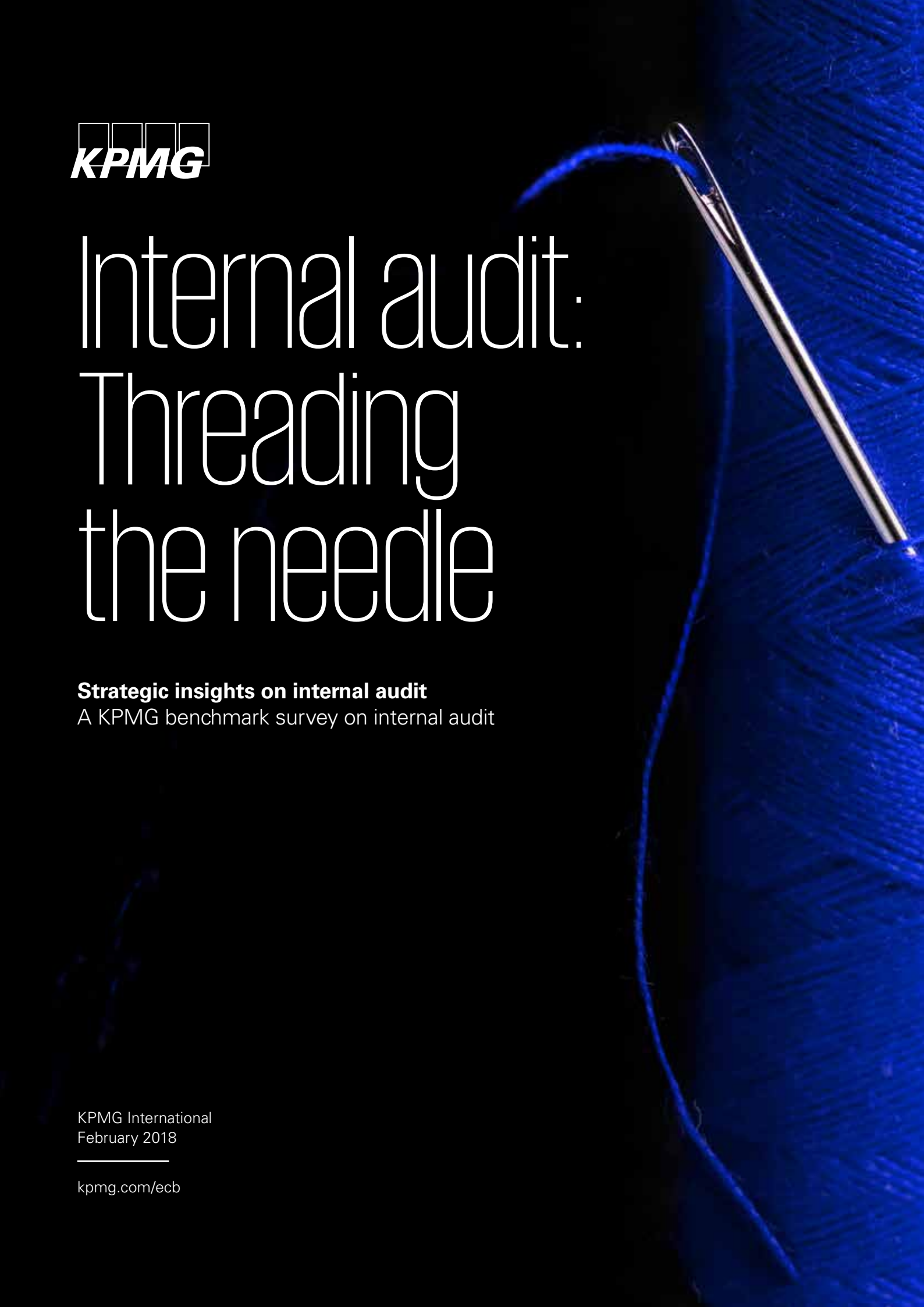


Internal audit: Threading the needle

Strategic insights on internal audit
A KPMG benchmark survey on internal audit

KPMG International
February 2018

kpmg.com/ecb

Executive summary

Over recent years, European banks subject to supervision by the European Central Bank (ECB) have been faced with the need to adjust their risk governance models to ensure they are deriving appropriate value from their internal control functions. Internal Audit (IA) plays a fundamental role in this drive for added value. Regulatory developments, stakeholder expectations, and increasing business and operational risks have all contributed to a broader and more complex mandate for IA functions.

How banks choose to respond to these challenges in the coming years will shape the impact that IA has on their entire organisation.

The traditional days of a 'checks and balances' approach are gone. IA functions can no longer rely on reactive annual reviews but must provide guidance on risk and its mitigation by harnessing data and analytics. It is critical that IA functions build a close working relationship with senior management and secures visible support from their audit committee. The more involved they become in strategy, leadership and steering committee meetings, the better positioned they are to add value. Remaining a trusted advisor, valued by banks' leaders and board members, is a key goal for many. But so too is achieving a culture that strikes the right balance between 'assurance' and 'consulting'.

> "It is critical that IA functions build a close working relationship with senior management and secures visible support from their audit committee."

Due to technological developments, new market entrants and rapid adoption rates by consumers, IA functions have had to evolve in order to stay relevant. They now need to balance a broad understanding of regulatory and financial reporting requirements with a detailed knowledge of the current issues, risks and controls that affect their organisation's business lines.

In line with the European Banking Authority (EBA) Guidelines published in September 2017, supervisors assess whether an organisation has established an effective, independent IA function, with sufficient authority, stature and resources. In particular, organisations need to ensure that the qualification of IA staff are adequate for the institution's size, locations, and complexity of risks associated with the business model, activities, risk culture and risk appetite.

Internal governance is one of the supervisory priorities of the Single Supervisory Mechanism (SSM) and a key element of the Supervisory Review and Evaluation Process (SREP) which takes place on an annual basis. In the 2017 SREP letters, supervisors highlighted areas for improvements within IA functions in more detail than they have in previous years, highlighting deficiencies in resourcing, independence, audit coverage and audit quality.

To better understand how banks are responding to developments that impact IA, KPMG professionals conducted a survey of 22 Heads of Internal Audit from DG1 and DG2 banks in 11 European countries subject to SSM Supervision. In this report we present the main findings from the survey, discussing how IA functions are currently positioned and resourced, and how strategic priorities might continue to shift in the near future.

