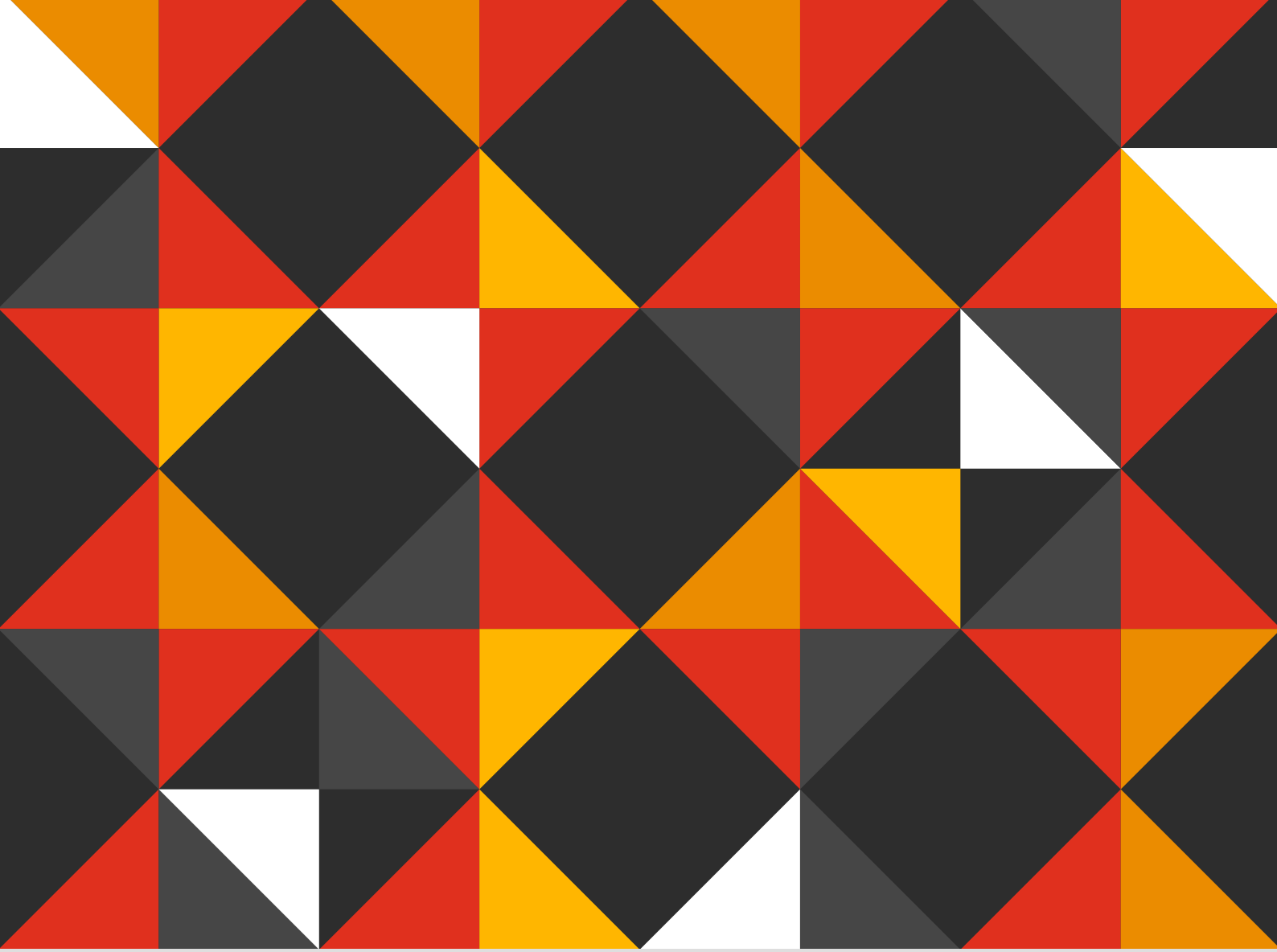


2021 Wealth Management Risk and Compliance Benchmarking Survey

As part of our 13th annual survey we recently polled over 30 Risk and Compliance functions of Australian asset managers and superannuation entities (collectively referred to as the Wealth Management sector). Questions addressed three topical areas: regulatory change, ESG and cybersecurity. Here we highlight the key observations on the industry's current challenges and provide practical actions firms can take to progress with these.

www.pwc.com.au

pwc

Executive summary

A year on from our previous survey the pace of regulatory and organisational change has only increased. Those responding best have established teams with representatives from across their organisation to develop and implement their change strategy. System and data driven solutions are being used in place of tactical, manual fixes.

