SWISS FINANCIAL INSTITUTIONS AND OUTSOURCING
PART 1 – NAVIGATING DIGITAL OPERATIONAL RESILIENCE ACT (DORA) FOR SWISS FINANCIAL INSTITUTIONS

Date: March 9th, 2025

Authors: Florian Ducommun; Crystal Dubois

Expert topics: Advanced technologies; Cybersecurity; ICT; Financial services;

In today's interconnected financial landscape, financial actors outsourcing to specialized Information Communications Technology (ICT) service providers is not merely a strategic option but a fundamental operational model.

Swiss financial institutions and ICT companies operating in or serving the European financial market are navigating an increasingly complex regulatory terrain governing outsourcing. This article, illuminates this intricate landscape, focusing on the EU's landmark Digital Operational Resilience Act (DORA), that is applicable from January 17th, 2025, and its interaction with the established Swiss regulatory framework.

We will delve into the scope of DORA for Swiss players, detail the key obligations and required documentation, and provide a comparative analysis of the EU and Swiss approaches to outsourcing and operational resilience for the financial sector.

Image generated with Midjourney

1. DORA : OBJECTIVES

The EU's DORA (Regulation (EU) 2022/2554)[1] marks a significant shift in financial regulation, aiming at strengthening the cybersecurity and operational resilience of financial entities across the EU. It was adopted in December 2022, is applicable from January 17th, 2025, and forms part of the EU's digital finance strategy.

DORA's key objectives are:

1) **Operation resilience**: ensure financial entities can maintain critical operations during disruptions such as cyberattacks or technical failures.
2) **Third-party risk management**: address risks associated with outsourcing to third-party IT service providers.
3) **Unified standards**: establish consistent requirements across the EU financial sector to reduce fragmentation in regulatory practices.

2. DORA'S SCOPE OF APPLICATION IN SWITZERLAND

While directly applicable within the EU, its impact extends beyond its borders due to its extraterritorial reach.

For Swiss financial actors, understanding this scope is paramount. DORA's extraterritoriality primarily manifests in two scenarios:

a) **Direct EU operations:** Swiss financial entities (e.g., banks, asset managers, securities firms) with a presence within the EU – whether through branches, subsidiaries, or direct service provision to EU clients – fall directly under DORA's purview for their EU operations. This means their EU-based activities must comply with DORA's requirements.

b) **ICT service providers to EU financial entities:** Swiss-based ICT third-party service providers offering services to EU financial entities are also brought within DORA's regulatory ambit. Even without a direct EU presence, if a Swiss ICT provider supports the operations of an EU-regulated financial institution, it becomes subject to DORA's ICT third-party risk management framework concerning those services.

3. DETAILED DORA OUTSOURCING OBLIGATIONS AND DOCUMENTATION

For entities within DORA's scope, the obligations related to outsourcing are not just principles-based guidelines but concrete, enforceable requirements. **Swiss financial institutions and ICT providers must be prepared to demonstrate compliance through robust documentation and operational practices**. Key obligations and associated documentation requirements include:

1) ICT third-party risk management strategy (Article 28 § 1-3 DORA)

- **Obligation:** establish, maintain, and regularly review a comprehensive strategy on ICT third-party risk as an integral part of the overall ICT risk management framework.

- **Documentation:**
  - **Formal ICT third-party risk management strategy document** outlining the approach, methodologies, and governance structure for managing ICT third-party risks.
  - **Policy documents and procedures** implementing strategy, covering aspects like risk assessment, due diligence, contract management, monitoring, and exit strategies.
  - **Register of information** at entity-level in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service

[1] Regulation available here: https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng.

providers, distinguishing between those that cover ICT services supporting critical or important functions and those that do not. Financial entities need to report, at least annually, to the competent authority information on new arrangements on the use of ICT services.

2) Risk assessment and due diligence (Articles 28 § 4-6 and 29 DORA)

- **Obligation:** conduct thorough pre-contractual due diligence to identify and assess all relevant risks associated with outsourcing to ICT third-party providers. This includes assessing the provider's financial soundness, expertise, operational capacity, cybersecurity posture, and compliance with relevant regulations.

