Deloitte.

AI Regulation in the Financial Sector: Opportunities and Challenges

MAKING AN IMPACT THAT MATTERS since 1845

1 Overview: EU Artificial Intelligence Act

The European Union has been at the forefront of developing the regulatory landscape in artificial intelligence (AI). In enacting the AI Act (Regulation (EU) 2024/1689), it has created a comprehensive framework that takes the complexity and potential risks of AI systems into account. A major priority of the EU Commission for the 2019–2024 cycle has been to create a "Europe fit for the digital age". This ambitious agenda has led to more than ten significant digital regulations being tabled, affecting areas such as the data economy, cybersecurity and platform regulation. The AI Act is a crucial piece of this complex puzzle. Indeed, while this article will mainly focus on the AI Act, this should be considered within the wider context of the EU's overall digital regulatory landscape.

The AI Act was published in the Official Journal of the European Union in July 2024 and entered into force on 1 August 2024. This date marks the beginning of a step-by-step process to implement the various regulations and obligations contained in the Act. Its goal is to promote human-centric AI and to facilitate the functioning of the European single market with regard to AI products.

The EU has adopted the OECD's latest definition of AI systems: as machine-based systems designed with varying levels of autonomy and adaptable after use that, for explicit or implicit objectives, process inputs to generate outcomes such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

The AI Act applies to providers, operators, importers and distributors of AI systems in the European Union, as well as EU users of AI systems regardless of their origin, and non-EU providers and users whose outputs are used in the European Union. The approach taken in the Act mirrors that of the General Data Protection Regulation, emphasising a robust legal framework that promotes security and innovation.

The AI Act creates a framework to regulate the use and application of artificial intelligence within the European Union, introducing a standardised procedure for the market entry and operational implementation of purpose-built AI systems to ensure a harmonised approach across all EU member states. As a product safety regulation, the AI Act takes a risk-based approach in classifying AI systems according to their use case and setting compliance requirements based on the risk level to users. As a consequence of this approach, certain AI applications that are considered unethical or harmful are banned, while high-risk AI applications are subject to detailed requirements to deal with potential threats effectively.

The Act also lays down transparency requirements for AI technologies that pose other associated risks. By adopting a principle-based approach, the Act should prove capability of adapting to as-yet-unknown iterations of AI technologies.

The proliferation of general-purpose (basic) AI models has also prompted legislators to differentiate between specific-purpose and general-purpose AI systems. The AI Act regulates market entry for universal AI models, regardless of the risk category assigned to each use case, as well as laying down comprehensive market surveillance, governance and enforcement rules with a view to preserving the integrity and public trust in AI innovations.

Although most requirements must be complied within a 24-month period, critical prohibited-use provisions will come into force after just six months. Providers of general-purpose AI models and systems must also comply with the AI Act within twelve months to enable downstream developers and operators to also deliver compliant solutions.

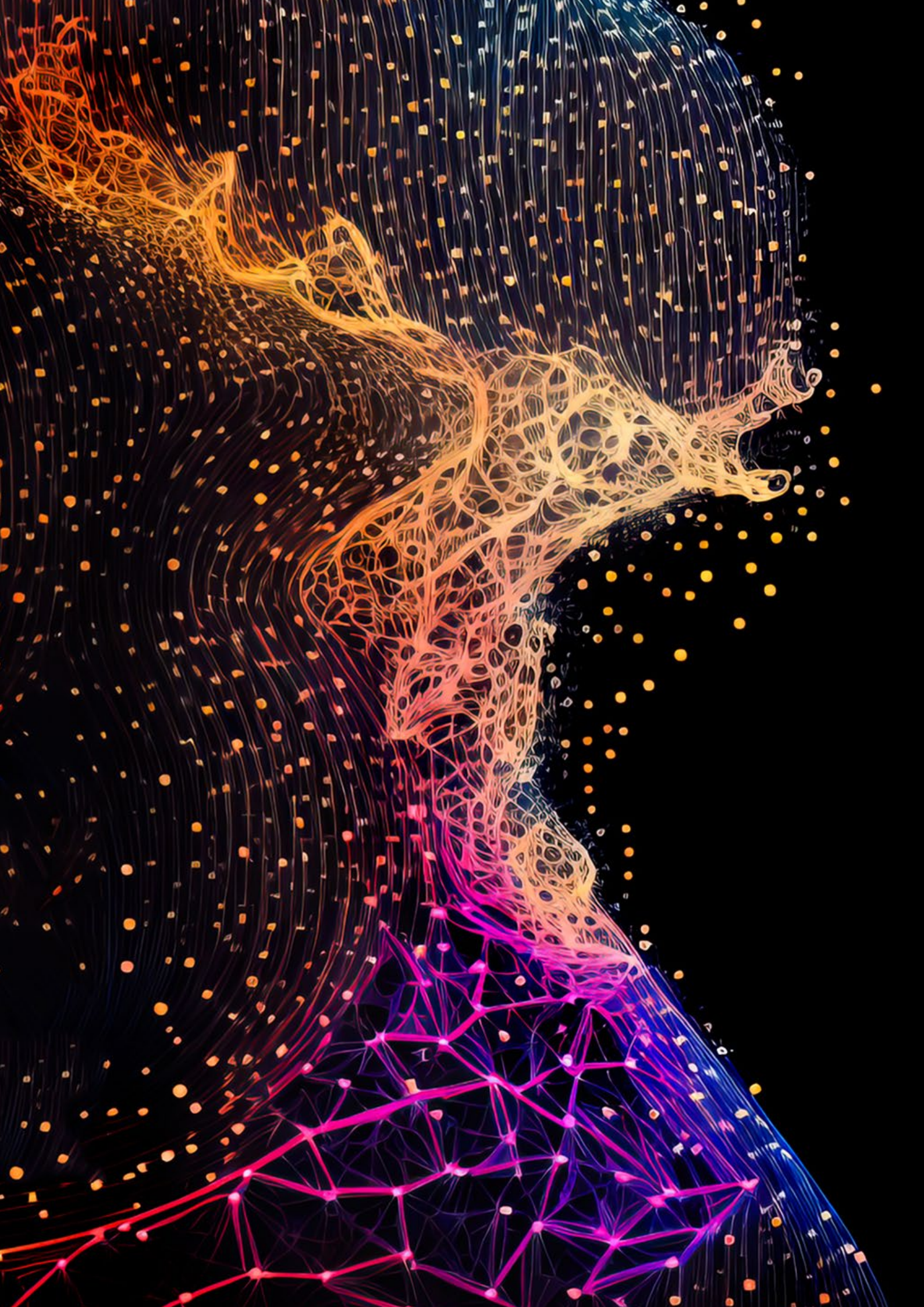
Due to its abstract nature, there are some areas of the AI Act are yet to be fully defined. These which are expected to be further elaborated through delegated and implementing acts, guidelines from EU institutions and harmonised standards developed by the European Standardisation Organisations. As a result, companies can expect more detailed guidance to be published and available from by the European Artificial Intelligence Office (or AI Office) in the near future.

