WHITE PAPER

Digital Operational Resilience Act (DORA)

Contract review as a mammoth task: minimising risks with CLM and AI-led contract intelligence

Eric Cissé, Senior Manager Strategy & Risk, Accenture

Jason Smith, Senior Principal, Strategy & Transformation, Conga

How financial service providers are increasing their digital resilience using contract management solutions and AI-led contract insights, all while harmonising with the EU regulation DORA.

The European Union (EU)'s Digital Operational Resilience Act (DORA) framework is designed to ensure that financial institutions can withstand and recover from disruptions to their key services and systems, thereby safeguarding the stability of the broader economy through resilient providers.

It is a regulation that introduces standardised processes for managing, reporting and reacting to information and communications technology (ICT) operational risks in the financial sector.

DORA's scope extends to all third-party ICT providers classified as critical, meaning their services are essential to the functioning of the financial system, thereby ensuring that these providers also meet rigorous operational resilience standards. As a result, financial firms will need to review all contractual agreements with their providers regularly, including descriptions of their scope of services. This is a potentially mammoth task, one that can be achieved efficiently with contract lifecycle management (CLM) and artificial intelligence (AI)-led contract intelligence solutions.

What is the DORA regulation?

DORA is an EU regulation that aims to improve the cybersecurity and operational resilience of the financial services sector. Its main goal is to provide a consistent legal framework in the EU for the security of ICT systems and digital services in the financial sector. UK organisations that provide financial services to EU-based entities or operate within the EU's financial markets must ensure compliance with DORA, despite the UK's exit from the EU.

DORA covers areas such as ICT risk management, incident reporting and operational resilience testing. The requirements are binding, not only for banks but also for payment service providers, credit institutions, investment companies, insurance companies, crypto providers and others.

DORA was published in the Official Journal of the European Union on 27 December 2022 and entered into force on 16 January 2023. The implementation deadline for financial institutions and ICT service providers is 17 January 2025.

While financial institutions are responsible for ensuring that their ICT service providers comply with DORA, the regulation also imposes obligations directly on critical ICT third-party service providers (CTPPs) to adhere to the established standards. This is explicitly described in chapter V of DORA.

As a result, financial firms must analyse their existing agreements with external ICT providers and modify the specifications if necessary. Before closing any new contracts, they must determine and assess all potential risks related to the fulfilment of those contracts, according to DORA. Furthermore, they must report new agreements with ICT service providers, including the type and content of those agreements, to the relevant authorities at least once a year.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554

Does DORA apply in the UK?

DORA is an EU regulation, but it also applies to non-EU companies that do business in the EU, along with 'critical ICT third-party service providers' (CTPPs) that provide relevant services.

DORA applies to a wide range of financial organisations, including banks, payment institutions, investment firms, insurance companies and crypto-asset service providers, among others, so it is expected to impact more than 22,000 financial entities and ICT service providers within the EU. Yet, the UK impact will also be significant, expected to equate to thousands of organisations. For many of these, DORA will be the first time they have needed to meet the kind of requirements it contains.

The time to act is now because companies need to know if they fall into DORA's remit and, if they do, they must ensure compliance. While DORA sets EU-wide standards, UK-based financial entities should consider it alongside existing local regulations, such as SS2/21 and ISO27001, which share synergies with DORA and can provide a foundation for compliance. Existing or in-progress compliance in these areas may help. Also, UK companies will already be familiar with the Financial Conduct Authority (FCA), Bank of England and Prudential Regulation Authority's operational resilience approach and the more recent Financial Services and Markets Act, which has a remit that extends to 'critical third parties' (CTPs), being relevant service providers.

What is the purpose of the DORA regulation?

Digitalisation enables financial institutions to provide better services to their customers and to launch new product offerings while also optimising their processes. However, as companies digitalise their operations, they must be wise to the potential security dangers associated with information technology (IT) and telecommunication infrastructure.

These dangers include, but aren't limited to, cyberattacks, such as ransomware and phishing incidents and targeted overloads caused by distributed denial-of-service (DDoS) attacks. They also include data leaks and outages of key IT and telecommunication systems.

To reduce the risks caused by using digital services, the EU passed the DORA regulation.