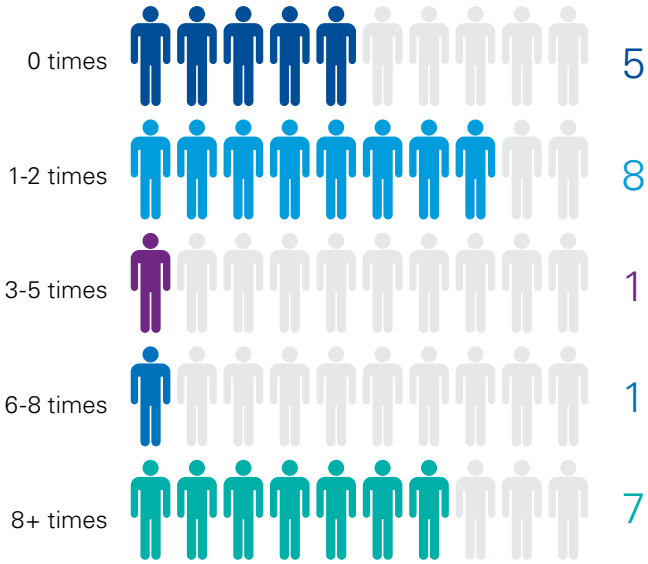
Key findings

Positioning

The majority of IA functions, as expected, have built strong relationships with the Audit Committee. However, by developing a relationship with the Executive Board, IA functions enhance their ability to challenge business objectives. This integral collaboration strengthens through timely and relevant communication.

In addition to IA strategies and annual plans, many executive boards have expectations that reach beyond their traditional services. This makes it all the more important for them to share a common understanding of IA activity. Frequent meetings with the Chair of the Board help to build a relationship as a trusted advisor and clarify expectations, while also building trust and credibility.

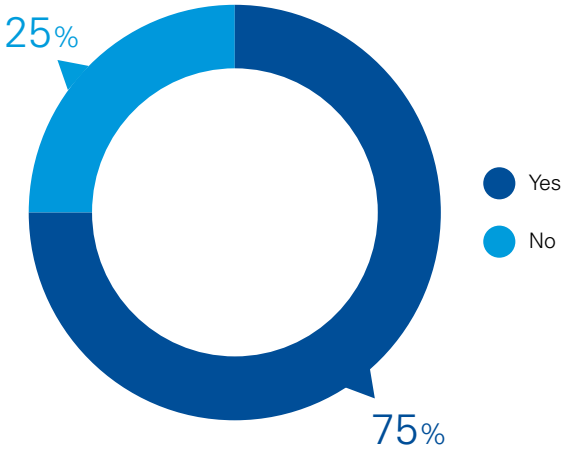
1 What is the frequency of 1-1's between the Head of Internal Audit and the Chair of Board (per year)?



For the majority of banks sampled, the most common frequency of meetings between Heads of Internal Audit and Chairs of the Board is from one to two times per year. On the one hand, 23% do not meet regularly but on the other hand, one third of respondents meet eight or more times per year.

The DG1 banks were more advanced with the frequency of meetings between the Heads of Internal Audit and the Chairs of Board, with 71% meeting eight or more times per year.

2 Do IA perform formal stakeholder satisfaction questionnaires with auditees?

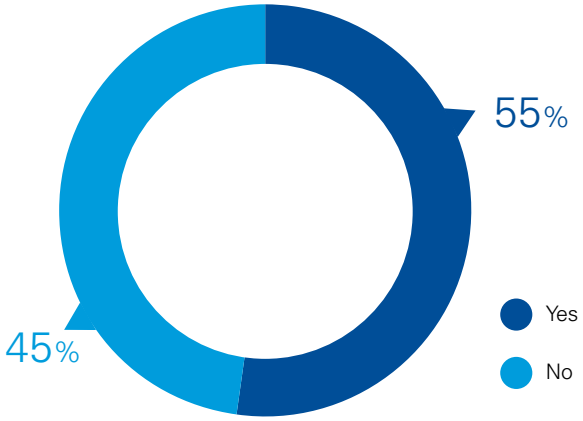


75% of respondents utilise stakeholder satisfaction questionnaires with auditees. These are performed across a mixture of individual audit assignments as well as on a cyclical basis across business units. This enables timely feedback and engagement with the business and auditee in relation to the 'service' provided by the IA function.

Mandate

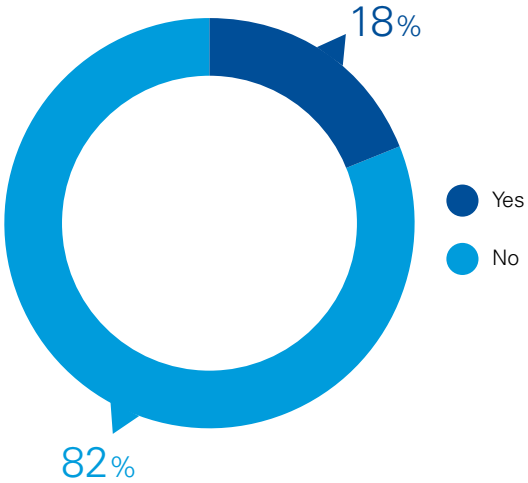
Regulatory developments, stakeholder expectations, and increasing business and operational risks have all contributed to a broader and more complex mandate for IA functions. They are finding this 'balancing act' between supporting supervision and adding value, increasingly challenging.

4 Does the IA function include a credit review function?



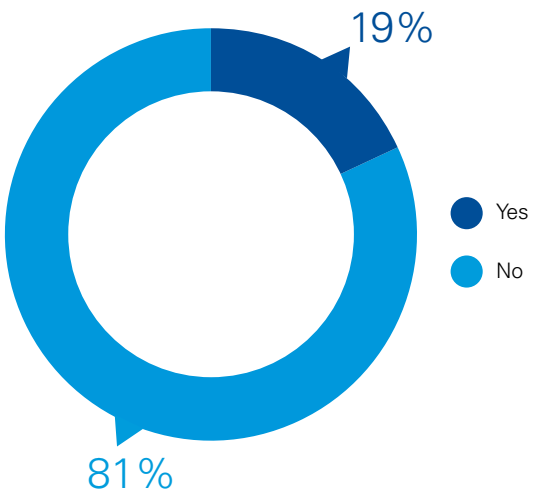
Credit review functions sit within IA functions across approximately 55% of the banks surveyed. Typically credit review functions perform both substantive compliance with lending policy testing as well as thematic reviews that enable "read across" the lending units to identify best practices. For the remaining 45%, credit review functions typically sit within the second line risk function.

