



## Digital resilience

### From a banking regulation standpoint

**Regulatory trends impacting cybersecurity and deployment of new technologies for the banking industry**

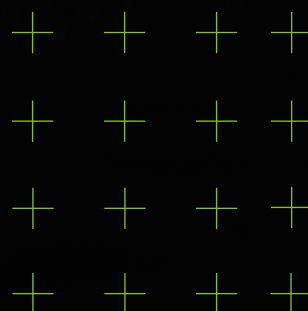
February 2023





Change is the law  
of life and those who  
look only to the past or  
present are certain to  
miss the future.

John F. Kennedy

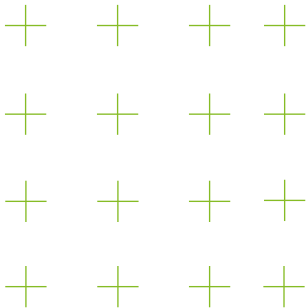






# Contents

A practical guide to digital banking regulations and their impacts on strategies, operations and risk profile	4
Our shortlist of digital banking regulations to watch	7
Digital resilience banking regulations	9
Next steps	26
Get in touch: key contacts	28







# A practical guide to digital banking regulations

and their impacts on strategies,  
operations and risk profile





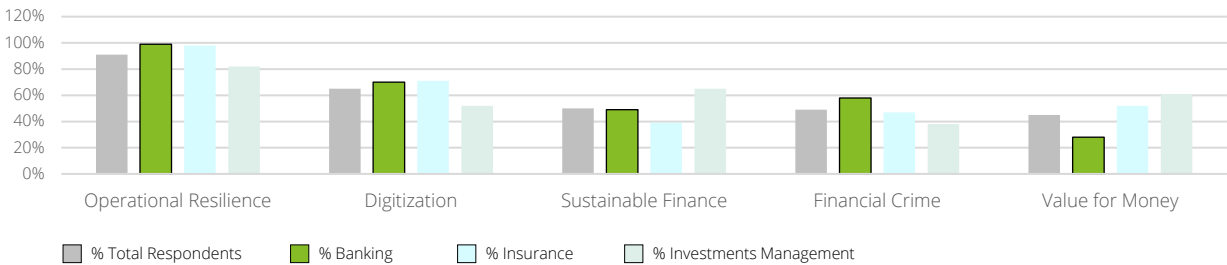
# A practical guide

## to digital banking regulations and their impacts on strategies operations and risk profile

Regulatory expectations and requirements for the banking sector are in constant motion. For years, Deloitte has closely monitored EU policymakers and supervisory bodies to connect the dots between various existing and forthcoming regulatory topics and understand their strategic implications on the banking industry.

This document aims to help banks assess the practical impacts of these regulatory trends on their business strategy, so they can efficiently adapt their organization and identify opportunities for growth. This edition focuses on the industry's digital and operational resilience, a top regulatory concern of senior banking executives, as highlighted in our last regulatory outlook survey (see Figure 1).<sup>1</sup>

**Figure 1:**  
**Which regulatory topic do you expect to require board/executive committee (ExCo) attention in 2022?** (ranked as a top-three priority)<sup>1</sup>



A cornerstone of the European Commission's strategy is to provide the conditions for a resilient and dynamic economic market that fosters innovation and growth. To achieve this objective, the European Commission has launched a series of regulatory initiatives:

- 1

Providing a framework for the use of new technologies and new financial products, such as digital assets

→ To limit the risk of new technologies and allow the traditional economy to explore their opportunities.
- 2

Defining minimum requirements for information and communication technology (ICT) risk management

→ To better monitor, detect and report ICT risks.
- 3

Setting standards for harmonized infrastructure and processes

→ To establish interoperable authentication rules and build a single market for relevant data access.

<sup>1</sup> Deloitte Centre for Regulatory Strategy EMEA, *New strategies for a changing world: financial markets regulatory outlook 2022*, p. 11. 93 senior executives and non-executives at financial services firms were asked to rank the top three regulatory topics that they expected to spend the most time on in 2022. Sustainable finance was the top priority (23% of respondents), narrowly followed by operational resilience and digitization (22% of respondents for both).

