Deloitte.

Navigating NIS2 Compliance

January 2025 - A current view on local NIS2 legislations for organizations with cross-border European operations

Executive Summary

The Network and Information Security 2 (NIS 2) Directive establishes more rigorous cybersecurity requirements for organisations in EU Member States, with a transposition deadline of October 2024. This whitepaper provides an analysis as of January 2025 of the current regulatory landscape, touching upon key aspects such as sector definition, identification of entities, registration requirements, and security measures, as well as management accountability and government oversight.

Across the EU, Member States display varied transpositions of the NIS2 Directive, with the following notable highlights:

- **Belgium, Croatia, Hungary, Latvia, Lithuania, Greece and Italy have transposed NIS2.**
- Belgium has adhered to the Directive's scope classifications, but defines a **custom cyber security controls framework to which entities can certify next to ISO 27001.** Lithuania has defined a **custom control framework of 76 technical requirements**. Italy and Greece also mention a custom control set.
- Italy will require organizations to be compliant by **October 2026** (transition period) and requires the adoption of a **National Cyber Security Framework (based on NIST CSF)** which will define basic obligations and long-term obligations. Basic security measures of this framework are foreseen for April 2025, while long-term security measure will be published in april 2026. These measures will be based on the Italian National Cyber Security Framework.
- Croatia, as well as in the drafts of the Czech Republic and Poland, have expanded upon the Directive's sector scope, recognizing **additional critical entities and sectors**.
- Croatia has not setup a registration platform, but the relevant governing body will request information from entities for categorization. **Croatian entities will thus not have to register themselves** and the initiative will be with the Croatian government
- Some countries also define specific requirements on top of the NIS2 directive, such as Hungary, Latvia, Lithuania, and Belgium.

The Directive's emphasis on management accountability is clear, with executive boards and managing directors mandated to ensure compliance with risk management measures. While Italy and Poland provide detailed definitions and responsibilities for management bodies, Belgium, Croatia, Hungary, and Greece amongst others do not elaborate further.

Government oversight and audit mechanisms vary, with a frequent audit for essential entities in Belgium, Greece, Croatia and Poland. Lithuania on the other hand has no periodic audits.

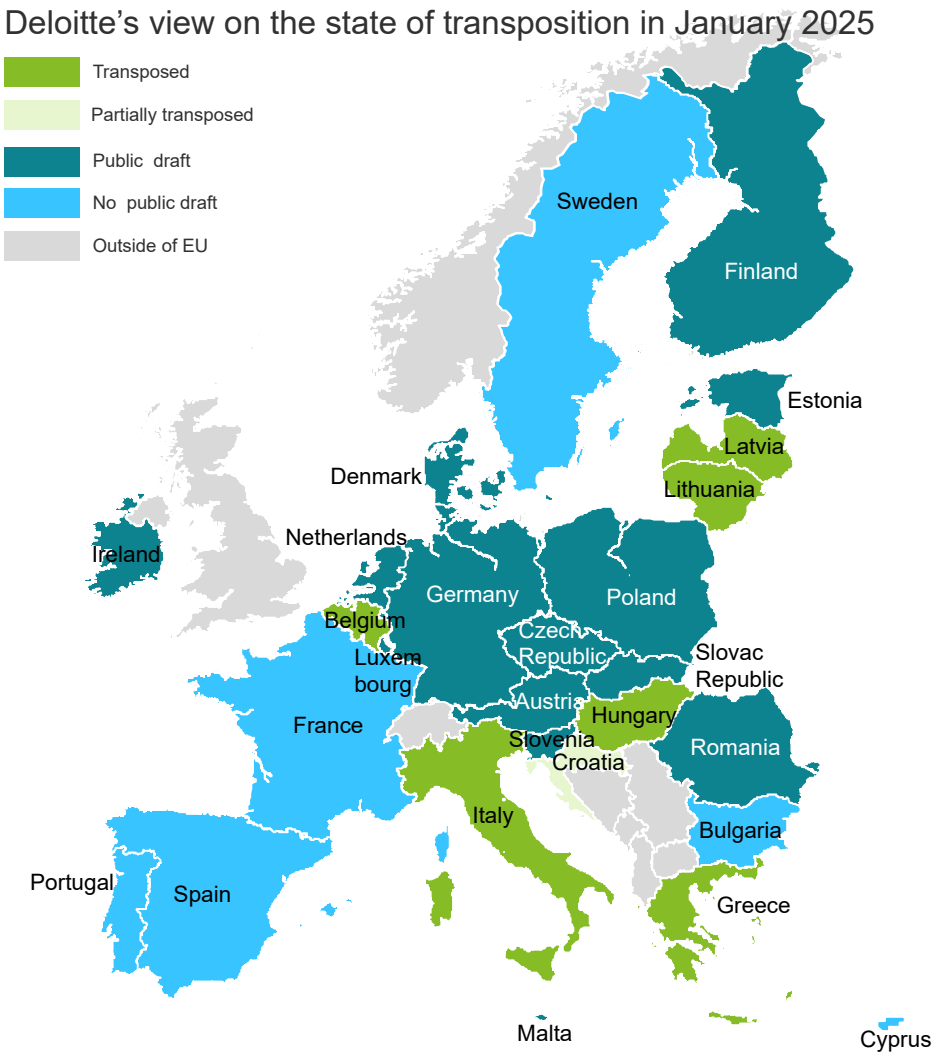
In essence, the transpositions studied showcase important specifics which can have significant impact for organisations operating in these countries. For these organisations, it means **closely following up on the transpositions now that the transposition deadline has passed and trying to define a common ground to reach a workable level of compliance**. Most of the NIS2 laws are expected in 2025. Having a strategic cybersecurity control framework to navigate this evolving regulatory landscape will be important moving forward.