The European AI Office was set up by the European Commission in February 2023 to streamline and monitor the implementation of the AI Act. As a Commission service, the AI Office is embedded within DG CONNECT, allowing

it more freedom in terms of decision-making and taking dynamic action.

Following its consumer protection and product safety based approach, the EU AI Act adopts a risk-based framework that focuses on the application of artificial intelligence rather than the AI technology itself.

This means that the higher risk to users, the more stringent the obligations.



A risk-based approach to protecting EU citizens

The AI Act demarcates four different risk categories, each with its own specific requirements: (i) unacceptable-risk AI systems; (ii) high-risk AI systems; (iii) AI systems with special transparency obligations; and (iv) AI systems posing other risks. Companies must assess how their AI applications fit into these four risk categories.

Prohibited applications

While recognising the benefits of AI, policymakers are also aware that certain AI applications could jeopardise fundamental EU rights such as the right to human dignity, freedom, equality, democracy, data protection and the rule of law. These fundamental EU principles have been weighed against the potential advantages of AI and, consequently, the AI Act prohibits certain AI systems in order to protect these rights. These prohibitions will take effect after a six-month grace period following the implementation of the AI Act. Prohibited uses include manipulative techniques, social scoring, real-time biometric identification and emotion recognition in the workplace.

High-risk AI systems

High-risk AI systems are those systems considered to pose a threat to the security or fundamental rights of EU citizens. As a result of this presumed risk, they need to be assessed before they are placed on the market and subsequently throughout their entire life cycle. High-risk AI applications include critical infrastructure and areas of application such as education, training, employment, essential private and public services (e.g., health services, banking), as well as specific law enforcement, migration and border management systems and justice and democratic processes (e.g., influencing elections).

One of the main obligations placed on providers of high-risk AI systems is that they must set up a risk management system (RMS) covering all phases of the AI system's lifecycle. This includes quality management for as long as the system is on the market. Before a high-risk AI system can be placed on the market, the AI Act requires it to undergo conformity assessments and for a "declaration of conformity" to be issued. The product must also be proven to comply with the obligations outlined above. Conformity assessments for high-risk AI systems can be carried out by the providers themselves or with the support of third parties, depending on the type of system in question. In turn, operators must follow the provider's instructions for using the AI system, ensure human oversight and report any malfunctions.

AI systems with special transparency obligations and AI systems posing other risks

AI applications posing limited risks to individuals must first and foremost comply with certain transparency requirements. An example of limited-risk AI systems are AI-based chatbots, which must explicitly inform users that they are AI applications before their use so that users know they are interacting with a machine.

Users must also be given the opportunity to be forwarded to a human. AI systems posing other risks are not subject to any obligations under the AI Act.

This classification could cover a large cross-section of existing AI applications across various sectors, including spam filters, AI-powered video games and inventory management systems. All operators can sign up to a voluntary code of conduct to comply with EU standards on ethics and trustworthiness.

General-purpose AI models

The AI Act also applies to general-purpose AI (GPAI) models that do not pose systemic risks. These are subject to only limited requirements, such as transparency obligations. However, models that do pose systemic risks are subject to stricter regulations, such as adversarial testing. As far as sanctions are concerned, the AI Act follows a graduated approach: the more serious the violation, the higher the penalty. In general, fines for AI Act violations are calculated as a percentage of the offending company's total annual turnover from the previous fiscal year or as a predetermined amount, whichever is greater. Proportionate administrative penalties are imposed on offending SMEs and start-ups. As an instrument that promotes innovation, the AI Act makes provision for AI regulatory sandboxes, which offer a controlled environment for developing, testing and validating innovative AI systems. These should also allow testing under real conditions.

