smarsh®

1LoD®

1st line Risk & Control
Forecast 2022

Time to reset the 1st line risk & control function?

The time has come for financial institutions to treat the 1st line risk and control function as an equal partner within the business [or, as a more integral part of the overall business] rather than as the trouble-shooting poor relation whose help is only sought when things go wrong. Regulators and banks now take a much more detailed and proactive approach to risk evaluation and mitigation, and this has important implications for the 1st line in terms of responsibilities, relationships with other lines, technology and staffing. And given the rapid changes in the market and overallbusiness, banks' control functions may be tested to the limit by any number of nasty surprises.

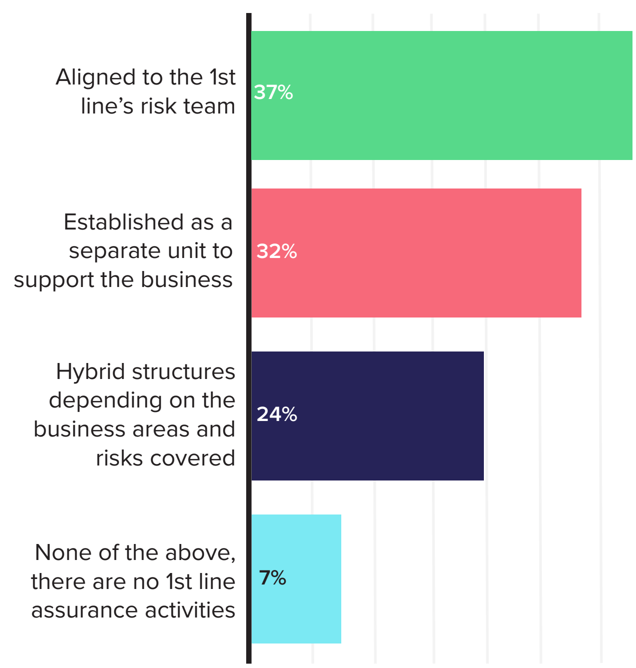
Key takeaways

- The 1st line must move away from admin and evidencing to true operational risk management
- 47% of bankers polled said that the 1st line needs to change significantly
- The risk and control self-assessment (RCSA) process misses too many risks and should be revised
- 63% of bankers said that change will mean a significant rise in investment over the next three years
- Control automation is a key priority for 46% of banks polled
- Getting data right requires local 1st line AND broader bank collaboration
- Substantial organisational challenges still reduce the effectiveness of the 3 lines model
- 58% of 1st liners said their biggest worry is the increase in the scope of risks they have to cover

Banks are struggling to stay ahead of change, even with the 3 lines of defence model and sophisticated layers of checking, monitoring, assurance and challenge. That was the main message from one of the keynote speakers at 1LoD's recent Deep Dive on the 1st line risk and control function. Surprises like Archegos, the accidental wiring of almost a billion dollars continue to happen and illustrate the enormous complexity of operational and process risk in banking. The need to minimise avoidable surprises, the need to cover an ever-increasing set of risks, is driving the evolution of the 1st line of defence.

As this keynote speaker put it when summing up the challenges and issues faced by the 1st line: "How do we use automation and MIS to give us better warning signals about the operating environment and especially the control environment? How can data generated by an automated control be leveraged to warn us about changing the risk profile? What patterns are meaningful and what patterns are just noise? What about our assurance functions? Can we evolve those from sampling and look backs to penetration testing and performance analytics? Continuing to evolve our thinking in all these respects is not just key to becoming more effective and more efficient. I would argue it's just essential for us to create the early warning systems.

My organisation's 1st line assurance activities are organisationally and operationally:



"I really gained a lot of insightful information as I attended this Deep Dive for the first time. I will review my notes and really focus on bringing these important points out in my future meetings with my business partners. Great sessions!"

NICOLE EBORN, ASSOCIATE, FANNIE MAE

In order to become this early warning system,the 1st line has to change. Several senior speakers talked passionately about the importance of the evolution of the 1st line risk and control function: in their view, it must become a valuable and pr fessional partner to the business, with a recognised skillset and value, rather than remaining as an administrative function that is isolated from the real business decision-making.

As one global head of front office supervision said: "We need a reset. We need to move away from being the control office and towards being a true non-financial risk team. That name by itself is important in framing our job as managing non-financial risks on an end-to-end basis with controls as just one tool, not as a team responsible for just a set of controls. We need to be more forwardlooking and more at the table when the business takes decisions about what it is going to do. We want to get to a position where the business, when making a decision, has us in the room and proactively asks, 'how does that affect non-financial risk' – and that doesn't happen very often at the moment. Otherwise we are just a firefightingand remediation function, not a true risk-mitigation function. To do that, we also need to stop acting as though our job is about risk elimination."

