Global CeFPro® Report

Supplier stability in operational resilience

Global survey insights and analysis

June, 2024

Supported by: Escode

Part of NCC Group

CONTENTS

TABLE OF FIGURES

ABOUT US

CeFPro®

About CeFPro:
The Center for Financial Professionals (CeFPro) is an international research organization and the focal point for the global community of finance, technology, risk, and compliance professionals from across the financial services industry. CeFPro is driven by high-quality, reliable, primary market research. It has developed a comprehensive methodology that incorporates data from its global community that has been validated by an international team of independent experts.

Examples of some of CeFPro's research include:

- Non-Financial Risk Leaders: the most comprehensive independent study of trends, opportunities, and challenges within non-financial risk

- Fintech Leaders: an international survey to assess the status of the fintech industry and provide details for informed decisions on technology and business-related matters.

To find out more, visit www.cefpro.com/research

Escode
Part of NCC Group

About Escode:
Escode, a division of NCC Group, is committed to ensuring operational resilience and peace of mind for both vendors and licensees. Whether vendors are safeguarding code or investors are licensing software, Escode's comprehensive services provide the necessary protection to safeguard investment in digital assets.

As the foremost provider of escrow services globally, Escode specializes in software and technology escrow, boasting unparalleled expertise in protecting invaluable digital assets.

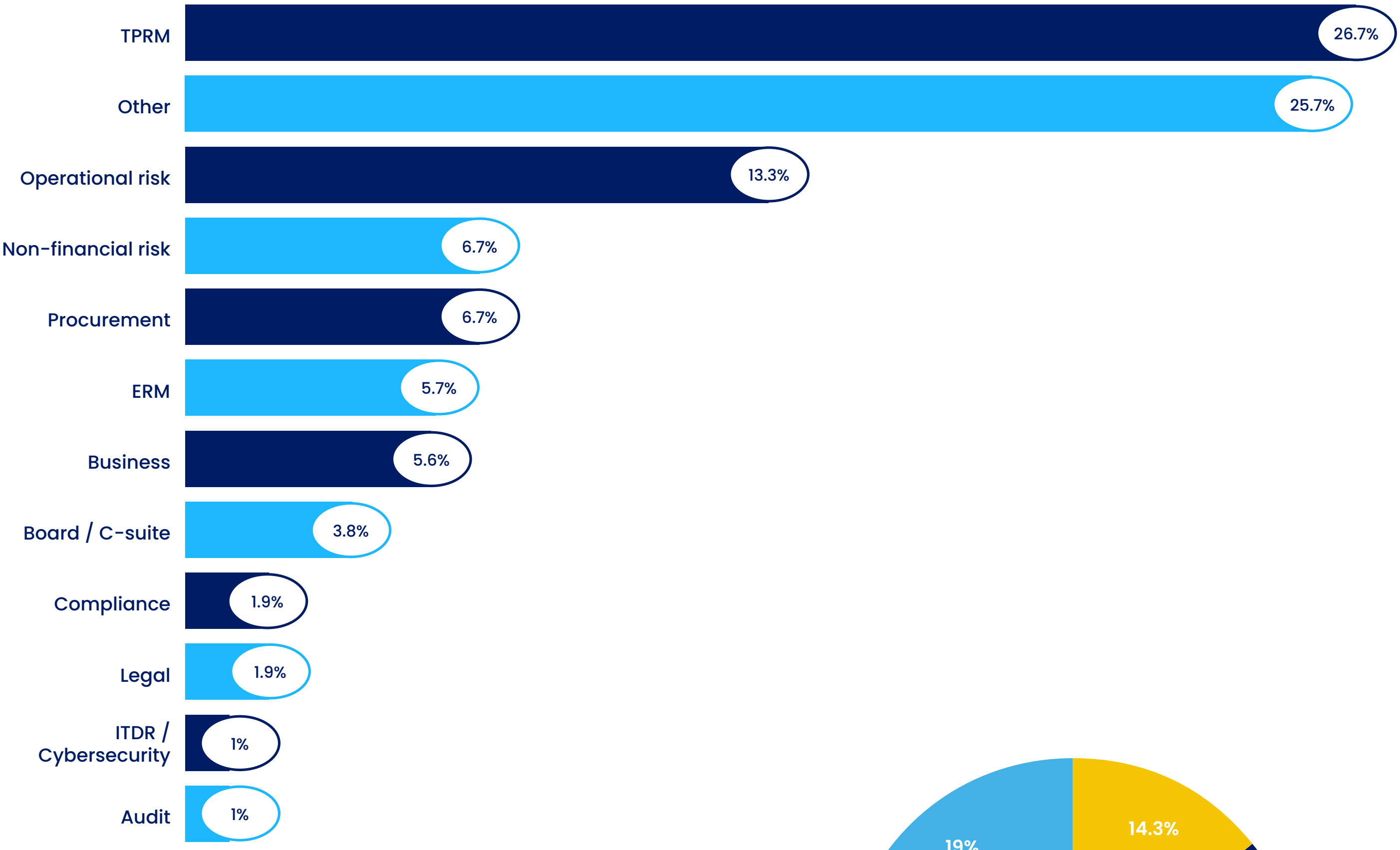
With over 40 years of industry experience, Escode has earned a reputation synonymous with trust and reliability.

SURVEY METHODOLOGY & DEMOGRAPHICS

CeFPro, in collaboration with Escode, a NCC company, conducted a global research survey to gain an international perspective on the rate at which the industry is progressing towards meeting its operational resilience requirements. The survey addressed predominantly non-cyber risks for all business-critical third party applications. The survey ran from October 16, 2023, until December 11, 2023, and received 107 responses. Upon conclusion of the survey, CeFPro's research team conducted a number of 1-on-1 interviews with industry experts, who predominantly comprised the heads of third party risk management at financial institutions in North America, the UK, and Europe. The follow-up interviews provided additional industry insight, analysis, and interpretation on the results of the survey. Their findings are referenced throughout this report.

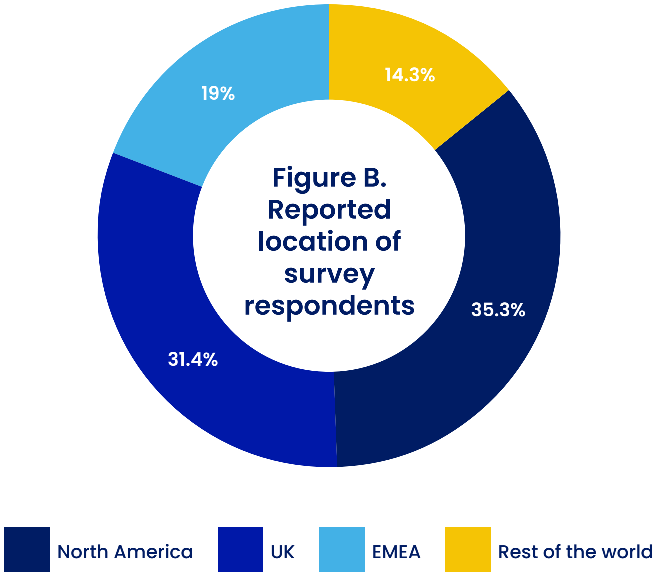
A large portion of the survey respondents were from banking institutions (46.7%). The survey also included responses from insurance, asset/wealth/investment management, service providers, fintech, and advisory organizations. Figure A outlines the range of functions represented by the respondents. A total of 26.7% of the survey respondents represented third party risk management (TPRM), while a further 13.3% represented operational risk, 6.7% represented non-financial risk, and 6.7% represented procurement, among others. It is worth noting that the second highest reported function was defined as 'Other', with the option being selected by 25.7% of respondents. It was unclear which function this cohort of respondents worked within.

Figure A. Reported functions that survey respondents work within



The geographical demographics of the survey respondents were also established, to identify any changes and variables regarding how progress is being made across geographies. Figure B outlines the breakdown of locations, with the majority of respondents, 31.4% and 35.3%, being based in the UK and North America, respectively. A further 19% of respondents cumulatively represented Europe, the Middle East, and Africa (EMEA), with an additional 14.3% representing the 'Rest of the world'; this jurisdiction and its respondents were excluded from the subsequent analysis.

With a diverse geographical split, alongside respondents from a range of organizations and functions, the survey data provides a snapshot of the industry on a broad scale. The survey results form the basis of this benchmark study, which reviews confidence levels across the industry, and how such levels align with current progress towards implementation.



BACKGROUND

In recent years, third party risk management and operational resilience have received increased regulatory and industry attention. Operational resilience has increased in stature and profile as a result of a number of regulatory initiatives, alongside a number of high-profile changes within third party risk and supply chains. As the reliance on third parties continues to evolve, and they continue to provide critical support and important business services, regulators have announced a number of global changes. As a result, effective third party risk management approaches have become more vital than ever, as the industry continues to increase its reliance on, and expand opportunities through, partnerships and third party software usage. While the use of such technologies and software provides an opportunity to advance the industry and its competitive landscape, such initiatives also introduce a potential new level of risk exposure, as supply chains evolve in complexity and risk becomes subsequently impacted/pressured by external forces.

Some examples of regulatory change referenced throughout this report are:

- The Digital Operational Resilience Act (DORA), which has been described as perhaps the most significant change to the industry in recent times. This came into force for European financial institutions on 16 January, 2023, and will apply as of 17 January, 2025.
- The joint interagency statement detailing revised guidance on outsourcing and third party risk management issued by US regulators, namely the Federal Reserve Board (FRB), the Office of the Comptroller of the Currency (OCC), and the Federal Deposit Insurance Corporation (FDIC)
- The Bank of England's Supervisory Statement (SS2/21) on outsourcing and third party risk management, which was issued by the Prudential Regulation Authority in March 2021, and the CP23/30 operational resilience joint consultation document, issued by the Bank, PRA, and the Financial Conduct Authority (FCA).

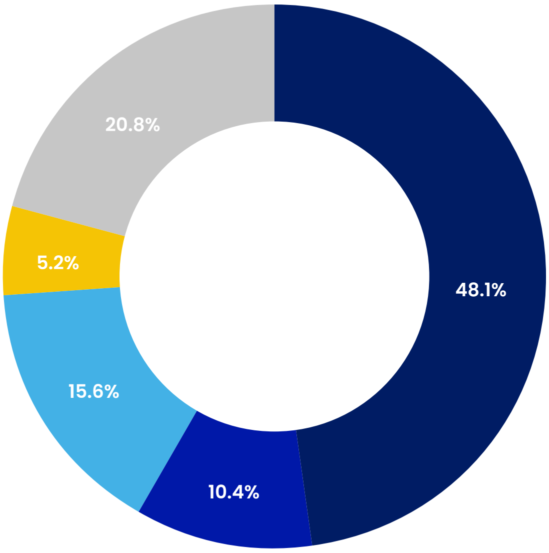
Globally, regulators have issued differing variations of these regulations. Despite minor divergences, all such changes aim to strengthen the management of third parties and mitigate the risk across supply chains. Recent regulations have placed an increased focus on important and critical services, as well as enhancing resilience.

This report views regulation on a global scale and aims to benchmark the rate of progress towards some of the transferable aspects, such as stressed exit plans and scenario testing. The research was conducted with organizations primarily across the UK, North America, and EMEA. The data is presented with a division between the EMEA, the UK and North America. The remaining 14.3% of respondents that fell under the 'Rest of the world' option were not included in the division. The survey respondents function as representatives for a range of organizations, with some representing larger organizations that operate globally and are subject to multiple regulatory requirements, and others representing smaller organizations that fall within one regulatory jurisdiction. The aim of the research is to provide the industry with a benchmark of progress, and, as many industry stakeholders work towards 2025 deadlines for aspects of their change projects, highlight the areas/sectors in need of increased focus and attention.