2 Strategic and operational implementation of AI in the financial sector

Focus on use cases and regulation

To take advantage of the opportunities offered to institutions by artificial intelligence, a targeted 5-step implementation strategy is required at the management level. Efforts should be focused on developing an institutional AI ecosystem which – in addition to providing an appropriate compliance and governance structure – also manages and implements specific business cases centrally. It would be sensible to separate AI responsibilities from the classic lineal structure.

Secondly, it is of fundamental importance that an Artificial Intelligence Center of Excellence (AI CoE) is established, bringing together an interdisciplinary team from all affected areas (including back-office functions). This should be regarded as an integral part of the existing business areas. The AI CoE, in collaboration with management, should develop a roadmap for AI use, addressing both specific use cases and regulatory aspects (e.g., compliance with the EU AI Act).

In this context, a uniform strategic approach should be followed.

The 5-step implementation strategy

1. Evaluate opportunities
This step is aimed at developing specific use cases and their economic benefits in concept workshops held with each department under the control of the AI CoE.

As part of the project selection process, the CoE AI evaluates projects specifically in terms of their regulation, economic benefit and time feasibility. Economic benefit and compliance with new regulatory requirements are weighted more heavily when use cases can be implemented within the same time frame. This step also aims to assess the extent to which solutions can be efficiently integrated into the existing process flows and their order of priority in the implementation of other tasks within the same area.

2. Classify risks
The risks associated with each new use case must be examined and documented separately. In addition, the inventory and categorisation must be carried out in accordance with the requirements of the AI Act regarding risk management. The relevant compliance and governance considerations must be flexible, since both the use case and the basic regulation change constantly and therefore require timely adjustments. At the end of this step of the process, a decision should be taken that weighs up the opportunity/risk profile of each use case.

3. Develop and test tools
The tool to be developed can be based on a specially developed solution or a solution already available on the market. It is essential that the tool developed is extensively tested by various stakeholders and that a corresponding test plan is available. Each test must then be carried out and documented. In this step, it is important to verify that the tool also meets the regulatory requirements over its entire life cycle and, therefore, is always compliant on a statutory level.

4. Implement tools
When implementing a use case in a lineal organisation, particular attention must be paid to ensuring that the AI takes over redundant processes and replaces the previous processes successfully. In the transition phase, a dual-line structure is recommended so that it is possible to fall back on the old processes in an emergency. At the same time, it is important that operational employees are required to implement the new solution consistently.

5. Operating and servicing
In the final operation and service step, the AI CoE should ensure that all operational employees working with the AI solution are comprehensively trained in both practical and regulatory terms. A corresponding knowledge bank should also be established, and backtesting and further development must be a constant area of focus.
In addition, the organisation should be prepared to focus its AI talent acquisition process on attracting new colleagues who are not only proficient in the complex field of AI development, but can also think and work across interfaces.

Although the entire process is centrally coordinated by the AI CoE, it is important to involve the entire organisation in the change process not only to make sure that AI solutions are accepted, but also to drive continued development within the organisation. In this context, in addition to considering the regulatory parameters of the EU AI Act, we will analyse some examples of specific use cases below.

3 Financial sector use cases under the EU AI Act

Artificial intelligence (AI) is revolutionising banking by increasing both efficiency and customer satisfaction. Banks are using AI to automate routine tasks such as customer service, credit scoring and fraud detection. Applications such as robo-advisors and virtual assistants offer personalised services and improve interaction with customers, while data mining and machine learning models enable more precise assessments of credit risks and the early detection of fraudulent activities. All of this leads to reduced operating costs and increased profits.

At the same time, however, AI systems also carry risks. Inaccurate data and biases can lead to wrong decisions. There are also security concerns about possible cyberattacks and data breaches. These challenges require strict adherence to compliance standards. Deloitte offers banks specialised solutions that are compliant with regulatory requirements. With its extensive expertise, Deloitte supports you in maximising the potential of AI while minimising the associated risks.

Applications of AI in banking: opportunities and risks

Banks are already successfully using large volumes of data and complex algorithms, as can be seen from their specialised capital market applications (algo-trading) and modern risk models. Artificial intelligence is now also being applied in many other areas of banking. Text and speech recognition are being integrated into chat- and talk-bots and are increasingly taking over the tasks of call centre agents. Robo-advisors (i.e., digital investment advisors) offer investment recommendations to private customers based on their individual preferences. They can also take over the task of composing, monitoring and restructuring investment portfolios, largely automatically and autonomously, all the while taking into account the current market situation.

There is a long list of possible uses for AI by banks, ranging from fraud detection in the credit card business and KYC processes, to detecting cyberattacks and automating various processes. Each of these applications offer banks considerable potential to reduce their costs and increase their revenues.