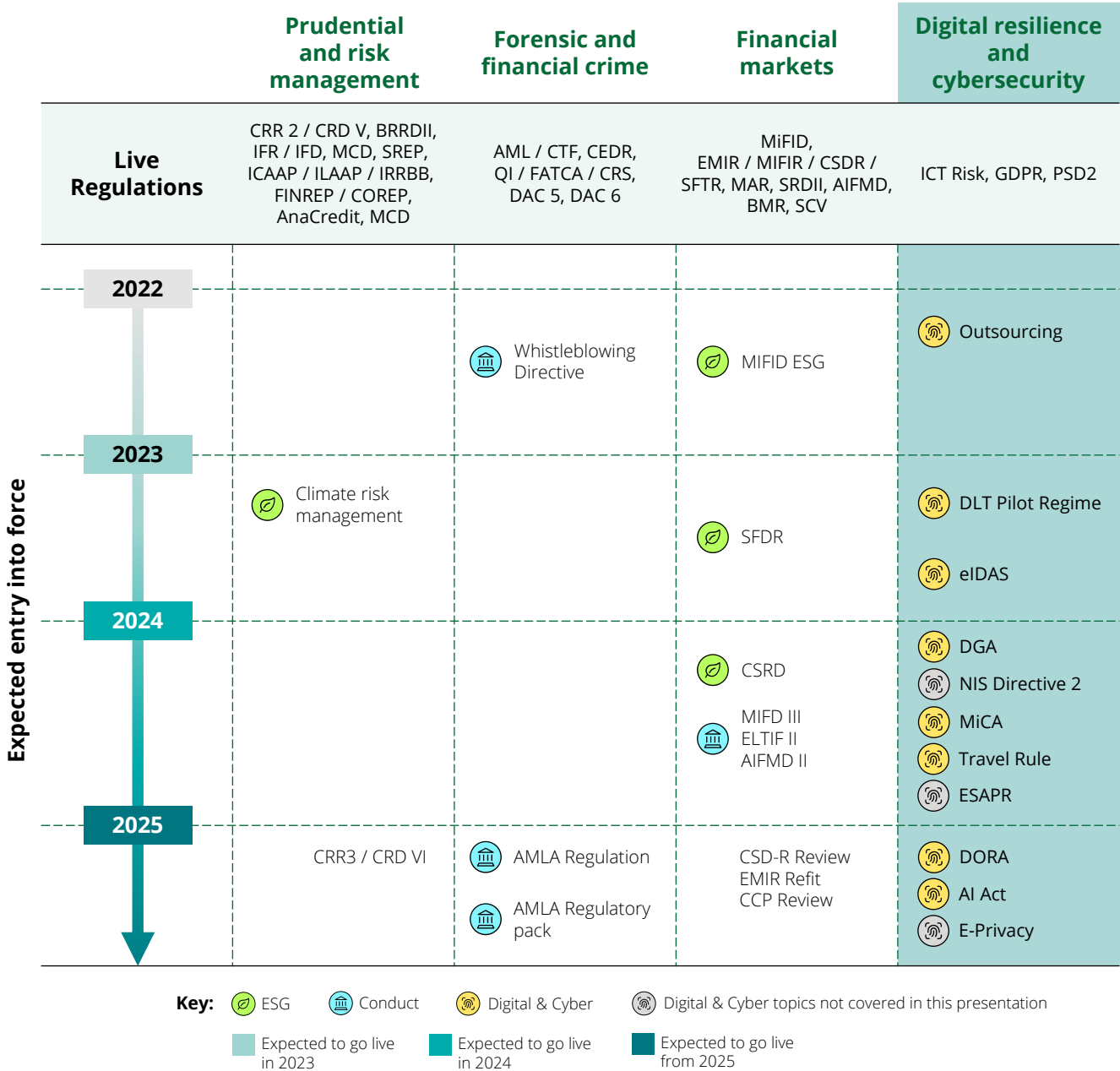


Figure 2 summarizes the key regulations and their projected timelines, divided into four overarching themes:

- environmental, social and governance (ESG) and sustainable regulations;
- anti-money laundering (AML) regulations;
- other financial regulations; and
- digital regulations, with the key milestones of the Distributed Ledger Technology (DLT) Pilot,

the Digital Operational Resilience Act (DORA), the Markets in Crypto-Assets (MiCA) Regulation , the data, Data Governance Act (DGA) and the Artificial Intelligence (AI) Act. The latter group— digital— is paving the way for a profound reshaping of the industry with the introduction of new communication techniques and products, but also new organization due to new products and services.

Figure 2:  
High-level timeline of the key regulations impacting the banking industry














# Our shortlist

## of digital banking regulations to watch

Regulation*	Expected entry into force	Brief description	Expected impact		
			Processes	Technology	People
Defining minimum requirements for ICT risk management	Outsourcing	Harmonize the supervisory requirements on outsourcing arrangements related to ICT previously disseminated in individual Commission de Surveillance du Secteur Financier (CSSF) circulars.			
	DORA	Develop a single regulatory and supervisory rulebook for ICT operational resilience in the financial sector, as well as mitigate risks of digital transformation.			
Providing a framework for the use of new technologies and new financial products such as digital assets	DLT Pilot Regime	Create a testing environment for the trade and settlement of DLT-based financial instruments.			
	MiCA	Create a regulatory framework for the crypto-asset market that supports innovation and harnesses the crypto space's potential, while also preserving financial stability and protecting investors.			
	TFR, the "travel rule"	Prevent the misuse of crypto assets to facilitate, fund and hide criminal activities and launder proceeds, by extending the traceability requirement to crypto-asset transfers.			
	AI Act	Create a common regulatory and legal framework for AI that is risk-based and encompasses all sectors and all types of AI.			
Setting standards for harmonized infrastructure and processes	eIDAS 2.0	Harmonize the digital identity capability for all EU citizens (EU Digital Identity Wallet) and put the end-user in control of all identifying information.			
	DGA	Create a single market for data that will ensure Europe's global competitiveness and data sovereignty.			

Key:  Low impact  Intermediate impact  Significant impact

\* The full name of each regulation is given in the next section.





**Digital resilience  
banking regulations**





# Outsourcing Circular

of digital banking regulations to watch

## Objectives and scope

The Outsourcing Circular aims to harmonize the supervisory requirements on outsourcing arrangements related to ICT previously disseminated in individual CSSF circulars.

- **Obligated entities:** credit institutions, payment institutions, central securities depositories, investment fund managers, undertakings for collective investments in transferable securities (UCITS), central counterparties, approved publication arrangements (APA), market operators, and administrators of critical benchmarks
- **Geographical reach:** authorized Luxembourgish financial institutions and new entrants

## Key requirements and impacts

The Outsourcing Circular lists the following implementation requirements for obliged entities:

- Set out the supervisory requirements on outsourcing arrangements (including sub-outsourcing);
- Organize the management body's responsibility and accountability;
- Design an outsourcing framework that includes:
  - Governance
  - Sub-outsourcing
  - Risk management
  - Oversight of outsourced function
  - Business continuity and exit strategy; and
- Notify the competent authority when outsourcing critical and important functions.

## In a nutshell



### 31 December 2022

Entities had until 31 December 2022 to review and amend their existing outsourcing arrangements.



### One single document

One single document for business process and ICT outsourcing (including cloud outsourcing).

## Related topics:

- European Banking Authority (EBA) Guidelines on outsourcing arrangements
- European Securities and Markets Authority (ESMA) and European Insurance and Occupational Pensions Authority (EIOPA) Guidelines on outsourcing to cloud service providers
- Delegated Regulation (EU) 231/2013 on safe-keeping duties of depositaries
- Solvency II



# Outsourcing Circular

of digital banking regulations to watch

## Key milestones

- February 2019**  
Publication of EBA Guidelines on outsourcing
- December 2020**  
Publication of ESMA cloud guidelines
- March 2022**  
Publication of CSSF Circular on Outsourcing Arrangements
- 30 June 2022**  
Application to new outsourcing arrangements
- 31 December 2022**  
Documentation of all existing outsourcing arrangements to be completed by the first renewal date of each existing outsourcing arrangement

## Risks and opportunities

Obligated entities that fail to systematically review the categorization of their existing and planned outsourced activities may not apply the proper scrutiny over their outsourcing relationships or meet their declaration requirements.

On the other hand, if the obligations of the new category of outsourced activity are reduced compared to the previous category, entities may be able to reduce their oversight of the outsourced activity.

These new outsourcing requirements are likely to impact the following key areas and business functions:

- Accounting
- Reporting
- Compliance, legal and tax
- Front, middle and back office
- IT
- Risk management
- Internal audit

## Deloitte experience and service offer

- Outsourcing framework gap analysis, design and implementation assistance
- Business process outsourcing (BPO), ICT and cloud outsourcing regulatory notifications
- Governance and outsourcing on-site inspection assistance
- Outsourcing governance internal audit outsourcing and co-sourcing



# Digital Operational Resilience Act (DORA)

Regulation (EU) 2022/2554 on digital operational resilience for the financial sector

### Objectives and scope


DORA aims to develop a single regulatory and supervisory rulebook for ICT operational resilience, whereby all firms must ensure they can withstand, respond to and recover from all types of ICT-related disruptions and threats, including cyber incidents.

