Beyond ERP:

Fostering trust in data, systems, and processes

PwC's 3rd SEE CFO Compass Survey

March 2026

Table of contents

1	Executive summary	03
2	Building the research: scale and scope	06
3	Control environment and system integration	12
4	Digital resilience and cybersecurity	24
5	Adoption of AI	35
6	About the survey	44

1

Executive summary

3rd SEE CFO Compass Survey: It comes down to trust

Three years into the SEE CFO Compass, **we've seen the conversation shift—from cost, to speed, to something more fundamental: trust.** Trust in the data behind decisions. Trust that systems will hold under pressure. Trust that the people overseeing AI truly understand what it's doing.

This year's survey findings reveal a paradox at the heart of finance in South-East Europe. Organisations are closing their books in five days yet burning out their teams to get there. They're exploring AI agents while half their workforce has never been trained to use such. They're investing in new ERPs while a third still carry out reconciliations in spreadsheets. Cybersecurity is on every agenda, yet 0% are investing in business continuity and disaster recovery. The ambition is real. The foundations aren't always there to support it.

But here is what makes this moment different from last year, or the year before: **finance leaders are no longer pretending the gap doesn't exist.** They're naming it—in their survey responses, in their priorities, in the way they talk about transformation. They're choosing certainty over speed, ecosystems over monoliths and upskilling before upgrading.

The road forward isn't a sprint. It's an act of honest construction—building controls that scale, data architectures that hold, teams that can govern what they adopt, and digital resilience that can't be achieved through funding alone. The organisations that get this right won't just have a modern finance function. They'll have one that survives. In a market where regulations and technology shift fast, **trust is more than a competitive advantage. It's what holds the business together.**

Petko Petkov

Partner
SEE Risk Assurance Services Lead
CEE Digital Identity Lead

When we first launched the SEE CFO Compass Survey, the main theme was about cost—the cost of transformation, the cost of compliance, the cost of keeping up. That conversation has moved on.

Today, **the question for finance leaders is no longer just how to move faster**, but **how to ensure that people trust the ground they're building on**. More than half of the surveyed CFOs are integrating AI agents into core finance operations, yet the organisations pulling ahead aren't necessarily the earliest adopters. These are the organisations investing equally in explainability, data governance and the human judgement that no algorithm should replace.

In a region where tax rules shift between fiscal years and businesses are replacing ERP systems with fit-for-purpose platforms, speed alone is no longer a competitive advantage. The real differentiator is integrity at speed.

Stefan Milenkov

SEE CFO Compass Survey Lead

Senior Manager,

Capital Markets & Accounting Advisory Services, Finance Function Transformations

One thing came through loud and clear in this year's survey: **the real bottleneck to transformation isn't technology—it's the people**. Adapting workforce competences to automation and digital tools is now the top priority and the reasoning is clear. You can implement the most sophisticated system or AI solution, but if your teams aren't ready for it, the investment doesn't pay off.

Beyond talent, organisations are working to get the fundamentals right—integrated systems, consistent data structures, robust control environments, minimal cyber-related risks, rolling cash-flow forecasts and improved planning and budgeting processes.

ERP modernisation remains high on the agenda, but the mindset in the SEE region has shifted. Relying on a single ERP isn't always possible or practical. Instead, companies are moving towards combinations of state-of-the-art, purpose-built solutions that offer flexibility and address specific business needs, regulatory requirements and compliance frameworks. That's the spirit we're seeing across the board.

2

Building the research: scale and scope

Creating value for CFOs, businesses and society

1. Find clarity amidst change

CFOs need clarity more than ever. The CFO Compass examines macroeconomic factors, actual practices, investment priorities and capabilities across the SEE region. The survey combines results with information gathered directly from finance leaders to help them anticipate market and business trends rather than simply respond to them.

2. Knowledge that empowers your choices

Our clients trust us to deliver solid expertise and sound judgement, grounded in real-world experience. Each survey edition enhances our grasp of the CFO agenda, boosting our ability to align our insights with our clients' sectors and operating models.

3. Insights that shape the market

Our purpose is simple yet powerful: To build trust in society and solve important problems. By presenting clear findings to the market, the CFO Compass helps create a stable business environment and promotes transparency. This approach ensures we remain a trusted partner, facilitating meaningful discussions within the finance community.

Creating value for CFOs, businesses and society

1. Understand Market Dynamics

CFOs need clarity more than ever. The CFO Compass examines macroeconomic factors, actual practices, investment priorities and capabilities across the SEE region. The survey combines results with information gathered directly from finance leaders to help them anticipate market and business trends rather than simply respond to them.

2. Competence Leader

Our clients trust us to deliver solid expertise and sound judgement, grounded in real-world experience. Each survey edition enhances our grasp of the CFO agenda, boosting our ability to align our expertise clients' sector and operating model.

3. Give Back Value to Society

Our purpose is simple yet powerful: To build trust in society and solve important problems. By presenting clear findings to the market, the CFO Compass helps create a stable business environment and promotes transparency. This approach ensures we remain a trusted partner, facilitating meaningful discussions within the finance community.

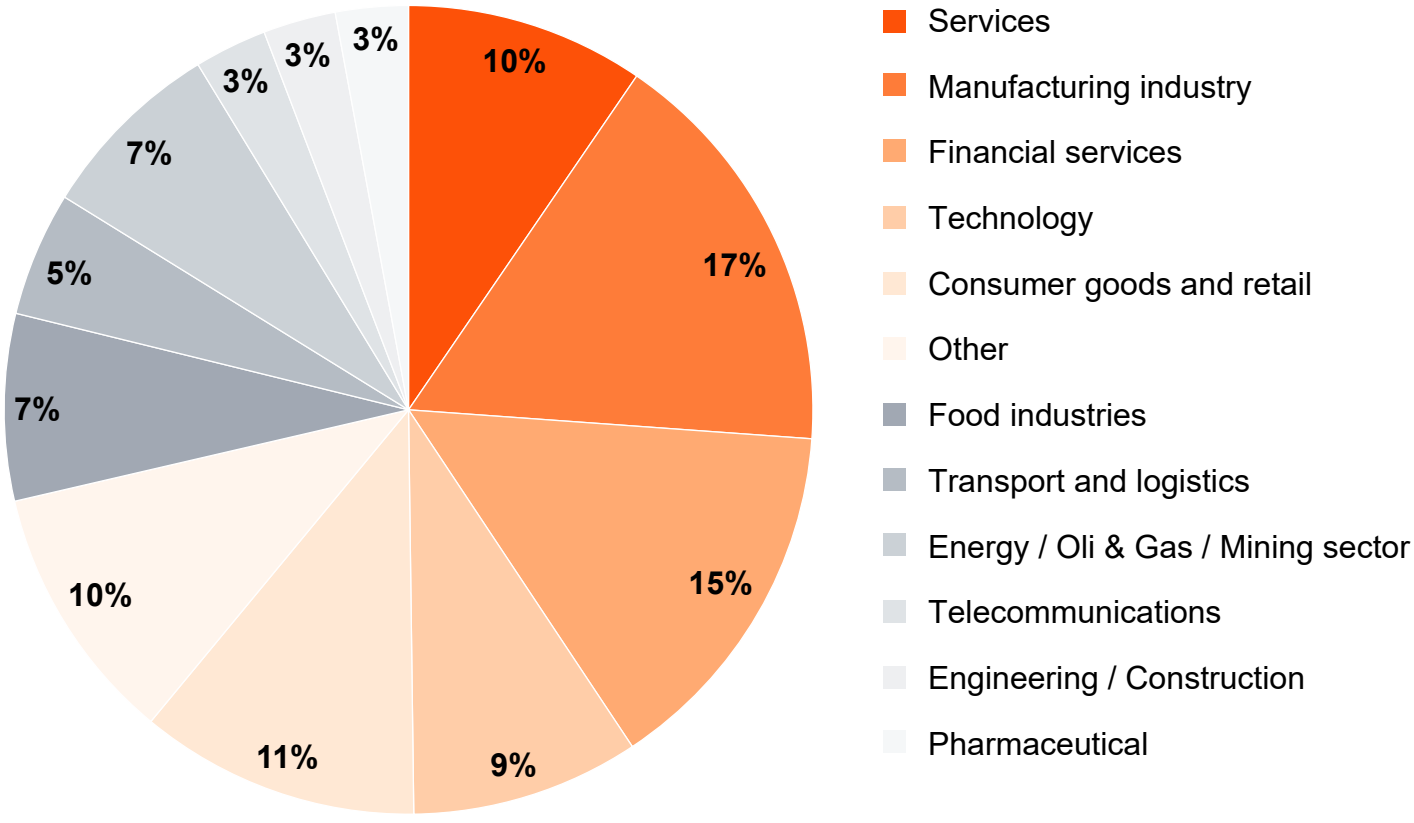
About the participants

Over 230 participants: Organisations from over **15 industries**

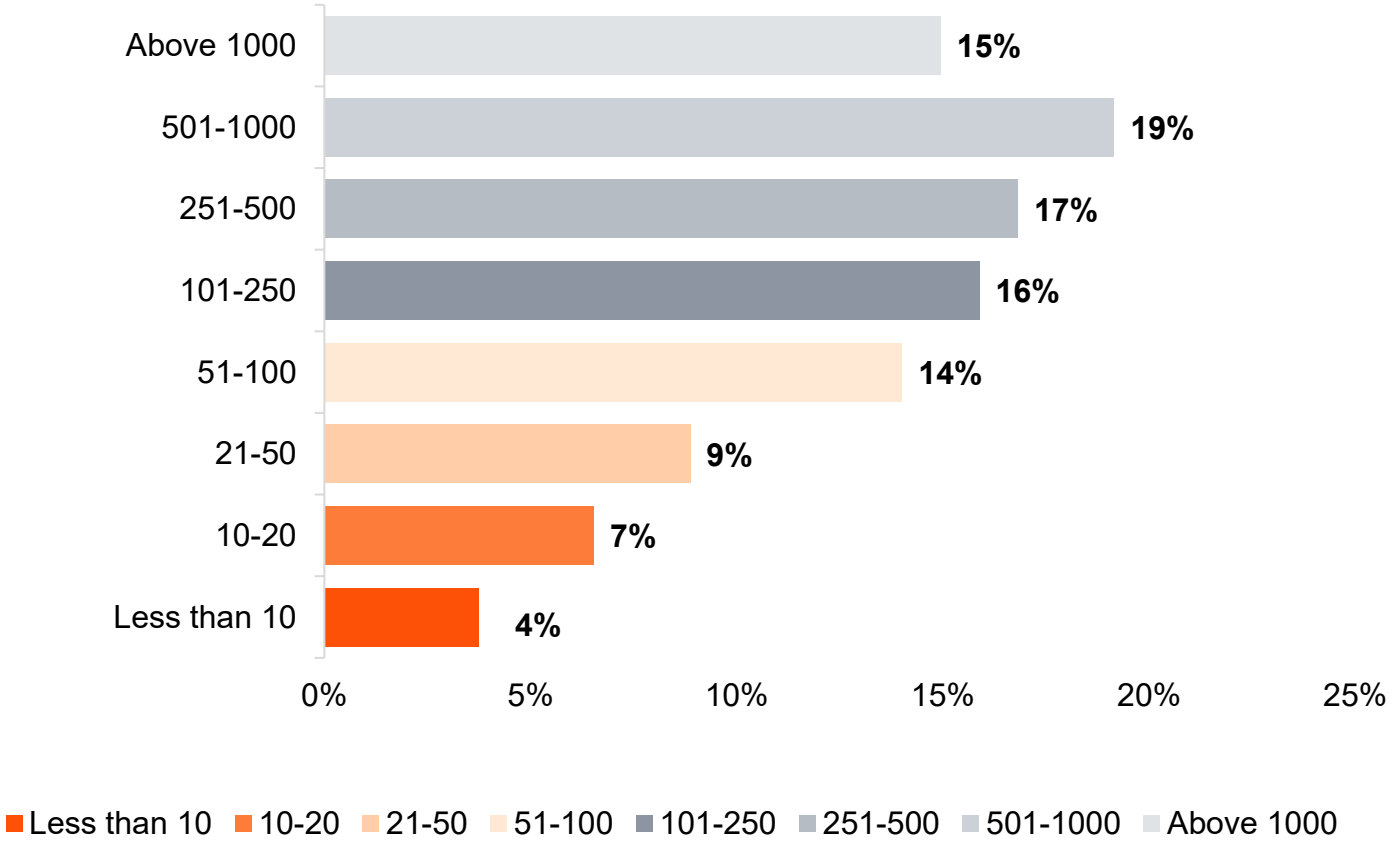
8 countries: Albania, Bulgaria, Croatia, Kosovo, Montenegro, North Macedonia, Republic of Serbia, Slovenia

3 domains:

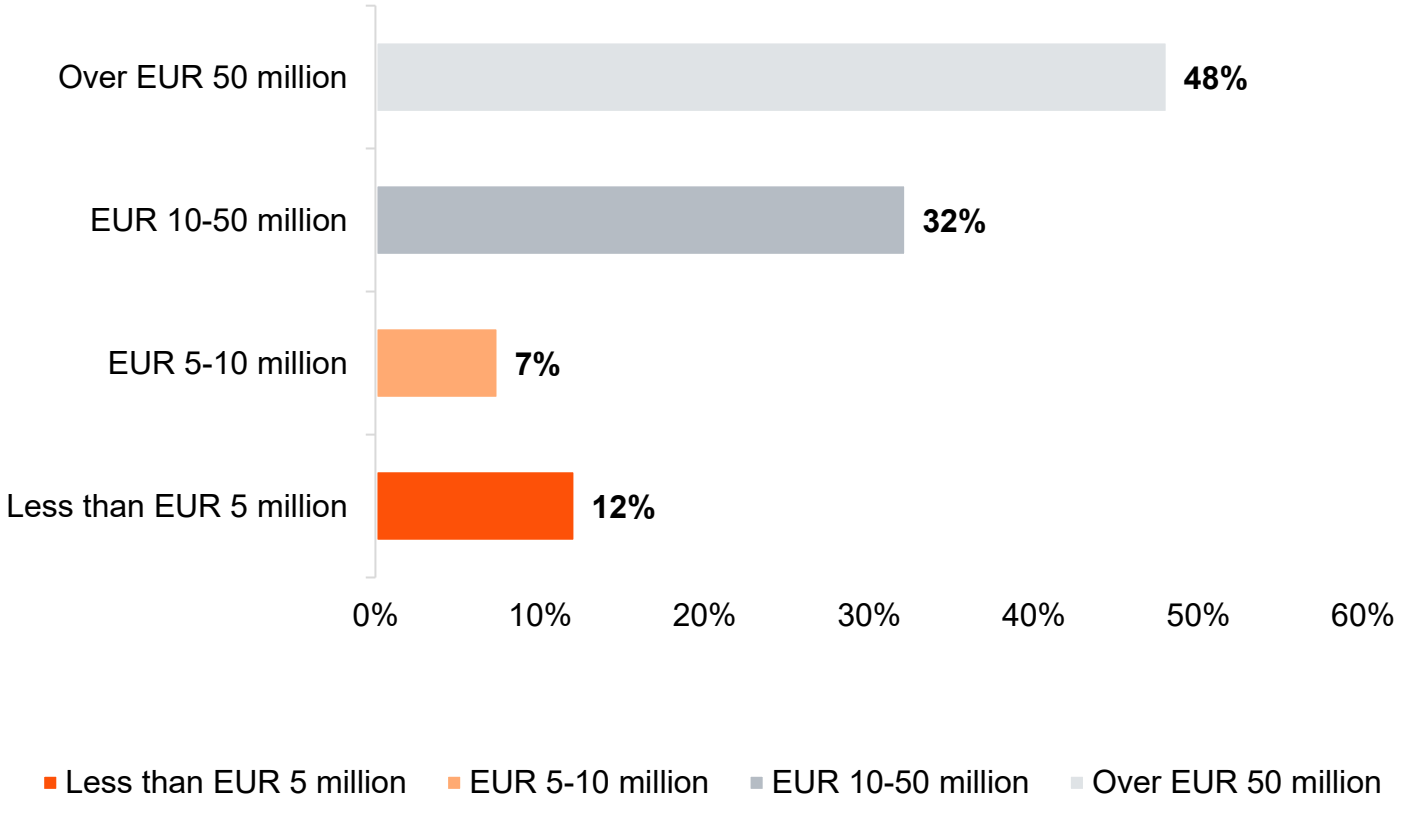
- Control environment and systems
- Digital resilience and cybersecurity
- Agentic, Analytic and Predictive AI: The next frontier in finance



Full-time employees



Revenue



Calibrating the Compass: Why do these domains matter now?

Our survey domains evolve each year, reflecting the issues that shape CFOs' decision-making.

The CFO Compass Survey is designed to adapt, not follow a fixed formula. Each edition responds to shifts in the economic environment, regulatory expectations and technological disruption. Last year, the focus centred on IFRS 18 and IFRS 19, alongside the growing ESG reporting demands, which were later postponed. This year, we explore the topics most relevant to today's dynamic environment.

Control environment and system integration
A resilient control environment remains the groundwork of every effective finance function. For the third consecutive year, this topic stands at the center of the CFO Compass as it continues to be the area where organisations experience the greatest operational pressure. Integrated systems, reliable data flows, clear access rights and proper segregation of duties are fundamental for maintaining accuracy, reducing risk and supporting business scalability.

Digital resilience and cybersecurity
In the era of digitalisation, exposure to cyber threats grows accordingly, especially when AI tools, cloud platforms and connected systems expand the attack surface. The risk profile of organisations of all sizes changes, and digital resilience isn't optional any more—it's mandatory for business continuity, investor confidence and regulatory compliance.

Agentic, analytic and predictive AI
AI adoption offers significant potential for transforming financial processes, from forecasting and scenario modelling to anomaly detection and workflow automation. Yet the rapid evolution of agentic and predictive models raises new questions around governance, data quality, accountability and ethical use. CFOs are now expected not only to explore AI opportunities, but also to understand the risks and set the right guardrails.

Control environment and system integration

Vasil Chinchev

Director,

Capital Markets and Accounting Advisory Services, Finance Function Transformation

The control environment and risk management have traditionally been the responsibility of financial leaders. Their challenge isn't just to introduce controls, but to establish the right ones.

Their role is to strike an optimal balance, reducing risk to an acceptable level without slowing down the business, hindering innovation or creating unnecessary administrative burdens. Efficient controls support agility, enable growth, and build trust with stakeholders—the backbone of a high-performing finance function.

The “One ERP” concept isn’t always applicable

54%

of surveyed CFOs still operate with moderate-to-no standardised accounting data within the group

34%

Load accounting data into spreadsheets that require manual adjustments

The problem?

Common chart of accounts and unified ERP systems aren’t yet in place for most organisations. This weakens data flow and amplifies error risk.

Why is standardisation so hard?

The cause

When around one-third of organisations operate mainly in Excel without automation, upgrading to more advanced solutions becomes challenging.

Where data isn’t standardised, manual reconciliation fills the gap.

Scenario 1: Single ERP

- Simplifies the system landscape
- Improves standardisation and governance
- Creates vendor dependency and sunk costs
- Requires strong internal capabilities
- Isn’t suitable for all SEE organisations

Scenario 2: Fragmented setup

- Preserves flexibility and scalability
- Enables gradual transformation
- Increases integration complexity
- Risks weaker controls if poorly connected
- Requires standardised data and strong interfaces

The solution

Ultimately, the goal is high-quality data. Achieving this requires balancing system design and integration while keeping risks at bay. **The right approach is the one that aligns with your business needs**, both short- and long-term.

IT architecture redesigned

Q. What software products/systems does your company use?

For years businesses believed that they should aim for a single, unified ERP as the backbone of their finance function. The 3rd SEE CFO Compass Survey, however, shows that this expectation no longer reflects the reality in South-East Europe. Diverse business models, local regulations, industry-specific requirements and legacy architectures make full standardisation across one platform difficult—and in many cases, not even desirable.

Survey responses illustrate this clearly. While SAP remains the predominant ERP across the region, spanning versions from ECC to S/4HANA, finance teams operate on a far broader technology base. Microsoft Dynamics is widely present, from legacy Navision to Business Central and F&O, with several respondents actively migrating to newer versions. Oracle also holds a significant footprint, alongside Hyperion for consolidation.

Beyond these global platforms, a substantial number of local and regional systems, such as Azure, Microinvest, Sonita, Hermes, Edusoft and many others, as well as fully custom-built ERPs appear with surprising frequency. Consolidation, reporting and payroll add further layers of variation, spread across tools like Tagetik, OneStream, Lucanet, Power BI, OMEX and Hrnet, or outsourced entirely.

This highly heterogeneous landscape isn't accidental. **It reflects real operational needs and illustrates why a single system rarely covers all business needs.**

Standardised data is the goal—but an ERP alone rarely delivers it.
The real enabler is **a well-designed ecosystem**, not a single monolithic system.

Modern finance organisations are shifting towards an **integrated ecosystem**—a coordinated set of systems that work together, each serving its strongest purpose, connected through structured processes and shared data models. This approach looks beyond siloed operations and manual handovers.

At the same time, an ecosystem can become counterproductive if it grows without structure. Too many systems, poorly connected or inconsistently governed, create the same problems organisations are trying to solve—fragmented data, manual workarounds and breakdowns in information flows.

The goal is not "many systems", but **the right mix of systems**, each selected to address a specific gap and integrated in a way that preserves data integrity, strengthens controls and supports the organisation's strategy.

This shift lays the foundation for stronger controls, faster reporting and the ability to adapt continuously to new regulatory, technological and economic demands.

Monthly processes

Manual effort doesn't scale into agility

Q. Currently, how many working days do the following processes take?

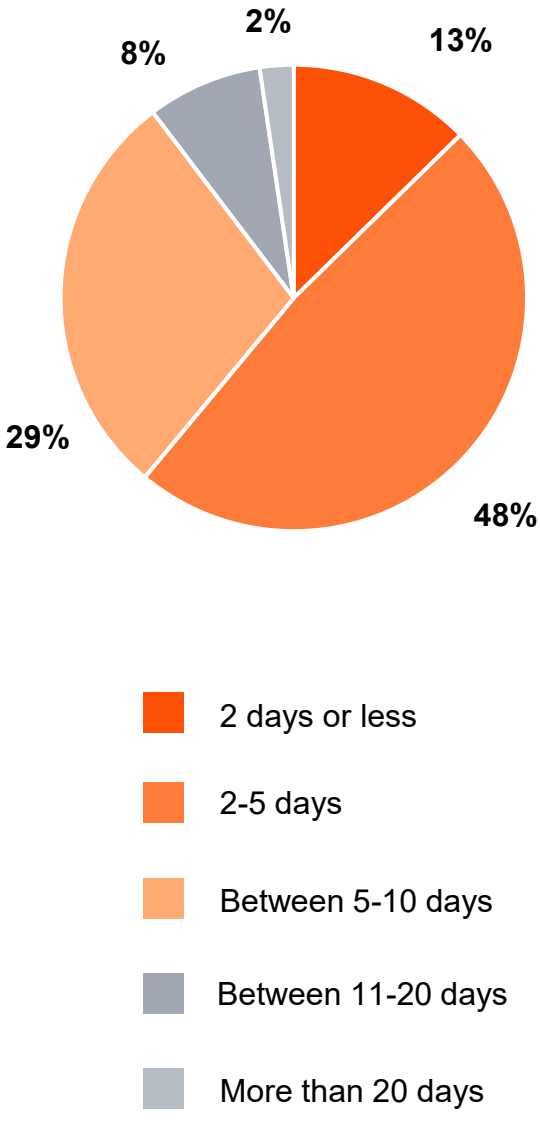
Monthly closing:

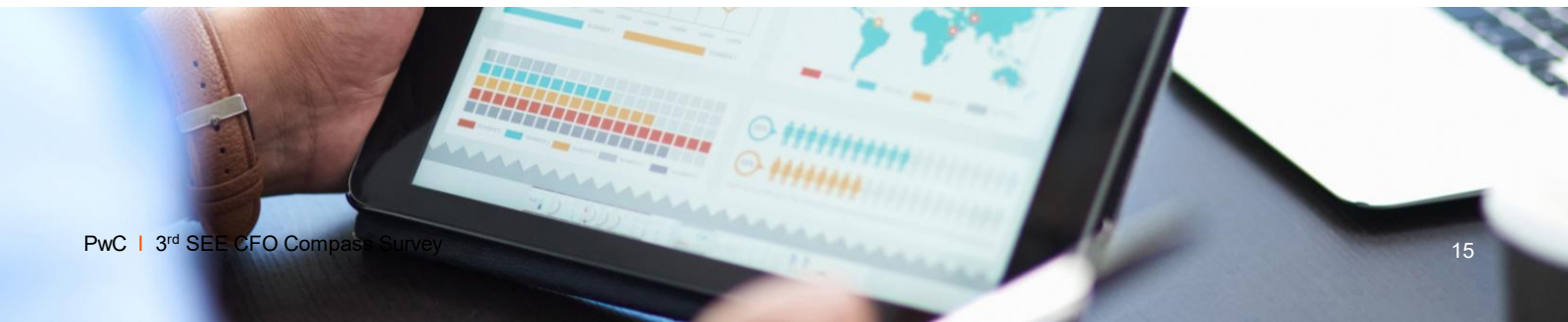
According to the survey, 61% of the organisations close within five days, establishing a strong regional benchmark and reflecting rising expectations for speed. **Nonetheless, calendar days alone are a blunt metric for efficiency compared to human effort involved.** A close that still requires 16-hour workdays shows that processes aren't scalable and control quality is at risk.

Even though finance functions report that internal systems perform reasonably well, the overall progress is slowed by external factors such as late documentation such as delayed invoices, slow approvals, and incomplete documentation from business units or suppliers. This forces teams to process large volumes of data within tight windows, often choosing between meeting a deadline and ensuring accuracy. Overtime drives fatigue-related errors, higher labor costs and post-close corrections and adjustments.

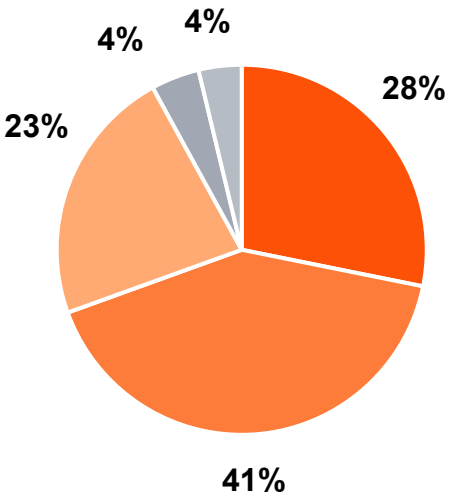
To achieve sustainable improvement, finance leaders are shifting from traditional month-end cycles toward continuous accounting, where reconciliations and validations occur throughout the month. The long-standing golden standard of "three-day close" is viewed as an operational risk if it's achieved through extreme overtime.