5 Pillars of DORA

Article 6	Article 17	Article 24	Article 28	Article 45
ICT Risk Management	**Incident Reporting**	**Digital operational resilience testing**	**Third-party risk management**	**Information sharing**
Establish framework for ICT risk management	Requires transparency about data security incidents for partners, employees, and clients.	Vulnerability assessments and scans	Establish procedures for detecting & managing ICT-related incidents	Establish framework for info sharing
Define roles and responsibilities	Must have robust systems to detect, report and analyze ICT incidents.	Open-source analyses	Classify incidents (severity, impact, urgency)	Define info sharing conditions
Regular assessments		Network security assessments	Report significant incidents	Coordinate with authorities
Proportionate measures		Gap analyses	Inform clients	Define types of info to share
Procedures to detect, manage and report incidents		Physical security reviews	Root-cause analysis	Confidentiality and anonymity
Business Continuity & Disaster Recovery Plan		Questionnaires	Incident Response Plan	Comply with data protection laws
Assess & manage ICT risk from third party		Source code reviews	Regular testing and simulation	
Comprehensive documentation		Scenario-based tests	Contractual agreements	
Continuous improvement		Compatibility testing	Record retention	
		Performance testing	Continuous improvement	
		End-to-end testing		
		Penetration testing		

DORA and cybersecurity

Financial firms, as guardians of sensitive data, can be prime targets of cyberattacks. Companies appear to recognise this risk. According to the Allianz Risk Barometer 2023, compiled by Allianz Global Corporate & Specialty (AGCS), 42 per cent of surveyed financial services companies mentioned "cyber incidents" as the biggest threat, followed by macro-economic developments (34 per cent) and modified laws and regulations (26 per cent).

Cybersecurity is a big part of ICT risk management and so it is not surprising that DORA concerns itself with procedures to detect, manage and report incidents. This extends beyond financial institutions' own walls; to ensuring that suppliers, including managed ICT service providers, IT hardware suppliers and consultancy services adhere to robust cybersecurity standards. This requirement aims to mitigate the risks posed by supply chain vulnerabilities, which have become a significant concern in recent years.

Risk example: ICT service providers' cybersecurity	
Data leak	
Incident type:	Cyberattack on ICT service provider
When:	July 2023
Issue:	Software with critical vulnerabilities
What happened	
The personal data and international bank account numbers (IBANs) of bank customers were compromised.	

Cyberattacks can lead to operational disruption in the moment, but also reputational and financial impacts that can last much longer. Companies incur the cost of fixing the weakness or flaw that led to the incident and may also be subject to fines imposed by industry regulators. They may find themselves facing legal action and will almost certainly suffer negative brand impact resulting in the potential loss of existing and future customers.

As technology develops and evolves, so too does cybercrime. It is a constant race to keep up with developments and their attendant risk factors. One current technology trend is AI and chatbots. These offer compelling business benefits, but come with cyber risks too, which companies must mitigate to reduce the vulnerability of their data, systems and service offerings to cyberattacks.

DORA and other digital risks

The purpose of the DORA regulation is to reduce risks caused by using digital services. Cybersecurity is a significant risk, but it is not the only one. Other potential digital service issues include disruptions that result in service outages.

Risk example: service disruption	
IT Outage	
Incident type:	IT outage that affected systems worldwide
When:	July 2024
Issue:	Defect in software update
What happened	
Significant impact was felt across industries including transport, health and financial services, with some experiencing offline systems.	

The important message to companies impacted by the DORA regulation is to identify, understand and manage the risks.

Challenge: Reviewing contracts with third-party ICT providers

Clearly, financial institutions must spend time understanding and complying with DORA regulations when it comes to ICT third-party risk. A broad range of ICT services are affected, including hardware-related services as well as software and firmware updates.

Every financial services company must therefore do regular checks, of a potentially high number of contracts, for DORA compliance. Each time, they should ask themselves:

- What IT security and data protection does the third-party provider have?
- Where is the customer data stored?
- How will data be returned in the case of a provider insolvency or company closure?
- Do service providers of the third party also act in compliance with DORA? Are they covered in this agreement?
- To what extent can we audit the services of the third-party provider?