Another participant talked about the need "to develop the discipline of the CCO and related functions into a role recognised as having the status and maturity and importance of roles such as the COO". They also described the importance of transforming the 1st line from a function whose job was essentially administrative, concerned with the gathering of evidence that controls exist and are tested and assured, to one whose job is about risk identification and management.

"We have to focus on risk, not evidencing – but how? The challenge is huge – remediation forces you into that evidencing exercise instead of closing the gaps in the control environment," said one participant.

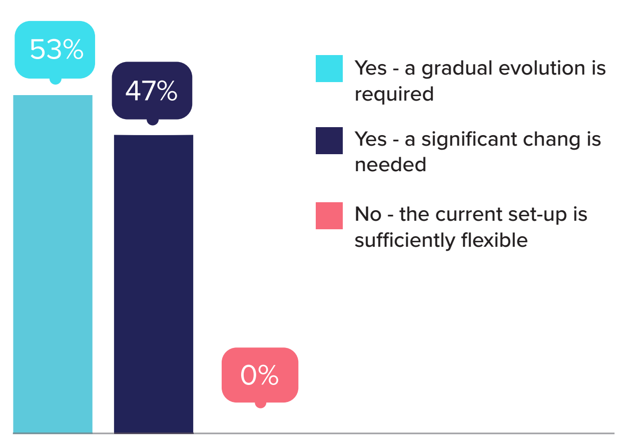
The key message was that change is crucial. None of those polled felt that the current function was sufficiently flexible to cope with the evolving demands of regulators and the business, while almost half (47%) said that significant change was needed [chart 1]

"Excellent opportunity to ideate on really complex industry challenges with the best in the business"

KEVIN KEENAN, SENIOR DIRECTOR OF DATA SCIENCE, SMARSH

Chart 1

The 1st line risk and control function needs to change if it is to sustainably meet evolving regulatory and business expectations:



Revising the RCSA

To become a true risk-management function, the 1st line needs to shift from episodic risk evaluation to a more realtime approach. Leading banks have aready moved away from the traditional risk and control self-assessment (RCSA) process, which could be an annual review of inherent and residual risk, to a live, daily, business as usual assessment of risk and control effectiveness. In the words of one 1st line head:

"We have had support from the top of house to create a process in which we can now look daily at the extent to which the 1st line feels there is heightened risk in the business. We look at internal loss or risk-event type data or external-event data and we rank risks in buckets to prioritise them."

This feeling that the RCSA process needs reform is shared across top-tier banks. As another head of change in the chief control office said, "It's failed in certain areas; it's failed to spot the things speakers have referenced around recent events – the issues that we've had in surveillance, record-keeping, AML. It's not as robust as we might want it to be. It needs a change. It needs a revamp. The business is only going to get more and more complex. Keeping up is not always layering control upon control. It's actually being better and smarter in the application of those controls. And regulatory sanction is not the only driver. It's actually the right thing to do in our industry to change those controls, to be much more effective and meaningful for the current climate."

Looking forward

One of the shortcomings of the traditional RCSA lies in identifying potential risks that have not yet emerged as threats. As one speaker said, "We are expected to be able to identify upcoming risks when we come up with op risk frameworks and doing RCSAs and looking at how those RCSAs should change. But that is very difficult as these are long-tail events.

Here banks need to distinguish between two main buckets of risks. "There are two ways to think about horizon scanning," said Paul Ford, founder and chief executive officer of Acin. "There is the horizon of things that you don't know about, but other firms do know about. So, it's on the horizon of your firm, but it's inside the horizon of other firms. And then there's horizon scanning as an industry, which are the things that no one has thought about sufficiently at this stage because it either was not on the radar or the impending change hasn't happened. The pandemic is a classic example of that because everyone has done disaster recovery (DR) and business contingency planning (BCP), but no one ever expected to have to do the whole firm all at once."

This approach most closely ties in with regulatory thinking, in that regulators are more likely to penalise failings across risk types that peer institutions have covered, but are more likely to be lenient on risks that no one in the industry has foreseen.