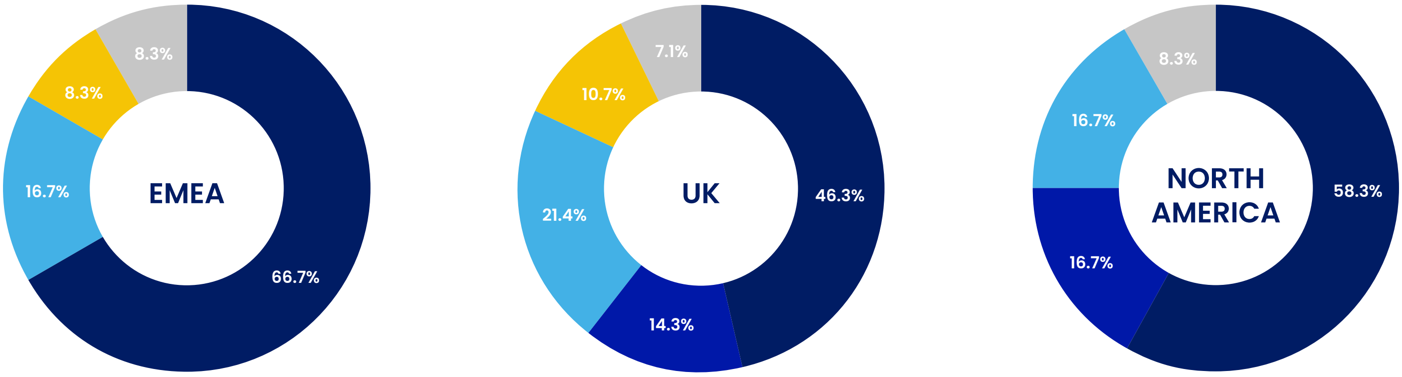
ANALYSIS

The survey began by exploring the relationship between organizations, license agreements, and stressed exit plans. There was a sharp divergence between the top two results, which are presented in Figure C. A total of 48.1% of respondents stated that they had only inserted stressed exit plans in 0–10% of their license agreements. In stark contrast, 20.8% of respondents stated that their organizations had inserted stressed exit plans in 76–100% of their agreements. There was no clear geographical reason for the division between responses, with the results remaining mostly the same across the EMEA, the UK, and North America. When conducting additional research with industry experts to validate and provide analysis on the results, those interviewed were somewhat surprised by the high percentage of respondents who stated that only 0–10% of suppliers have inserted the stressed exit plan into license agreements.

Figure C. Rate at which suppliers have implemented stress exit plans



■ 0-10% ■ 11-25% ■ 26-50% ■ 51-75% ■ 76-100%



It was highlighted that given that only 20.8% of respondents reported that their organizations had inserted stressed exit plans across 76–100% of license agreements, only 20.8% of such organizations could be considered as operating at best practice. There were varying interpretations of the question, with some respondents stating that stressed exit plans were a regulatory requirement for contracts and license agreements, and others stating that they would expect it to be applicable to only 50% of license agreements due to their nature. Others highlighted that the regulation states that stressed exit plans should be in place for material services, or services with the potential to become material over the course of their lifetime. However, it is worth noting that not all important business services require a license agreement. It could be suggested that the 20.8% of respondents who stated '76–100%' are more prepared for change, and are updating contractual terms to include the requirement and future-proof their relationships. The number of respondents in the 76–100% bracket could also be lower due to their focus on license agreements, whereas regulators and organizations have typically focused more on master service agreements. Yet, even with the focus just on license agreements, interviewees expected the majority of respondents to report that they operated in the 51–75% bracket, which only received 5.2% of votes.

Another area discussed in interviews was the scope of the 0–10% bracket. It is possible that of the 48.1% of respondents that fell within the 0-10% bracket, some have not even started inserting the requirements, and may in fact be on 0%. The same can be said of the higher end of the scale, where it was seen as unlikely that organizations included the requirement in 100% of their service agreements, given some of the limitations of, and pushbacks from, some technology providers. It was repeatedly highlighted that cloud service providers often do not accept terms and conditions that would be included within contractual terms to allow organizations to cover 76-100% of service agreements. There were several internal challenges highlighted that may also slow progress, the first of which being whether senior management had the buy in and drive to push the program forward. Without a push from leadership, changes and the development of metrics can be slow. Some services were also seen as so substantial that they would require an entire change in business model to develop effective plans, and require far more detailed stressed exit plans and contingencies as a result.

Historically, technology companies have been very difficult to secure license agreements with, or even get the right terms in place prior to a potential agreement. Companies like Amazon, Google, and Microsoft are so large and dominant in the market that they offer only a small amount of negotiation. Organizations have limited capacity to negotiate, and only have the option to report to regulators that the vendor has not added or agreed to clauses for stress exit plan requirements. The Bank of England's SS221 outlines that organizations must notify regulators for review as to whether the relationship can continue, especially for global systemically important banking organizations (G-SIBs). In larger companies, there are existing issues where high-risk suppliers are struggling to arrange contingencies due to the demand across the industry; questions remain, and are highlighted throughout this report, as to whether they will be able to close the gap in time.

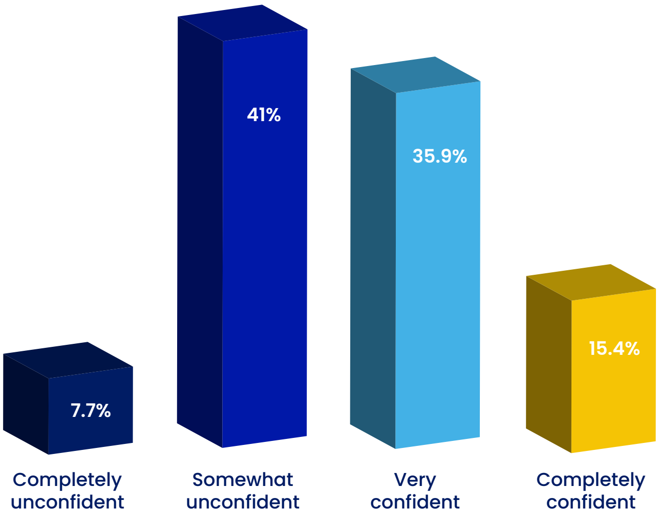
The subject of resources was raised as another potential reason as to the range of disparities reported in the data. Analysts suggested that the respondents that reported 76-100% could represent larger organizations with more substantial teams and resources, which would make them capable of reviewing and updating terms for a high percentage of license agreements. Larger organizations are also perceived to have the technical capabilities and resources for long-term remediation plans and are expected to look beyond compliance to best practices to ensure their security. However, this is only hypothesized and cannot be proven with the currently available data set with some views stating the contrary. Others have seen smaller regulated entities as having a better grip on the situation. Larger financial institutions can tend to use larger suppliers who are inundated with requests and therefore facing difficulties in keeping up with the changes.

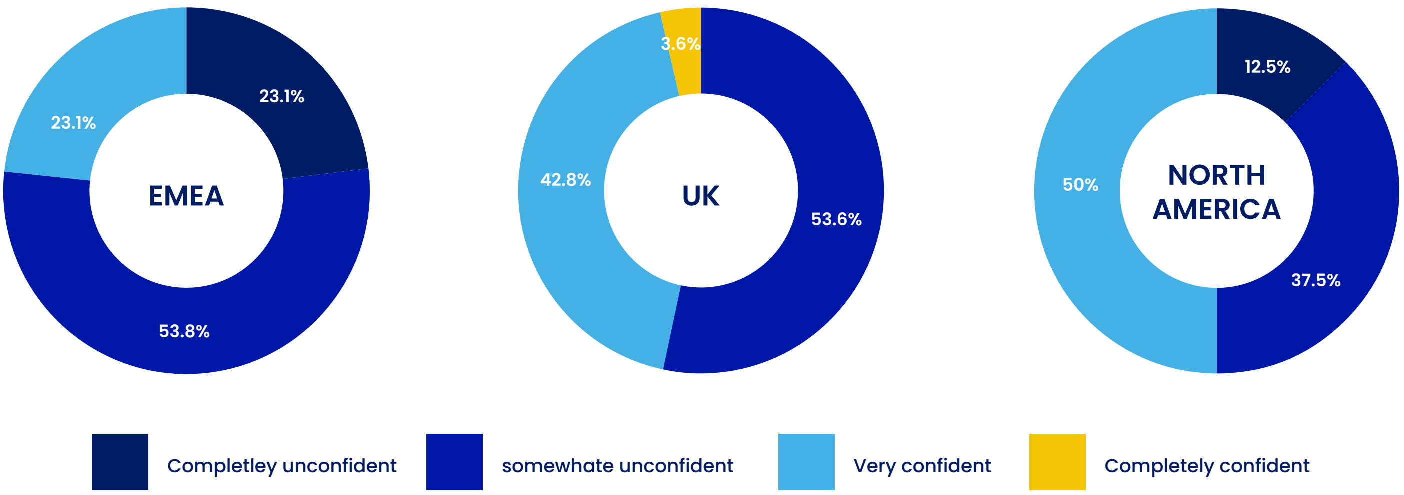
This report explores in much more detail some of the challenges organizations are facing in interpreting the regulations, and understanding their influence across jurisdictions. It also examines the challenges suppliers are having with understanding the requirements, and the root of their occasional unwillingness to provide the required information or agree to terms.

IMPLEMENTATION PROGRESS

The survey also explored progress towards implementation, with respondents rating their confidence level regarding how far their organizations had progressed towards implementing the regulatory expectations. A total of 41% of respondents were 'somewhat unconfident' of their progress, with an additional 35.9% reportedly 'very confident' (Figure D). This is where the survey saw some greater demographic variations. While only 7.7% of the overall survey respondents reported that they were 'completely unconfident' in their capability, this represented 23.1% of EMEA respondents. This low level of confidence appears to be more represented in the EMEA region than others, particularly when contrasted to the results provided by the UK-based respondents, none of which reported feeling 'completely unconfident'. This could be due in part to delays in the requirements being published in January 2024. The UK was the only demographic of the three included in analysis to have any respondents rate 'completely confident', with 3.6% reportedly certain of their organization's capabilities; the 'Rest of the world' respondents make up a large portion of the 'Completely confident' responses.

Figure D. Respondent confidence regarding stressed exit plan implementation





It was highlighted in additional 1-on-1 research with industry experts that the majority of respondents were working in risk in some capacity – a field of financial services known for being somewhat pessimistic in nature. The level of confidence is also somewhat conducive with Figure C where, on the whole, the industry has made limited progress inserting the stressed exit requirements into license agreements. With the percentage actioned in Figure C, it could be argued that the confidence levels in Figure D are somewhat high. As respondents are working towards different implementation requirements and timelines, there was an expectation that the confidence levels would evolve over the course of 2024, as many organizations work towards a 2025 deadline. It was highlighted in multiple discussions with industry experts that budget allocation within TPRM can often be challenging when a deadline is not imminent.

There were concerns, highlighted primarily in the UK- and North America-based research interviews, that organizations may not have the technical ability to implement and meet the requirements in time. However, given implementation timelines for 2025, there was an expectation that the UK would be further along; however, more than 46% of UK respondents were 'somewhat unconfident', though also receiving the highest level of 'completely confident' respondents, with 7.2%. North America saw the next highest levels of confidence, with 45.5% of respondents reportedly 'very confident' and 4.5% 'completely confident'. This could be due to the UK regulations being announced much earlier than the US, therefore providing an advantage.

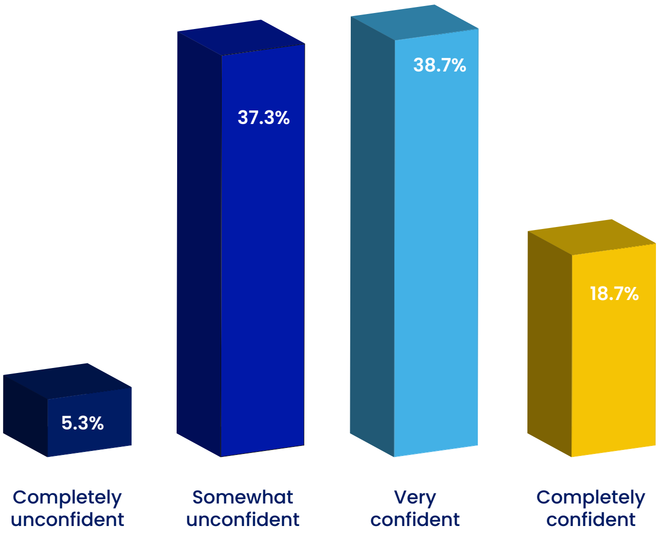
Many of the EMEA-based respondents highlighted that DORA was a key obstacle and/or challenge for TPRM professionals. The Act is considered by many to be the most significant regulatory change initiative in recent times, primarily due to its inclusion of the provision for critical third parties, and other requirements that have not been utilized in Europe previously. DORA poses a significant challenge to larger organizations, as it complicates their ability to communicate the change and messaging across business units and across a larger vendor network; indeed, DORA was described as more substantive than the resilience requirements used by the UK, US, and Australia. This is reflected, in part, by the figures presented in Figure D, which demonstrates that only 15.4% of EMEA respondents had any level of confidence regarding the Act.

