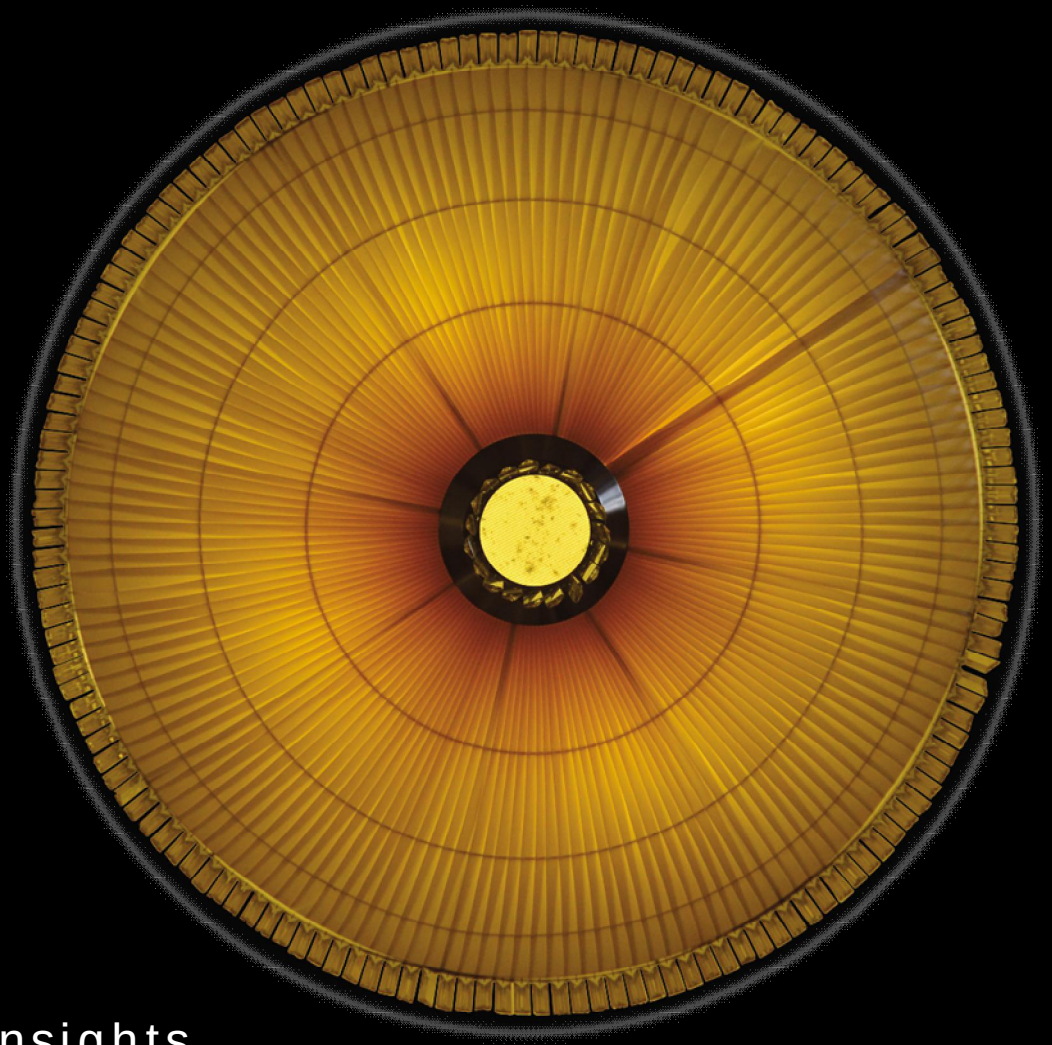
Deloitte.



Third Party Insights

7th Annual Edition, including 2016 Third Party Assurance Report Benchmarking

May 2017

Introduction and context

Deloitte has been performing an annual benchmarking survey of third party control assurance reports issued in Australia for seven years. To the best of our knowledge, it is the leading survey of this nature in the market.

Our 2016 benchmarking analysis covers ~50 third party control assurance reports and includes an assessment of the nature of underlying controls and the root causes for deviations in controls.

The findings 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, and this report provides 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 its extended enterprise.

Executive Summary
Insights and Perspectives

#1 - Qualified opinions in control reports more than doubled compared to previous years

Deloitte's Perspective

Consider how effective your control design and assurance process is, and the level of preventative controls in place.

Do your control assurance activities help drive (and/or start) the conversation about issues such as risk culture, cyber risk and conduct that may arise from third party services?

- The number of qualified reports in 2016 increased to 7% (compared to the 'normative; 2%-3% of previous years), with control deviations increasing slightly on the previous year
- Qualifications related to a range of issues, such as:
  - Ineffective control design and inadequate reviews;
  - Compliance and data integrity; and
  - Inappropriate user access.
- Contributory factors to the increased control deviations included greater client awareness of controls (in part, due to rising regulatory expectations) and continuing scrutiny by auditors
- Some users of these reports questioned whether it was timely to revise the purpose and scope of the reports, and use them to drive continuous improvement by:
  - Broadening and/or deepening assurance activities in specific areas such as cyber security, unit pricing and third party monitoring;
  - Adding enterprise-wide risk aspects such as, compliance culture, conduct and governance.
- There is continuing (and high) reliance on manual (vs. automated) controls, indicating the complexity and/or cost to implement automated controls
- Contrary to previous years, the survey shows that organisations have been investing in preventative controls as an option to manage risk in a cost-effective manner.

#2 - Within an increasingly pervasive, complex and business-critical third party landscape, control reports provide only one lens of assurance

Deloitte's Perspective

Consider how effective and fit-for-purpose your third party management process is – across critical dimensions such as due diligence, monitoring, accountability, risk and governance.

Have you got an enterprise wide view, in addition to a service-level, business unit view – to target areas to strengthen your control environment in a cost-effective manner?