In Germany, banks are currently facing significant challenges, as illustrated by the cost-income ratio, which has been rising ever since the 2008 financial crisis. This situation derives from various factors – for instance, the European Central Bank's ongoing policy of low interest rates, which is affecting banks' interest income and is intensifying the already intense competition in the industry. Meanwhile, commission income has remained stable, while trading profits are showing some weakness. On the cost side, banks are facing rising administrative costs caused by increased regulatory obligations and higher capital adequacy requirements.

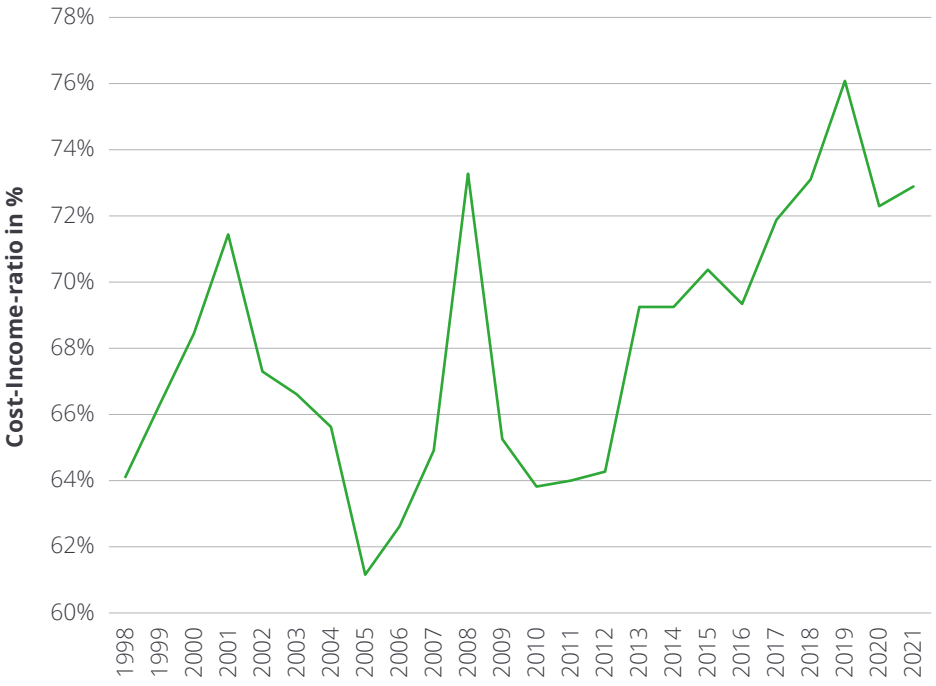


Figure 1 *Cost-income ratio of banks in Germany*

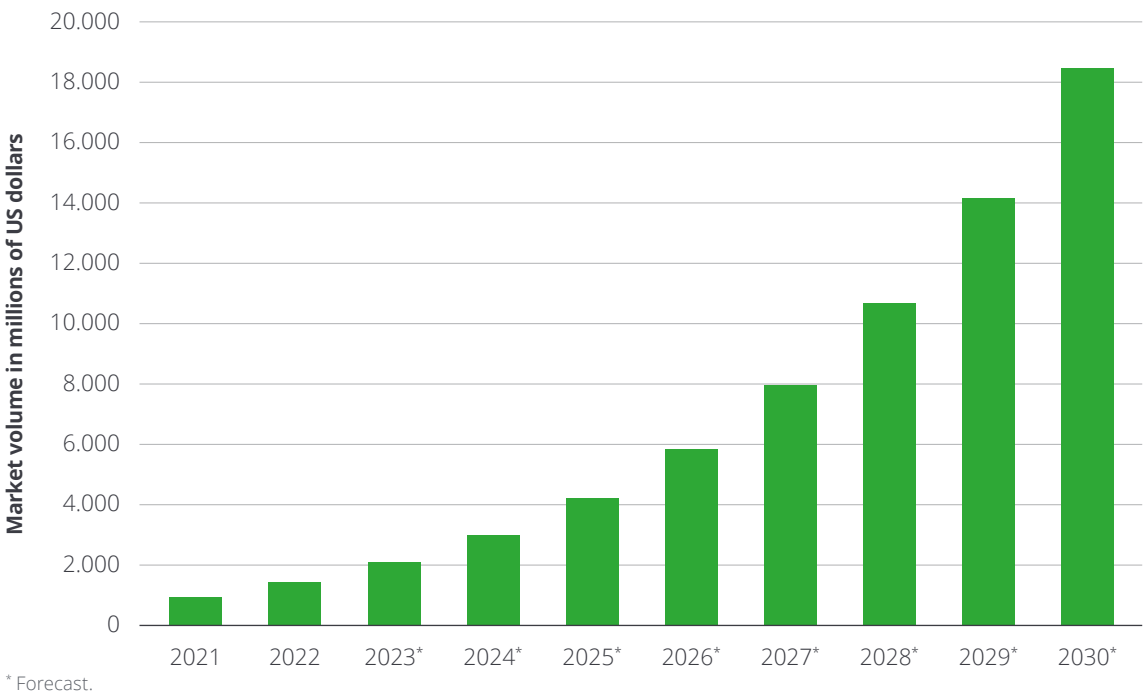


Figure 2 *Global AI market volume by 2030*

The entry into the financial market of digital companies such as Google, Apple, Facebook and Amazon has increased competition and brought new dynamism to the industry. These tech platforms, together with numerous innovative FinTechs, have focused heavily on critical customer interfaces in recent years. They are setting new standards with their digital solutions, while at the same time offering highly individualised services complete with fast processing times, improved interaction and intuitive usability. These developments are changing what customers are coming to expect from modern banking services and expanding the range of opportunities for customer engagement and retention.