- **Obligated entities:** all EU financial actors, from credit institutions to alternative investment fund managers (AIFMs), payment institutions and insurance companies, and also includes critical ICT third-party providers
- **Geographical reach:** authorized EU financial institutions and third-country ICT firms operating in the EU

## Key requirements and impacts

- DORA sets the minimum standards to operate digital and ICT infrastructures in a safe environment, such as:
- ICT risk management requirements (including a digital operational resilience strategy) with a broader focus across critical business functions;
  - ICT incident reporting rules that consolidate existing requirements while making significant enhancements;
  - Digital operational resilience testing requirements that introduce challenging new obligations, including “advanced” threat-led penetration testing (TLPT); and
  - ICT third-party risk management requirements, which harmonize the minimum contractual elements of relationships with ICT third parties and creates a direct oversight framework of third-party providers.

### In a nutshell



**The top three root causes of major technology outages** are change management, third-party failure and software/application issues, while cyberattacks are in fourth place.

**Known root cause of major technology outages and cyber-attacks** reported to the FCA (Financial Conduct Authority) between Oct. 2017 and Sept. 2018:

Change management	91
Third-party failure	70
Software/application issue	67
Cyber attack	60

Source: Financial Conduct Authority, “Cyber and technology resilience: themes from cross-sector survey 2018”

### Related topics:

- EBA Guidelines on ICT security and risk management(CSSF Circular 20/750)
- EBA Guidelines on outsourcing arrangements (CSSF Circular 22/806)
- EIOPA Guidelines on ICT security and governance & EIOPA Guidelines on outsourcing to cloud service providers
- Network and Information Systems ( NIS) Directive
- The Threat Intelligence-based Ethical Red Teaming ( TIBER-EU )framework, adopted by the Central Bank of Luxembourg as TIBER-LU
- ESMA Guidelines on outsourcing to cloud providers and on operational resilience assessment
- ESMA consultation of the first batch of DORA policy products (June 19, 2023)



# Digital Operational Resilience Act (DORA)

Regulation (EU) 2022/\*\*\* on the creation, maintenance and organisation of digital resilience

## Key milestones




## Risks and opportunities

As DORA moves towards finalization, firms should be mindful of the scale involved; the 2-year implementation period provides a short window of time to get things right. Firms can stay on the front foot by proactively assessing the requirements' impact to develop a realistic and achievable implementation plan. DORA will likely affect the following key areas and business functions:

- Management body
- IT and ICT
- Risk management (IT risk)
- Compliance and legal
- Internal audit
- Front, middle and back office

## Deloitte experience and service offer

- 
- Digital operational resilience and strategy definition, along with an ICT risk and resilience awareness and education program
  - Risk landscape awareness, from assessment to assistance in third-party risk management
  - Crisis prevention, issue management and contingency plan assistance through a risk-based approach
  - Crisis response and recovery enhancement and business continuity improvement
  - Digital operational resilience framework training
  - Security testing and assessment program, threat-led penetration testing and implementation of key risk indicators assistance





# DLT Pilot Regime

Regulation (EU) 2022/858 on a pilot regime for market infrastructures based on distributed ledger technology (DLT)

### Objectives and scope

The DLT Pilot Regime Regulation allows market operators to test and explore the use of such innovative technology for the trading and settlement of DLT-based financial instruments.

- **Entities in scope:** DLT market infrastructures (trading and settlement systems) and their operators
- **Geographical reach:** EU financial institutions and new entrants with specific permission to operate the DLT market infrastructure

## Key requirements and impacts

The regulation sets out the conditions for:

- Permission to operate a DLT market infrastructure;
- DLT financial instruments that can be traded and settled on the DLT; and
- Cooperation between the DLT market operators, competent authorities and ESMA.

By temporarily lifting certain requirements of existing regulatory frameworks, the regulation will allow DLT operators to deploy a multilateral trading facility (MTF) and/or a settlement system (SS) using this innovative technology for tokenized financial instruments. This DLT permission will come with an “EU passport” and be valid throughout the EU.

### In a nutshell

**Testing environment**

The regulation represents a “sandbox” approach—or a controlled environment—which allows temporary derogations from existing rules. The intention is to allow regulators and the market to test and learn more about how these rules work in practice.

**Supporting innovation**

With this regulation, the European Commission is prioritizing digital finance to boost Europe's competitiveness and innovation in the financial sector.

### Related topics:

- Crypto assets
- Blockchain
- Digital finance
- Tokenization of financial instruments
- Trade and post-trade environment







# DLT Pilot Regime

Regulation (EU) 2022/858 on a pilot regime for market infrastructures based on distributed ledger technology (DLT)

## Key milestones

**September 2020**  
DLT Pilot Regime proposal

**June 2022**  
Publication in the  
Official Journal (OJ)  
of the EU

**23 March 2023**  
DLT Pilot Regime started to  
apply throughout the EU

## Risks and opportunities

While DLT poses its own risks and challenges like any other advanced technology, it is one of the most promising new technologies to emerge in the last few years.

Therefore, forward-thinking banks should consider DLT and the tokenization of assets as core elements when modernizing their business activities and internal processes.

Banking actors can expect the following key areas and business functions to be impacted:

- Digital asset personnel in risk, compliance, treasury and regulatory affairs teams
- Front, middle and back office
- IT and reporting
- Risk management
- Internal audit

## Deloitte experience and service offer

- Digital asset strategy and business case creation
- Development of more efficient trading and settlement models through new technology
- Asset tokenization assistance
- Management and compliance team training
- Dedicated “Regulatory Watch” service to anticipate and evaluate the impact of this dynamic regulatory landscape





# Market in Crypto-Assets Regulation (MiCA)

Regulation (EU) 2023/1114 on Markets in Crypto-Assets

Objectives and scope

MiCA aims to create a pan-European market for crypto assets that do not qualify as financial instruments, such as stablecoins and utility tokens. As such, MiCA is heavily inspired by the Markets in Financial Instruments Directive (MiFID), effectively applying MiFID's prescribed principles and requirements to the crypto space.


- **Obligated entities:** issuers of crypto assets and crypto-asset service providers (CASPs)
- **Geographical reach:** all EU CASPs, and EU and non-EU crypto-asset issuers offering such assets in the EU

## Key requirements and impacts


Crypto-asset issuers will be required to produce and publish a whitepaper with all relevant information on the specific crypto asset. Members of the issuers' management body will have to meet probity standards, and misleading marketing communications will be prohibited.

CASPs (such as custodian wallet providers, crypto-asset trading platforms, and crypto-exchanges against fiat currencies or other crypto assets) will need to be EU-based and authorized to operate within the EU. They will be subject to prudential and organizational conditions, and rules on the safekeeping of clients' funds, mandatory complaint-handling procedures and conflicts of interest.

In a nutshell

**Stablecoins or ARTs**

MiCA imposes stricter rules regarding asset-referenced tokens (ARTs) due to these assets' increased risk, as users could widely adopt them as a means of payment.

**Non-fungible tokens (NFTs) escape MiCA**

Out of scope of MiCA are crypto assets that are unique, not fungible with other crypto assets, and whose value is attributable to each token's unique characteristics and the utility it gives to the token holder.

