



Aurexia

REGULATORY WATCH

Luxembourg

November 2023

ESMA Q&A updates on MiFID II & MiFIR Market structures topics

Adoption of the EBA's revised guideline on AML, Circular CSSF 23/842 – 23/843

List of countries under embargo

PSD3 : Modernizing payment services and financial services data

Retail Investment Strategy : how to increase retail investors' participation in Capital Markets

Regtech Corner : Examin



Aurexia
Institute

Agenda

ESMA Q&A updates on MiFID II & MiFIR Market Clarifications related to the fee schedules towards CCPs	03
Adoption of the EBA's revised guidelines on AML, Circular CSSF 23/842 – 23/843	04
List of countries under embargo	06
PSD3 Modernising payment services and opening financial services data: new opportunities for consumers and businesses	07
Retail Investment Strategy How to increase retail investors' participation in Capital Markets	09
Regtech Corner : Examin	11

ESMA Q&A updates on MiFID II & MiFIR Market structures topics : clarifications related to the fee schedules towards CCPs.

In June 2014, the MiFID II and MiFIR regulatory texts entered into force to define a clear framework for the financial instruments markets. MiFID II defines the framework around the investor's protection and transparency while MiFIR completes it, defining clear rules of disclosure with regard to pre- and post-trade information. Those requirements cover among others credit institutions, investment firms, market venues, CCP, OTF, and MTF.

However, the combination of those two rulesets is not always straightforward to interpret for both market participants and the relevant supervisory authorities. In this aim, a Q&A for MiFID and MiFIR market structures topics has been published and is regularly enriched with new Q&As.

On the 13th of October, the ESMA answered two new questions on the specific topic of the fees levied by the trading venues.

Question 8 clarifies the conditions under which a trading venue could apply different fee schedules to different CCPs under Article 36¹ of MiFIR. The answer from the ESMA is pointing out that, it is not expected under the requirements from this Article, that a different fee schedule applies to different CCPs. A difference in the fees from one CCP to another should only be explained by an objective reason such as a different access arrangement but the fact of having a close link with this CCP would not constitute a valid reason.

In question 9, ESMA further clarifies that there could be different costs incurred from other elements than the access arrangements but those need to be clearly detailed per service and as granular as possible to ensure that the arising fees are predictable.

In case an agreement has already been set between a CCP and a trading venue, but additional fees have to be charged by the trading venue, there is the need for the agreement to be changed under the agreed procedure between those two parties and those new fees have to be justifiable and resulting from the need to maintain or update the access arrangements with such CCP.

¹ Under Article 36, trading venues are "required to provide trade feeds on a non-discriminatory and transparent basis, including as regards fees related to access, upon request to any CCP authorized or recognized by Regulation (EU) No 648/2012 that wishes to clear transactions in financial instruments that are concluded on that trading venue." MiFIR

Adoption of the revised guideline, by the EBA, on money laundering and terrorist financing risk factors

Fortifying Financial Safeguards: Unraveling the Impact of Circular CSSF 23/842 on Anti-Money Laundering and Counter-Terrorist Financing Strategies in the EU

Circular CSSF 23/842 represents a significant regulatory development, as it pertains to the adoption of revised guidelines by the European Banking Authority (EBA) on money laundering and terrorist financing risk factors. This circular serves as a complementary piece to Circular CSSF 21/782, emphasizing the continuous efforts of financial institutions and regulatory bodies to enhance anti-money laundering (AML) and counter-terrorist financing (CTF) measures across the European Union.

The European Banking Authority, as a central regulatory authority, periodically reviews and updates guidelines to address the evolving landscape of financial crime and security threats. The revised guidelines incorporated into Circular CSSF 23/842 likely stem from a recognition of emerging trends, innovative money laundering techniques, and the need for a more robust and adaptive framework to combat financial crimes effectively.

One of the primary objectives of Circular CSSF 23/842 is to provide financial institutions with clear and updated guidance on identifying, assessing, and mitigating the risks associated with money laundering and terrorist financing. The document likely outlines specific risk factors that institutions should consider in their risk assessments, incorporating lessons learned from recent cases, global trends, and regulatory insights.

It's crucial to note that Circular CSSF 23/842 operates in conjunction with Circular CSSF 21/782, suggesting a strategic approach to strengthening the regulatory framework over time. Circular CSSF 21/782 likely established a foundation for AML and CTF measures, and the subsequent Circular CSSF 23/842 complements and builds upon this foundation, reflecting the dynamic nature of financial crimes and the necessity for continuous adaptation.