3 Is IA responsible for performance of SOX control testing?



5 Is IA responsible for performing audit procedures over the closure of Risk Mitigation Programme actions from regulatory authority inspections?

6 Do you formally place reliance on other assurance providers?



While 81% of the banks surveyed do not formally place reliance on other assurance providers, there is a recognition of the need to move towards a combined assurance model. A combined approach to assurance activities among the assurance providers would improve efficiency, enhance coverage, eliminate potential duplication of efforts and ultimately provide a more meaningful opinion to the audit committee. Typical initiatives being considered include commonality of reporting/grading criteria, consistency of assurance planning cycles and reliance on assurance providers as part of IA planning activities.

81%

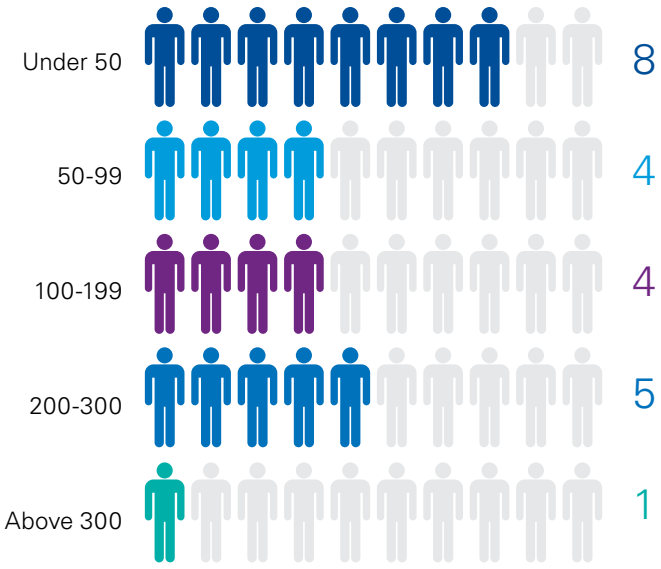
of banks do not formally place reliance on other assurance providers.

People

IA functions are expected to deliver high quality audits and act as a trusted advisor to their organisation, while keeping costs down.

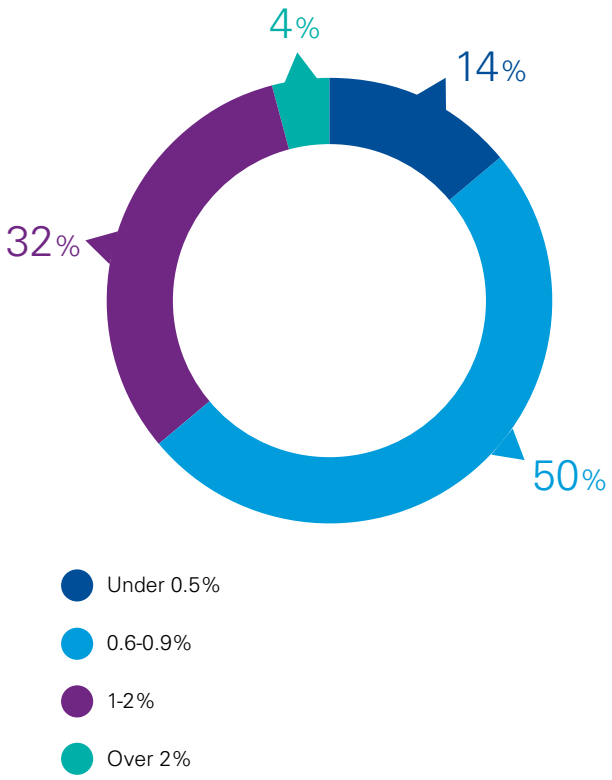
To understand how banks are meeting these expectations, we asked them how they resource and structure their IA functions.

7 **What is the headcount size of the IA function (excluding Support, Professional Practices, Quality Assurance teams)?**



Over one third of the banks sampled have a headcount under 50 in their IA function. Respectively, 27% have a headcount of over 200 individuals, all representing DG1 banks. Supervisors have identified a lack of resources in banks' IA functions and according to this year's SREP letters, the ECB expects some banks to increase their overall size. 9% of the DG1 banks in the survey have a headcount under 50 in their IA function.

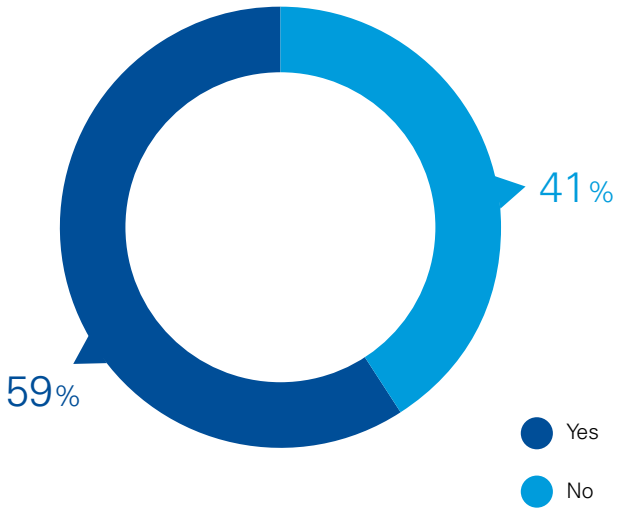
8 **What is the approximate IA function size as a % of total employees?**



Over two thirds of the banks sampled have an IA function which represents under 0.9% of their total employees. For 36% of the banks, the size represents over 1% of their organisation.

92% of DG1 banks surveyed have an IA function which represents under 0.9% of their total employees.

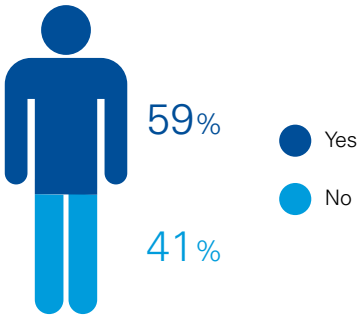
9 Are there dedicated Subject Matter Experts which deliver audits across audit teams?



The majority of IA functions have 'pooled' SME's which are then allocated across the teams as required.

Typically these SMEs include IT, operational risk, data analytics, market risk, credit risk, liquidity risk and treasury risk.