Related topics:

- Crypto assets
- Blockchain
- Digital finance
- Trade and post-trade environment





# Market in Crypto-Assets Regulation (MiCA)

Regulation (EU) 2022/\*\*\* on the creation, maintenance and organisation of digital resilience

## Key milestones



## Risks and opportunities

Banks should consider seizing the opportunities the crypto space offers and figuring out the type of role they would like to play in the ecosystem. In this context, MiCA is an important step forward as it significantly reduces regulatory uncertainty. Partnerships could be considered to widen banks' services while keeping a consistent risk approach. Running strategic opportunity assessments, building business cases, and nurturing selected relationships with potential providers could strengthen banks' digital service offering and provide a competitive advantage. MiCA will mostly affect the following key areas and business functions:

- Digital assets personnel in risk, compliance, treasury and regulatory affairs teams
- Front, middle and back office
- IT and reporting
- Risk management
- Internal audit

## Deloitte experience and service offer

- Business opportunity and impact assessment, and business case creation
- Crypto-asset strategy creation, helping institutions embed MiCA's key focus areas in their compliance plans
- Policies and procedures adaptation to MiCA standards
- Risk and compliance approach assistance to ensure they stand the test of time
- Management and compliance team training
- Dedicated "Regulatory Watch" service to anticipate and evaluate the impact of this dynamic regulatory landscape







# Transfer of Funds regulation and the “travel rule”

Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets (TFR)

### Objectives and scope

The Transfer of Funds Regulation (TFR) will introduce a traceability requirement for crypto-asset transfers to prevent the misuse of crypto assets to launder proceeds or facilitate, fund and hide criminal activities.

- **Obligated entities:** All “obliged entities” under the AML Directive
- **Geographical reach:** EU CASPs and intermediaries in the transfer chain

## Key requirements and impacts

When CASPs send or receive crypto-asset transfers on behalf of a customer, they will be required to obtain and submit information on the transaction’s originator and beneficiary (the so-called “travel rule”). This information will be required for all crypto-asset transfers, regardless of the transfer value.

The travel rule will also apply to transfers from or to “self-hosted wallets”, provided that a CASP or another obliged entity is involved, as well as to intermediary providers of crypto-asset transfers. However, TFR will not apply to consumer-to-consumer transfers of crypto assets; transfers where both the originator and beneficiary are CASPs acting on their own behalf; internet, cloud and software providers; and NFTs.

### In a nutshell

**Wide-spread impact for all banks**

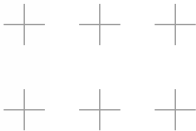
Intermediary providers of crypto-asset transfers will be in scope of the travel rule, notably by being obliged to record the relevant information received and ensuring no required information is missing.

**Data privacy compliance risks**

With each transfer, the confidentiality of the originator’s personal data should be protected, especially for transfers outside the EU.

### Related topics:

- Crypto assets
- Blockchain
- Digital finance
- Tokenization of financial instruments
- Trade and post-trade environment





# Transfer of Funds regulation and the “travel rule”

Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets (TFR)

## Key milestones

- July 2021**  
Proposal first introduced as part of the EU’s comprehensive AML package
- 9 June 2023**  
Publication in the Official Journal (OJ) of the EU
- 30 December 2024**  
TFR will apply at the same time as MiCA

## Risks and opportunities

The travel rule will pose a distinctive challenge for all involved in the crypto-transfer chain because blockchains are not necessarily designed to send personally identifiable information alongside transactions. Various interoperable communication systems are in development to transmit the relevant data to comply with the travel rule. The travel rule is expected to mostly affect the following key areas and business functions:

- AML compliance teams
- Front, middle and back office
- IT and reporting
- Risk management
- Internal audit

## Deloitte experience and service offer

- Digital asset strategy creation
- CASP screening, transaction monitoring and AML/KYC compliance
- Data privacy and GDPR impact assessment
- Management and compliance team training
- Dedicated “Regulatory Watch” service to anticipate and evaluate the impact of this dynamic regulatory landscape



# Artificial Intelligence (AI) Act

Proposal for the Regulation (EU) 2021/0106 Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts

Objectives and scope

The AI Act aims to foster collaboration and a **level playing field** between EU Member States and protect the fundamental rights of EU citizens in the age of AI. It establishes processes and roles to **enforce quality** at launch and throughout, while emphasizing the **ethical application of AI** to instill European values and improve transparency.

- **Obligated entities:** all providers introducing AI systems to the EU market and AI systems users
- **Geographical reach:** all AI systems in the EU market, even if their providers are from a non-EU country

## Key requirements and impacts

The AI Act defines four risk levels requiring different actions and considerations:


- **Unacceptable risk:** these AI systems are prohibited
- **High risk:** permitted but subject to compliance with AI requirements and ex-ante conformity assessments
- **Transparency risk:** permitted but subject to transparency obligations
- **Minimal or no risk:** permitted with no restrictions

The AI Act sets the following requirements for High-Risk AI systems (HRAIS):


- **HRAIS providers:**
  - Relevant, representative, error-free and complete input data;

- Appropriate data governance;
- Sufficient technical documentation;
- Sufficient understanding and control of the HRAIS;
- A continuous risk management process;
- Possibility for a human to safely and instantly interrupt the operation; and
- Robustness to failures, accurate results, and resilience to cyberattacks.
- **HRAIS users:**
  - Ensure data quality;
  - Monitor operation;
  - Generate logs; and
  - Generate the Data Protection Impact Assessment (DPIA).

In a nutshell

**Legislative framework for AI**

This proposal establishes a legislative framework for AI playing a leading role in Europe and globally. The AI Act's guidelines are ethical and do not inhibit innovation, providing opportunities for smaller players such as start-ups and small-and-medium-sized enterprises (SMEs).

**What does AI encompass?**

The AI Act defines AI as machine learning (ML) as well as statistical and knowledge-based approaches. The fact that the current text does not distinguish it from traditional mathematical models, such as the capacity to learn, is a highly debated topic in commentaries to the proposal. AI Act will be instrumental in the use of GPT tools across the EU both current, to be developed and embedded into current tools for all industries, financial and others.

**Related topics:**

- Data Act
- GDPR
- Data Governance Act
- European Interoperability Framework
- BCBS 239/Solvency II

20





# Artificial Intelligence (AI) Act

Proposal for the Regulation (EU) 2021/0106 Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts

## Key milestones



## Risks and opportunities

The AI Act will pose the following risks and opportunities:

- Infringements on prohibited practices can lead to a fine of up to €30 million or 6% of the entity's global annual turnover (e.g., social scoring by governments);
- Other forms of non-compliance may result in a fine of €20 million or 4% of the entity's global annual turnover (e.g., critical infrastructure safety systems); and
- All other violations were lowered to €10 million or 2% of global annual turnover (e.g., privacy).