Financial institutions are expected to align their internal policies and procedures with the guidelines set forth in Circular CSSF 23/842. This may involve implementing enhanced due diligence measures, improving customer screening processes, and staying abreast of the latest typologies and red flags associated with money laundering and terrorist financing. The circular likely emphasizes the importance of a risk-based approach, encouraging institutions to tailor their AML and CTF efforts based on the specific risks they face.

Furthermore, Circular CSSF 23/842 could address the role of technology and innovation in the fight against financial crimes. As criminals become more sophisticated, financial institutions are encouraged to leverage technological solutions to enhance their detection and prevention capabilities. The circular may highlight the importance of investing in advanced analytics, artificial intelligence, and other technological tools to stay ahead of evolving threats.

In conclusion, Circular CSSF 23/842 represents a crucial step in the ongoing efforts to combat money laundering and terrorist financing within the European Union. By adopting the revised guidelines from the EBA, financial institutions are provided with updated and comprehensive guidance to strengthen their AML and CTF measures. The complementarity with Circular CSSF 21/782 indicates a strategic and evolving approach to regulatory oversight, acknowledging the need for continuous adaptation in the face of dynamic financial crime landscapes. Financial institutions are urged to promptly incorporate the recommendations outlined in the circular into their risk management frameworks to ensure a robust defense against illicit financial activities.

Strengthening Financial Guardrails: Decoding the Impact of Circular CSSF 23/843 on Access to Financial Services

Circular CSSF 23/843 marks a significant regulatory development with its adoption of guidelines by the European Banking Authority (EBA) on money laundering and terrorist financing risk factors in the context of providing access to financial services. This circular underscores the ongoing commitment of regulatory bodies to fortify anti-money laundering (AML) and counter-terrorist financing (CTF) measures within the financial services sector.

The guidelines incorporated into Circular CSSF 23/843 are likely tailored to address specific risk factors associated with providing access to financial services. This focus suggests an awareness of the unique challenges and vulnerabilities present in this particular aspect of financial operations. The EBA's involvement indicates a harmonized approach across the European Union to tackle money laundering and terrorist financing risks in the context of facilitating financial access.

Financial institutions subject to Circular CSSF 23/843 are expected to align their practices with the guidelines outlined in the circular. This may involve a thorough examination of their customer onboarding processes, due diligence procedures, and risk assessment frameworks to ensure they are in line with the newly adopted guidelines. The circular likely emphasizes the importance of vigilance and a risk-based approach to address potential vulnerabilities associated with granting access to financial services.

It's conceivable that Circular CSSF 23/843 addresses the need for financial institutions to strike a balance between facilitating access to financial services and mitigating the inherent risks. The guidelines may provide insights into the types of risk factors that institutions should consider when assessing new customers or when providing expanded financial services to existing clients.

In conclusion, Circular CSSF 23/843 reflects the regulatory intent to enhance AML and CTF measures specifically in the context of providing access to financial services. The adoption of EBA guidelines underscores the collaborative and coordinated efforts across the EU to address the evolving landscape of financial crimes. Financial institutions subject to this circular are urged to promptly integrate the guidelines into their operational frameworks, ensuring a comprehensive and effective approach to managing risks associated with providing access to financial services.