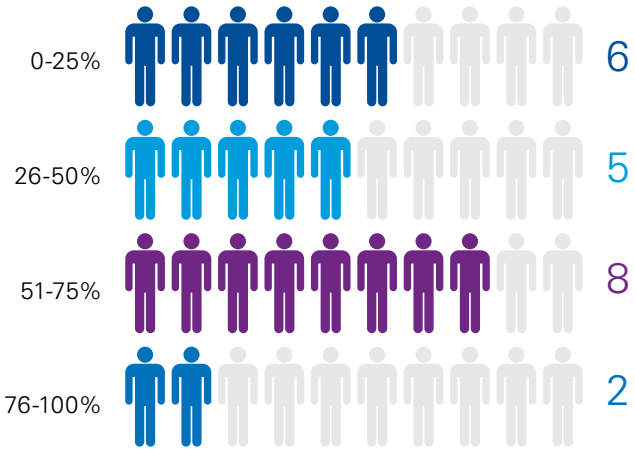
10 Do you rotate staff members between audit teams to support cross training?



Most of the banks surveyed have dedicated Subject Matter Experts who deliver audits across multiple audit teams. An optimal allocation of internal auditors, based on their expertise, plays a key role in successful audit. In addition, the rotation of staff members enhances common audit standards across the banking group and extends the knowledge transfer.

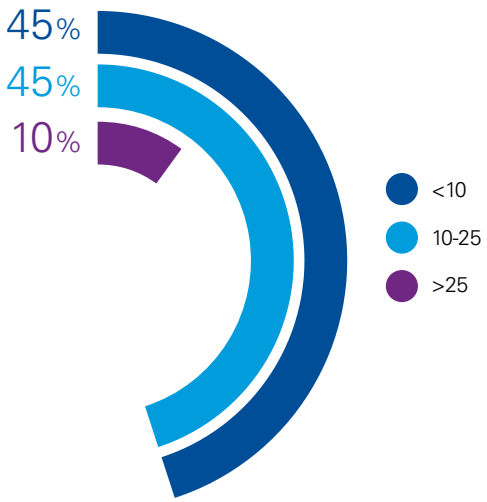
"Most the banks surveyed have dedicated Subject Matter Experts who deliver audits across multiple audit teams."

11 **Approximately what % of the team holds professional qualifications?**



There is a good balance within IA teams between those who hold professional qualifications and other team members with business experience.

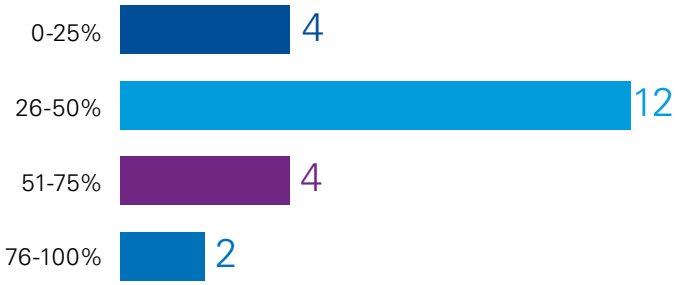
12 **Approximately how many days training are allocated per employee on an annual basis?**



76%

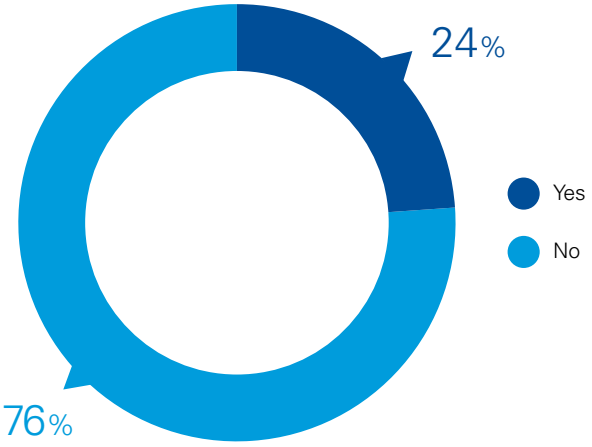
of banks surveyed have no mechanism to support secondment of resources from the business into the IA function and vice versa.

13 **Approximately what % of team have prior business experience from within your organisation?**



Maintaining a balance between business and audit experience supports cross-skilling, knowledge transfer and the delivery of pragmatic, value adding recommendations arrived at through practical business experience and technical IA experience.

14 **Do you have a mechanism to support secondment of resources from the business into the IA function and vice versa?**



Most of the banks in the survey have an IA function of which 26-50% have prior business experience within the bank. 76% have no formal mechanism to support secondment of resources from the business into the IA function and vice versa.

15 Approximately what proportion of training is externally delivered?

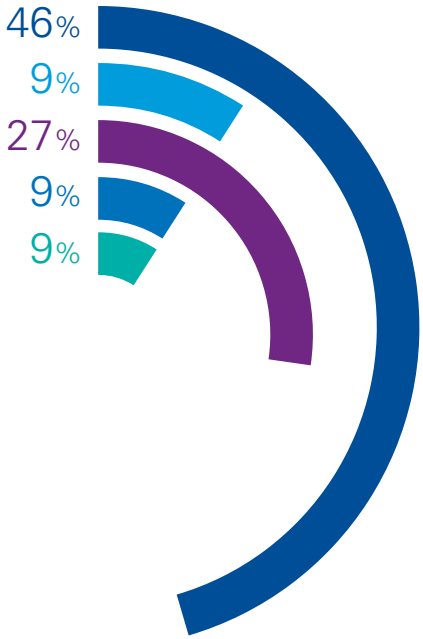
16 Do you have a formal graduate programme in place?

All of the banks in the survey use externally delivered training but there was variety in the proportion of training being outsourced. 41% of the banks in the sample have a formal graduate programme in place. Out of all the DG1 banks sampled, 46% have a formal graduate programme in place.

Internal audit structure

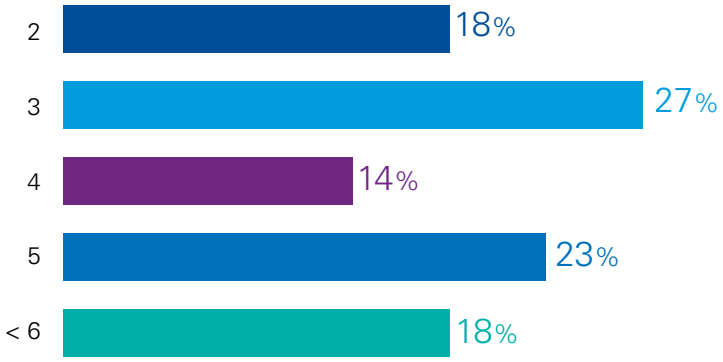
The structure of IA functions varies between banks according to their business models and size. They must be flexible enough to meet the needs of their business as well as supervisors. Almost 50% of banks surveyed have structured their IA functions by business organisation.