The integration of artificial intelligence into the banking industry represents an unprecedented opportunity to both reduce costs and significantly increase efficiency. Integrating AI into the financial sector is expected to enable savings of over one trillion US dollars worldwide. These savings will be achieved mainly through a reduction in operating costs, a large part of which in the front office. However, the success of this transformation depends heavily on how comfortable consumers are with AI and how much they trust this technology.

Banks are already using AI in various areas to improve their services and increase operational efficiency. Some banks have introduced virtual assistants that allow customers to access account information, transfer money and make appointments by voice command, text messages or touch. This type of AI-powered customer service can personalise interactions and make them more efficient.

Despite the potential benefits of AI, consumers are still sceptical about its use in banking. While AI is well received in areas such as healthcare, only a small proportion of consumers trust that their personal data will be safe in AI applications. However, one area where AI is gaining widespread adoption is fraud monitoring.

CEOs at banks across the world can see the significant potential of artificial intelligence for further developing their business models. The wide range of its applications makes clear that this is not a temporary trend: AI is supporting the industry's ongoing digitisation process, paving the way for new fields of application where automation was previously considered either too complex or too cost-intensive.

Fraud prevention

Data mining to detect loan fraud

Data mining encompasses various methods and techniques that are used to analyse large volumes of data to discover patterns, correlations and anomalies. Common applications include data classification, where data is divided into predefined categories such as "legitimate" or "fraudulent"; and clustering, where data is grouped into clusters based on their shared characteristics. The latter is used, for instance, to segment customers based on their financial behaviour. Regression analysis helps to identify relationships between variables and to create predictive models that banks can use to predict credit risk. Association analysis, on the other hand, looks for patterns and correlations between different data points, enabling banks to analyse transaction patterns so as to recommend products that are often purchased together. Finally, anomaly detection identifies unusual data points that deviate from the norms – this is particularly useful for fraud detection.

Data mining techniques have made a significant contribution to improving fraud detection at European banks. Many institutions use advanced analytical methods to identify suspicious transaction patterns that could indicate fraudulent activity. These techniques have helped to detect fraudulent transactions more quickly and accurately, resulting in a significant reduction in losses due to fraud.

Data mining techniques are also used to assess credit risks and predict default probabilities. By analysing extensive data on customer behaviour and loan repayments, banks can develop more precise lending models and thus optimise their loan portfolios. This can increase the accuracy of their credit risk assessments and improve the bank's financial stability.

In addition, data mining supports banks in optimising their operational processes. By analysing internal data, they can identify and exploit potential efficiencies to reduce costs and improve operational performance. In addition, data mining offers opportunities for market and competitor analysis. Banks can make informed strategic decisions and strengthen their position in the market by analysing external data sources such as market indicators, competitive activities and macroeconomic trends. Overall, the use of data mining by institutions shows that these techniques contribute not only to fraud detection, but also to an all-round improvement in the decision-making and performance of the banking industry as a whole. Loan fraud detection systems are not defined as high-risk AI systems under the EU AI Act.

Credit scoring analysis to avoid payment defaults

Credit scoring analysis is an advanced method of assessing the creditworthiness of potential borrowers. This data-driven approach is based on statistical analysis and machine learning techniques and is used to predict the risk of default on loans. These default prediction models use cumulative customer data collected from various sources, including past loan applications, transaction history, credit reports and possibly sociodemographic information. By analysing this data, patterns and trends can be identified that indicate potential credit risks. For example, studies show that greater predictive accuracy is achieved by integrating transaction data and credit reports.

The models have proven to be extremely precise and accurate, which means they can reliably predict which borrowers are likely to default on their obligations. By analysing cumulative customer data, they can identify and prevent potential cases of fraud at an early stage. This is achieved by the model detecting unusual patterns or anomalies in the data that could indicate fraudulent activity.

Credit scoring analysis is an advanced method of assessing the creditworthiness of potential borrowers. This data-driven approach is based on statistical and machine learning techniques and is used to predict the risk of default on loans.

A practical example of this is the use of the random forest algorithm, which has been successfully implemented in a credit risk scoring system and has helped to reduce fraudulent lending. The model can be continuously adapted and optimise by introducing new data and verifying the model's performance. This iterative improvement process makes it possible to respond to changing market conditions and new trends in the lending process and to further improve forecasting accuracy. For example, one study has shown that performance can be increased over time by regularly retraining the model on new data.

Credit scoring systems are classified as high-risk AI systems under the EU AI Act because they have a significant impact on lending and can potentially be subject to significant distortions. Consequently, companies that use comparable systems are subject to strict compliance requirements.

Smartphone transaction data

Advanced scoring systems analyse transaction data to detect fraud patterns and take preventive measures. By continuously monitoring and evaluating large volumes of data, banks can proactively respond to suspicious activity and identify potential risks at an early stage. These preventive measures help to minimise losses from fraud and protect customers' financial transactions.

