Securing the future:

Data security and governance in financial services

Research Report

Optalysys

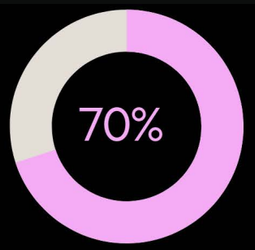
Foreword

Dr Nick New, CEO of Optalysys

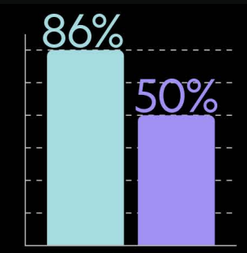
“Businesses today operate with copious amounts of data and are responsible for protecting it, whether that’s on behalf of stakeholders and partners or their own customers. Ensuring that data remains secure is a constant challenge, especially for financial services firms. Data security is no longer just a compliance issue — it is a strategic imperative for financial institutions.

The good news is that advanced privacy enhancing technologies can unlock data’s potential without compromising security. At Optalysys we are proud to be adopting a proactive, collaborative approach where financial institutions can not only safeguard their assets but also drive growth and innovation in an increasingly digital world. With this research we have been able to highlight the sometimes difficult choices that IT decision makers within these organisations have to face to ensure good data governance. We also know that the time to act is now — incoming regulations must be studied for compliance and new technologies must be investigated in order to ensure your business is fit for the future.”

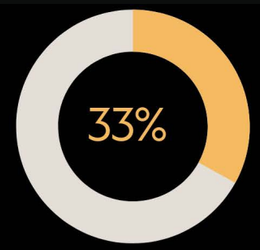
Key Findings



70% of IT decision-makers (ITDMs) believe growth is being constrained by challenges in securely handling data and adhering to evolving regulatory requirements.

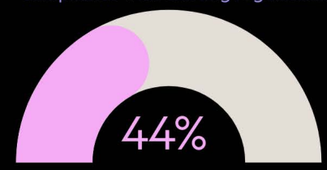


While 86% of ITDMs acknowledge the importance of data security, only 50% are confident in their organisation’s compliance with existing regulations.



Just 33% of respondents feel fully equipped to meet the stringent demands of DORA.

52% of ITDMs cite the high cost of implementing robust data security measures as a significant obstacle, alongside complexity and performance concerns.



44% of organisations have experienced data breaches or unauthorised access, underlining the sector’s persistent vulnerabilities.

39% of respondents report that data security constraints have hindered external collaboration, limiting opportunities for growth and innovation.

Emerging Privacy Enhancing Technologies (PETs) are being adopted to address these challenges:

52% exploring Confidential Computing

44% adopting Multi-party Computation

29% leveraging Fully Homomorphic Encryption (FHE)

FHE adoption is currently slow due to perceived complexity (57%) and high power consumption (47%). Innovations in silicon photonics show promise in overcoming these barriers, enabling more scalable and efficient data security solutions that align with regulatory requirements like DORA.

©2025 All Rights Reserved Optalysys Ltd

Introduction

Data security has always been a critical concern for the financial services sector. However, in the digital age, the stakes are higher than ever. With the rapid proliferation of sensitive data and increasingly sophisticated cyberattacks, organisations are under mounting pressure to safeguard information while adhering to stringent regulatory frameworks. The consequences of failure - ranging from significant breaches and regulatory fines to irreparable damage to customer trust - are severe.

At the same time, organisations recognise the untapped potential of their data as a driver of growth and innovation. Yet, strict compliance requirements and heightened data sensitivity often create a paradox: businesses must balance the need to protect their data with the desire to unlock its value.

This report from Optalysys examines the current state of data security in the financial services sector, the barriers organisations face, and the technologies and strategies they are adopting to address these challenges. The findings are drawn from an online survey of over 250 key IT decision-makers (ITDMs) across the UK, working within financial services. The report sheds light on the concerns of key decision-makers around data security and regulation.

Is data security restricting business growth?

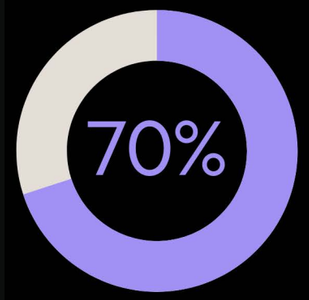
Our research reveals a significant tension between the need for better data security and the desire for business growth. A striking 70% of ITDMs in financial services organisations believe that growth is being jeopardised due to uncertainty about handling data securely and how regulations may impact business operations.