Banks described several different approaches to the problem of horizon scanning. One is an industry platform that collates risk assessments and control details from more than a dozen major banks (whose identities are kept secret) so that each can see whether they have missed something that the others have spotted. Another is the creation by one leading bank of a specialised legal and regulatory risk identification team: this is tasked with gathering the huge numbers of global regulatory changes that are announced and translating these into possible actions required by the 1st line and others.

The latter raises questions about 1st line/2nd line boundaries. As one speaker said, "If you put the onus for regulatory risk on a 1st line horizon-scanning, riskassessment process, that is a big shift in responsibility from the 2nd to the 1st line. As a 1st line person, I say 'no' to that: I want that to come from compliance; they are the regulatory and legal experts; they talk to regulators and they should be coming to me to talk about the types of fines they are expecting in the industry and about regulatory changes.

Chart 2

Delivering the required change in the 1st line risk and control function will require

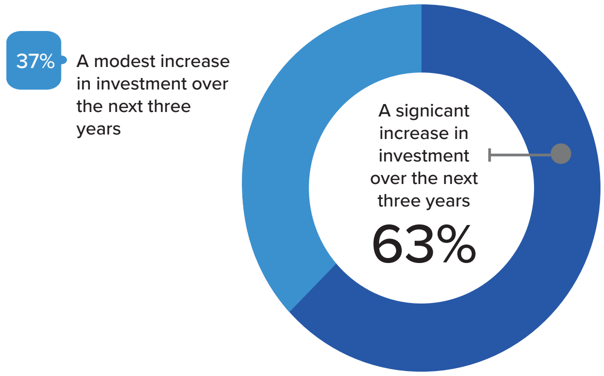


Chart 3

My top technology priorities for the 1st line control function are

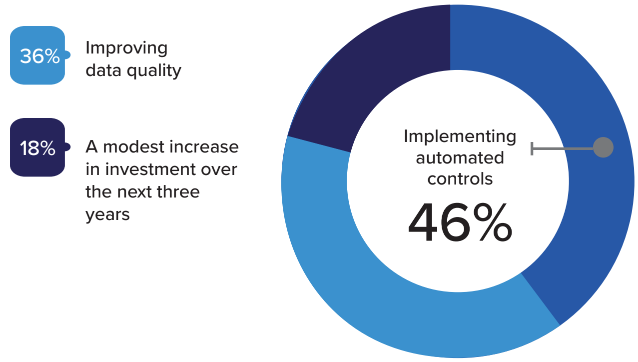


Chart 4

I estimate that the percentage of controls that are automated in my area is:

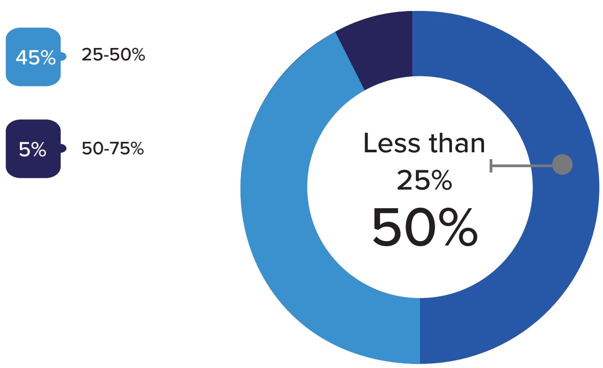
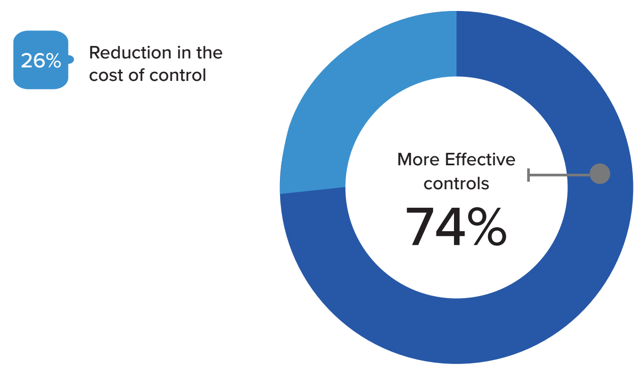


Chart 5

In my firm I think the most important driver for investment in control automation is:



More money, tech needed

All of these aspirations require investment. Almost two thirds of the attendees felt that achieving the required change in the 1st line risk and control function would require a significant increase in investment over the next three years [chart 2].

Much of this will have to be spent on technology. The transformation of a control function into a strategic business partner requires the overhaul of many of the current practices of the 1st line risk and control function. “Within the 1st line of defence we have, as an industry, too many spreadsheets, too many manual processes, too much bespoke activity. So, we all need to upgrade our infrastructure to make it more professional,” said one head of business controls management.