Introduction

The adoption of the Network and Information Security 2 (NIS 2) Directive by EU Member States, marks an important milestone in the European Union's cybersecurity landscape. Building upon its predecessor, **NIS2 introduces stricter requirements and broadens its reach.** This legislative move aims mainly to strengthen national and cross-border cybersecurity resilience.

In this whitepaper, we will cover the EU NIS2 regulatory landscape as of January 2025, providing a comprehensive overview of its current state. Please note that the NIS2 landscape is rapidly evolving. This whitepaper reflects the current state of knowledge and regulations as of its publication date. Readers are encouraged to stay informed about new developments and evolving laws in this area.

We already know that Member States have clearly outlined different requirements and timelines and with still so many unknowns, organizations may question whether it is even possible to start on a NIS2 implementation. However even with those differences and uncertainties, waiting would be the lesser option. **Even in countries the NIS2 Directive hasn't been transposed in, organisation can already start with common requirements** outlined by the directive and should not lose any time (after all, hackers are also not waiting), especially for legal entities in countries where the law is in place.



The different stages of NIS2 adoption and implementation across the EU

As we are past the transposition deadline of October 2024, the implementation of the NIS2 Directive is currently making its way across the European Union. With all Member States at varying stages of adoption and readiness, the new regulatory landscape can quickly become overwhelming, especially for organizations that operate cross-border. But what does this mean concretely?

As only a minority of countries have adopted a transposed NIS2 law in their country, **notable differences exist in adoption and readiness timelines**. As we look forward, countries have updated their timelines for the transposition with the majority aiming towards 2025 for the transposition. In the following part, we will examinate the current landscape more closely.

The following **final laws were analysed: Belgium, Croatia, Hungary, Latvia, Lithuania, Greece and Italy**. Hungary released a new version of its law on December 20th 2024. When additional **decrees** were issued, these were also analysed. For Belgium and Italy additional decrees are made. **Lithuania** has added an amendment.

The following **draft laws were analysed: Finland, Poland, Netherlands, Czech Republic, Germany, Slovak Republic, Estonia, Austria, Ireland and Luxembourg**.

For **France, Portugal, Spain, and Sweden** no draft law is available at moment. Meaningfull expectations are also taken up in the analysis. For the **United Kingdom**, security requirements similar to NIS2 will be included in the NCAS CAF with a law expected next year.

A comparison of the transposition of the NIS2 Directive will be made on the following aspects:

- Essential and important entities
- Sector definition
- Registration processes
- Security controls requirements
- Board level/management accountability
- Government oversight and audit

For other countries Deloitte has insights, but draft laws are not publicly available. In this whitepaper we limited ourselves mainly to public draft or final laws.

Essential and important entities

The NIS2 Directive has identified the sectors that are in scope, which has expanded significantly compared to its predecessor as is visualised below and now includes two classification levels, Essential and Important.

This classification determines the application of different requirements regarding supervision and sanctions. While some Member States align closely with the European Commission's enterprise size criteria for classifying essential and important entities, others take a more tailored approach.