Default prediction models have been shown to be highly precise and accurate. By analysing cumulative customer data, systems can identify and prevent potential lending fraud at an early stage. By using data collected through smartphones, a more comprehensive picture can be formed of a user's creditworthiness.

The concept is based on the notion that almost everyone uses a smartphone that captures different types of data, including SMS confirmations of bank transactions. These SMS messages contain important information, such as the amount, account number and account balance, which can be used to create a detailed financial profile. In addition to transaction data, information from social media is also used to better assess a user's general social and economic status. The system automatically collects all relevant data via a smartphone app, which regularly sends transaction details and other important information to a central database. This eliminates the need to manually collect data from different banks and allows for a continuous and up-to-date assessment of creditworthiness.

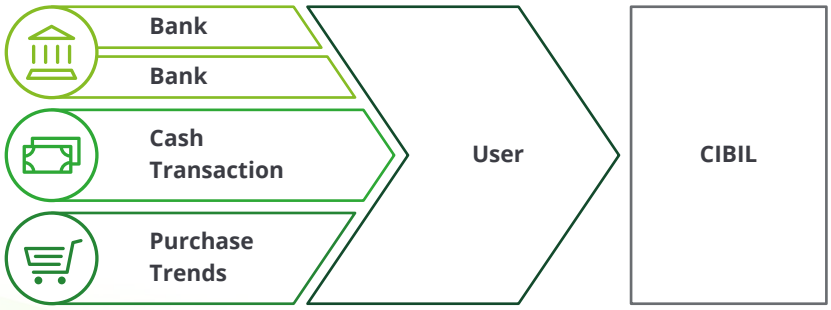


Figure 3 *Collection of user data from smartphone apps*

A unique aspect of this model is the use of social media to assess creditworthiness. Factors such as level of education, professional background and social media use can be important indicators of a user's financial stability and are included in the calculations. These additional data sources enable a more precise and holistic assessment of creditworthiness.

By using modern technologies and integrating data from various sources, the system can not only detect fraud at an early stage, but can also optimise credit decisions. Banks and financial institutions can thus ensure that loans are granted to trustworthy and financially reliable borrowers, which significantly reduces the risk of default.

In summary, credit scoring analysis enables financial institutions to accurately assess credit risks and detect fraud at an early stage, leading to better lending and default rates. By integrating machine learning and statistical methods, existing risks can be better managed and future challenges can be mastered more effectively.
The use of smartphone data and social media increases prediction accuracy and strengthens reliability in the credit scoring process.

Nevertheless, implementing technology-based fraud prevention systems at banks also entails various risks. A key risk is the dependence on the quality and accuracy of the data used. Incomplete or inaccurate data can result in fraudulent activity not being detected or legitimate transactions being incorrectly classified as fraudulent. Due to the complexity of the AI models and the algorithms used, the systems may contain unintended biases that lead to discriminatory decisions, or they may allow for misinterpretations that can affect the effectiveness of the fraud detection process. Moreover, these systems are only as good as the people who develop and monitor them. Without trained employees

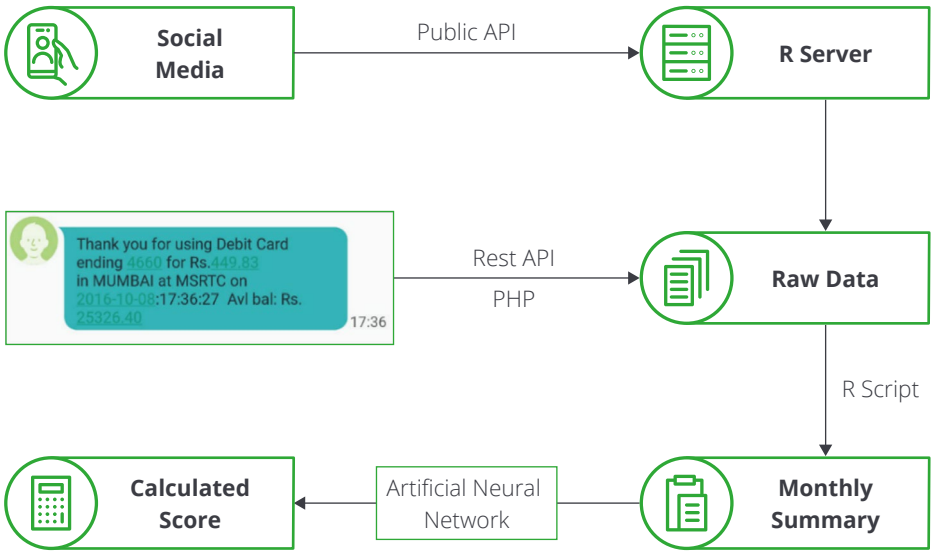


Figure 4 *Algorithm of a proposed solution based on smartphone data*

who continuously adapt and improve the solutions, prevention systems can become less effective.

The security of the systems themselves also poses a significant risk. Cyberattacks and data leaks can not only lead to financial losses but can also significantly damage customers' trust in the bank. Attackers who gain access to sensitive data could use it to develop even more advanced methods of fraud.

Regulatory and legal challenges are another risk, and the systems must meet current data protection and compliance requirements. Otherwise, banks could face significant legal consequences and fines.

