



THE RESILIENCE PLAYBOOK:

How Private Markets Firms Can Build Stronger, Smarter Operations

BETTER OUTPUTS,
BETTER OUTCOMES_

WHY RESILIENCE NOW?

EXECUTIVE SUMMARY

In today’s fast-changing and increasingly regulated financial landscape, operational resilience has become a defining advantage. However, many private market firms are still relying on outdated, fragile processes that leave them vulnerable. The Resilience Playbook is a practical guide for forward-thinking operational leaders, COOs and CFOs who want to build smarter, more secure, and future-ready fund operations.

This eBook explores why resilience matters now, drawing on market data, expert interviews, and real-world insights. We examine the risks of overreliance on spreadsheets, the operational blind spots that come with legacy workflows, and the pressure points introduced by growth, compliance demands, and talent churn. Through conversations with qashqade’s CPO and CTO, you’ll get a behind-the-scenes view of the thinking that shaped the platform. You’ll discover why features like audit trails, role-based access, and security by design weren’t added later, but built in from the start to meet the real-world demands of resilient fund operations.

You’ll also find a focused self-check to assess how resilient your fund operations really are, especially around areas like waterfall calculations and key data workflows. It’s designed to help you spot risks like single-person dependency, version confusion, or reliance on fragile spreadsheets. From there, we offer clear, practical steps to strengthen what matters most: Things like adding audit trails, automating sensitive calculations, and shifting critical workflows to a secure SaaS platform.

The bottom line? In private markets, there’s no room for fragility in core processes. The firms building operational resilience now - where it counts - will be the ones leading tomorrow. And with LPs and regulators sharpening their focus, resilience is fast becoming a core pillar of due diligence.

CONTENTS

INTRO WHY RESILIENCE NOW?	2
POSITION PAPER FROM FRAGILE TO FUTURE PROOF	3
EXPERT INSIGHT A CONVERSATION WITH OUR CPO	6
OPERATIONAL RESILIENCE SELF-CHECK	10
EXPERT INSIGHT INTERVIEW WITH CTO	12
CONCLUSION	16



“Relying on spreadsheets in today’s private markets is like building a house on sand”

Oliver Freigang
CEO & Co-Founder

FROM FRAGILE TO FUTURE-PROOF: WHY PRIVATE MARKETS NEED RESILIENCE

Private markets have seen extraordinary growth over the past decade. According to Blackrock, global private markets are estimated to grow from \$13 trillion to more than \$20 trillion by 2030, reflecting increased interest from institutions and a growing number of high-net-worth individuals. However, while capital flows have surged, the operational foundations supporting this growth have remained surprisingly fragile. For many firms, spreadsheets, manual workflows, and disconnected systems still form the backbone of their day-to-day operations.

This reliance on legacy tools creates significant risks. Errors in spreadsheets are common. Studies indicate that over 88% contain mistakes ranging from simple data entry errors to flawed formulas. In the high-stakes world of private markets, even minor mistakes can lead to costly consequences, from incorrect investor reporting to compliance breaches. Moreover, spreadsheets offer limited

transparency and traceability, making audits complex and time-consuming. Data security also suffers when sensitive information is stored on local drives or shared via email, exposing firms to potential breaches.

“Relying on spreadsheets in today’s private markets is like building a house on sand,” says Oliver Freigang, CEO of qashqade. “As firms grow and regulations tighten, the risk of operational failure increases exponentially. Building resilient, scalable infrastructure is no longer optional. It’s a strategic imperative.”

Operational resilience is under the spotlight as regulatory pressure intensifies. The EU’s Digital Operational Resilience Act (DORA) mandates that firms not only ensure their systems can withstand and recover from disruptions but also embed resilience into every aspect of their operations. This shift isn’t just technological - it’s also cultural. As qashqade’s CTO, Paul Foley, explains, “DORA is forcing

private market firms to rethink resilience. Not as a bolt-on to compliance, but as a core principle that informs infrastructure, processes, and mindset. It requires moving from a reactive posture to a proactive, preventative one, adopting modern infrastructure that’s secure by design, continuously monitored, and capable of rapid response. Operational resilience today is as much about strategic thinking and preparedness (including regular DR exercises) as it is about systems and tools.”

