Cordial Systems

21 ANALYTICS

DORA in MiCA and TFR Compliance: A Practical Guide for Institutions

Introduction

Over the last few years, plenty of literature has been published about the various swaths of European regulations coming into effect that will impact Crypto Asset Service Providers (CASPs). Less has been mentioned about the practical considerations that an executive team and nominated compliance officer face when trying to implement an appropriate control framework that addresses the requirements. This topic is increasingly dominating the conversation amongst CASPs operating in or serving the European market, particularly as important regulatory deadlines begin to loom. As such Cordial Systems (a custody technology solution following zero trust security principles) and 21 Analytics (the only privacy-first Travel Rule compliance software provider) have teamed up to publish this short guide to help relevant stakeholders think through some of the pertinent questions they face in preparing to continue operating in Europe in a compliant manner.

What are MiCA and TFR?

The MiCA (Markets in Crypto-Assets) regulation is a comprehensive legal framework introduced by **the European Union to regulate the crypto-assets market. It covers crypto-assets that are not currently regulated by existing financial services legislation. The MiCA regulation aims to create a harmonised regulatory environment across the EU, addressing the opportunities and risks associated with new financial technologies**. It is applicable to all legal persons intending to provide crypto-asset services in the EEA, requiring such entities to submit an application for authorisation containing all the information set out as requirements in Article 62(2) of MiCA.

TFR stands for the Transfer of Funds Regulation, an obligation on financial firms to accompany transactions with information on their originators and beneficiaries, extended in 2023 to also apply to crypto-asset service providers (CASPs) as defined by MiCA. It is the European Union's implementation of the Travel Rule. CASPs in the EEA must collect, hold and share data on the people involved in all cryptocurrency transactions with their CASP counterparties.

What is the Digital Operational Resilience Act (DORA)?

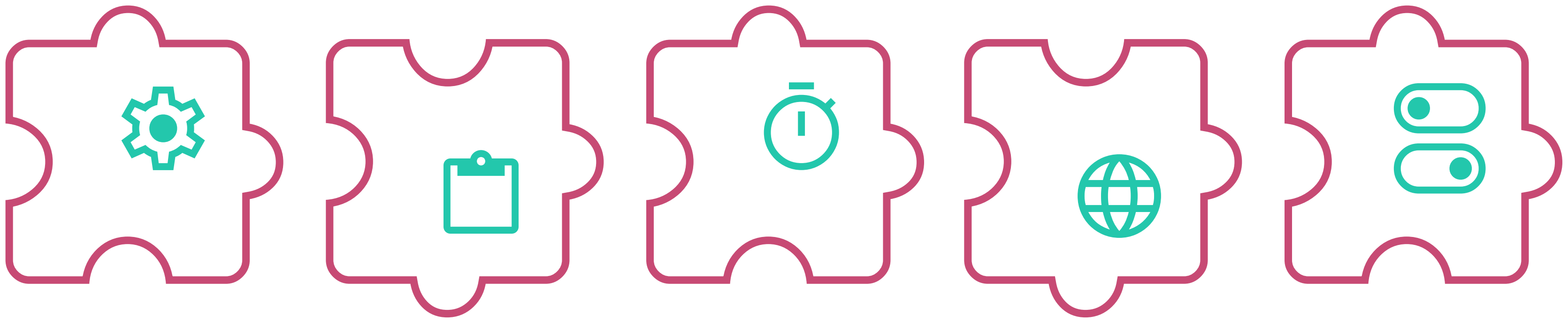
The Digital Operational Resilience Act (DORA), initially drafted on 24 September 2020 with the final version becoming applicable by 17 January 2025, is a separate body of work that lays out uniform requirements concerning the security of network and information systems supporting the business processes of financial entities (CASPs are in scope). The requirements range from: ICT risk management, reporting of incidents, digital operational resilience testing, and proper management of third-party risk. DORA has two main objectives: strengthening the financial sector's resilience to Information and Communication Technology-related incidents and harmonising existing risk management regulations within the European Union.

