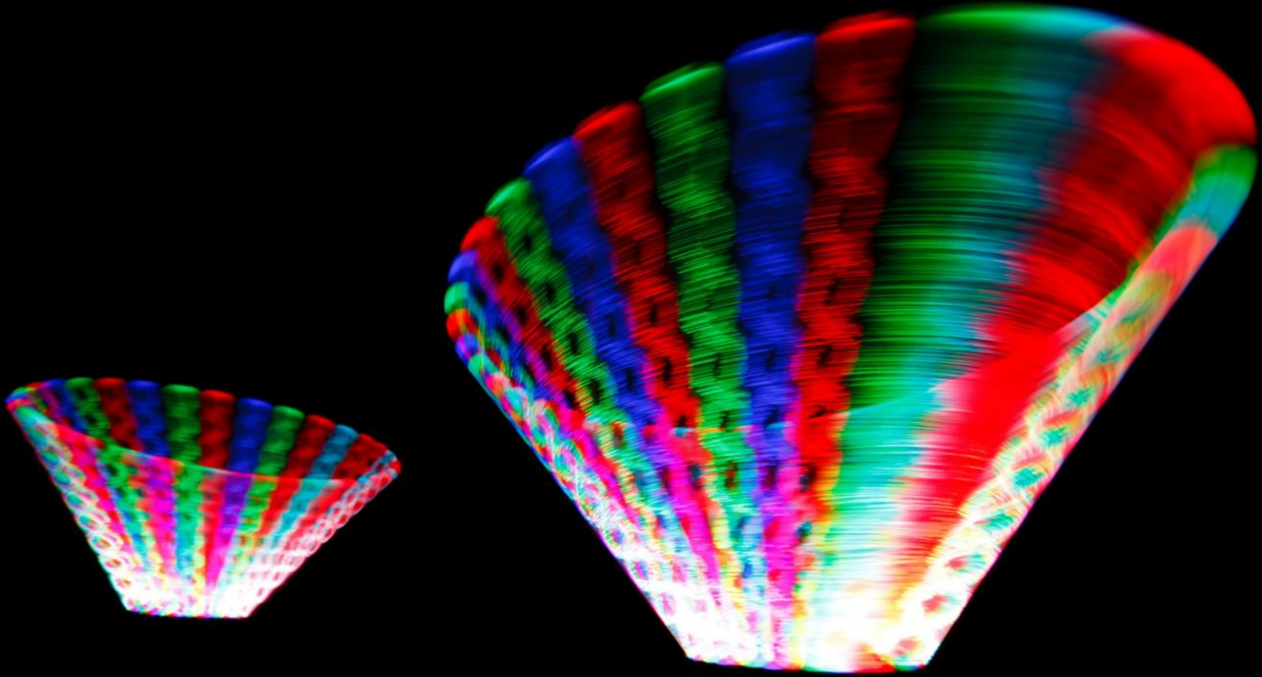
Deloitte.



Third Party Assurance Reporting

Insights and perspectives, including 2016 benchmarking results

Introduction

Deloitte’s Third Party Assurance & Advisory team performs an annual benchmarking survey in order to analyse third party control assurance reports issued in Australia. To the best of our knowledge, it is the leading survey in the Australian market.

Our benchmarking analysis includes an assessment of the nature of underlying controls and root causes for deviations in controls.

The findings of our survey can be used to help benchmark your own organisation’s report, or those received by you from your service providers.

There are several standards and guidance statements on which controls reporting is based in Australia and overseas. This report is not aimed at the technical reader, however it does provide a technical update on these standards and guidance statements.

The confidentiality of service and user entities is maintained at all times. Please contact a member of our team if you would like to have a more detailed discussion about the trends we are seeing and how this might relate to your organisation and it’s extended enterprise.

Executive Summary: Insights and Perspectives

Observations and trends in respect to our benchmarking analysis

Deloitte Insights

- The increased rate of qualifications and deviations are, in part, a consequence of **client and regulator expectations rising,** leading to higher auditor scrutiny.
- Some users of these reports are calling for a r**evision of the scope and purpose** of third party assurance reports in order to **gain greater assurance** over third party risks beyond core operational and financial risks.

For the past seven years, Deloitte have performed an annual benchmarking survey in order to analyse approximately fifty (50) third party control assurance reports issued in Australia. Below we summarise our key takeaways from the 2016 benchmarking analysis.

Increase in qualified reports

In 2016 there was an increase in the number of qualified reports to 7% of the overall population. Each qualified report was the result of **ineffective control design across a number of control objectives**, in combination with control deviations identified.

Increase in deviations

- In 2016, control deviations from surveyed reports **increased 6% from 2015**. There was an average of 4 deviations per report.
- The top 2 deviation in 2016 related to **inappropriate user access** and **inadequate review** controls. This is consistent with previous years.

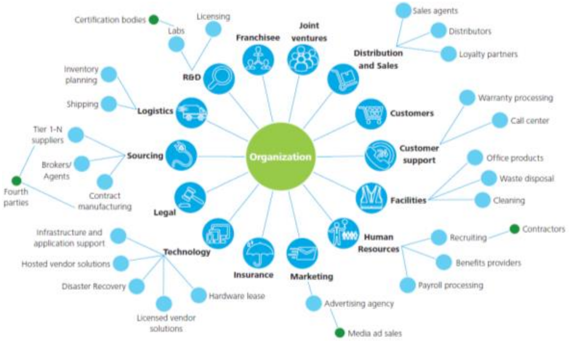
Scope and Purpose of Third Party Assurance Reports

Some users of these reports are challenging whether the purpose and scope should be revised to **broaden and/or deepen assurance activities** in certain areas to drive continual improvement, including areas such as cyber security, compliance, culture, conduct, governance, unit pricing, and third party monitoring.

Internal control efficiency and effectiveness

- The reports surveyed show an overall **greater reliance on manual compared with automated controls**. This is in line with previous years' surveys. This can be explained by the complexity and cost in implementing automated controls.
- Contrary to previous years, the survey showed that **organisations have been investing in preventative controls** more than manual controls. This is cost effective and reduces risk.

Overall third party landscape –insights and perspectives



An organisations third party landscape is increasingly pervasive, complex & critical to their market success.

Deloitte can help your organisation:

1. Understand its third-party landscape ("Map");
2. Identify the maturity, strengths & gaps in the Third Party environment across 10 focus areas ("Assess");
3. Build (or improve) a fit-for-purpose Third Party Governance & Risk Monitoring Framework ("Build");
4. Implement the strengthened approach ("Embed")

Third party control assurance reports are just one source of comfort for users of third party providers.

As third party failures increase and continue to get media coverage and regulator attention globally, implicating both the third party and user organisations, we are seeing increased focus by Boards to enhance the maturity of their third party frameworks.

Some common activities being undertaken by organisations to mature their third party frameworks include:

2. 1. Developing an enterprise wide view of their extended enterprise / third party landscape. This includes both a detailed list as well as a 1-2 page map / diagram.
3. Appointing a third party framework executive sponsor to champion change activities and drive a common set of standards and guidelines for the business
4. Re-assess current third party vulnerabilities, and identify gaps in skills and process within your organisation to effectively assess and manage these risks. Enhance the effectiveness of current due diligence and monitoring activities.
5. Look for opportunities to further create and protect the value third parties bring to your organisation, such as new innovations, technology, operational efficiency and cost reductions.
6. Develop a roadmap to optimise the third party framework, including in areas around strategy, governance and policy, people, process and technology.

INSIGHTS AND PERSPECTIVES
DETAILED ANALYSIS
TECHNICAL UPDATE
CONTACT US
APPENDIX A

Under the spot light: APRAs survey results on cyber security incidents

Cyber-security is a hot topic & cyber-attacks on business and government are increasing in Australia. Their impact goes far beyond personal embarrassment and corporate reputational damage.

Are your service providers prepared to address concerns about Cyber Risks?

