Financial Services
IT Strategy:

Key trends shaping the industry

kerv

Executive Summary

Financial services firms are under immense pressure. Whether navigating tightening regulations, preparing for audits, integrating new acquisitions, or protecting data across global jurisdictions, IT is now at the centre of strategic growth, risk management, and regulatory survival.

But for mid-sized firms, the path forward isn't always clear. Evolving frameworks like DORA, expanding compliance obligations, and increasing demand for real-time reporting mean that traditional IT approaches no longer cut it, but without a full in-house tech team, many businesses struggle to set a clear strategic direction.

This eBook distils key trends shaping financial services IT today, based on frontline insight from Kerv's industry specialists gathered whilst fulfilling fractional CTO roles for financial firms. From AI's growing role in regulatory compliance, to proactive strategies for M&A readiness, to cross-border operational resilience, you'll find practical guidance on what to prioritise and how to futureproof your firm.

Whether you're expanding internationally, facing regulatory scrutiny, or simply looking to optimise IT investments, this guide will help you take a more strategic, confident approach to IT planning and delivery.

The new mandate for financial services IT

For financial services firms, the IT function is a business-critical driver of compliance, performance, and growth.

In an industry shaped by complex regulatory obligations, global operations, and ever-increasing cybersecurity risk, the pressure on internal tech teams has never been higher. At the same time, smaller and mid-sized firms are expected to meet the same standards as global players, despite having much smaller resources at their disposal.

From navigating regulatory requirements, to managing security and service delivery across jurisdictions, firms must now demonstrate resilience, transparency, and control at every turn.

To achieve this, the firms leading the way are using IT strategy as a competitive advantage. They're responding proactively to regulatory evolution, building long-term roadmaps, leveraging AI to automate compliance processes, and integrating acquisition targets faster and more smoothly than ever before.

At Kerv, we work with financial services clients every day to tackle these challenges head-on, from health checks and compliance reviews to 24/7 managed services and strategic advisory at board level.

This guide brings together those insights to help your organisation think beyond short-term fixes, and towards IT that actively enables regulatory readiness, innovation, and sustainable growth.

Proactive security by design

Embedding Protection and Proactive Response into Financial IT

For financial services firms, security must be an intrinsic part of every IT decision. With rising cybercrime, tightening regulatory expectations, and increasing cross-border data exposure, organisations need to embed protection from the ground up and maintain constant vigilance across their digital estate.

Security starts with architecture

A “security by design” approach is now widely regarded as best practice. This ensures every layer of the IT environment, from endpoint to cloud, is designed with both security and compliance in mind. Whether deploying Microsoft 365, managing hybrid cloud platforms, or onboarding third-party tools, controls and safeguards should be built in from the outset, not bolted on later.

This is particularly critical for regulated firms operating without a full-time CTO or dedicated compliance team. Bringing in sector-specific knowledge through internal hires or trusted advisors can help align infrastructure with regulations. For smaller firms, fractional security leadership (e.g. CISO/CTO support) is an increasingly popular option for closing gaps in oversight and governance.

Kerv regularly supports financial services firms in embedding this “security by design” mindset, whether through technical assessments, project design input, or leadership support at board level.

24/7 monitoring is the key to resilience

With most data breaches occurring outside of office hours, round-the-clock monitoring and rapid incident response are becoming baseline expectations. Regulatory pressure is growing for firms to not only protect systems but to demonstrate their ability to detect, respond, and recover in real time.

Many firms now adopt a dual-layered model: partnering with a Security Operations Centre (SOC) for 24/7 threat detection while maintaining internal or third-party support for triage and remediation. This approach delivers operational assurance while helping boards and audit committees meet evolving supplier risk obligations.

Regulatory resilience

Meeting compliance goals today and tomorrow

The regulatory environment for financial services is only set to accelerate. From DORA to GDPR expectations, financial firms must prove they're proactively evolving their compliance approach. Organisations are expected to demonstrate continual improvement, cross-jurisdictional alignment, and a robust strategy for what's next.

Compliance is no longer a one-off milestone

Today's regulators expect more than a tick box approach. Firms must show that they are evolving in line with regulatory expectations, proactively identifying risks, closing gaps, and preparing for what's next. Questions like "What's changed since your last audit?" or "How are you improving supplier oversight?" are fast becoming standard.

Yet, many organisations still tackle these challenges reactively, rushing to meet deadlines rather than building the structures that enable long-term compliance.

The goal is resilience, not just readiness

Resilient firms take a proactive stance, embedding compliance into operations, governance, and IT strategy. They invest in monitoring systems, define clear roles for reporting, and take a cross-functional approach to meeting obligations across jurisdictions.

In this context, technology plays a supporting role, but it's strategy that turns compliance into a source of trust and differentiation.