NIS1 vs NIS2

Essential sectors

- Energy
- Transport (air, rail, water, road)
- Banking
- Financial market infrastructure
- Health
- Digital infrastructure
- Drinking water
- Waste water
- Public administrator
- Space
- ICT service management (B2B)

Important sectors

- Postal and courier services
- Waste management
- Food
- Chemicals (manufacturing, production, distribution)
- Manufacturing
- Digital providers
- Research

Sectors defined by NIS1

New sectors added by NIS2

For instance, the Polish (Draft) law also **elevates several sectors from 'important' to 'essential'**,. Concretely these are the production and distribution of chemicals, food, medical devices, and various manufacturing industries.

Most other countries such as Belgium (Final), Greece (Final), Lithuania (Final), Germany (Draft), Czech Republic (Draft), Croatia (Final), Luxembourg (Draft), Italy (Final) and Austria (Draft) have essentialy taken over the classification in essential and important entities as specified by the NIS2 directive.

Important to note is that for certain digital service providers (characterised by the cross-border nature of their services) such as managed (security) service providers, an exclusive jurisdiction is determined by the location of their so-called "main establishment" within the European Union. This means that these organisations will need to comply only to the NIS2 law applicable for this location.

Sector definition

When we look at how different countries are expanding the scope of sectors required by the NIS2 directive, we see a variety of approaches. At least Belgium, Lithuania, Luxembourg, Germany, Finland, Ireland, Greece and Austria have chosen to stay within the scope outlined by the Directive itself, without adding new sectors.

Croatia, Czech Republic, Poland, Czech Republic and Italy identify **additional sectors** that are classified as essential:

- Croatia's law includes entities crucial in the electronic invoicing space. As well as entities that play a pivotal role in managing, developing, or maintaining the information infrastructure of the government. Moreover, Croatia has recognized the education system as a critical sector, extending this to both private and public educational entities.
- The Latvian law has added education system maintainers as important entities
- Poland, in its draft law, has opted as well for an expansive adaptation by incorporating additional subsectors within the energy and transport sectors. This includes entities involved in the extraction of energy resources and managed cybersecurity service providers with clients in the energy sector. Service providers to airlines and other aircraft users are considered critical as well.
- The Czech Republic includes the Defense Sector to its list of essential sectors.
- Italy has defined that universities are also in scope as research organisations.

Sector-wise, an interesting overlap with NIS2 in the regulatory landscape is the Digital Operational Resilience Act (**DORA**). In several Member States, like Belgium (Final Law), Germany (Draft Law) and Finland (Draft Law), financial entities need to adhere only to DORA, which will supersede NIS2 compliance requirements in these countries. In other countries, like Croatia, the law does not reference to DORA, making both NIS2 and DORA applicable to organisations from the banking and financial market infrastructure sector. In Ireland, competent authorities have been designated to oversee implementation and enforcement in their respective sector. For the financial sector, tthe Central Bank of Ireland has been assigned.

Registration processes

When looking at registration requirements, we see the differences increasing. In the case of Croatia, there currently isn't a dedicated registration platform. Instead, the governing body tasked with implementing the law will actively reach out to entities in scope, requesting the necessary information for categorization and for maintaining an up-to-date list of entities. These entities must respond with the required information within a 45-day timeframe.

Looking at other countries, Belgium's law allows for a five-month period to register. The Italian law requires entities to register by February 28th 2025. Greek entitities have a two month registration window, so by January 27th 2025. For some entities (managed service providers), both Belgium and Italy have defined seperate deadlines, December 18th 2024 and January 17th 2025 respectively.For Hungary the deadline of October 31st 2024 already passed.

Most countries have or are creating an online portal by which countries can register themselves. Examples are Belgium, Luxembourg, Italy, Austria, Hungary, Slovak Republic, Lithuania and the Czech Republic. They require entities to submit information, but the specific details are not always known yet. In most cases

contact details need to be shared, and in Belgium and Lithuanian's case even IP addresses. The Czech Republic and Lithuania expands the scope of the portal not only registration functionalities but also real-time threat intelligence sharing and other NIS2-relevant services.

Finland, the Netherlands and Germany through their draft legislation, also mandate registration, but the specifics are not yet available.

Latvia on the other hand requires registration by April 1st 2025, but this needs to be done through e-mail.

While registration platforms and timelines are being defined in some Member States, **there is less uniformity regarding FAQs or guidance on NIS2 implementation**.

