Robin AI™

Using Legal AI to achieve DORA compliance

for banks, financial institutions and insurers

www.robinai.com / hello@robinai.com

EXECUTIVE SUMMARY

Oversight of vendor contracts has always been a core responsibility of regulated banks that have integrated third-party suppliers (vendors) into their technology infrastructure. With the adoption of DORA (Digital Operational Resilience Act), that responsibility is becoming more complex and imperative.

The use of Legal AI is growing within law firms and in-house legal departments across industries. In this paper, we will discuss how Legal AI can help in-house teams at banks, financial institutions and insurers to comply with DORA while reducing the cost of legal services, improving the efficiency of legal teams, and reducing multiple types of risk associated third party vendors. Then we will look at how insights gleaned from Legal AI can be leveraged by colleagues outside the legal department to improve the operational process of Vendor Risk Management (VRM).

DORA

Requirements

DORA is a new regulation that requires financial institutions providing services into the EU to ensure resilience in the technology supply chains of these organisations. Agreed in 2023, DORA came into force on Jan. 17, 2025, so firms are against the clock when it comes to preparation for compliance. The key impetus for establishing DORA was to harmonise rules around cybersecurity. Banks have many tasks to complete before readiness for DORA is attained; however, the management of third-party risk is one where the application of Legal AI can mitigate risk, reduce costs, and empower employees.

High level objectives | *5 categories*

Banks are already managing third-party vendors carefully; with DORA, there may be a need to reconfigure the structure of vendor risk management and the reporting of VRM activity to match the specific needs of the new regulation. For DORA, a comprehensive approach to risk management encompasses five categories of focus.

- **Standardizing risk management**: DORA unifies risk management practices across the EU.
- **Enforcing regular testing**: DORA requires financial institutions to perform regular testing of their ICT systems.
- **Mandating incident reporting**: DORA requires financial institutions to report incidents in detail.
- **Overseeing third-party providers**: DORA includes strict oversight of third-party ICT providers, such as cloud computing services, software, and data centres.
- **Harmonising rules**: DORA harmonizes rules for digital operational resilience across 21 different types of financial entities.

Third party risk management | *4 Key Concepts*

Prime among the objectives of DORA is improved governance of the oversight of vendors. Whether it is referred to as Vendor Risk Management, Supply Chain Management or Outsourced ICT Management, these four areas must be considered.

Third-Party Risk Management and Outsourcing

- **Third-party oversight**: Ensure effective due diligence is carried out on ICT third-party providers (e.g., cloud service providers, fintech companies) before onboarding and throughout the relationship.
- **Risk assessments**: Implement ongoing risk assessments for third-party service providers, including regular reviews of their cybersecurity controls.
- **Exit strategies**: Develop exit strategies for third-party relationships to minimize disruption in case the service provider fails or breaches contractual agreements.
- **Contractual obligations**: Ensure all outsourcing contracts meet DORA requirements, including the right to audit third-party providers and provisions for sharing risk information.

All of these tasks are important; however, it is logical to start with the last one, contractual obligations.

CONTRACTS

7 Essential Components

To be DORA compliant, banks must ensure that all vendor contracts contain seven components, including audit rights, subcontracting limitations, termination rights, data protection and security, incident reporting obligations, business continuity and disaster recovery, and Service Level Agreements (SLAs). All existing contracts must be reviewed to ensure they contain these points. Teams of compliance officers or lawyers would need sufficient time to review hundreds of contracts. Using Legal AI software could reduce the time to review contracts while at the same time improving the results of detection.

For the specifics of the seven clauses:

- **Audit rights**: Financial institutions must retain the right to audit the provider's operations, including their cybersecurity practices, business continuity capabilities, and data protection measures. These audits can be done periodically or triggered by significant events (e.g., data breaches).
- **Subcontracting limitations**: Contracts should specify whether the provider can subcontract any services, and if allowed, the institution must have visibility and approval over these subcontracting arrangements.
- **Termination rights**: Institutions should have the ability to terminate contracts in the event of persistent non-compliance, major operational failures, or security breaches.
- **Data protection and security**: Include clear provisions on the provider's obligations to protect sensitive financial and personal data, comply with the EU's GDPR, and report data breaches promptly.
- **Incident reporting obligations**: The provider must inform the financial institution of any ICT-related incidents that could impact the services, particularly if those incidents would be reportable under DORA.
- **Business continuity and disaster recovery**: The provider should commit to mAIntaining a robust disaster recovery plan and business continuity framework. Additionally, the contract should define recovery time objectives (RTOs) and recovery point objectives (RPOs) that align with the financial institution's own resilience targets.