Sharpening regulatory requirements, and an increase in third party failures (with customer and reputation impact), Management and Boards are taking actions to strengthen their third party management processes, such as:

- Developing an enterprise wide view of their third party landscape
- Appointing an executive sponsor to champion change activities and drive a common set of third party standards business guidelines
- Assessing and improving their due diligence, monitoring and governance approach
- Targeting value creation opportunities with third parties, such as new innovations, technology, operational efficiency and cost reductions.

#3 – Cyber security is in the spotlight, with an APRA survey on cyber security incidents identifying many areas for improvement

Deloitte's Perspective

Cyber-security is a topical threat, with increasing cyber-attacks on business and government.

It's impact is far reaching – service disruption, brand reputational damage, financial costs and loss of confidence by customers and the market.

How focused and organised are your cyber security controls relating to third party services?

- Governance: Ensure Management and the Board 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 sources 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.

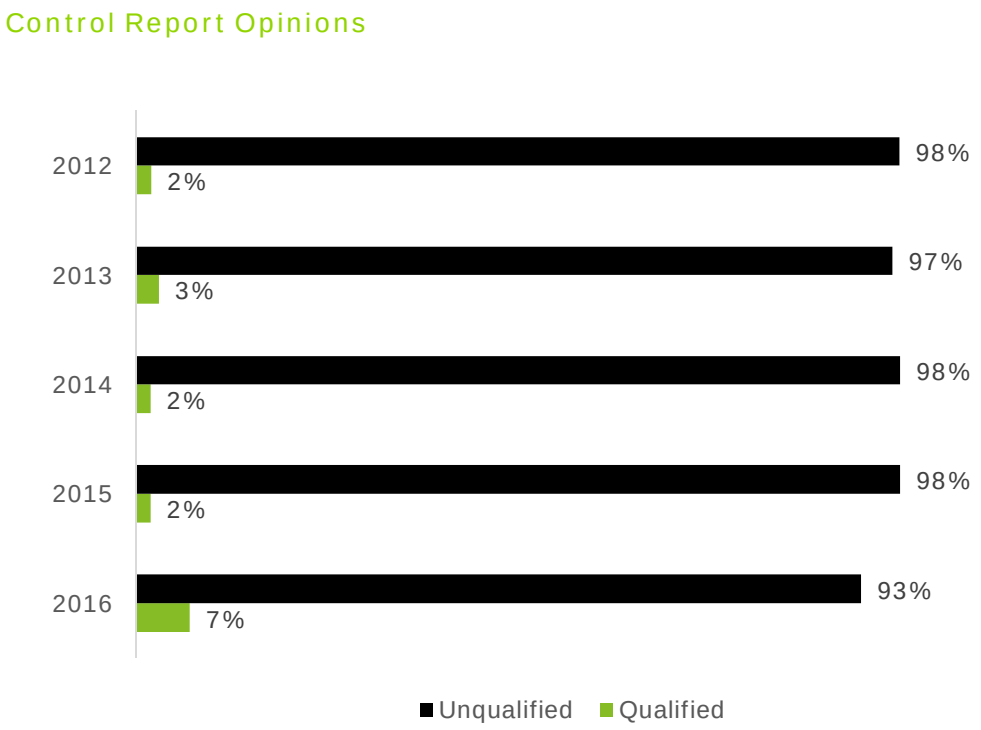
Detailed Benchmarking Analysis

1. Qualifications more than doubled compared to previous years

The percentage of qualified opinions has increased to 7% compared with the 'norm' 2-3% in previous years.

These were caused by ineffective control design, poor user access, inadequate review, compromising compliance and data integrity issues.

The increased rate of qualifications and deviations are also a consequence of client and regulator expectations rising, leading to higher auditor scrutiny.



2. Deviations went up slightly, and were mapped to specific risk categories*

In 2016, deviations 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?

** See next page, and (for details by sector), refer to Appendix A.*

3. Operational risk and data management risk were most frequently associated with control deviations

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

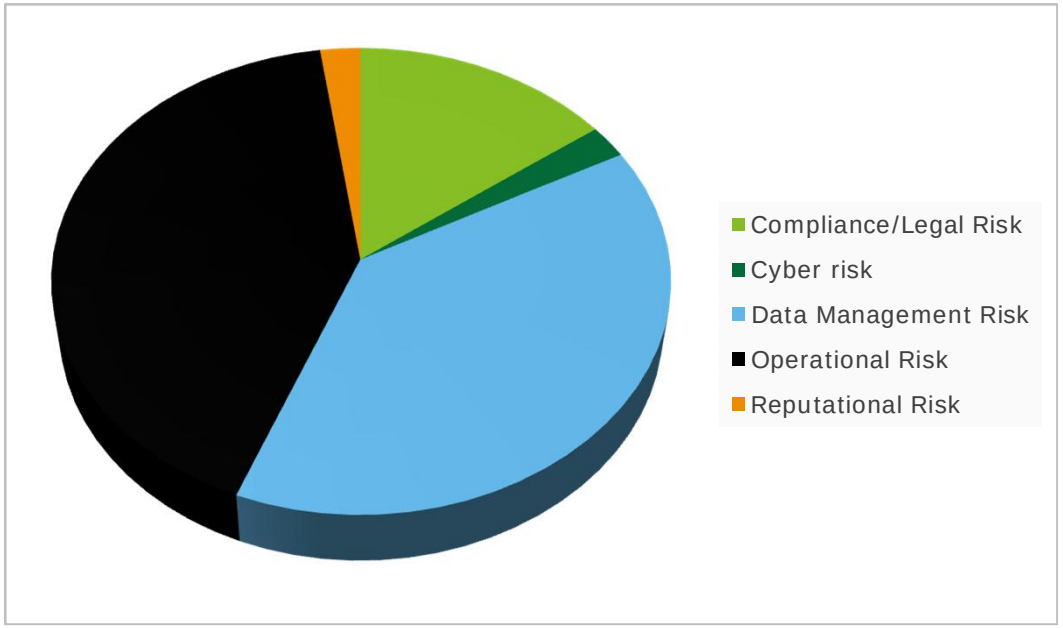
Data Management Risk
Third party lacks the necessary infrastructure, policies, or procedures to protect information and intellectual property from unauthorised access, modification, destruction, disclosure or misuse, potentially resulting in financial and reputational loss or legal or regulatory action.

