Deloitte.

Third Party Assurance

Insights and Benchmarking of 2017 and 2018 Third Party Control Reports

November 2018

Foreword

Welcome to our 2017 and 2018 Third Party Assurance Benchmarking and Insights report. In this report, we provide a summary of the results from over 47 organisations in Australia on the key issues and trends impacting their approach to managing and mitigating third party risk.

The results indicate that Third Party Risks are maturing in many organisations, not just to enable better management and mitigation of risks but also show trends that management are beginning to understand and exploit the risks associated with their third and fourth parties.

We hope this report enables you to enhance your understanding and organisational positioning in relation to your peer group across a number of key risks that span across your third party service providers and also your peer group perspectives to assist you in strategic decision making around emerging issues and risks related to third party risk management.

★ Please contact a member of our team (refer to page 19) if you would like to have a more detailed discussion about the trends we are seeing and how this might relate to your organisation.

Executive Summary
Insights and Perspectives

Observations and trends in respect to our benchmarking analysis

Greater reliance on preventive and manual controls

- Conventional wisdom tells us that automated controls are better (effective and efficient) than manual controls. However, our benchmarking indicated that:
  - The reports surveyed indicated an overall **greater reliance on manual controls than on automated controls**.
  - This situation is driven by many factors. **It can be more complex and costly to implement automated controls**.
  - Similarly, preventative controls are regarded as being more effective and efficient than detective controls. Therefore, it is encouraging to see that **preventative controls were more common than detective controls**.
- As GS 007 reporting matures, Audit Committees are **challenging whether control objectives should be shaped to the entity in order to fairly describe its process and goals and drive continual improvement.**

Decline in deviations continues

- In 2017 and 2018, we observed 117 control deviation from the 47 surveyed reports with an average of about 2 deviations per report.
- Since our benchmarking analysis began in 2010, control deviations have continued a **declining trend**. This could be testament to the **improving control frameworks** operated by service providers generally.

Nature of deviations

- **Information Technology** continues to be the source of the majority of deviations.
- The nature of controls which failed were predominantly **manual and preventative**.
- The root causes for a majority of the deviations related to **inadequate monitoring and supervision.** This is consistent with previous year findings.

Themes arising from the Royal Commission into Misconduct, Superannuation, Banking and Financial Services Industry

The key themes arising from the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry identified organisations had inadequate monitoring and supervisions controls over third party service providers:

"Poor record-keeping of client files obstruct complaints, remediation, management assurance and risk controls."

"no supervision or monitoring to identify whether ongoing service obligations were being met."

"acting in "ethically unsound" ways that delayed remediation by negotiating with ASIC and advocating for an opt-in remediation or "fair value" approach to ultimately reduce the amount paid to members"

"deficiencies in monitoring and supervision standards and controls effectiveness.

"the Corporations Act and Superannuation Industry Act were breached with respect to plan service fees (PSF) and adviser service fees charged that rendered no services in return

"failed to have controls and risk management systems in place to turn off ongoing fees for members who may have left the funds and were no longer receiving services."

"There are some key risk management frameworks and processes that are either not operating as designed or require updating to ensure that they meet ASICs expectations and industry better practice."

"failed to prioritise the interests of the affected members over the interests of advisers contrary to the SIS Act"

Deloitte's Point of View

A key theme arising from the Royal Commission into Misconduct, Banking, Superannuation and Financial Services Industry, revealed 'execution gaps' resulting from the inability of supporting processes, controls and technology to monitor and supervise the organisations extended enterprise.

Going forward, organisations will need to focus on either implementing or refining their existing Third Party Risk Management frameworks to ensure it appropriately addresses the emerging risks and issues.

These findings resonate with the key findings we noted from our Global 2016 and 2017 Extended Enterprise Risk Management survey (Key findings have been summarised on the next slide).

https://financialservices.royalcommission.gov.au/public-hearings/Pages/transcripts.aspx

Global perspectives: What are other organisations saying?

Deloitte's 2016 and 2017 Global Extended Enterprise Risk Management survey reveals the following challenges facing organisations:

87% of respondents faced third party disruption incident(s) in the past year

74% of respondents believe third parties will play a highly important /critical role in the year ahead, vs. 60% a year ago

89% of respondents have low to moderate confidence in the quality of their Third Party Risk Management processes

From a typical clients point of view

I am not comfortable that I know all of my third/fourth parties and whether they have access to our network and critical data.

Chief Information Officer

I don't have confidence or transparency into whether my critical relationships are performing to the best of their ability?

Chief Operations Officer

I need a simple way to keep a pulse on my third parties, so I can react quickly to any issues impacting my operations in order to protect my brand.