But while mindset and strategic planning are essential, they must be backed by robust, modern infrastructure. Without the right systems in place, even the most resilient intentions can fall apart, often with serious consequences. Our **summer survey** captured numerous real-world examples of costly errors and their ripple effects. Respondents reported losses including missed distribution payments going back over a decade, significant financial

misstatements affecting tax positions, miscalculated fees, and even client relationships irreparably damaged due to operational mistakes. One respondent shared a case where a 10% error in equity rollover calculations resulted in a \$20 million overpayment during a deal; a costly and stressful mistake.

Other examples included errors causing liquidity issues, overpayments to investors, inaccurate performance attributions leading to wrong investment decisions. Beyond the financial impact, many highlighted the reputational damage and stress these errors caused, affecting both clients and internal teams. These pressures affect people as much as processes. Around half of survey participants indicated they use automation and technology primarily to reduce errors and gain peace of mind.



For us resilience is
not a buzzword.
**It's the backbone
of sustainable
growth in private
markets.**

The sustainability of private markets operations hinges on addressing these risks head-on. Automation improves data integrity and reduces human error. Modern platforms facilitate real-time collaboration and eliminate black-box data silos. Together, these capabilities allow firms to meet regulatory demands, protect investor confidence, and safeguard their reputations.

Industry voices increasingly emphasize this shift. As consulting firms note, portfolio companies in private markets create value when they can withstand operational disruptions and continue serving their markets, underscoring why operational resilience has become a top priority for private equity.

At qashqade, we built our platform precisely to solve these challenges. By automating complex calculations, ensuring robust audit trails, and embedding security by design, we enable private market firms to transition away from fragile spreadsheet-driven processes towards future-proof operations.

“For us resilience is not a buzzword. It's the backbone of sustainable growth in

private markets,” adds Oliver Freigang. “Technology is the enabler that finally allows firms to reduce errors, increase transparency, and secure their operations for the long term.”

The future of private markets depends on operational resilience. Firms that take on a mindset change, adopt smarter technology and rethink their infrastructure now will be better positioned to navigate the complexities ahead, avoiding costly errors, protecting reputations, and delivering the transparency their investors demand. The time to move from fragile to future-proof is here.

A portrait of Gregor Kreuzer, a man with short brown hair, wearing a dark suit and white shirt, smiling slightly. The background is a dark blue gradient with faint, stylized line graphs and data points in a lighter blue color. The quote text is overlaid on the lower left of the image.

“We built qashqade to be bespoke.
Not an off-the-shelf template, but a
platform designed specifically for the
realities of private markets.”

Gregor Kreuzer
CPO & Co-Founder

A CONVERSATION WITH OUR CPO. DESIGNED FOR RESILIENCE

LET'S START AT THE BEGINNING: WHY DID YOU CREATE QASHQADE IN THE FIRST PLACE?

When you strip private markets down to their core, the most important question is: who gets what. And yet, in a multi-trillion-dollar industry, that question was often being answered with the help of ... spreadsheets.

I was convinced there had to be a better way, something purpose-built that could handle complex waterfall calculations without the fragility, opacity, and manual risk of Excel. At one conference, an industry veteran told me flat-out that it was impossible to build such a tool. As a physicist, I took that as a challenge.

At its heart, qashqade is a highly specialized calculator. One that can control, understand, and trace every single input and logic step behind even the most intricate calculations.



WHAT GUIDED YOUR DESIGN PHILOSOPHY WHEN BUILDING QASHQADE?

We built qashqade to be bespoke. Not an off-the-shelf template, but a platform designed specifically for the realities of private markets. Every decision came back to one principle: fit for purpose.

But “fit for purpose” isn’t just about functionality, it’s about resilience. From

day one, we designed the platform so it could absorb change without breaking: whether that’s adapting to new fund structures, regulatory shifts, or a team reshuffle. By building flexibility and transparency into the core architecture, we’ve ensured that qashqade isn’t just a tool that works today. It’s one that will keep working when conditions change tomorrow.

CAN YOU SHARE A CHALLENGE EARLY ON THAT SHAPED THE PLATFORM?

Two words: data and flexibility. Everyone in this industry wants something slightly different. That diversity of needs became the pattern for our design. qashqade had to handle variation without breaking, and it had to ensure that no matter how data was structured, the calculations remained reliable.