Monthly closing process

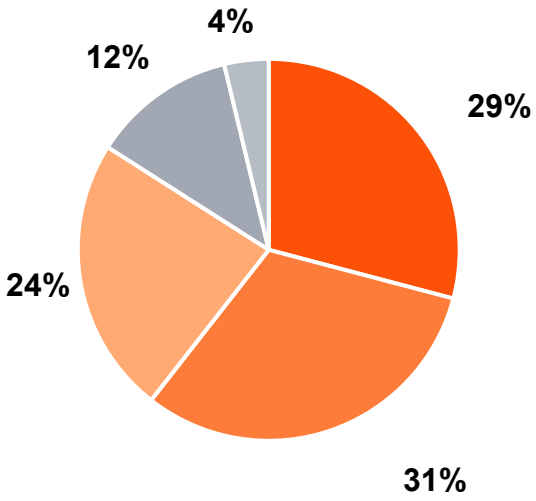




Monthly management report



Detailed report / cost center / line of revenue



2 days or less | 2-5 days | 5-10 days | 11-20 days | 20+ days

Monthly management reporting

Management reporting is seeing a shift in executive expectations. Senior management now demands transparency and a real-time summary of key points.

Modern analytics platforms such as Power BI and Tableau offer a comprehensive view of business performance to the board of directors, investors and stakeholders. Through a user-friendly interface, finance teams can prepare interactive dashboards and tailor analysis of large datasets to specific questions, while protecting sensitive information through controlled access.

To meet these expectations, the reporting environment should evolve from monthly snapshots to dynamic, continuously updated analysis. Finance units across SEE typically deliver monthly management reports within a 5-day window – by contrast, top-performing companies now refresh dashboards daily or weekly, indicating that this remains an area for improvement.

Detailed reporting

Four in ten companies report being slowed down by long turnaround times for detailed reports. Last year, 22% said these were more time-consuming than standard ones. Despite differences in respondent pools, the message is clear—**detailed reporting is an urgent concern**.

The challenge is structural and damages senior management's ability to monitor and manage expenses on specific-level units (departments, projects, and products). The issue of the modern FP&A function can be solved by moving business data into an ERP system with a seamless data flow. By establishing consistent business-unit collaboration, all teams can work with the same information simultaneously.

Natural language processing (NLP) solutions enable managers to interact with data by asking simple questions or holding conversational queries, receiving instant, evidence-based answers.

Improving speed in management reporting

Advanced analytics come after ensuring solid underlying data architecture

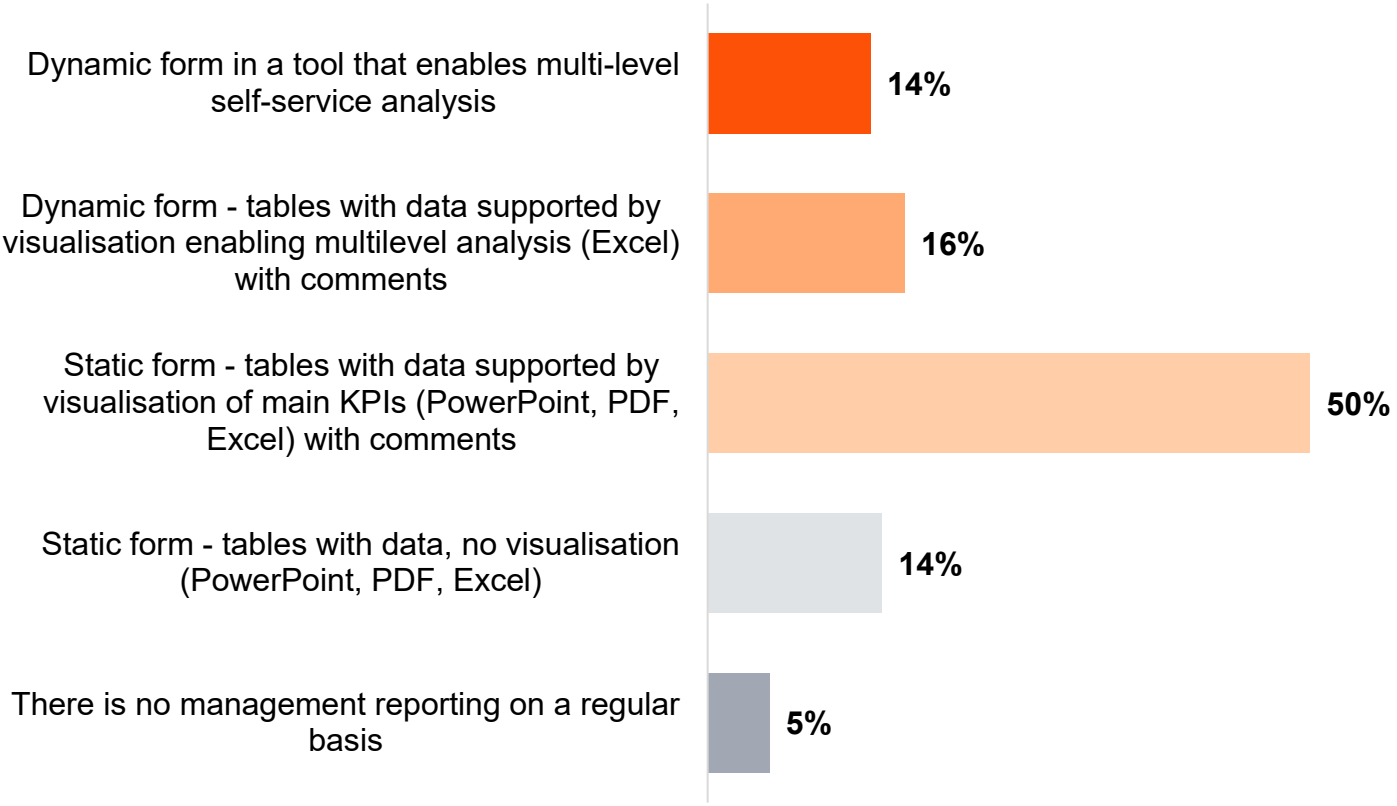
Last year's survey results already showed low adoption of dynamic multi-level analysis—a finding now supported by this year's respondent base. This reveals that a deeper problem persists and that dependence on static reports with limited visualisations is only a consequence of it. **Many organisations are trying to go faster, while the bottleneck sits in the data foundation.**

Finance teams are currently attempting to promptly build a reporting structure on a fractured foundation. Whether it's an integrated BI solution or a specialised ERP module, employees should use an automatic tool for their management reporting rather than being obliged to collect, analyse and visualise data on their own. Management reports remain manually fed, resulting in the current 5-day lag. Finance teams may also lack the time or expertise to develop more advanced dashboards. When competence is low, the finance team reverts to what they're familiar with–static tables, which are easier to control.

BI tools have been introduced but not fully adopted across businesses in SEE, limiting their full impact. There's a fundamental misconception that they'll automatically grant the desired speed and quality. In reality, **speed isn't a feature of the interface—it's a by-product of a strong underlying architecture.** A dashboard is only as fast as the processes that feed it. Smaller companies may be reluctant to adopt analytic platforms because of the high maintenance and licensing costs, which quickly become recurring monthly expenses.

Finance directors should start investing in data integration. Over the next 12 to 18 months, it's crucial to lay a solid IT foundation before exploring new advancements like AI.

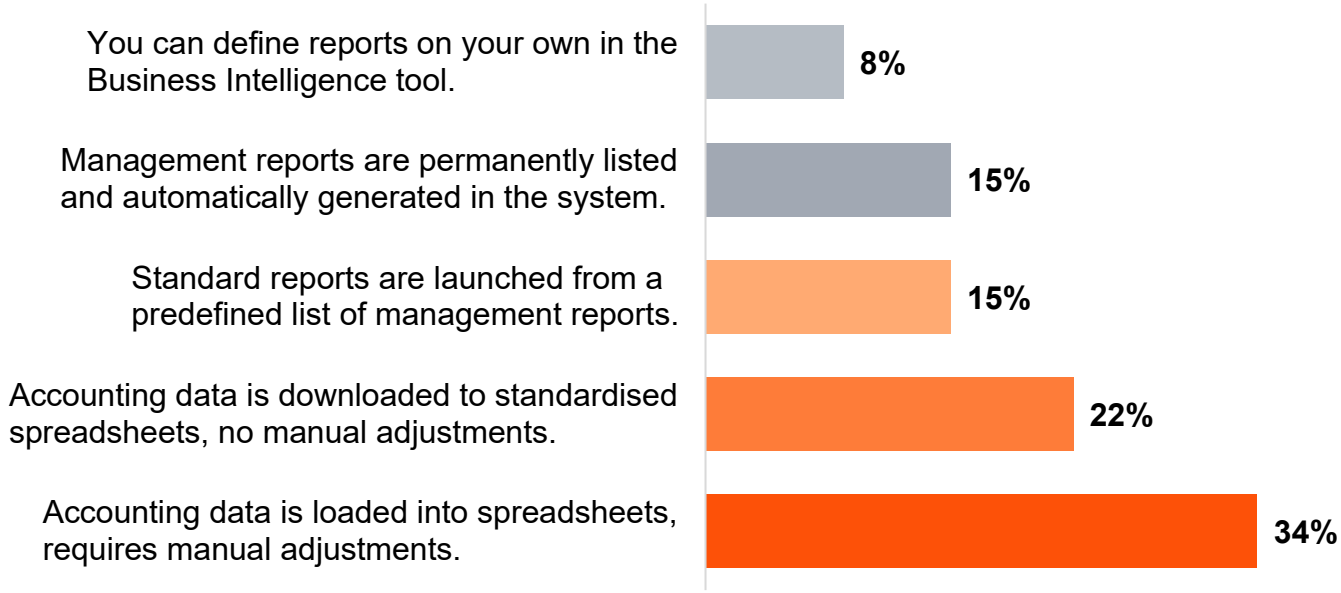
Q. In what form is the basic set of management reports communicated to the stakeholders on a monthly basis?



Many finance teams still rely on Excel-based reporting structure that presents outdated numbers to decision-makers and can't keep pace with the needed agility

34% of the organisations still load accounting data into spreadsheets and make manual adjustments

Q. How is the reconciliation between financial and management reporting typically performed?



A definitive measure of a finance function's maturity is how effectively it reconciles financial and management reporting. According to the survey, 34% of organisations still load accounting data into spreadsheets for manual adjustment. In the SEE market, defined by rising employee costs and talent shortages, manual reliance imposes a growth ceiling on expanding companies. An automated workflow mitigates this risk by maintaining consistent performance regardless of transaction volume.

Financial and management reporting serve distinct roles that must remain perfectly aligned, without additional adjustments, to ensure compliance and trustworthiness. Financial reporting is the backbone of management reporting. When aligned, both functions act as the decisive control point for finance directors. Any discrepancy here can undermine a CFO's authority before the Board: e.g. if management reports reveal a 25% margin while audited financial statements reflect 15% due to differing overhead allocations. Unifying internal performance metrics with the general ledger is therefore a governance necessity rather than a technical advancement.

To strengthen the control environment, finance leaders are increasingly adopting integrated data platforms that replace manual processes with automated logic, such as Microsoft Fabric and Azure Data Factory that allow for the standardisation of data collection and transformation. Dynamics 365 Finance acts as the core system of record under the protection of Microsoft Purview governance against cyberthreats. Power Automate then delivers this verified information directly into Power BI to support real-time decision-making.

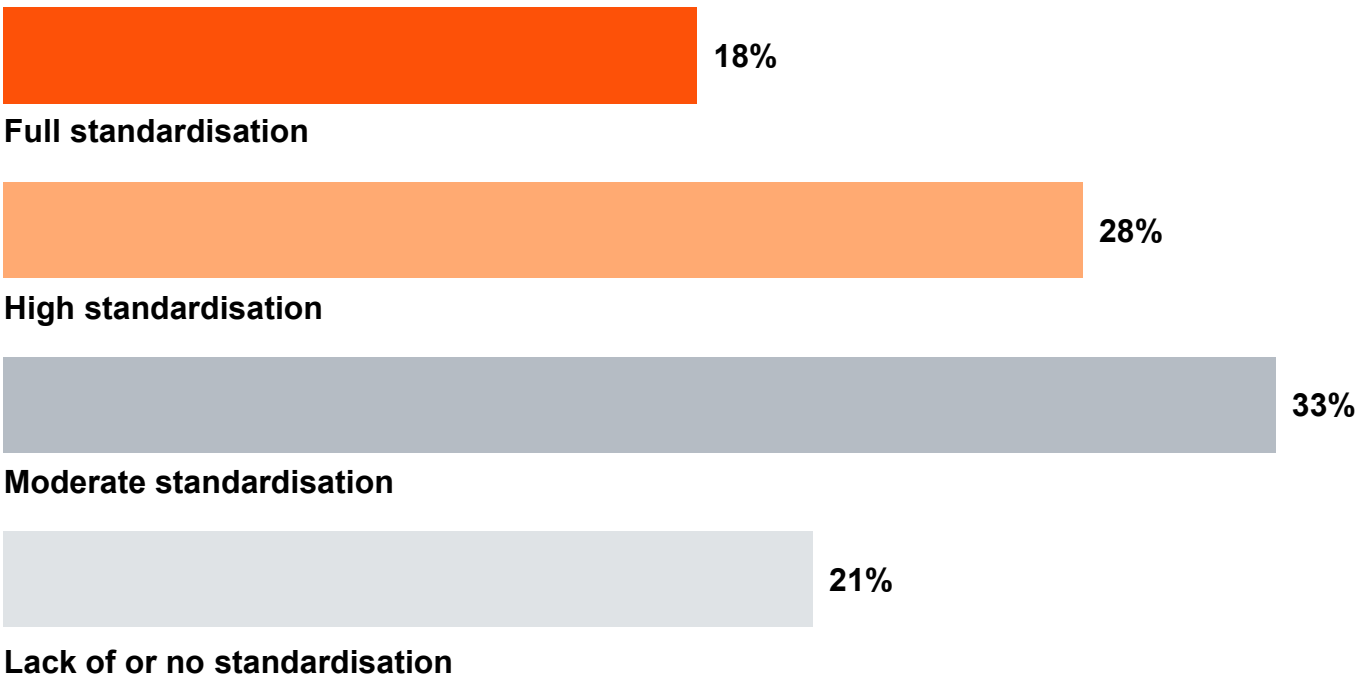
Common chart of accounts aren’t yet in place. What else is missing?

