



ALWAYS-ON FINANCIAL SERVICES COMPLIANCE

How to stay one step ahead of financial services regulation today and tomorrow

nuix

TODAY'S CHAOTIC REGULATORY LANDSCAPE – SEEING THE OPPORTUNITY

Banks and other financial institutions create, process and store more personally identifiable data than ever before.

Today, financial services institutions operate in the most data-rich, regulated, and litigated sector. While financial institutions come in many shapes and sizes, there are essentially only two types:

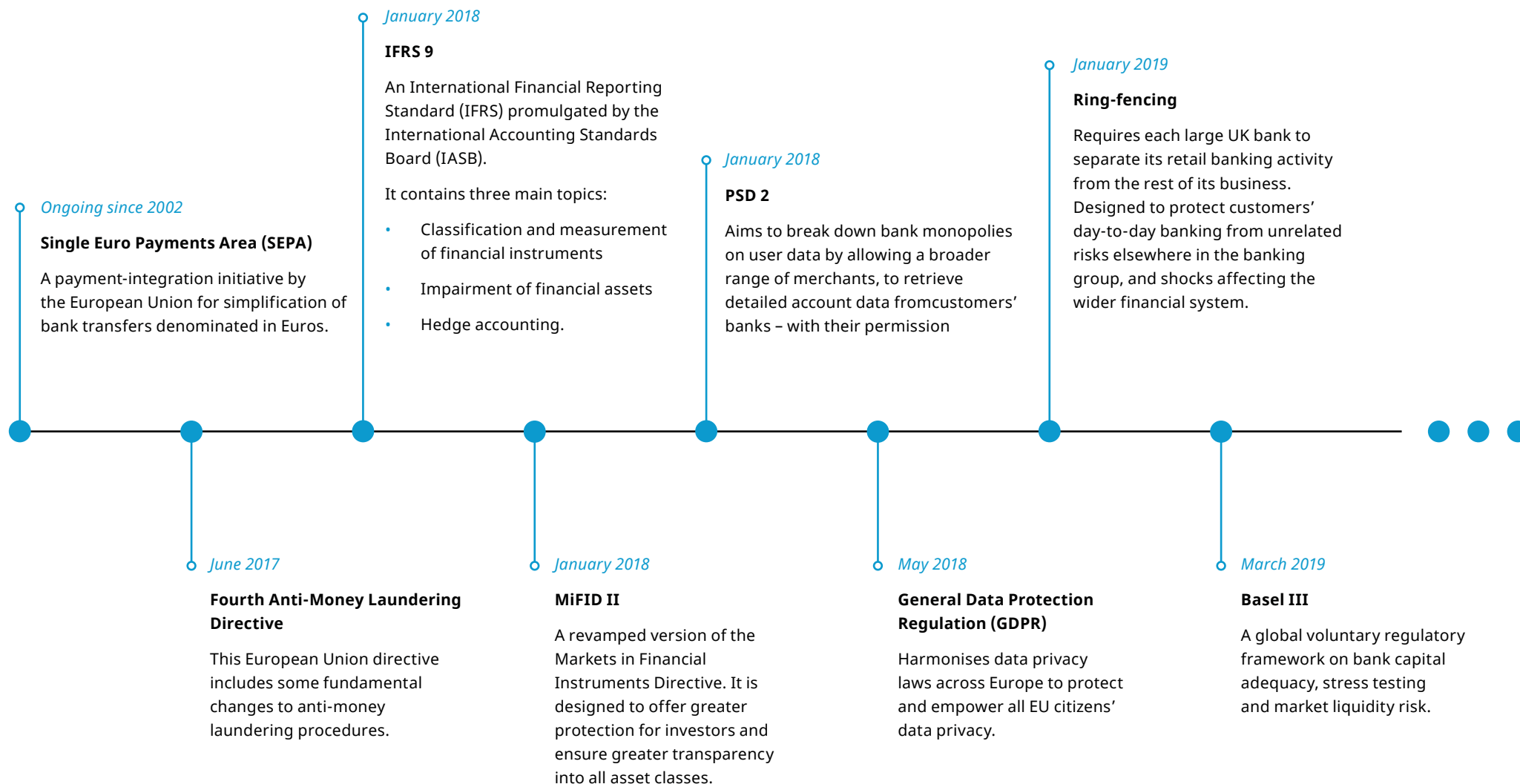
- Those proactively dealing with major regulatory investigations
- Those that soon will.