During 2016, APRA undertook a survey to gather information on cyber security incidents and their management, in line with expectations raised on CPS / SPS 231 'Outsourcing'. Below we present results from the survey which identified the following areas for improvement:

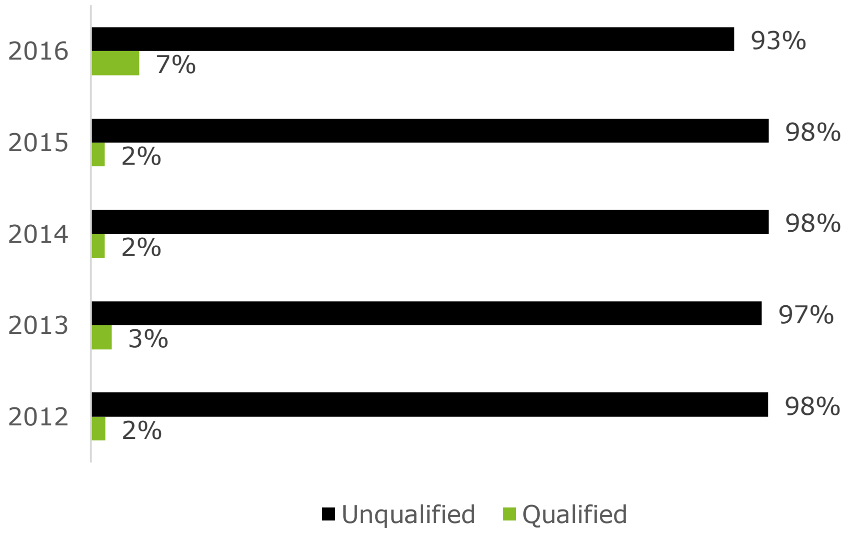
- Governance: Ensure boards and executive management are well informed regarding cyber risks and **prepared to prevent, detect and respond them**.
- Preparedness: Regularly test **response plans and recovery capability**
- Scope: **Cover the extended enterprise**, including services providers, joint ventures and offshore locations.
- Strategy: **Investment** to address evolving forms of cyber risks
- Capabilities: **Access to specialist** cyber security resources
- Situational awareness: **Establish information source** on security practices, monitoring and responses.
- Incident response: Invest in capability to **detect and respond to incidents in a timely manner**
- Assurance: Maintain **ongoing assurance over effectiveness** of prevention, detection and response.
- Collaboration: **share threat and response information** with Government, industry and customers.

Detailed benchmarking analysis

Qualifications

- The percentage of qualified opinions has increased to 7% compared with the 'norm' 2-3% in previous years.
- There is no commonality of break downs of controls between qualified reports. Issues related to ineffective control design, poor user access, inadequate review, compromising compliance and data integrity issues.
- The increased rate of qualifications and deviations are, in part, a consequence of client and regulator expectations rising, leading to higher auditor scrutiny.

Control Report Opinions



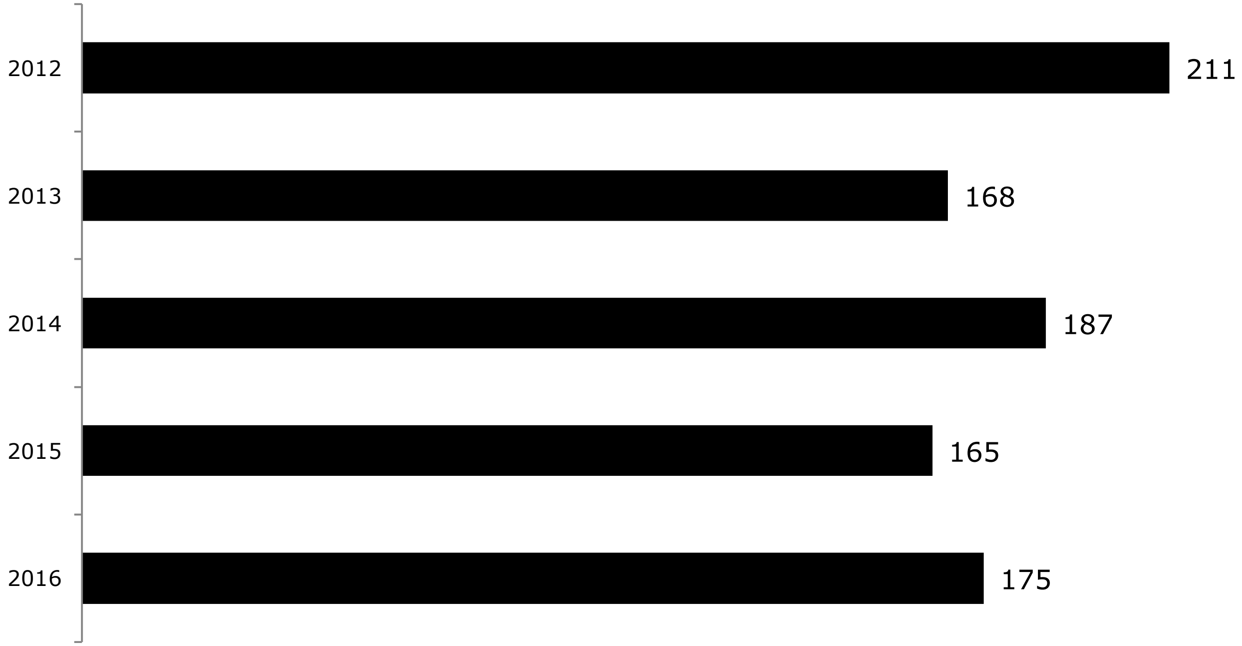
Deviations

- In 2016, deviation have increased slightly from 2015. Our analysis shows an average number of deviations per report of just under 4.

Key questions:

- Do you seek guidance from your auditors on changes to controls throughout the year?
- What type of risks are related to these deviations?
- Are the instances of control deviations improving in your organisation? If not, why are you falling behind the improving trend?

Total number of deviations



For details by sector, refer to Appendix A.

Risks associated to the deviations

Each control deviation identified was mapped to a risk category. The two most frequent risks associated to deviations raised in third party reports surveyed are:

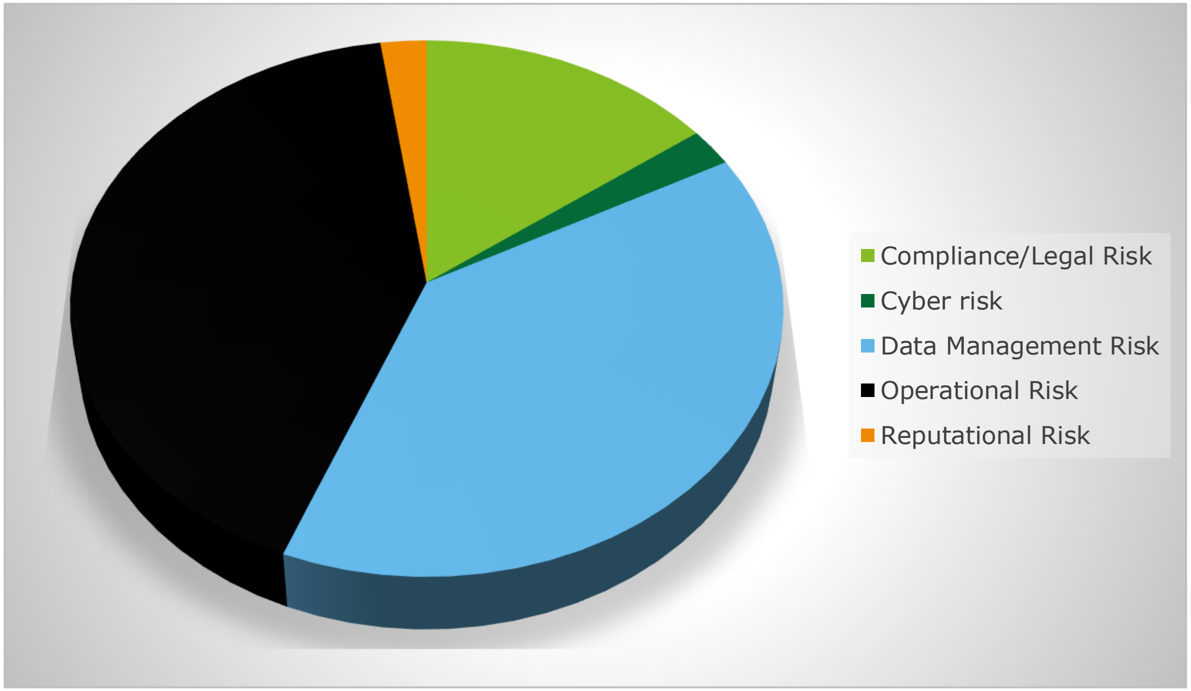
Operational Risk

Third party operational excellence is inadequate to provide the required services at the expected levels and consistent with service level reporting requirements.

Data Management Risk

Third party lacks the necessary infrastructure, policies, or procedures to protect information and intellectual property from unauthorized access, modification, destruction, disclosure or misuse, potentially resulting in financial and reputational loss or legal or regulatory action.

