme taking into account the ICT third party risks and ICT risk strategy (see Pillar 2) and overall nature, scale and complexity of the financial entity's business.
- Assess whether TLPT requirements apply, and if so:
  - Assess whether it is appropriate for a third party ICT provider to enter into testing arrangements provided directly on a pooled basis, and if so, include in the relevant contract.
  - Establish detailed procedures for notification and reporting of TLPT findings and implementation of corrective action.
  - Establish TLPT notification procedures and ensure that the relevant employee(s) receive adequate training on their new TLPT notification requirements to the competent authority.

Pillar 5: European Supervisory Authorities Oversight

Designation of Critical ICT Third-party Service Providers (Article 31)

Pillar 5 deals with the process set out by the European Supervisory Authorities (the "ESAs") to designate an ICT TPP as critical, which requires an assessment taking into account:

(a) the global impact of a failure in providing those services,

(b) the reliance of financial entities on the particular ICT provider, and

(c) the degree to which the service provider can be substituted for another.

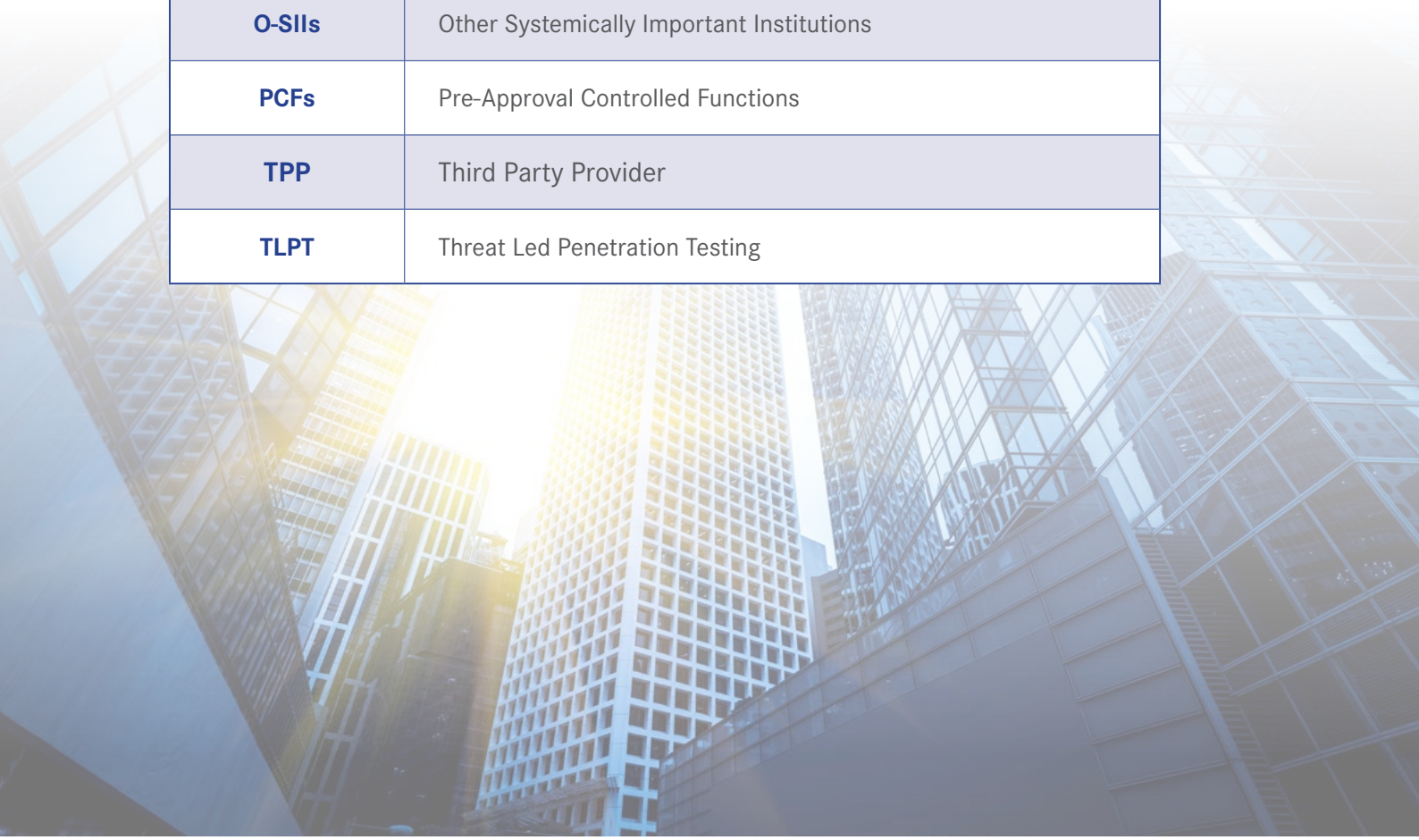
ICT TPPs shall be notified by the ESAs of their designation under Article 31 to the extent applicable.