WHAT DOES ‘RESILIENCE’ REALLY MEAN IN THE CONTEXT OF PRIVATE MARKETS OPERATIONS?

Resilience means that the bumps in the road don’t push you off the road. In private equity, that means if someone leaves the team, the knowledge doesn’t leave with them. If a new fund launches, you don’t reinvent the wheel. And if an investor calls you late at night, it doesn’t cause a heart attack - or a divorce.

HOW DO YOU BALANCE ROBUST SECURITY WITH USABILITY?

By never stopping to ask: what is necessary? Security and usability naturally pull in opposite directions, but by questioning assumptions constantly, we find the middle ground where the platform is both safe and efficient.

EXPERT INSIGHT

WHAT TOP THREE FEATURES CONTRIBUTE MOST TO RESILIENCE?

- 1 **Immutable history:** Results stay tied to their inputs and logic. They cannot be altered.
- 2 **Audit and change tracking:** Every modification is logged and recoverable.
- 3 **Unified operations:** Everything lives in one tool, accessible from anywhere.

AND A 'SMALL' FEATURE THAT MAKES A BIG DIFFERENCE?

There's no single magic switch. True reliability comes from invisible layers working together. But if I had to choose, it's that the information stays with the platform, not with the individual user.

HUMAN ERROR IS A MAJOR RISK IN PRIVATE MARKETS. HOW DOES QASHQADE MITIGATE THIS?

Two ways: first, by helping users find errors through transparency; and second, by reducing repetitive work through automation and standardization (so mistakes are less likely in the first place).

WHAT ROLE DO DATA TRANSPARENCY AND TRACEABILITY PLAY IN RESILIENCE?

Operational resilience is really about continuity. The more transparent the data, the less dependent you are on individual people or fragile processes. In qashqade, results are stored in a way that they can be cleaned up, but never changed. That history - and the ability to share it - ensures continuity. And when automation frees up time, teams can focus on innovation, which is perhaps the strongest form of resilience.

WHAT ADVICE WOULD YOU GIVE TO FIRMS RELYING ON SPREADSHEETS?

It starts with a mindset shift. Ask yourself why you work the way you do and whether it's truly the best way forward. Moving away from spreadsheets isn't just a technology decision; it's an operational transformation.



WHERE WILL THE RESILIENCE CONVERSATION GO IN THE NEXT 2-3 YEARS?

Resilience will move from being an internal operational goal to a market-wide expectation. As interconnections between firms deepen, the impact of one organisation's failure will ripple further and faster. The conversation will shift

toward ensuring that entire ecosystems, not just individual firms, can withstand shocks. That means greater emphasis on shared standards, interoperability, and transparency, so that resilience is baked into how the industry operates as a whole.

WILL RESILIENCE BECOME PART OF LP DUE DILIGENCE?

Indirectly, yes. LPs are asking more about processes, tools, and responsibilities. The answers reveal a lot about a GP's resilience.

WHAT EMERGING TRENDS WILL SHAPE THE FUTURE OF FUND OPERATIONS AND RESILIENCE?

Technologies like blockchain, advanced recovery and backup strategies, and multi-platform integrations will all play a role. The key will be using them to make resilience inherent - built into the process, not bolted on.

88%

Operational resilience is at risk when using spreadsheets. Studies show 88% of spreadsheets contain errors.

1%

In private markets, even a 1% discrepancy can mean millions in lost capital, misallocated fees or regulatory missteps threatening operational resilience.

60%

To keep errors in check, over 60% of respondents of a recent **qashqade survey** rely on a second set of eyes to review their work, a human failsafe.

45%

In a recent qashqade survey, more than 45% of respondents are now ready to use specialist automated tools wherever possible, signaling a shift toward smarter, more scalable ways of safeguarding accuracy and operational resilience.

HOW RESILIENT IS YOUR OPERATIONS STACK?

Answer **Yes** or **No** to the questions below and see where your risk really lies.

PROCESS VISIBILITY & MAPPING

Do you have a documented view of your end-to-end fund operations process, including dependencies, tools used, and ownership?

- Yes
- No

Why should you care?
Unmapped processes are where surprises and failures live. You can't strengthen what you can't see.