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 detailed analysis by sector, refer to Appendix A.

4. Timeliness of reporting deteriorated, with average days to issue an opinion increasing to 53 days (from 47 days in 2015)

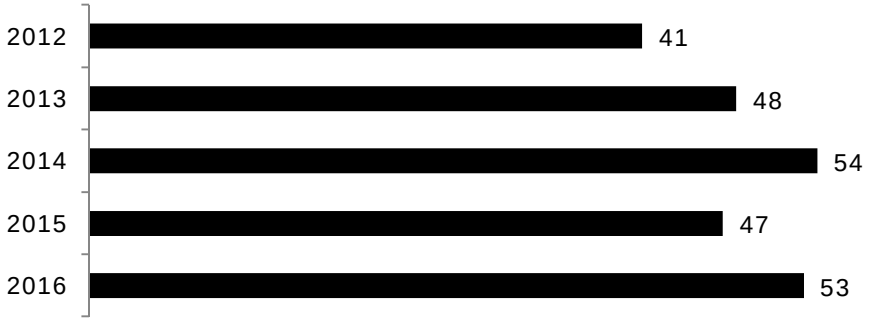
Time to report ranged from 41 days (the Registry sector) to 62 days (Asset Management sector)

There was one significant outlier contributing to the delay noted for Asset Management issuance; excluding this would bring the days to issuance in line with other sectors to 54 days.

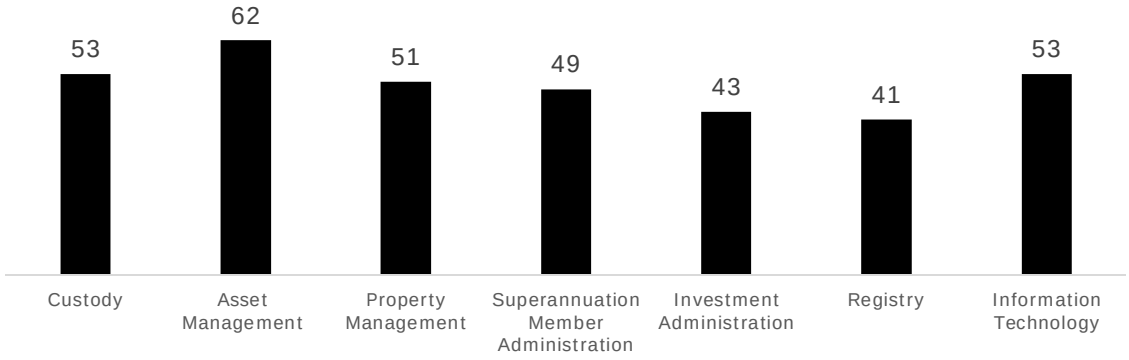
Key question:

- 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



5. Manual controls continue to be significantly higher than automated (outside of the IT category), suggesting a preference for ‘people & process’ over the perceived ‘cost-of-automation’