The standardisation of accounting data hasn’t yet reached the desired level of maturity across the corporate landscape. According to the survey, 54% of finance leaders categorise their standardisation process as moderate to none. For group reporting purposes, companies are trying their best to align their chart of accounts—through ERP systems or highly structured, software-like Excel solutions—to reduce the burden of consolidation. This shift away from fragmented practices suggests an uplift in the quality of the control environment. Yet, half of finance professionals are near the finish line to minimise manual intervention.

In a multi-entity structure, any inconsistencies from total standardisation require corrections to address local regulatory exemptions and complex consolidation requirements. For the CFO, this often results in a false sense of stability. As groups approach full standardisation, unresolved data gaps stand out more clearly and continue to slow the close of the books.

A primary obstacle to achieving full architectural integration is the specific structural position of SEE subsidiaries. Often operating as regional branches of foreign parent entities, these businesses must balance local fiscal and legislative mandates (essential for independent audits and domestic tax compliance) with the mandatory mapping requirements of a global group ecosystem. Unlike independent enterprises, which possess the autonomy to adopt agile, cloud-native infrastructures, group subsidiaries are frequently required to reconcile local requirements with parent standards. This constraint lowers the level of operational efficiency and achievable automation.

Q. Assess the degree of standardisation of accounting data across group entities

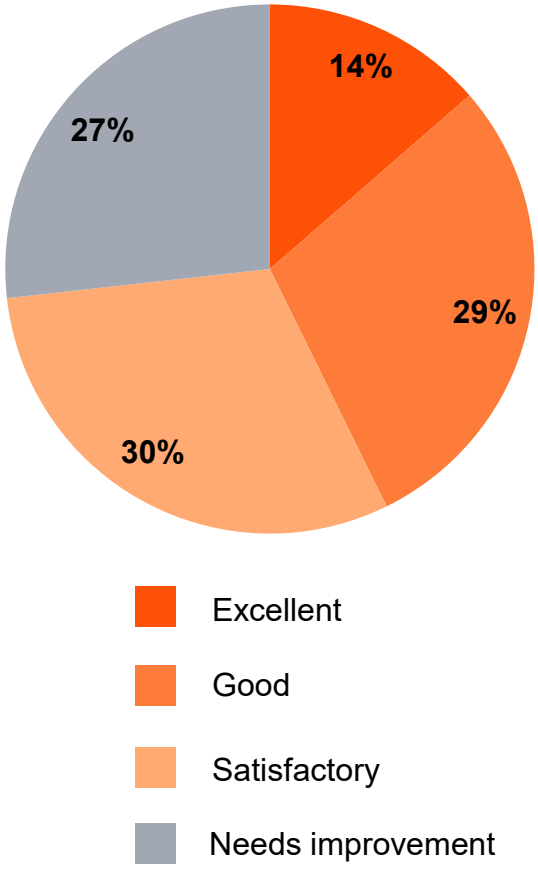


Q. How would you rate the integration and data flow among the systems in place?

While 43% of CFOs view their integration capabilities positively, the reality for the remaining 57% is a struggle with deficient data flows that make a “continuous close” impossible. In most organisations, data remains trapped in silos.

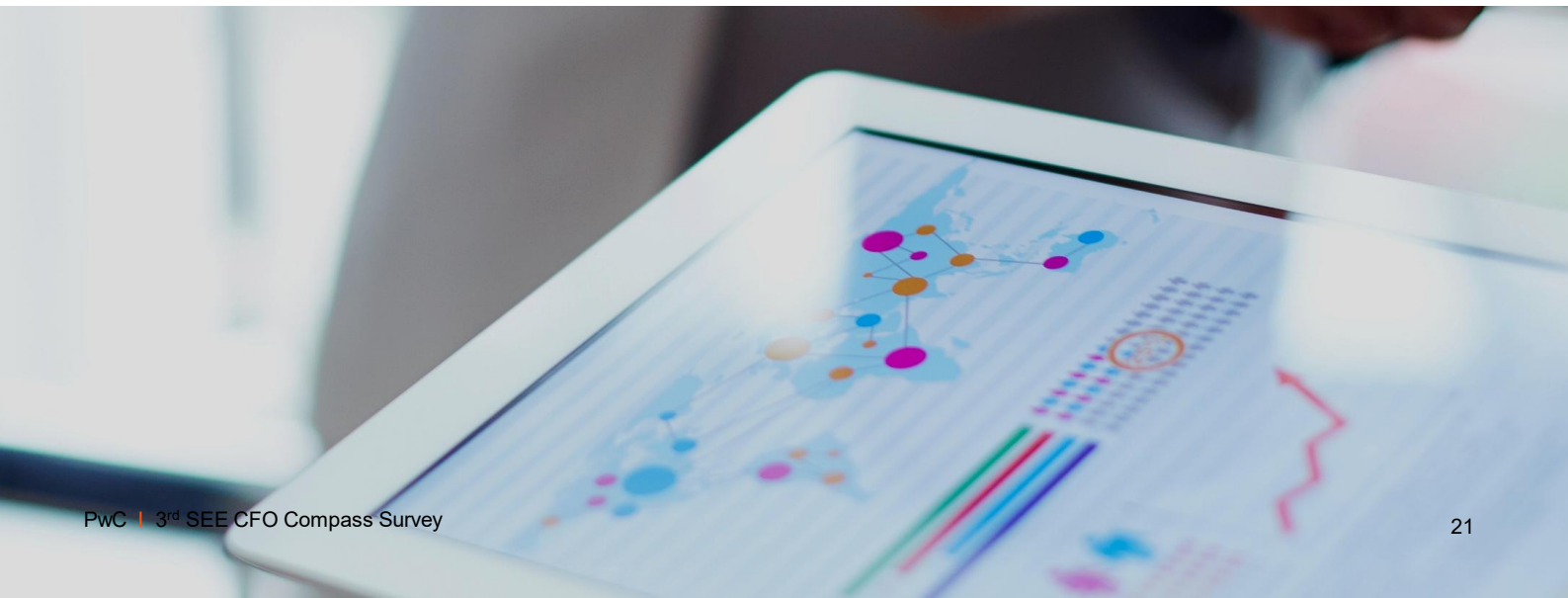
The promise of integrated banking was meant to solve this. By using direct API connections, companies are able to enjoy real-time cash management and banking.

However, security controls might stall automation like the current situation in the SEE region. Strict authentication rules (SCA) often force executives to approve bank transactions every few days and validate every individual payment via physical tokens. This leads to frequently interrupted data flows since big batches of payments still require human intervention. Furthermore, the absence of a common policy between banks and accounting software results in inconsistent data payloads, often returning statements with missing counterparty IDs or payment references.

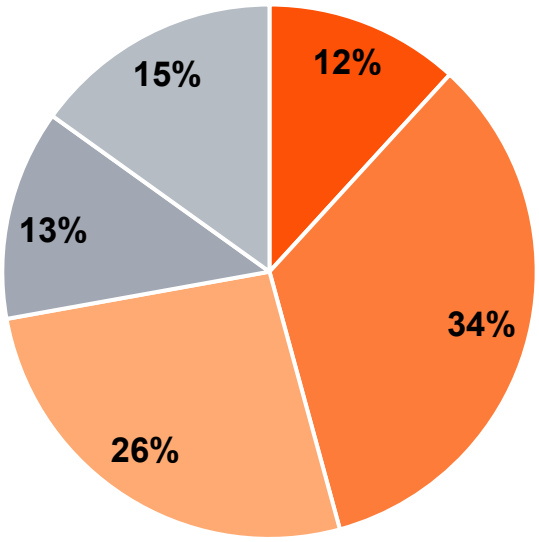


To move toward a truly autonomous finance ecosystem by 2026, the CFO agenda must shift from simple digitisation to intelligent orchestration. The goal is no longer just to connect a bank to an ERP, but to utilise Agentic AI that can navigate these authentication hurdles and handle inconsistent data payloads without requiring constant staff oversight.

Prioritise “API-first” Partners: when selecting ERP or accounting vendors prioritise those with proven, direct bank integrations that minimise manual re-approvals.



Q. How would you describe the current state of the systems your organisation uses?

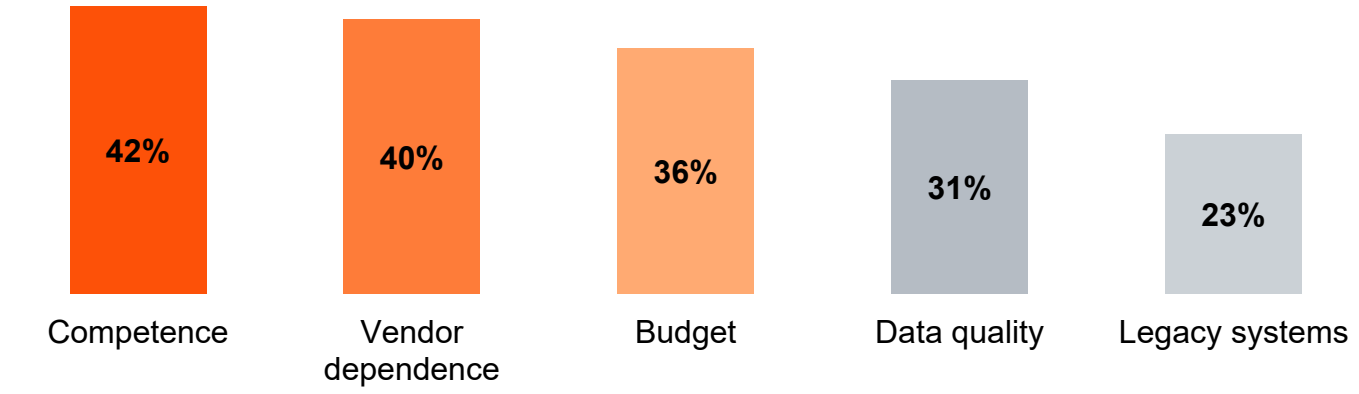


- We have a system / systems that we plan to expand to better support the financial functions in the organisation.
- We have an ERP class system (as above) with additional systems supporting the financial functions of the organisation and it meets our expectations.
- We have an ERP class system (e.g. SAP, Oracle, IFS) and it meets our expectations in terms of supporting financial functions.
- We plan to replace the current financial and accounting system with a system from another manufacturer.
- We plan to upgrade our current system to take advantage of its new features.

Where material barriers to ERP implementation exist, organisations should reconsider rather than ignore these warning signs. **Fragmented but flexible systems often better reflect the business reality in SEE, reducing vendor dependency** and enabling specialised solutions. However, this approach requires greater discipline to maintain a strong control environment.

Q. What are the biggest problems/challenges you encounter during ERP implementation?

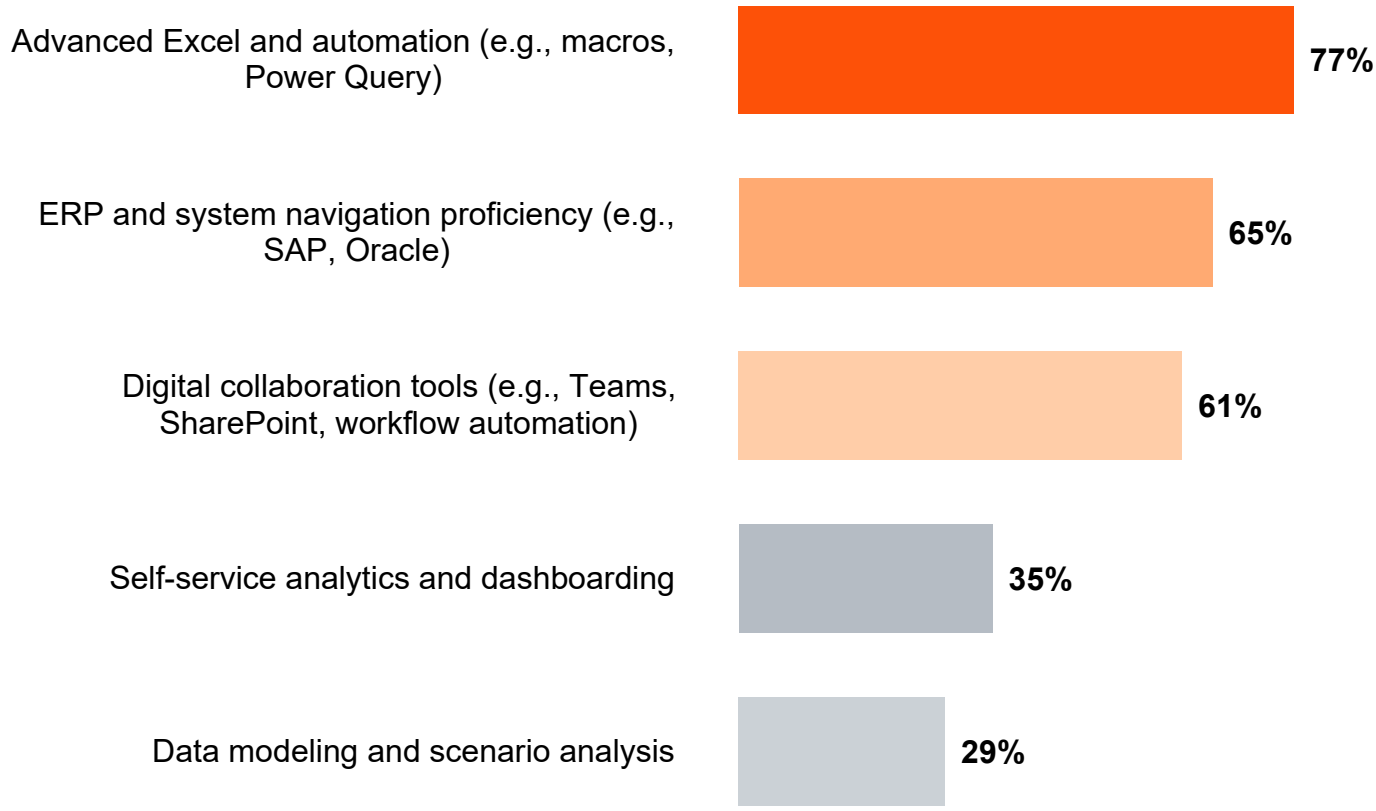
CFOs report a combination of overlapping issues: limited internal expertise, dependence on external vendors and constrained budgets that often stall projects



Internal competence is the number one challenge for implementing an ERP. And it goes beyond ERP. Across all industries, **people remain the foundation that no business can operate without.** Whether it's adopting a new system, adapting to a new interface, or simply working differently—the friction starts with people. And that friction is growing. Human capital is becoming harder to attract, retain, and upskill.