Failure or success relies on readiness and the ability to act fast. You need clear visibility into behavioural patterns and data streams. Often, clues within data remain invisible to internal investigative teams because the patterns or even the entire data streams are deliberately obscured from view.

It is a trying time for financial institutions as they implement the overlapping demands of so many regulatory frameworks. However, by adopting an always-on approach to information governance, you can streamline and reduce the cost of your compliance processes.



FINANCIAL REGULATIONS 2018-2019



THE EUROPEAN UNION'S FOURTH ANTI-MONEY LAUNDERING DIRECTIVE (AML IV)

WHERE DID IT COME FROM?

AML IV is designed to prevent illegally sourced income entering the global banking network.

The EU's fourth directive on money laundering and terrorist financing covers market manipulation, the trade of illegal goods, corruption of public funds, and tax evasion. It came into force on 26 June 2017.

WHAT YOU NEED TO KNOW

- The detailed due-diligence procedures on customers and prospects are mandatory.
- It's the responsibility of FS institutions to establish and maintain stringent group procedures for data protection and information sharing to prevent money laundering and terrorist financing.
- Client due diligence documents and supporting evidence must be stored for at least five years after the end of the business relationship or transaction.
- Employees and other agents involved in an organisation's AML activity must be regularly screened.
- Each firm must establish an independent audit function to assess the efficacy of its policies and procedures.

HOW NUIX SUPPORTS YOU

Structured data analytics can only identify anomalous activity, it cannot provide the insight your business needs to complete thorough due diligence or stop fraud.

Nuix can help you to put all transaction data, email, correspondence, text messages and phone calls into a single searchable index. You can review topics, discussions, transaction amounts, and critical keyword terms in a timeline to see changes or anomalies and detect issues before they become investigations. If you find an issue, Nuix can help identify the people, objects, locations, events and data sources that someone had access to and what they talked about, providing the investigative proof you need to stop the unauthorised activity and protect your organisation.

With the ability to uncover greater intelligence using analytics and machine learning, Nuix can provide insight from within and across cases, comprehensively monitoring user activity at the endpoint to draw the line between suspicion and proof.

To find out more about how Nuix keeps you in line with AML regulation – [click here](#).

HOW AML IV LOOKS TODAY



28 Countries



US and EU regulators imposed \$342 billion in fines since 2009



\$850 billion in profit loss for the top 50 global banks since 2008

THE MARKETS IN FINANCIAL INSTRUMENTS DIRECTIVE (MIFID II)

WHERE DID IT COME FROM?

The Markets in Financial Instruments Directive (MiFID II) is the European Union legislation designed to make European trading markets safer and more transparent. It looks to move a large part of over-the-counter trading onto regulated, electronic trading venues.

MiFID came into effect in the UK from November 2007 and was replaced by MiFID II in January 2018, which outlines a number of new requirements.

WHAT YOU NEED TO KNOW

- The legislation covers banks, brokers, exchanges, institutional investors, hedge funds and high-frequency traders.
- MiFID II affects trade in jurisdictions outside the EU. If a fund manager wishes to purchase an underlying product listed within the European Union, such as a Microsoft stock in New York which has been re-listed in the EU, it falls under MiFID II's scope, regardless of where the asset manager is based.
- MiFID II covers shares, bonds, units in collective investment schemes, and derivatives, as well as the venues where these instruments may be traded.
- It demonstrates a strong desire to remove phone trading in favour of regulated, electronic venues, where audit and surveillance trails are more accurate and easier to keep track of.
- It will completely overhaul the current market structure with its new and extended requirements relating to trading transparency.