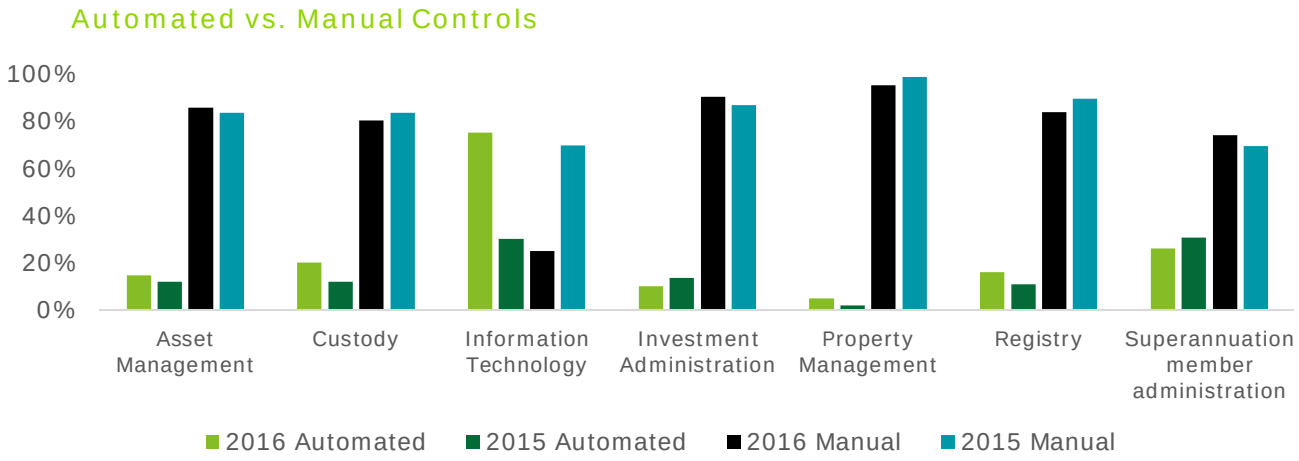
Automated vs Manual Controls

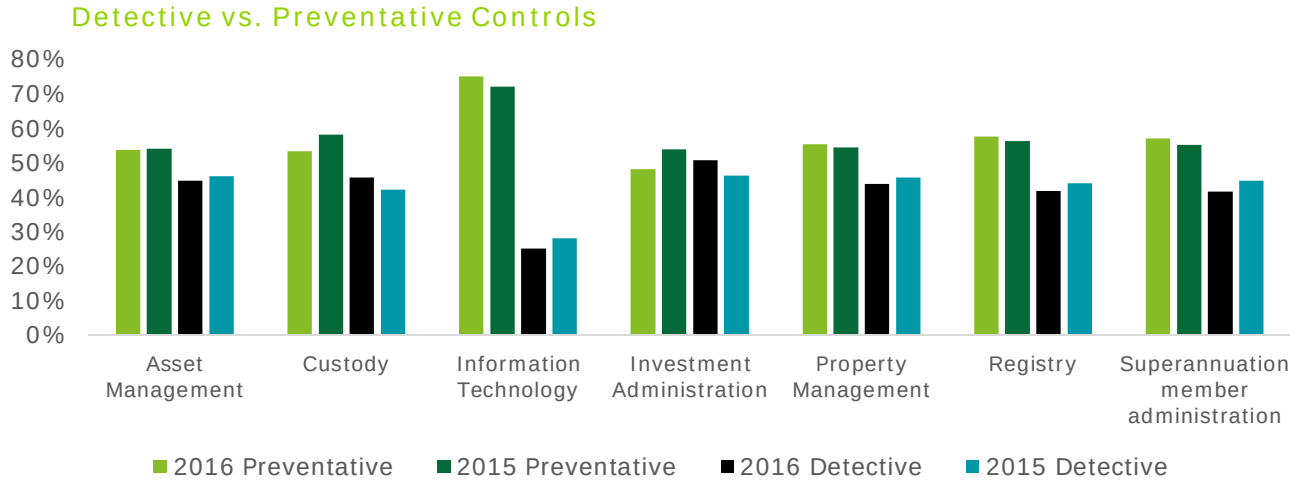
Across all sectors, except information Technology, manual controls were more prominent than automated controls. The Property Management sector showed a very large proportion (95%) of manual controls compared to the most automated areas. Information technology has invested in automation increasing to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





6. There were 3-6 controls per objective on average

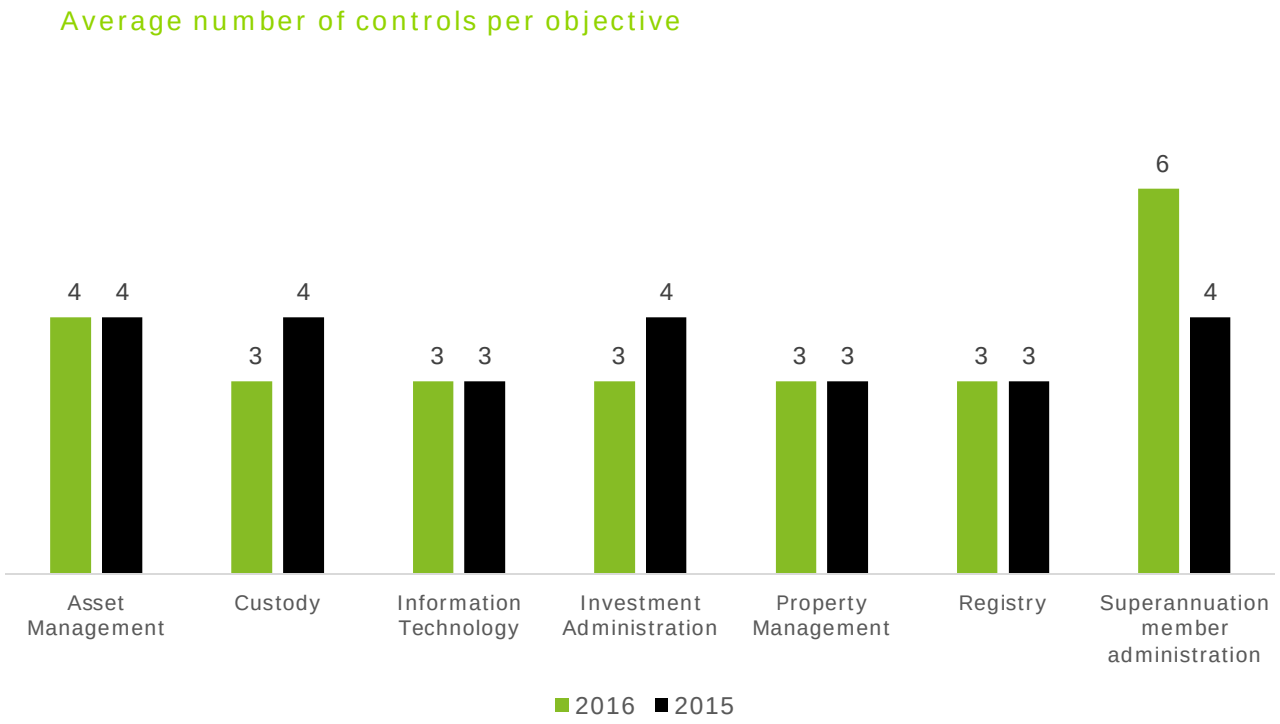
The number of controls listed for each control objective varies between 1 and 11 across each sector, with the average representing 3-6 controls.

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.

Key question:

- Are the number and nature of controls in your organisation appropriate for the risks emerging from your third-party landscape?



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 organisations

The service organisation's description of the system and scope of services should include controls performed by management to monitor the effectiveness of controls at the subservice organisations, 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 organisation controls

SSAE 18 introduces the concept of Complementary Subservice Organisation 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 organisations could consider including a mapping of the CUECCs to the control objectives as a leading practice.