Most finance teams are comfortable with traditional digital skills, such as advanced Excel, ERP navigation, or routine automation. But far fewer have moved toward the analytical tools that enable faster insights and stronger decision-making. The shift from one system to another is rarely welcomed, and with every upgrade, fewer people keep up. This isn't surprising. CFOs operate in an increasingly complex and competitive environment where technology evolves faster than teams can absorb it.

Q. Which of the following digital capabilities are currently well-developed within your finance team?



Note: Only the top 5 results are displayed

Digital expertise and analytical thinking extend well beyond the finance function. They are becoming critical in the context of cybersecurity and digital resilience. Recognising threats—including deepfakes—requires constant awareness, not just annual training. The same applies to navigating a regulatory environment that is evolving just as fast. New compliance frameworks mean new systems, new integrations, and new points of exposure.

The more connected the finance function becomes, the more it needs to be protected. Companies must continuously develop their security systems, their compliance readiness, and most importantly—their people.

4

Digital resilience and cybersecurity

Kristian Viktorov

Senior Manager,

Cybersecurity & Digital Identity

Imagine the following: on a Tuesday morning, your colleague responsible for payments receives a video call from you. You tell them there is an urgent transfer that must be executed immediately, otherwise a key project will be blocked. The voice, the face, the details—everything matches you. Except that… it isn't you.

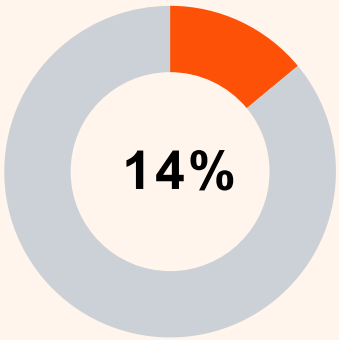
Deepfake hacking campaigns are no longer a movie scenario but a reality for many organisations. In a world where we can't fully trust our own eyes and ears anymore, cyber resilience stops being merely a technical matter. It becomes a financial, strategic, and leadership responsibility.

Cybersecurity: a non-profit function with critical value

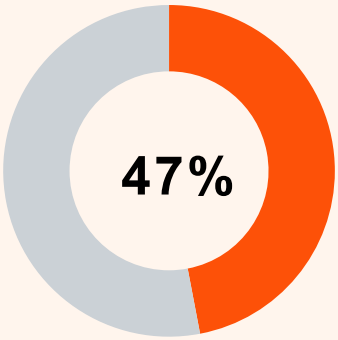
28%

of companies overestimate their cyber capabilities by failing to leverage external expertise. This signals an urgent need for deeper cybersecurity consulting.

Most organisations are only beginning their journey toward mature cybersecurity—highlighting an urgent need to move from reactive fixes to fully developed resilient security functions.



have established a cybersecurity function



are establishing a cybersecurity function

The majority of companies are directing their digital resilience budgets toward core modernisation efforts while deprioritising important digital resilience areas such as Zero Trust Architecture and Business Continuity Management/Disaster Recovery.

Only

2%

of respondents report allocating budget to **Zero Trust Architecture,** and

0%

allocate budget for **Business Continuity Management/Disaster Recovery**, indicating that these critical areas remain largely undervalued.

Strengthening focus in these domains will be essential for building true digital resilience.

Digital resilience: where compliance and cybersecurity collide

Regulatory change doesn't just create compliance work—it creates exposure. As frameworks like SAF-T and ViDA push finance functions toward standardised data models, real-time reporting, and digital submission channels, they also multiply the points where systems can be compromised.

SAF-T implementation alone forces organisations to modernise legacy ERP systems and remap internal data fields to match state-specific requirements. ViDA, while still years from full enforcement, is already prompting system updates and new integration points. Each new connection—to regulators, to platforms, to third parties—is a potential vulnerability.

At the same time, regulations like DORA and NIS2 are reshaping how organisations manage digital risk, operational continuity, and cyber resilience. The compliance burden is growing, but so is the attack surface. More automation, more data flows, more interconnected systems—all essential for regulatory readiness, yet all expanding the perimeter that needs to be secured.

This is where digital resilience stops being a budget line and becomes a strategic imperative. It isn’t enough to meet the next regulatory deadline. Organisations must protect the very infrastructure that compliance now depends on, or risk building on a foundation that can’t hold.

Navigating regulatory changes

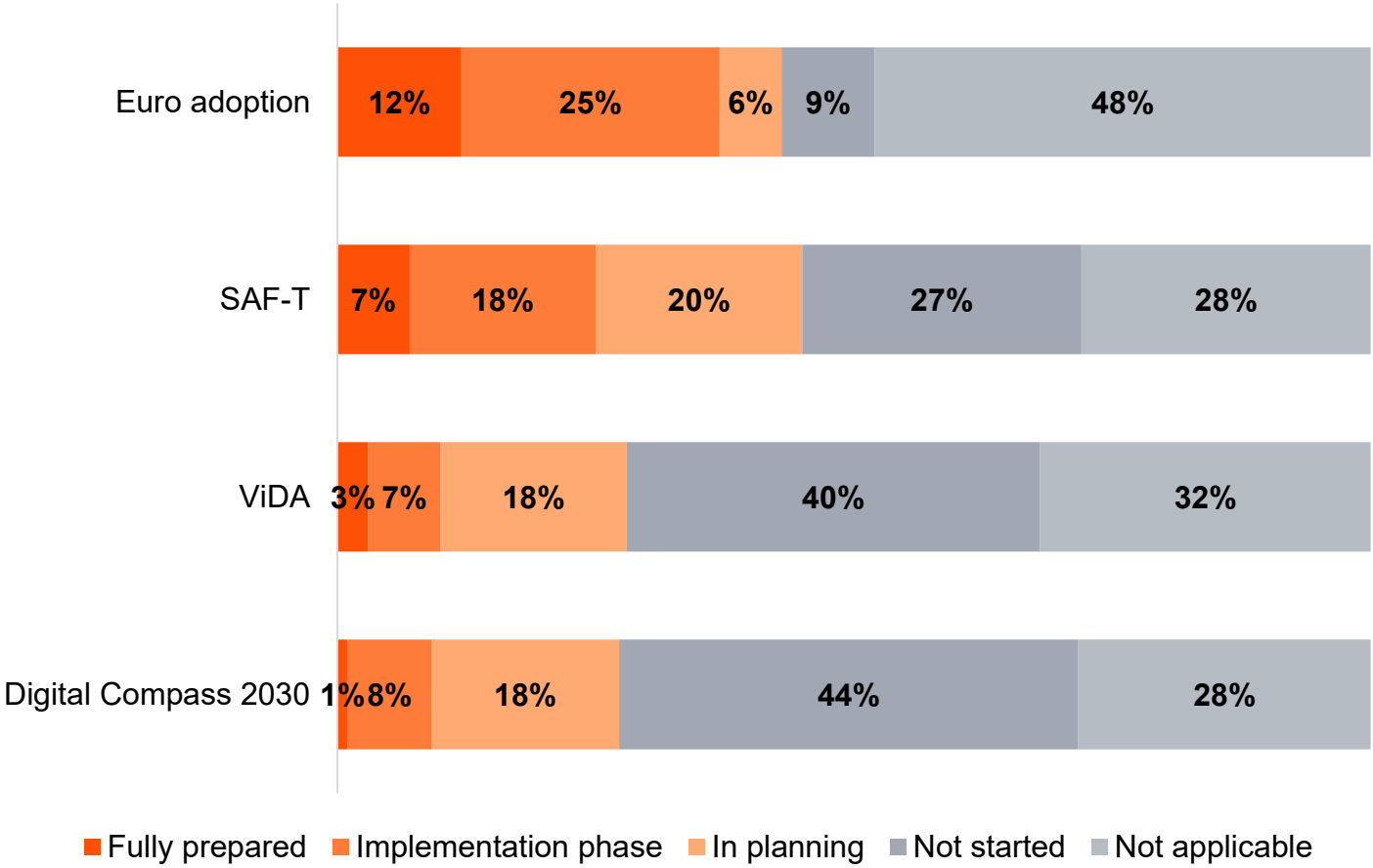
Euro adoption: In Bulgaria, the changeover was met with high levels of readiness, as most finance functions had successfully completed their preparations or were in the final stages as they entered 2026. This indicates that organisations had allocated enough time and resources to prepare for the adoption of the new currency.

SAF-T: Regarding the implementation of SAF-T, only a small proportion of respondents reported being fully prepared. This slower progress is largely due to the phased introduction of SAF-T in the region, which has led many CFOs prioritise other business needs until the requirements become immediately applicable. Nevertheless, businesses should start their technical transition early to meet their regulatory requirements on time and to avoid unnecessary operational disruptions, which could result in both financial and reputational harm.

ViDA: Much like the SAF-T, the ViDA Regulation remains a low priority for most finance leaders, with full implementation anticipated by 2035. Still, member states are allowed to introduce mandatory e-invoicing ahead of schedule. The upcoming year offers a period for businesses to identify compliance gaps and initiate required system updates at a manageable pace. CFOs can utilise this as a strategic opportunity to future-proof financial operations, strengthen data integrity, and position their organisations to respond swiftly as regulatory timelines accelerate.

Digital Compass 2030: As for the Digital Compass 2030, finance directors aren't yet actively monitoring their progress. Survey participants report a generally low level of preparedness. Unintentionally, their ongoing focus on automation and technical upskilling is already contributing to broader EU objectives. Some examples include the 75% Cloud and AI adoption target. CFOs in the region are well-positioned to build long-term resilience and ensure their organisations are equipped for the rapidly evolving digital landscape.

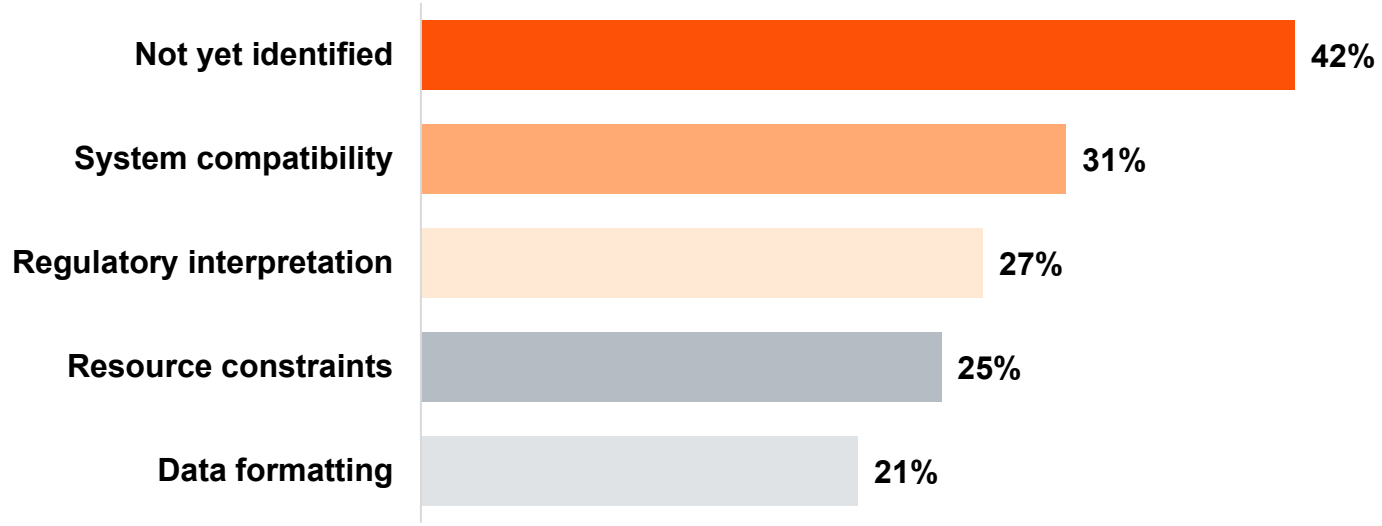
Level of preparation for legislative and regulatory transitions



The challenging path to SAF-T implementation

31% **of respondents have system compatibility issues when implementing SAF-T**

Q. What challenges have you encountered in SAF-T implementation?



Diving deeper into one of the key regulatory transitions in the coming years—the adoption of the Standard Audit File for Tax (SAF-T)—the survey seeks to identify the main challenges organisations encounter throughout its implementation.