Service Level Agreements (SLAs): SLAs should be detAIled and align with DORA's operational resilience requirements, covering the expected uptime, response times, and penalties for non-performance.

Retrospective use of legal AI to review legacy contracts

A comprehensive look back of a bank's vendor contracts could be a substantial deployment of manpower and time. If a bank had 100 third party vendors, and a team of in-house (or outside counsel) lawyers devoted five hours reviewing time per contract, that would be 500 hours of billable time. If the same lawyers employed Legal AI, they could review 100 contracts 98% faster. A Report could be built and generated within minutes providing clear responses to specific questions about compliance. In this case, a lawyer, instead of spending an hour reading through a contract to search key words and terms such as "business continuity" can instead get straight to the answers using AI and quickly identify the relevant omissions.

Leveraging AI to complete this task removes all the manual work searching, extracting, synthesising data and populating spreadsheets and databases. Legal teams are equipped with the information they need to verify information in primary documents. The information is structured in the form of a data asset which enables simple filtering and sorting of the data, for example by dates, vendors, or specific provisions.

Prospective use of AI for new contract origination

Once a bank's legacy contracts have been reviewed, analysed and remediated, Legal AI can be used to create new, DORA-compliant contracts suitable for negotiation with vendors. An "AI First" approach can shorten the review, mark-up, and signatory cycle of contract completion. Additionally, when vendors submit periodic status or progress reports on operational resilience, lawyers and compliance colleagues can use Legal AI to match the reports with the original contract requirements.

Beyond contracts:

Vendor Risk Management and the Three Lines of Defence Model of Governance

Many banks use the Three Lines of Defence (3LoD) governance framework to manage their operations, including the functional area of Vendor Risk Management (VRM). Many aspects of the lifecycle of a VRM programme can be enhanced using Legal AI across a bank's governance structure. Colleagues with different levels of risk ownership in various departments can benefit from using AI.

First LoD

Once a decision to outsource part of a bank's infrastructure to a third-party vendor, the first line of business owners and IT leaders often identify and evaluate potential vendors. Procurement owns the process of vetting and ranking vendors with the additional role of pricing negotiation. Using AI, procurement colleagues can identify and screen vendors that are compliant with DORA, other EU regulations, and regulations in other jurisdictions.

After vendor onboarding is successfully implemented, VRM teams can use AI as part of their relationship management effort. Ongoing monitoring of and reporting from vendors can be facilitated more effectively and efficiently.

If a vendor were found to be in breach of DORA regulations, Legal AI could be used to expedite the process of off-boarding and the search for a replacement vendor.

Second LoD

The control functions of Finance, Risk, Compliance and Operations are critical to the implementation of a VRM programme. The use of AI by non-legal colleagues working in partnership with legal staff can lead to shared organisational learning about VRM, with better outcomes. For example, if AI revealed to Operations that a vendor was having difficulty updating its software according to its contractual deadlines, this discovery might trigger an inquiry to the vendor relating to its ability to maintain a robust cyber protection against hacking. The financial health of vendors is often a red flag to clients.

If Finance discovered that a vendor's senior executives were selling stock, an investigation into the financial stability and cash flow might ensue.

Third LoD

If Audit colleagues were able to use AI to detect anomalies in data reported from business units to Audit, this discovery could lead to an investigation of the root cause(s) of the problem. Audit can use AI to test the integrity of the data it receives from the business to validate the immutability of data that is used as a "golden source". In addition to its critical internal function, Audit has a key role to play in managing relationships with regulators. In some cases, regulators audit the Audit department, requiring the Audit team to evidence that proper procedures have been followed. In extreme cases, a regulator has found a bank's Audit function weak and required the bank in question to hire an external firm to supplement its Audit team. The use of AI could help Audit colleagues to back test their processes and systems internally to ensure that a regulatory audit would be passed with flying colours.