How Aurexia can help you

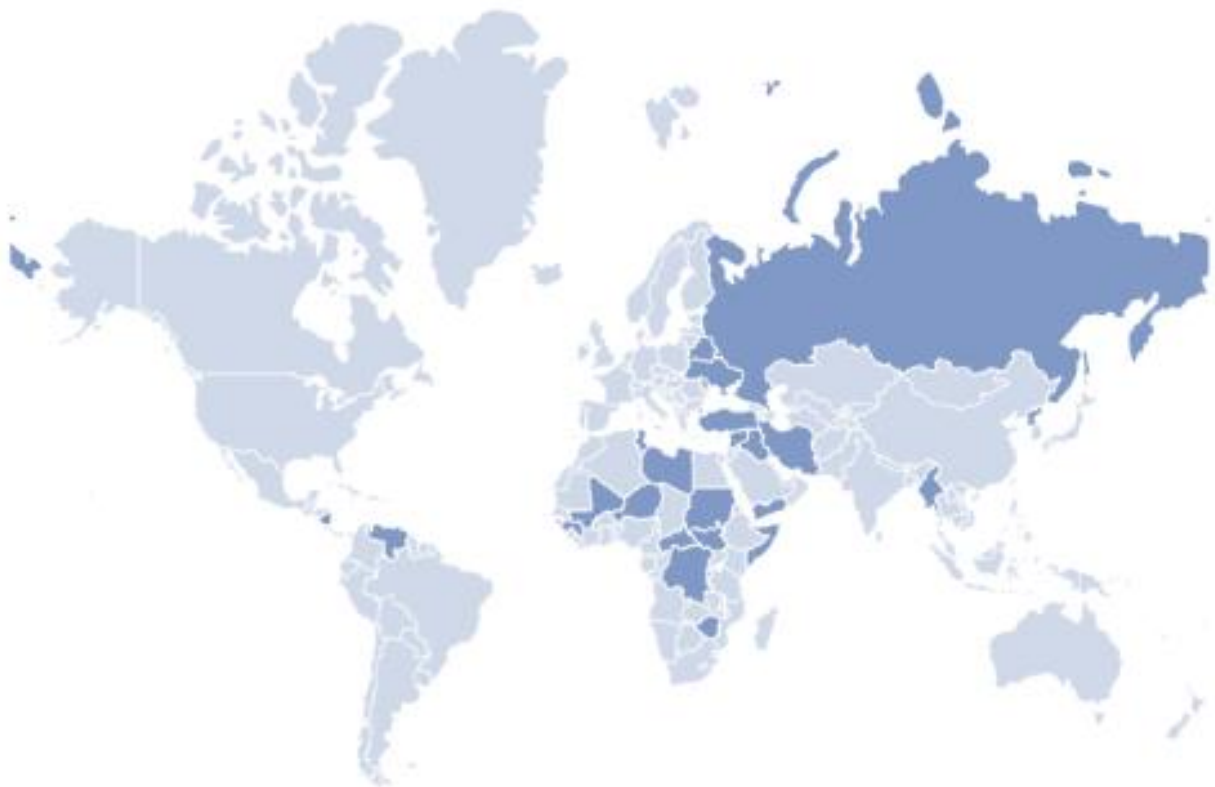
- **Audit and test your processes to ensure that they comply with the regulator's instructions**
- **Support you in improving these processes**
- **Support the teams at the various levels of compliance control to manage large backlogs that can have an impact on daily control management**
- **Make sure your control reflexes are flexible, depending on the case and the context of each situation**
- **KYC, KYT and KYB management**

List of countries under embargo

In the dynamic international context in which we live, it's important to have important up-to-date information. In the November issue of Aurexia, we bring you an update on countries and zones under financial embargo, which means extra vigilance in our day-to-day business.

→ OFFICIAL LIST OF GEOGRAPHICAL AREAS UNDER FINANCIAL EMBARGO

Belarus, Burundi, Congo , North Korea, Guinea-Bissau, Guinea, Haiti, Iran, Iraq, Lebanon, Libya, Mali, Moldavia, Myanmar (formerly Burma), Nicaragua, Niger, Central African Republic, Russia, Somalia, Sudan, South Sudan, Syria, Tunisia , Turkey, Venezuela, Yemen, Zimbabwe.



PSD3: Modernising payment services and opening financial services data: new opportunities for consumers and businesses (1/2)

In recent years, the European Union has been at the forefront of shaping regulatory frameworks to enhance the efficiency and security of the payments sector. Two key initiatives, the Payment Services Directive 3 (PSD3) and the Payment Service Regulation (PSR), are poised to play pivotal roles in reshaping the landscape of financial transactions in the EU. These initiatives are part of the broader efforts to foster innovation, enhance consumer protection, and ensure the security of payment services. This summary will delve into the key aspects of PSD3 and PSR, exploring their implications and the transformative impact on the payments sector.

PSD3: Evolution of Payment Services Directives

The Payment Services Directive 3 (PSD3) represents a significant evolution of its predecessors, PSD1 and PSD2. Building on the foundation laid by these directives, PSD3 aims to further harmonize the payments landscape, foster competition, and bolster consumer protection. The directive recognizes the dynamic nature of the financial industry, particularly the rise of innovative payment services and emerging technologies.

One of the noteworthy aspects of PSD3 is its expanded scope. While PSD2 primarily focused on traditional payment service providers, PSD3 broadens its reach to include new players in the market. This includes providers of crypto-assets and virtual currencies, reflecting the EU's commitment to staying abreast of technological advancements. The directive also places emphasis on enhancing security measures, mandating stronger authentication processes to mitigate the risks associated with fraudulent activities.