17 How is the IA function structured?



- Business organisation (e.g. retail, commercial, treasury)
- Business process (e.g. lending, deposit taking)
- Risk taxonomy (e.g. credit, market)
- Other (typically a mix between business process and risk taxonomy)
- Executive committee (one primary IA contact for each ExCo member)

18 How many organisational levels exist within the IA function?



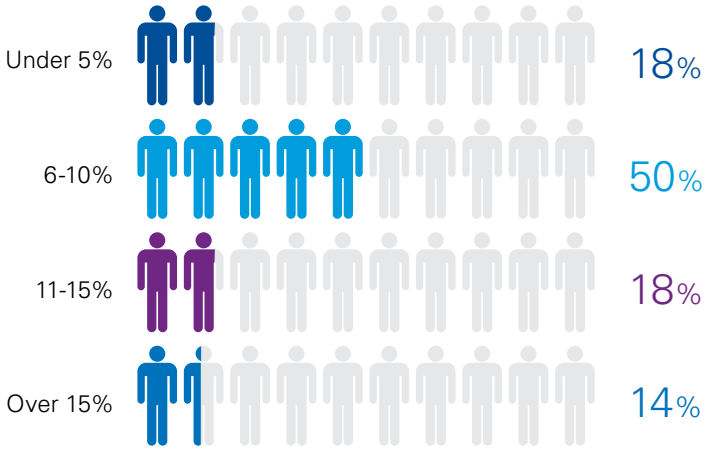
The number of organisational levels depends on the size of the audit team and the number of audit topics. Within our sample, we found significant variation in organisational levels within the IA function in banks.

The DG1 banks in the survey hold more organisational levels within their IA function than DG2 banks.

Internal auditors are expected to provide independent, objective and constructive insights for a bank's management and employees. To do this, they need to hold a remarkably varied mix of skillsets, experience and knowledge. Internal auditors may advise project teams running a difficult change programme one day, or investigate a complex fraud the next. In addition to this, identifying key risks and evaluating how well they are being controlled across the organisation requires advanced audit technique skills.

A focus on the recruitment and retention of suitably qualified and experienced staff, together with knowledge strengthening, is evident in banks' self-identification of main challenges.

19 **What is the headcount size of the IA professional practices/support team (as a % of the total IA function headcount)?**



32% of the banks in the survey have over 10% of total headcount allocated to IA professional practices/support.

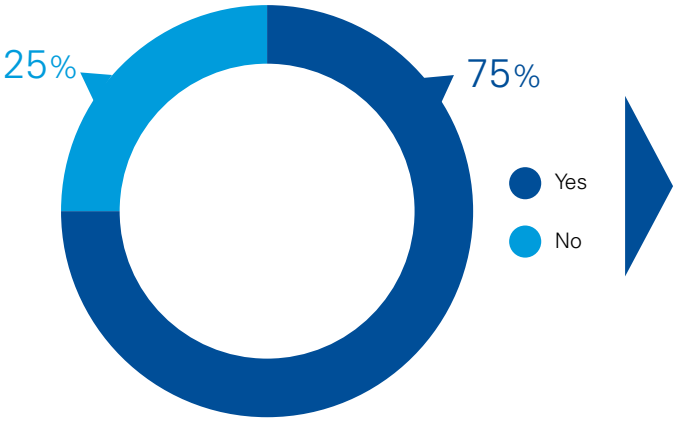
Given the need for increasing agility and ability to respond to ad-hoc requests, a number of IA functions are investing in the development of a COO function.

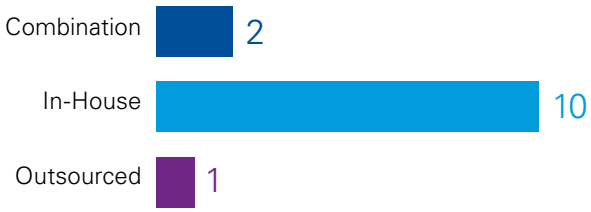
Over

50%

of banks surveyed have four or more organisational levels within the IA function.

20 Do you have an independent QA function over IA activities?





The majority of sampled banks have an in-house, independent QA function over IA activities.

21 Approximately, what % of annual audits are subject to independent QA?

The percentage of annual audits subject to independent QA varied significantly among the banks sampled.