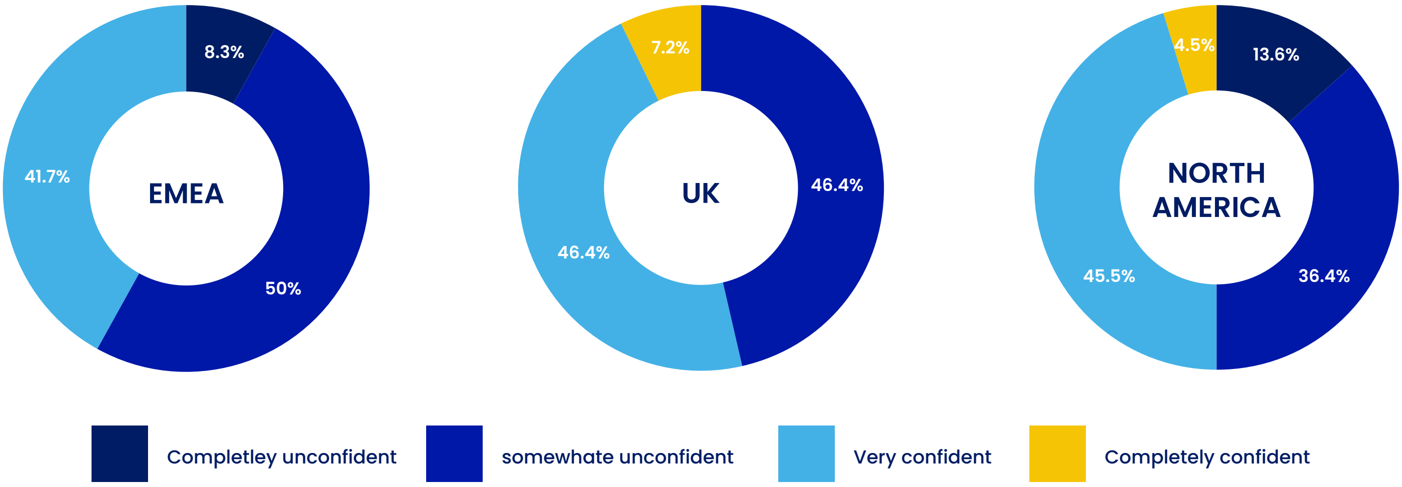
STRESSED EXIT PLANS

Looking ahead to deadlines for stressed exit plans, the survey asked participants about their confidence level in having stressed exit plans in place before the compliance deadlines. While respondents were subject to their regional- and geographical-specific deadlines, there was a fairly high rate of confidence across the board, with 38.7% of respondents stating that they were 'very confident' and 18.7% stating they were 'completely confident' (Figure E). The responses to this question did not significantly diverge based on jurisdictional variations, with all demographics seeing the largest percentage of respondents stating they were either 'somewhat unconfident' or 'very confident'. The UK saw both the highest rate of both 'very confident' responses (46.4%), and 'completely confident' responses (7.2%). Once again, the EMEA region reported the largest level of low confidence, with 50.0% of respondents stating they were 'somewhat unconfident', and 8.3% 'completely unconfident'.

Many of the industry experts CeFPro interviewed as part of their follow-up research were surprised by the results. Several expected the level of respondents reporting 'very confident' to be higher. There was a sense that there should be a higher level of confidence across the industry, both more broadly and within jurisdictions, due to the prior establishment of implementation timelines and previous investment into the area.

Figure E. Reported confidence levels in the implementation of stressed exist plans prior to deadline





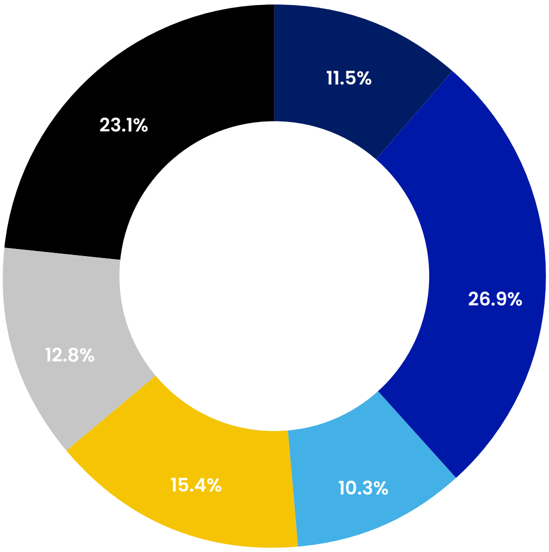
Respondents were also asked to describe what percentage of their existing material suppliers they already had demonstrably successful stressed exit plans in place for. The question produced interesting results. Approximately 26.9% of respondents stated that they have demonstrably successful stressed exit plans in place for 1–20% of their material services, and 23.1% reported having similar plans in place for 81–100% (Figure F). In exploring the results further, follow-up interviews highlighted that the outlying pieces of data from this could reflect the time spent on specific aspects of implementation, with the heavy load falling at the front end. The process of writing and testing plans was highlighted as being highly time-intensive. Therefore, although some respondents may only be able to demonstrate successful stressed exit plans for 1-20% of their suppliers, they may have completed the bulk of the remaining 'heavy lifting' tasks for the others, or be in the testing phase of written plans. Again, results here were expected to change drastically towards the end of the year, as organizations begin wrapping up and implementing the plans. Assuming plans have been written in priority order, and testing conducted the same, finalizing plans for material business services could be more advanced than the chart would imply.

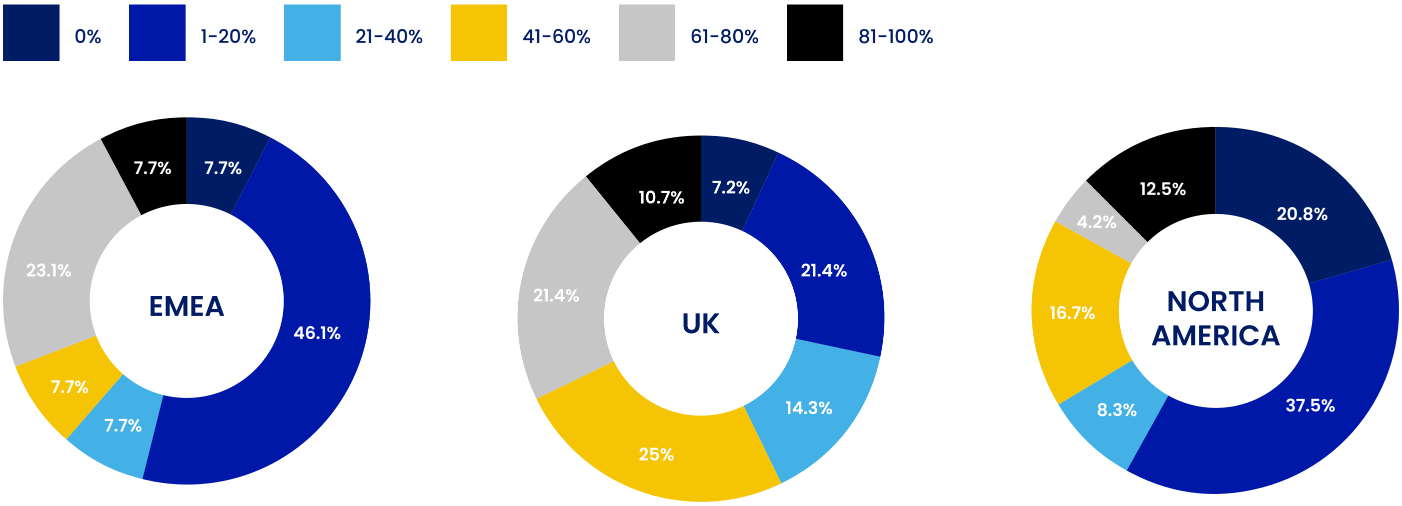
Figure F highlights a significant disparity in progress across the industry, specifically relating to progress across jurisdictions and individual respondents. The divergence here is indicative of inconsistencies in approaches across organizations. This could be as a result of internal challenges, with smaller organizations or teams being less resourced and able to manage/negotiate the changes, or suppliers being unwilling to supply, or unable to resource, plans on the scale required. Other suppliers and larger tech companies, such as Amazon, Google, and Microsoft, are often difficult to negotiate contractual clauses with, or collect information from, as required. This further compounds the need for the UK/EU critical third party regulation, and the need for more focus in North Americas on more vigorous critical third party regulations.

Industry experts were surprised that, given the requirements for material service providers to have exit plans in place and accommodate stressed exit plans is mandatory and fast approaching, any organizations reported that they had less than 61% of their services covered were risking non-compliance. As organizations are required to report to regulators any suppliers unwilling or unable to comply, we may see a sharp uptake of suppliers being reported towards the end of the year. It is worth noting that this step should be the exception and not the norm. As exit plans have been a requirement in some regulations for some time, there should be a level of maturity in certain jurisdictions.

When comparing Figures E and F, levels of confidence across geographies were fairly consistent, with more than 57% of respondents stating they were either 'very confident' or 'completely confident' that they would have stressed exit plans implemented before the compliance deadline, compared to the 38.4% who have reportedly 20% or less demonstrably successful stressed exit plans in place. This could further support the hypothesis that although organizations may not have fully demonstrable stressed exit plans in place, much of the upfront work in planning and testing may have been completed. With only 23.1% nearing finalization of the plans and implementation of the full requirement, confidence seems to outweigh progress. 2024 may yet prove to be a pivotal year, with exploration required to see how the industry will progress.

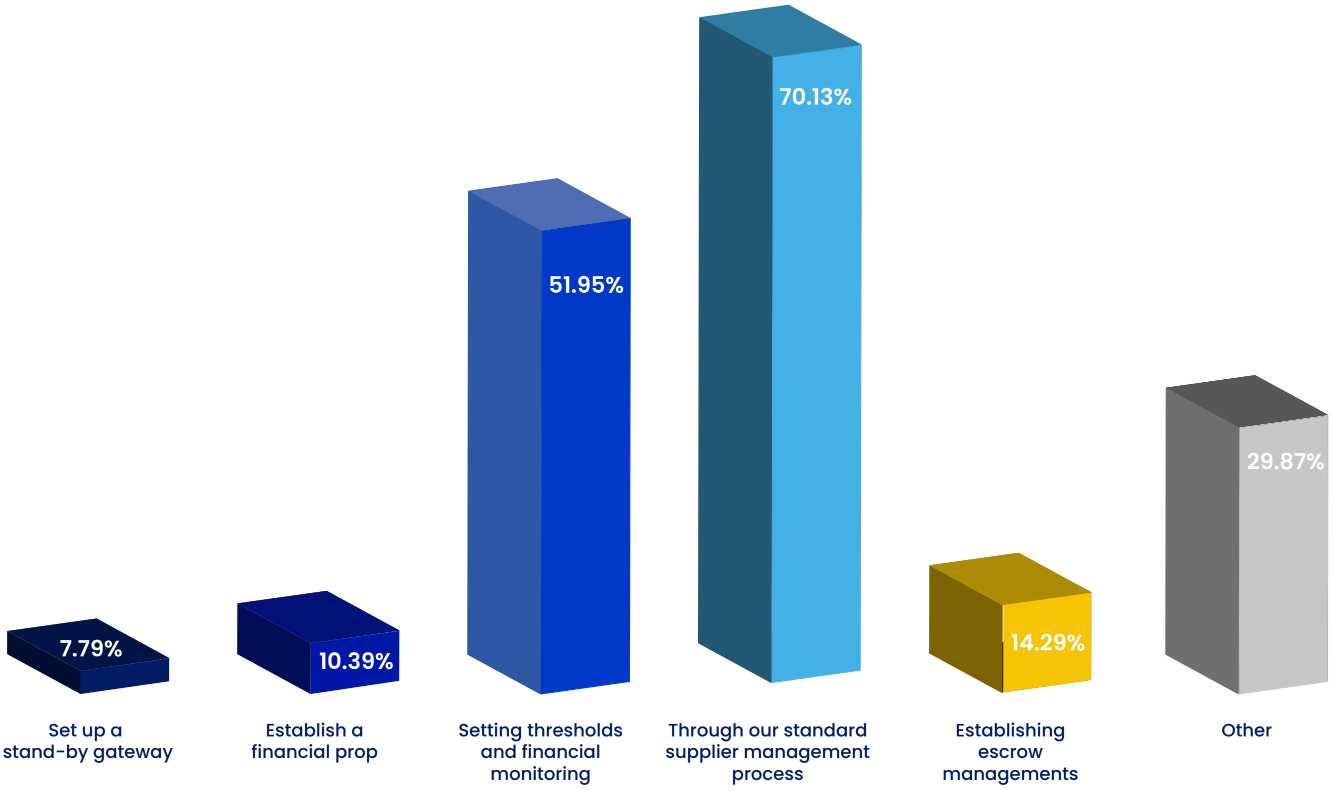
Figure F. Distribution of stressed exit plans across material services, overall and by jurisdiction