PSD3 introduces a more comprehensive framework for cross-border payments, streamlining processes and reducing barriers. The directive encourages the adoption of standardized technical solutions to facilitate interoperability among different payment systems, thereby fostering a more interconnected European payments ecosystem.

Furthermore, PSD3 reinforces the importance of cooperation and information-sharing among competent authorities. This collaborative approach is designed to enhance regulatory oversight and ensure the effectiveness of the regulatory framework across EU member states.

PSR: Safeguarding Payment Services

Concurrent with PSD3, the Payment Service Regulation (PSR) aims to fortify the regulatory framework governing payment services. The PSR focuses on ensuring the integrity, security, and resilience of payment systems, thereby safeguarding the interests of both consumers and businesses.

One of the key elements of the PSR is its emphasis on operational resilience. Recognizing the critical role that payment services play in the functioning of the economy, the regulation mandates that payment service providers establish and maintain robust mechanisms to ensure the continuity of services, even in the face of disruptions.

The PSR also places a spotlight on cybersecurity, requiring payment service providers to implement stringent measures to protect against cyber threats. This includes regular risk assessments, the implementation of effective security measures, and the development of incident response plans to mitigate the impact of cyber incidents.

PSD3: Modernising payment services and opening financial services data: new opportunities for consumers and businesses (2/2)

Moreover, the PSR introduces measures to enhance the oversight of payment service providers, granting competent authorities the tools needed to monitor and address potential risks effectively. This includes the power to impose sanctions and penalties for non-compliance with the regulatory requirements, thereby incentivizing adherence to the highest standards in the industry.

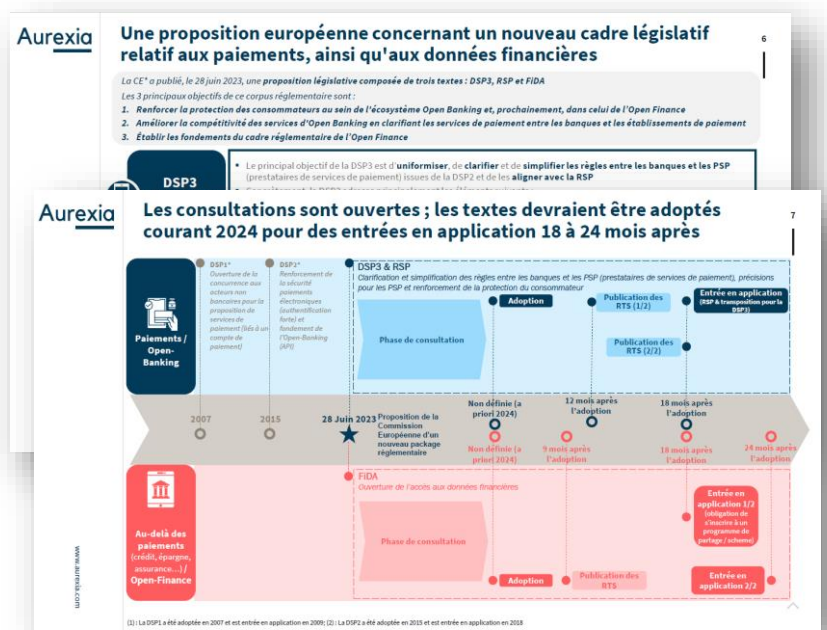
Implications for the Payments Sector

The combined impact of PSD3 and PSR on the payments sector is profound. These initiatives not only reflect the EU's commitment to fostering innovation but also underscore the importance of a secure and resilient payments infrastructure. For businesses operating in the payments sector, compliance with the new directives is paramount. The expanded scope of PSD3 requires both traditional and emerging payment service providers to adapt to a more comprehensive regulatory framework. This may involve the implementation of new security measures, the adoption of standardized technical solutions, and enhanced cooperation with regulatory authorities. The emphasis on operational resilience and cybersecurity in the PSR has far-reaching implications for payment service providers. Investments in robust infrastructure, regular risk assessments, and the development of effective incident response plans are imperative to ensure compliance and maintain the trust of consumers.

In conclusion, PSD3 and PSR represent significant milestones in the evolution of the European payments sector. As these directives come into effect, they are set to shape a more secure, innovative, and interconnected landscape for financial transactions within the EU. Businesses operating in this sector must stay vigilant, adapt to the new regulatory environment, and prioritize the highest standards of security and operational resilience to thrive in this evolving landscape.