Key challenges and considerations highlighted in this year's responses include:

- Engagement with third parties to determine the form and substance of data required to address Design and Distribution Obligation and RG 271: Internal Dispute Resolution requirements is proving challenging across the sector. There is a risk that products may need to be removed from the market temporarily due to non-compliance if external stakeholders have not yet been engaged.
- Looking ahead, future ongoing processes, controls and monitoring should be developed and documented by internal regulatory change working groups, including accountability for each action, to enable a smooth transition to business as usual.
- From a sustainability perspective, operational processes and controls are not keeping pace with public carbon and other ESG commitments. Risk and Compliance departments will need to become more involved in addressing these gaps and influencing the metrics measured across organisations and portfolio companies. It is not clear how targets are to be met without incremental checkpoints and standardised, quantified disclosure.
- The risk profile of cybersecurity continues to grow while regulators observe too many basic cyber hygiene issues. Upskilling boards and management to enable effective monitoring of baseline controls in place at organisations and third parties remains a priority.

Regulatory change - the pace is not slowing

Significant ongoing regulatory change continues to occupy the whole sector. Treating this as an opportunity to improve accountability, connect with investors and improve operational processes will help organisations realise the most value from adoption of these changes.

In response to the frequency of change we have seen a number of good examples of internal working groups formed. The best have representatives from: line one; ensuring sufficient knowledge of current business practice and accountability for business as usual controls in the future, and line two; providing familiarity with the requirements of new regulations, considering risk and controls and providing necessary specific expertise such as legal and information technology. This structure helps ensure streamlined design of end-to-end processes, avoiding siloed or duplicated manual controls implemented with only one regulation in mind.

Financial Accountability Regime

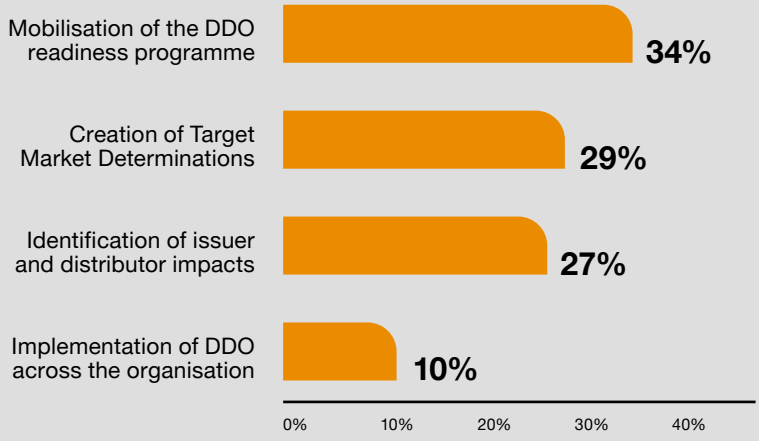
With APRA regulated entities currently reviewing the draft Financial Accountability Regime (FAR) legislation consultation package released by Treasury in July 2021, 36% of Registrable Superannuation Entities (RSEs) have already commenced implementation. Unsurprisingly, improved clarity on roles, responsibilities and accountability is seen as the main benefit (25%). The Regime, if implemented well, is also seen to have the potential to enhance collaboration both at the executive level and across the organisation (23%), driven by executives feeling more empowered to make decisions once clarity of roles and accountabilities has occurred. These benefits are consistent with those identified by banks who have already implemented the Banking Executive Accountability Regime (BEAR)[1]. The most common implementation activity undertaken to date is identifying the Accountable Persons population and starting to think about how Accountable Persons discharge their responsibilities. With the release of CPS 511 Remuneration and FAR, many firms are also considering the design of their remuneration frameworks as remuneration is an essential part of an accountability framework.