MITIGATING SUPPLIER FAILURE

Figure G. Responses to mitigating failure, overall and by jurisdiction



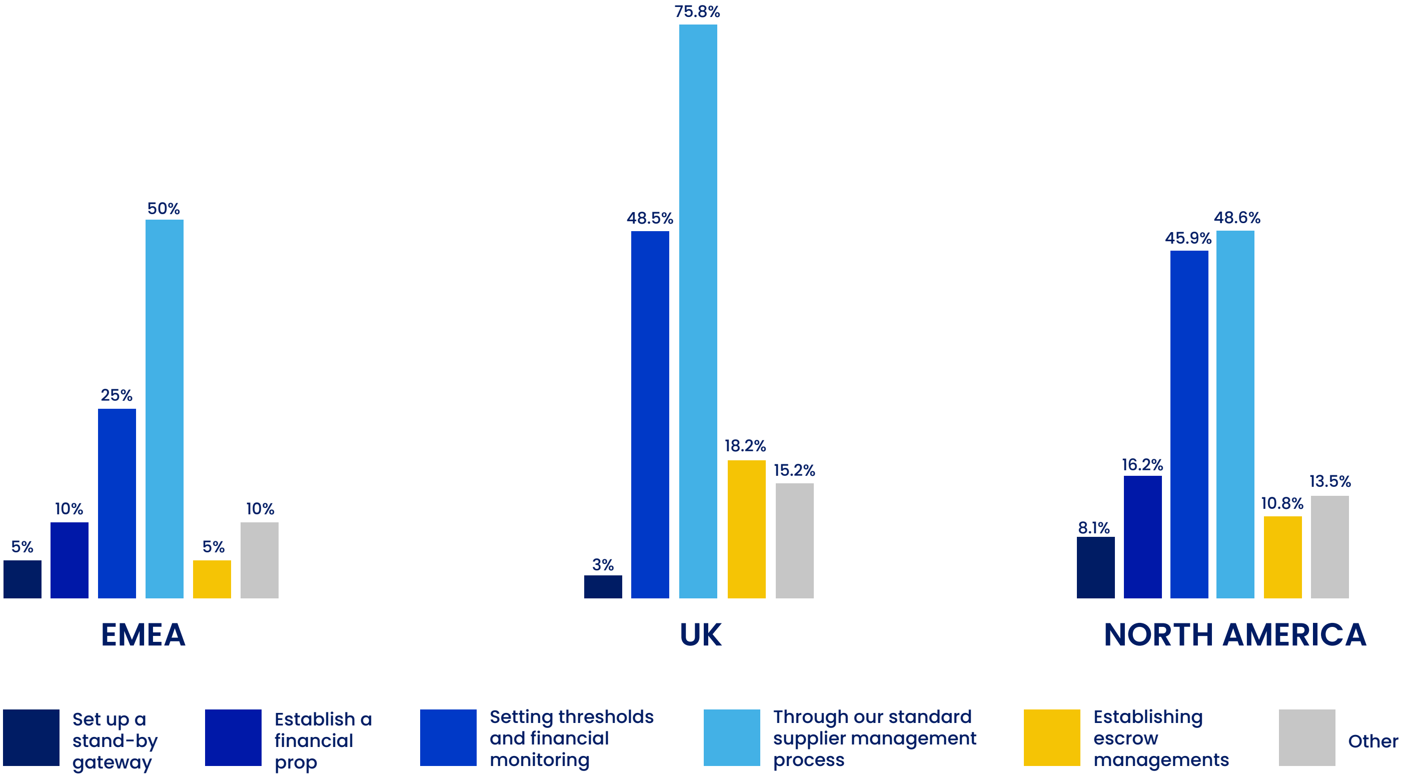


Figure G explores approaches to mitigating supplier failure. Approximately 70.1% of respondents reported that they did so 'through our standard supplier management process', while almost 52.0% reported that they set 'thresholds and [conducted] financial monitoring'. The third highest reported category was 'Other', with 29.9%; however, when prompted to outline what that could consist of, most respondents highlighted areas that would typically be classified under standard supplier management processes; areas included operational resilience frameworks, exit strategies, TPRMs, business continuity, contracts, etc. To maintain the integrity of the data, these responses were not included 'through supplier management process'.

Approximately 52% of respondents selected 'setting thresholds and financial monitoring' as a key tool for mitigating supplier failure. While there were minor fluctuations in percentages across jurisdictions, it was consistently ranked as the second most popular option. Although a popular tool across jurisdictions, setting thresholds and financial monitoring provides a short-term view of financial health and only gives an indication at the point of impending failure. It does, however, provide an understanding of the risk profile, though challenges arise with monitoring financial thresholds. The industry experts noted that this should have been ranked higher, as it could be considered a part of standard supplier management processes, and that tracking supplier failure and monitoring against service level agreements (SLAs) is something that all organizations should engage in.

Less popular responses were 'set up a stand-by gateway' and 'establish a financial prop', receiving 7.8% and 10.4%, respectively. These results were not a surprise to the industry experts. Establishing a financial prop was described as a highly reactive approach that exposes the organization to huge expenses that cannot be scenario-tested. As an approach to mitigate supplier failure, it is very hard to assess the funds required, as well as the length of time the financial prop can buy the organization providing said prop. The funds allocated to the financial prop are effectively unavailable, and the prop should be ring-fenced due to its risky nature. It is worth noting that as respondents could have selected all options that applied to their organizations', it is likely that this was not any organizations' sole response; if this is the case, it would suggest that several such organizations have very high risk appetites.

Mitigating supplier failure by jurisdiction

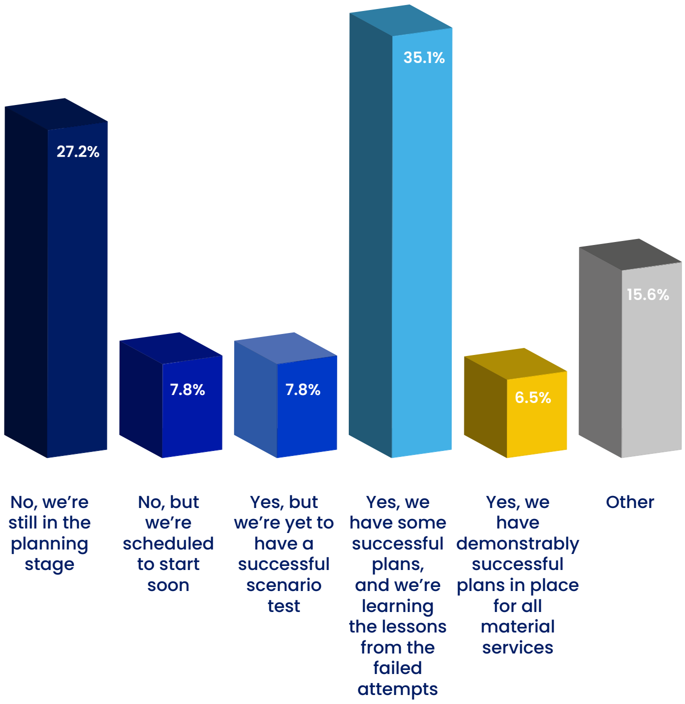
Overall, a total of 14.3% of respondents reported that they were 'establishing escrow managements to mitigate supplier failure. As industry experts mentioned that escrow Is a solution used across the UK, US, and APAC, it was surprising to see that it had not been selected by more respondents. When broken down by jurisdiction, the UK seemed to leverage this option the most, with 18.2% of respondents selecting it, followed by 10.8% of the North American cohort, and 5% of the EMEA. Escrow management is an area that may require further education across the industry as to its value and inclusion within regulations. With 85% of the total survey respondents not leveraging escrow management, decisions will need to be reviewed annually to establish an alternative mechanism to mitigate risks of supplier failure. It is particularly surprising that escrow isn't used at a higher frequency in both the US and UK, as it is directly named in both sets of regulations. Lower escrow usage in the European region is understandable due to the limitations of directly naming a solution by the regulator. However, it was also highlighted that escrow is not applicable to all relationships, which may explain its limited selection by respondents. This could be indicative of the type of relationships organizations are engaged with, rather than the value of using escrow management as a tool to mitigate supplier failure.

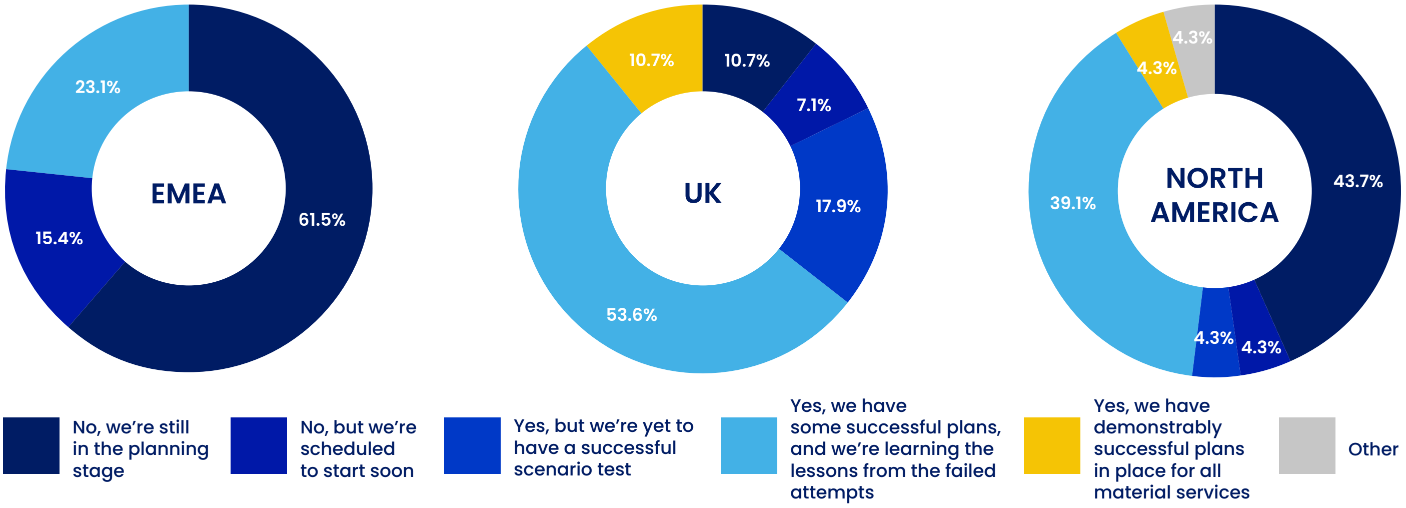
SCENARIO TESTING

Next, the survey looked into scenario testing and to what extent organizations have undergone it as part of their compliance programs. Scenario testing is a big change with a host of challenges for implementation. It was, therefore, not as surprising as it perhaps it could have been that 27.2% of respondents reported that their organizations had not undergone testing, but were in the planning stage. A further 7.8% of respondents reported that their organizations had not undergone testing, but were scheduled to start it soon (Figure H). Considering that more than 34% of the surveyed organizations had not undergone any level of scenario testing, and a further large portion are still in the planning stage, questions can again be raised as whether the high confidence levels reported in Figure E regarding the capacity of organizations to meet the implementation deadlines are well-founded.

The results to this question yielded the greatest level of disparity between jurisdictions, with 61.5% of EMEA respondents voting 'no, we're still in the planning stages', compared to 43.7% and 10.7% from North America and the UK, respectively. In was again highlighted that resources could be a challenge here, given the scale of the work required. Smaller organizations or teams may struggle with having the resources and expertise to come up with a viable solution. While large firms may have more contracts that would require testing, they would also be expected to have sizeable contracts that vendors would not want to lose; therefore, they would be expected to prioritize testing due to the leverage that larger organizations often hold. The industry has seen a lot of discussion as to how scenario testing works, and how to practically deliver it and make it meaningful, without introducing an entire team of people to see it through. The industry is still on a journey regarding the optimized outcome for this, with differing levels of maturity across sizes of organizations and jurisdictions.