Ownership and management of legal AI

As banks adopt Legal AI, ownership and governance of the technology can be logically situated into existing organisational structures. Executive ownership can be co-owned by the office of the General Counsel and the Chief Compliance Officer. AI governance can be integrated with governance of other emerging technology. The champions of Legal AI can work with HR and other groups to embed AI training into the Learning & Development curriculum and include AI competencies as part of annual performance appraisals.

Board ownership of Legal AI policy and governance can be the responsibility of the Chair of the Audit Committee. This director can include an overview of the governance, effectiveness and efficiency of Legal Ai with the company Audit report at each board meeting.

From contracts to continuous process improvement

Legal AI can benefit most business processes, including those relating to compliance and regulatory management of multiple regulations and jurisdictions. A cycle of continuous improvement can be initiated and sustained. With AI, colleagues can:

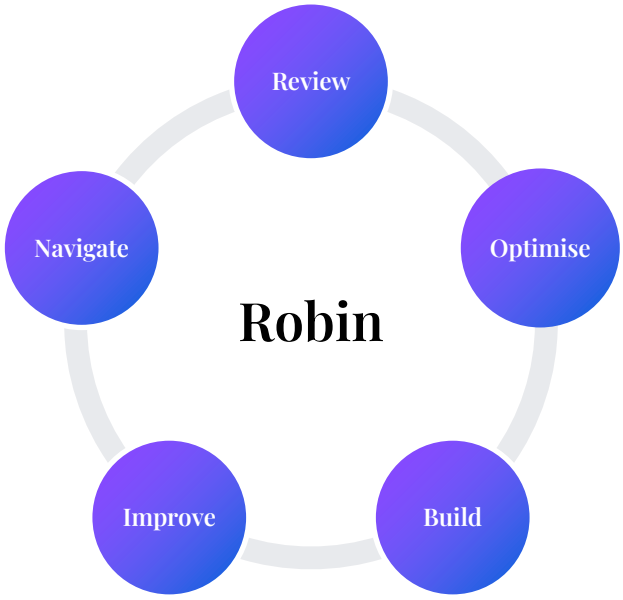
R eview contracts and other documents to interrogate for patterns, trends, corrections and omissions

O ptimise processes by suggesting concise and logical workflows across departments and within them

B uild systems by connecting data from dispersed areas of a bank and unifying data for more informed decision-making

I mprove governance by delivering data as actionable information so that colleagues can make decisions free of cognitive bias

N avigate change by offering multiple options to employees within a rule-driven framework



CONCLUSION

Using Legal AI to analyze vendor contracts can help banks achieve compliance with DORA in record time, while mitigating risk, reducing costs, and empowering compliance and legal staff to learn about AI and focus on higher value-added skills. At a time when employees are asked to do more with less in an environment of tight time constraints, Legal AI can tip the balance towards effective audit and control of not just third-party contracts, but the associated workflow underpinning the ongoing risk management of vendors in banks. Legal AI can lead to better outcomes in UK banks across multiple quantifiable dimensions: risk, cost, skill optimization, efficiency, and effectiveness.

Robin AI has a track record of helping in-house legal teams at leading banks, financial institutions and insurers to achieve dramatic improvements in their productivity and effectiveness in contract review, regulatory compliance and audit. At Robin AI, we believe our technology and approach to client relationships can add immediate value to UK banks facing the challenge of DORA compliance or indeed compliance with other EU, UK, US or international regulations.

Get in touch with Robin AI for a consultation today.

Sources

https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/managing-when-vendor-and-supplier-risk-becomes-your-own

https://www.herbertsmithfreehills.com/insights/reports/global-bank-review-2024/legal-function-transformation

https://www.taylorwessing.com/en/global-data-hub/2024/cyber-security---weathering-the-cyber-storms/how-will-the-eus-dora-impact-uk-businesses

https://www.grantthornton.co.uk/insights/model-risk-management-working-with-third-party-vendors/

https://deloitte.wsj.com/cio/managing-vendor-risk-considerations-for-banks-01671224269

https://kpmg.com/uk/en/home/services/kpmg-law/contracts-and-third-party-risk.html

https://www.deloitte.com/global/en/services/risk-advisory/perspectives/third-party-risk.html

Robin AI™

IN PARTNERSHIP WITH

ANTHROPIC aws

www.robinai.com / hello@robinai.com