The AI Act is expected to affect the following key areas and business functions:

- Risk Management
- IT
- Marketing
- Finance

## Deloitte experience and service offer

- AI and ML strategy definition
- AI implementation support
- Existing AI models assessment
- Algorithm assurance
- Data governance and data management maturity assessment
- Data quality framework definition
- AI risk management







# eIDAS 2.0: a digital identity revolution

Proposal for amendment of Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity

## Objectives and scope

The electronic identification, authentication and trust services (eIDAS) regulation aims to establish an interoperability framework for Member States' different authentication systems to promote the development of a digital trust market. It creates a harmonized digital identity capability for all EU citizens (the EU Digital Identity Wallet) and puts the end-user in control of all identifying information.

- **Obligated entities:** to be determined once the text is finalized
- **Geographical reach:** to be determined once the text is finalized

## Key requirements and impacts

All EU Member States will need to implement eIDAS 2.0, which will create a digital version (known as the European Digital Identity Wallet) of users' ID and other official documents that:

- **Is available to anyone who wants to use it:** any EU citizen, resident, and business in the EU who would like a European Digital ID can have one;
- **Is widely used:** the European Digital ID Wallets will be a common way to identify users and/or prove certain personal attributes to access public and private digital services across the EU; and
- **Allows users to keep control of their data:** the European Digital ID Wallets will allow people to choose which information they share with third parties, and to keep track of this sharing.

## In a nutshell



**Ursula von der Leyen,**  
**President of the European Commission,**  
**declared in her State of the Union**  
**address on 16 September 2020:**

*"Every time an app or website asks us to create a new digital identity or to easily log on via a big platform, we have no idea what happens to our data in reality. That is why the Commission will propose a secure European e-identity. One that we trust, and that any citizen can use anywhere in Europe to do anything from paying your taxes to renting a bicycle. A technology where we can control ourselves what data is used and how."*

## Related topics:

- Crypto assets
- Blockchain
- Digital finance
- Tokenization of financial instruments
- Trade and post-trade environment

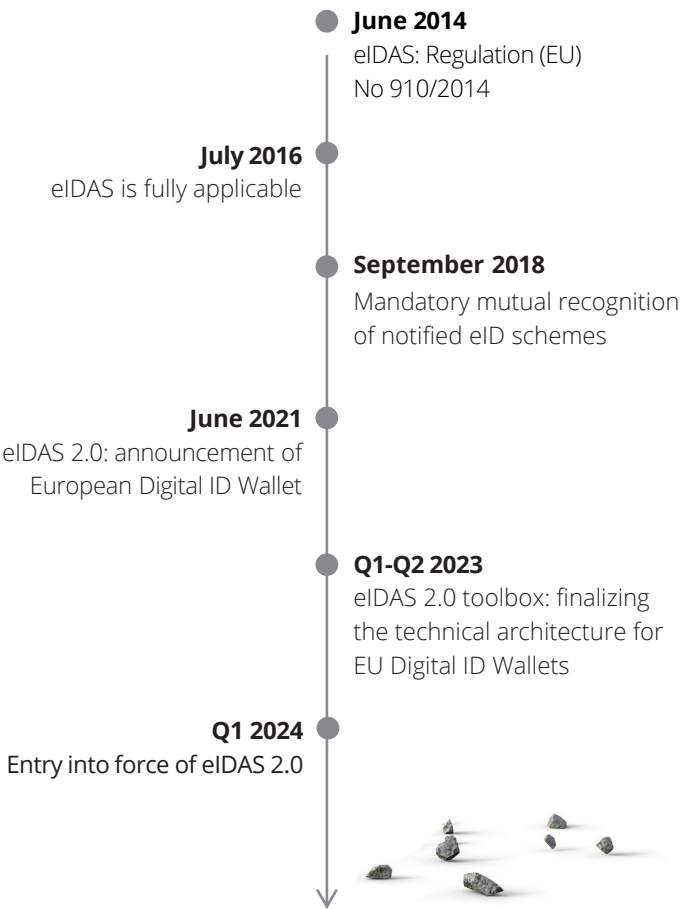




# eIDAS 2.0: a digital identity revolution

Proposal for amendment of Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity

## Key milestones



## Risks and opportunities

Using a European Digital ID Wallet could drastically reduce the paperwork needed to open a bank account or apply for a loan, while also making these processes safer, in a sense eIDAS will serve as a form of pan-European personal LEI (legal entity Identifier). Customers could select the necessary documents stored locally on their digital wallet when filling out a form, and the verifiable digital documents would be sent securely for the bank to check. The challenge for the banking industry will be to connect to the European Digital ID Wallet as swiftly, smoothly and securely as possible. Implementing eIDAS 2.0 processes will affect the following key areas and business functions:

- Front and back office
- IT
- Risk management
- Customer relationship management
- Compliance know-your-customer (KYC) teams
- Customer/account mobility

## Deloitte experience and service offer

- eIDAS 2.0 readiness assistance
- Digital transformation journey assistance
- EU Digital ID Wallet risk assessment
- GDPR compliance assessment







# Data Governance Act (DGA)

Regulation (EU) 2020/0340 on European data governance (Data Governance Act)

## Objectives and scope

The DGA provides a framework to enhance trust in voluntary data sharing for businesses and citizens. It aims to ease the sharing of and fair access to relevant data for businesses of all sizes, foster data-driven innovation initiatives, and ultimately strengthen Europe's global competitiveness.

- **Obligated entities:** public sector bodies, data altruism organizations and data intermediaries
- **Geographical reach:** EU organizations

## Key requirements and impacts

DGA sets out several requirements:

- **Re-use of public sector data:** make it easier for public bodies to exchange “protected” data (third-party intellectual property rights) with the private sector;
- **Data altruism:** allow data subjects/holders to give consent/permission for their personal/non-personal data to be shared for free for general interest purposes;
- **Data intermediation service:** setup of data intermediary services to handle the sharing of data by individuals, public bodies and private companies; and
- **European Data Innovation Board:** responsible for overseeing data intermediaries and providing advice on best practices for data sharing.

## In a nutshell



### Europe’s digital sovereignty by 2030

DGA, together with the Data Act and Digital Services Act, is part of the European data strategy and complements the European strategy on artificial intelligence. This strategy aims to develop a single market for data by supporting the responsible access, sharing and re-use of data while respecting the EU's values, especially regarding protecting personal data.



### The European Data Protection Board

To support the implementation of the data governance framework and the standardization of best practices, the European Data Innovation Board will be established as an expert group.

## Related topics:

- AI Act
- European AI strategy
- Data Act
- GDPR
- European Interoperability Framework
- BCBS 239/Solvency II





# Data Governance Act (DGA)

Regulation (EU) 2020/0340 on European data governance (Data Governance Act)

## Key milestones

- **February 2020**  
European data strategy is published
- **3 June 2022**  
Publication in the OJ
- **24 September 2023**  
Application of DGA

## Risks and opportunities

Entities that implement DGA must make sure they still comply with the GDPR. Reusing sensitive data requires a robust and flexible framework that appropriately monitors the data platform and “removes” data that may no longer have the user’s consent.