- **Documentation:**

  - **Due diligence reports:** comprehensive reports documenting the due diligence process, findings, and risk assessments for each prospective ICT third-party provider.

3) Contractual Arrangements (Article 28 § 7-8 and 30 DORA)

- **Obligation:** ensure written contractual agreements with ICT third-party service providers include a comprehensive set of mandatory clauses as stipulated in DORA. These clauses are designed to protect the financial entity and ensure regulatory oversight.

- **Documentation:** Key clauses to include in either standards template contracts or individual outsourcing contracts include:
  - *clear and complete description of functions to be outsourced;*
  - *Service Level Agreements (SLAs) and performance metrics;*
  - *data location and accessibility requirements;*
  - *provisions on accessibility, availability, integrity, security, and protection of data, including personal data;*
  - *audit and inspection rights for the financial entity and competent authorities;*
  - *obligation of the ICT third-party provider to provide assistance to financial entity at no additional costs, or at a cost determined ex-ante, when an incident is related to the services provides;*
  - *obligation of ICT third-party provider to cooperate with competent authorities;*
  - *termination rights and exit strategies;*
  - *incident reporting obligations of the ICT third-party provider;*
  - *liability and indemnification clauses;*
  - *sub-outsourcing conditions ;*
  - *law and jurisdiction governing the contract.*

Finally, DORA sets specific requirements and oversight for '**critical' ICT third-party service providers**, a pivotal shift that both IT service providers and financial actors must understand. DORA designates ICT providers as "critical" based on their potential to disrupt financial stability, the systemic importance of their services, and the difficulty of replacing them. These criteria, described under Article 32 DORA, aim to identify providers whose failure would have significant repercussions across the financial sector.

⇨ For IT service providers, this means potential designation as a 'critical' entity, triggering direct oversight by the European Supervisory Authorities (ESAs), which are composed of the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA) and the European Securities and Market Authority (ESMA). As outlined in

the ESAs' roadmap dated February 18th, 2025[2], this will involve stringent reporting obligations, detailed risk assessments, and the potential for on-site inspections.

⇨ Financial actors, in turn, must proactively assess their reliance on these providers and ensure their contractual agreements align with DORA's requirements. This includes scrutinizing sub-contracting arrangements and ensuring robust incident reporting procedures are in place. The ESAs' ongoing development of technical standards and the establishment of a register of these critical providers will necessitate both IT service providers and financial actors to closely monitor developments and adapt their operational frameworks to comply with these evolving regulatory expectations, ensuring the resilience of the EU's financial ecosystem

4. SWISS REGULATORY FRAMEWORK FOR OUTSOURCING

While Switzerland does not have a direct equivalent to DORA, it has a regulatory framework that ensures financial institutions meet high cybersecurity and ICT risk management requirements. FINMA's circulars on outsourcing and operational resilience, along with the Federal Act on Data Protection (FADP), establish clear obligations to protect data and manage operational risks. Additionally, federal cybersecurity principles from the Swiss National Cybersecurity Strategy (NCS) and international frameworks like ISO 27001 provide further guidance for strengthening cybersecurity measures. Financial institutions also use these standards to develop and implement their internal operational risk management frameworks, including ICT security, to enhance their resilience against cyber threats and operational disruptions.

Swiss financial institutions that are under FINMA's supervision (for e.g. banks, securities firms, financial market infrastructures, or investment firms) need to comply with the following circulars with regards to outsourcing and operational resilience:

- FINMA Circular 2018/3 – Outsourcing[3]; and
- FINMA Circular 2023/1 – Operational risks and resilience – banks[4].

Financial market laws stipulate that financial actors may delegate some of their tasks to third parties, provided that some safeguards are met, such as appropriate organization and risk limitation.

FINMA Circular 2018/3 on Outsourcing applies to banks and securities firms, insurance companies, managers of collective assets, and SICAVs[5]. Pursuant to this circular, "*outsourcing [within the meaning of this circular] occurs when a company mandates a service provider to perform all or part of a function that is significant to the company's business activities independently and on an ongoing basis*"[6].

FINMA prohibits outsourcing core leadership functions, including strategic decision-making, central management, supervision, and decisions on business relationships. However, other key functions, such as operational risk management and compliance, may be outsourced if regulatory requirements are met. Special rules apply to insurance companies, asset managers, fund management companies, and SICAVs.