TEAM REDUNDANCY & KNOWLEDGE SHARING

If your key operations person left tomorrow, could someone else pick up their work without disruption?

- Yes
- No

Why should you care?
Institutional memory should live in your systems, not in someone's head.

OPERATIONAL RESILIENCE SELF-CHECK

CONTROLS, ACCESS & AUDITABILITY

Do your systems offer clear version control, role-based permissions, and audit trails for sensitive workflows?

- Yes
- No

Why should you care? You can't afford blind spots when regulators, LPs, or internal teams need answers fast.

WORKFLOW RESILIENCE & SCALABILITY

Have you pressure-tested your processes for growth (e.g., added more funds or deals to test impact)?

- Yes
- No

Why should you care? Growth shouldn't expose cracks, your workflows should scale without stress.

AUTOMATION & INFRASTRUCTURE

Are critical calculations (like waterfalls) handled in a secure, automated platform, not Excel files?

- Yes
- No

Why should you care? SaaS systems reduce human error, increase transparency and confidence in outputs.

Scoring

- **5 Yes:**
You're ahead of the curve. Keep refining.
- **4 Yes:**
Solid foundation, but room to strengthen.
- **3 or fewer Yes:**
It's time to invest in resilience.

KEY TAKEAWAY

5 steps to make your operations more resilient



Map process dependencies (where are points of failure)



Check single-person risk



Add controls & visibility (role-based, logs, versioning to fix blind spots)



Stress-test workflows (simulate growth e.g. by adding more deals) to discover hidden weaknesses



Shift to automated systems (move key computations e.g. waterfalls to a secure SaaS platform)



“Security by design isn’t a checkbox.
It’s cultural.”

Paul Foley
CTO

INTERVIEW: WHAT SAAS DOES THAT SPREADSHEETS CAN'T.

LET'S START WITH THE BASICS. WHAT DOES "SECURITY BY DESIGN" MEAN TO YOU AS A CTO?

Security by design means thinking about risk from the very beginning, not as an afterthought. It's like this: even in the Garden of Eden, telling people not to eat the apple wasn't enough. You'd need access control, monitoring, and escalation paths before things go wrong.

If you take that metaphor further, a security-minded architect would've recognized that while good users might follow the rules, bad actors (or even uninformed users) might not. The risk would be modeled: unauthorized access to the apple tree. And from that, you'd introduce controls: gated access to the garden, rights and privileges around the tree, perhaps alerting at the perimeter. Notice: we're still not discussing how the tree works. The focus is entirely on risk and

mitigation, long before the system is even in development.

In practice, this means designing systems with failure and bad actors in mind. We map how the system will be used, how it might be misused, and how to defend against it. I'm a fan of risk frameworks like PASTA because they start with business outcomes and align security decisions accordingly.

Security by design isn't a checkbox. It's cultural. If you're not thinking about threats at the design stage, you're not building resilience, you're just hoping nothing goes wrong.

YOU'VE SAID SECURITY IS A MINDSET, NOT A CHECKLIST. HOW DOES THAT SHOW UP IN HOW QASHQADE IS BUILT AND OPERATED?

At qashqade, security starts with a clear question: What outcomes are we

safeguarding and from which threats? It's not just about technology; it's about trust. And that must be owned across the business, not just by IT.

We embed that mindset in four ways:

- 1. Culture first:** Security is everyone's business. Our teams are encouraged to see client trust as part of their job description. That mindset beats any policy.
- 2. Proof through audit:** We hold a SOC 2 Type II certification, which means our controls aren't just written, they're independently verified. Policies are reviewed regularly and shaped by input from across the company.
- 3. Simulating real-world risk:** We run red team exercises and disaster recovery drills that turn theory into experience. These sessions surface practical insights and sharpen our response capabilities.

- 4. Empowering ownership:** Security isn't something handed down, it's something our people lead. When regulation and risk evolve, our teams don't just react; they anticipate, adapt, and drive qashqade forward as a trusted partner.

When security becomes part of how you work (not just what you document) that's when resilience becomes real.

MANY FIRMS STILL USE SPREADSHEETS TO MANAGE INVESTOR DATA. WHAT'S THE RISK IN THAT MODEL?