Figure H. Number of organizations that have undergone scenario testing, overall and by jurisdiction





However, it should also be highlighted that more than 48.0% of respondents reported some level of success with stressed exits, with 35.1% stating they have 'successful plans, and [are] learning the lessons from failed attempts', and an additional 6.5% reportedly having 'demonstrably successful plans' in place for all material services. Again, it is worth noting that of the 6.5% of overall respondents who reported having successful plans in place for all material services, the majority of them are from the UK; 10.7% of UK-based respondents stated that it was their position. An additional 53.6% of UK respondents reported that they had 'some [level of] successful plans' in place, and only 17.8% stated that they had not undergone scenario testing or were scheduled to start soon.

Industry experts outlined that while scenario testing is an expectation as part of business continuity testing, regulators have offered little guidance on it so far. Therefore, it could be expected that as more organizations begin seeing successes and lessons learned, more information and guidance could become available as the industry continues to develop in response to the change. Regulators have become more prescriptive in recent releases, though there remains much to be learned as the industry progresses. Jurisdictional differences are noted in the expectations for scenario testing, with the UK seemingly more advanced than other regions, potentially due to the more prescriptive nature of the requirements.

GOVERNANCE

The next portion of the survey explored governance structures, delving into ownership, responsibility for mitigating risks, and the management of supplier failure. Question 11 explored who was responsible for 'mitigating the risks of supplier failure, service deterioration, and concentration risk for Saas?' (Figure I). The most striking finding reported in in Figure I is the level of uncertainty across the industry; approximately 32.3% of respondents reported that they were 'unsure' regarding who in their organization was responsible for the mitigation of supplier failure, service deterioration and concentration risk for SaaS. While this result was less prominent in the UK-based cohort of respondents, with only 7.7% of them selecting it, the EMEA and North American cohorts reported it in greater numbers, with 30.0% and 23.5% of them selecting it, respectively. The level of uncertainty demonstrates a lack of understanding of the responsibilities across organizations. These responsibilities have been described as 'poorly defined', which, in some cases, could lead to inconsistencies across jurisdictions and organizations. Given the target of this survey, it raises questions as to whether people are aware of their responsibilities and what they are responsible for. The level of uncertainty also demonstrates a lack of maturity in the industry, and an overall lack of firm-level implementation. However, it is worth noting that as not all organizations group supplier failure, service deterioration and concentration risks together, with concentration risk being seen as an outlier by some, these results may not be completely reflective.

According to the regulations, the 'correct' answer is 'end-user'. However, this option only received 12.3% of the overall respondent votes. Interestingly, when the results were broken down by jurisdiction, the EMEA region scored the best, with 20% of EMEA-based respondents voting end-user - though it is worth noting that this region also received the highest percentage of 'unsure' responses (30.0%). Only 19.1% of the UK-based respondents voted 'end-user', as did only 5.9% of North America-based respondents. Industry experts highlighted that it was worrying that more than 87.0% of the survey's respondents were not aware of the correct answer, with so few knowing that the end-user is responsible for risk across all regions. Again, when reviewing this result in conjunction with the levels of confidence reported in Figure E (50%), the levels of progress and understanding reported by the survey respondents appears to be misaligned with their confidence in their organizations capacity to meet the upcoming deadlines. The end-user remains responsible for supplier failure, service deterioration, and concentration risk; SaaS providers do not need to comment on any, as they are not responsible for it. The question demonstrates the levels of further education that are required for those working in the industry, as 'SaaS providers', 'cloud providers', and their associated risks as yet not appearing to be well understood or addressed.

The survey went on to further explore the concepts of ownership and accountability as it applies to supplier failure, service deterioration, and concentration risk within organizations. Question 12 asked respondents who they felt owned the risk for all three categories and who manages the risk (Figure J). Overall, 35.9% of respondents identified the 'Board/C-Suite' as owners of the risk of supplier failure, service deterioration and concentration risks, with 'business continuity' following with 18.8%, and 'TPRM' with 17.2%. The results here were somewhat alarming, highlighting that organizations may not be communicating effectively to the business, as some industry experts believed that the Board/C-Suite should ultimately own the risk, while others defined 'ownership' as sitting with the business.

Figure I. Range of roles deemed responsible for mitigating risks of supplier failure, service deterioration and concentration risks for Saas

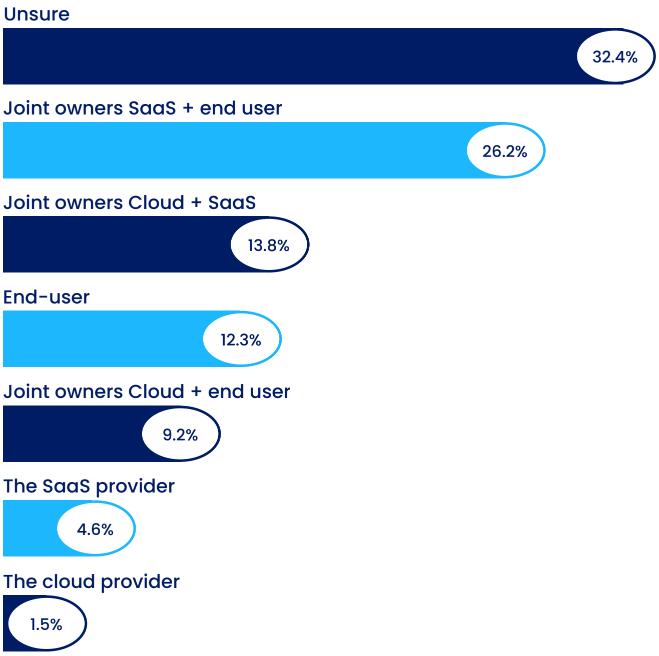
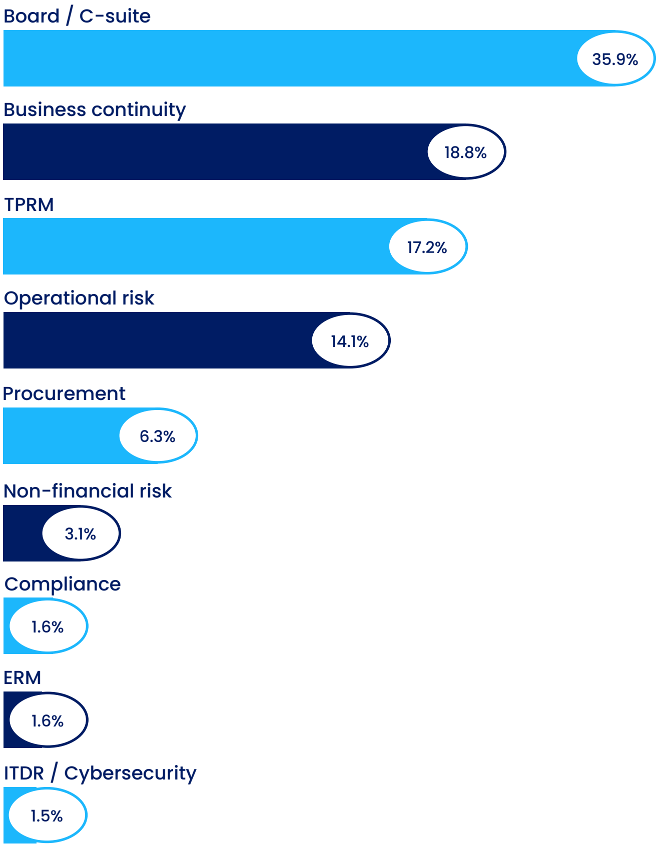


Figure J. Sectors deemed responsible for ownership over supplier risk, service deterioration and concentration risk

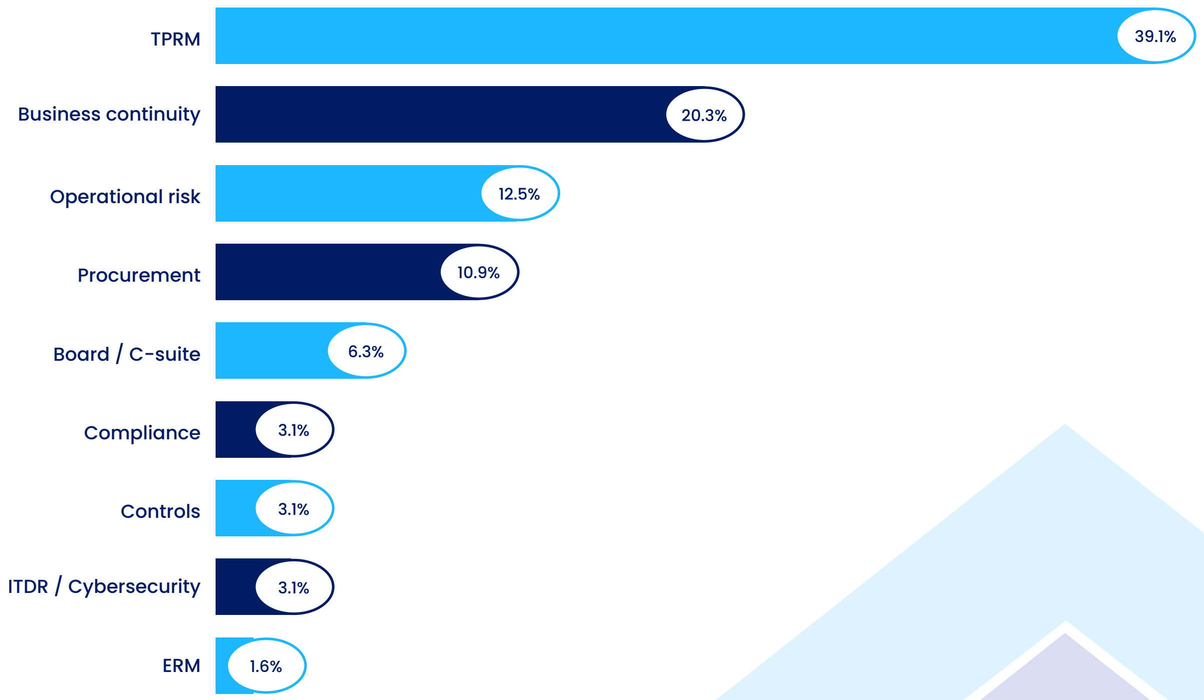


Ownership is another area that is inconsistent across the industry, particularly across jurisdictions. While the UK and EMEA both voted the Board/C-suite as having ownership of the risk, the majority of North American respondents (43.8%) voted that ownership of the risk of supplier failure, service deterioration, and concentration risk instead fell to TPRM. This was followed by an additional 18.7% of respondents who voted that operational risk were the owners, alongside 18.7% for Board/C-suite, which placed both options as the joint second most reported result for the North American audience.

In one follow-up interview with industry experts, it was outlined that regulators define accountability and, therefore, ownership, as sitting with the Board. Responsibility for management lies with the business, with options like TPRM, operational risk, and business continuity providing a service to the business, platform, or workflow, as well as allowing them the ability to manage the risks.

In contrast, Figure K reviews the approaches for management of the risks of supplier failure, service deterioration, and concentration risk within organizations. When asked, the survey respondents overwhelmingly selected 'TPRM', with 39.1% of the overall respondents electing it as their primary response. This was followed by 'business continuity', which received 20.3%. Although TPRM was the most popular response across all the respective jurisdictions, it serves to demonstrate the divergence in approaches across the industry. There does not appear to be a standardized approach with an identified management of the risk, or ultimate ownership. This could leave financial institutions open to risk/dangers if uncertainty remains as to how responsibilities are handled internally. As much as all the teams highlighted in Figure K should feed into the decision-making process, ultimately, TPRM teams should be managing the risk. The fact that TPRM, who should be ultimately handling the risk, was not selected by over 50% of respondents demonstrates a lack of consensus between what is expected by industry regulators, and the courses of action that organizations/respondents themselves are taking.