Currently, businesses face significant technical and investment barriers, struggling to align legacy ERP systems with these new standardised data models. The results indicate that 31% of respondents have system compatibility issues when implementing SAF-T, highlighting the scale of the adjustment needed. Additionally, organisations report difficulties interpreting the regulatory requirements of the new standard, while finance leaders struggle to allocate sufficient resources to support the transition effectively.

Implementation requires precise data mapping (data formatting) to match internal fields with state-specific nomenclatures. This often forces an expensive modernisation of financial infrastructure to ensure data integrity at the source, revealing deep-rooted obstacles in older accounting systems.

Adoption isn't yet universal, and regulatory ambiguity causes finance leaders to hesitate. Because national institutions define their own unique fields and rules, SAF-T isn't a one-size-fits-all process across countries. Multinational groups must treat each market as a unique technical project, building localised solutions to ensure a truly resilient and compliant finance function.

Cybersecurity and operational resilience functions

Companies are just starting to realise the impact of strengthening their cybersecurity and operational resilience functions

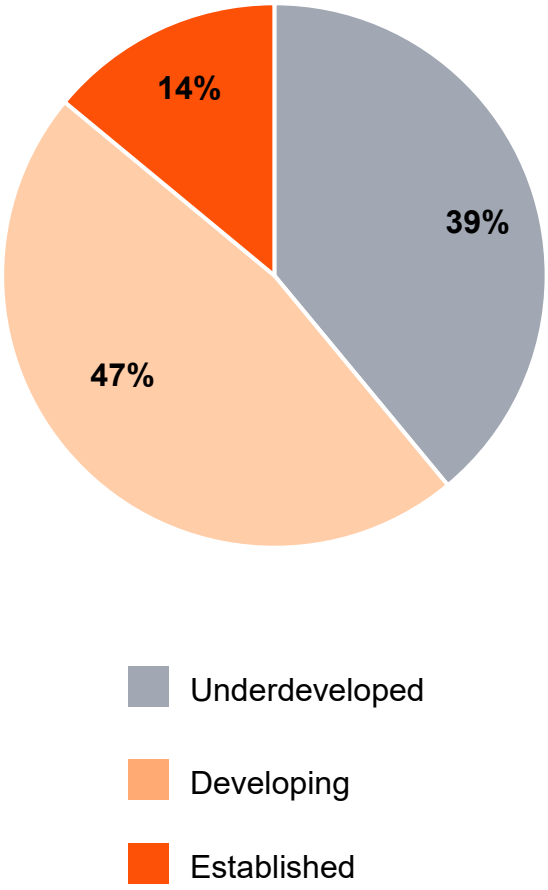
Q. How mature is your cybersecurity function in terms of compliance?

Cybersecurity and operational resilience are often used interchangeably, but they serve distinct purposes. Cybersecurity is the first line of defence—the firewalls, access controls, and preventative measures that protect systems, data and information from being compromised. Operational resilience is the plan for when those walls are breached. It is the ability to absorb the impact, adapt, and continue operating. One aims to prevent disruption and the other ensures survival when disruption occurs.

Cybersecurity isn't merely an IT concern, it's a fundamental pillar of operational business resilience, and the wave of new digital regulatory frameworks entering into force reflects exactly that shift. As organisations of all sizes undergo digital transformations, concern over data privacy and cyber risk is no longer confined to large enterprises.

Yet awareness in the region is only beginning to turn into action. Fewer than one in six organisations describe their functions as well-developed, while nearly half are still in the process of building out their capabilities. This is a positive trend, but one that leaves them exposed to cyberattacks, system failures and digital disruptions in the interim.

The message is clear: don't wait for a regulatory deadline or a security incident to act. Invest in operational resilience now, while the cost of building is still lower than the cost of recovering.



Most organisations don't have the capability to overcome cyber challenges by themselves

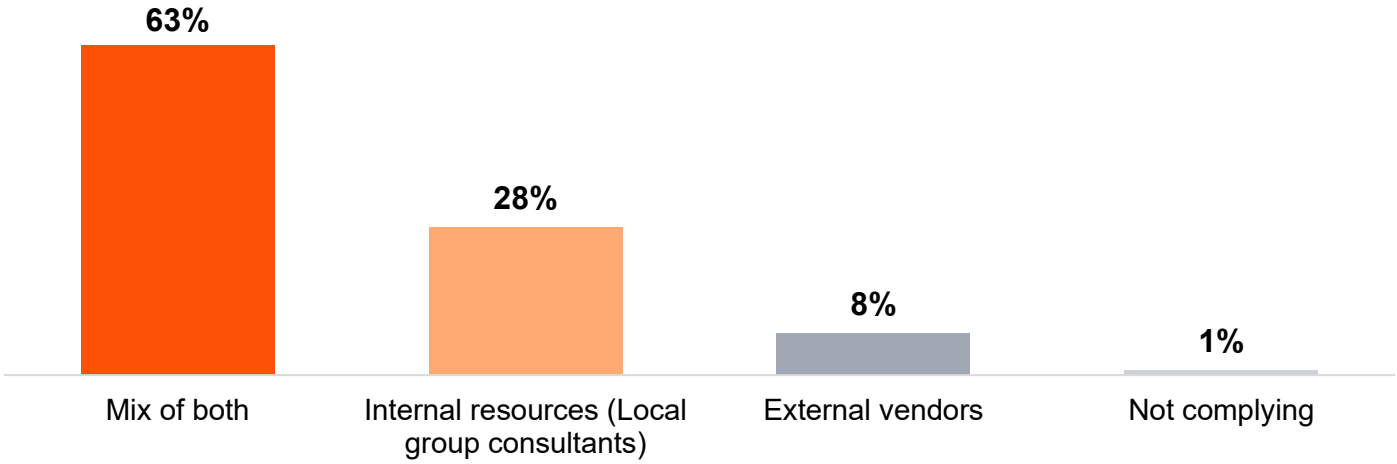
Q. How do you address your cybersecurity requirements?

Most organisations in the SEE region don’t have the capacity to address cybersecurity challenges entirely on their own. Around two-thirds prefer to meet these requirements with a mix of in-house and external resources.

Internal teams have a profound grasp of business needs, while external partners bring specialised knowledge and the ability to scale—capabilities that no single function can maintain independently.

Specialised providers are often at the forefront of implementing new solutions and updating skills, drawing on experience gained across multiple clients and industries.

The 28% organisations relying solely on internal resources face a different trade-off: greater customisation, but potentially slower adoption of new technologies and methodologies due to budget constraints or internal processes. With the knowledge gap between attackers and defenders continuing to widen, combining both is less a preference and more a necessity.



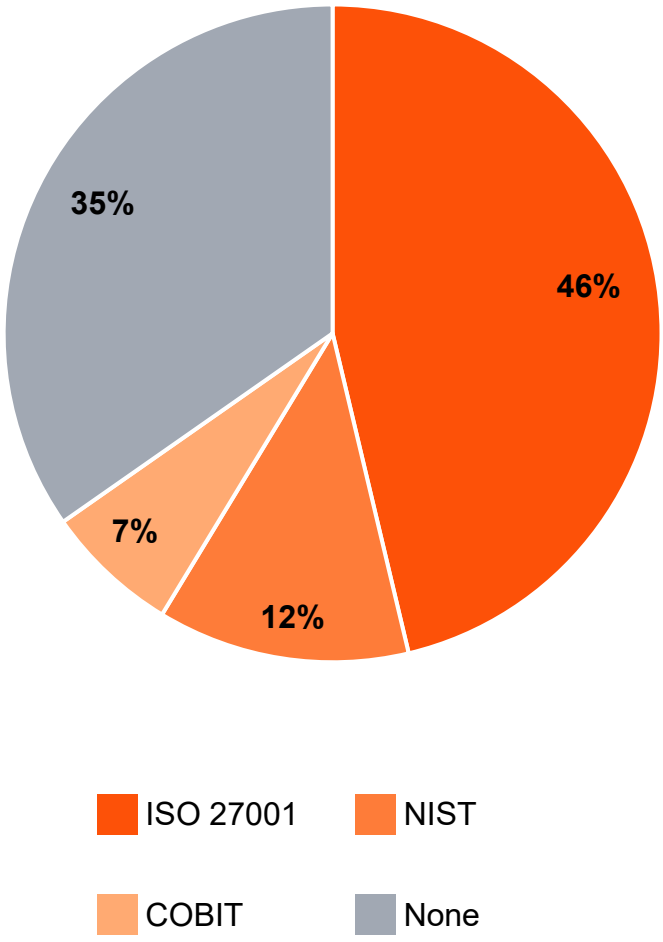
Implementation of cybersecurity frameworks

Q. What cybersecurity frameworks are currently implemented?

The majority of survey participants choose ISO 27001 as their primary cybersecurity framework for good reason. As the most widely recognised international standard, it does more than just provide a solid foundation for a security function. It also serves as a trust partner to stakeholders. In a diverse region like SEE, where businesses operate across both EU and non-EU jurisdictions, the universal applicability of ISO 27001 makes it a natural baseline.

While not as common, NIST is a voluntary risk-based framework that allows organisations to integrate security practices alongside existing standards. It can be tailored to a company's specific needs without the pressure of formal certification. In contrast, COBIT addresses a different requirement by aligning technical security with business strategy. It's particularly valuable for finance leaders because it focuses on governance and specific areas that ensure all budget invested in security delivers quality, and supports the firm's broader objectives.

Perhaps the most striking finding of this year's survey is that over **a third of respondents still operate without any formal framework**. While these frameworks aren't mandatory, their absence leaves the finance function and the whole organisation vulnerable to cyber risks that are difficult to manage, defend, and explain to regulators, clients, and shareholders.



Q. Are you actively seeking compliance with the following regulations?

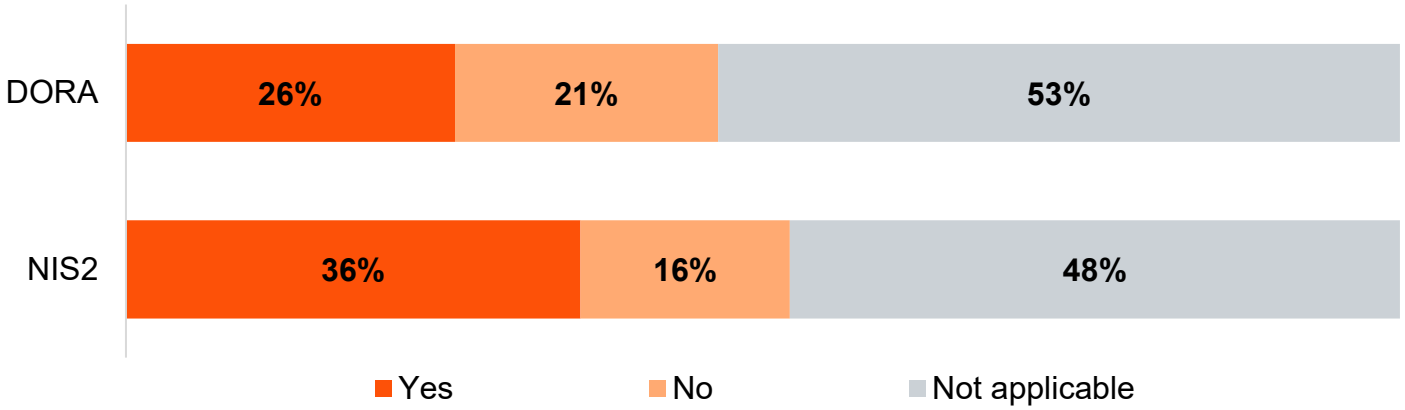
The voluntary frameworks discussed above provide a strong foundation, but NIS2 and DORA are a different matter. These are legally binding European regulations with defined scope and real consequences for non-compliance.

DORA applies to financial entities and the third-party ICT providers that support them. Roughly half of our respondents fall within its scope, and when we look only at those organisations, nearly half haven't yet taken action. This is particularly concerning because DORA became fully enforceable on 17 January 2025 with no grace period. Organisations that haven't started are in immediate breach.

NIS2 targets entities classified as essential or important across sectors like energy, health, banking, and digital infrastructure. Again, roughly half of respondents fall within scope. Of those, the majority confirm compliance, but approximately one in four have not yet aligned their practices.

The regulatory landscape continues to evolve. In January 2026, the European Commission proposed targeted amendments to NIS2 as part of a broader cybersecurity package, introducing a "small mid-cap" category, reducing administrative burdens for nearly 29,000 businesses, and establishing a Single Reporting Portal for cyber incidents. For organisations that have been waiting for greater regulatory clarity before acting, that clarity is now arriving.

Organisations that have already adopted standards such as ISO 27001 or NIST will find compliance with both regulations far more manageable, since NIS2 and DORA build on the same principles of risk management, incident response, and governance. For those that haven't done so, the time to act is now.



Top priority cybersecurity areas

The priorities at the bottom of the chart tell an important story. Only 4% of the surveyed CFOs allocate budget to Threat Intelligence, 2% to Zero Trust Architecture, and none to Business Continuity Management and Disaster Recovery. These aren't optional measures. They represent the structural layer of digital resilience that the entire cybersecurity domain depends on.

As already mentioned, the traditional model of network security is no longer enough. Zero Trust operates on the principle of "never trust, always verify", treating every user, device, and connection as a potential threat, regardless of whether it sits inside or outside the organisation. With remote work, cloud adoption, and third-party integrations expanding the attack surface, the assumption that internal networks are safe isn't valid anymore. Yet investment hasn't followed. The absence of BCM/DR from the budget is equally concerning. Operational resilience isn't just about prevention, but about the ability to absorb disruption and recover. BCM/DR ensures that when an incident occurs, the business has a tested plan to return to normal operations. Its complete absence directly contradicts the resilience objectives that DORA and NIS2 are designed to enforce.