Entities may be able to leverage data altruism to gain a competitive advantage, by exploiting the new or increased data that is made available.

The effect of DGA might be felt more by Companies outside of the financial universe that will have the opportunity to monetize certain information through a regulated framework and generate new revenues. DGA will affect the following key areas and business functions:

- Management body
- IT
- Marketing, finance and risk management
- Internal audit
- Compliance and legal

## Deloitte experience and service offer

- Data strategy definition
- Data valorization and monetization
- Data governance and data management maturity assessment
- Data quality framework definition





**Next steps**



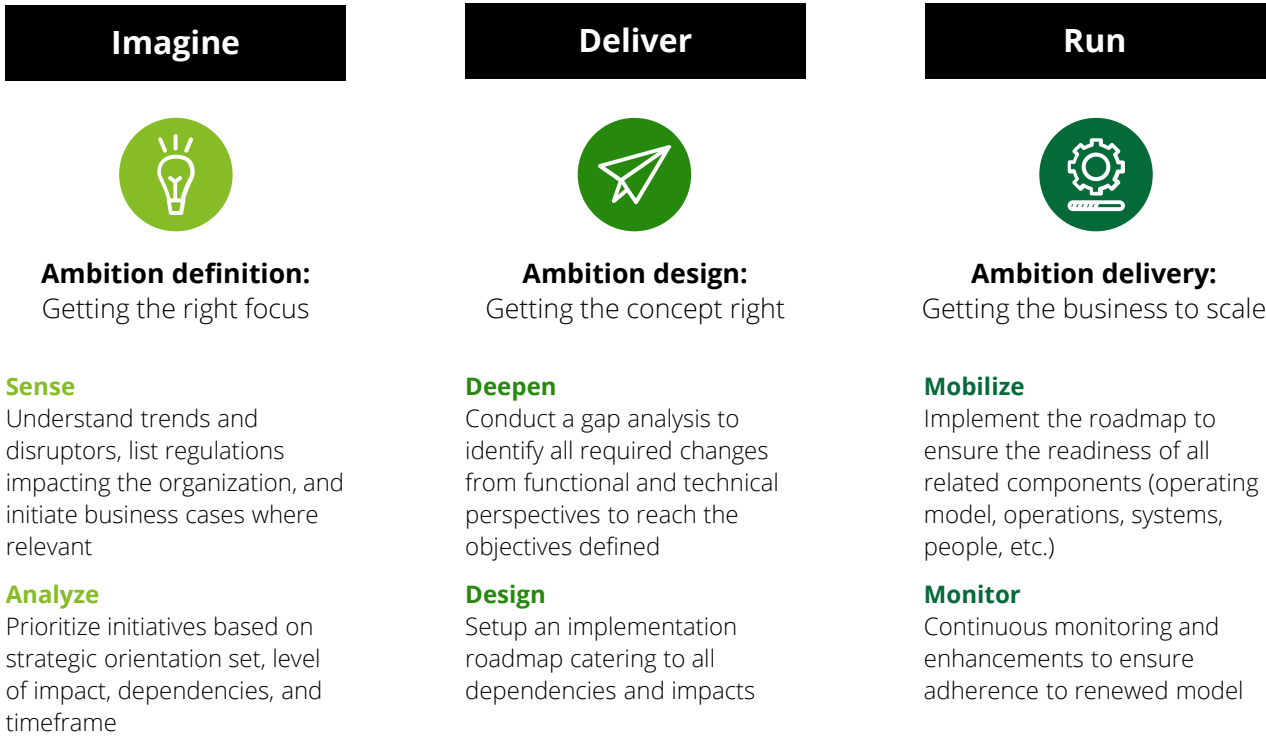
# Next steps...

The regulatory timetable has slowed somewhat due to changes and delays. While this can bring business benefits in the short term, such as reduced compliance costs , it also denies firms the opportunity to broaden their products and services, especially regarding digital assets .

Financial services firms will need to closely monitor the shifting regulatory timelines from both a business and operational perspective. More specifically , boards and senior management will need to incorporate these considerations into their forward planning.

Operationally, regulatory timetable changes complicate resource planning, especially across change implementation and IT teams, bringing the associated risk of bottlenecks or, less likely, teams having to be stood down.