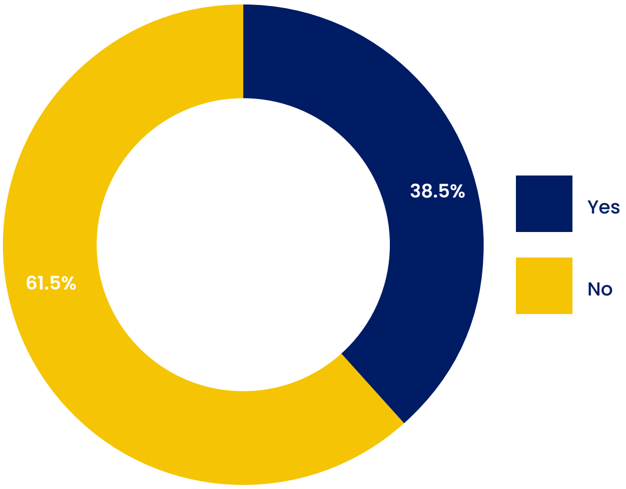
Figure k. Management of risks of supplier failure, service deterioration, and concentration risks



CLOUD

Although they are a relatively new type of provider, cloud service providers have significantly increased in number of late, with uses across the industry and varying degrees of concentration. When considering the global regulatory change initiatives, the survey asked respondents whether their organizations were adopting any different approaches to on-premise versus cloud applications. 61.5% of the overall respondents stated no, with 38.5% stating yes (Figure L). This distribution changed across jurisdictions, where more than 50.0% of the EMEA- and UK-based respondents stated that they did adopt different approaches in the treatment of on-premise versus cloud applications.

Figure L. Variations in approach to on-premise vs. cloud applications



In the follow-up research with industry experts, it was generally accepted that cloud applications should have a different approach due to their unique nature and the criticality of their relationships. Some went as far as to say that it should be 100% of the industry stating 'yes' to the question. However, cloud services need to be understood in greater detail before this can be possible, as the end user has no sight of deployment mechanisms, processes, or overall architecture. As outlined in Figure I, the end user can be seen as responsible for mitigating risks of supplier failure, service deterioration and concentration risks. Therefore, insight and unique processes to understand cloud applications are required. Global regulations also highlight that due to the materiality of cloud services, a higher level of resilience is required, or more detailed resilience plans need to be put in place. A one-size-fits-all approach to supplier resilience was seen as potentially non-compliant due to the risk introduced. Cloud services introduce a high level of concentration risk in some respects. This report has identified several areas in which industry figures diverge in terms of their understanding of ownership, accountability, and management. This lack of comprehensive understanding could contribute to the one-size-fits-all approach.
Those respondents that selected yes were asked, where appropriate, to provide a text response as to what these approaches looked like, some examples are highlighted in Figure M.

The text responses demonstrate why approaches should differ to on-premise versus cloud applications. Variations in approaches appear across the board, with many highlighting a higher level of scrutiny, with others reliant on the cloud provider themselves. Overall, understanding of resilience within cloud providers was lower than expected, with more than half allowing potential risk to enter. Others are exploring options and developing ways to ensure the risk is properly managed by adopting different approaches.

Figure M. Outline of differences in approaches to on-premise vs. cloud applications

'Material outsourcing arrangements carry more due diligence requirements being classed as critical suppliers'

'The controls that are assessed are bespoke for each'

'More in-depth analysis of cloud apps to ensure reliability and data security'

'More robust controls and a shared responsibility model in place for cloud application'

'We run hybrid models for internal data, and on-premise for confidential and higher classified data'

'Follow cloud service providers recommendations on approach to cloud applications and apply own policies to on-premise application's

'Review network connection dependencies'

'There is more due diligence on data protection for cloud applications'

'Controls for cloud are still in development'

'Different span of control, redundancy is easier to accomplish on-site'

'There is more scrutiny of cloud as it sits in the third party domain. Therefore, data privacy, cybersecurity, and risk assurance protocol will apply'

'Cloud very restricted, as we only deal with private cloud, not public cloud, in addition to the regulatory requirements'

'Hosting review board process for cloud'

'Very different scenario - one is a service with reliance on supplier, the other is a deployment of software internally'

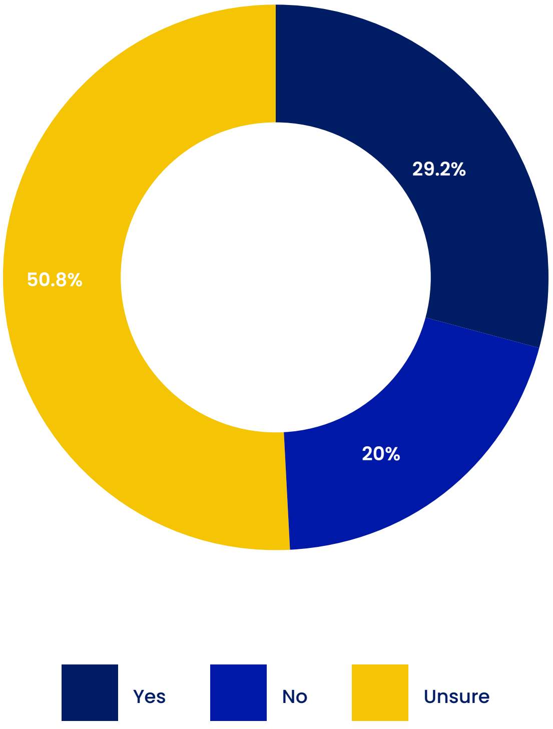
'Much more vigorous onboarding due diligence and ongoing oversight and monitoring of cloud applications'

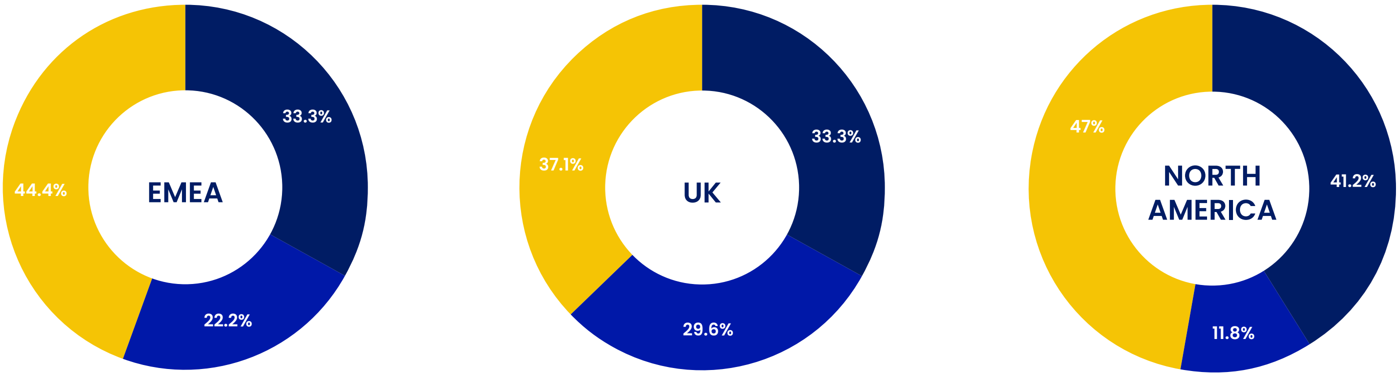
SUPPLIER REQUIREMENTS

Returning to the requirements for stressed exit plans, respondents were asked whether their stressed exit plans included escrow of software source code. Again, the most frequently reported answer was 'unsure', with 50.8% of respondents selecting it, followed by 'yes' with 29.2%, and 'no' at 20.0% (Figure N). These results were somewhat surprising, as only 14.3% of respondents in Figure G stated that they used escrow management. This question saw limited variations based on jurisdiction; 'unsure' was the most common result across the EMEA, UK and North America. The only minor variation in jurisdiction was seen in North America, where 41.2% of respondents stated that they did include escrow of software source code in their stressed exit plans. Upon further research, the use of escrow appeared to be more prominent in North America; while all interviewees were aware of its potential and uses, they had not yet all utilized it to its full potential. This was in contrast to the UK and EMEA jurisdictions, where some of the respondents were unaware of its uses and application to TPRM and resilience.

Organizations face a barrage of challenges when implementing stressed exit plans; the survey reviewed some of the most common reported stumbling blocks. When asked, 56.3% of respondents said that 'supplier refusal/ contractual negotiations required' were a common issue with stressed exit plans (Figure O), and 51.6% stated that 'a technical inability to deliver' was also a common concern. Survey respondents could select multiple answers, which further demonstrated how multifaceted the challenges are. Each option was selected by a minimum of 20% of the survey respondents; these options included: 'supplier education required', 'materiality objections from supplier', 'proportionality objections from supplier', 'service re-design required' and 'other'. Some respondents expanded on their 'other' responses with free-text answers, which included: 'web-readiness', 'practicality', 'reliability of regional failover plan', 'in-house expertise', and 'resources', among others.

Figure N. Inclusion of escrow in software source code

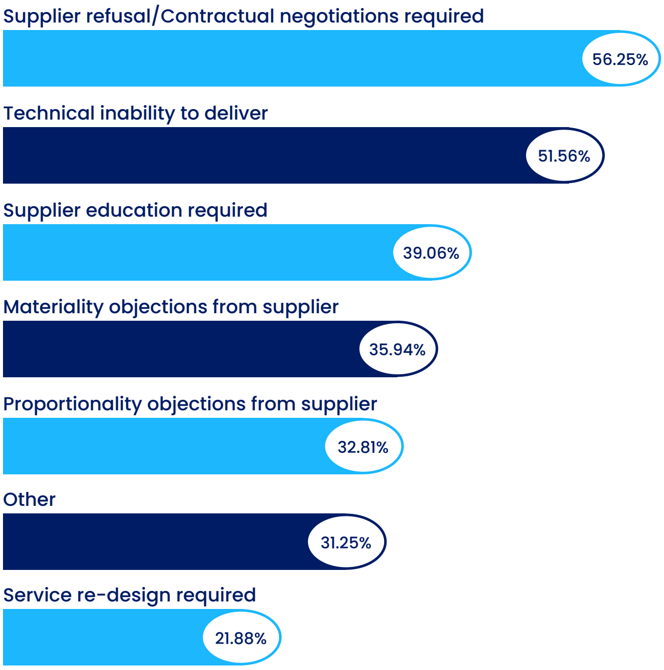


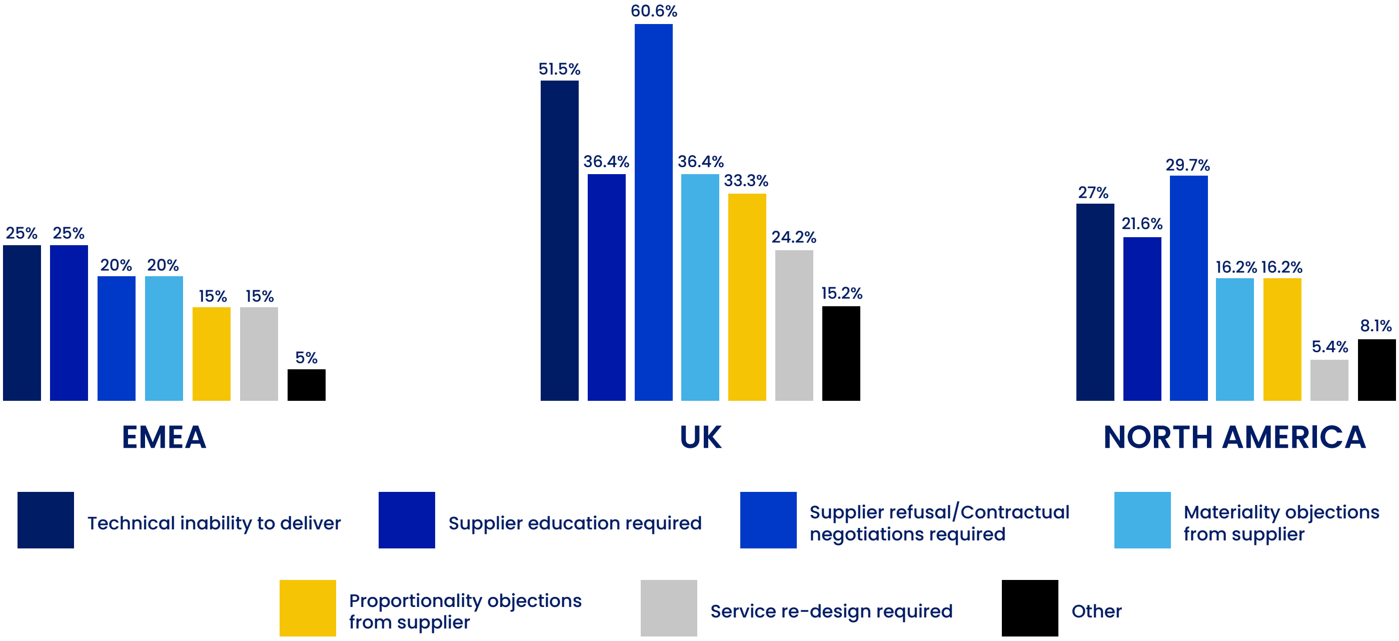


The results displayed in Figure O demonstrate a high level of contractual pushback, with supplier refusal and contractual negotiations required being frequently selected. The process in collecting or producing stressed exit plans is long and expensive, so organizations are seeing reluctance from suppliers to provide necessary information and update clauses. Moving forward, an inclusion of a right to have a stressed exit plan should be inserted into all contracts as a best practice. Robust sections in contracts should be included; although as the sharing and receiving of supplier plans is challenging, many suppliers may be guarded and reluctant to share. In additional follow up interviews, industry experts highlighted that they had received high levels of supplier pushback, with many suppliers questioning the classification of material or critical. This was reflected in the survey results, with 32.8% of respondents selecting ‘proportionality objections from suppliers’ as a common issue. Again, organizations are receiving high levels of pushback due to proportionality; there is an expectation that end-users may form consortiums to reduce costs and ensure proportionality.