- **Hungary:** Engaged in extensive outreach through public consultations and media to disseminate information;
- **Finland:** Provided draft recommendations for local authorities;
- **Czech Republic:** The Czech cyber authority operates a website entirely dedicated to NIS2 implementation;
- **Germany:** Designated the BSI[1] as the central reporting office without stipulating a registration timeline;
- **Poland:** Acknowledges the need for registration in its draft law, but also has yet to detail the timeline;
- **Belgium:** Engaged through public consultations and public-private working groups and conferences. On the website of the CCB[2] template security policies are shared, as well as tools to facilitate risk assessments per sector and current state assessments of the security controls. The registration timeline is 5 months as of October 18th; and
- The **Italian** law requires entities to register within February 28th 2025. For some entities (e.g. managed service providers) the deadline is January 17th 2025.

Timelines

In order to give entities in scope time to adhere to the stricter requirements, countries define timelines by which the entities need to be compliant:

- Greece mentions February 27th 2025 (3 months) to approve the cyber risk measure to be taken by management and start monitoring their implementation;
- Italy will require organizations to be compliant by October 2026 (transition period);
- Hungary requires organisations to conduct their cybersecurity due diligence by December 31st 2025;
- Belgium requires entities to get compliant by 18 april 2027. For essential entities this means certification against the Belgian control framework (cyberfundamentals) or ISO 27001.

Cyber Security requirements

When looking to the approach to defining and implementing security measures, different approaches are becoming clear. Some countries like Finland (Draft), Czech Republic and Germany (Draft) however still need to further clarify the specific security requirements.

When evaluating what is currently known for the other countries, some initial conclusions can be drawn:

- The CCB in Belgium, has made the security controls requirements specific and has established their **Cyberfundamentals Framework**, mainly based on the **NIST Cybersecurity Framework**, providing a structured baseline of controls for organizations to follow. Belgium also expands the 10 cybersecurity risk-management measures from article 21 with a new one, namely a coordinated vulnerability disclosure policy.
- Similarly Italy leverages their **National Cyber security Framework from 2016** based on NIST CSF which is regularly updated.
- Hungary references a detailed framework and list of controls based on **NIST 800-53**. Hungary in its updated law also requires the payment of an annual cybersecurity monitoring fee. Exact fees still need to be determined.
- Latvia references a framework to be developed by the government. The law also requires a cyber risk management and information and communication technology business continuity plan, as well as the mandatory installation of cybersecurity early warning sensors in the IT infrastructure.
- Greece mentions a **unified cybersecurity policy** for which a template will be provided. This policy will need to be approved by the government and

1 Bundesamt für Sicherheit in der Informationstechnik
2 Centre for Cyber Security Belgium

shared afterwards on a yearly basis. Next to this this, Greece will also develop a national framework of cybersecurity requirements with technical, operational and organizational measures.

- Poland (Draft) has chosen to align with recognized international standards, such as **ISO/IEC 27001 and ISO/IEC 22301**, as benchmarks for compliance.
- Ireland's National Cyber Security Centre (NSSC) aims to leverage NIST CSF 2.0 and is also looking at ISO 27001 certification.
- Lithuania expanded on the aspects required by the directive with a mandatory policy for granting and managing access rights of users, administrators, suppliers and their subcontractors. Each of the aspects required by the directive has been further worked out in 76 technical requirements applicable to essential or important entitiies
- Croatia (Final Law), Netherlands (draft) and Luxembourg (draft) do not further define specific security controls requirements.

Appointment of specific formal roles

Next to requiring specific cybersecurity controls, a number of countries want the formal appointment of roles within entities in scope:

- Hungary requires the appointment of a security officer
- Latvia requires the formal appointment of a cyber security manager.
- The Lithuanian law also mandates the appointment of a cyber security manager and a cyber security officer who have at least two years of experience and have never been convicted for data-related penalties.
- Greece requires the appointment of an Information and Communication Systems Security Officer (ICSSO)

Board level/ management accountability

NIS2 explicitly mandates bodies of essential and important entities to supervise and ensure compliance with risk management measures. This is complemented by a requirement for targeted cybersecurity training for these management bodies, emphasizing the importance of informed leadership in mitigating cyber risks.

However the concept of management bodies as specified in the NIS2 Directive is not well defined. Poland's draft law provides a comprehensive definition of a Management Body, inclusive of a broad spectrum of leadership roles, and stipulates explicit responsibilities for cyber security oversight, though without additional sanctions beyond those in the directive.