How Aurexia can help you

- Monitor the PSD3/PSR regulatory developments and anticipate key challenges and opportunities
- Conduct impact assessments on upcoming PSD3 requirements
- Identify businesses that will be affected to size the work to be planned.
- Support on your regulatory compliance project and ensure your key stakeholders are aware on the expected regulations within your organization.
- Review existing PSD framework including processes and policies



Retail Investment Strategy: how to increase retail investors' participation in Capital Markets (1/2)

Before introducing the impact of the Retail Investment Strategy ("RIS") on the new legislative framework for retail investors, this proposal of RIS from the European Commission dated **May 24, 2023** follows action no. 8 of the September 2020 Action Plan for the European Capital Markets Union. It is part of the European Commission's long-term strategy. Its aim is to change the current rules governing the marketing of investment products to the public. Through this proposal, the European Commission aims to enable retail investors to increase their participation in the capital market, and to strengthen reliability and confidence in this market. The proposal also aims to amend several existing directives, such as MiFID 2, Insurance Distribution Directive (IDD), Solvency II, PRIIPS and UCITS & AIFMD Directives.

Various problems have been observed in recent years. Retail investors find it difficult to access relevant, comparable and easily understandable information to make informed investment choices. They risk being influenced by social media marketing and new marketing channels. Financial advice is not always in the best interest of individuals, and some investment products do not always offer good value for money to the retail investor.

This new proposal guides financial institutions towards a new model with multiple measures. Eight distinct pillars will have a greater or lesser impact on financial institutions :

- **Information** - Greater visibility of sustainability-related features and understandable information.
- **Fees** - Identification and quantification of product-related costs and fees, such as conditions and rules relating to costs, particularly for UCITS (AIFM) (fees paid by retail investors are 40% higher than those paid by institutional investors (e.g. pension funds) costs and performance). Also, restrictions and guarantees to avoid conflicts of interest. The Commission will extend MiFID II's ban on inducements to insurance-based products under IDD and will continue to prohibit inducements for sales of products for which no advice is provided.
- **Marketing** - Companies will be required to keep a register of all communications and marketing strategies relating to marketing practices, to ensure that the competent authorities have sufficient information to carry out investigations and the possibility of suspending or banning communications or marketing practices (to request restriction of access or removal of online content if necessary).

- **Advisory** – Improve the assessment suitability and appropriateness before providing the investment service ; Provide advice with a range of diversified, non-complex and cost-effective financial instruments ; Focus on MiFID II with specific requirements for advisor knowledge and skills. For example, in 2021, only 17% of EU household assets were held in the form of financial securities (such as shares or bonds) according to Eurostat, and 45% of Europeans are not convinced that the investment advice they receive from financial intermediaries is in their best interests (Eurobarometer 2023).

Two objectives will have a major impact on financial institutions. To simplify the comparison of investment products in terms of value for money, supervisory authorities will undertake the creation of specific benchmarks ("design and distribution references") which will enable appropriate assessments to be made. The introduction of a pricing process aimed at assessing and justifying costs and fees in terms of the product's expected value and appropriate proportion, will have a strong operational impact and repercussions on strategy and products brought to market.

To ensure that financial advice is aligned with the best interests of retail investors, it is planned to address potential conflicts of interest by prohibiting retrocessions in the context of Receiving Order Transmissions (RTO) and tightening the criteria for authorizing advisory-related retrocessions. The main operational impact will be the prohibition of retrocessions in the context of RTO, with specific exceptions, notably for value-added RTO or advisory management.

In conclusion, all financial institutions will be directly affected by the RIS in 2024. While this proposal will empower retail investors on EU capital markets, it will also have consequences for financial institutions. There will be increased complexity and regulatory burden, as well as intervention in product pricing, and enhanced supervision and standardization.

How Aurexia can help you

- **Assessment on the scope of products and services concerned**
- **Identification of impacts on Governance, Organization, Process and IT & implementation**
- **Steering and coordinating work: organizing committees and workshops**

Retail Investment Strategy: how to increase retail investors' participation in Capital Markets (2/2)

Main impacts on retail market players Retail Banking, Asset Management, Wealth Management

	Information		Fees		Marketing		Advisory	
	Adapting information to digital distribution and ESG preferences		Optimizing costs and protecting investors' interests		Avoid misleading marketing (including on social networks)		Better meet investors' needs and objectives	
Magnitude	Strong	Medium	Strong	Medium	Strong	Medium	Strong	Medium
	Producers	Distributors	Producers	Distributors	Producers	Distributors	Producers	Distributors
Business			Ban on incentives	Cost/performance benchmark (ESMA)			Diversified, uncomplicated and cost-effective range	
Compliance	KID : new sections and digital requirements						Strengthening products suitability	
Legal							Customer categorization	
Risk & Reporting	Annual statement of costs and performance				KID : new sections and digital requirements		More warnings on risky financial instruments	
Training							New in-depth training courses for advisors	
IT	KID : new sections and digital requirements				Retention of marketing communications for 5 years		Strengthening products suitability	