Investing in people is the right starting point, but it can't be the only one. Recognising threats, including deepfakes, requires continuous awareness, not just annual training. Without these structural measures in place, even well-trained teams will lack the contingency plans and systems needed to respond effectively when prevention fails.

As we explore AI within the finance function in the next section, this imbalance becomes even more relevant. AI adoption without the right security architecture and crisis management doesn't just create inefficiency. It creates exposure that can compromise the entire function.

Q. What areas are your top priorities for budget allocation?

5

Adoption of AI

Deyan Savov

Director,

Risk Assurance Services

In 2025 the investment in AI startups soared above $200 billion, representing an over 75% jump from the previous year, according to Crunchbase. Half of all new companies now incorporate AI as a core component of their products. This trend echoes the dot-com bubble of the late 1990s, when countless firms failed due to unsustainable business practices.

Just like back then, today's real challenge isn't the technology—it's the way we put it into practice.

Organisations that build strong business processes and clear controls are better positioned to generate reliable, high-quality data and unlock the full potential of new technologies.

Technology isn't the challenge. Integration is.

61%

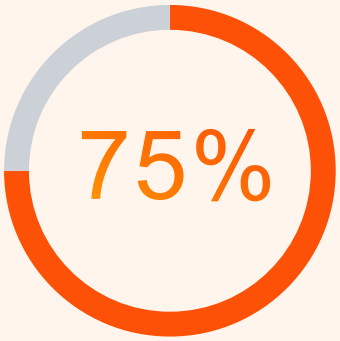
are exploring or have already implemented AI agents

almost

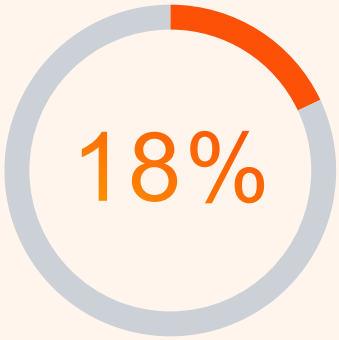
80%

allocate less than €50,000 for AI implementation

Reliable controls aren't yet established despite the high interest towards implementing AI



Not evaluated yet



Human oversight

AI's potential is limited by the top 3 constraints:

50%

Employees' skills

39%

Data privacy

38%

Cyber risk

Supervision is only effective when people understand AI's opportunities and limitations. Yet, every second organisation hasn't trained its employees to use AI, let alone supervise it.

Level of AI automation

RPA and AI aren't substitutes. They complement each other but both depend on clean data and controlled processes.

Although the interest in AI and machine learning is high, only **around 7%** of such solutions are fully implemented, and nearly **one-third** of CFOs report **no progress at all**.

This slow adoption doesn't reflect a lack of ambition. Instead, it reveals a more fundamental issue: many organisations haven't yet reached the level of automation maturity required for AI to work safely and reliably at scale. When day-to-day processes are still manual, fragmented, or undocumented, AI tools struggle. The models need stable inputs, predictable workflows, and structured data—conditions that simply don't exist in many finance functions in the region.

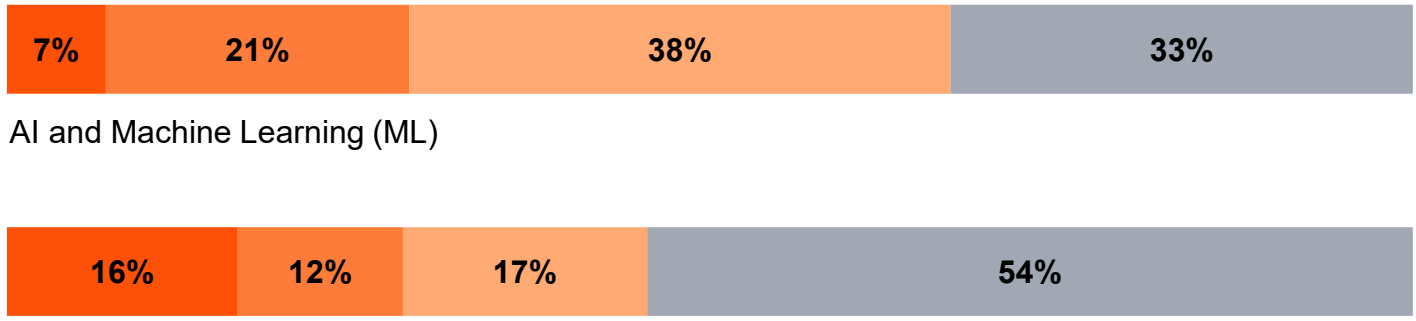
This is why combining **AI/ML with foundational RPA** is crucial. RPA stabilises routine workflows and provides the structured environment AI needs to operate on top.

On the other hand, RPA shows **striking segregation**—it has the highest rate of non-use (54%) alongside a peak adoption rate (16%). Rather than replacing traditional tools to chase the "AI hype", organisations should invest in the foundations that make sophisticated AI scalable in the first place.

This remains true even for businesses that view automation as a secondary concern due to lower transaction volumes. Although modernising legacy processes may not feel like an immediate necessity, staying ahead is vital for long-term resilience and shouldn't be underestimated. Manual workflows might remain manageable for now, but by the time workload increases to a critical point, the cost of catching up to better-prepared peers becomes significantly harder to justify.

Treat RPA not as a tool for large-scale operations, but as the essential architecture required for business continuity. Implement it today to build the infrastructure your enterprise will demand tomorrow.

Q. To what extent have the following solutions been implemented within your area of responsibility?



Level of AI automation

Data Mining, Business Intelligence and Data Visualisation is the **most mature category**, with 18% of the surveyed CFOs having already implemented these technologies and a further 28% being in progress.

Finance teams are progressively moving away from static, descriptive reports towards interactive models with drill-through functionalities. AI-enabled tools, such as Co and the Key Influencers visuals within Power BI, perform root-cause analysis in real time and identify the top drivers behind a specific metric.

As traditional reporting gives way to more dynamic formats, the focus for 2026 is shifting towards “chat-to-report" interfaces. This approach allows stakeholders to interact directly with data, rather than navigating complex dashboards. Users simply ask, "Show me travel expenses for the SEE region compared to last year's forecast," and receive a tailored visual in seconds. Finance functions can eliminate the time-consuming cycle of ad-hoc report building and provide the business with immediate, actionable clarity.

Data Mining, Business Intelligence, Data Visualisation

Big data, Predictive Analytics

Already implemented

Implementation in progress

Implementation is considered

Not implemented

Big Data and Predictive Analytics follow a familiar pattern to AI/ML adoption. Only 8% have achieved full implementation, while one-third haven't progressed at all.

This similarity isn’t coincidental: predictive analytics isn’t a standalone solution. It’s a direct application of AI and ML, requiring massive volumes of diverse data gathered from multiple sources. Therefore, the implementation of predictive capabilities depends on the same groundwork that companies are still building.

Yet with 19% of organisations already in progress and a further 37% actively considering implementation, momentum is clearly building. For those willing to invest in these foundations, the potential is substantial. Where traditional BI answers “what happened”, predictive analytics addresses the consequential question “what is likely to happen next”.

For finance teams, this means tangible capabilities: cash-flow forecasting, revenue projection modelling, early risk detection, and improved customer retention.

CFOs who haven’t yet taken the initiative should invest in data quality and process standardisation now. Predictive analytics can only deliver meaningful results on solid foundations—not on the inconsistencies of the legacy systems it’s built on.

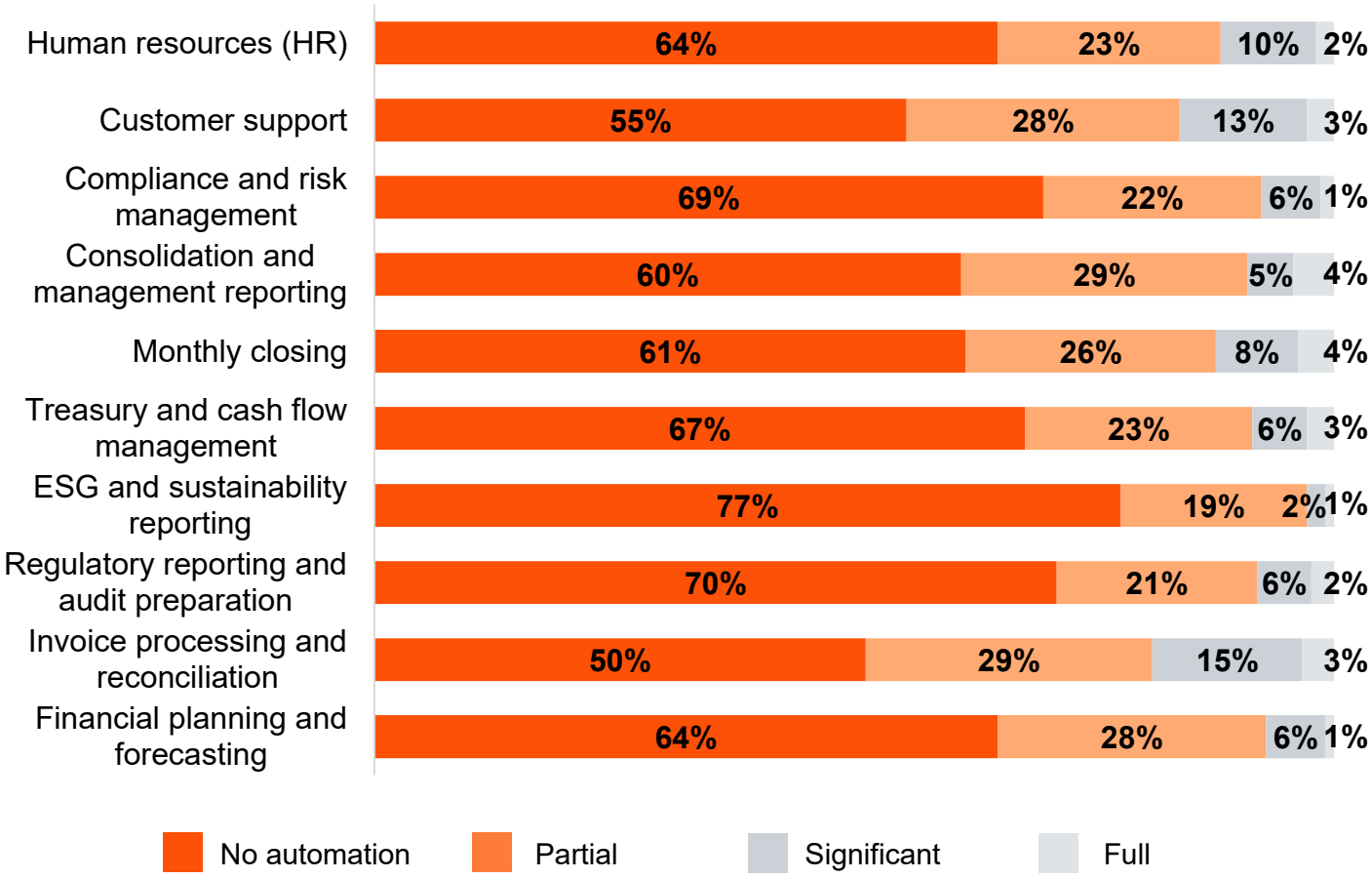
Level of AI Adoption – in proven use cases

Adoption starts where the risk is lowest

Some processes have become clear early wins for AI and automation: invoice processing, customer support and communication, and HR and hiring workflows. These use cases share one thing: **errors can be reviewed quickly and corrected without reputational impact.**

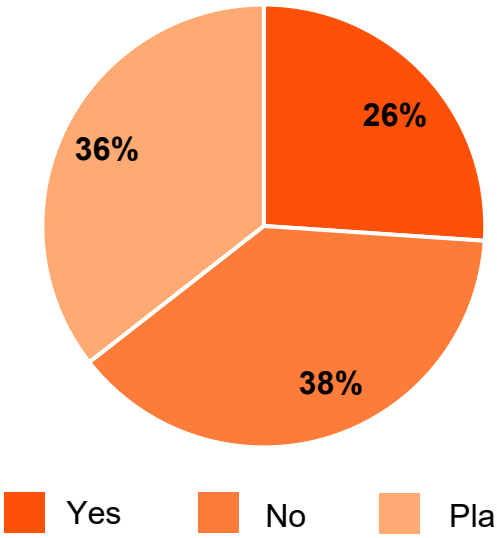
On the other hand, main processes in the finance function, such as compliance and financial reporting, remain unautomated. The reason isn't the lack of tools—it's the nature of the work: traditional RPA is deterministic and follows strict, predefined rules, producing the same output every time. By contrast, AI is probabilistic, meaning it generates the "most likely" answer based on patterns and probabilities. This introduces a margin of uncertainty. In finance, where a single incorrect figure in a statutory or management report carries real economic and regulatory consequences, certainty isn't a preference, it's a requirement. This is why the right controls, validations, and solid data foundation must be in place.

Finance is still working for its data—not the other way around.
A practical way to start is to work backwards from the business problem rather than the technology. Before selecting a tool or model, define what you want to improve and how you'll measure success: **where exactly will AI add value?** Without a clear strategy, AI efforts can become inefficient and increase exposure to inappropriate use. To avoid these pitfalls, the COBIT framework provides the domain "Align, Plan and Organise", establishing discipline and compliance for digital transformation projects through a reliable governance structure.



Agentic AI in the finance function

Q. Is your finance function exploring AI agents?



6 in 10 CFOs have begun taking a step past the research phase to pilot

Organisations look for practical ways to apply AI. This is a major milestone towards human-centered intelligent finance. The peak interest is due to agents' capabilities to operate autonomously (within set boundaries). In other words, they can perform work that previously required hours of manual judgement.