Despite a large majority of ITDMs (86%) acknowledging that data security is a concern for their organisation, only half (50%) are confident that their own organisation is compliant with data regulations. This highlights a concerning gap between awareness and readiness, particularly as financial services face a growing array of regulations, from the General Data Protection Regulation (GDPR) to the Digital Operational Resilience Act (DORA).

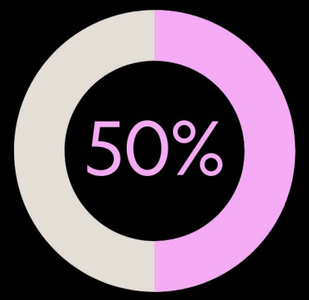
The data regulations a business needs to comply with depend on various factors, including the industry, geographic location, and the type of data processed. In the UK, GDPR applies to any organisation processing personal data of EU residents and covers a wide range of data protection rights and obligations, including data security and data breach notification.

While financial organisations have adapted to the requirements of regulations like GDPR over the years, and compliance is widespread, other regulations that have recently come into force, such as the Digital Operational Resilience Act (DORA) on 17th January 2025, are less well understood. Only one-third of respondents believed their organisation was fully prepared for DORA.

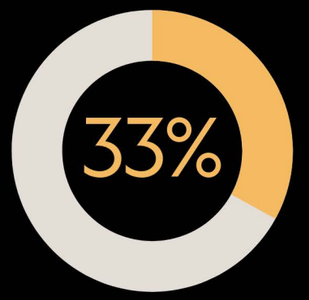
Key insights:



70% of ITDMs agree that their organisation's growth is being held back by data security.



Only 50% of ITDMs are confident that their organisations is compliant with data regulations.



While compliance with existing regulations like GDPR is well understood, only 33% of respondents believe their organisation is fully prepared for DORA.

What challenges do organisations encounter with data security?

Data is increasingly being described as the most valuable asset that an organisation owns. It drives innovation, improves decision-making, and when utilised correctly can lead to competitive advantage. The inherent value of data is also well known by malicious actors who seek to exploit weaknesses in data handling and security to access troves of potentially sensitive data.

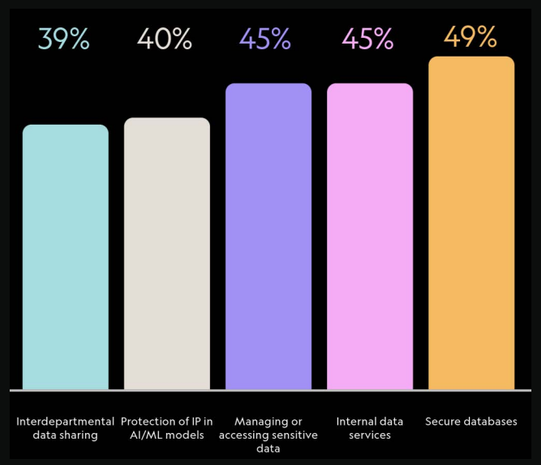
This is perhaps why **high costs** associated with data security measures was cited as the **most prevalent constraint (52%)** when it comes to ITDMs securing data within their organisation. Even with the expenditure and resources that organisations are dedicating to keeping data secure, 44% have still encountered data breaches or unauthorised access.

This is broadly in line with national average where research conducted by the UK government found that half of businesses (50%) reported having some form of cyber security breach or attack in the previous 12 months.

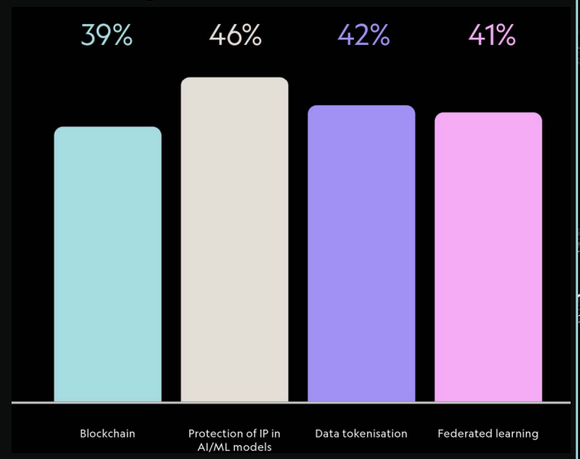
Over one-third (39%) of all ITDMs have experienced being unable to collaborate with external organisations due to data security constraints. By breaking down silos both inside and outside of company data ecosystems, financial services organisations can inform a system of best practices that benefit the industry at large.

