Brussels, 15 February 2021

Position paper on a proposal for a Digital Operational Resilience Act (DORA)

The **European Association of Co-operative Banks** (EACB) represents, promotes and defends the common interests of its 27 member institutions and of co-operative banks, with regard to banking as well as to co-operative legislation. Founded in 1970, today the EACB is a leading professional lobbying association in the European banking industry. Co-operative banks play a major role in the financial and economic system. They contribute widely to stability thanks to their anti-cyclical behaviour, they are driver of local and social growth with 2.800 locally operating banks and 51,500 outlets, they serve 209 million customers, mainly consumers, SMEs and communities. Europe's co-operative banks represent 84 million members and 713,000 employees and have an average market share in Europe of about 20%.

For further details, please visit www.eacb.coop

EACB AISBL – Secretariat • Rue de l'Industrie 26-38 • B-1040 Brussels
Tel: (+32 2) 230 11 24 • Fax (+32 2) 230 06 49 • Enterprise 0896.081.149 • lobbying register 4172526951-19
www.eacb.coop • e-mail : secretariat@eacb.coop

Introduction

The EACB is grateful that the proposed 'Digital Operational Resilience Act' (DORA) looks to achieve an integrated approach for all participants in the financial system and across Europe to mitigate cyber-attacks and other ICT risks.

The EACB welcomes the harmonization of the various regulatory requirements in Europe and national approaches for operational resilience, which is one of the main challenges of the digital age. Consistency around the ICT risk management requirements is important to the financial sector with all participants.

Below we highlighted the EACB's key concerns and suggestions.

Key concerns and recommendations

Art. 2 PERSONAL SCOPE – Statutory auditors and audit firms

According to the legislative proposal, DORA applies to a variety of financial institutions, but also to statutory auditors and audit firms (Art.2.1(q)). Hence, co-operative auditing associations – and their auditors – would also be included in the personal scope of the proposed regulation on digital operational resilience, although they are neither "financial institutions" nor run operative ICT systems, but audit data only.

According to Art. 24a Paragraph 1(b) of the directive on statutory audits of annual accounts and consolidated accounts (Directive 2006/43/EC[1]), a statutory auditor or an audit firm (co-operative auditing associations included) already shall have in place sound administrative and accounting procedures, internal quality control mechanisms, effective procedures for risk assessment, and effective control and safeguard arrangements for information processing systems.

To include the entire profession of auditors (in our case co-operative auditing associations) in the very extensive cyber resilience framework, which is actually tailored to the business model and specific risks of financial institutions, is neither useful nor proportionate.

The IT-systems and the related risks of co-operative auditing associations differ significantly from the IT-systems and risks of a financial institution. Auditors are not part of the financial system. They neither steer cash flows nor execute transactions. They also do not grant credits or offer insurance contracts. On the contrary, auditors make sure that companies apply the accounting principles and standards properly. Co-operative auditing associations make sure that co-operatives apply the accounting principles and standards properly. Hence, it is not justified to impose the strict requirements, which were tailored to the financial sector, on co-operative auditing associations.

Moreover, pursuant to Art. 4.1(26) of the Capital Requirements Regulation (CRR2)[2] and Art. 3.1(22) of the Capital Requirements Directive (CRD)[3] 'financial institution' means (only) an undertaking other than an institution, the principal activity of which is to acquire holdings or to pursue one or more of the activities listed in points 2 to 12 and point 15 of Annex I to Directive

[1] 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.
[2] Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012.
[3] 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 and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC.

2013/36/EU, including a financial holding company, a mixed financial holding company, a payment institution within the meaning of Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market, and an asset management company, but excluding insurance holding companies and mixed-activity insurance holding companies as defined in point (g) of Art. 212(1) of Directive 2009/138/CE.

Hence, including statutory auditors and audit firms under the term 'financial institution' would clearly contradict Art. 4.1(26) CRR2 and Art. 3.1(22) CRD respectively. For the same reasons, the European legislator should not amend Art. 24a of the directive on statutory audits of annual accounts and consolidated accounts.

➔ The EACB recommends excluding statutory auditors and audit firms from the personal scope of the proposed regulation. Additionally, in the proposal for a directive amending directives 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 and EU/2016/2341, "Article 1 Amendments to Directive 2006/43/EC" should be deleted.

Art. 3 DEFINITIONS

As a general comment, the EACB recommends checking for consistency and aligning the definitions to those ones of operational resilience to the BCBS definition and of the FSB Cyber Lexicon.