Design and Distribution Obligations

In contrast, as of April, 34% of respondents remained in the mobilisation phase in response to the Corporations Amendment (Design and Distribution Obligations and Product Intervention Powers) Act 2019 (DDO), where compliance is required much sooner.

Q3.6

What is the current stage of your Design and Distribution Obligation (DDO) implementation project?



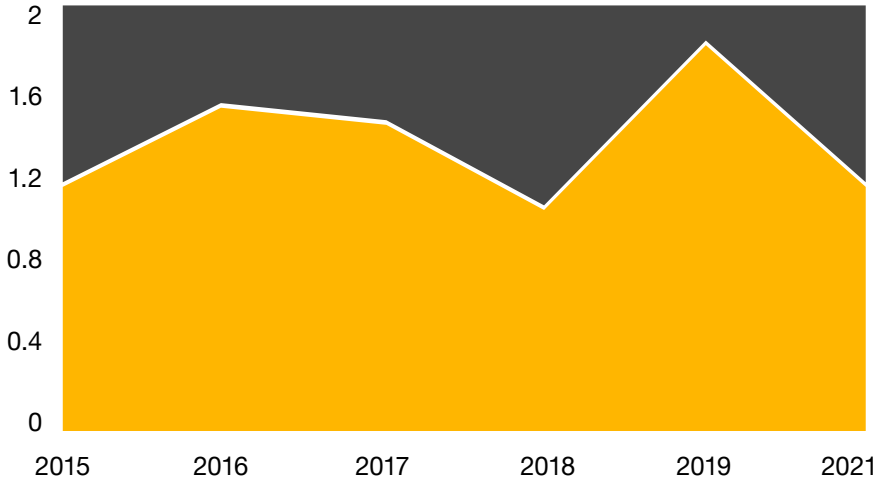
Complexity surrounding engagement with external stakeholders and data requirements is holding many organisations back. It remains a matter of uncertainty across the industry as to the best approach to manage these complexities, in particular the form and substance of data required from distributors to issuers after implementation. Where organisations are yet to engage with third parties, the risk that products may need to be withdrawn from the market temporarily due to non-compliance, as seen with similar legislation in the UK, is increasing. If not already in place, a communication and education plan should be developed as a matter of urgency and external stakeholders engaged.

1 APRA, Implementation of the Banking Executive Accountability Regime (BEAR)

Breach reporting

Responses this year have indicated that the volume of self-reported breaches continues to average between 1 and 2 per organisation. We have also observed that the frequency and granularity of requests for further detail by regulators have increased, leading to more effort spent by organisations on regulatory correspondence. With the upcoming changes from the Strengthening Breach Reporting regime applicable October 2021, it is anticipated that there will be a significant increase in the volume of breaches being self-reported arising from both more incidents being deemed significant and the expansion of the scope of the breach reporting regime.

Average number of breaches reported to regulators in the previous 12 months



This makes the development of an effective and efficient target operating model for the end-to-end incident management and breach reporting process necessary with organisations needing to refresh their policies and processes in order to meet the new requirements and ensure they are capturing all relevant matters in their incident register and assessment process.

Complaints

Reduced timeframes to respond to complaints under RG 271: Internal Dispute Resolution will be a challenge to those still dealing with an increased volume due to COVID-19. 42% of respondents had an average time for resolution and remediation outside the new 30 calendar day requirement.

42% of respondents also indicated dissatisfaction with service as the most common nature of complaints. This suggests targeted actions by line one to address common root causes could relieve pressure on complaint response teams. ASIC is also concerned with the number of manual processes and are looking for the sector to integrate broader technology solutions which allow organisations better visibility of their customers.