However, financial institutions remain cautious about sharing their machine learning (ML) models with partners, regulators, competitors or adjacent businesses due to concerns over revealing proprietary algorithms. Technologies such as encrypted compute could address some of these concerns. For example, a bank could securely share a credit risk assessment model with a fintech partner to develop a joint lending product, without exposing the underlying algorithm.

Where do ITDMs *have* challenges with data security?



Where do ITDMs *anticipate* challenges with data security?



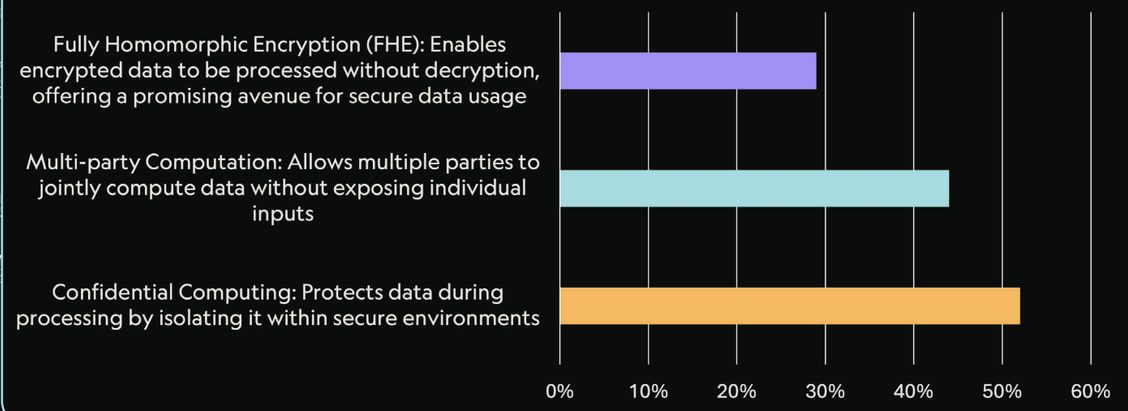
How are organisations planning to address data challenges and what solutions are on the horizon?

Financial services organisations will continue to grapple with data security and governance as businesses continue to shift to increasingly digital environments. It is therefore unsurprising that respondents highlighted cybercrime (50%) as one of the most significant challenges they face to keep data secure. Despite even the biggest global organisations investing large sums into security budgets, it appears no target is too big or too safe when faced with sophisticated cyber criminals. With financial services firms controlling swathes of potentially sensitive customer and proprietary information, ITDMs know that their systems present an obvious target for malicious attackers.

For instance, banks aim to offer personalised services but are constrained by the need to use anonymised or aggregated data to comply with privacy regulations. Emerging technologies, such as Fully Homomorphic Encryption (FHE), could bridge this gap. By processing data while it's encrypted, financial institutions can analyse individual-level customer data without ever exposing sensitive information. This could enable banks to offer tailored investment recommendations based on a customer's unique spending habits and financial goals, all while keeping their data encrypted and secure.

Organisations of all sizes must try to mitigate data stolen by third parties and also prepare for unintended data leakage. **49% of ITDMs reported that leaking private data** is a key challenge when managing data security followed closely by **regulatory compliance (43%)**. Data inadvertently being lost or leaked, potentially by a business' own employees due to poor technical systems or organisational processes is evidently a concern. Insider threats, even without malicious intent, can pose a threat to businesses as can simple user error and system misconfigurations.

How are organisations planning to address data challenges within the next two years



While FHE adoption is currently low due to perceived complexity (57%) and power consumption concerns (47%), its potential is immense. Our findings indicate that there is no clear frontrunner when it comes to identifying a solution to overcome data security challenges. Each different PET has its advantages and drawbacks, and its adoption hinges on many competing factors.