AI agents can handle tasks that traditional automation (RPA) can't, such as analysing unstructured documents (emails, chats, PDFs), interpreting natural language, spotting patterns, and extracting context from images.

Successful adopters take a gradual approach. They start with **specific, high-value use cases**, validate results and expand only when the organisation's technical and regulatory foundations are ready.

Over time, finance teams can benefit not only from a single-purpose agent, but from a multi-agent systems, where specialised AI engines operate together to accelerate existing processes.

Implementation approach

There is no single model that fits all organisations.

- **Pre-built models** can be faster and cost-effective, but may not fit unique workflows.
- **Custom models** can address specific needs, but require stronger data, governance and delivery capacity.

Value in practice

Within ERP systems, agents not only flag intercompany transaction discrepancies, they also scan supporting documents to investigate root causes and propose adjustments and eliminations, while maintaining transparent audit trails.

What's holding finance function back?

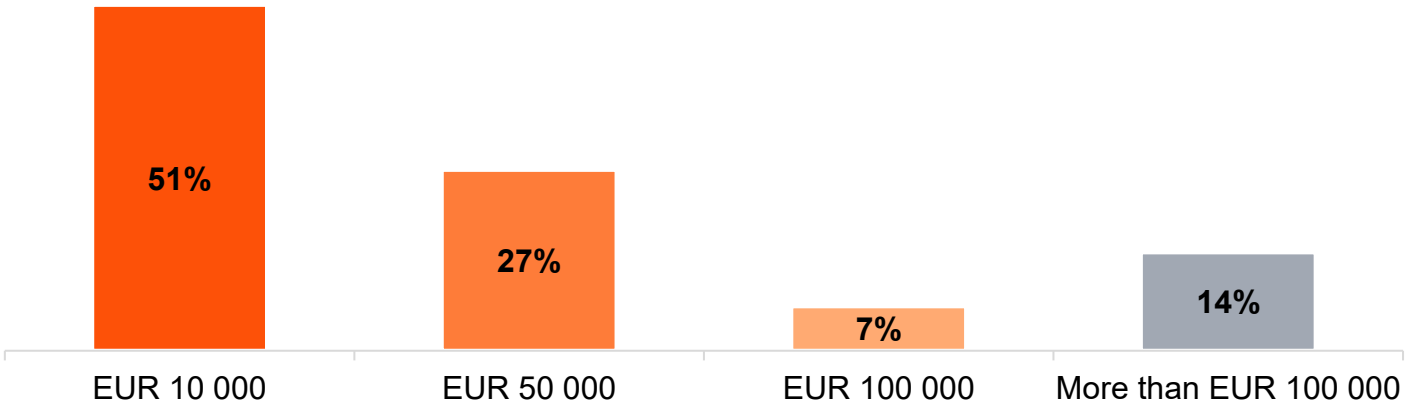
Q. How much budget do you plan to allocate for AI and GenAI products?

Ambition is high, but investment often falls short

Companies assume they can "adopt AI" quickly, cheaply, or even at no cost, mainly because they lack an understanding of how AI works and the many forms it takes. To account for the growing complexities of AI and deep learning, we can expect an increase in how traditional software and systems are priced.

The same organisations that invest tens or hundreds of thousands in ERP projects often hesitate to allocate even a fraction of that amount to a tailored AI agent, despite AI's potential to solve precisely the gaps ERPs leave behind. This results in partial implementations: systems that demonstrate promise in a proof-of-concept but fail under production realities because data, controls, documentation, and user training weren't part of the budget.

What often goes unnoticed is that AI isn't a one-time expense. Developing and maintaining it involves ongoing investment. Constant model training and system upkeep become recurring costs. CFOs must choose whether to rely on in-house or external experts.



In-house development isn't always the safest path

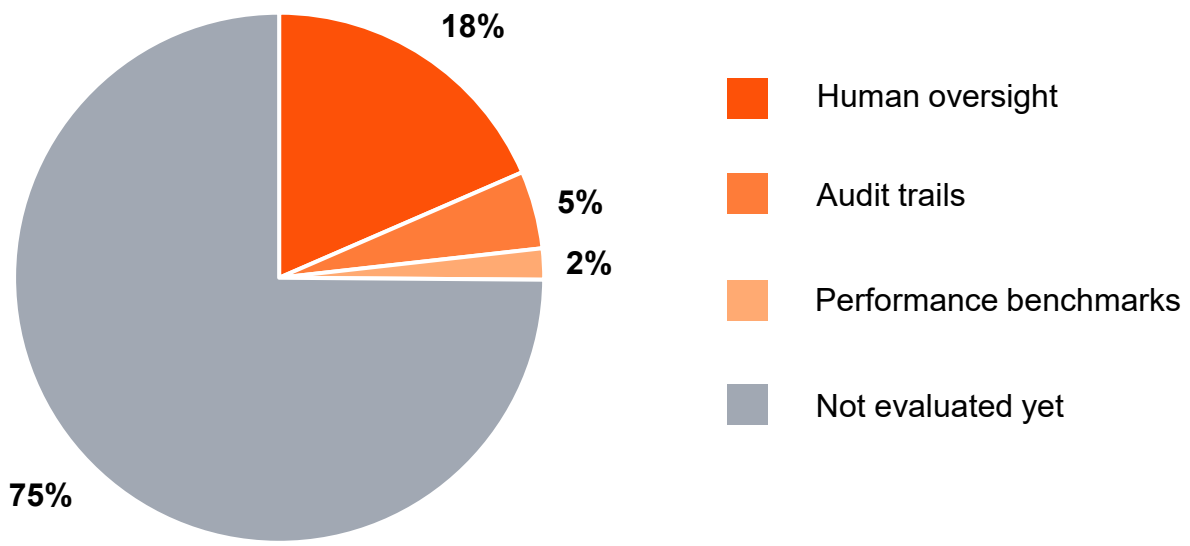
Some organisations try to build AI internally because it feels innovative. But in finance, this often leads to tools that can't be audited or governed—especially when coding happens directly on public models like GPT.

This is why many organisations benefit from **externally governed, specialised AI solutions**, built together with experienced teams.

When internal capacity is limited, combining internal process knowledge with external specialists provides a faster and safer route to results and reduces the risk of "quick fixes" that compromise data or controls.

How do we currently control AI?

Q. Do you have policies / controls in place to evaluate the trustworthiness of autonomous AI?



Trustworthiness must be demonstrated, not assumed

Most organisations haven't yet established formal AI policies, despite the huge interest towards AI implementation. Even early AI adopters rarely have clear codes of conduct, leaving "not evaluated yet" as the common response.

This creates a considerable risk—users frequently exhibit automation bias, leading them to over-rely on AI-generated content. Combined with occasional AI hallucinations, this can result in flawed budgets and cash flow projections based on fictional sales and market trends, or duplicated vendor payments.

Human oversight therefore remains the most preferred control, especially in high-priority areas like FP&A. Supervision is only effective when the people involved clearly understand the technology's abilities and limitations, and are trained to challenge outputs rather than accept them by default.

To demonstrate AI trustworthiness, organisations should introduce clearly defined metrics and measurable outcomes. Protocols and established procedures must be continuously refined in response to unexpected challenges and risks. AI governance should evolve continuously, just like the tools themselves.

Control mechanics to integrate: define acceptable thresholds, keep logs of actions and decisions taken by automation, use benchmarks and exception rules and apply segregation of duties—AI shouldn't create, approve and execute the same process end-to-end.

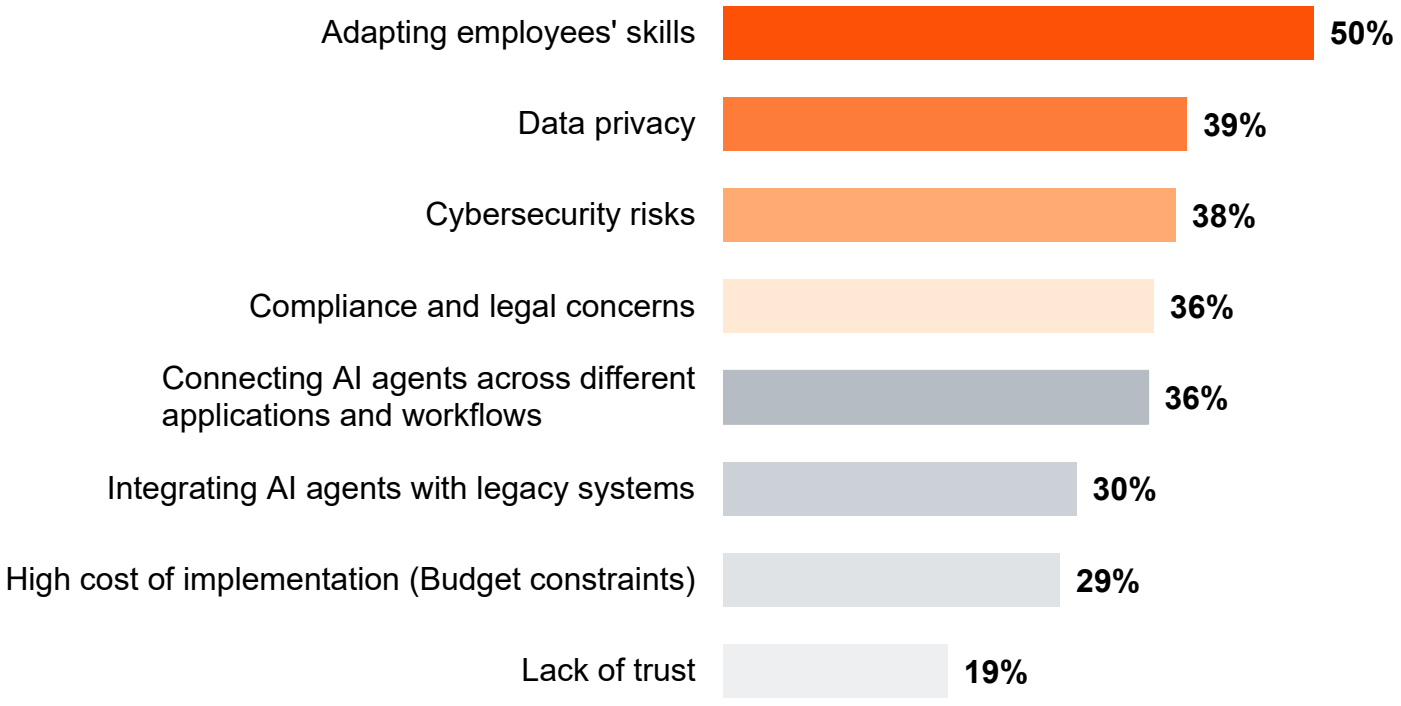
People: the most important control and the biggest barrier

Q. What are the biggest challenges/barriers in realising value from AI agents?

There's no need to hit the brakes on AI adoption. Instead, let's embrace it in a way that teams can maintain

Employees' insufficient technical competence—not budget or trust—stands out as the biggest barrier to realising value from AI. Technology is advancing faster than teams can adapt, creating a skills gap that directly slows implementation. Human review is currently the most trusted and most widely used control. Finance leaders rely on their teams to challenge inconsistencies, identify unusual patterns, and prevent automation errors. Yet the survey results reveal a striking contradiction: **the same employees we rely on to supervise AI are also viewed as one of the biggest obstacles to realising its value**.

Data privacy and cybersecurity worry 40% of finance leaders as AI gains access to sensitive and regulated information. To adopt AI responsibly, CFOs should prioritise upskilling programmes for AI literacy and prepare legacy systems. This includes role-based training for reviewers, clear documentation of expected behaviours, practical examples of correct and incorrect outputs, and guidance on when human judgement must prevail.



Note: Only the top 8 results are displayed

6

About the survey

The SEE CFO Compass Survey

We launched the CFO Compass Survey in the South-East Europe cluster, leveraging our deep expertise in finance transformation. Our aim was straightforward: to create a **platform for CFOs to share insights, exchange practices, and gain new perspectives.**

As interest grew, so did the survey's reach and participation within the region, mirroring its dynamic growth, varied business maturity, and complex market dynamics. The data gathered enabled us to compare peers more precisely and share valuable findings.

By examining organisations across industries and countries, the CFO Compass Survey provides finance professionals with a tool to evaluate their finance function's maturity and identify opportunities for real improvement.

Looking forward, we're set to expand this initiative. Our vision is to make the CFO Compass the go-to resource for the modern finance agenda—a hub where companies, partners, and stakeholders can discuss emerging challenges, stay informed, and access practical advice.

Our consistent aim is to work across our network to **deliver quality, unique experiences, helping you tackle today's challenges with tomorrow in mind.**

Let’s shape the future of finance together.

2023

127

participating organisations

2024

150

CFOs and finance leaders

2025

230+

professionals joined the initiative

SEE Partners:

Petko Petkov
Partner, Assurance
Bulgaria
petko.petkov@pwc.com

Milivoje Nesovic
Partner, Assurance
Serbia
milivoje.nesovic@pwc.com

Slaven Kartelo
Partner, Assurance
Croatia
slaven.kartelo@pwc.com

Primoz Kovacic
Partner, Assurance
Slovenia
primoz.kovacic@pwc.com

Authors and contributors:

Stefan Milenkov
Senior Manager, CMAAS,
Finance Function Transformation
stefan.milenkov@pwc.com
T: +359 894 332 940

Vasil Chinchev
Director, CMAAS,
Finance Function Transformation
vasil.chinchev@pwc.com
T: +359 895 444 356

Deyan Savov
Director,
Risk Assurance Services
deyan.savov@pwc.com
T: +359 889 409 814

Kristian Viktorov
Senior Manager
Cybersecurity & Digital Identity
kristian.viktorov@pwc.com
T: +359 893 058 585

3rd SEE CFO Compass Survey