Calls to action

- Treat upcoming regulatory change as a strategic opportunity to clarify responsibilities, improve accountability, connect with customers and improve operational processes.
- Consider system and data driven solutions that integrate with the business and address multiple regulatory requirements in place of siloed, manual fixes.
- Ensure future ongoing processes, controls and monitoring are developed and documented by internal implementation working groups, including accountability for each action, to enable a smooth transition to business as usual.

ESG - the gap between commitments and actions

Overview

ESG reporting and metrics are an important indicator of an organisation's overall health and can provide a strong foundation about the company's impact in the world. Globally, funds with ESG credentials are increasing. Between January to November 2020 BlackRock noted that over US$288 billion was invested in sustainability assets globally, an increase of 96% from 2019.[2]

53%

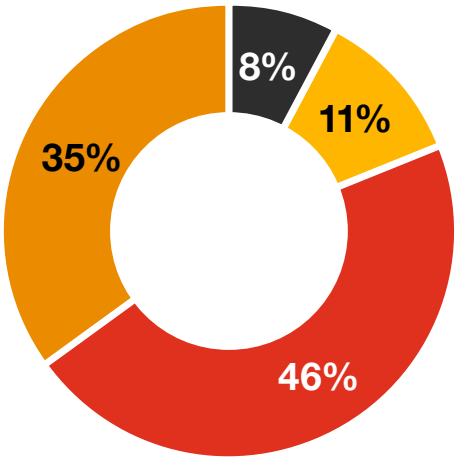
of respondents offer an investment product with ESG credentials.

2 BlackRock, Larry Fink's 2021 letter to CEOs

With this increased focus on ESG, the expectations from stakeholders for disclosures that support decision making have also increased. Asset owners and managers are calling for better ESG disclosures, not only to enable their assessment of the materiality of ESG risks and potential financial consequence on their portfolios but also to help address disclosure expectations from their own investors.

In addition to increased focus on disclosures, companies around the world are making public commitments in relation to ESG performance. For organisations in the Wealth Management sector, these commitments not only relate to a company's own operations but also their investment portfolios. 48% of participants in this survey have made a public net zero commitment on their own operations, while 44% of respondents have made a public net zero commitment in relation to their investment portfolio. The respondents' net zero commitments range from ambitious targets set for 2025 (for own operations), 2030 (for investments) to those stretching out to 2050.

How is climate risk assessed in your investment portfolio?



It is critical that companies begin to demonstrate consistency between public commitments and internal activities to manage and measure progress.

Of respondents that have made a commitment to decarbonise their portfolios, 22% are measuring carbon intensity across all of their investments while 33% are measuring a subset of their portfolios. This potential gap between commitments and measurement will present challenges for those organisations unable to demonstrate progress to investors.

The US Securities and Exchange Commissions (SEC) published a risk alert in April 2021[3], noting deficiencies between public statements, disclosures and commitments, and internal processes. The SEC observed issues where:

- Portfolio management practices did not align with disclosures about ESG approaches;
- Controls were inadequate to maintain, monitor, and update clients' ESG-related investing guidelines, mandates and restrictions;
- Proxy voting may have been inconsistent with advisers' stated approaches;
- Unsubstantiated or otherwise potentially misleading claims regarding ESG approaches;
- Inadequate controls to ensure that ESG-related disclosures and marketing are consistent with the firm's practices; and
- Compliance programs did not address adherence to the firms' stated ESG frameworks.

Closer to home, ASIC recently undertook a surveillance exercise on climate-change-related disclosure and governance practices of a cohort of large listed companies. They noted that the quality of disclosure still varies significantly with limited consistency in adoption, application and disclosure. Greenwashing was also prevalent in some disclosures reviewed. ASIC's Corporate Plan 2020-24 highlights that further surveillance will take place to assess the extent to which product issuers are engaging in greenwashing that results in consumer harm. A wide range of material has been reviewed by ASIC to date, including blog posts.

Investors are also challenging the manner in which organisations are managing and disclosing climate risk with thousands of lawsuits globally and over a hundred in Australia.