The draft in the Netherlands explicitely names the board of directors as a management body requiring cyber security training. Belgium's and Croatia's final NIS2 laws on the one hand, and Hungary's and Germany's draft, on the other hand, are less prescriptive and do not provide a further clarification of management bodies.

Government oversight and audit

Lastly, Member States are tailoring their oversight and audit mechanisms to align with the NIS2 Directive.

In the German draft a **3-yearly verification process** for operators of critical systems is defined, with random checks for essential entities and occasional audits for important entities. Poland and Croatia simplify the audit frequency to at least once every two years for all entities under its jurisdiction.

Belgium has opted for a **3-yearly cerfication with yearly surveillance audits** for essential entities. Important entities can voluntarely choose for a verified self-assessment. Ireland is simarly looking at a **voluntary certification scheme** to showcase compliance. The Slovac Republic opts in its current draft for a 2-yearly audit cycle for essential entities.

Italy as well has mandatory audits for essential entities and ad-hoc audits post-incident or in case of non-compliance concerns. The same is currently defined in the Dutch draft law. Greece also mentions regular audits for essential entities, but the frequency has not been further defined.

Lithuania foresees **only inspections in case of suspition of violation** of the law.

Luxembourg and Finland have yet to define the precise audit frequency but have established the principle of periodic and risk-based audits. Finnish competent authorities retain the right to conduct audits, utilizing parties with the requisite expertise.

In summary: NIS2 transposition requirements and timelines require attention moving forward

The analysis of the transposed draft and final laws of the NIS2 Directive across the EU shows a **complex set of nuances to the original Directive**. Now that the deadline of October 17th has passed, timelines are less clear for the majority of EU countries that have not yet transposed the directive. The expectation there is that the majority of NIS2 laws will only be available somewhere in 2025.

As most organisations have already started working on compliance towards NIS2, this fragmented landscape will pose challenges. This is especially the case for multinationals with activities in countries for which there is a NIS2 law in certain countries and not in other countries. Given that the specific requirements are unclear, organisations will adapt their cyber roadmaps to reflect this need for compliance.

For those who assumed that by the transposition deadline, the impact would be clear, we will have to remain patient. It is important however for organizations to remain vigilant and aware of changes to critical sectors, specifics on management responsibilities, registration protocols and timelines, as well as audit frequencies as they arise. Organisations should take ownership of their cyber strategy and make informed decisions on the way forward.

Collaboration and knowledge exchange will be key to navigating this dynamic environment.

With so many unknowns, is it even possible to start on the implementation of NIS2?

NIS2 compliance, especially for organizations with cross-border operations, might seem very overwhelming at first. For countries with a final law, the requirements are tangible, but for other countries the unknowns remain. That's why focusing on the key areas as outlined in the NIS2 Directive is essential to start preparing on:

- Risk management (a risk-based approach to cybersecurity);
- Management/ board level accountability and specific training and awareness plans;
- Supply chain and third party risk management;
- Incident reporting obligations to (national) authorities;
- Business continuity and the ability to recover from cyber attacks.

These aspects should form the basis of the cyber roadmap both on the short term and long term.

The value of public-private partnerships and cross-organization information sharing cannot be overstated. Alliances should help to facilitate the exchange of threat intelligence and collaborative response strategies, significantly enhancing an organization's capacity to identify and respond to specific sectoral cyber threats. The adaptability of an organization's cybersecurity control framework is equally crucial, allowing for the incorporation of new control requirements as legislation gets more clear.

If you have **already implemented ISO 27001** and have a well-functioning ISMS, you are significantly closer to achieving NIS2 compliance. However an analysis should be well made towards the Directive and transpositions when they are available. Large organizations may opt for a centralized approach, or leave the implementation up to local subsidiaries, while maintaining strong reporting lines and situational awareness.

As organizations work towards NIS2 compliance, it is essential to view the directive not as a regulatory hurdle but as an opportunity to elevate their organization's cybersecurity maturity. The distinction between a compliance-driven and a security-driven approach will be a clear indicator of an organization's cybersecurity maturity. By implementing a structured, informed, and collaborative approach to cybersecurity, leaders will not only ensure compliance with the NIS2 Directive but will also contribute to a more secure and resilient digital infrastructure within the EU, which is of course the ultimate goal of the Directive.

In the coming months, **Deloitte will keep following up** on the transposition of the NIS2 directive in order to provide further guidance. Reach out in case you want to get further updates.