Solution: Contract lifecycle management with purpose-built AI

Most businesses won't find it feasible to check their contracts manually because of the vast resources that would require. Instead, they can turn to end-to-end contract lifecycle management (CLM) solution, such as Conga CLM, enabling companies to easily search and quickly identify the contracts requiring action.

In addition, Conga Contract Intelligence, supported by artificial intelligence (AI) and machine learning (ML), used in combination with Conga CLM, provides a way to accurately uncover contract insights to meet obligations, manage risk and optimise revenue.

This AI-led contract management and analysis uses a central data repository as a single source of truth. That way, financial institutions can store, view, review and analyse all their contracts with external ICT providers in a single place. This minimises the risk of overlooking certain agreements, and contravening DORA requirements, as well as helps companies meet the DORA requirement to maintain a contract register of all ICT services.

Conga CLM and Conga Contract Intelligence can help meet the need to monitor ICT third- party risk in a secure, efficient and transparent way. The contract management solution maps the entire lifecycle of contracts from negotiation and signature, through execution and fulfillment, to renewal or termination, and shows changes over time to the contracts, clauses and related documents.

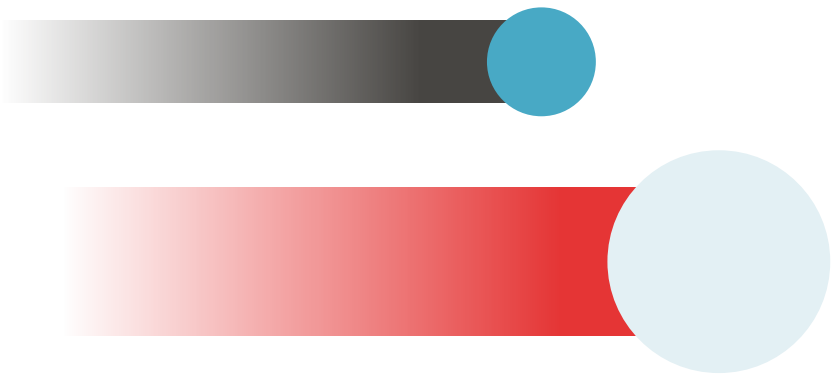
Contract intelligence can also digitise existing ICT provider contracts and automatically extract and transform the legal language into actionable data. Once tagged in the CLM system, the data can be used efficiently in searches, reporting, risk analysis and alerts.

AI-led contract search

Many financial institutions, for resilience purposes, use various external ICT providers. They need a powerful contract search function that enables IT and compliance specialists to enter specific keywords and systematically locate individual contracts, fields and clauses, even in large directories, to analyse the data.

With Conga Contract Intelligence, financial firms can create a central repository and quickly find information on any contract using context-based topic search. They can also locate data with filterable, customisable dashboards. Contract specialists and compliance professionals can further tailor these tools to meet their specific needs to comply with the DORA requirements.

.



Checking contracts for potential risks

Financial service providers and their external ICT providers must also align existing contracts with the DORA requirements, and this poses a significant challenge. It requires a detailed analysis of existing contracts and obligations —a potentially enormous effort for legal departments.

Often, critical information is held in the form of unstructured data, buried in thousands of legal agreements. Extracting the full scope of governing terms accurately would be expensive in time and skilled resources and would likely return inconsistent results.

Smart technology solutions, such as Conga Contract Intelligence and Conga CLM, offer an alternative way. Conga Contract Intelligence extracts commercial terms and transforms them into verified data. It has the optional feature of extracting and digitising contract data using Optical Character Recognition (OCR) and AI-based, automated processes. This can even be done in bulk for large numbers of documents.

Furthermore, Conga Contract Intelligence's risk management feature helps customers accelerate third-party contract review by identifying risks, scoring them and offering alternative language to mitigate these risks. The tool also tracks extracted obligations within the CLM, enhancing management and compliance through clear visibility, reporting and alerts. Specialists in financial institutions 'teach' the AI engine to identify potential contract risks by setting criteria for classifying clauses or contracts as unacceptable, in line with DORA guidelines. This process also applies to 3rd party paper contracts from external ICT providers. A risk score indicates where and how much a contract deviates from requirements, allowing legal experts from both the financial services company and ICT service provider to revise problematic areas.