Third Party Risks



For detailed analsis by sector, refer to Appendix A.

Risks associated to the deviations

Other associated risks descriptions are:

Compliance/Legal Risk

Third party fails to comply with all applicable laws , industry related regulations and standards, or internal policies, or fails to provide adequate governance and oversight, placing the organisation at risk of regulatory or legal action.

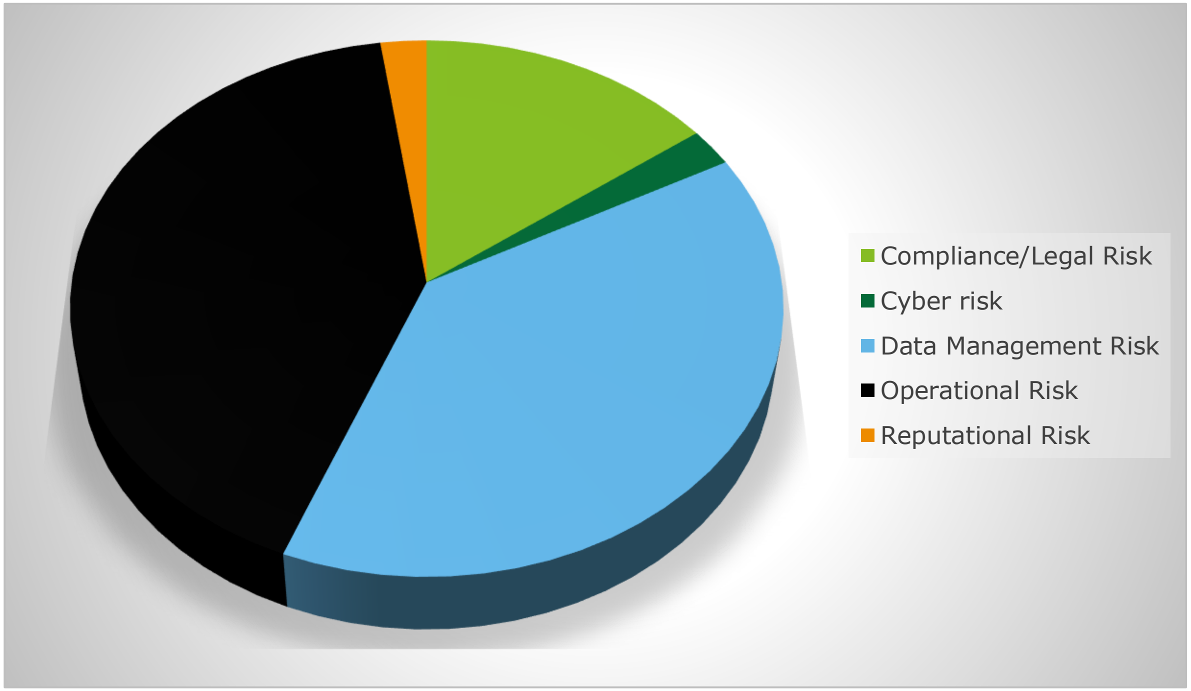
Reputational Risk

Third party activities pose the risk of negative public opinion due to poor customer service, fraud, or other factors, resulting in financial or reputational loss.

Cyber Risk

Third party fails to protect their digital assets and safeguard their organisational security, customer data and security controls.

Third Party Risks



For details by sector, refer to Appendix A.

Days to report

Timeliness of reporting deteriorated in 2016, with the average time to issue an opinion on control reports being 53 days compared to 47 days in 2015.

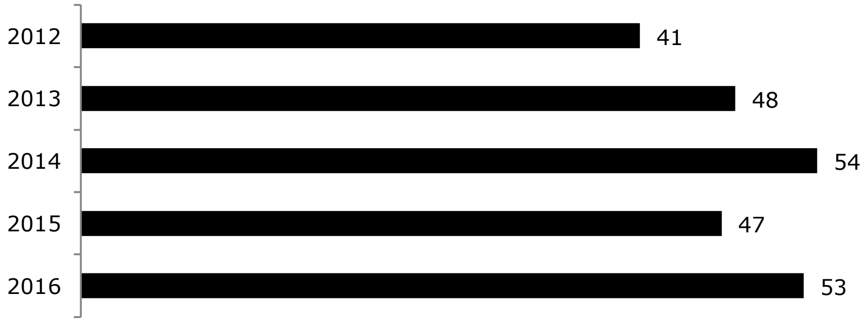
The Registry sector had the fastest turnaround of reports at 41 days whilst the Asset Management sector was the slowest at an average of 62 days.

There was one significant outlier contributing to the delay noted for Asset Management issuance in 2016. Excluding the outlier brings days to issuance in line with other sectors to 54 days.

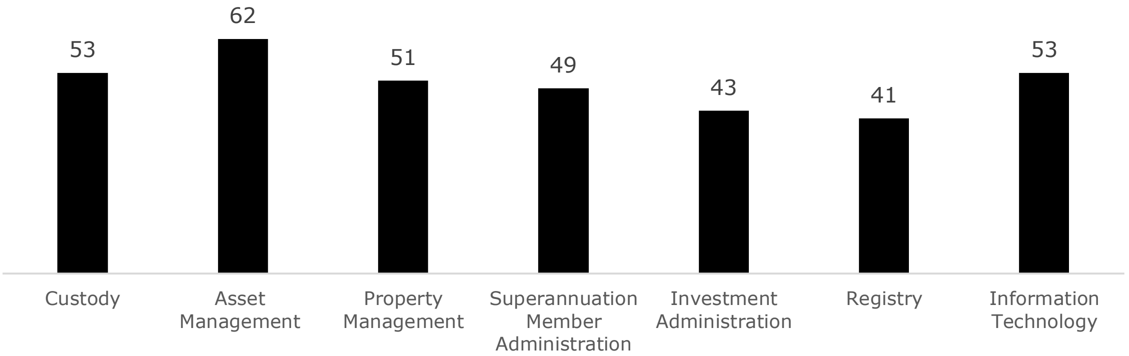
Key question:

- If you are a service provider, are you doing what you can to help your clients meet their deadlines?

Average Days Elapsed Overall by Year



Average days elapsed after balance date per sector



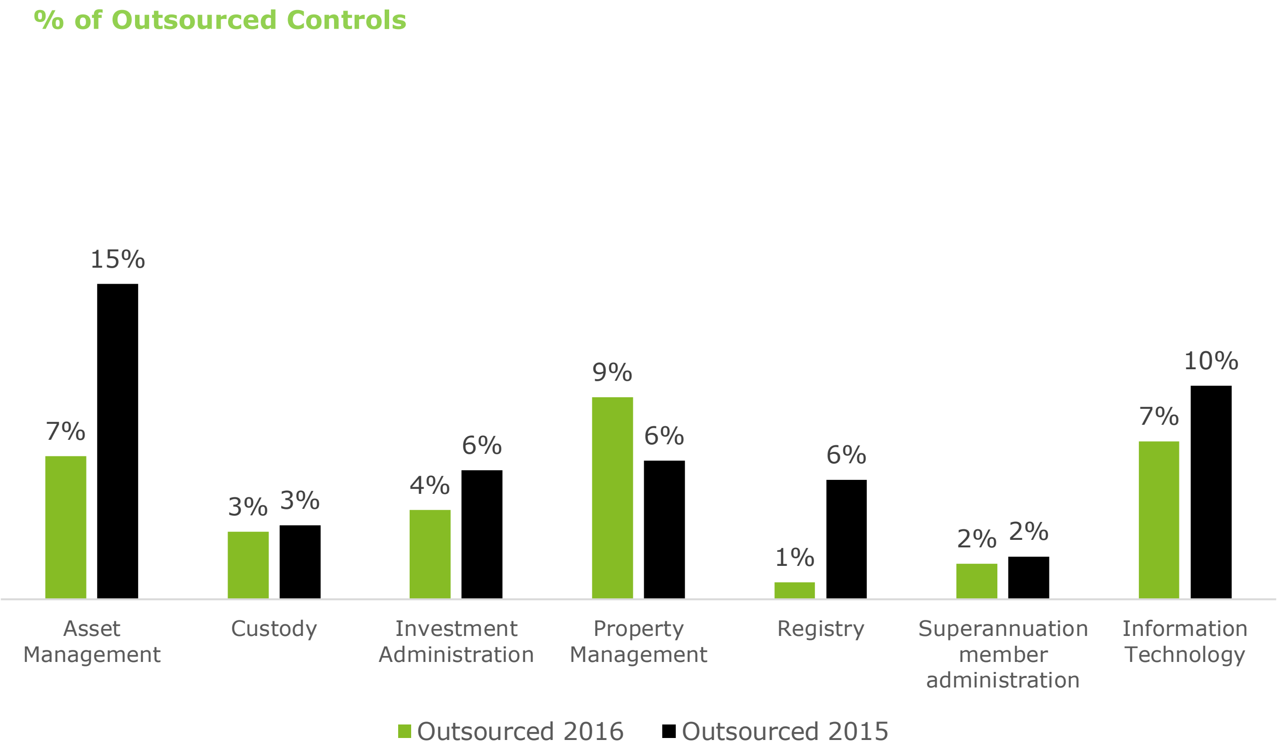
Outsourced Controls

In 2016, the number of outsourced controls were highest in the Property Management sector.