Supply Chain Officer

Why does it take so long to on-board a third party and why do I have to complete all this paperwork?

Relationship owner

Are my third parties compliant with the various global industry regulations?

Chief Compliance Officer

I need to cut costs with managing my third party relationships.

Chief Procurement Officer

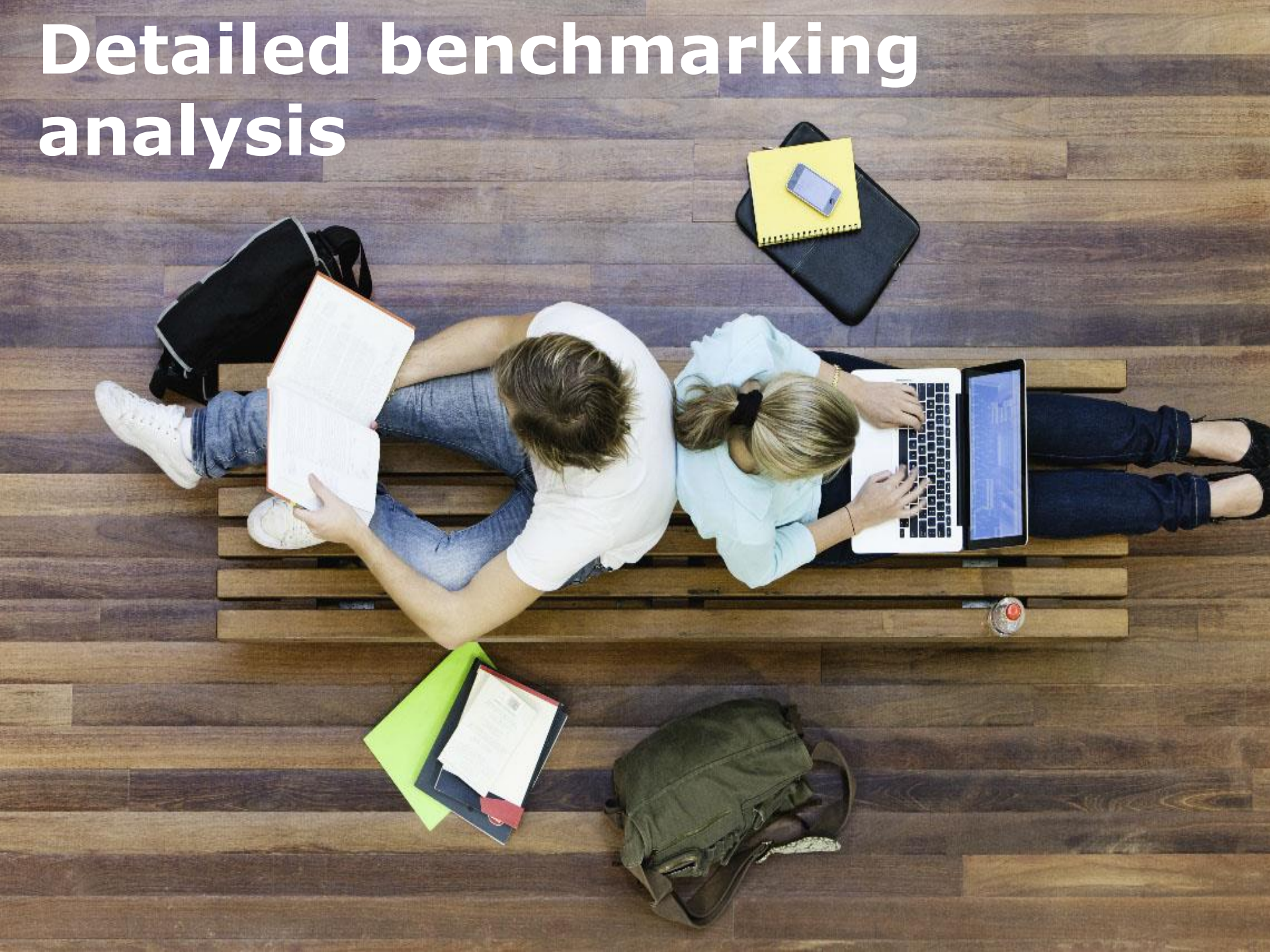
Board Member

Where do we use third parties and how could our reputation be harmed by them?