More than half of the respondents (51.6%) outlined that a ‘technical inability to deliver’ was a key issue. This could indicate several internal shortfalls, including that services have not always been designed to operate in a resilient manner. This further compounds the aforementioned skepticism as to whether organizations, despite their high levels of confidence, will be able to meet the deadline on time.

Figure O. Range of issues associated with stressed exit plan





When analyzing answers across jurisdictions, the UK seemed to experience much higher levels of supplier refusal (60.6%) compared to the EMEA and North America, who experienced 20% and 29.7%, respectively. The same can be said for an organization’s technical inability to deliver, which was highlighted by 51.6% of UK-based respondents, compared to 25% in the EMEA and 27% in North America. The UK generally seems to have higher pushback from suppliers from a technical, education, refusal, materiality, proportionality, and service re-design perspective. Given respondents could select all options that applied to them, it is highly likely that respondents from the UK are subject to at least one of the above, with likelihood being that many are subjected to several. This could be in part due to the UK regulation being in place for longer than others. As the Technical Standards Framework for DORA had not been announced, organizations could have been holding off on implementing their plans until they had a full view of the requirements. As the UK has a 3 year implementation period, many critical services will have had a contractual renewal within the transition period. The route to compliance in Europe is compounded by a 1 year timeline, with many critical service contracts not renewing in that timeframe, adding an additional element to amend mid-contract. This could pose a significant impact to costs and time required.

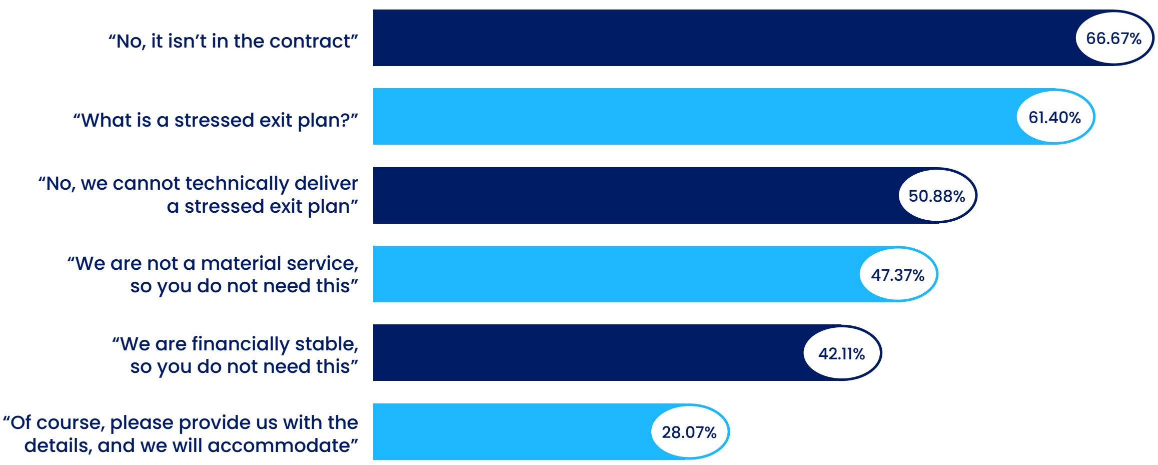
Many organizations across the industry have received pushback from their suppliers, as outlined in Figure O. CeFPro's follow-up analysis explored this further, and developed participants' responses upon approaching material suppliers to set up stressed exit plans. The highest response received by respondents from suppliers was 'no, it isn't in the contract', which demonstrates a lack of maturity across the industry, as stipulations such as these should be included in all contracts (Figure P). While legacy contracts may not have the updated language, they should at least include clauses to share summary of plans. The results also demonstrate a lack of education across suppliers, who appear to be largely not prepared for the change. The inability or unwillingness to accommodate stressed exit plans would need to be reported to regulators by the end-user as part of the regulation. A further 61.4% of respondents stated that they received pushback from suppliers that were unaware as to what a stressed exit plan is, and another 50.9% of respondents reported that some suppliers have stated that they do not have the technical ability to deliver a stressed exit plan. This further serves to demonstrate the lack of understanding across suppliers regarding the evolving regulatory environment. Suppliers seem unaware of the ramifications of responses, with some oblivious of the level of change and work that needs to be undertaken. This could be a potential cause for concern, as these figures could be further inflated by other suppliers that are aware of the required changes but deny the contractual obligations, and appear to not understand the potential repercussions should they be reported to regulators.

However, it is worth noting that some suppliers (47.4%), as stated by the survey respondents, reported to present some level of understanding regarding stressed exit plans, and contested that they did not require them as they did not operate as a material service. Along a similar line, 42.1% also stated that they were 'financially stable', so such plans were not required.

Organizations appear to be facing a wide range of objections, both due to a lack of education or understanding of the requirements, and their overall inexperience, lack of resources, or technical capability. This, again, brings into question the level of confidence seen in Figures D and E, with so many struggling with internal capabilities, compounded by high levels of supplier pushback, it is difficult to understand why more than half of respondents were fairly confident that they would meet the requirements in time.

As demonstrated in Figure P, the UK received high levels of supplier pushback, whether through refusal, technical inability, education or materiality objections. The UK also saw higher levels of negative responses, with 42.4% of UK respondents reporting to have heard 'no, it isn't in the contract', compared to 10.0% in EMEA, and 32.4% in North America. In contrast, the UK also received the highest number of positive responses, with 30.3% of respondents reporting to have heard 'of course, please provide us with the details and we will accommodate accordingly'. This statistic contrasts sharply to those reported by the EMEA and North America, which were 10% and 8.1%, respectively. EMEA respondents reported to have received the largest amount of pushback, with 40.0% of EMEA-based suppliers reporting to have asked 'what is a stressed exit plan?'. These responses raise concerns of insufficient industry-level education being provided to/by organizations. However, while these results were highlighted as being alarmingly high, they can be explained somewhat by the pre-existing lack of confidence in the EMEA region towards stressed exit plans. Figure D demonstrated that 76.9% of EMEA-based respondents felt 'somewhat' or 'completely unconfident' regarding their progress towards implementation.

Figure P. Supplier reactions when asked about stressed exit plans

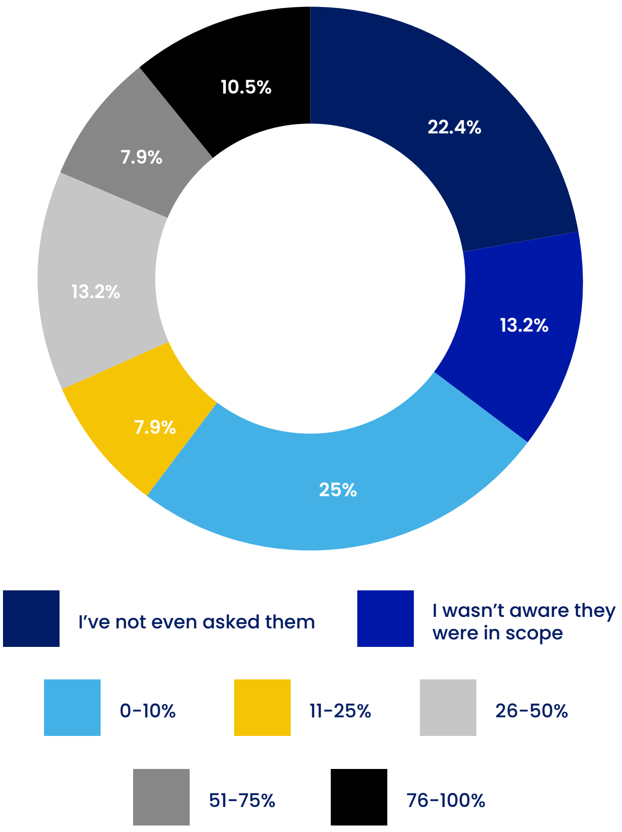


MATERIAL SERVICES

As the industry continues to progress, the deadline for the inclusion of stressed exit plans in material services edges closer. This includes intragroup outsourcers, who can provide some, or all, of an organization's IT services. The survey reviewed what percentage of material services organizations' intragroup outsourcers had provided demonstrably successful stressed exit plans for. The results highlighted limited progress in this area, with 25.0% respondents reporting to only having plans in place for 0–10% of their intragroup outsourcers, and 22.4% reporting to have not even asked them about the issue (Figure Q). Industry experts highlighted that as all are due to be included by the upcoming deadline, seeing that only 10.5% of respondents reported to have completed stressed exit plans for 76-100% of their intragroup outsourcers, the industry continues to demonstrate slow progress. As outlined in Figure J and Figure K, the responsibility and ownership of risk should sit with the Board/C-suite, with TPRM teams managing the risk. The responsibility to mitigate the ramifications of supplier failure and check other business functions is not being effectively managed or communicated at a C-suite level in some organizations. Policies, standards, and procedures are not disseminated throughout the organization, and accountability and management oversight are not always clear. This could lead to uncertainty in the treatment of such relationships, and a failure to allocate both responsibility for the risk, and the responsibility to ensure that demonstrably successful stressed exit plans are in place for all intragroup outsourcers providing material services.

Furthermore, it is alarming that 35.6% of respondents either had not yet asked their intragroup outsourcers, or they were unaware that they even fell within scope. This suggests that a large percentage of the industry may be unaware of the requirement for stressed exit protection from intragroup outsourcers.

Figure Q. Percentage of stressed exist plans provided by IT-focused intragroup outsourcers