Digital operational resilience is a broad term with far reaching scope and responsibilities. Specifically, it is defined in the act as: *"the ability of a financial entity to build, assure and review its operational integrity and reliability by ensuring, either directly or indirectly through the use of services provided by ICT third-party service providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity uses, and which support the continued provision of financial services and their quality, including throughout disruptions."*

While that is a mouthful, the **main thing to note is that obligations don't just extend to the financial entity directly, the entity has a responsibility to ensure they remain compliant when leveraging outsourcing or service provider relationships** and is therefore considering a greater surface area of risk which extends to contracted vendors and their subcontractors. As DORA has a great impact on financial entities in the EU and how they manage their technological choices, this guide also explores how to consider different software delivery models and what level of responsibility might be appropriate when relying on a third-party provider.

Why is compliance urgent?

MiCA became part of EU law in June 2023. Its provisions, however, will not be fully applicable, i.e., mandatory and enforceable, until 30 December 2024. There is also a transitional regime which provides some extra time for CASPs operating under existing legislation (e.g. pursuant to a local license or registration). Meaning, if a CASP has already been operating in a compliant manner within the local state, then they may continue to do so until 30 June 2026 - or sooner depending on the local authority, who can shorten the transition period (Germany is one state that has shortened to 30 December 2025, the grandfathering period in Lithuania is 5 months and in the Netherlands 6 months). The EU gives Member States the option for existing CASPs to apply a simplified procedure for license applications that are submitted between 30 December 2024 and the final date of that particular state's transition period. This simplified procedure is only available in Malta, Germany, and France but under certain conditions.



DORA's Pillars

ICT Risk Management
Specific requirements on ICT risk management cycle: detection, identification, response, recovery. Frameworks to be reviewed at least annually.

Managing 3rd Party Risks
Risk management over full lifecycle: pre-engagement, monitoring, termination, exit strategies. Also a focus on concentration risk.

ICT Related Incidents
Reporting of major incidents to the national competent authority is mandatory.

Information Sharing
Enphasis on sharing cyber threat information and intelligence to enhance resilience of all.

Digital Operational Resilience Testing
Additional threat-led penetration requirements and specific criteria on who performs the different testing.

MiCA applications are a lot of work!

An important initial step of a competent authority's authorisation process is to check whether the application is complete. On this basis, the competent authority assesses the submitted information on whether the applicant is capable and ready to comply with the relevant requirements of the MiCA framework and other applicable regulations (such as TFR, AML, etc). The requirements for the information to be included in the application are also set out in the draft Regulatory Technical Standards (RTS) and Implementing Technical Standards (ITS) as high-level provisions. Right now only a handful of RTS drafts have been adopted by the European Commission as a Delegated Regulation - which themselves are directly binding on CASPs and financial entities needing to comply with MiCA & DORA.

If the submitted application and information lacks appropriate specification, or misses any requirements in the draft technical standards, then the competent authority may have to request additional information from applicants to be able to conduct a meaningful assessment on whether authorisation should be granted or not. In short, you need to build a strong case that shows you understand the risk profile of your company, and have factored in the appropriate controls in relation to the specific requirements in order to satisfy having your MiCA application looked at beyond the initial check.

Concretely, an application should contain a program of operations, describing the notifying entity's (the CASP's) organisational structure, strategy in providing cryptoasset services to its targeted clients, and its operational capacity for the three years following notification. There are also the usual accompanying components, such as:

- Showing compliance with prudential and organisational rules,
- Adhering to transparency and disclosure rules (such as issuance of a whitepaper),
- Implementing robust governance and operational frameworks,
- Segregation of clients’ assets,
- Safekeeping of clients’ crypto assets and funds,
- Risks and internal controls systems,
- Record keeping,
- Trading rules including transparency, policy and procedure on fair and orderly trading and best execution policy,
- Stress testing,
- Business continuity and disaster recovery plans,
- Cybersecurity requirements,
- Investors and consumer protection measures,
- Requirements for preventing insider dealing and unlawful disclosure of inside information and market manipulation related to crypto-assets,
- Having strong compliance programs and systems in place, which includes transaction monitoring and trade surveillance, allowing for prevention, detection and reporting.

If handling client assets then a description of the entity’s procedure for the segregations of client assets to ensure they are bankruptcy remote as well as a description of the overarching custody and administration policy. When describing the strategy used to target clients, the notifying entity should describe the marketing means that it intends to use, for instance, websites, mobile phone applications, face-to-face meetings, press releases, or any form of physical or electronic means, including social media campaign tools, internet advertisements or banners, retargeting of advertising, agreements with influencers, sponsorships agreements - this all forms part of the regulatory business plan.