Spreadsheets are good for quick analysis, not for running fiduciary-grade operations. Using Excel to model a private markets LPA is like trying to build a skyscraper with a Swiss army knife.

EXPERT INSIGHT

Key risks include:

- **Security:** Spreadsheets get emailed, cloned, and modified. Every copy is a new attack vector. No access controls, no audit trail.
- **Integrity:** Excel's VBA code mutates silently across machines. Six months later, you don't know what code is running or if it changed.
- **Resilience:** There's no version control, rollback, or CI/CD pipeline. One overwritten file can bring operations to a grinding halt.

SaaS gives you what Excel can't: centralized governance, role-based access, real-time monitoring, and resilient infrastructure. It's not just more efficient, it's fundamentally more secure and scalable.

WHAT STEPS HAS QASHQADE TAKEN TO ENSURE INFRASTRUCTURE AND DATA RESILIENCE, ESPECIALLY FOR DISASTER RECOVERY OR BREACHES?

We made a strategic decision to move our platform to Azure. Not because our old stack was broken, but because

we wanted to scale with confidence and deliver a truly world class service.

Here's how that plays out:

Data-first risk management:

In any crisis, we're not worried about rebuilding servers, we're focused on restoring data. That's why we align everything around two core metrics:

- **RTO (Recovery Time Objective):** how quickly we can restore services
- **RPO (Recovery Point Objective):** how much data, if any, could be lost

Azure's continuous backup capability allows us to restore to any point in time within our retention window, eliminating surprises like "last night's backup failed."

Geo-redundancy & invisible failover:

Backups are replicated across regions, and Azure's infrastructure includes built-in patching, hardware repair, and multi-zone failover. This gives us resilience most teams couldn't build alone, without increasing headcount. (It's worth noting: we keep client data in the region they specify, even if broader redundancy is technically available.)

Elastic scaling & performance under load:

We scale compute and storage resources dynamically. That means even under peak demand, our performance holds and in most cases we don't need to pre-provision hardware.

Security built into the platform:

- Data is encrypted in transit and at rest, using customer-specific keys
- Role-based access control ensures least privilege down to the resource level
- We extend Microsoft's 24/7 threat monitoring, pen testing, and compliance coverage into our own stack

This is the advantage of modern SaaS infrastructure: resilience isn't something we add, we're not retrofitting resilience, it's baked into the platform. That lets our team focus on innovation, not firefighting.

HOW IS REGULATION - LIKE DORA - SHAPING WHAT CLIENTS EXPECT FROM TECHNOLOGY PARTNERS?

Regulations like DORA don't just define compliance, they clarify expectations. Clients now ask: "What guarantees do you offer, and how can you prove them?" Regulation turns that question into something tangible.

From Ambiguity to Accountability

Standards like DORA demand measurable practices:

- We define and test our RTO and RPO thresholds, not just once, but regularly
- We run full recovery drills, not just server failovers
- We assess third-party vendors with the same scrutiny as our internal systems

It's not about checking boxes, it's about demonstrating operational discipline.

EXPERT INSIGHT

Regulation as an Accelerator

Good regulation doesn't slow us down, it aligns us with what clients value:

- Transparent recovery commitments
- Scheduled audit reports (like SOC 2)
- Documented vendor oversight

The C-Suite Role

Our job as leaders is to translate regulatory demands into clear commitments and then back them up with proof. Regulation isn't creating new client needs; it's just spotlighting the ones that already mattered.

YOU'VE SPOKEN ABOUT THE DIFFERENCE BETWEEN BEING SECURE AND FEELING SECURE IN THE PAST. CAN YOU EXPLAIN THAT?

Feeling secure is walking your dog at night in a Swiss forest. It's quiet. Peaceful. But you're surrounded by wild animals and hunters. Meaning you're not secure, you're just unaware of the risk.

In IT, you might have great policies and smart people. But:

- Do you test your defences?
- Do you simulate real-world attacks?
- Do you verify if policies are followed?

Without evidence, you're just hoping. We pair tools like SAST/DAST with red team simulations and DR exercises. Security means knowing the body armor works, not just owning it.

“

Feeling secure is walking your dog at night in a Swiss forest. It's quiet. Peaceful. But you're surrounded by wild animals and hunters.