Evaluating reliability of information produced by the service organisation

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

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

Ally MacLeod (Technology Partner)

Partner

Risk Advisory – Technology Specialist
Tel: +61 (0) 2 9322 5369
Email: amacleod@deloitte.com.au

Vincent Sita (Sydney)

Director

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

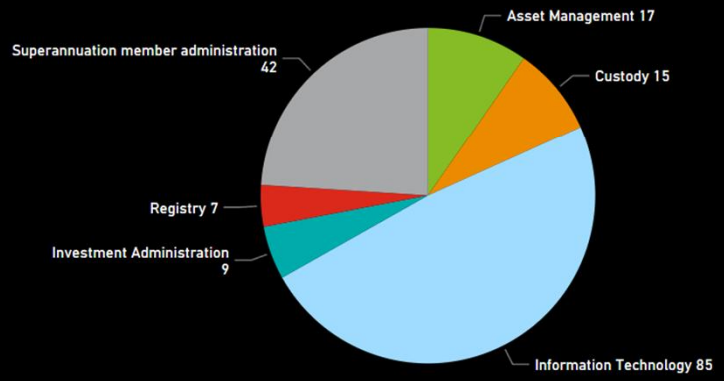
Appendix A
Industry Snapshots

Overall Results

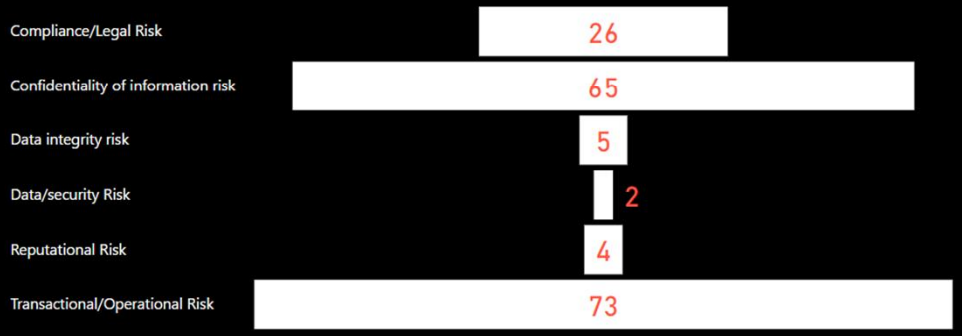
Total Number of Deviations

175

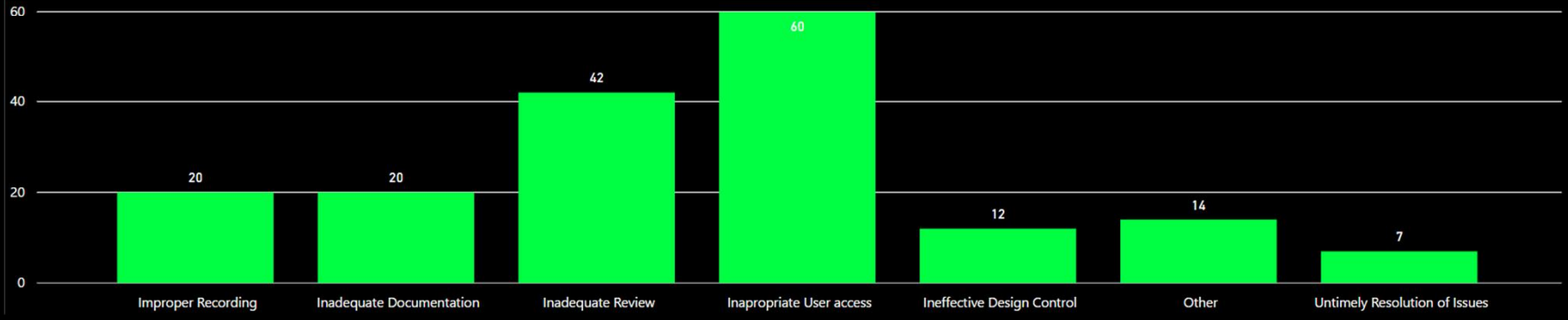
Deviations & Associated Risks



Associated risks



Cause of Deviation

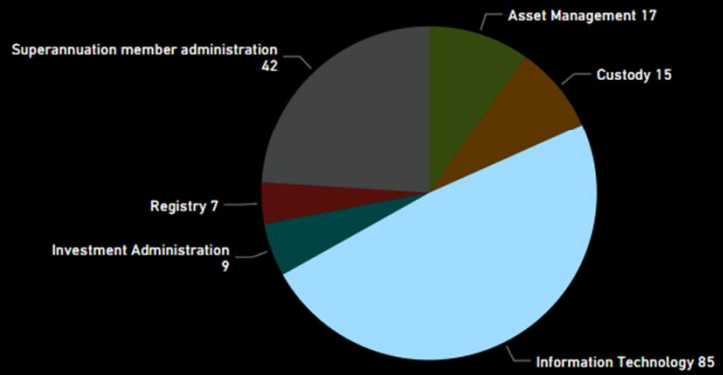


Information Technology

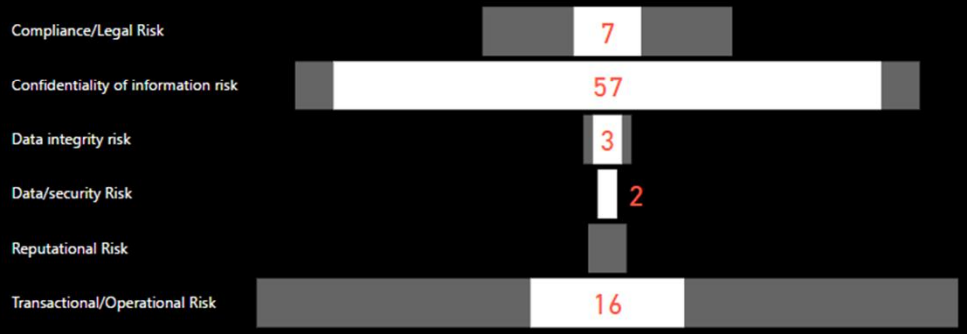
Total Number of Deviations

85

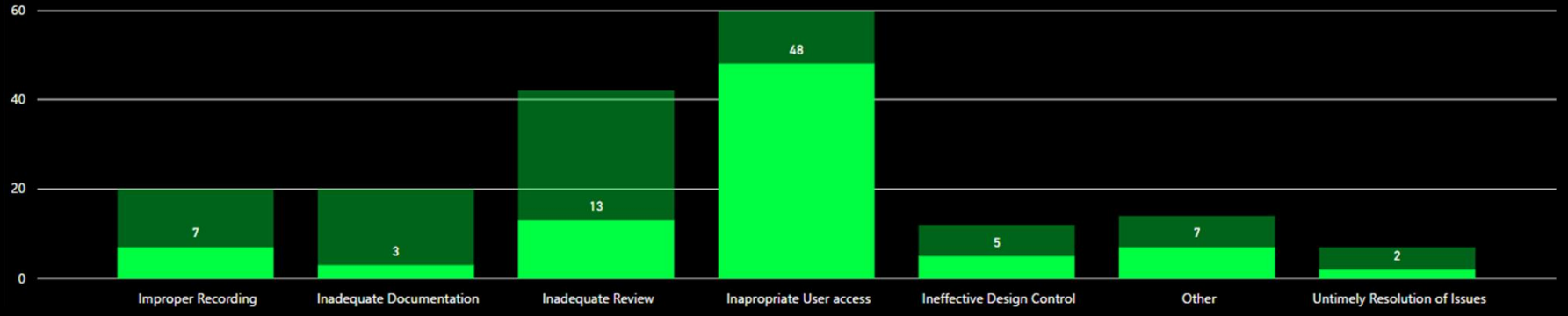
Deviations & Associated Risks



Associated risks



Cause of Deviation

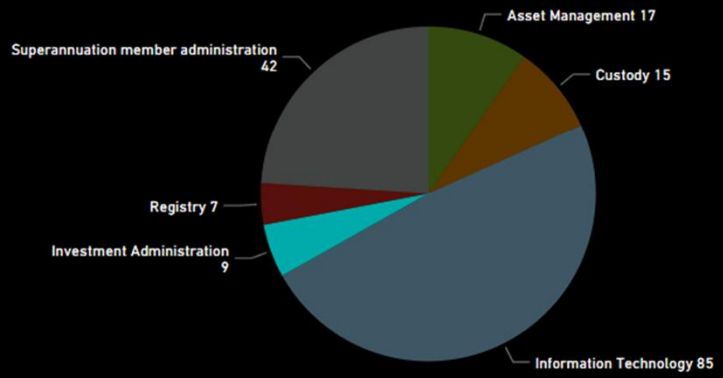