Complexity of adoption (50%) was the most common reason for ITDMs to have not integrated the solutions. **Cost (48%) and performance (47%)** were almost as much of a hindrance. Levels of risk aversion and the availability of skilled staff to implement new technology and solutions are always going to differ between businesses. Our findings do indicate that providers of such solutions may have to work more closely with ITDMs to help them understand and navigate any perceived complexities with the technology.

If ITDMs knew with complete certainty that their organisation's data was fully secure and could be processed without compromising that security, **half of all organisations (49%)** would bestow more freedom on their data analysts. This suggests that roles within financial services organisations where handling sensitive data is paramount are subject to too much oversight out of fear of data being mishandled. These firms may also be more likely to commercialise their data (48%) and collaborate more closely with other departments within the same organisation (48%).

Key insights:

- The biggest constraint ITDMs face to enact data security measures are the high costs
- Over one-third (39%) of all ITDMs have experienced being unable to collaborate with external organisations due to data security constraints

Spotlight on DORA: The next frontier in regulation

The Digital Operational Resilience Act (DORA) is a landmark regulation introduced by the European Union as part of its Digital Finance Strategy. Aimed at strengthening the cybersecurity and operational resilience of financial institutions, DORA is designed to address the growing sophistication and frequency of cyberattacks that threaten the stability of the financial sector. The regulation sets comprehensive requirements for institutions to ensure they can withstand, respond to, and recover from ICT-related disruptions, marking a pivotal moment in financial regulation.

A majority of respondents in the research **(80%) believe that DORA marks the beginning of greater regulatory scrutiny over data in use, a sentiment echoed by industry professionals**. One participant noted, "*I think the DORA Act is a key step in improving the financial industry's ability to respond to cyber threats. In the past, many of our security measures focused on data protection and compliance, but as cyberattacks become more complex and frequent, traditional defence methods are no longer sufficient.*"

Another respondent reinforced the importance of embracing this change, stating, "*I agree that DORA will lead to more regulatory scrutiny, but it is nothing for the industry to be concerned about. It is something we should all embrace.*"

One of the most significant shifts introduced by DORA is its emphasis on data in use, sensitive information that is actively being processed, rather than simply stored or transmitted. While traditional cybersecurity measures have focused on securing data at rest (stored) and data in transit (being transmitted), DORA explicitly requires institutions to design and implement policies that protect data during active use.

This focus stems from the evolving nature of cyber threats. Attackers increasingly target data when it is most vulnerable — while it is being processed — making comprehensive in-use protection a key priority for compliance.

To address these challenges, DORA mandates that financial institutions implement measures to ensure the availability, authenticity, integrity, and confidentiality of data across all states, whether at rest, in transit, or in use. For example, the Regulatory Technical Standards (RTS) outlined in DORA require financial institutions to design, procure, and implement ICT policies and tools that support resilience, continuity, and security for critical systems.

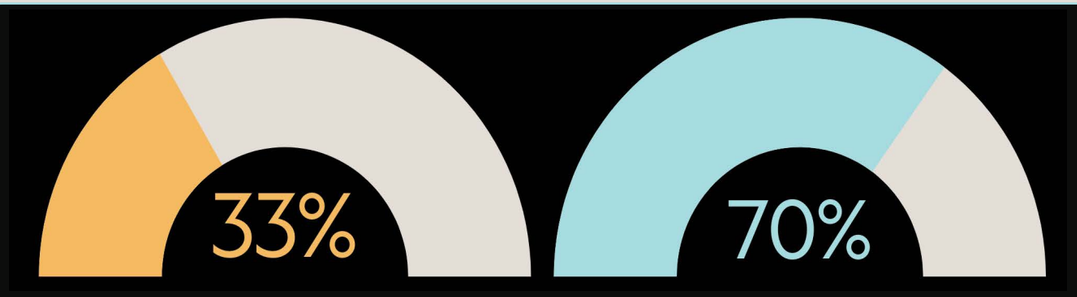
Despite widespread recognition of DORA's importance, the findings reveal a stark gap in readiness:

- Only one-third (33%) of respondents believe their organisation is fully prepared to meet DORA's stringent requirements
- 70% of respondents believe that data security and governance regulations are holding back growth

This lack of preparedness could lead to uncertainty and hesitation, especially among financial services organisations that handle sensitive customer data.