WHAT'S A RESILIENCE FEATURE FIRMS OFTEN OVERLOOK, BUT THAT YOU BELIEVE WILL BECOME ESSENTIAL?

Supply chain resilience.

Too often, vendor conversations stop at "Do you do DR?" Instead, they should start there. Ask: What did you test? How do you test it? What were the outcomes? In other words, it's time to shift from a compliance mindset to a capability mindset – from feeling safe to actually being safe.

The next evolution in resilience is predictive. Most firms have a SIEM (Security Information and Event Management system) in place, but few are leveraging its full analytical power. With the rise of AI (especially multi-agent models and external threat intel feeds) SIEMs are evolving from passive monitors into predictive engines. The next step is to correlate data across third parties, model weak points, and forecast threats before they surface.

That's a resilience capability many firms haven't yet considered but soon won't be able to ignore.

ONE LAST QUESTION. IF YOU COULD GIVE ONE PIECE OF ADVICE TO A PRIVATE MARKETS' COO OR CTO STILL USING EXCEL FOR CRITICAL PROCESSES, WHAT WOULD IT BE?

If you're still running sensitive workflows in Excel: lucky you. You're standing at a point where you can drive meaningful change. You can modernize processes to reduce your company's IT risk profile, make a positive contribution to the company security stance and reduce your company's risk due to human error.

And isn't that what any of us want in the COO/CIO or CTO role – to innovate, reduce risk, increase productivity and to help our organization achieve its full potential.

I'll leave you with a thought, a quote, something that I believe speaks to the C suite in general – Jack Welch (former General Electric CEO) said it best "Change before you have to."

CONCLUSION

BUILDING RESILIENCE FOR THE FUTURE OF PRIVATE MARKETS

Operational fragility is no longer just a risk, it's a barrier to growth, compliance, and sustainability in private markets. As this ebook has highlighted, firms relying on spreadsheets, manual workflows, and siloed systems expose themselves to costly errors, regulatory scrutiny, and operational blind spots. The stakes are too high, and the pace of change too fast, for old approaches to persist.

Building resilience requires more than just new tools; it demands a fundamental mindset change. Firms must move from reactive, manual firefighting to a proactive culture that prioritizes continuity, transparency, and scalability at every level. This shift from seeing resilience as a compliance checkbox to embedding it as a strategic priority, is what will enable private market firms to navigate increasing complexity and regulatory pressure with confidence.

The future demands infrastructure designed for continuity, scale, and

security. Tools that embed resilience at their core. qashqade is not simply a nice-to-have upgrade; it represents the foundational technology platform that private market firms need to transform their waterfall calculation operations and confidently meet tomorrow's challenges. By automating complex calculations, maintaining transparent audit trails, and reducing single-person dependencies, it enables firms to build operational muscle and regain control.

As we have seen with our fund administrator clients, the combination of expert fund administration and smart technology unlocks new levels of efficiency and reliability. Together, they move fund operations beyond compliance towards true operational excellence, empowering firms to scale smarter.

KEY TAKEAWAYS TO REMEMBER:

- Operational fragility is no longer acceptable in a competitive, regulated private markets landscape.
- Building resilience starts with a mindset change: Shifting from reactive to proactive, from manual to automated, and from fragile to future-proof.
- Firms need tools and platforms that ensure operational continuity, scalability, compliance, and data security.
- qashqade is the resilient infrastructure that future-ready private market firms depend on to reduce risk and unlock growth.
- Those investing in operational resilience today (both in mindset and technology) will be the market leaders of tomorrow.

NEXT STEPS TO START BUILDING RESILIENCE NOW:

- Take the operational resilience self-check if you skipped it, to identify whether you need to act.
- **Book a demo** to see how qashqade can transform your fund operations and bring resilience to life.
- Take one resilience step this quarter. For example, shift a critical waterfall calculation to qashqade's platform and build your foundation from there.

The time to move from fragile to future-proof is now. The firms that do, starting with a mindset shift and supported by the right technology, will not only survive but thrive in the complex, evolving world of private markets.

THE RESILIENCE PLAYBOOK



CONTRIBUTORS:

Oliver Freigang
CEO & Co-Founder

Gregor Kreuzer
CPO & Co-Founder

Paul Foley
CTO

contact@qashqade.com