---

[2] Available at : https://www.eba.europa.eu/publications-and-media/press-releases/esas-provide-roadmap-towards-designation-ctpps-under-dora.

[3] FINMA Circ. 18/3 "Outsourcing" of 21 September 2017, available at: https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2018-03-01012021_de.pdf?sc_lang=en&hash=0DD08D6FE1C2B6D6CA7576CE036D4713.

[4] FINMA Circ. 23/1 "Operational risks and resilience – banks" of 7 December 2022, available at: https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2023-01-20221207.pdf?sc_lang=en&hash=1529FC7CCFD70F24BCC75C4D1B033ECF.

[5] FINMA Circular 2018/3, no. 5-6.3, p. 3

[6] FINMA Circular 2018/3, no. 3, p. 3.

Financial institutions outsourcing tasks must comply with FINMA's supervisory standards to ensure transparency, risk management, and accountability. Supervised entities need to comply with the following requirements :

- **Updated inventory**: maintain a current list of outsourced functions;
- **Risk-based selection**: carefully assess service providers based on economic and operational risks;
- **Internal oversight**: integrate outsourced functions into internal controls and designate a monitoring unit;
- **Contracts:** define responsibilities, document services, and establish contractual agreements;
- **Subcontracting rules**: ensure early notification of key subcontractor changes and maintain termination rights;
- **Audit and control rights**: grant oversight access to the company, its auditors, and FINMA, even for providers abroad; and
- **Security measures**: establish IT security requirements and continuity plans for critical functions.

In all cases, the outsourcing company remains accountable to FINMA in the same way as it would if it performed the outsourced function itself. It is worth noting that FINMA may impose further conditions on a company or grant a company partial or total exemption from compliance with this circular.

FINMA Circular 2023/1 outlines the requirements for managing operational risks and ensuring operational resilience for banks and other supervised financial institutions[7]. In this context, FINMA refers to operational resilience as "*the institution's ability to restor its critical functions in case of a disruption within the tolerance of disruption*"[8]. This entails the institution's ability to identify threats and possible failures, to protect itself from them and to respond to them, to restore normal business operations in the event of disruptions, through a business continuity management (BCM) approach, and to learn from them, so as to minimize the impact of disruptions on the provision of the critical functions. These requirements are to be implemented on a case-by-case basis, depending on the size, complexity, structure and risk profile of each institution. FINMA maintains discretionary power in the application of such requirement in individual cases.

FINMA Circular 2023/1 mandates institutions to achieve operational resilience through proactive management of operational, ICT, and cyber risks. Specifically, institutions must:

- **Manage operational risks:** categorize, inventory, assess, and monitor operational risks, defined as financial losses from internal process or system failures[9]. Report regularly, including semi-annual updates to the executive board and annual risk tolerance approval by the board of directors.

- **Ensure effective ICT governance:** implement robust governance, change management, and incident response procedures.

- **Implement comprehensive cyber risk management:** identify threats, implement protective measures, detect and respond to cyber incidents, and conduct regular security tests.

- **Secure critical data:** classify and protect critical data, control access, and oversee third-party data handling.

[7] Namely banks under article 1a and persons under article 1b of the Banking Act (BA), securities dealers under article 2 para. 1 let. 3 and article 41 of the Financial Institutions Act (FinIA) and financial groups and financial conglomerates under article 3c BA and 49 FinIA.
[8] FINMA Circ. 23/1, no. 18, p. 4.
[9] FINMA Circ. 23/1, no. 3, p. 3.

- **Establish Business Continuity Management (BCM):** conduct business impact analyses, develop recovery plans, implement crisis management, define critical functions, set disruption tolerances, and regularly test resilience measures.

These requirements aim to ensure institutions maintain operational continuity and resilience in the face of disruptions.

Moving on to the legal framework around data protection and cybersecurity, the FADP requires data controllers, meaning financial institutions processing personal data of individuals (clients, employees, and others), to implement appropriate organizational and technical measures to ensure the security of personal data in proportion to the risks involved. These measures must be designed to prevent any data security breaches and ensure the confidentiality, integrity, and availability of personal data[10]. This includes access control, protection against unauthorized modification, deletion, or destruction, rapid data restoration in case of incidents, regular system updates, and monitoring of access and modifications to ensure traceability and detect potential security breaches[11].