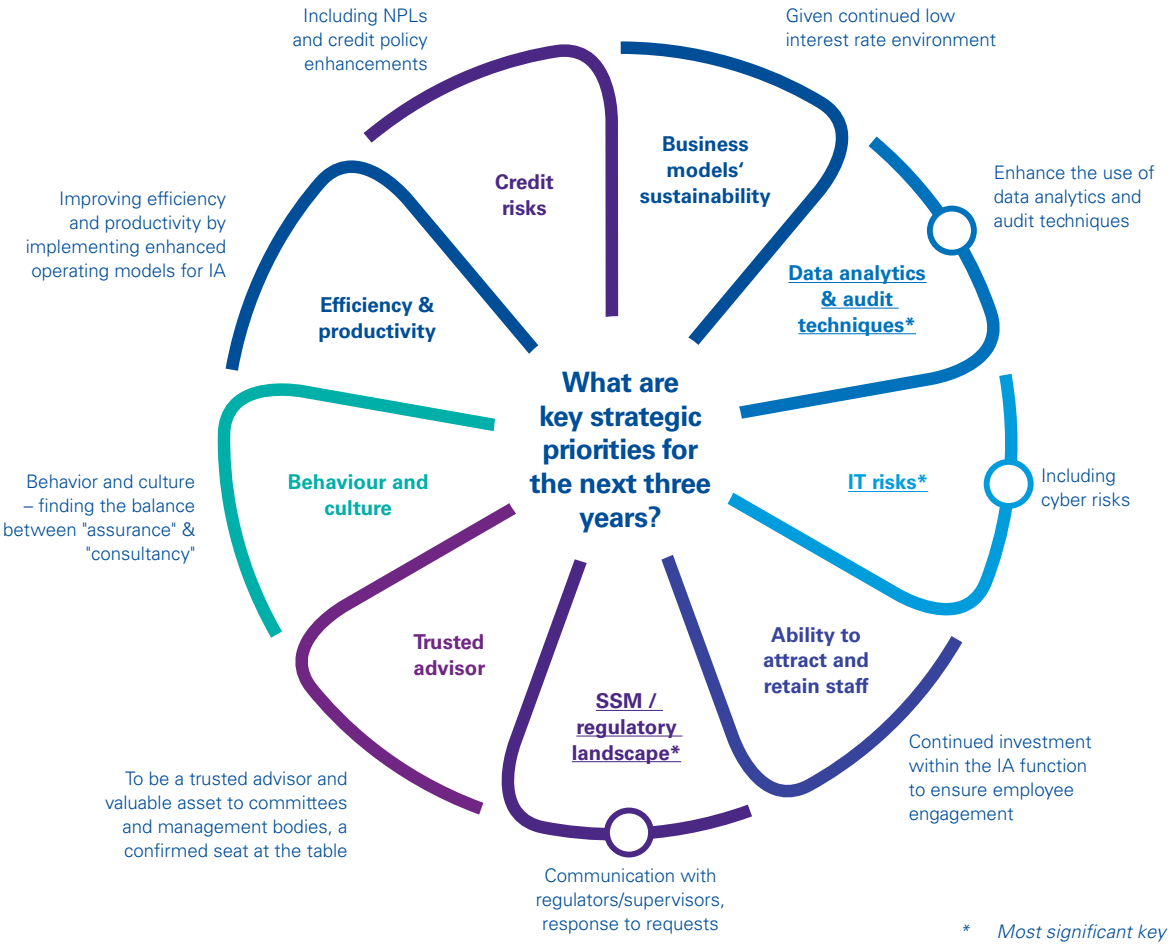
Internal audit plan

Most of the banks in the sample identify enhancement of data analytics and audit techniques, response to IT risks (including cyber), cooperation with the SSM and the regulatory landscape as key strategic priorities over the next three years.

Rapid change in business processes, fuelled by digitalisation and market environment, requires IA functions to be experts in advanced data analytics methods. They need to be able to recognise and respond to IT risks robustly, with appropriate team competencies.

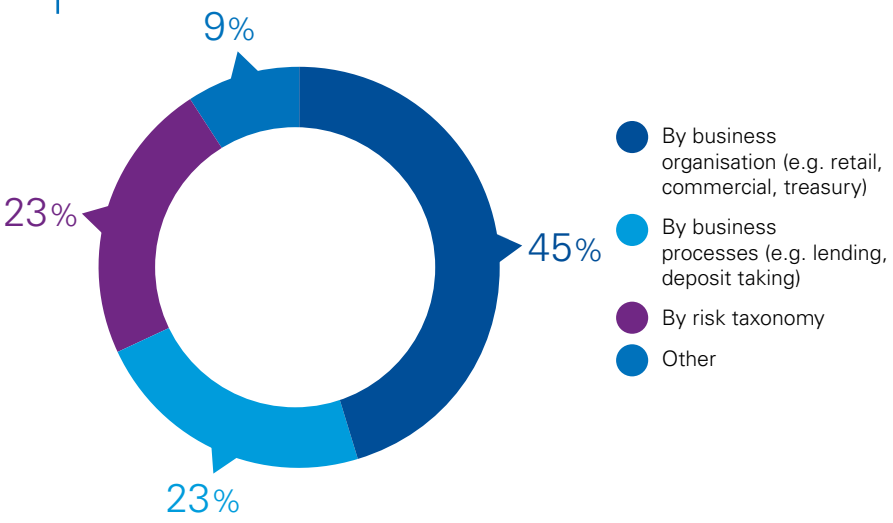
In response to new requirements and expectations set by regulators and supervisors, banks are focusing on the recruitment and retention of suitably qualified and experienced staff, in addition to in-house knowledge building.

62% of the banks sampled use a governance, risk and compliance audit tool to support audit planning and execution.



* *Most significant key strategic priorities of the banks sampled*

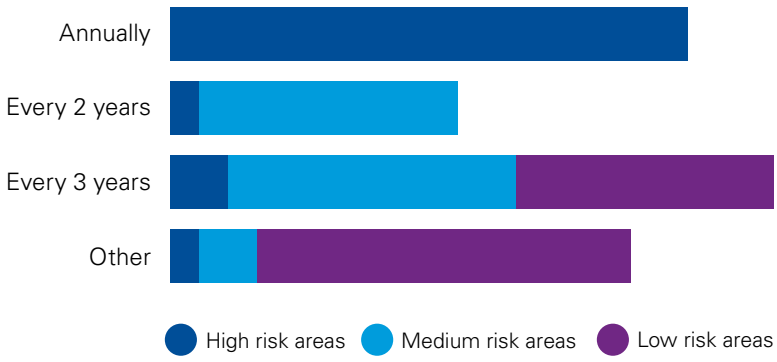
22 How is your audit universe constructed?



45% of banks in the survey have structured their audit universe by the type of business organisation (e.g. retail, commercial, treasury).

54% of the DG1 banks surveyed have over 200 audits on Group Internal Audit Plan. Respectively, 22% of the DG2 banks in the survey have over 200 audits on Group Internal Annual Plan.

23 What is the frequency of coverage for risk areas?



81% of the banks sampled cover high risk areas annually. 100% of banks sampled cover low risk areas at most every three years, unless specifically requested by management or the audit committee.

45%

of banks in the survey have structured their audit universe by the type of business organisation (e.g. retail, commercial, treasury).

81%

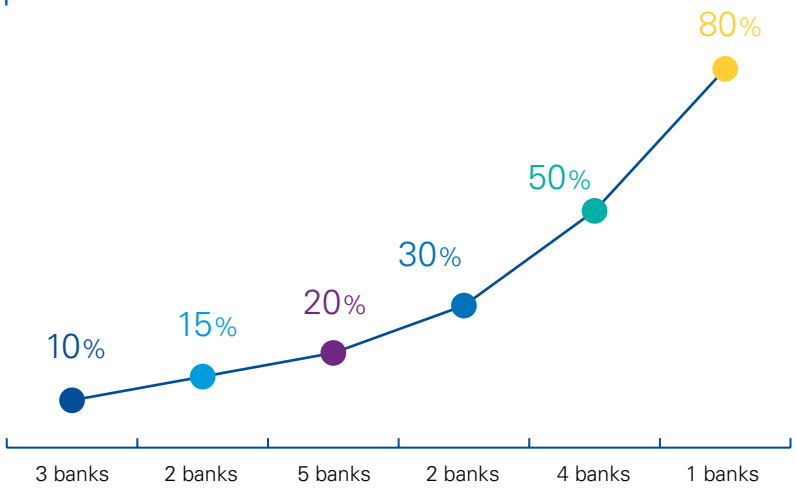
of the banks sampled cover high risk areas annually

24 The survey results highlighted the following differences between DG1 and DG2 banks' audit plans:

- 31% of the DG1 banks in the survey had under 100 in-scope/auditable entities in the audit universe. 38% had over 300 in-scope/auditable entities.
- In addition to the Internal Audit Plan, on average 20% of DG1 banks' internal audits are requested either by regulators, SSM or management.
- Over 20% of DG1 banks' audits in the Internal Audit Plan are mandatory audits for the majority of DG1 banks.
- Total number of available audit days per annum (including planned and ad-hoc audit requests) for DG1 banks are on average 23,676.