Advanced technologies like Fully Homomorphic Encryption (FHE) are gaining traction as potential solutions for meeting DORA's in-use data protection requirements. FHE allows computations to be performed on encrypted data without needing decryption, addressing a key vulnerability in traditional security frameworks.

However, while FHE provides a promising layer of protection, it alone cannot fulfil the comprehensive standards set by DORA. The regulation calls for a holistic approach, embracing advanced technologies that enhance security across all data states, including in use and establishing comprehensive procedures and policies that align with DORA's standards.



Only one-third (33%) of respondents believe their organisation is fully prepared to meet DORA's stringent requirements.

70% of respondents believe that data security and governance regulations are holding back growth.

Fully Homomorphic Encryption (FHE)

Fully Homomorphic Encryption (FHE) is an advanced quantum-resilient cryptography method that allows encrypted data to be processed without ever needing to be decrypted. This capability makes FHE uniquely suited to solving data security challenges, particularly for organisations in the financial sector that handle highly sensitive data. By allowing secure computation of sensitive data, FHE can enable financial institutions to unlock the full value of their information without compromising security.

While often referred to as the most valuable global asset, the actual value of data is only realised when it is used to make informed decisions – be it improving operational efficiency, developing products or understanding societal trends. Organisations increasingly seek ways to optimise this value through new technologies such as AI, ML and data collaboration. However, valuable data often remains siloed within organisations and the most valuable data is usually the most sensitive.

Today, most encryption methods protect data only during storage or transit. To process data, it typically needs to be decrypted first, exposing it to risks. This presents a dilemma – protecting data and limiting its use or utilising the data and increasing exposure to breaches. FHE solves this dilemma by enabling secure, encrypted data processing, allowing financial organisations to maximise the value of their data while ensuring its security.

Innovation in Fully Homomorphic Encryption (FHE)

FHE enabled by silicon photonics — using light to transmit data — offers a solution that promises to make FHE more scalable and efficient. Unlike traditional electronic systems, which are reaching their limits in handling the demands of FHE, silicon photonics is built to support large-scale, secure data processing.

Optalysys is at the forefront of making FHE scalable and efficient through silicon photonics. By leveraging light rather than electricity to transmit data, its technology addresses performance and power consumption concerns. Optalysys is working to create the world's first silicon photonics chip specifically designed for FHE.

For financial organisations, FHE powered by silicon photonics represents a fundamental shift in how sensitive data is handled and shared. One of the most significant use cases is interbank data sharing, where sensitive financial data must often be decrypted and processed on external systems. This practice introduces security risks and slows down collaboration, often taking weeks or months to complete. With FHE, these barriers are removed. Banks can securely share and process encrypted data in real-time, streamlining operations while maintaining confidentiality.

Additionally, as AI technologies like Large Language Models (LLMs) and Generative AI become more deeply ingrained in our everyday lives, the need for secure data processing has never been greater. These AI systems rely on vast amounts of unencrypted data, leaving sensitive information vulnerable to breaches. FHE provides a way to process encrypted data directly, enabling secure AI.

In financial services, joint machine learning (ML) initiatives between organisations are often hindered by the need to protect sensitive data. Secure AI allows multiple organisations to collaboratively train models without sharing raw data. For example, multiple banks could collaboratively develop a fraud detection model by training on encrypted datasets, enhancing security while benefitting from shared insights.

The report's findings indicate a strong awareness of FHE's potential. **More than half (53%) of respondents are aware that FHE can support data security in secure AI, and 51% know it can support processing always-encrypted data.** By addressing the complexity and power consumption challenges that have hindered its adoption, Optalysys is paving the way for scalable, efficient, and secure data processing.

53% of respondents are aware that FHE can support data security in secure AI.

51% are aware that FHE can support processing always-encrypted data.

In Conclusion

Data security is a paramount concern for financial institutions, as it underpins their ability to innovate, grow, and maintain customer trust. Our research underscores the pressing need for organisations to:

- Prioritise compliance with new regulations like DORA
- Address cost, complexity and performance concerns associated with advanced PETs
- Embrace innovative solutions like FHE to unlock data's potential without compromising security
- By adopting a proactive, collaborative approach to data governance, financial institutions can not only safeguard their assets but also drive growth and innovation in an increasingly digital world

To learn more about how Optalysys can help secure your organisation's future, get in touch with our team today: info@optalysys.com

©2025 All Rights Reserved Optalysys Ltd