Result: Verified data for compliance and beyond

After contracts have been checked and updated, both the financial firm and ICT service provider will have DORA-compliant contracts based on verified data. This minimises the danger of outdated, or even non-compliant, clauses creeping into contracts.

The benefits of a technology-based solution for contract checking extend beyond DORA compliance though. Companies can integrate verified contract intelligence data with operational systems such as customer relationship management (CRM) and enterprise resource planning (ERP). That way, contract insights can be sent instantly to a range of departments, such as finance, sales, support and procurement teams, for more efficient cross-discipline communication and action.

Additionally, contract intelligence and contract management automation equips financial services companies to proactively manage ICT contract renewals and to check potential alternative providers. The obligations and services of providers, including the financial implications of potentially closing a contract, can be compared. This transparency is indispensable to optimise the partner environment—financially and with respect to regulatory requirements such as DORA.

How to ensure compliance with DORA contractual requirements?




Discovery & Mapping	Gap Analysis	Remediation	Outreach & Negotiation
Identify & Locate all ICT third party contracts	Identify the gaps in compliance with DORA contractual requirements	Review & Update templates and contracting standards	Reach out to all ICT third parties to negotiate DORA amendments
Review & Categorise them per DORA requirements		Develop a plan for remediation of legacy ICT contracts	

Conclusion: Time is of the essence

It is vital that financial services companies understand DORA, what it means for their business and the actions they need to take. They must work with their external ICT service providers to plan and action any requirements that result from their assessments and audits as DORA, quite unlike some of the other regulations companies are familiar with, is explicit in its application to financial institutions and their providers.

Time is short, but effective and time-efficient technology solutions are out there that can help. Conga Contract Intelligence and Conga CLM allow businesses to manage all contracts in a single place, extract key data points from these agreements, gain insights into their contractual obligations and identify and mitigate risk while ensuring regulatory compliance.

About the authors

Jason Smith

Senior Principal, Strategy & Transformation, Conga

Jason has over 26 years of experience as a practicing attorney and legal technology consultant. Prior to joining Conga, he co-founded a successful legal technology startup, served as a legal technology consultant, was in-house counsel for a software company, launched a Contract Management consulting practice and served as AVP, Risk and Financial Advisory for a Big Four firm. He focuses on law department transformations, emerging technology trends and innovation in the legal profession and has received the Award of Merit from the State Bar of Texas for service to the legal technology community. He has led a number of global contract lifecycle management projects for some of the world's largest companies.

Eric Cissé

Senior Manager Strategy & Risk, Accenture

Eric holds a M.Sc. in Computer Science, an MBA from Yokohama University and a Business Strategy Certification from INSEAD Business School. He is Lead Auditor ISO 27001, ISO 27005 Risk Manager, PECB Certified Data Protection Officer / CISM / CRISC / PCI-DSS and a member of the French DPO Association (AFCDP). He provides strategic, transformational and technical offerings in Regulatory and Compliance (DORA / NIS / NIS2 /CMMC 2.0) with a comprehensive view that enables him to help clients grow their business while staying ahead of key risks, anticipating regulatory changes and instilling cyber resilience best practices.

Conga

Conga, the Revenue Company, is the pioneer and market leader in Revenue Lifecycle Management. Its platform is chosen by the world's growth champions to accelerate the end-to-end revenue lifecycle and achieve a Revenue Advantage. Conga brings Configure, Price, Quote, Contract Lifecycle Management and Document Automation capabilities together on a single open platform that works with any ERP, any CRM and any Cloud. Conga is born for the top line—powered by a unified revenue data model, complete revenue intelligence and purpose-built AI—to help companies grow, protect and expand their revenue.

Conga delivers a Revenue Advantage to over 10,000 customers and 6.4 million users around the world. More than 7 million contracts and 46 million quotes are generated annually with Conga. Founded in 2006, the company is headquartered in Broomfield, Colorado with global operations across North America, Europe, Asia and Australia. Visit conga.com for more information.

Find out how Conga can support you with the new DORA requirements, get in touch through conga.com/contact-us:

Email: info@conga.com
LinkedIn: @Conga
Website: conga.com