Asked about their technology priorities, 46% of attendees put the implementation of automated controls at the top of the list [chart 3]. Half of the attendees estimated that the percentage of controls that are automated in their area at present is less than 25%, indicating the size of the job ahead [chart 4].

Getting the budget for automation may require the functional reset mentioned at the outset. Too often, 1st line technology requirements are framed in the narrow terms of the controls required for regulatory compliance. But framing it like that puts it a long way down the list of banks’ investment priorities. As one head of business controls explained, “We should be working with our business partners to make investment in automation of controls part of the general operating model, rather than just an automation of controls operating model. It’s harder to justify an investment when it’s a segregated pot of money that's set aside to deliver on controls automation, because the return only comes when something goes wrong and even then it can be hard to quantify. So, for me, being successful in this space means partnering with your respective business line heads and corporate functions to be able to drive investment through the strategic initiatives of the firm. Build it into their funding that they're going to do, whether they're bringing in a new technology platform for the firm, or whether they're looking to create efficiency within their processes."

The technology challenges of the 1st line require buy in from multiple stakeholders outside of the function. Several speakers talked about senior management's commitment to providing them with the tools they need. But for many, it is hard to get away from narrow justifications for investment. When attendees were asked what was the most important driver for investment in control automation, 74% replied 'more effective controls' [chart 5].

The good news is that the technology is now able to cope with some of the banks' most intractable challenges. One of the problems in getting the budget has been the costs associated with projects that require the replacement of core legacy systems. Control automation has often seemed to require this. But as Matthew Perconte, managing director, risk and compliance, Protiviti, explained, this is no longer the case. "It is clearly more difficult to implement change if control automation is bound up in the broader modernisation of legacy tools. But I've seen a lot of controls groups drive improvement in automation in ways that sit on top of those tools, through RPA [robotic process automation] ETL- [extract, transform, load] type tools, intelligent workflow and process automation. This can give a lot of the wins that we're talking about without having to undertake a full-on ripping out of a core banking platform and then replacing it with new tech."

Getting data right

Technology is only as good as the data fed into it and it is clear that the 1st line still faces a host of challenges here. To run controls, the 1st line needs to identify the internal and external data feeds it requires: this isn't easy given the proliferation of trading venues, comms channels and risk types that it has to cover. It needs additional data from internal sources, from prop desks and quant teams to HR and legal. And it must be able to aggregate that data in the face of huge inconsistencies in how the data is configured, and how individual pieces of information – client identifiers, trader IDs, instrument IDs etc. – are encoded.

This problem can be solved in two ways – either piecemeal within the first line or more broadly within the bank – and the approach differs from institution to institution. But for most 1st liners, the requirement to operate their controls generally forces them to do whatever it takes to clean up the data sufficiently for whatever purpose it has.

"I'm trying to use technology now to help me clean up some of the inputs that I've always needed to," said one controls head. "Our biggest barrier to using more advanced technology to do the smarter risk management we want has been rubbish in, rubbish out. I need a consistent, standardised set of data from the support functions that provide our information. Talking about automation as the prize is running ahead of the curve."

Cleaning dirty data locally in this way is not best practice to broader data professionals. They prefer frameworks in which enterprises commit to better data capture-at source and to provide individual businesses with a golden source. Those desions are taken above control offices and require business recognition that a modern enterprise data architecture, probably in the cloud, is worth building.

As John Holland, senior vice president, Smarsh, said, "It is absolutely true that analytics have moved on substantially. But what we often see, that is frequently overlooked, is whether or not you are actually capturing all the data that you need in the first place. It is very easy to miss an important communication channel, particularly given all the new channels that are coming on board such as Reddit, YouTube, RingCentral etc, and we've all seen the level of fines imposed where the regulator has found companies that haven't been doing that. Without all the data, the analytics may actually be giving you a false picture too. Ensuring that you have an effective programme to capture all the data communication channels you use, that is both kept up to date with format changes to existing channels and also responds rapidly to new channels as they become generally used, is an essential part of your end-to-end surveillance solution."

Back to basics

However, it's not just about technology. The foundations also have to be right and here, too, there is more work to be done. A quarter of banks are still working on developing a structured approach to 1st line roles and accountabilities for risk and control (chart 6); more than 50% of firms have only partially assessed and mitigated the risks of inherent conflict in 1st line risk control roles and responsibilities (chart 7); and more than 60% of firms have not completely solved the problems of having clearly defined risk and control responsibilities in the 1st line [chart 8].