HOW NUIX SUPPORTS YOU

Under MiFID II, Financial institutions are required to report more information on trades, with 65 fields mandated. This has resulted in the generation of petabyte-scale data.

With much greater responsibility sitting on the shoulders of asset managers, Nuix ensures compliance by providing complete visibility and reporting power over swathes of data.

This data must be stored for a minimum of five years, and requires next-level information governance to extract the data, but also report on it.

Nuix has the power to provide you with access to the broadest possible range of historical data on the question at hand and display it in real-time so you always know the state of current activity. Nuix can also help you dispose of expired data after those five years with full remediation capabilities.

To find out more about how Nuix can provide you with a compliance framework for MIFID II, which contextualises all data to provide you with the insight you need – [click here](#).

HOW MIFID II LOOKS TODAY



28 EU member countries



£1.50 fine per line of incorrect or non-reported data



65 reportable fields for data



Original source may include a mobile phone, a new or legacy call recording system or a cloud storage system



All transaction data must be stored for five years



Fines determined by FCA. Amounts will reflect the seriousness of the breach



Over 1.4m paragraphs of rules

GENERAL DATA PROTECTION REGULATION (GDPR)

WHERE DID IT COME FROM?

The General Data Protection Regulation (GDPR) is set to significantly restrict what has, until now, been largely ungoverned in the EU: the processing of personally identifiable information (PII) by those who are not the rightful owners of that data.

Focused on ensuring the privacy of all individuals within the European Union, it was announced on the 14th April 2016, and came into force on the 25th May 2018. GDPR replaces the Data Protection Directive.

WHAT YOU NEED TO KNOW

- Members of the public are now free, and encouraged, to report GDPR breaches to law enforcement. This means almost all companies in the EU are now subject to forensic data examination by the authorities.
- Applies to an enterprise established in the EU, or with EU customers, regardless of its location or the citizenship of the data subject.
- Organisations must implement measures to meet the principles of the GDPR's data protection by design and by default requirement.
- Provides EU citizens with a right of access and a right to erasure, otherwise known as right to be forgotten.

HOW NUIX SUPPORTS YOU

The scope of GDPR is global and executives are waking up to the fact their organisations, in the eyes of the law, are data processors and data controllers. Those carrying out unauthorised or careless data processing are now easily identifiable by the organisation or law enforcement.

Nuix provides the intelligence you need to identify, manage, and monitor the information you hold on any individual across all systems in the enterprise, so you can identify risky activities, locations or systems that need special attention. Sources include structure data, unstructured content, emails, instant messages, voicemails, call recordings, and anywhere you process customer or employee data.

It assesses risk using pattern recognition, and then maps data strings likely to be an issue back to a specific end point, system or other data source.

Nuix knows that effective GDPR compliance involves two processes: one for consumer-led enquiries such as data subject access requests and one for internal and external breach notifications.

With fines large enough to warrant significant prosecutions, betting on leniency from EU authorities is risking everything. Nuix solutions are trusted by regulators and legal teams worldwide to protect their systems from vulnerabilities.

HOW GDPR LOOKS TODAY



28 Countries



500 million citizens (in EU and overseas)



No cost to the citizen to make an EU subject request



72 hours to report breaches once detected



Up to 4% of global turnover at risk



\$5.3 billion estimated fines by 2021

To find out more about how Nuix can help with the production and redaction of data, to meet a subject's right to be forgotten – [click here](#).

PAYMENT SERVICES DIRECTIVE 2 (PSD2)

WHERE DID IT COME FROM?

The first Payment Services Directive (PSD1) was adopted in 2007 and created an EU single market for payments. Its aim was to establish safer and more innovative payment services across the EU, and it did so by making cross-border payments easier, more secure and more efficient.

The second Payment Services Directive (PSD2) is a different kind of change. Enforced on January 18th 2018, PSD2 caters to three fundamental demands of EU financial services customers: more choice, better deals and better customer service.