This is where external specialists can add value. Kerv works with financial services firms to interpret shifting regulations, develop cross-border compliance strategies, and build governance frameworks that scale with the business.

From reactive updates to credible evidence

Being compliant is not enough - you must be able to demonstrate it. That means putting in place the right audit trails, reporting tools, and decision-making documentation.

Firms without a specialist in-house compliance function can benefit from fractional expertise - advisory input that translates technical measures into audit-ready narratives. For larger firms, an external viewpoint can highlight inconsistencies or blind spots in multi-region estates and help realign efforts with regulatory expectations.

Smarter ecosystems

Vendor Management, Data Strategy & IT Integration

Modern financial services firms rely on increasingly complex digital environments. Dozens of applications, platforms, and partners underpin day-to-day operations, from document management and client communication to compliance tracking and reporting. But this growing reliance on digital tools comes at a cost: without clear integration and oversight, complexity can stifle performance and undermine regulatory confidence.

Fragmented tools create fragmented oversight

Without a clear strategy, critical functions can quickly become siloed. Business-wide tools like Microsoft 365, Citrix, and iManage or FS-specific platforms such as DealCloud and eFront, may work well in isolation, but without thoughtful integration, firms often face duplicate costs, overlapping functionality, inconsistent user experiences across teams or regions, and limited reporting insights due to disconnected data.

Siloed systems and poor visibility translate to increased risk, and slower responses to both market and regulatory demands.

Vendor complexity requires active oversight

It's common for financial firms to work with a mix of infrastructure providers, SaaS vendors, resellers, and support partners. These partners play a critical role in delivering against organisational objectives. However, unclear roles and inconsistent handovers can create gaps in accountability and potential compliance risk.

A clear vendor strategy, backed by documented SLAs and coordinated support models, is essential to ensure resilience, security, and value for money. Partners who offer multi-vendor integration support can act as a bridge, helping ensure that your business, not your toolset, drives decision-making.

A cohesive ecosystem for agility, control, and compliance

Whether preparing for expansion, integrating new acquisitions, or reducing operational risk, a smart, well-integrated ecosystem is the foundation of a future-ready IT strategy.

Financial firms that succeed in today's environment are those that treat IT ecosystems as strategic assets. That means:

- Aligning platforms and tools with business objectives
- Consolidating where needed, integrating where valuable
- Ensuring consistent security, access controls, and user journeys

At this stage, firms often benefit from external support from expert IT partners who can help assess how systems are interacting (or not), identify consolidation opportunities, and develop roadmaps that make infrastructure, SaaS platforms, and data environments work together effectively.

M&A readiness

Using it to accelerate integration, reduce risk & unlock value

In financial services, where compliance, security, and system integrity are paramount, the success of an M&A deal increasingly hinges on how well technology is assessed, planned, and integrated. Yet too often, IT is treated as an afterthought, brought into the process only after key decisions are made.

M&A is a test of both technology and leadership. A well-planned, technically sound integration can accelerate returns, reduce compliance headaches, and deliver a unified platform for future growth.

IT must have a seat at the table from day one

Bringing technology considerations into early-stage discussions can uncover risks, reveal hidden costs, and surface opportunities to unlock long-term value. For example, identifying outdated infrastructure, cyber vulnerabilities, or incompatible platforms during due diligence helps deal teams avoid disruption and set realistic timelines for integration.

Firms assessing an acquisition target should seek clear answers to questions such as:

- What systems and platforms are in use, and how well are they maintained?
- Are they compatible with your current estate, or likely to increase complexity?
- What will it take to integrate them securely, cost-effectively, and at pace?

This clarity is vital not only to protect the deal, but to plan for the first 100 days post-close.

Making integration faster, smoother and safer

Once a deal is approved, speed and alignment become critical. Delays in system consolidation, user onboarding, or policy harmonisation can erode confidence and productivity. **Effective integration means:**

- Consolidating core systems such as Microsoft 365
- Migrating and securing sensitive data
- Aligning device policies and access controls
- Ensuring consistent, scalable user experiences across entities

Cultural and operational misalignment can also introduce risk. Whether it's differing attitudes to BYOD, remote working, or access governance, these nuances must be addressed early to ensure the newly merged business runs smoothly.

Designing with divestment in mind

M&A strategy doesn't always stop at acquisition. For some firms, the goal is to prepare for future divestment or spin-out. In these cases, building modular, segmentable IT infrastructure from the outset is key. This means designing user access, data ownership, and network structures to support future separation, minimising cost, risk, and disruption when the time comes.

AI, automation & the future of financial IT

Driving smarter, faster, more secure operations

In a sector where precision, efficiency, and accountability are non-negotiable, AI and automation are becoming critical pillars of modern IT strategy. For financial services firms, the challenge is how to adopt these technologies in a way that drives genuine impact without compromising on governance, compliance, or control.