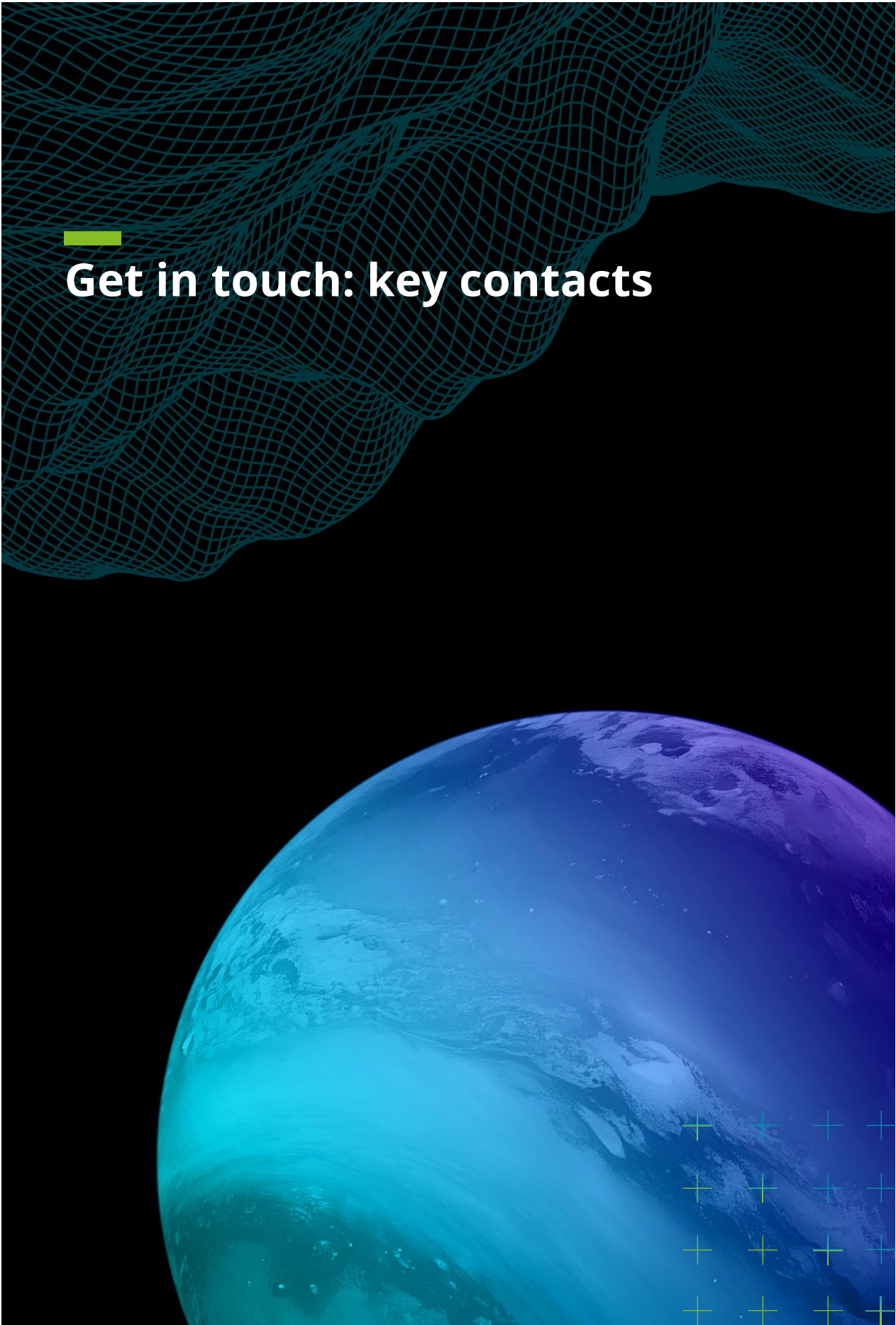
# ... start now







# Get in touch: key contacts



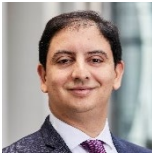


# Get in touch: key contacts

## Your Banking contacts



**Pascal Martino**  
Partner, Consulting  
Core Business Operations  
  
+352 621 246 523  
[pmartino@deloitte.lu](mailto:pmartino@deloitte.lu)



**Adil Sebbar**  
Managing Director, Audit  
Assurance  
  
+352 621 370 716  
[asebbar@deloitte.lu](mailto:asebbar@deloitte.lu)



**Astrid Brandy**  
Senior Manager, Consulting  
Core Business Operations  
  
+352 621 652 514  
[abrandy@deloitte.lu](mailto:abrandy@deloitte.lu)

## Your Regulatory Watch contacts



**Arnaud Duchesne**  
Managing Director, Risk Adv.  
Regulatory & Legal Support  
  
+352 661 451 443  
[aduchesne@deloitte.lu](mailto:aduchesne@deloitte.lu)

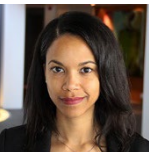


**Benoit Sauvage**  
Director, Risk Advisory  
Regulatory & Legal Support  
  
+352 621 652 496  
[bsauvage@deloitte.lu](mailto:bsauvage@deloitte.lu)

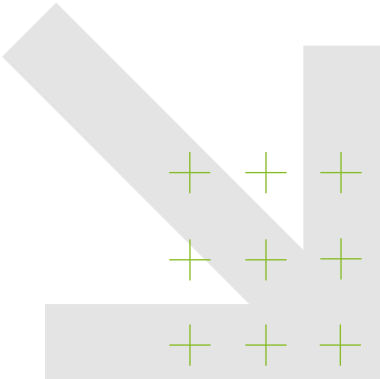


**Marijana Vuksic**  
Senior Manager, Risk Advisory  
Regulatory & Legal Support  
  
+352 621 412 051  
[mvuksic@deloitte.lu](mailto:mvuksic@deloitte.lu)

## Your Client & Industry contacts



**Charlene Massolin**  
Assistant Manager, Consulting  
Core Business Operations  
  
+352 621 960 220  
[cmassolin@deloitte.lu](mailto:cmassolin@deloitte.lu)





Outsourcing

DORA

DLT

MiCA

Travel rule

AI

eIDAS

DGA



## Our experts



### Roland Bastin

Partner, Risk Advisory  
Accounting & Int. Controls

+352 621 364 630  
[rbastin@deloitte.lu](mailto:rbastin@deloitte.lu)

Roland is responsible for Deloitte Luxembourg's Information & Technology Risk Services, and has led its IT audit and IT security services since 2001. He specializes in IT audit and information security for the banking and investment fund sectors.

DORA

eIDAS

OUTSOURCING



### Thibault Chollet

Partner, Consulting  
Core Business Operations

+352 621 173 293  
[tchollet@deloitte.lu](mailto:tchollet@deloitte.lu)

Thibault's main areas of expertise are designing IT strategies, roadmaps, enterprise architecture and operating models, and managing corporate-wide transformation projects. Before joining Deloitte, he acquired strong technical skills in the development of financial software.

MiCA/DLT



### Laurent Collet

Partner, Consulting  
Core Business Operations

+352 661 451 411  
[lcollet@deloitte.lu](mailto:lcollet@deloitte.lu)

Laurent specializes in securities, asset management and capital markets. He has professional experience in business development, communication and organization management. Prior to joining Deloitte in 2011, he held positions in a major bank and consulting firm.

MiCA/DLT



### Nicolas Griedlich

Partner, Consulting  
Analytics and Cognitive

+352 661 451 343  
[ngriedlich@deloitte.lu](mailto:ngriedlich@deloitte.lu)

Nicolas is mainly involved in Information Management & Analytics projects. He has expertise in business intelligence, data governance and the financial services industry (FSI). He is driven to enhance the value of data while aligning its management with applicable regulation and data standards.

AIA

DGA



### Irina Hedeia

Partner, Risk Advisory  
Cyber & Strategic Risk

+352 621 243 652  
[ihedeia@deloitte.lu](mailto:ihedeia@deloitte.lu)

Irina has worked at Deloitte for 15 years. She is mainly involved in IT risk, information security, IT regulatory, digital trust and risk, eIDAS, data protection and GDPR, DORA, business continuity management and project management projects.

DORA

eIDAS

OUTSOURCING



### Stéphane Hurtaud

Partner, Risk Advisory  
Cyber & Strategic Risk

+352 621 211 308  
[shurtaud@deloitte.lu](mailto:shurtaud@deloitte.lu)

Stéphane has 21 years of experience in the IT risk, cybersecurity, IT audit and IT governance fields (with a strong focus on the FSI). He started his career at Deloitte before moving to Dexia Group and BIL, where he endorsed key functions. In 2013, he returned to Deloitte.

DORA



### Maryam Khabirpour

Partner, Audit  
Analytics & Cognitive

+352 621 568 390  
[mkhabirpour@deloitte.lu](mailto:mkhabirpour@deloitte.lu)

Maryam has more than 14 years of experience in audit and is seasoned in leading and coordinating audits of large banking clients of international groups. Her expertise includes audits of public interest entities, internal control and regulatory compliance.

AIA

DGA



### Jean-Pierre Maissin

Partner, Consulting  
Core Business Operations

+352 621 273 652  
[jpmaissin@deloitte.lu](mailto:jpmaissin@deloitte.lu)

Jean-Pierre has strong expertise in IT with a particular focus on insurance, banking and the public sector. He has delivered multiple business intelligence (BI) centers of competence, IT strategy and regulatory projects. He has also been involved in multiple BI architecture initiatives.