55% of respondents who offer a product with ESG credentials do not measure the carbon intensity of their portfolio, with only 9% stating they are planning to in the future. Moreover, for

3 SEC, Review of ESG Investing

broader ESG issues, such as pollution, waste, social issues, natural resources and stakeholder opposition, companies are most likely to either adopt an informal approach to consideration or use standardised enquiries to help assess the topics' impact across the portfolio. While standardised enquiries may be appropriate in some circumstances, to measure against targets and derive greater insight companies may require more tailored information.

The survey noted that only the minority of respondents are relying on quantitative ESG data. Climate change, with 35% of respondents quantifying information, was the most quantified topic, while issues such as stakeholder opposition were as low at 16%.

The mismatch between external commitments and internal processes highlighted in our survey is consistent with the findings in the SEC's risk alert. Without adequate measurement, companies may be opening themselves up to claims of greenwashing or misleading information in the future.

Climate risk reporting

The quantity and quality of ESG disclosures has escalated in the last 18 months; with a strong focus on climate risk reporting in particular. Between 2019 and 2020 the increase in companies reporting on climate risk in alignment with the recommendations of the Task Force on Climate Related Financial Disclosures (TCFD) increased by 85%.[4] The structure of these recommendations, focusing on disclosure of governance, strategy, risk management and metrics and targets, aims to enable investors to price climate-related risks and opportunities.

41% of respondents have either begun to report, or are reporting on the TCFD recommendations in relation to their portfolios, while 25% of respondents are reporting on the recommendations only in their own operations. As a financial services company, reporting on climate risks to operations but not looking at portfolio emissions may result in the most material impacts to an organisation not being assessed.

4 FSB, 2020 Status Report: Task Force on Climate-related Financial Disclosures

Involvement of risk

The survey responses reflect the broader trends observed in the Wealth Management sector; there is no one-size-fits-all approach in the involvement of risk in ESG.

One thing is clear, if companies are going to use ESG information in decision making, Risk and Compliance will play an increasingly important role. Not only will their involvement be crucial in ensuring appropriate controls exist to manage ESG risks but understanding and helping to quantify the potential financial implications of these risks will require integration of risk management processes.

Financial institutions therefore need to go beyond the current regulatory minimum. Only those companies which take a holistic approach - starting with their own strategy - will be able to stand out from the competition, manage emerging risks and pioneer new business areas.

Calls to action

- Where you have made commitments ensure you have designed and implemented processes able to measure related ESG performance. For Net Zero commitments, identify the operational and strategic risks to achieving the target and manage to within appetite.
- Integrate ESG processes with other related activities rather than performing as a stand alone activity.
- Extend existing ESG due diligence performed on investment acquisition to measure and assess ongoing performance.
- As an asset owner, if portfolio management is outsourced to an asset manager, ensure your asset managers are adequately gathering decision useful ESG information to help you achieve your commitments and meet your investment mandates.

Cybersecurity - a continually evolving threat

Overview

In 2020, the cybersecurity risk landscape of many organisations was impacted by changes in the ways of working (influenced by the pandemic), accelerated digitisation and a surge in intrusions, ransomware, data breaches and phishing attempts across the globe[5]. As cyber threats rise, regulatory expectations around cybersecurity have also heightened. In August 2020, ASIC filed first of its kind legal proceedings against RI Advice, an Australian financial services licensee, for failing to have adequate cybersecurity systems in place.

From 1st of January 2022, Section 56 of the Financial Sector Reform (Hayne Royal Commission Response) Bill 2020 concerning the extension of indemnification prohibitions will also mean that any future civil or criminal penalties can no longer be funded from member funds, creating another area of exposure for Trustees. Fines may limit capital for investment and could ultimately impact returns and brand reputation.