In particular:

- Art. 3(15) 'ICT third-party service provider'
  DORA defines the scope of third-party suppliers with a different logic than the European Banking Authority (EBA). According to the EBA, the ICT risks must be considered for all providers, in application of the guidelines on ICT risks and outsourcing.
- Art. 3(50) 'microenterprise'
  DORA tries to achieve proportionality by exemption with a lighter regime for microenterprises (especially concerning reporting and advanced testing). However, the EU definition of "microenterprises" (with a balance sheet total ≤ €2 million according to EU Recommendation 2003/361) does not work for banks and especially small and medium-sized co-operative banks, because neither the balance sheet total nor the number of staff would be relevant to classify small or medium-sized banks.
  ➔ Therefore, the EACB proposes amending the definition and aligning it to that of "small and non-complex institution" already enshrined in CRR2 (Art. 4.1 (145)).
- A definition on "Intra-group ICT service provider" should be added in Art. 3. See also our comments under the below subject.

INTRA-GROUP ICT SERVICE PROVIDER

Due to their distinctive "division-of-labour" structures, group / network entities or central institutions, co-operative groups and networks provide numerous services for the affiliated banks. This traditional supporting pillar finds its basis in the respective national legal frameworks. For example, the laws and statutes governing local co-operatives or their central institutions or associations regularly stipulate that the central support services organized in the respective network are to be offered by the central institution or used by the local banks belonging to the network. Also the CRR and the Commission delegated regulation on liquidity coverage requirement for credit institutions make reference to this situation[4]. Moreover, it is stipulated in the statutes of many co-operative central institutions / bodies that their main mission is to provide services to local banks.

[4] Regulation (EU) No 575/2013 of the European Parliament and of the Council on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012.. E.g. Art. 10, 113(7), 400(2)(d).

Such organizational structures, especially the bundling of tasks in specific entities, not only improve their cost efficiency and achieve economies of scale. In many cases, the local banks would not be able to reach the level of quality, maintenance and stability, which is now ensured by the central institution or common specialized entities due to the size, resources, specific technical knowledge of the latter.

This is also why co-operative banks often use centralized intra-group ICT service providers according from the logic that such function can be performed better by a larger and consolidated entity for all and especially small and medium-sized co-operative banks.

The EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02[5]) specifically reflects of outsourcing arrangements within a group - including the situation where institutions are permanently affiliated to a central body - and within an institutional protection scheme (IPS).

➔ Therefore, the EACB recommends that the facilitation of outsourcing by banking groups, institutions permanently affiliated to a central body and institutions that are members of an institutional protection scheme, as provided for in the EBA Guidelines on outsourcing arrangements, should also be applied to the management of ICT third party providers. This arrangement should allow centralised monitoring of ICT services and reporting of ICT incidents.

Finally, the EACB recommends that as regard to the ESAs' designation of critical ICT third-party service providers (Art. 28) it is clarified that ICT providers that are part of a group as defined by prudential rules would be excluded by this mechanism. Consequently, we also suggest including a definition on "Intra-group ICT service provider", which is missing, in Art. 3.

CONSISTENCY WITH OTHER EXISTING OUTSOURCING AND OPERATIONAL RISK MANAGEMENT REQUIREMENTS

The DORA framework appears to add a certain layer of regulation in certain areas with existing European (e.g., EBA Guidelines on outsourcing arrangements) and international requirements including:

- The Basel Committee proposed its "Principles for operational resilience" and updated its "Principles for the sound management of operational risk " (PSMOR) on 6 August 2020.
- The FSB has published a discussion paper "Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships[6]". Among other things, it makes specific reference to the concentration issues associated with a small group of cloud providers and the associated data protection and location constraints.

Therefore, many guidelines concerning Outsourcing and Operational Risk Management in general already exist. But DORA does not describe the process, how an alignment and harmonisation would be achieved across Europe or internationally. In addition, there are many inaccuracies in both definitions and requirements that could complicate implementation. It is necessary to anticipate operationally the transition from the current framework to the one established by DORA.

The danger of such additional layer can be seen in Art. 4 "Governance and organisation", as the responsibility of the management body in managing financial entity's operational risk and outsourcing relationship is already fully established in the regulatory framework and there is no need for requirements that would make the assessment of compliance only more complex without any

COMMISSION DELEGATED REGULATION (EU) 2015/61 to supplement Regulation (EU) No 575/2013 of the European Parliament and the Council with regard to liquidity coverage requirement for Credit Institutions. E.g. Recital 12, Art. 7(2)(b), Art. 16, Art. 27(1)(b), Art. 29(1)(b), Art. 34(1)(b).

[5] EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02), available here: https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing-arrangements.

[6] FSB discussion paper on "Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships", available here: https://www.fsb.org/2020/11/regulatory-and-supervisory-issues-relating-to-outsourcing-and-third-party-relationships-discussion-paper.

benefit in terms of risk management. The current proposal goes far beyond the harmonisation approach initially planned. The additional detailed requirements in the legislative proposal would lead to increasing efforts (e.g., in documentation) and additional costs without actually improving cyber-resilience. The Regulatory Technical Standards (RTSs) of the ESAs which are foreseen by the current proposal are expected to result in an even greater density and depth of regulation. There should be no fixed definition of methods via RTS, as short-term adaptability of methods and practices is required, especially in the field of ICT security.