With exception of Property Management, outsourced controls have decreased in comparison with 2015.

This trend may be of concern to user organisations who are increasingly expecting greater control over third party monitoring activities.

.



Split between Automated/Manual Controls, Detective/Preventative Controls

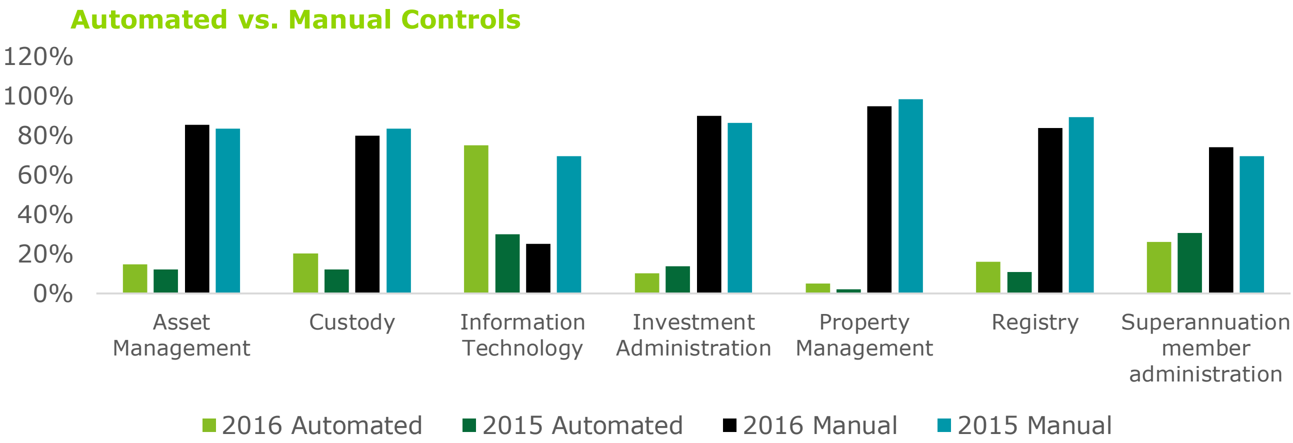
Automated vs Manual Controls

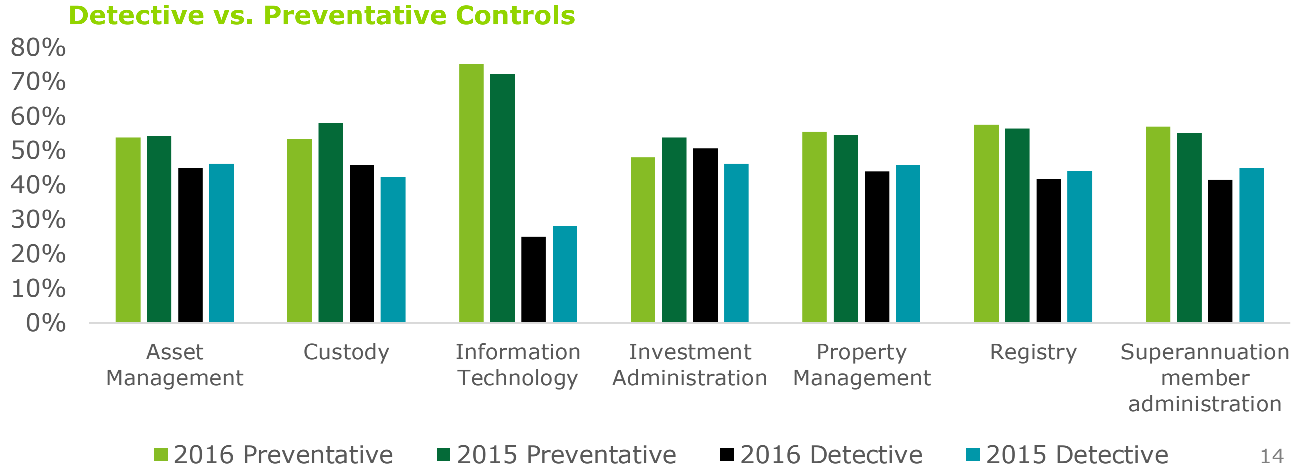
Across all sectors, except information Technology, manual controls were more prominent than automated controls. The Property Management sector showed a very large proportion (95%) of manual controls compared to the most automated areas. Information technology has invested in automation increasing to 75% compared against 30% last year.

Preventative vs Detective Controls

We saw a relatively consistent split and, pleasingly, a marginally higher proportion of preventative controls than detective controls. Information Technology (75%) had the high proportion of preventative controls.

The graph shows that there is still a reliance on people to, manually, prevent issues.





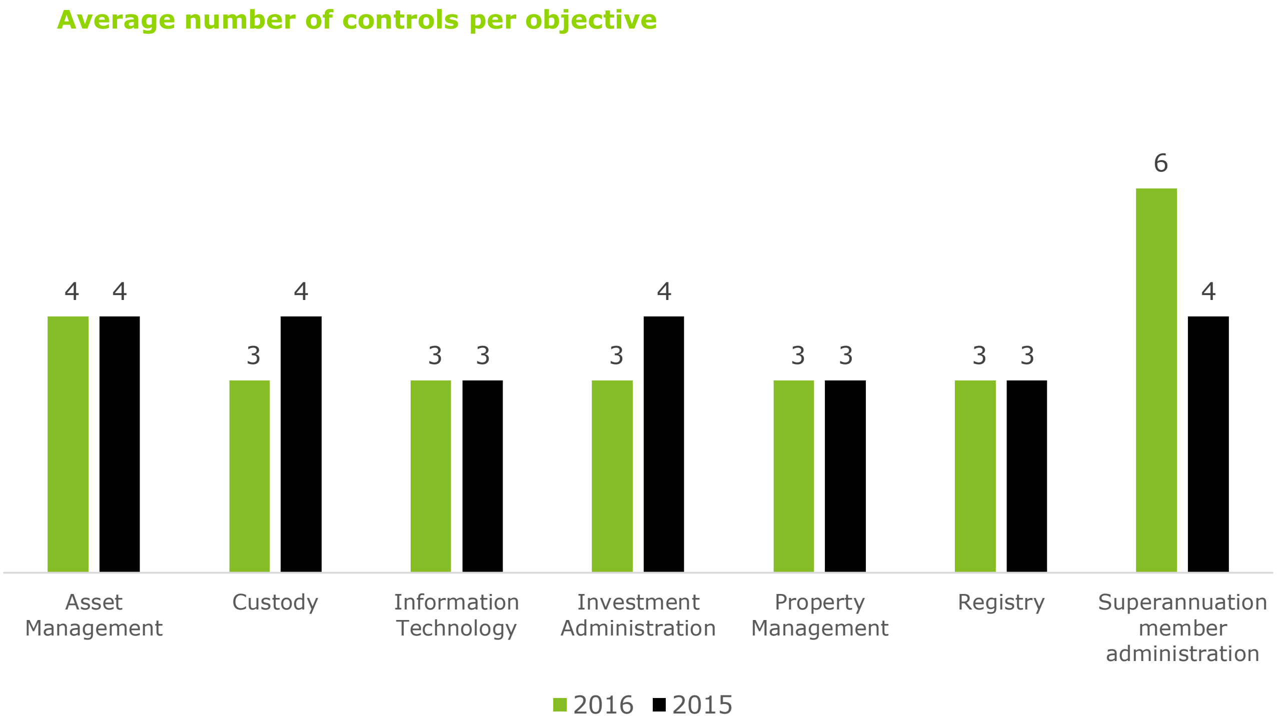
Number of controls per control objective

The number of controls listed for each control objective varies between 1 and 11 across each sector, with the average representing 3-6 controls. We are regularly asked what is the 'right' number of controls. Of course there is no 'right' answer and this analysis is intended to help you benchmark your reports against the average for each sector.