This work to define responsibilities more precisely comes at a time when the 1st line is ever more concerned about how to cope with increasing risk. When asked to identify their most significant concerns about the current operating model for 1st line risk and control, 58% replied that it was an increase in the scope of risks to be covered, while 14% said it was the migration of tasks from 2nd line risk functions' [chart 9].

A seat at the table

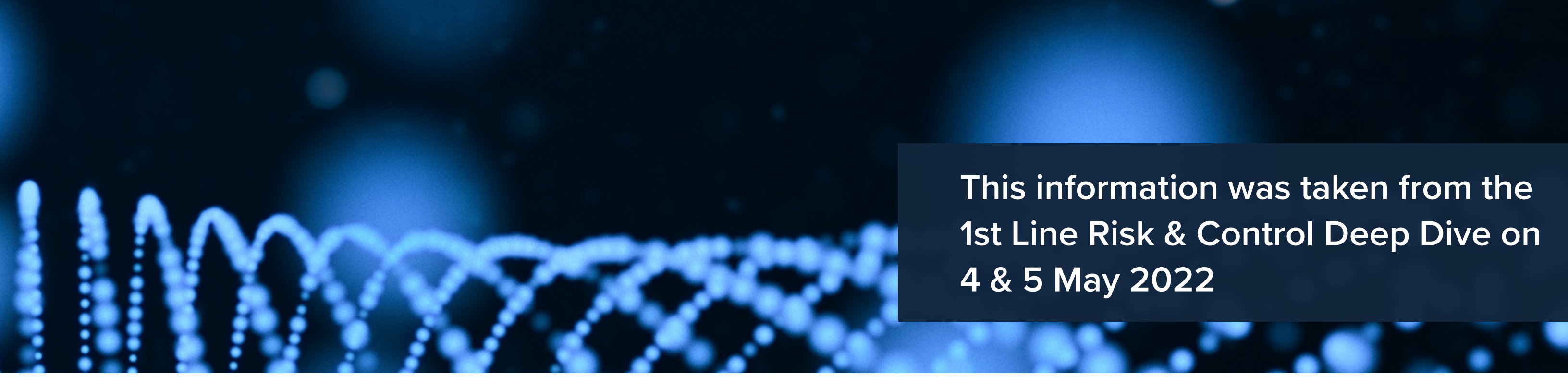
To ensure that they have the resources and the information to cope with these challenges, heads of the 1st line risk and control function are clear: they need to build a strong rapport and relationship with the business. As one participant said: "We are operational risk professionals, and we have to be very careful that we don't describe our purpose as a list of activities that we perform. We need to be embedded in the business, attending management committee meetings, the OpCos and SteerCos, so that we have a seat at the table and they see us as peers and not someone that comes to them to pester them about their weakness and gaps in their control environment."

Testing and assurance in the 1st line

Duplication across the 1st and 2nd line has long been a concern, and the organisation of testing and assurance within the 3 lines model is an important topic. Attendees at 1LoD's Deep Dive agreed that additional testing in the 1st line was desirable, but at the same time, they agreed it was important to "avoid marking our own homework – the business operating controls and signing-off alerts from a surveillance tool, for example".

So, 1st line risk and control functions are struggling to balance the need for independence (to be able to assure the business that controls work) with the need to have its work assured by the 2nd line.

To avoid duplication, banks are devising different types of testing and assurance to be deployed in different lines of defence. So, for example, one bank is building out testing and assurance in the 1st line using war-gaming, scenario analysis, and live testing, to make it complementary to 2nd and 3rd line assurance. Those lines then check design and operational effectiveness matters, and maintain a QA process. Other banks argue that the 2nd line has to have a better testing and assurance regime than simply a QA process around the 1st line testing. The debate continues!