In order to minimise these risks, it is crucial that institutions employ trained staff who are able to develop, monitor and continuously improve complex fraud prevention systems. Regular training and updates, as well as compliance with the highest safety standards, are essential to ensure the reliability and effectiveness of solutions.

In terms of regulatory compliance, it bears underlining that anti-fraud systems do not fall under the EU AI Act as currently defined. This highlights the potential to use AI-based anti-fraud applications in the banking sector, as their use does not result in any further regulatory hurdles. The systems can therefore be implemented and used directly.

AI is also used to process loan applications. Previously, customers often had to wait days or weeks for their application to be reviewed and approved. With AI, loan applications can be analysed and decided in real time. With the help of AI credit scoring systems, banks have been able to reduce processing times for loan applications to just a few minutes. This has not only increased customer satisfaction, but has also significantly increased banks' efficiency.

Customer experience-optimised financial advice with AI

Customer analytics with real-time reactions and transactional data

Companies that use AI-based customer analytics systems are thought to achieve higher customer satisfaction and retention. Indeed, financial institutions that use AI for customer analysis have seen a significant improvement in customer satisfaction. In addition, the ability to provide real-time recommendations has noticeably increased customer loyalty.

AI-based systems are revolutionising financial consulting by enabling in-depth analysis of customer behaviour and preferences. These systems use advanced algorithms to process large volumes of data and detect patterns that human analysts might miss. For example, AI models can analyse transactional data, social media profiles, and other relevant information to provide a comprehensive picture of the customer.

Customer analytics with real-time responses and transactional data offers numerous benefits to financial institutions in terms of optimising their services and increasing customer satisfaction. By using modern technologies and data analysis tools, banks can not only better understand their customers' behaviour but can also respond more quickly to their needs.

A practical example is the use of real-time data to create personalised offers. When a customer makes a major transaction such as buying a car, the system can immediately process this information and offer the customer suitable financial products such as car loans or insurance. Banks that use real-time data experience increased sales through these personalised offers. Real-time data analysis also helps improve the customer experience.

For example, if a customer has repeated difficulties with online banking, the system can use this information to proactively offer support.

These practical examples show how integrating real-time responses and transaction data can improve the efficiency and effectiveness of banks. The rapid adaptability and deeper understanding of customers' needs enables financial institutions to significantly increase both customer satisfaction and operational performance.

Automated request processing (NLP, virtual assistants)

Another significant advantage of AI in financial consulting is the automated processing of customer inquiries. Virtual assistants and natural language processing (NLP) technologies can process routine requests more quickly and efficiently than human employees. These systems are able to understand natural language and answer complex questions by accessing an extensive knowledge base.

A good example can be found in the implementation of AI-based chatbots. These can use NLP to identify interlocutors and adapt to their needs in real time. For example, if a customer asks a question about his account balance, the chatbot can not only provide up-to-date information, but can also make contextual recommendations based on the customer's past spending patterns. This significantly improves the customer experience by making interactions more personal and relevant.

Using AI in banks' call centres is another practical application. Virtual assistants can automatically answer frequently asked questions such as balance queries, transaction details and credit card information. This frees up human employees to focus on more complex issues.

In conclusion, the use of AI in financial consulting not only improves the customer experience, but also significantly increases the efficiency and effectiveness of service delivery. By combining in-depth customer analysis and automated query processing, financial institutions can deliver greater value to their customers while reducing their own operating costs. Using AI systems in this area gives rise to transparency obligations. The EU AI Act stipulates that companies that use such systems must regularly disclose information about the systems. These are classified as limited-risk AI systems.

4 Conclusions and Action

In the financial sector, leading global companies are using automation to make resource-intensive processes more efficient. Particular focus is being placed in areas with a high potential for standardisation, with the use of AI applications such as automated payment reconciliations. These technologies have dramatically reduced costs in industries such as food, chemicals, energy and construction. At the same time, they are capable of processing payment differences more quickly, increasing efficiency and minimising delays in receivables.

Yet manual financial processes with considerable potential for automation still exist. This includes analysing and reconciling differences between deliveries of goods and incoming invoices. By using intelligent solutions based on historical data, a higher level of automation can be achieved. These solutions can then support financial accountants in processing problematic orders effectively.

Integrating artificial intelligence into banking offers considerable potential to institutions. AI-powered solutions can help reduce costs, increase efficiency and improve the customer experience. Outcomes include automated request processing, more precise credit risk assessment through data mining, and personalised financial advice with real-time responses. Investments in advanced AI systems are crucial if institutions are to remain resilient in the highly competitive financial market and if they are to set new standards in the sector.

Overall, integrating AI into banking not only offers opportunities to improve operational efficiency and customer satisfaction, but it also requires a strategic approach to manage the potential risks and to ensure long-term competitiveness in the financial market.

Potential risks and regulatory challenges

Nevertheless, there are also risks that must be considered when implementing AI-powered systems in banking operations, in particular concerns about data quality and protection.

Other significant risks include potential bias and ethical issues. AI models may contain unintentional bias that could lead to discriminatory decisions. Deloitte attaches great importance to ensuring that our algorithms are fair and transparent in order not only to meet regulatory requirements, but also to consistently comply with ethical standards.