From manual to machine-optimised

Despite the digital progress made in recent years, many firms still rely on manual, time-intensive processes that slow teams down and increase the risk of error. From regulatory reporting and client onboarding to access reviews and audit preparation, automation has the power to remove friction and refocus skilled staff on higher-value tasks.

Firms are beginning to see the benefits of automating routine compliance workflows and standardising repetitive processes to reduce operational risk.

The goal isn't to replace people, but to give them better tools. Automation, done right, enables faster responses, lower overheads, and more scalable service delivery.

Real-world AI in action

AI, too, is already proving its value in financial services. Take the example of a UK-based wealth management firm that developed a custom AI model to interpret regulatory documentation. Instead of manually reviewing spreadsheets and PDFs, staff can now ask a plain-language question - such as “What’s the current rule on reporting client interest?” - and receive a clear, auditable response within seconds.

Tools like Microsoft Copilot are also entering the mainstream. Embedded into everyday applications like Outlook, Word, and Excel, Copilot empowers firms to speed up administrative tasks such as drafting and summarising investment reports, analysing regulatory updates or audit histories, or translating board reports and communications on demand.

With the right governance in place, these tools can significantly increase productivity and reduce operational lag, especially in firms with limited internal IT or compliance bandwidth.

Balancing innovation with oversight

But AI is not plug-and-play. Adopting it responsibly means putting clear controls in place from the outset. That includes:

- Defining acceptable use cases based on role and risk
- Ensuring outputs can be reviewed, explained, and audited
- Building confidence in the data sources that underpin results

Kerv works with clients to shape and support responsible AI enablement, offering guidance on use case design, platform configuration, and security controls that align with sector expectations.

Belasko: Building a Resilient and Scalable IT Ecosystem

Belasko, a rapidly growing provider of corporate and fiduciary services, had big ambitions: to scale their operations across Guernsey, Jersey, the UK, and Luxembourg while maintaining consistent service quality and regulatory alignment. But legacy infrastructure and siloed systems were holding them back.

The Challenge

With only 30 staff at the time, Belasko faced a trio of pressures familiar to many mid-sized financial firms:

- **Scalability bottlenecks:** Their on-prem, multi-tenant setup made it difficult to grow efficiently or onboard new team members quickly.
- **Mounting compliance demands:** Meeting evolving expectations from regulators were becoming increasingly complex without a more segmented and secure network.
- **Operational fragility:** Their systems lacked the flexibility to support modern working practices and posed continuity risks, particularly during disruptive events like COVID-19.

These challenges echoed many of the themes covered in this guide, from the need for strategic, scalable IT ecosystems to the importance of security-first design and compliance readiness.

Case study (Continued): belasko.

The Solution

Kerv worked closely with Belasko to define and deliver a transformation strategy grounded in resilience, integration, and regulatory confidence.

- **Cloud-first foundation:** Belasko's environment was migrated to Microsoft Azure, unlocking secure scalability while meeting cross-border compliance obligations.
- **Zero-downtime implementation**: Business continuity was prioritised throughout the transition, ensuring no disruption to service.
- **Security by design:** Cyber security was embedded from the outset, with Microsoft Defender, a 24/7 managed SIEM (powered by Microsoft Sentinel), Citrix for secure desktops, Mimecast for email protection, and Webroot for endpoint defence.
- **Standardised IT onboarding:** Tailored laptop builds were rolled out across all locations, streamlining device management and ensuring consistent user experiences.
- **Proactive education:** Bespoke cyber security training empowered employees to stay alert and responsive to threats.

The Results

Belasko's IT is now a platform for growth, not a barrier to it.

- **Rapid scaling:** From 30 to 130+ employees across four jurisdictions, without compromising service or security.
- **Stronger compliance posture:** A future-ready infrastructure now aligned with regulators' expectations across multiple regions.
- **Operational resilience:** Cloud-first architecture ensured seamless performance and secure remote working during COVID-19 and beyond.
- **Strategic alignment:** With regular board-level input and ongoing technical reviews from Kerv, Belasko's IT continues to evolve in lockstep with their business goals.

Future-ready IT for financial services

From M&A readiness to AI integration, cross-border compliance to 24/7 resilience, the demands on financial institutions are growing. But with the right partner, these challenges become catalysts for smarter, more secure, and more scalable operations.

At Kerv, we combine deep sector expertise with technology leadership to help financial services firms modernise with confidence, balancing innovation with compliance, and growth with governance.

Ready to align your IT with your business goals? Let's talk about how we can help you build an IT and data ecosystem that supports long-term success.

☎ 0330 1078009
✉ hello@kerv.com
www.kerv.com