This information was taken from the 1st Line Risk & Control Deep Dive on 4 & 5 May 2022

Chart 6

My organisation has a structured approach to 1st line roles and accountabilities for risk and control:

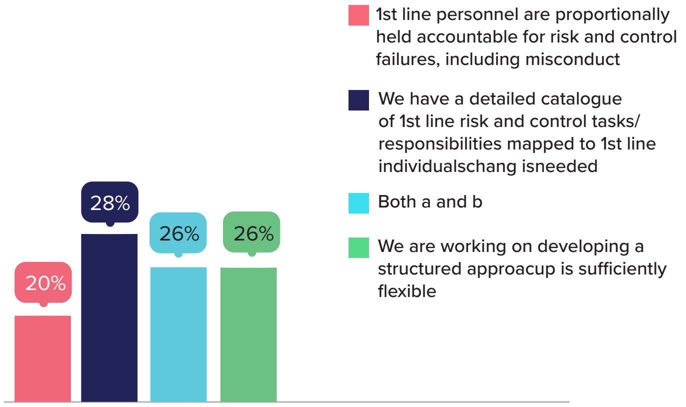


Chart 7

My organisation has assessed and mitigated the risks of inherent conflict in 1st line risk control roles and responsibilities:

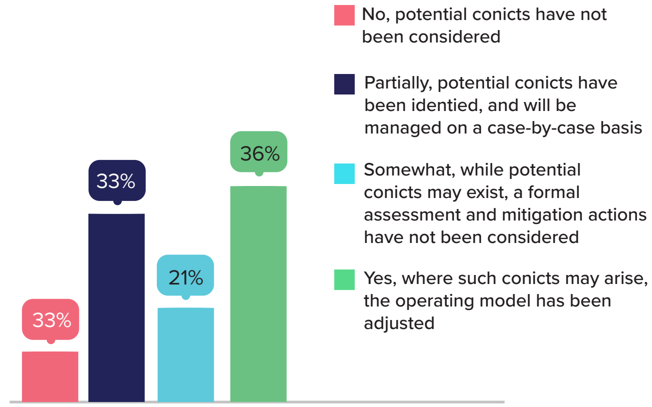


Chart 8

My organisation has clearly defined risk and control responsibilities in the 1st line:

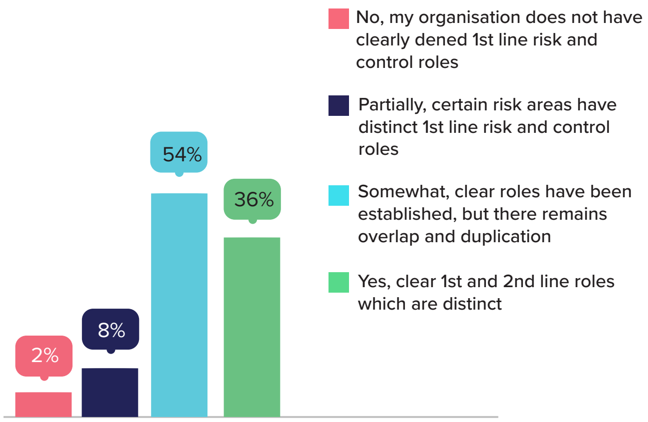
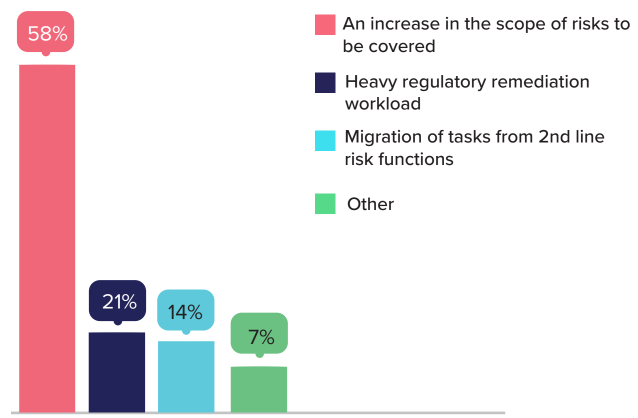