Operational resilience is one of the biggest areas of concern!

The competent authority should be able to assess the notifying entity's resilience to withstand external financial shocks, including those concerning the value of cryptoassets. Therefore, the notifying entity should include stress scenarios simulating severe but plausible events in its forecast accounting plan. It is critical to maintain operations or at least essential functions and to minimise downtime due to unexpected disruptions (such as cyberattacks, or a key outsourced process is temporarily unavailable). A MiCA application should thus contain detailed information on the entity's arrangements to ensure continuity and regularity in the performance of its crypto-asset services. A lot of this is familiar to compliance individuals, such as the business continuity and disaster recovery plans.

However, due to the decentralised and digital nature of crypto-assets, cybersecurity risks for crypto-asset service providers are significant and take many forms. **To ensure that applicants are able to prevent data breaches and financial losses that may be caused by cyberattacks, competent authorities should be provided with information on the applicants' deployed ICT systems and related security arrangements, including the human resources dedicated to addressing cybersecurity risks**.

The segregation of client crypto-assets and funds is an important part of the regime regulating crypto-asset services as it protects clients from losses of the crypto-asset service provider and from misuse of their crypto-assets and funds. CASPs are therefore subject to an obligation to make adequate arrangements to safeguard clients' ownership rights which has been a mainstay of financial regulations over the years and in more recent times to CASPs as well. This requirement applies to any CASPs holding client assets, not just those which provide custody and administration services.

CASPs' Outsourcing to Service Providers

Financial institutions, including CASPs, often rely on third-party providers to support their operations. The new regulatory framework impacts these relationships. It is proving to be one of the trickiest parts of ensuring your entity remains compliant, these external sources of risk have a real probability of materializing and impacting your ability to operate. Therefore, a lot of attention is needed in understanding the different types of solutions, software delivery models, and who has responsibility for what between vendor and CASP - keep in mind that these are responsibilities in the service model sense, **the CASP is still responsible for all compliance obligations**.

MICA's Outsourcing Provisions: Article 73

Going back to the program of operations, this also includes an outsourcing policy and how it was adapted to crypto-asset services as well as a detailed description of the entity’s planned outsourcing arrangements, including intra-group arrangements, and how the entity intends to comply with the requirements set out in Article 73 of MiCA.

Regulators have long imposed obligations directly on financial entities through guidance, requirements and principles of a risk-based approach to third-party risk management. This is all old hat for tenured legal and compliance individuals. However, we are now seeing regulators push requirements past the financial entity and down onto their engaged ICT service providers - as well as their subcontractors in some cases. Article 73 is very clear in its intentions here, and for that reason copied verbatim:

"Crypto-asset service providers that outsource services or activities to third parties for the performance of operational functions shall take all reasonable steps to avoid additional operational risk. They shall remain fully responsible for discharging all of their obligations pursuant to this Title and shall ensure at all times that the following conditions are met:

a. Outsourcing does not result in the delegation of the responsibility of the crypto-asset service providers;

b. Outsourcing does not alter the relationship between the crypto-asset services providers and their clients, nor the obligations of the crypto-asset service providers towards their clients;

c. Outsourcing does not alter the conditions for the authorisation of the crypto-asseet service providers;

d. Third parties involved in the outsourcing cooperate with the competent authority of the crypto-asset service providers' home Member State and the outsourcing does not prevent the exercise of the supervisory functions of the competent authorities, including on-site access to acquire any relevant information needed to fulfill those functions;

e. crypto-asset service providers retain the expertise and resources necessary for the evaluating the quality of the services provided, for supervising the outsourced services effectively and for managing the risks associated with the outsourcing on an ongoing basis.;

f. crypto-asset service providers have direct access to the relevant information of the outsourced services;

g. crypto-asset service providers ensure that their parties involved in the outsourcing meet the data protection standards of the Union.

For the purposes of point (g) of the first subparagraph, crypto-asset service providers are responsible for ensuring that the data protection standards are set out in the written agreements referred to in bullet 2 below.