- 67% of the DG2 banks in the survey had under 100 in-scope/auditable entities in the audit universe and none had over 300 in-scope/auditable entities.
- In addition to the Internal Audit Plan, on average, 16% of DG2 banks' internal audits are requested either by regulators, SSM or management.
- Over 20% of DG2 banks' audits in the Internal Audit Plan are mandatory audits for under half of the DG2 banks in the survey.
- Total number of available audit days per annum (including planned and ad-hoc audit requests) for DG2 banks are on average 5,472.

25 What % of the audits use data analytics to support audit activities?

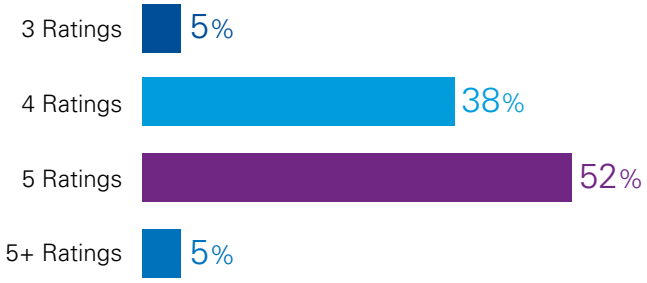


All survey respondents utilise continuous auditing techniques. Typically, we observe these being utilised across medium/low and low risk areas, thereby reducing formal audit coverage.

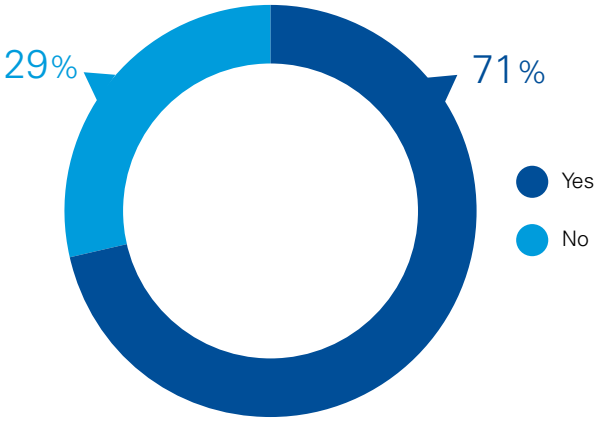
Audit reporting

Internal auditors are responsible for reporting into several organisational levels all with different interests. The rating system used for IA findings and reports need to be clear for all stakeholders. Ineffective reporting structures may result in misunderstandings and undermine the significance of their findings. In our survey we asked banks about their rating scales for audit findings and reports.

27 **How many rating scales for audit reports (number of ratings) do you use?**

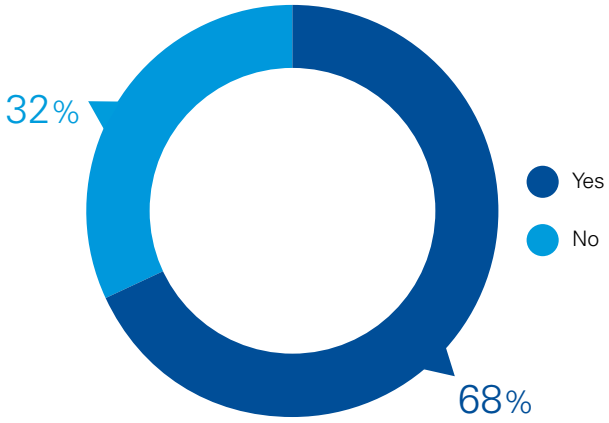


26 **Do IA issue any unrated 'products'?**



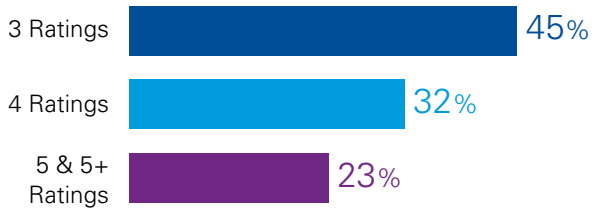
The majority of IA functions surveyed issue unrated reports as part of their 'suite' of products. Typically, IA functions have clearly defined criteria of when such unrated product is suitable for use.

28 **Do IA and other assurance providers use a consistent enterprise rating scale?**

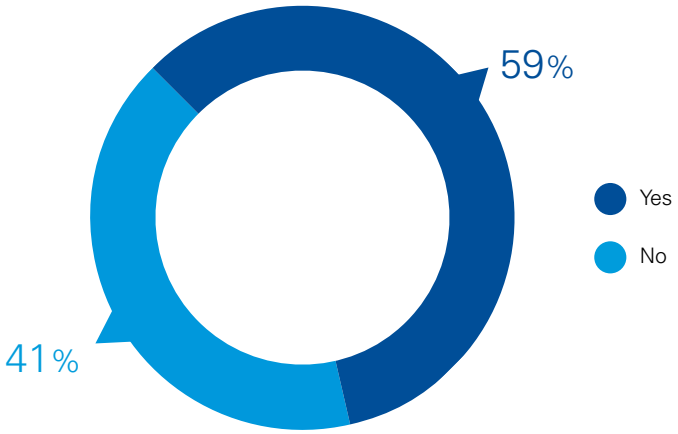


29 How many rating scales for audit findings (number of ratings) do you use?

The rating system used for IA findings and reports need to be clear for all stakeholders. Ineffective reporting structures may result in misunderstandings and undermine the significance of their findings.



30 Do Business Unit Management attend the audit committee to discuss/explain overdue IA issues?



Business Unit Management attend the Audit committee to discuss/explain overdue IA issues in more than half the banks in the survey.

This helps to drive accountability for the ownership and resolution of identified IA issues.