System security is our top priority, as cyberattacks and data leaks could seriously jeopardise the trust of our customers. Therefore, we implement robust security measures to effectively minimise these risks.

In addition, regulatory compliance is an essential aspect of our work. We ensure that all our AI-powered systems comply with current legal requirements to avoid potential legal consequences or penalties.

By taking proactive measures to mitigate these risks, we at Deloitte can make the most of the benefits of AI in banking while also protecting the integrity and security of our services.

Deloitte's support

Banks should analyse how the use of artificial intelligence impacts on their products and business models at an early stage. In this context, it is essential to understand whether the AI systems used fall within the scope of other supervisory regimes. Particularly in the context of the EU AI Act, banks should examine how to classify and inventory their internal AI systems, with the main focus falling on the different requirements for each risk classification. In addition, any adjustments made within the organisation itself or to its processes should be factored in. It is advisable to check the regulatory requirements as early as possible to counteract any compliance gaps.

Deloitte has extensive experience and expertise to help banks leverage AI. With tailor-made solutions, Deloitte helps financial institutions meet regulatory requirements and make the most of the opportunities offered by AI. Finally, Deloitte demonstrates its cross-industry expertise in the use of AI by developing and publishing detailed case studies. These case studies set out the specific benefits and measurable results achieved by using AI, as well as offering potential customers an insight into successful projects.

Deloitte will be happy to advise you in planning, creating and implementing the necessary measures necessary to help you clear the regulatory hurdles and fully exploit the potential of AI.

Get in touch

Central Europe Regional Leads

Jan Michalski
Partner
Central Europe GenAI Leader
jmichalski@deloittece.com

Simina Mut
Partner at Reff & Associates
Deloitte Legal,
Leader of Deloitte Legal Central Europe
smut@deloittece.com

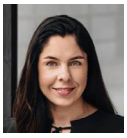
Gregor Strojin
Deloitte Legal Central Europe
AI Regulatory CoE Leader
gstrojin@deloittelegal.si

Albania

Ened Topi
Senior Manager
etopi@deloittece.com

Ina Cota
Manager
icota@deloittece.com

Baltics



Ruta Passos
Manager
rpassos@deloittece.com

Bosnia

Elma Delalic-Haskovic
Manager
edelalic@deloittece.com

Zerina Pacariz
Manager
zpacariz@deloittece.com

Bulgaria

Adelina Mitkova
Senior Managing Associate,
Deloitte Legal
amitkova@deloittece.com

Mila Goranova
Manager
mgoranova@deloittece.com

Croatia

Zrinka Vrtarić
Attorney at law in cooperation
with Deloitte Legal
zvrtaric@kip-legal.hr

Ratko Drča
Director
rdrca@deloittece.com

Czech Republic

Jaroslava Kracunova
Partner,
Deloitte Legal
jkracunova@deloittece.com

Jakub Holl
Director
jholl@deloittece.com

Hungary

Linda Al Sallami
Partner, Head of Banking, Finance & Capital Markets
lalsallami@deloittece.com

Daniel Nagy
Managing Associate, Deloitte Legal
dnagy@deloittece.com

Gergő Barta
Senior Manager
AI Risk & Compliance
gbarta@deloittece.com

Kosovo

Donika Ahmeti
Senior Manager
dahmeti@deloittece.com

Ardian Rexha
Senior Manager
Deloitte Legal
arrexha@deloittece.com

Poland

Ścibor Łapieś
Partner
slapies@deloittece.com

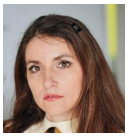
Tomasz Ciećwierz
Partner,
Deloitte Legal
tciecwierz@deloittece.com

PhD Michal Mostowik
Senior Managing Associate,
Deloitte Legal
mmostowik@deloittece.com

Romania

Andrei Paraschiv
Partner
anparaschiv@deloittece.com

Simina Mut
Partner at Reff & Associates Deloitte Legal, Leader of Deloitte Legal Central Europe
smut@deloittece.com



Silvia Axinescu
Senior Managing Associate
maxinescu@reff-associates.ro

Serbia

Miroslava Gaćeša
Director
mgacesa@deloitteCE.com

Stefan Ivic
Partner
stivic@deloittece.com

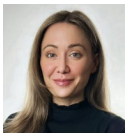
Stefan Antonic
Attorney-at-law in cooperation with Deloitte Legal
santonic@deloittece.com

Slovakia

Pavol Szabo
Senior Managing Associate
Deloitte Legal
pszabo@deloittece.com

Dagmar Yoder
Partner
Deloitte Legal
dyoder@deloittece.com

Slovenia



Ana Kastelec
Attorney at law,
Local Partner in Law Firm Deloitte Legal Reff – Branch in Slovenia
akastelec@deloittelegal.si

Lan Filipič
Director
lfilipic@deloittece.com

Ukraine

Mykhailo Koliadintsev
Manager,
Deloitte Legal
mkoliadintsev@deloittece.com

Dmytro Pavlenko
Partner
dpavlenko@deloittece.com

Authors

Christophe Crnkovic
Partner
FSI Assurance
ccrnkovic@deloitte.de

Max Weltersbach
Manager
FSI Audit & Assurance
mweltersbach@deloitte.de

Deloitte.