We found that Superannuation Member Administration had the largest average number of controls per objective, whilst Property Management, Registry and Information Technology had the lowest average number of controls per objective.

Key question:

- How does your organisation's control compare?



Technical update

Update to auditing standards impacting controls reports

Adopting SSAE 18 for SOC 1 reports

In April 2016, the American Auditing Standards Board issued SSAE No. 18, Attestation Standards: Clarification and Recodification, which seeks to clarify the requirements and provide application guidance for performing and reporting on examinations, reviews, and agreed-upon procedure engagements.

The updated attestation standards emphasise the requirement for service organisations to **understand, consider, and demonstrate oversight of service providers** they use that are relevant to a user entity's financial reporting

Monitoring the effectiveness of controls at subservice organizations

The service organization's description of the system and scope of services should include controls performed by management to monitor the effectiveness of controls at the subservice organizations, e.g. reviewing and reconciling outputs reports, periodic meetings, site visits, monitoring of external communication and customer complaints relevant to the service organisation. Service auditor's test procedures will test effectiveness of such controls.

Identifying complementary subservice organization controls

SSAE 18 introduces the concept of Complementary Subservice Organization Controls (CSOCs), which represents controls that management of the service organisation expects will be implemented by the subservice organisations and are necessary to achieve the controls objectives stated in management's description of the system, when the carve-out method of reporting has been used.

Similar considerations will be reflected in the written assertion by management and the management representation letter.

To meet this requirement we anticipate that the description of the system will include a sub-section for CSOSs.

Update to auditing standards impacting controls reports

Clarification of complementary user entity control considerations

The CUECCs should only include those controls and procedures that are relevant to achieve the control objectives within the service organisation's report.

Service organizations could consider including a mapping of the CUECCs to the control objectives as a leading practice.

Evaluating reliability of information produced by the service organization

The auditor needs to establish accuracy, completeness and reliability of information received during the examination, e.g. population lists, exception reports, user access lists.

Assessing the risk of material misstatement

The service auditor need to consider risks and likely sources of misstatement , including those related to fraud. Therefore, it will be necessary to obtain internal audit and regulatory reports and work with management to understand the likelihood of material misstatement to design and perform procedures whose nature, timing, and extent are based on and responsive to the assessed level of risk of material misstatement.

Changes are effective for service auditors' reports dated on or after May 1, 2017. Early adoption is permitted.

These changes will be applicable to service auditor reports currently issued under SSAE 16 and reports issued under both **SSAE 16** and **ISAE 3402** standards.

Contact us

INSIGHTS AND PERSPECTIVES

DETAILED ANALYSIS

TECHNICAL UPDATE

CONTACT US

APPENDIX A

Contact our third party assurance specialist team

James Oliver (National Lead)

Partner

Financial Services – Third Party Assurance Specialist
Tel: +61 (0) 3 9671 7969
Email: joliver@deloitte.com.au

Vincent Sita (Sydney)

Director

Financial Services – Third Party Assurance Specialist
Tel: +61 (0) 2 9322 5919
Email: visita@deloitte.com.au

Kevin Nevrous (Melbourne)