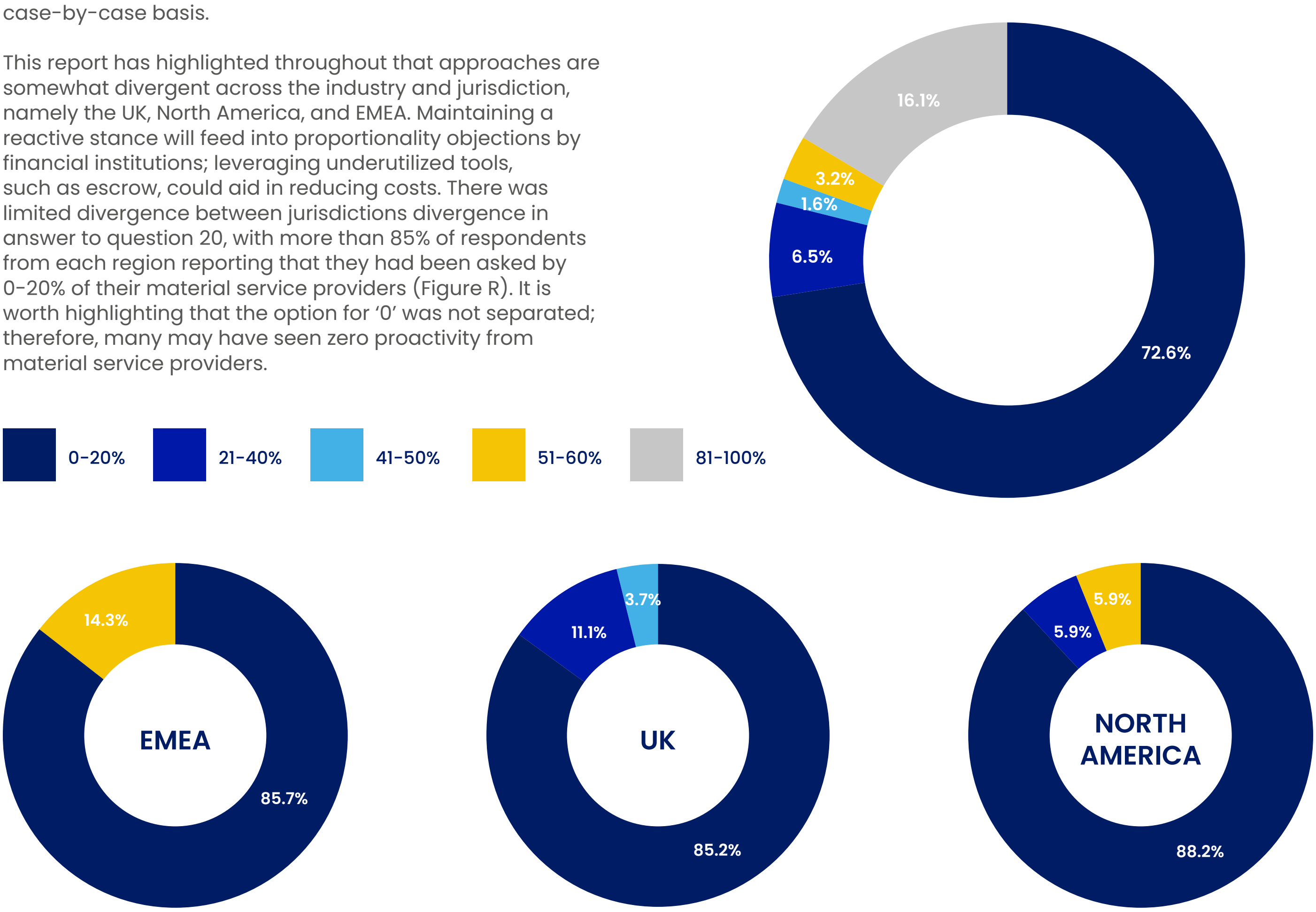
When breaking down the data by jurisdiction, some disparities were highlighted, potentially due to the wording of the question, and requirements across different regulators. 37.5% of EMEA respondents reported to have not asked intragroup outsourcers, with a further 25.0% unaware that they fell into scope. Collectively, 62.5% of all the respondents from the EMEA region reported to have made no progress in collecting demonstrably successful stressed exit plans for intragroup outsourcers. Somewhat confusingly, the EMEA region also saw the highest number of respondents (25%) reporting to have asked 51–75% of their intragroup outsources about the inclusion of stressed exit plans. The EMEA demonstrated both the highest level of progress and uncertainty across its jurisdiction. The UK saw a much more divergent set of results, with a more even spread across answers, the largest percentage of respondents (33.3%) reporting to 'have not asked them', followed by 20.8% who reported to have stressed exit plans for 0-10% of their intragroup outsourcers. While progress reported by the UK-based respondents seems to be behind that of their EMEA peers, their understanding of the expectations could potentially be higher, as only 12.5% of UK-based respondents reported to be unaware that intragroup outsourcers were in scope, compared to the 40.0% of the EMEA cohort. Finally, North America received the biggest number of votes for the 0-10% option, with 53.3% of their respondents falling within this category. Respondents fell evenly between the '11–25%', '26–50%' and 'not even asked' options, which each received 13.3% of the cohort's vote. Only 6.7% of the North American respondents felt they were unaware that intragroup outsourcers fell within the scope of programs.

Overall, progress in receiving demonstrably stressed exit plans for intragroup outsourcers providing material services is slow, and to some degree, not widely understood. Those that have begun work appear fairly early on in their progress, with many unaware that they fall within scope.

When reviewing how proactive material service providers are in their approach to setting up stressed exit plans, an overwhelming majority of respondents (72.6%) stated that only 0–20% of their material service providers had approached them with plans (Figure R). Many suppliers appear to be not demonstrating proactivity in their approach, and remain unlikely to be forthcoming with plans, unless explicitly asked by financial institutions. As much as this would be an opportunity for suppliers to take control of the process and submit upfront stressed exit plans before banks start chasing, it appears that very few are electing to do so. This could be a risky approach for suppliers, who risk having their customers coming to them at the same time demanding plans in advance of implementation deadlines. An upfront approach may assist in the concentration of submissions. Remaining reactive could prove a costly approach for suppliers, who may end up individually accommodating stressed exit plans when requested on a case-by-case basis.

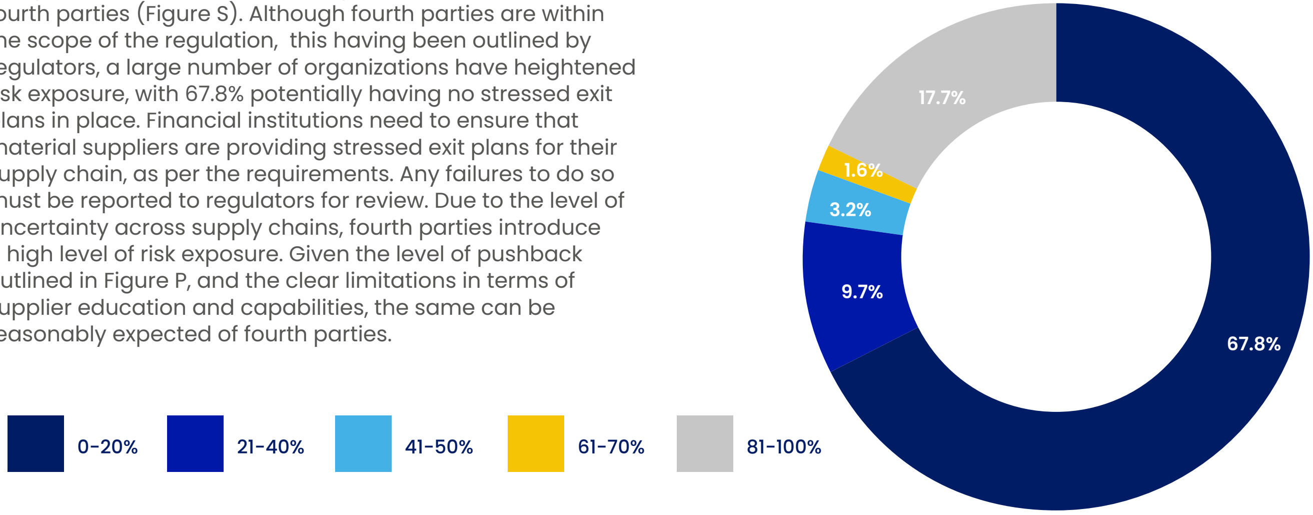
This report has highlighted throughout that approaches are somewhat divergent across the industry and jurisdiction, namely the UK, North America, and EMEA. Maintaining a reactive stance will feed into proportionality objections by financial institutions; leveraging underutilized tools, such as escrow, could aid in reducing costs. There was limited divergence between jurisdictions divergence in answer to question 20, with more than 85% of respondents from each region reporting that they had been asked by 0-20% of their material service providers (Figure R). It is worth highlighting that the option for '0' was not separated; therefore, many may have seen zero proactivity from material service providers.

Figure R. Number of organizations that have been proactively approached regarding stressed exit plans



The final section on material service providers looked into the percentage that have presented their stressed exit plans for their own material providers (fourth parties). Again, a majority emerged, with 67.8% of the overall respondents stating that only 0–20% of their material service providers had presented their stressed exit plans for their own material fourth parties (Figure S). Although fourth parties are within the scope of the regulation, this having been outlined by regulators, a large number of organizations have heightened risk exposure, with 67.8% potentially having no stressed exit plans in place. Financial institutions need to ensure that material suppliers are providing stressed exit plans for their supply chain, as per the requirements. Any failures to do so must be reported to regulators for review. Due to the level of uncertainty across supply chains, fourth parties introduce a high level of risk exposure. Given the level of pushback outlined in Figure P, and the clear limitations in terms of supplier education and capabilities, the same can be reasonably expected of fourth parties.

Figure S. Percentage of material service providers that have presented stressed exist plans for fourth parties



CONCLUSION

The results from the research demonstrated a clear divergence in approaches across the industry, whether it be across organizations or geographies. Many firms are, as yet, not where they need to be, although confidence remains fairly high. Roughly half of the respondents were confident to some degree on their progress to date and their ability to move forward and ensure timely compliance. It was highlighted throughout that the regulation represents the next step, with much work to be undertaken beyond the initial compliance dates, moving towards best practice and inclusion of all legacy contracts will remain an ongoing task.

The scale of the change, both for financial institutions and suppliers typically outside the scope of regulation, is demonstrated throughout the results. The inclusion of stressed exit plans across third and fourth parties is a substantial shift in approach and poses a challenge for organizations to varying degrees. The research appears on the surface to highlight slow progress; however, it was highlighted throughout in the additional follow-up interviews that the upfront work is substantial in nature, and time consuming. Many organizations on a surface level appear to be falling behind, however this background work is being undertaken, and a fairly swift turnaround is expected throughout 2024 as plans are finalized and tested. Confidence levels further reflect this, with more than 50% of respondents confident of the rate of progress towards implementation. There appeared to be more confidence in the UK and North America, though it was also highlighted that the scale of change under DORA could be reflected in the work needed to be undertaken by European organizations.

Adoption of new tools and approaches is an area that organizations can look towards. Many industry experts highlighted the use of standard supplier management processes, and setting thresholds and financial monitoring, as key tool to mitigate supplier failure. Exposure to, and the effective leverage of, tools such as escrow management were reported to be very low across geographies. In additional follow-up research, it became evident that the escrow management as an opportunity is yet to be fully understood.

However, there remained positive takeaways, as organizations move towards scenario testing compliance processes, with 35% of respondents seeing some success with their plans and developing processes to learn from failed attempts. Many are still in planning stage, though many remained confident in their approach and ability to meet the deadline.

A big area of divergence was around management, ownership, and accountability for risk of supplier failure, concentration risks or service deterioration. This has a ripple effect across a number of areas where it is not immediately apparent where the responsibility lies, and messaging is not always translating across business lines, or from the top down.

Overall, despite some positivity in terms of confidence, there remained a fair degree of uncertainty across the industry. 2024 is expected to be a pivotal year for organizations moving towards final implementation. Suppliers should also not underestimate the work required in both submitting stressed exit plans for themselves, but also their third parties.

A WORD FROM ESCODE

EXECUTIVE SUMMARY

This report highlights critical insights into the financial stability and compliance readiness within the supply chains of the financial services industry. Despite slow progress in meeting compliance of the pending regulatory deadlines, there remains an unusually high confidence among firms regarding their ability to comply. This disconnect underscores the importance of this comprehensive research, which seeks to provide concrete evidence of the challenges faced by regulated entities.

Key findings of the report include:

- Focus on Security Over Financial Stability: While significant attention has been given to security and service durability, financial stability within the supply chain has been largely overlooked. This imbalance poses significant risks, particularly in regions where upcoming operational resilience regulations will soon mandate stringent oversight of supplier failure, service deterioration, and concentration risk.

- Inevitability of Supplier Failure: The report emphasizes that market forces make supplier failure unavoidable and unpredictable. Current reliance on early detection of financial instability provides only short-term notice, highlighting the necessity for regulated entities to assume potential supplier failure as a default scenario.

- Lack of Understanding of Escrow Benefits: There is a significant lack of understanding regarding the value of escrow solutions, with only 14% of respondents recognizing their importance. This awareness gap is most notable in regions with imminent compliance deadlines, such as the UK and the US.

- Ownership of Risks in SaaS: An alarming 87% of respondents either incorrectly identified or were unaware of the ownership of risks associated with supplier failure, service deterioration, and concentration risk within SaaS environments. This finding raises concerns about the reliability of firms’ stressed exit plans and the confidence levels of respondents.

- Regulatory Confusion and Resilience Threats: Differing regulatory requirements for intragroup outsourcing are causing confusion, which threatens the resilience of regulated entities. The inconsistency in approaches to stressed exit plans is largely due to these varied regulations.

- Proactive Risk Management by Suppliers: The report identifies a clear opportunity for suppliers to proactively manage risks, rather than reactively responding to customer requests. Failure to do so could lead to increased costs and risks across the market.

Escode advocates for the development of proportional preventive and detective controls to mitigate the duration, severity, velocity, and total cost of supplier failures. Escrow solutions, increasingly recommended by global financial regulators, offer temporary yet effective support during stressed exit scenarios.

The facts of the Third Party Risk Management report are believed to be correct at the time of publication but cannot be guaranteed. Please note that the findings, conclusions and recommendations that CeFPro® delivers will be based on information gathered in good faith, whose accuracy we cannot guarantee. CeFPro® acknowledges the guidance and input from the Advisory Board, though all views expressed are those of the Center for Financial Professionals, and CeFPro® accepts no liability whatever for actions taken based on any information that may subsequently prove to be incorrect or errors in our analysis. For further information, contact CeFPro®.