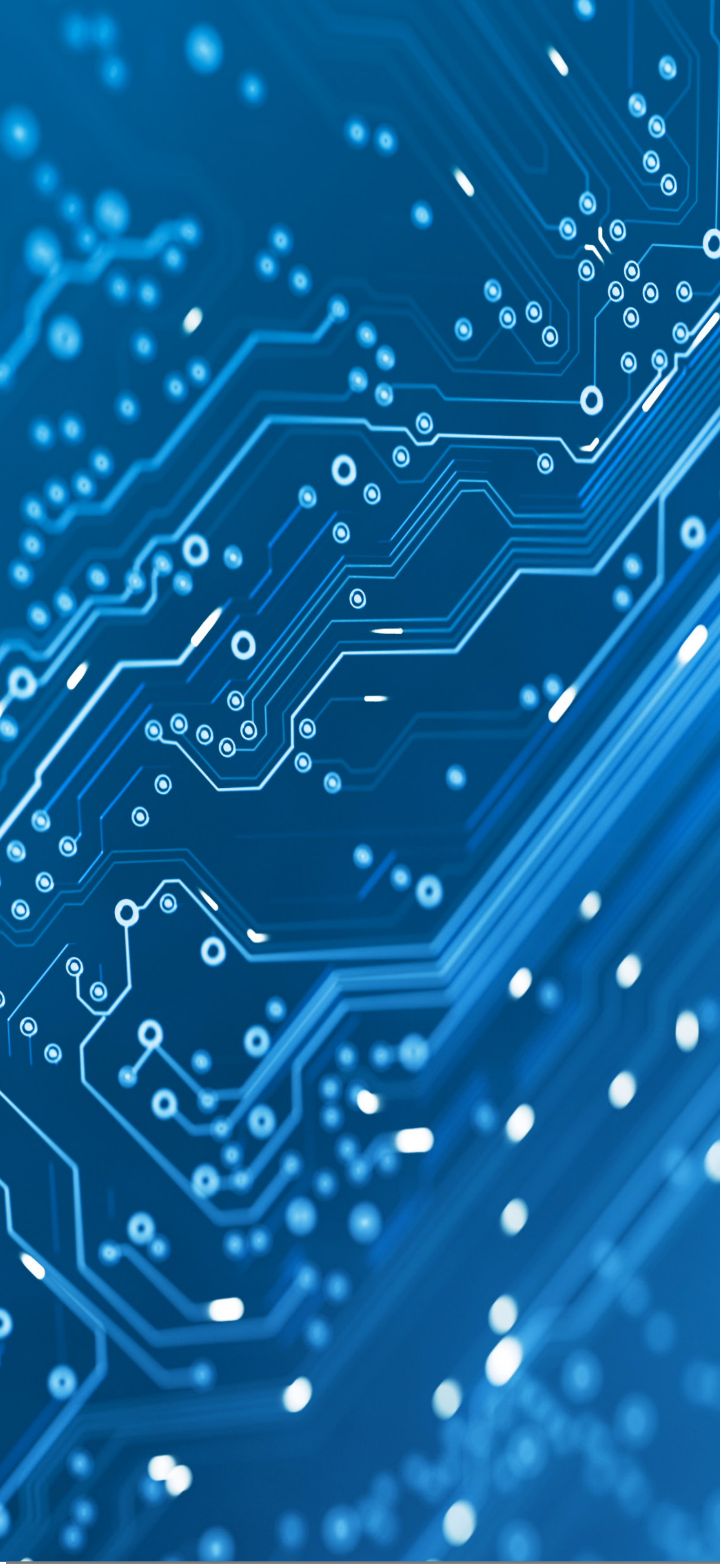
Chart 9

What are your most significant concerns about the current operating model for 1st line risk and control:

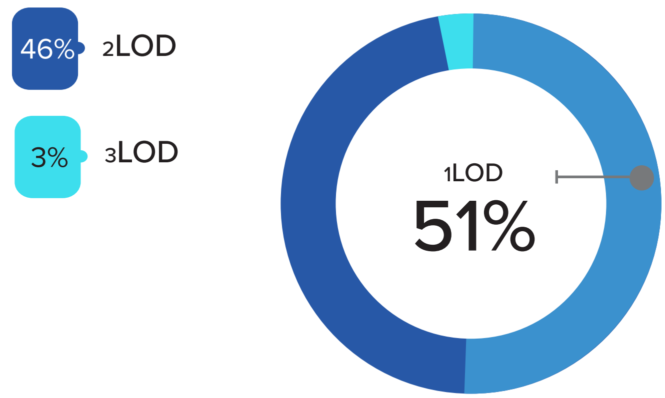


"An excellent and well run event. It's great to interact with industry peers and debate some of the current issues and trends."