5. A COMPLEMENTARY APPROACH?

Both frameworks have the following differences:

	DORA (EU)	**Switzerland**
Regulatory Approach	Prescriptive and **enforces harmonized rules across the EU**.	Principles-based, allowing **flexibility in implementation**.
Supervision of ICT Providers	ICT third-party providers are **directly regulated** and must comply with specific obligations.	ICT providers are **not directly supervised**, but financial institutions must manage outsourcing risks under FINMA Circular 2018/3.
Resilience Testing	Mandatory **penetration testing, threat-led tests (TLPT), and scenario-based testing** for key financial entities and ICT providers.	**Encouraged but not mandatory** under FINMA's operational resilience framework.
Incident Reporting	**Strict reporting timelines** to national regulators, requiring cross-border incident sharing.	Reporting obligations **depend on severity**, with no unified cross-border sharing requirement.
Scope	Covers **all financial entities and ICT providers** operating in the EU.	Covers **banks, insurers, and financial institutions**, but ICT providers **fall under outsourcing rules, not direct supervision**.

Although DORA and the Swiss regulatory framework differ in structure, financial institutions can leverage both frameworks to enhance their cybersecurity and ICT risk management strategies.

- For Swiss financial institutions operating in the EU, aligning with DORA's stricter requirements **ensures compliance** across jurisdictions while reinforcing risk management practices in Switzerland.

[10] Article 8 Federal Act on Data Protection of 25 september 2020 (FADP, RS 235.1).
[11] Articles 2 and 3 Ordinance on Data Protection (OPDo, RS. 235.11).

- For third-party risk management, DORA introduces direct oversight of ICT providers, while Switzerland requires financial institutions to manage outsourcing risks. Institutions working with EU-based ICT service providers may benefit from DORA's structured requirements, enhancing their **security posture**.

- For resilience testing and incident reporting, Swiss institutions can voluntarily adopt DORA's penetration testing and structured reporting protocols to strengthen their cyber resilience beyond FINMA's minimum expectations.

By integrating elements of both frameworks, financial institutions can achieve a more robust, internationally aligned risk management approach, ensuring resilience against evolving cyber threats while maintaining regulatory compliance in multiple jurisdictions.

6. CONCLUSIONS

With DORA introducing strict requirements in the EU and FINMA overseeing outsourcing and operational resilience in Switzerland, **both financial institutions and ICT service providers must assess their regulatory obligations and take steps to ensure compliance**.

For Swiss financial institutions:

1. Check **applicability**: determine if your organization falls under DORA's scope, especially if operating in the EU.
2. **Assess gaps**: identify where your outsourcing, ICT risk management, and resilience measures may not meet DORA or FINMA requirements.
3. **Plan and adapt**: develop a strategy to align internal frameworks with both regulatory standards.
4. **Review internally**: conduct audits to ensure compliance with third-party risk management, operational resilience, and cybersecurity obligations.
5. **Train staff**: educate employees on incident reporting, ICT risk governance, and outsourcing management under both DORA and FINMA regulations.

For ICT service providers operating in Switzerland and the EU:

1. **Determine your regulatory exposure**: identify if your services to EU-based financial institutions require compliance with DORA's ICT provider obligations.
2. **Align with client expectations:** ensure that your risk management, security controls, and incident response processes meet the requirements of financial clients under both DORA and FINMA's outsourcing rules.
3. **Enhance cyber resilience**: implement stronger security frameworks, such as ISO 27001, and conduct regular resilience testing.
4. **Demonstrate compliance**: be prepared to provide financial clients with evidence of compliance with applicable cybersecurity and operational resilience standards.
5. **Stay updated on regulatory changes**: monitor developments in DORA enforcement and FINMA regulations to adapt your compliance strategy proactively.

By taking these steps, Swiss financial institutions and ICT service providers can enhance resilience, manage regulatory risks, and maintain trust with clients and regulators in both Switzerland and the EU.

***

Your contacts

Florian Ducommun
Partner
fd@bonnard-lawson.com

Crystal Dubois
Senior Associate
cd@bonnard-lawson.com