Legislative timetable and next steps



Date yet unknown



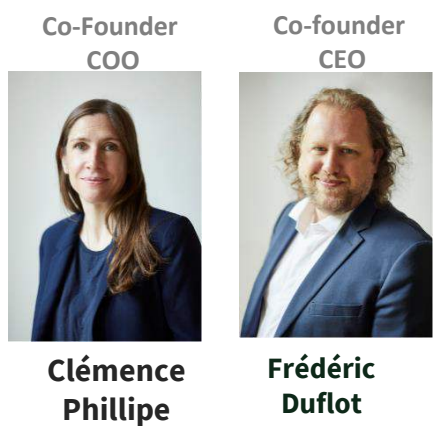
Regtech Corner: EXAMIN



Established 2019

Headquarter Paris

Target services Compliance & Cybersecurity



Companies are facing an avalanche of compliance regulations (data, insurance, finance, cybersecurity, ESG...) that they must comply with. This avalanche is complicated to attend for big companies, and it is almost an impossible mission for medium sizes companies..

EXAMIN provides a digital assistant (SaaS platform) to help companies to simplify their compliance and governance obligations. Thanks to the platform, a company can:

- Organize the compliance of the company (headquarter and subsidiaries);
- Visualize the level compliance in real time;
- Identify the gaps and the risks;
- Implement the action plans;
- Evaluate and control the people and companies (internal and external) involved in the compliance;
- Increase the level of compliance and the level of trust of the business partners;
- Anticipate controls from authorities.

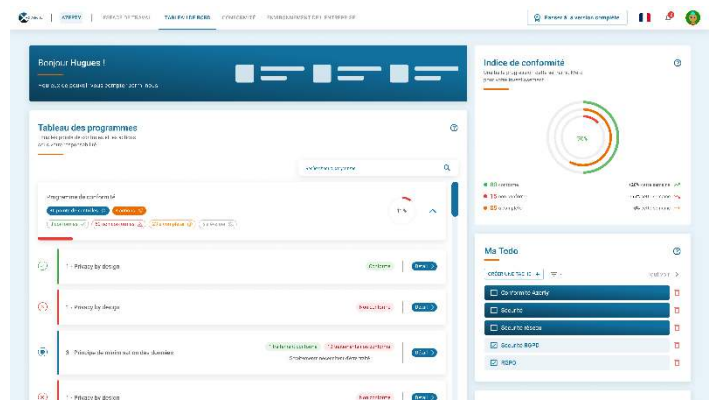
Examin also provides support services to help companies to be compliant and to implement the necessary processes and documentations required by the regulations (e.g. GDPR, ISO27XXX, DORA, NIS2...). The services are provided by experts (legal

advisors, lawyers, expert in cybersecurity...).

EXAMIN simplifies your business and transform legal and regulatory constraints in strengths. EXAMIN brings you objectivity, speed and fluidity to compliance.

- By making standards understandable and easy to follow
- By giving decision maker a clearer picture of their regulatory situation
- By providing day-to-day support for your compliance issues (platform and services)
- By making compliance accessible for end users

Thanks to Examin, compliance means time savings, added value, transparency, traceability, and safety.



Aurexia

For any additional information, please contact :



Alain de CIDRAC

Partner

alain.decidrac@aurexia.com

+ 352 27 86 40 32

21, Rue Glesener,
1631, Luxembourg

**PARIS – LONDON – LUXEMBOURG –
HONG KONG – SINGAPORE – MONTREAL**

Aurexia



Bringing value, together

© 2023 Aurexia Luxembourg. Material in this publication may not be copied, reproduced or republished in any way except for your own personal, non-commercial use. Prior written consent of Aurexia Luxembourg must be obtained if you intend to reuse. The contents of this publication represent the views of Aurexia and should not be taken as advice or the provision of professional services in any way.

Aurexia Luxembourg is a limited liability company registered in Luxembourg. The companies house registration number for Aurexia Luxembourg is B197317. Aurexia Luxembourg is part of the global Aurexia group, which also has offices in France, England, Singapore, and Hong Kong.