> The attendance of Business Unit Management at audit committees helps to drive accountability for the resolution of issues identified by IA functions.

Conclusion

The IA functions of SSM banks find themselves challenged by regulation and supervision, technological change and scarce resources. Faced with a rapidly evolving risk environment, team leaders want to develop new capabilities. But the greatest challenge for banks' IA functions could be to retain their independence while balancing the needs of the business against the demands of supervisors.

European banks continue to face a challenging operational and regulatory environment, putting their IA functions in a more prominent – and more pressurised – position than ever. Our findings show that regulation and supervision are seen as the leading challenges for IA. There are several aspects to this, including:

- The need to monitor banks' compliance with an ever-expanding regulatory burden;
- The need for close co-operation with Joint Supervisory Teams (JSTs), including conducting follow-up work based on SREP findings; and
- The need to meet supervisory expectations on internal governance, including IA functions themselves. Internal governance is a key priority for the SSM, and the on-site inspections of the 2017 SREP generated more IA-specific findings than in previous years. Some of the most common recommendations by JSTs focused on the resourcing, independence, coverage and quality of IA activities.

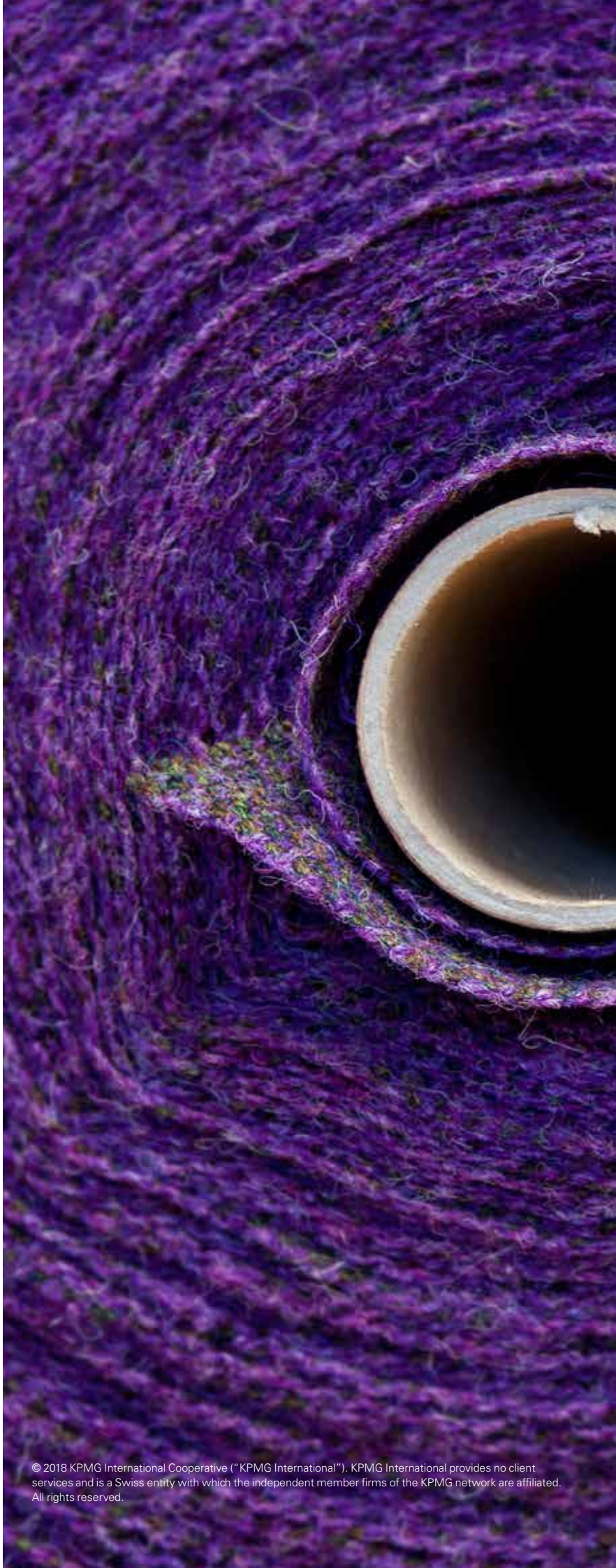
> "Looking ahead, IA leaders identify a number of key priorities for the next three years."

Apart from regulation and supervision, our survey shows that IA functions face two other major challenges. The first is technology. The rapid advance of digitalisation, data analytics, artificial intelligence and other technologies poses a number of problems for IA teams. These include the need to tackle growing cyber risks; the importance of adapting to rapidly changing business processes; and the desire to develop new IA tools and techniques that harness the latest technology.

The other major challenge is resourcing. Banks are finding it increasingly difficult to attract and retain suitably qualified and experienced IA staff as was seen in the 2017 SREP letter which judged some IA functions as having insufficient resources to fulfil their remit.

Once again, banking supervision has a significant impact on these so-called 'soft' factors, including culture and IA status within the banks. On one hand, the desire to advise banks' leaders about supervisory thinking carries the risk of compromising the independence that is essential to any effective IA function. On the other hand, the need to support JSTs in their work carries the risk of IA functions being perceived as supervisors' agents.

In short, IA functions – already under pressure to develop new capabilities while reducing costs – face a growing challenge to balance between supporting supervision, retaining their independence, and adding value to the business.



> It is critical that IA functions build a close working relationship with senior management and secures visible support from their audit committee.

Contacts

Patrick Farrell

Partner, Risk Consulting KPMG in Ireland
T: +35 387 050 4029
E: patrick.farrell@kpmg.ie

Mark Brangam

Director, Risk Consulting KPMG in Ireland
T: +35 387 050 4095
E: mark.brangam@kpmg.ie

Emma Hogan

Manager, Risk Consulting, KPMG in Ireland
T: +35 387 050 4042
E: emma.hogan@kpmg.ie

Henning Dankenbring

Co-Head KPMG's ECB Office EMA Region
T: +49 172 6852 808
E: hdankenbring@kpmg.com

Daniel Quinten

Co-Head KPMG's ECB Office EMA Region
T: +49 89 9282 4910
E: dquinten@kpmg.com

Tiia Kataja

Director, KPMG's ECB Office EMA Region
T: +49 170 264 1792
E: tiiakaisakataja@kpmg.com

Nicolas Baudoyer

Manager, KPMG's ECB Office EMA Region
T: +49 69 9587 2224
E: nbaudoyer1@kpmg.com

kpmg.com/ecb

Designed by **CREATE.** | CRT091483 | February 2018