WHAT YOU NEED TO KNOW

- A cultural as well as technological shift, PSD2 paves the way for 'open banking', and ensures traditional banks are no longer the only choice for consumers looking for financial products.
- Designed to break the monopoly banks have over customer data, ecommerce giants such as Amazon can now take payments without a third party.
- Requires banks to open possibly their most valuable asset: their payments infrastructure. PSD2 sees customer data assets shared with third parties who now have the power to develop information, and payments services to customers.
- Organisations need to be aware of how the complexity of GDPR integrates with PSD2 activity.

HOW NUIX SUPPORTS YOU

PSD2 presents a data challenge not just for banks, but many commerce companies within the EU. An increasing number of transactions across multiple organisations means service providers need to transfer ever-increasing workloads of sensitive data, likely resulting in petabyte-sized databases in multiple languages.

Banks must know what they are sharing, with whom, and which data of other institutions they are using. This requires professional-grade eDiscovery and information governance tools.

The forensics-grade NuiX systems work in harmony with your existing data privacy program, helping you answer the following questions:

- Which data do I expose?
- Which data do I keep?
- Can I scale my security operations?
- Will my information governance approach scale?
- Can I interrogate obscure sources of data such as audio from my call centre?

For more information about how NuiX can help you thrive with PSD2, rather than just survive – [click here](#).

HOW PSDII LOOKS TODAY



28 EU member countries



Facebook has held a banking licence since 2017



Fines TBC

RING FENCING

WHERE DID IT COME FROM?

Coming into effect on 1st January 2019, ring fencing requires the largest UK banks to separate their core retail banking environment from their investment banking environment.

Arising from the 2008 financial crisis, ring fencing was initially introduced through the Financial Services (Banking Reform) Act 2013. Details of this regime are laid out in legislation passed in 2014, 2015 and 2016, and contains rules set by the Prudential Regulation Authority and the Financial Conduct Authority.

WHAT YOU NEED TO KNOW

- Business banking within larger companies may fall on either side of the ring fence.
- The legislation is designed to protect customers and their important day-to-day banking services from unrelated risks elsewhere in the banking group keeping them at arm's length from the repercussions of the wider financial system.
- Improves UK banking stability by increasing transparency and making issues easier to resolve. If either part of the ring fence fails, it can be mitigated without the need for a government bailout.
- As well as ensuring UK taxpayers do not have to support bailouts, ring fencing will mean fewer and less severe financial crises in the future, ultimately intended to benefit the UK economy.

HOW NUIX SUPPORTS YOU

In order to comply, banks need to first know exactly where assets are stored within internal systems, a number of these data repositories then may need to be moved inside or outside the ring-fence.

Nuix provides you the clearest picture on where your assets are, and what your data contains, so you can stay in control, and stay compliant.

Facing information risks means making informed decisions; the powerful Nuix engine searches complex data sources skipped by other platforms because of their complexity.

Network file shares, archives, collaboration systems, current and legacy email platforms, and cloud services across the enterprise are all considered so you know the correct assets are being kept on the right side of the ring fence. Nuix can also track these details at the communication level, identifying conversations and content sharing through the fence even from separate systems. We provide timeline and communication network analysis options to spot problems.

To find out more about how Nuix can help you prepare for Ring Fencing – [click here](#).

HOW RING FENCING LOOKS TODAY



Affects only large UK banks with three-year average of more than £25 billion in core deposits



Applicable if the bank offers:

- Deposits or other payments into an account
- Facilities to withdraw money or make payments from an account
- Overdraft facilities



ALWAYS-ON INFORMATION GOVERNANCE

The way organisations use and store consumers' data has changed. The financial institutions we trust with our hard-earned capital and investments must work even harder, to stay one step ahead of existing and upcoming regulation at all times.

Nuix's fundamental strengths in indexing and processing huge, complex data sets along with its built-in investigation capabilities, make it the first choice of professionals—whether investigating huge cases like the Panama papers or securing convictions on insider attacks.