1. *Crypto-asset service providers shall have a policy on their outsourcing, including on contingency plans and exit strategies, taking into account the scale, the nature and the range of crypto-asset services provided.*

2. *Crypto-asset service providers shall define in a written agreement their rights and obligations and those of the third parties to which they are outsourcing services or activities. Outsourcing agreements shall give crypto-asset service providers the right to terminate those agreements.*

3. *Crypto-asset service providers and third parties shall, upon request, make available to the competent authorities and other relevant authorities all information necessary to enable those authorities to assess compliance of the outsourced activities with the requirements of this Title."*

This is just the start. As part of setting up, or detailing out, the program of operations and how to handle outsourcing and service providers, let’s also take a look at what DORA has to say about this. This will help collect all the necessary informational inputs which need to go into any plans for not only MiCA and Travel Rule readiness but also as part of being prepared for DORA. You can’t do one without the other. Therefore, the requirements for outsourcing and service providers are actually more extensive than as seen at first glance.

To quickly summarise, DORA mandates that in-scope entities have an internal governance and control framework for effective and prudent management of ICT risk in order to maintain high standards of availability, authenticity, integrity and confidentiality of data. The management body bears the responsibility for setting and approving the digital operational resilience strategy including the determination of the appropriate risk tolerance of ICT risk **i.e. any failure or program deficiency is risk that runs all the way up the chain of command - in some jurisdictions, executive management are personally accountable for regulatory failings**.

This includes familiar requirements of building controls and programs internally, similar to those highlighted above under MiCA outsourcing, covering topics from: risk identification, listing of controls, ongoing monitoring, protection and prevention strategies, incident response and recovery plans, business continuity planning, and periodic testing arrangements. However, what is striking (and in keeping with a trend seen by regulators globally) is the amount of language and emphasis on third-party arrangements. DORA is comprised of 64 Articles, of which 17 touch directly upon managing third-party outsourcing and service providers, which presents some of the biggest challenges to CASPs! Note, that this is not just in the form of your typical third-party risk management program, but also imposes obligations which the CASP must pass on to its key ICT outsourcing and service providers. Let's unpack it.

Intra-group arrangements

First is to distinguish between intra-group arrangements (yes, these need documenting too) and true third-party arrangements with unaffiliated entities. For the former, you might have some common tech resources supporting all entities or other shared services within the group; those should be documented with an arm's length agreement and will also require ongoing monitoring and auditing. Moreover, the local European entity will need its own boots on the ground and compliance leaders who have direct access to local executive management. Meaning the **mind and management should be local to the European entity with material substance in the way of resources for the entity, rather than falling back on a parent entity or affiliate** in another country which has its own regulatory licensing and compliance department.

Contractual rights amendments (DORA)

Segmenting down further into service providers and outsourcing arrangements, it quickly becomes clear under DORA that template Master Software Agreements of popular third-party service providers in crypto will need to be forced to make significant changes and take on significant ownership (at the contractual level) for upholding their end of the bargain. This will become clear in the gap analysis for a CASP getting ready to submit its regulatory application. Few providers are proactively working on this, so it will be up to the CASP to force the point home and ensure the appropriate additions and contractual provisions, where appropriate to do so, are added into their current and prospective Master Software Agreements - or find a vendor who is already taking this seriously.

To mitigate risks associated with a provider's ability to help meet the CASPs regulatory obligations, the CASP should obtain a commitment from the provider in their service agreement to provide and maintain the features, functionality, and tools necessary for all use cases. Making sure that it all works appropriately and compliantly before deployment. The contractual arrangements referred to shall also distinguish between those that cover ICT services supporting critical or important functions and those that do not. If deemed critical ICT, the CASP in question needs to put in place exit strategies and transition periods that ensure an orderly continuation of business should any contractual termination rights be exercised.

Ongoing commitments from 3rd parties

Business Continuity Plan (BCP) & Disaster Recovery (DR) testing

This goes back to shared responsibility models and understanding the division of responsibilities and implementing appropriate controls over operations. A fully vendor-side hosted solution may hinder the CASP's ability to participate in business continuity plan testing, citing reasons of security and confidentiality. This has been common practice in traditional markets with cloud computing providers as an example. However, it is hard to know if this is some vague security through obfuscation rather than an honest rationale for denying a regulated entity trying to satisfy its obligations.