➔ Therefore, the EACB proposes clarifying the relationship between DORA and the existing Outsourcing and Operational Risk Management requirements to achieve overall consistency and avoid replications of roles, function, processes, reporting etc. The requirements for the management of ICT third-party risk should distinguish whether or not the ICT service supports critical/essential functions.

Moreover and in order to allow the necessary adaptability, the RTS should be replaced by EBA guidelines, which allow a risk-oriented interpretation of principle-based requirements and the consideration of national specificities.

ICT-RELATED INCIDENTS

DORA and the proposal for a directive amending directives on statutory audits of annual accounts and consolidated accounts, UCTIS, Solvency II, AIFMD, CRD, MIFID2, PSD2 and IORPs[7] have the objective to streamline (incident) reporting with common reporting templates, deadlines, one competent authority to report to, etc. However, there are remaining unclarities e.g., when does an ICT incident leads to a payment incident?

The EACB strongly stresses the need for articulation between the various reporting obligation e.g., data breach under the General Data Protection regulation (GDPR) (Articles 33 and 34), incident reporting under the second Payment Systems Directive (PSD2) (Art. 96 and EBA Guidelines on major incidents reporting under PSD2[8]) and incident notification under the Network and Information Security Directive (NIS) (Art. 14.3). The problem of banking institutions is the concomitance of three notification obligations in the event of incidents with different authorities. In this respect, the EACB looks with favour upon the idea of the European Hub project.

➔ A holistic approach to ICT/Operational Risk/Payment incident reporting would be recommended to avoid (i) fragmentation of incident reporting in various silos and (ii) confusion as to how to classify an incident event and where to report in which format. The reporting of major ICT-related incidents must be combined in a single procedure that includes PSD2 and NIS incident reporting.

Moreover, should the European Hub be set up, it should replace all pre-existing ICT-related incident reporting. We also suggest clarifying the objective of the Hub project, and the nature of the use of this data by public authorities, to specify what feedback is provided to financial entities, the added value for banks and to indicate what the cost of this Hub will be. Finally, attention should be given to the security of this possible database. The centralization of all European incidents in the same system and in the same place can be a target for cyber-attacks (leaks of sensitive data, etc.).

[7] Proposal for a Directive amending directives 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 and EU/2016/2341 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0596.
[8] EBA Guidelines on incident reporting under PSD2 (EBA-GL-2017-10).

DIGITAL OPERATIONAL RESILIENCE TESTING

The EACB believes that the obligation to perform TLPT tests should be limited to critical functions. In this regard, the EACB suggests deleting the wording "at least" in Art. 23.2.

In addition, the audit rules for Threat Led Penetration Testing (TLPT) tests should be uniform at European level to avoid discrepancies and to respect the level playing field.

For Art. 23 "Advanced testing of ICT tools, systems and processes based on threat led penetration testing" of the proposal, the EACB proposes to refer to the TIBER-EU standard (the European framework for threat intelligence-based ethical red-teaming) to define the methods of carrying out this type of TLPT tests. Moreover, the Regulatory Technical Standards indicated in the proposal (Art. 23.4) could rely on this standard.

SUPERVISION MECHANISM FOR CRITICAL ICT THIRD-PARTY SERVICE PROVIDERS

The EACB welcomes the new oversight framework for critical ICT third-party service providers for a better sharing of responsibilities. However, the EACB believes more attention should be devoted to the following:

- Increasing the accountability of ICT third-party service providers, including non-critical ones. Currently, it is difficult for European banks, even major banks, to impose the regulation to certain dominant players (e.g., cloud providers) simply through contractual negotiations. Moreover and concerning auditing, the focus should be particularly on those international ICT service providers for which the enforceability of audits at the level of the individual financial institution cannot be sufficiently guaranteed (i.e., so-called hyperscaler). Financial institutions should not be requested to perform furhter auditing for critical ICT third-party service providers as proposed by the new legal framework.
- There is a lack of clarity on the responsibilities of each party regarding sub-outsourcing, e.g.: Who is responsible for not refusing a non-critical provider if it has recourse to a critical cloud provider from a third country? How to define (and better limit) the chain of responsibility?
- Ensuring that there are no discrepancies between the EBA Guidelines on outosurcing and DORA regarding contractual provisions.
- Excluding intra-group ICT service providers from the supervisory framework.

Contact:

The EACB trusts that its comments will be taken into account.

For further information or questions on this paper, please contact:

- Ms Marieke van Berkel, Head of Department Retail Banking, Payments, Financial Markets (marieke.vanberkel@eacb.coop)
- Mr Udo Milkau, Digital Counsellor to the EACB (udo.milkau@eacb.coop)
- Ms Chiara Dell'Oro, Senior Adviser on Digital Policies (chiara.delloro@eacb.coop)