Investment Administration

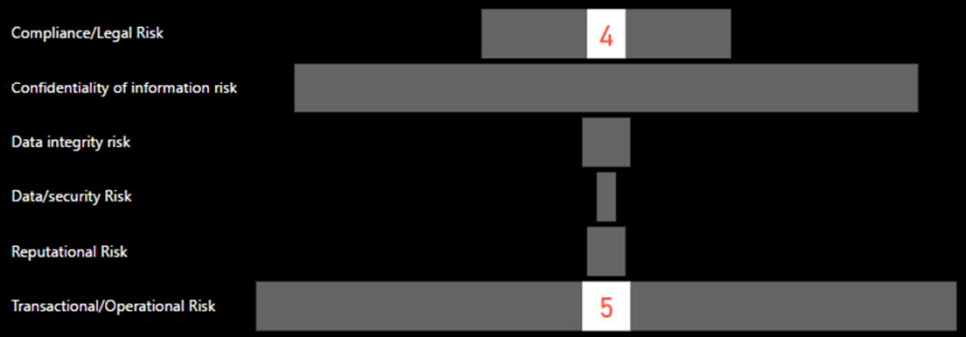
Total Number of Deviations

9

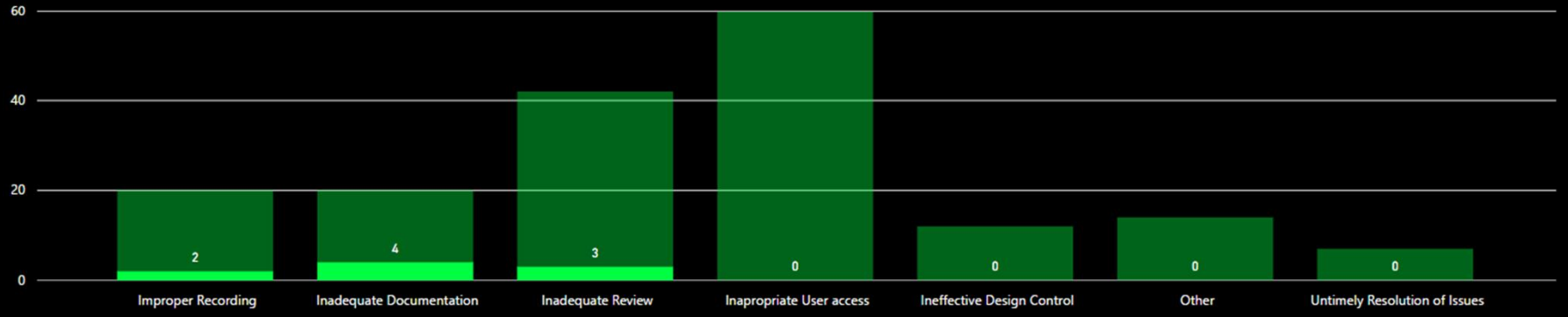
Deviations & Associated Risks



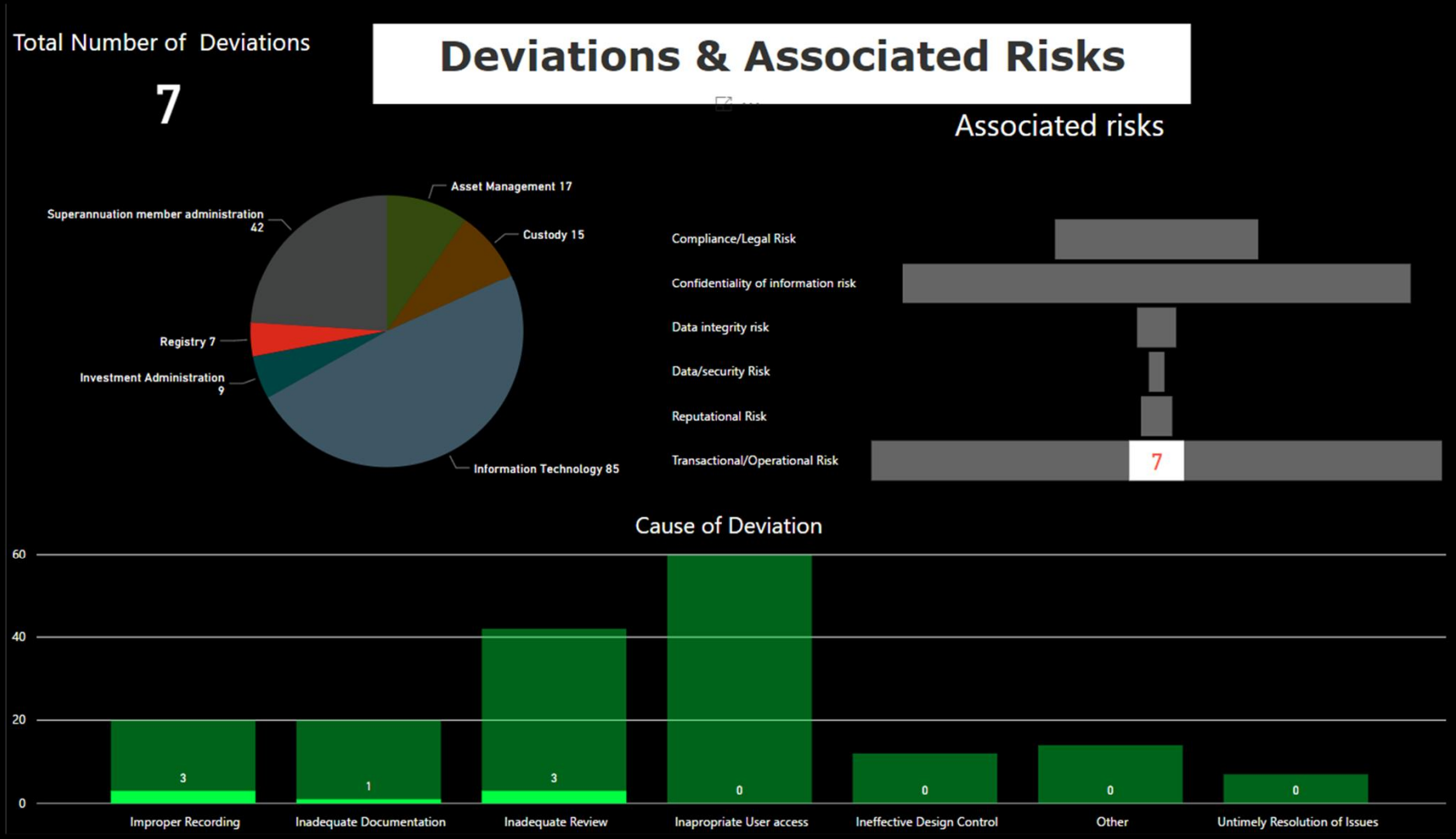
Associated risks



Cause of Deviation



Registry

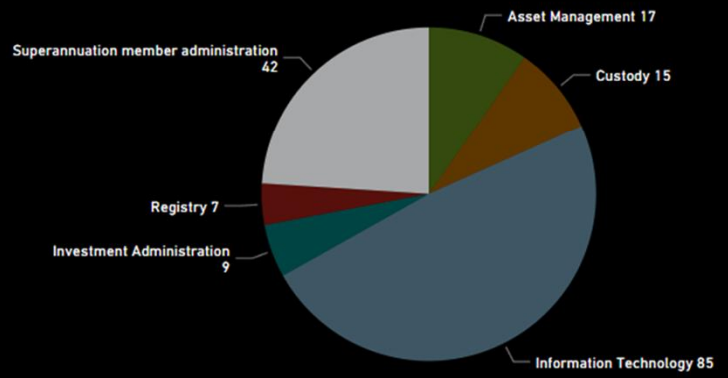


Superannuation Member Administration

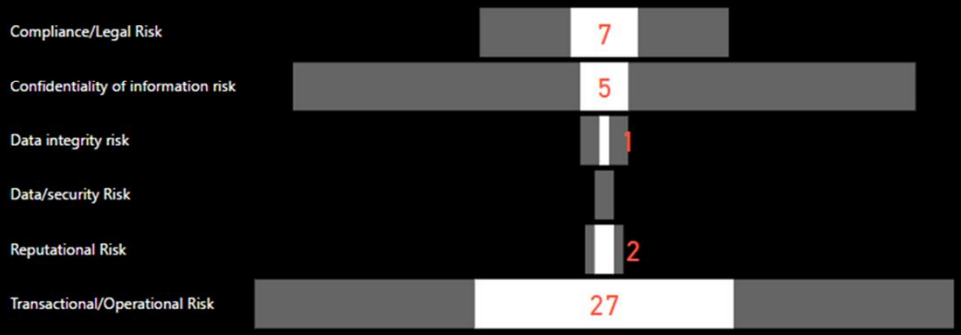
Total Number of Deviations

42

Deviations & Associated Risks