As far as MiCA/DORA is concerned, these are ad hoc annual tests which might be challenging to coordinate with a SaaS-hosted vendor. Can they even accommodate these off-cycle requests coming from several different European customers? Might it impact their ability to serve other end users in their production environment? These are all legitimate concerns for both parties. On the other hand, if the same CASP can host all the components locally within their four walls, then they not only have full control over the technology and security-critical components, they also have the ability to run in depth BCP and DR exercises end to end without impediment and without worrying about any impact through sharing infrastructure with other tenants since it is all deployed and dedicated to them.

Threat led penetration testing

Subsets of the TIBER-EU framework, for threat intelligence-based ethical red teaming, form part of DORA’s requirements for network security and information systems security. This is designed to mimic the tactics, techniques, and procedures of real-life attackers to highlight where a CASPs strengths and weaknesses are. Again, this penetration testing exercise extends to a CASP’s critical third-party providers. Therefore critical ICT such as wallet providers and Travel Rule providers need to participate and fully cooperate in a CASPs threat led penetration testing exercise as referred to in Articles 26 and 27. This needs to be a contractual provision in the agreement with the third party. While a SaaS-based wallet will again be pulled into multiple directions for European regulated entities performing penetration testing, if you self-host your wallets then you are not as dependent on the third-party vendor in order for you to perform the exercise.

Audit rights

A CASP will also need to include contractual provisions for exercising access, inspection and audit rights over the ICT third-party service provider. Financial entities shall, on the basis of a risk-based approach, pre-determine the frequency of audits and inspections as well as the areas to be audited by adhering to commonly accepted audit standards in line with any supervisory instruction on the use and incorporation of such audit standards. Depending on the level of risk associated with the service provider this could extend to reviews of a vendor’s premises, data centers, and systems in order to verify and ensure compliance with the Service Agreement and applicable laws and regulations. For self-hosted critical ICT you have direct access and responsibility, therefore reducing the responsibilities and dependencies on the third party which, in turn, reduces the audit scope.

Cyber Security and Data Protection

Earlier in 2024, the European Banking Authority (EBA) published the risk assessment report (RAR), which found that cyber risks and data security rank the highest among operational risks for financial entities.
In addition, **the German regulator BaFin has also highlighted the "higher than ever" cybersecurity risks for the financial sector due to interaction with two valuable assets: money and sensitive data. According to BaFin, the high potential for damage is also relevant when the financial entities' third party service providers are targets, due to the growing attack surface**.

Hence, this is one of the main concerns for compliance teams, going beyond GDPR and adding DORA requirements to the housing and transmission of data which will happen regularly through a CASPs Travel Rule obligations. Even more so than the usual KYC providers which may be in contact with a customer's onboarding data, the Travel Rule requires such Personally Identifiable Information (PII) to be attached to their transaction information and will be part of routine operations for most business models.

When one provider stores this information for several CASPs, it becomes a centralised honeypot, holding a larger volume of valuable data. As the blockchain's pseudonymity is no longer kept if this very sensitive data is breached, such information must be held to the utmost security standards.

Before DORA, CASPs could potentially overlook a higher data and cybersecurity risk by trusting their SaaS providers' "full encryption" disclaimers and that auditable data would be available when needed. Now, CASPs need to thoroughly inspect outsourced data flows and storage, as well as put agreements in place to protect them from incidents. We shall evaluate later in this document the different software delivery models, highlighting where a SaaS third-party provider may become a heavier burden, and where CASPs leveraging on-premises software can guarantee their level of security as it is controlled by the CASP and in line with its own technology stack.

Data Residency

The location of data is always an important consideration for regulators. In some instances they may insist that it lives on a server within the borders of their country. Therefore, you need to know how an IT vendor handles this themselves, but also the subcontracting arrangements they may have. The introduction of subcontractors and sub-processors for data is common but may also raise complex compliance issues, especially when they are located outside of the country of the regulated institution and if there is a cross-border transmission of regulated data.

Where privacy laws under GDPR are relevant to a CASP, it may not always be necessary for them to pre-approve subcontractor arrangements with their vendor; however they should have the right to receive notification of, and the right to object to, each new subcontractor being engaged. That is the reality of regulation in a lot of countries with sophisticated regulatory frameworks. Once again invoking the question of how can the product itself be made fit for purpose. Consider what you, the customer as a regulated CASP, can host and directly control versus what the vendor should hold, and what is appropriate subcontracting or sub-processing. If there is a data breach on the vendor side, then the CASP should have a contractual provision in the agreement which allows them to be notified promptly so that they may satisfy their own obligations should they be impacted.