The general criteria and structure to be considered when establishing this framework are detailed in **Article 31** and outlined below.

No.	Requirement	Guidance
1.	**Systemic Impact**	The ESAs must measure the potential impact/disruption to the provision of service, in the event of a large scale operational failure by CTPP upon the stability, continuity, or service provision.
2.	**Systemic Importance**	The ESAs will need to measure the importance of the financial entity relying on CTPP, with reference to: ▪ the number of other G-SIIs or O-SIIs which rely on the third-party service provider; and ▪ the interdependence between G-SIIs, O-SIIs and financial entities regarding such services.
3.	**Reliance**	The reliance placed by financial entities on the services provided by the CTPP in relation to critical or important functions.
4.	**Substitutability**	Develop the ability of the financial institution to substitute the CTPP. With reference to: ▪ the unavailability of alternative providers due to commercial realties or technical complexity; and ▪ difficulties in migration of services; due to the significant cost in time or finances that will ensure, or the operational risks that such migration will entail.
5	**Group Liability**	Where the financial institution concerned is part of a group, the criteria above are to be referenced against the ICT activities of the group as a whole.

Definitions

	Meaning
BCP	Business Continuity Plan
CFs	Controlled Functions
CTPP	Critical Third Party Provider
DORA	Regulation 2022/2554 on digital operational resilience for the financial sector and amending regulations (EC) No 1060/2009
GDPR	General Data Protection Regulation (EU) 2016/679
G-SIIs	Globally Systemically Important Institutions
ICT	Information and Communication Technology
O-SIIs	Other Systemically Important Institutions
PCFs	Pre-Approval Controlled Functions
TPP	Third Party Provider
TLPT	Threat Led Penetration Testing



Contacts:

Joe Beashel
Partner
T +353 1 232 2101
E joe.beashel@matheson.com

Anne-Marie Bohan
Partner
T +353 1 232 2212
E anne-marie.bohan@matheson.com

Gráinne Callanan
Partner
T +353 1 232 8211
E grainne.callanan@matheson.com

Connor Cassidy
Partner
T +353 1 232 2364
E connor.cassidy@matheson.com

Tara Doyle
Partner
T +353 1 232 2221
E tara.doyle@matheson.com

Elaine Long
Partner
T +353 1 232 2694
E elaine.long@matheson.com

Shay Lydon
Partner
T +353 1 232 2735
E shay.lydon@matheson.com

Darren Maher
Partner
T +353 1 232 2398
E darren.maher@matheson.com

Niamh Mulholland
Partner
T +353 86 102 8773
E niamh.mulholland@matheson.com

Ian O'Mara
Partner
T +353 1 232 2874
E ian.o'mara@matheson.com

Karen Reynolds
Partner
T +353 1 232 2759
E karen.reynolds@matheson.com

Deirdre Crowley
Partner
T +353 21 465 8219
E deirdre.crowley@matheson.com

Schedule 1

Regulatory Technical Standards

First batch of RTS/ITS

- Commission Delegated Regulation on RTS on ICT risk management framework and simplified ICT risk management framework: Commission Delegated Regulation (EU) 2024/1774;
- Commission Delegated Regulation on RTS on classification of ICT-related incidents: Commission Delegated Regulation (EU) 2024/1772; and
- Commission Delegated Regulation on RTS on contractual arrangements with ICT third-party service providers: Commission Delegated Regulation (EU) 2024/1773

Second Batch of RTS/ITS (finalised by ESAs, now with the European Commission)

- RTS and ITS on the content, format, templates and timelines for reporting major ICT-related incidents and significant cyber threats;
- RTS on the harmonisation of conditions enabling the conduct of the oversight activities;
- RTS specifying the criteria for determining the composition of the joint examination team (JET); and
- RTS on threat-led penetration testing (TLPT)

Matheson

DUBLIN
70 Sir John Rogerson's Quay,
Dublin 2
Ireland

T: +353 1 232 2000
E: dublin@matheson.com

CORK
Penrose One,
Penrose Dock,
Cork, T23KW81

T: +353 21 465 8200
E: cork@matheson.com

LONDON
Octagon Point,
5 Cheapside,
London EC2V 6AA

T: +44 20 7614 5670
E: london@matheson.com

NEW YORK
200 Park Avenue
New York, NY 10166
United States

T: +1 646 354 6582
E: newyork@matheson.com

PALO ALTO
530 Lytton Avenue
Palo Alto, CA 94301
United States

T: +1 650 617 3351
E: paloalto@matheson.com

SAN FRANCISCO
156 2nd Street
San Francisco CA 94105
United States

T: +1 650 617 3351
E: sf@matheson.com