Partner

Technology RIsk
Tel: +61 (0) 3 9671 7745
Email: knevrous@deloitte.com.au

Appendix A

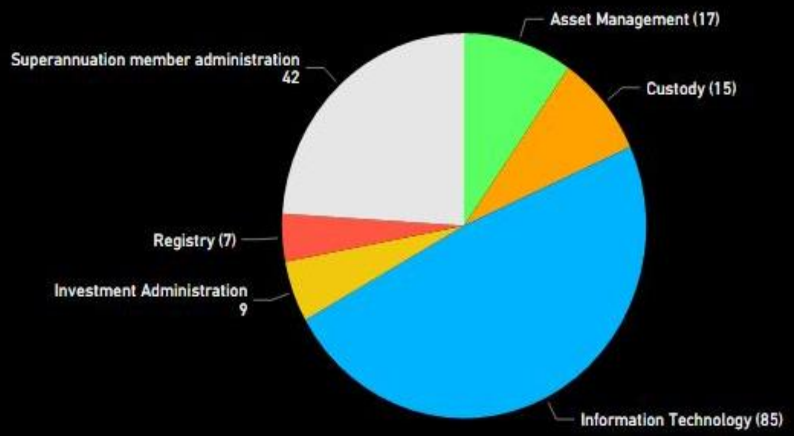
Industry Snapshots

Overall Results

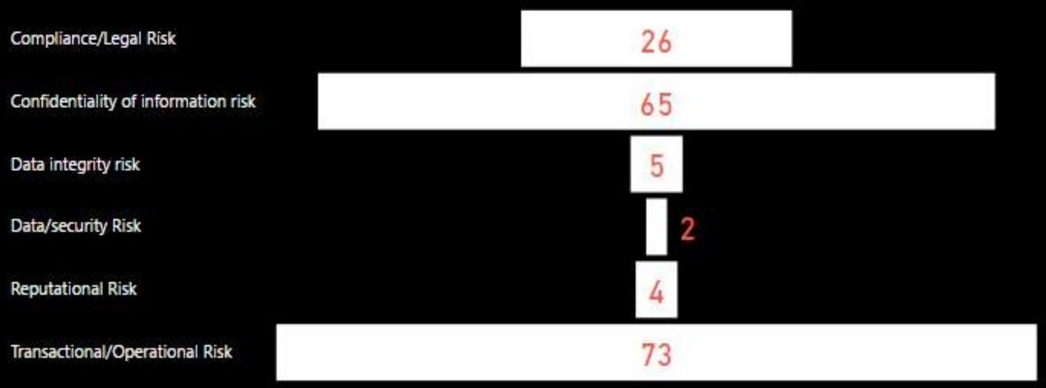
Total Number of Deviations

175

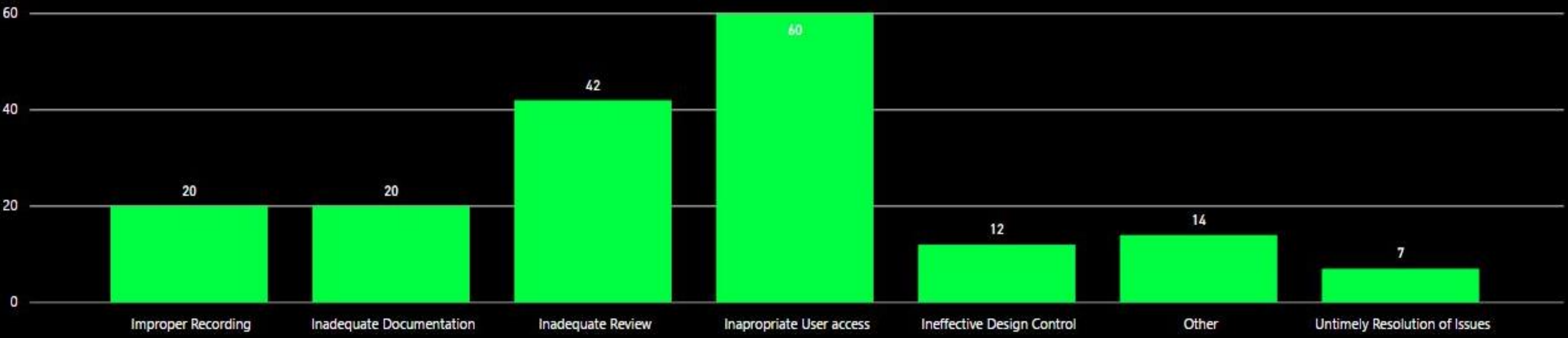
Deviations & Associated Risks



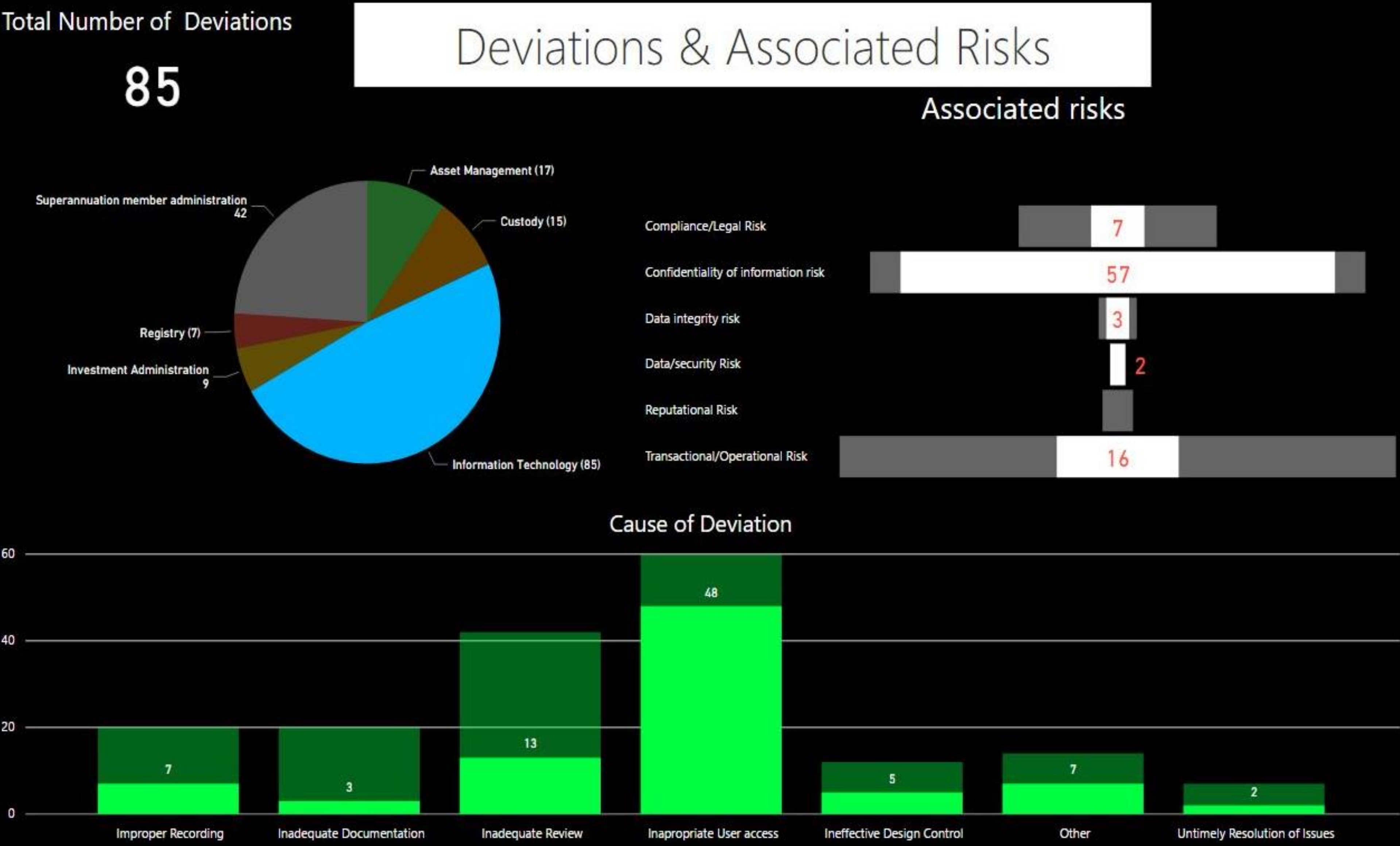
Associated risks



Cause of Deviation



Information Technology



Total Number of Deviations

85

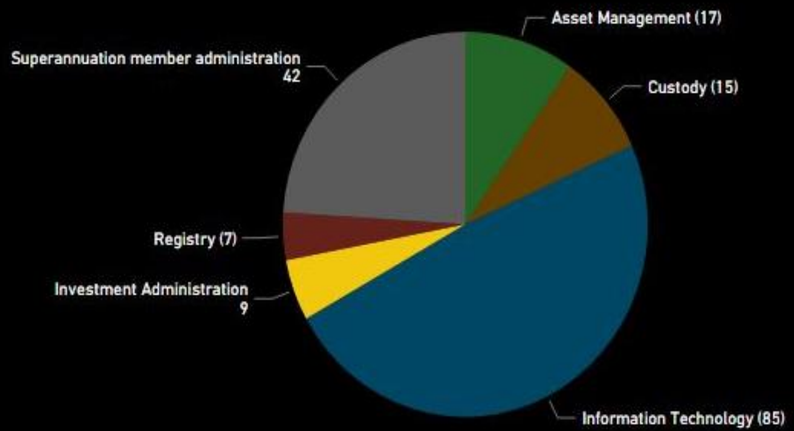
Deviations & Associated Risks

Investment Administration

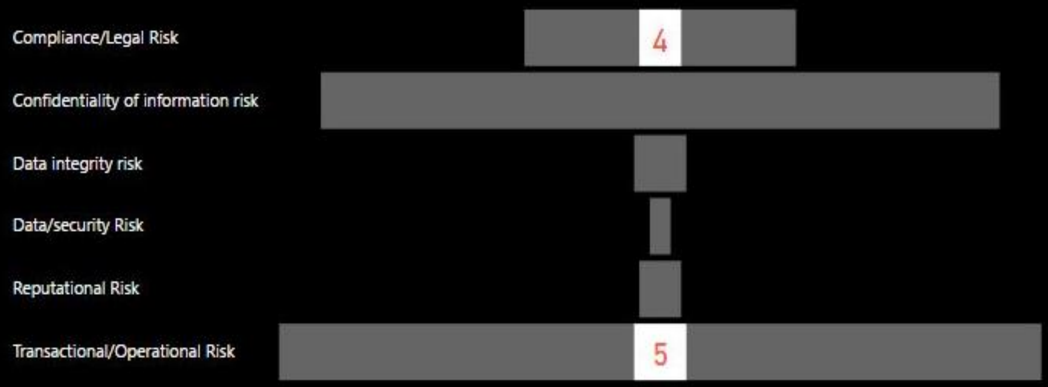
Total Number of Deviations

9

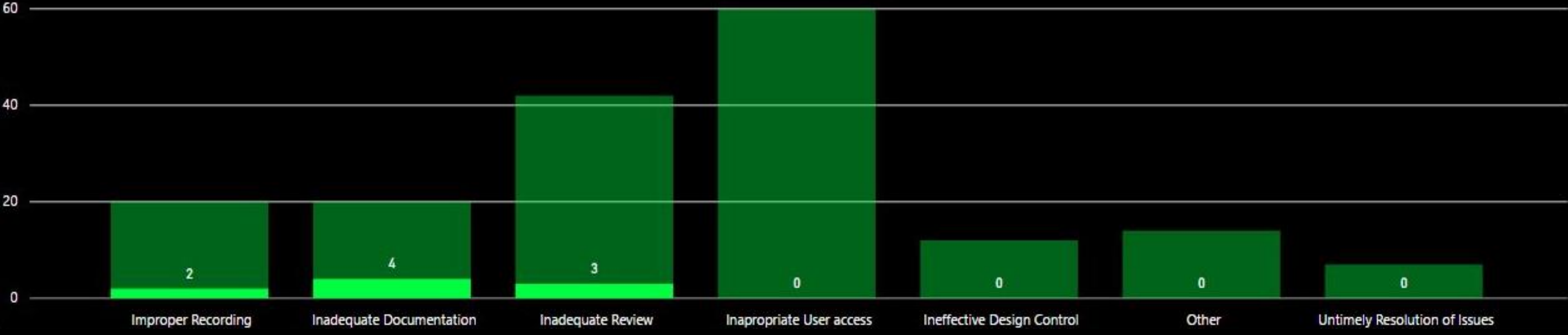
Deviations & Associated Risks



Associated risks



Cause of Deviation

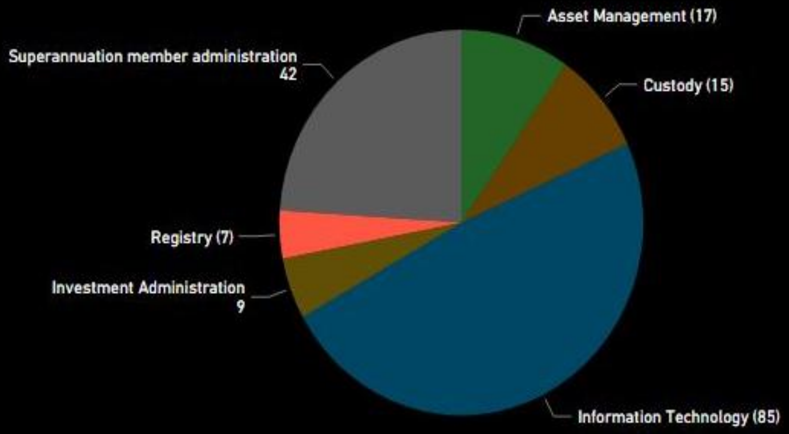


Registry

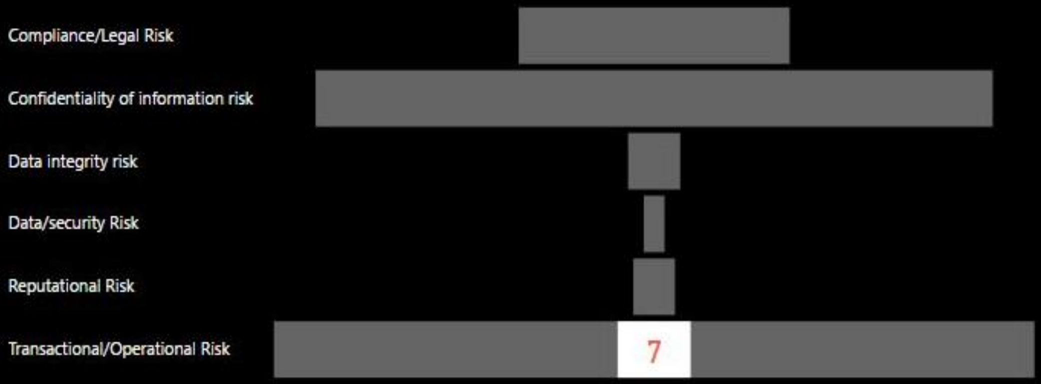
Total Number of Deviations

7

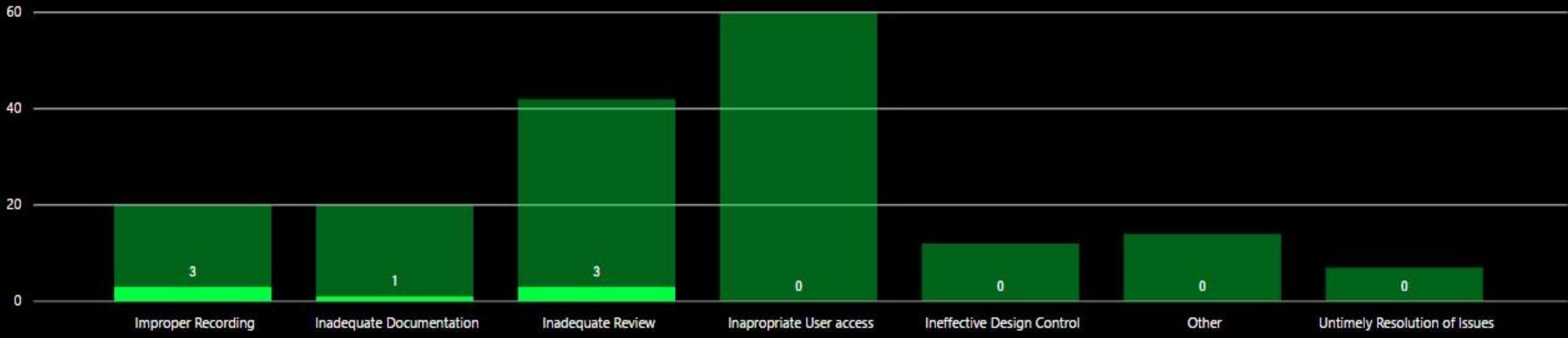