For decades now, those with a need to know have relied on Nuix's unrivalled data insights to unlock answers hidden away deep inside the data which flows constantly through the arteries of financial institutions. Unlike generic big data solutions, standalone eDiscovery, or perimeter-focused cyber security, Nuix expertly copes with the complexity and diversity of the data these businesses deal with. It's also why all the world's leading financial regulators use Nuix.

Nuix finds the issues that have the power to break a business, then joins the dots so those dealing with these issues can make better decisions and act.

As personalised communication channels cause data volumes to grow at a compound rate of 24% each year (up to 40 zettabytes by 2020), Nuix's ability to see through huge data sets, is invaluable.

- Identify where data is stored and safely triage it for compliance
- Reduce your organisation's exposure to risk
- Minimise the impact of security incidents
- Identify and remediate private data at risk of being lost in a breach
- Avoid becoming the focus of international news headlines.

The organisations we trust with our wellbeing, financial independence and liberty – in roles such as defence, banking, and law enforcement – focus heavily on information governance.

- For them, only the most advanced capabilities will do. These organisations are Nuix customers.
- Nuix works for the professionals because they know our Total Data Intelligence approach unlocks their resources and helps them work smarter.
- With Nuix, we've already done the hard thinking about sensitive issues such as how to protect against insider threats by the time we reach you.

NUIX UP CLOSE

With its background in information governance and digital forensics, Nuix has more capabilities relevant to reducing cost and improving the quality of financial services compliance processes than any other solution.

Four powerful capabilities that will help you are deep insight, forensic clarity, horizontal scalability, and rapid diagnosis.

FORENSIC CLARITY

Nuix's approach is steeped in data forensics, making the handling of data a particular focus.

The advanced capabilities of the platform state with certainty whether data has been processed (copied, encrypted, compressed or deleted) helping eliminate time-consuming searches of data sources unlikely to yield results.

HORIZONTALLY SCALABLE

The architecture of the Nuix engine offers unparalleled speeds of up to 120 GB per processing core every 24 hours, and is linearly extensible to increase the search speed of other servers. A typical installation can get through terabytes a day, and even terabytes per hour is possible with the right hardware.

This ability to scale can mean the difference between compliance and non-compliance, particularly where corporate data is spread geographically and over thousands of devices.

RAPID DIAGNOSIS

Out-of-the-box acceleration techniques—such as scanning for the LUHN checksum commonly used by credit card issuers—mean

Nuix quickly eliminates noise as well as false positives, so you can focus on the real issues.

Nuix operates with zero delay, presenting initial findings during ingestion. Other technologies need to complete indexing before delivering results.

DEEP INSIGHT

Unlike many basic eDiscovery tools, Nuix comes pre-loaded with regular expressions for common data types – shortcuts to detect and alert searchers to likely areas for deeper dive enquiries.

In this way, Nuix focuses efforts on where your search results are more likely to be –avoiding application files for instance, which are not likely to hold useful insights, in favour of other file types more likely to yield results.

Forensic audits and data investigations use Nuix to illuminate the shadows in which financial services fraudsters and malicious insiders hide their exploits. Nuix seeks out the compliance failures which could bring a financial institution to the attention of regulators and makes investigations faster and more conclusive. Wielding this investigative power improves compliance and fraud-fighting ability and results in successfully litigating and negating insider threats.

Financial services institutions choosing Nuix have the power to delve deep into their data, look closely at how it is being used and detect anomalies and patterns faster to decipher connections and make better decisions. That's why financial professionals globally bank on the intelligence Nuix provides.



“We keep finding new ways to do things faster and smarter with Nuix. Every time we've invested in Nuix software, it has paid for itself before the year is out.”

BOB LEWIS MBE

Global Head of Cyber Forensics and eDiscovery Barclays


nuix

Nuix understands the DNA of data at enormous scale. Our software pinpoints the critical information organisations need to anticipate, detect and act on cybersecurity, risk and compliance threats.
To learn more visit www.nuix.com.

NORTH AMERICA

USA: +1 877 470 6849

EMEA

UK: +44 203 934 1600

APAC

Australia: +61 2 8320 9444