This also extends to regulation around books and records keeping. Typically, CASPs need to retain Travel Rule and other financial data for a significant period of time, usually around five years. This also extends to personally identifiable information, data collected during investigations, and more, which can be anywhere from 5 to 10 years depending on the data and jurisdiction. **If a CASP moves away from a vendor, they may well need to port the data with them in order to keep it available** - there have been some horror stories in the cryptocurrency space of vendors retaining data as a hostage when a customer has terminated the agreement.

All of the above subsections should form part of your vendor due diligence and inform how to appropriately paper the relationship and customer rights, both in the beginning and as part of monitoring over time.

Examples of Critical ICT

We have provided a lot of food for thought when reviewing and evaluating critical ICT providers. A quick side note on definitions, the relevant national competent authorities will decide which providers are deemed critical ICT in their definitions. However, as an executive or nominated compliance officer you should also know what is critical ICT to your operations in the sense that if a provider is unavailable, is there a disruption to your ability to provide your own service? Financial entities may, in the context of a digital operational resilience strategy, define a holistic ICT multi-vendor strategy, at group or entity level, showing key dependencies on ICT third-party service providers and explaining the rationale behind the procurement mix of providers. As such we will now review the use of a couple of tools, wallets and travel rule solutions, which are fundamental to the operation of almost any CASP in Europe.

Wallets

If you are a very active trading desk or an exchange operating a central limit order book, you may have multiple wallet providers all being used for different use cases, however, they are all deemed critical IT infrastructure (regardless of whether it’s a cold storage offering, or basic in-browser wallet extension). While they may each serve unique use cases (large cap coins, exotic trade flow, DeFi, offline vs online storage etc) they almost certainly have varying sophistications in control frameworks and likely won’t be able to operate as backup vendor options to each other. In fact, the juggling of multiple wallet providers came about because no single vendor could meet all the needs of their customers.

On the other end of the spectrum, you may just pick a multi-party computation (MPC) wallet provider and keep all of your cryptocurrencies there - which then highlights the issue of concentration risk. What is your business continuity plan if they are suddenly unavailable, or in a disaster recovery scenario? You may point to using another third party for use of disaster recovery services to retrieve your keys, but then what?

If a 1,000 customers are all reaching for the emergency exit because the same vendor is down then how certain are you that you can recover your keys within an acceptable time frame? You could easily be looking at several days to recover your assets, breaching your own service level agreements, and potentially other contractual business obligations. We will revisit third-party dependencies later on in this document and how to think through the appropriate service and responsibility model for your business. Just note that you need to go much deeper than surface-level answers and analysis if you are to competently show the regulator that you understand your surface area of risk.

Next **you will need to test your contracts with key IT providers for conformity with MiCA and DORA - a discovery and mapping exercise that highlights any gaps. The list of key contractual provisions is extensive**. Over 20 areas are highlighted in DORA’s Article 30 requirements and with targeted rules, along with more detailed requirements in the RTS. Therefore, you likely have some remediation work to bring the contracts with your wallet or custody vendor into compliance with Article 30. Likewise, you should incorporate procedures around this body of work into your Third Party Risk Management program as part of your broader vendor procurement strategy when entering into, monitoring, and terminating contracts with critical IT service providers - as per the overall risk management framework eluded to by Article 6(1) of DORA.

Travel Rule solutions

All financial entities need a Travel Rule solution that enables collecting, storing and, ultimately, sharing the originators' and beneficiaries' data with their counterparties when facilitating transactions on behalf of their customers. CASPs usually rely on their Travel Rule solution (and their associated technology standards of data exchange) to identify and connect to their counterparties, fundamentally enabling transactions to be executed and data to be transmitted. According to the regulation in the European Union and many other jurisdictions, CASPs should not allow for the initiation of a transfer (when acting as the originator CASP), or credit the incoming funds (when acting as the beneficiary CASP) before guaranteeing compliance with the Travel Rule. Hence, it is clear that compliance with the Travel Rule plays a key part in allowing transactions in and out on a day-to-day basis.