Deviations & Associated Risks



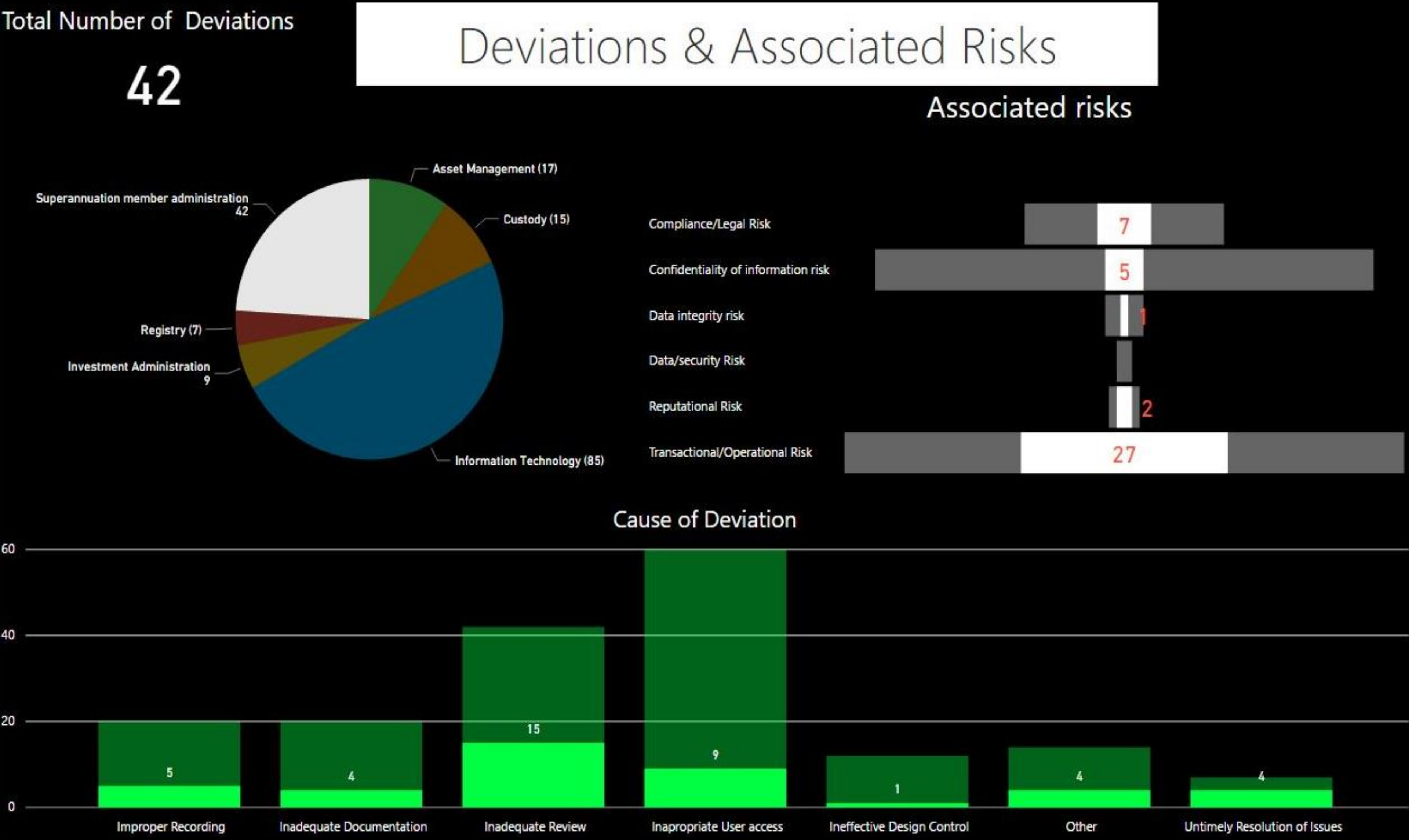
Associated risks



Cause of Deviation



Superannuation Member Administration



Total Number of Deviations

42

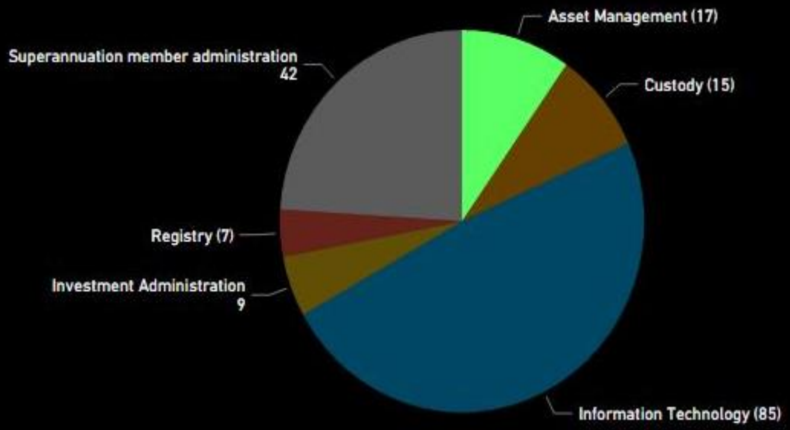
Deviations & Associated Risks

Asset Management

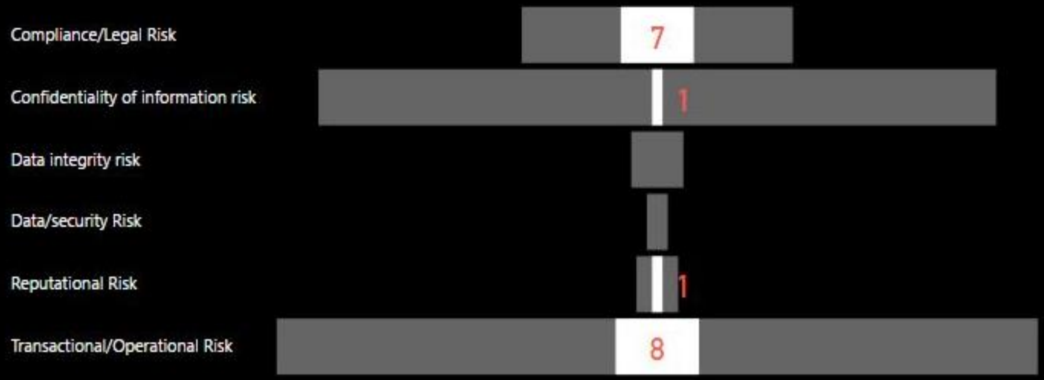
Total Number of Deviations

17

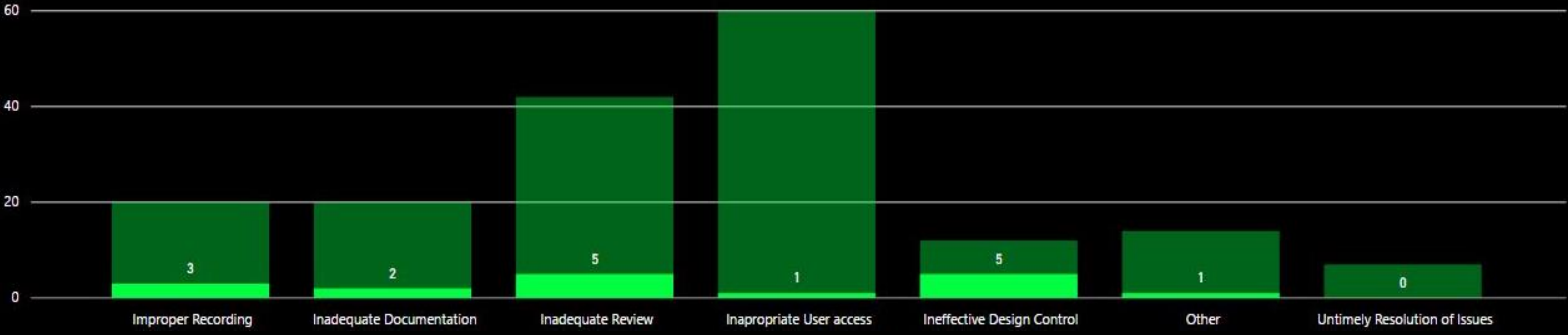
Deviations & Associated Risks



Associated risks



Cause of Deviation

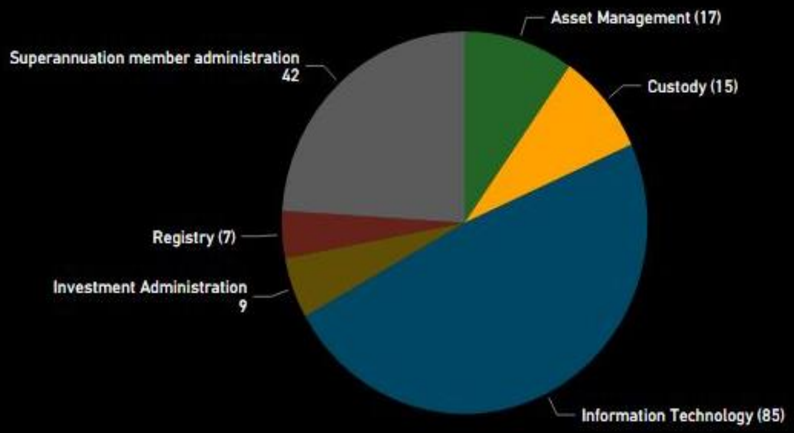


Custody

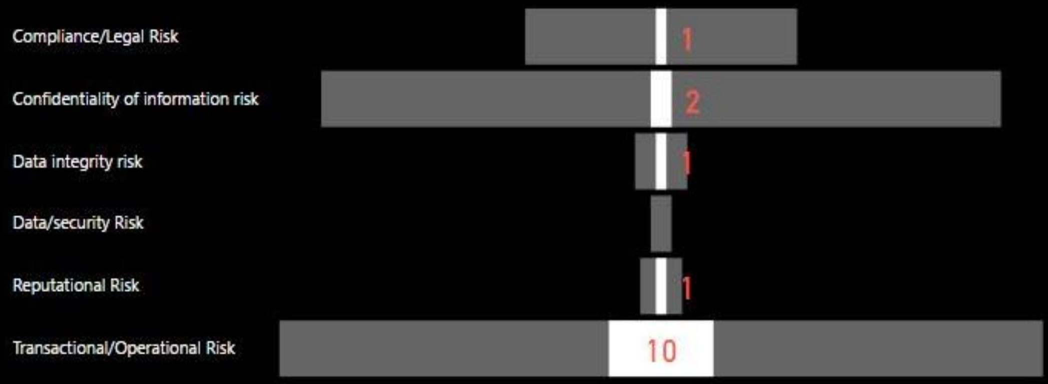
Total Number of Deviations

15

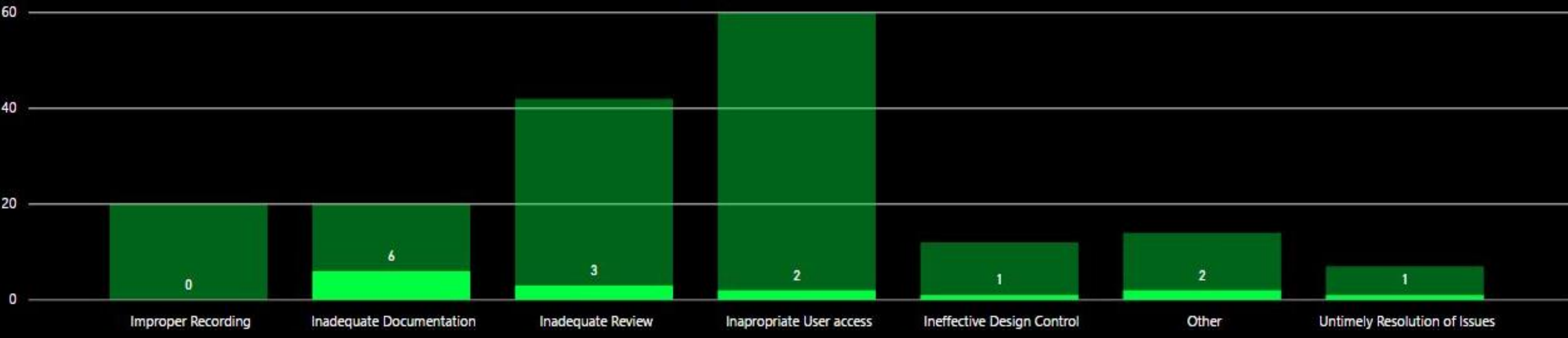
Deviations & Associated Risks



Associated risks



Cause of Deviation



Deloitte.

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively the "Deloitte Network") is, by means of this publication, rendering professional advice or services.

Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/au/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte's approximately 195,000 professionals are committed to becoming the standard of excellence.

About Deloitte Australia

In Australia, the member firm is the Australian partnership of Deloitte Touche Tohmatsu. As one of Australia's leading professional services firms, Deloitte Touche Tohmatsu and its affiliates provide audit, tax, consulting, and financial advisory services through approximately 6,000 people across the country. Focused on the creation of value and growth, and known as an employer of choice for innovative human resources programs, we are dedicated to helping our clients and our people excel. For more information, please visit Deloitte's web site at www.deloitte.com.au.

Liability limited by a scheme approved under Professional Standards Legislation.

Member of Deloitte Touche Tohmatsu Limited