5 PwC, Global Digital Trust Insights Survey 2021

58%

The proportion of data breaches reported to the Office of the Australian Information Commissioner in the last six months of 2020 which were due to a malicious or criminal attack.[6]

$1.25m

The average ransomware payment made in Australia.[7]

This survey responses reflect the broader cyber risk trends identified as part of the PwC Global Digital Trust Insights Survey 2021 and our recent research in the Superannuation sector (co-authored report by PwC Australia and Gateway Network Governance Body Ltd ("GNGB") – Securing the future: Protecting Australia's superannuation ecosystem against cybersecurity threats). Key calls to action for Risk and Compliance specialists include the need for better understanding of cyber risk, and improved industry collaboration to deal with the increasing cybersecurity threats associated with the complex web of third parties in the Wealth Management sector.

Understanding and monitoring of cyber risks

The Australian Prudential Regulation Authority (APRA) has signalled concern that regulated entities in financial services may not be doing enough on cybersecurity and that too many financial services organisations may not be in full compliance with CPS 234, its first mandatory prudential standard for information security. As local and global regulators heighten their expectations around cyber, it is important that Wealth Management organisations take steps to understand their cyber risk exposure and their compliance status with relevant cybersecurity regulatory requirements and guidelines, such as CPS 234, ASIC Cyber Resilience Good Practices and ASIC RG 132 Funds management: compliance and oversight. The following are instrumental to establishing sound practices around cybersecurity risk and compliance:

- Understand what your top cyber risks are;
- Determine whether your residual cyber risk profile is in line with your organisation's risk appetite;
- Identify the cybersecurity regulatory requirements and guidelines for your organisation and the controls to manage these;
- Establish a good understanding across the organisation around the reportable notification requirements of cybersecurity incidents and material control weaknesses; and
- Consider the impact of potential changes in the regulatory landscape (e.g. Security Legislation Amendment (Critical Infrastructure) Bill 2020 and heightened expectations around APRA Prudential Practice Guide CPG 235 - Managing Data Risk and ASIC RG 132 Funds management) in your compliance plan and cybersecurity strategy.

6 OAIC, Notifiable Data Breaches Report: July-December 2020

7 PwC, Building a ransomware resilient Australia 2021

Monitoring and managing third party security risk

As organisations continue to increase the use of cloud and other third party providers to support their operations, the threat of a third party compromise increases. Financial service organisations, in particular, are also facing increased regulation through CPS 234 around data handled by third-party providers.

63%

of respondents indicated the high degree of outsourcing / heavy reliance on third parties is one of the main factors that drive cyber risk.

At the heart of effective third party security risk management practices lies the following principles:

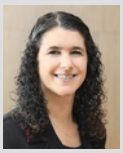
- Establish good visibility and monitoring over third parties that handle your organisation's sensitive and non-sensitive data. Understand the cybersecurity risk associated with those third parties based on the type of data they handle, host and related contractual arrangements;
- Review third party contractual requirements for inclusion of obligations to protect your data, notify significant incidents and provide assurance over their information security control environment; and
- Have appropriate governance practices in place to monitor and manage remediation of third party security risks.

Calls to action

- Upskill on cybersecurity across all levels, from the Board to frontline customer representatives.
- Invest in skilled resources, processes and tools to meet requirements for baseline controls.
- Monitor the operating effectiveness of baseline controls across your environment and obtain an appropriate level of assurance.
- Assess your third parties' adherence to their control environment.

Contacts

Risk and Compliance



Deanna Chesler

Partner
deanna.chesler@pwc.com

Adrian Gut

Partner
adrian.gut@pwc.com

Paul Collins

Partner
paul.d.collins@pwc.com

Duncan Key

Senior Manager
duncan.b.key@pwc.com

ESG

John Tomac

Partner
john.tomac@pwc.com

John O'Donoghue

Partner
john.odonoghue@pwc.com

Lucie Knorr

Senior Manager
lucie.knorr@pwc.com

Cybersecurity

Peter Malan

Partner
peter.malan@pwc.com

Nicola Costello

Partner
nicola.costello@pwc.com

Regulatory Assurance Leadership

Craig Cummins

Partner
craig.cummins@pwc.com

Sarah Hofman

Partner
sarah.hofman@pwc.com

WLT127082905