DGA



### Jean-Philippe Peters

Partner, Risk Advisory  
Reg. & Legal Support

+352 621 251 230  
[jppeters@deloitte.lu](mailto:jppeters@deloitte.lu)

Jean-Philippe leads the Risk Advisory practice and has expertise in various risk and capital management aspects of financial institutions, with a focus on prudential regulatory frameworks. He has been involved in numerous risk and regulatory projects in Luxembourg and abroad.

eIDAS



Outsourcing

DORA

DLT

MiCA

Travel rule

AI

eIDAS

DGA



## Our experts



### Bettina Werner

Partner, Audit Assurance

+352 621 587 366  
[bewerner@deloitte.lu](mailto:bewerner@deloitte.lu)

Bettina has 16 years of experience managing external audit and assurance engagement at Deloitte. She provides assurance on the design and effectiveness of financial reporting controls and manages the go-to market of innovative and tailored assurance services.

AIA DGA



### Georges Wantz

Managing Director, Cons. Core Business Operations

+352 621 652 164  
[gwantz@deloitte.lu](mailto:gwantz@deloitte.lu)

Georges is in charge of the public sector advisory team. He has over 20 years' experience in the finance industry covering fund services and custodian, retail and private banking activities, as well as project management and software development.

AIA DGA



### Yasser Aboukir

Director, Risk Advisory Cyber & Strategic Risk

+352 621 568 392  
[yaboukir@deloitte.lu](mailto:yaboukir@deloitte.lu)

Yasser is a member of Deloitte Luxembourg's Risk Advisory service line, where he focuses on information and technology risk. Specifically, he is the Team Leader of the Threat and Vulnerability Practice and has managed several security assessments.

DORA



### Benoit Sauvage

Director, Risk Advisory Regulatory & Legal Support

+352 621 652 496  
[bsauvage@deloitte.lu](mailto:bsauvage@deloitte.lu)

Benoit is a member of Deloitte's RegWatch Team, developing regulatory watch services for financial institutions. He has a specific interest in digital finance regulations, such as AI, DLT and tokenization. He also has expertise in lobbying for financial firms.

MiCA/DLT



### Laureline Senequier

Director, Risk Advisory Accounting & Int. Controls

+352 661 451 843  
[lsenequier@deloitte.lu](mailto:lsenequier@deloitte.lu)

Laureline is part of the Risk Advisory practice, focusing on information and technology risk. She helps her clients navigate the risk and regulatory challenges of outsourcing, ICT risks, digital resilience and cloud computing, especially in the financial sector.

DORA OUTSOURCING



### Maxime Verac

Director, Risk Advisory Cyber & Strategic Risk

+352 661 451 546  
[mverac@deloitte.lu](mailto:mverac@deloitte.lu)

Maxime works in our Cyber Risk Services team, where he focuses on information and technology risk. He leads Deloitte Luxembourg's cybersecurity transformation offering and has extensive experience conducting cybersecurity transformation projects.

DORA



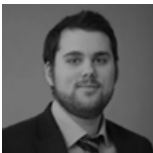
### Anke Joubert

Senior Manager, Consulting Analytics & Cognitive

+352 621 583 361  
[ajoubert@deloitte.lu](mailto:ajoubert@deloitte.lu)

Anke is part of the Artificial Intelligence & Data department and the Deloitte AI institute leadership team. She has published academic articles on big data in journals and written AI thought leadership articles for various Deloitte publications.

AIA DGA



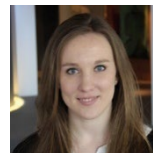
### Sébastien Müller-Borle

Senior Manager, Risk Adv. Cyber & Strategic Risk

+352 661 452 339  
[smullerborle@deloitte.lu](mailto:smullerborle@deloitte.lu)

Sébastien has over 9 years of experience in information and technology risk services. Specifically, he has been involved in security management, incident response and forensics, and information technology and security audits. He has followed the evolution of the eIDAS regulation closely.

eIDAS



### Giulia Pescatore

Senior Manager, Consulting Innovation

+352 621 568 587  
[gpescatore@deloitte.lu](mailto:gpescatore@deloitte.lu)

Giulia works in Deloitte's Advisory & Consulting department, where she has been involved in projects entailing the preparation of banking and payment license application files for various companies. She is now responsible for the development of FinTech-related projects.

MiCA/DLT



Our experts



**Aleksandra Suwala**

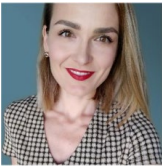
Senior Manager, Risk Advisory  
Cyber & Strategic Risk

+352 621 412 719  
[asuwala@deloitte.lu](mailto:asuwala@deloitte.lu)

Alexandra is a qualified attorney admitted to the Warsaw Bar Association and a Certified Information Privacy Professional/Europe (CIPP/E). Boasting extensive experience in the field of data protection, she advises Deloitte's clients in data protection and regulatory compliance.

DORA

OUTSOURCING



**Marijana Vuksic**

Senior Manager, Risk Advisory  
Regulatory & Legal Support

+352 621 412 051  
[mvuksic@deloitte.lu](mailto:mvuksic@deloitte.lu)

Marijana is a seasoned lawyer with 16 years of experience in financial services field. She helps forward-thinking financial firms to comply with respective regulatory obligations, so that their business models can overcome the legal hurdles required to fully tap the potential of new technologies.

MiCA/DLT

Travel Rule

AIA



**Alexandre Bodin**

Manager, Consulting  
Analytics and Cognitive

+352 621 661 246  
[abodin@deloitte.lu](mailto:abodin@deloitte.lu)

Alexandre has worked for more than 8 years in consulting and has experience in information and data management for the FSI. He has mainly been involved in multiple analytics and information projects for regulation and strategic purposes in Luxembourg, Europe and the Middle East.

eIDAS



**Selim Lachiheb**

Manager, Risk Advisory  
Cyber & Strategic Risk

+352 621 727 467  
[slachiheb@deloitte.lu](mailto:slachiheb@deloitte.lu)

Selim works in Deloitte's Risk Advisory practice and has strong experience in implementing and integrating digital trust solutions based on Public Key Infrastructures (PKI). His area of expertise includes cryptography, digital identity, mobile ID, digital signature and strong authentication.

eIDAS





Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see [www.deloitte.com/about](http://www.deloitte.com/about) to learn more.

Deloitte provides industry-leading audit and assurance, tax and legal, consulting, financial advisory, and risk advisory services to nearly 90% of the Fortune Global 500® and thousands of private companies. Our professionals deliver measurable and lasting results that help reinforce public trust in capital markets, enable clients to transform and thrive, and lead the way toward a stronger economy, a more equitable society and a sustainable world. Building on its 175-plus year history, Deloitte spans more than 150 countries and territories. Learn how Deloitte’s approximately 415,000 people worldwide make an impact that matters at [www.deloitte.com](http://www.deloitte.com).

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms or their related entities (collectively, the “Deloitte organization”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.