Overview of legislation per EU country

Country	Status NIS2 law	Link to local NIS2 legislation	Link to local NIS2 underlaying regulation / recommendation or control list	Link to registration website
Austria	Draft	Link	Not yet available	For now, there is no registration website.
Belgium	Final	Moniteur belge (fgov.be)	Link	Register my organisation | CCB Safeonweb
Bulgaria	Not transposed	Not yet available	Not yet available.	Not yet available.
Cyprus	Not transposed	Not yet available	Not yet available.	Not yet available.
Croatia	Final	Link	Not applicable	Not applicable.
Czech Republic	Draft	Sněmovní tisk 759/0 (psp.cz)	Sněmovní tisk 759/0 (psp.cz)	Portál NÚKIB (gov.cz)
Denmark	Draft	Høringsdetaljer - Høringsportalen (hoeringsportalen.dk)	For energy sector: Link For financial sector: Link	The link has not yet been determined, but it is anticipated that registration will be conducted through this government portal: https://businessindenmark.virk.dk/
Estonia	Draft	Link	Not yet available	Not yet available
Finland	Draft	He 57/2024 vp (eduskunta.fi) Government working group: Link	Link	Not yet available
France	Not transposed	Not yet available (no offical document). Leaked document is available here: Link	Not yet available.	Link
Germany	Draft	BMI - Gesetzgebungsverfahren - Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheits managements in der Bundesverwaltung	The latest version of the NIS 2 Umsetzungsgesetz: Link This has not officially been published yet and is a draft. NIS 2 will effect critical operators (as in NIS1), essential and important entities. NIS 2 Umsetzungsgesetz will replace/add to IT Sicherheitsgesetz 2.0	Currently unknown On this page you can check if your company falles under NIS2 Directive. Link
Greece	Final	Link	Not yet available.	Not yet available.
Hungary	Final	Link	Link	Link
Ireland	Not transposed	Link	Not yet available.	Not yet available.
Italy	Final	Link	Not yet available	Link
Latvia	Final	Nacionālās kiberdrošības likums	Not yet available.	Not yet available.
Lithuania	Final	XIV-2902 Lietuvos Respublikos kibernetinio saugumo įstatymo Nr. XII-1428 pakeitimo įstatymas (e-tar.lt)	Link	Link
Luxenbourg	Draft	292642.pdf (chd.lu)	Not yet available	Link
Malta	Draft	Link	Not yet available.	Not yet available.
Netherlands	Draft	Link	Not yet available.	Website is not yet available, will probably be available in the fall
Poland	Draft	Link	Not yet available.	Not yet available
Portugal	Not transposed	Not yet available	Not yet available.	Not yet available.
Romania	Draft	Link	Not yet available.	Not yet available.
Slovak Republic	Draft	Link	Not yet available.	Link
Slovenia	Draft	Link	Not yet available.	Not yet available.
Spain	Not transposed	Not yet available	Not yet available.	Not yet available.
Sweden	Not transposed	Not yet available	Not yet available.	Not yet available.

Contacts

Contributors:


Evert Koks
Director
ekoks@deloitte.com
+32 476659927


Julie Colle
Senior Consultant
jcolle@deloitte.com
+ 32 478608496


Davide Lo Prete
Senior Consultant
dloprete@deloitte.it
+ 39 3385300577

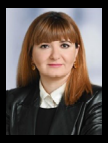
Subject matter experts:


Julia Kitzmüller
Manager
jkitzmueller@deloitte.at
+ 43 1537003779


Balazs Agardy
Senior Manager
bagardy@deloittece.com
+ 36 302392475


Ratko Drca
Director
rdrca@deloittece.com
+ 38 5916786091


Tapio Rihimaki
Manager
tapio.riihimaki@deloitte.fi
+ 35 8406787470


Tamara Okropiridze
Manager
tokropiridze@deloitte.de
+49 69756957215


Viktor Paggio
Senior Manager
vpaggio@deloittece.com
+42 0725009732


Pawel Klosek
Senior Manager
pklosek@deloittece.com
+48 664199134


Francesco Binaschi
Senior Manager
fbinaschi@deloitte.it
+39 3475399463


Nastassia Salash
Senior Consultant
nsalash@deloitte.lu
+352 621568298


Malik Vaibhav
Partner
vaimalik@deloitte.ie
+353 871504992


Lorenzo Russo
Partner
lorusso@deloitte.it
+39 3401766111

Deloitte.