In that scenario, CASP's businesses that focus on trading or facilitating transfers, such as trading platforms and exchanges, could consider their Travel Rule compliance service providers as critical ICT, since the service heavily touches their core operations. However, this may not be the same for CASPs that focus on long-term custody or advisory services, for instance, where transacting in and out is not the core business, resulting in less stringent DORA requirements to comply with.

When using a SaaS solution, the required Travel Rule data might be held by the CASP's provider. Due to the considerably bigger data breach and reputational risks, DORA requires CASPs to monitor third-party provider risks, know how their customer's PII data is handled, as well as implement robust security policies to avoid hacks, interception or unauthorised access. These must be reflected in detailed contracts that specify service levels and data processing locations, but still present the risk of non-fulfilment. When relying on an on-premises solution, CASPs have an easier time guaranteeing security measures are complied with at all times, gaining more control and visibility over their customer's data protection and satisfying these obligations directly rather than relying on a sub-contractor or processor.

Another relevant third-party risk aggravated by centralised SaaS Travel Rule solution providers is completely relying on them for counterparty identification. If the provider is unavailable, CASPs become unable to even find the relevant counterparty CASP of a crypto transfer, halting transactions and disrupting the business. Customers effectively cannot withdraw some or all of their funds, a worrying scenario for both them and their CASP. DORA requires CASPs to have an incident management plan, which, again, is easier to put in place and control if the CASP does not completely rely on the provider to exchange Travel Rule data, but leverages open standards to do so, like TRP for counterparty identification and data transmission or IVMS for its data structure.

Software Delivery Models

We have touched upon this throughout, yet it is worthy of its own section. While a SaaS solution (vendor-side hosted products) offers some extra convenience, they do offer a significantly larger surface area of risk as you put your trust in them to run all the infrastructure, secure the hardware, endpoints, data, network controls, access rights, and more to deliver the service. This translates to placing more trust in your third-party provider to satisfy your compliance obligations. There might be a proportionality argument here that small CASPs lack the resources to do this themselves, in which case a vendor-side hosted solution may be more prudent. You swap the ability to design your own control frameworks for inheriting that of the provider hosting the solution, as such you need to heavily document and ensure you understand everything as discussed throughout this guide. However, for a larger firm following a risk-based approach, there is a strong argument to be made that this could well necessitate retaining more of the responsibility internally with comprehensive and rigorous oversight as we shall see.

SaaS and vendor hosted products

Of course, SaaS products that are critical IT can be managed to be compliant. However, there are many good reasons why established legacy financial institutions run certain critical systems on-premises. Adding DORA's prescriptive requirements around the responsibilities of the third-party entity to the regulated entity itself only increases the reasons to spend time critically evaluating these two delivery models. A cloud-hosted CRM tool with PII data might be easier to manage the risk, versus a vendor-hosted crypto wallet. The market reality for the latter is that a lot of CASPs have adopted a handful of SaaS-based MPC wallets which run on a common infrastructure for all clients as a monolithic design and introduces concentration risks across many vectors of concern. This is only exacerbated by the fact that a lot of these solutions run as a black box, making it almost impossible for a CASP to follow a risk-based approach. Diligent buyers therefore end up taking a leap of faith and the customer’s risk officers subsequently impose risk limits on how much dollar exposure they want to face from that provider.

Continuing with crypto wallets as an example of critical ICT, an effective approach to risk management requires a full understanding of the structure of the service arrangement. Responsibility for security and availability of data and services, e.g. where are the key shares, who hosts the policy engine on how keys are used, how is hardware secured, infrastructure, endpoints, data, network controls and access just to name a few. With SaaS-based wallets a lot of this is the responsibility of the vendor - but you are still on the hook for any failures as the regulated CASP.

Similarly, SaaS compliance solutions are a typical choice for CASPs. As internal IT resources are often scarce, businesses can independently upgrade their operations by quickly signing up to a web service.

In Travel Rule compliance, this approach gives the third-party access to the very sensitive customer data destined for a CASP's counterparty, as well as the CASP's business sensitive information, such as their wallet addresses and traded volume. Here, the black box acts as the mailman; collecting and storing data, as well as finding out which counterparty CASP is the destination. Therefore, CASPs relying on centralised providers are risking their data protection, but also effectively making the critical function of transferring funds in and out highly dependent on the provider's availability and business continuity.