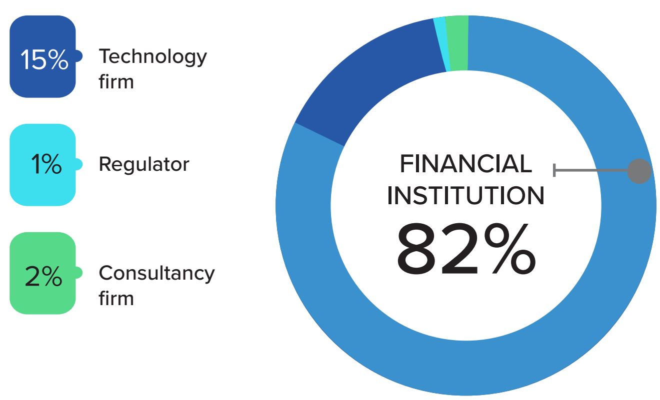
REVINDER SHERGILL, SENIOR MANAGER,
STANDARD CHARTERED BANK



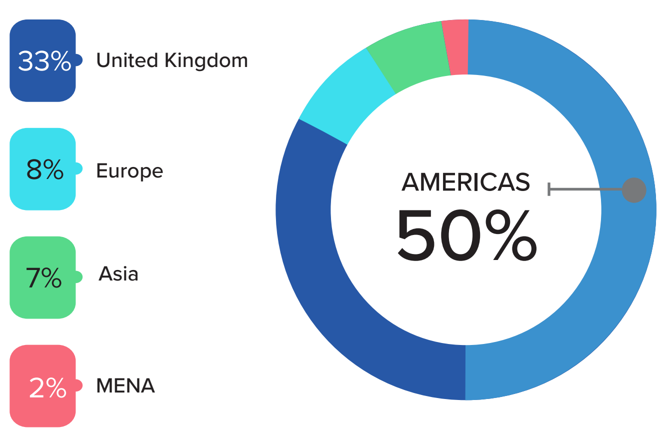
Financial Institution by Line of Defence



Delegate Profile by Type

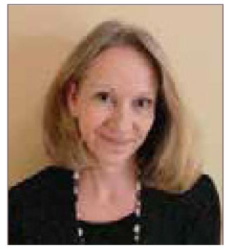


Geographical breakdown



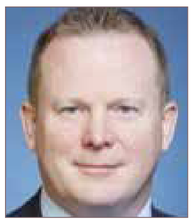
Speakers

Tim Thompson
Senior Vice President Trading and Execution Program,
FINRA



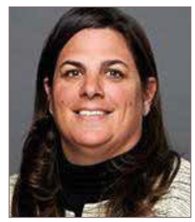
Mary Lou Peters
Managing Director, Head of Control for the Corporate & Investment Bank
Wells Fargo

Simon Nye
Executive, Chief Risk officer
National Australia Bank Europe SA.



Jeremy Kirk
Managing Director, Divisional Control Officer, IB
Deutsche Bank

Mark Satterthwaite
Managing Director, Chief Compliance offier Europe
Citigroup

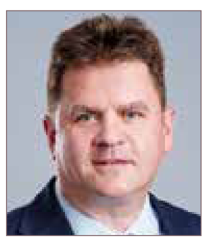


Antonia Lester
Chief Operating Officer for Investment Banking & Capital Market – EMEA
Credit Suisse

David Breen
Global Head Of IB Buisness Risk Management
UBS

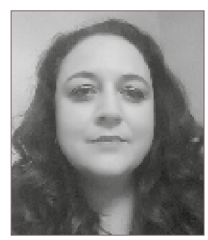
Chris Dickens
Managing Director, Head of Non-Financial Risk for Markets & Securities Services
HSBC

Ruth Kemmer
Managing Director, Global Head of Front Office Supervision, Conduct and Control Global Markets
Nomura

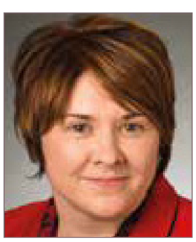


Paul Ford
Founder & Chief Executive Officer
Acin

John Holland
Senior Vice President
Smarsh

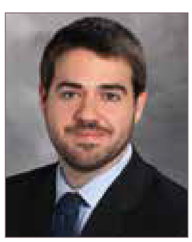


Karen Edwards
Managing Director, Business Risk Executive Global Markets EMEA
State Street



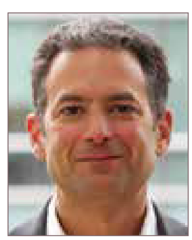
Joanne Cash
Head of Operations Control Managment
BNY Mellon

Dominique Benz
Managing Director, Head of Business Controls
Mizuho Americas

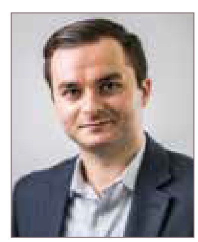


Matthew Perconte
Managing Director, Risk & Compliance
Protiviti

Roz Smith
Head of Strategy & Change, Markets & Securities Services, Head of Non Financial Risk, Securities Services
HSBC



Joseph Rondinelli
Managing Director, Business Control Management
J.P. Morgan



Stan Yakoff
Head of Americas Supervision, Citadel Securities & Adjunct Professor
Fordham Law School