Associated risks



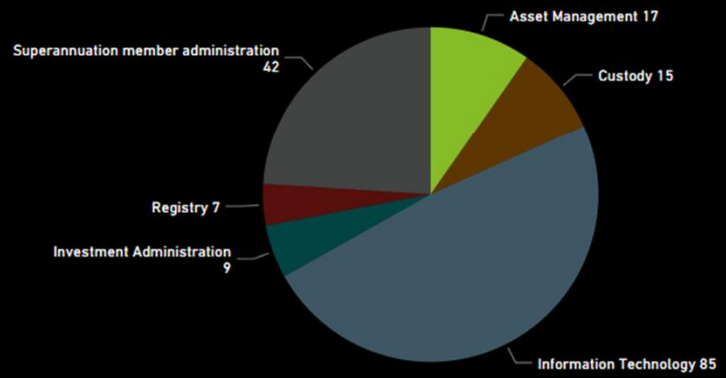
Cause of Deviation

Asset Management

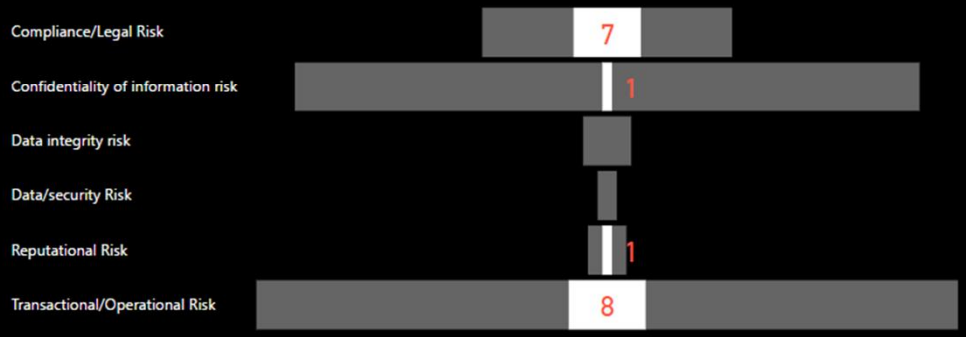
Total Number of Deviations

17

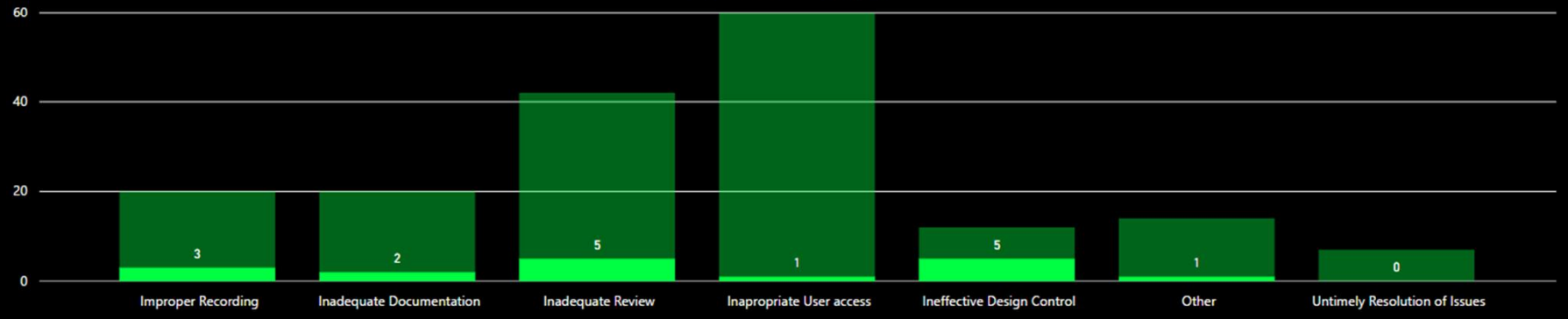
Deviations & Associated Risks



Associated risks



Cause of Deviation

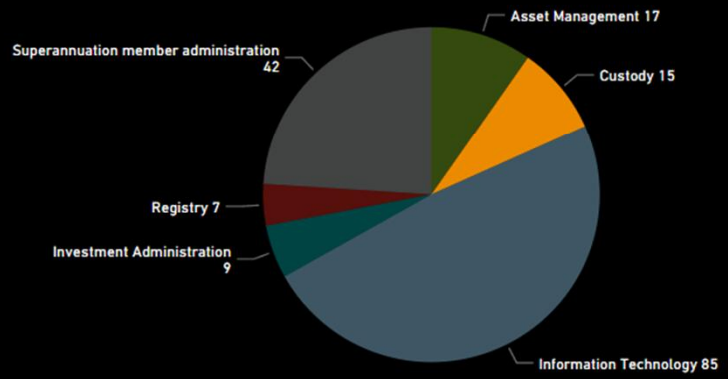


Custody

Total Number of Deviations

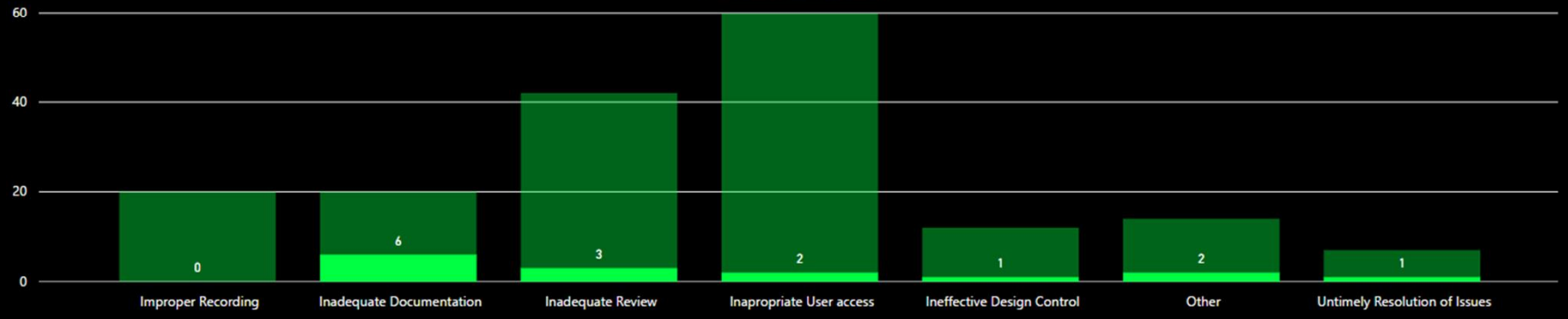
15

Deviations & Associated Risks



Associated risks

Cause of Deviation



Deloitte.