On-prem and self hosted

This is why more CASPs are turning to running infrastructure on-prem or on their own virtual servers as this shifts the ability to satisfy the long list of regulatory requirements into their own hands. There is no right or wrong when it comes to hosted or self-hosted critical IT, however, given the depth of compliance obligations under MiCA, DORA, and TFR it is easier to be compliant over controls which you directly own and implement locally providing that you have some internal resources to handle a local deployment.

A further consideration in evaluating a hosted offering, **even if you could get your critical IT vendors to incorporate all of these obligations, do you trust all of these providers to uphold their end of the bargain? This is where deployment models become even more of a consideration in the risk analysis**. For self-hosted solutions your response to a regulator is no longer pointing to a third party and hoping they are upholding their end of the bargain. Instead, your answer is determined first-hand by the CASP, and you can have full confidence in critical ICT that you control and build policies and procedures around.

Again, there might be a proportionality argument here that small CASPs lack the resources to do this themselves, in which case a vendor-side hosted solution may be more prudent. However, for a CASP of any significant size or looking to “level up” their security posture and approach to risk and compliance, the ability to self-host is more viable and has long been the approach of highly regulated firms in various markets. It is now becoming a question that is getting tackled in various management meetings as firms prepare themselves on a forward-looking basis for these new regulations and what it means for their operations.

	Service Provider's Delivery Model	
	On-premises (Self-hosted)	Software-as-a-Service (SaaS)
Security measures and contractual changes	Greater flexibility in changing security policies and protocols.	Limited flexibility as CASPs must rely on vendor's architecture and policies.
Business Continuity Plan (BCP) and Disaster Recovery	CASP has full control over BCP and disaster recovery testing, and can conduct end-to-end tests.	Testing may be limited by the provider due to security and confidentiality concerns. Other customers compete for resources and impact results when testing at the same time.
Audit Rights	Direct audit of local systems, reducing audit scope and complexity.	Requires comprehensive audit rights in contracts, including knowledge of vendor premises and data centres.
Data Protection	CASP can control how, where, and which data is stored, to protect customer's sensitive PII complying with local laws.	Data is managed by the provider, raising concerns and obligations on safety, subcontractors and cross-border data flows.
Costs	Potentially higher upfront investment in infrastructure, but long-term control benefits.	Potentially lower upfront costs, but increased reliance, reputational and third-party management risks.

In summary

The European regulatory landscape has developed rapidly over the last few years and the time for taking action internally is already here. Whether it is reviewing your vendor due diligence, contract management, or deciding how to partition the duties of the vendor and the CASP in a shared responsibility model, there is a lot required in bringing third-party risk management and critical ICT up to the standard demanded by regulators enforcing MiCA, DORA, and TFR.

Both routes, hosted and self hosted, can be handled appropriately to be compliant. We reviewed the advantages and disadvantages of each and explored some pertinent questions in understanding the risks associated with them. When choosing SaaS providers, CASPs value convenience, likely they have very limited technical resources internally, and will lean heavily on a provider to maintain uptime availability, data, cyber security and more. Be sure to understand exactly what each party is responsible for and appropriately paper your contractual provisions to ensure you are compliant, and have certainty that the provider will engage in annual testing exercises that you are required to do.

Beyond clarifying these risks and testing the resilience of the technology you must have a plan for incidents affecting any type of provider. In this scenario, SaaS solutions are no longer viewed as just a convenient option, as any step to comply with DORA will depend on that provider's willingness to facilitate the needs of a regulated CASP and can become more complex where non-transparent third-party software is involved. This has led towards firms of a larger maturity favouring the advantages that come with on-premise solutions, CASPs will have all this information available at all times - eliminating vendor dependencies - and taking first-hand responsibility for controlling the risks and protecting the business' operational resilience in order to minimise the responsibility of the third-party provider. Ultimately what works will be unique to your business, your own risk appetite, and approach to security. Just be sure that you are entering into everything with eyes wide open, whether that is your MiCA application or reviewing a third-party provider.

About the Authors

The information in this document does not constitute legal advice.

Cordial Systems

Sebastian Higgs
Co-founder & COO

✉ seb@cordialsystems.com

🌐 www.cordialsystems.com

21 ANALYTICS

Hannah Zacharias
Marketing & Regulatory Engagement Lead

✉ hannah@21analytics.ch

🌐 www.21analytics.ch