https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-extended-enterprise-risk-management.pdf

https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-EERM-survey-2016.pdf

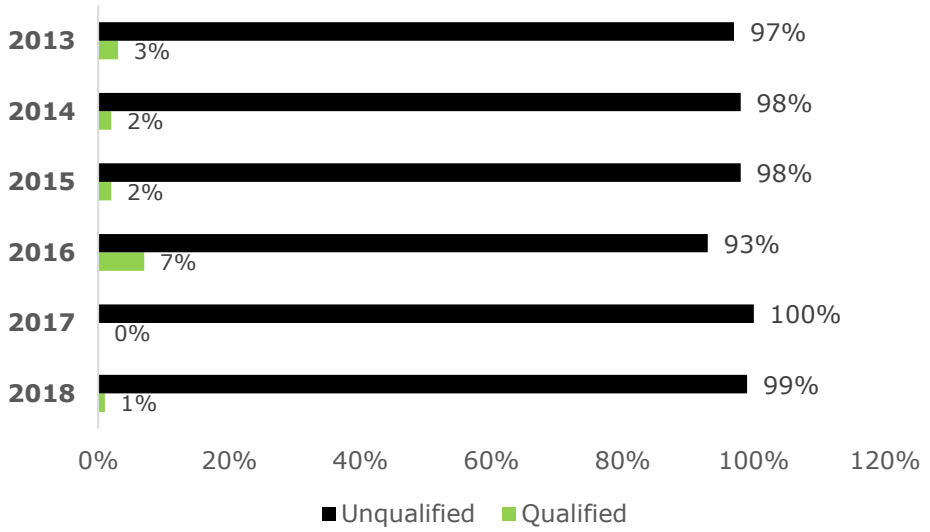
Detailed benchmarking analysis



1. Improvement in the execution of controls has resulted in a decrease of qualified reports

- The percentage of qualified reports, as compared to 2016, has reduced to 1%, in line with the 'norm' of 2-3% of what we have seen in the previous years .
- Contributing factors and drivers for this includes increased client awareness to manage and monitor their third parties, greater focus on IT controls, and increased regulatory scrutiny.
- Organisations have been investing in preventative controls as preference to manage risks in an effective and efficient manner.

Control Report Opinions



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?

2. Number of deviations per sector and causes associated with control deviations raised in 2017 and 2018 reports

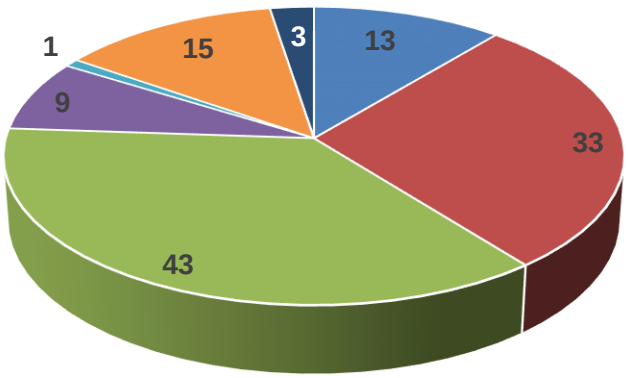
In 2017 and 2018, the number of deviations have decreased by approximately 50% on comparison to 2016. Our analysis shows an average of about 2 deviations per report.

Information Technology continues to be the source of the most deviations, particularly in relation to the user access controls that are critical in ensuring appropriate segregation of duties and IT security.

Inadequate review appears to be the main cause of the deviations, predominantly raised in the control reports from Superannuation Member Administration and Information Technology sectors.

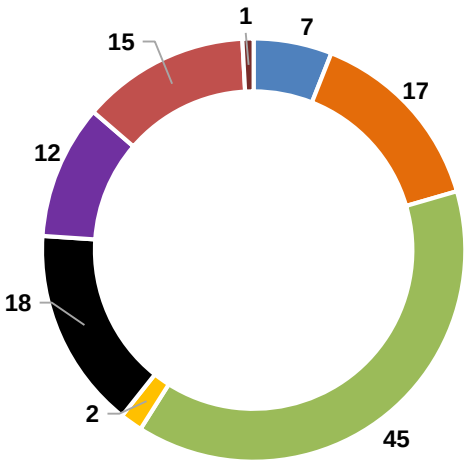
One impact of this is an increase in incident reporting which has resulted in customer service risk.

Number of deviations per sector



- Asset Management
- Custody
- Information Technology
- Investment Administration
- Registry
- Superannuation member administration
- Unit Registry

Causes of deviations per sector



- Improper Recording
- Inadequate Documentation
- Inadequate Review
- Other
- Untimely Resolution of Issues
- Ineffective control design
- Inappropriate User access
- Inadequate documentation

4. Operational and technology risks were most frequently associated with control deviations …

Risk Classes: Definitions

Operational Risk
Third party provider's operations are inadequate to provide the required services at the expected levels and consistent with service level reporting requirements.

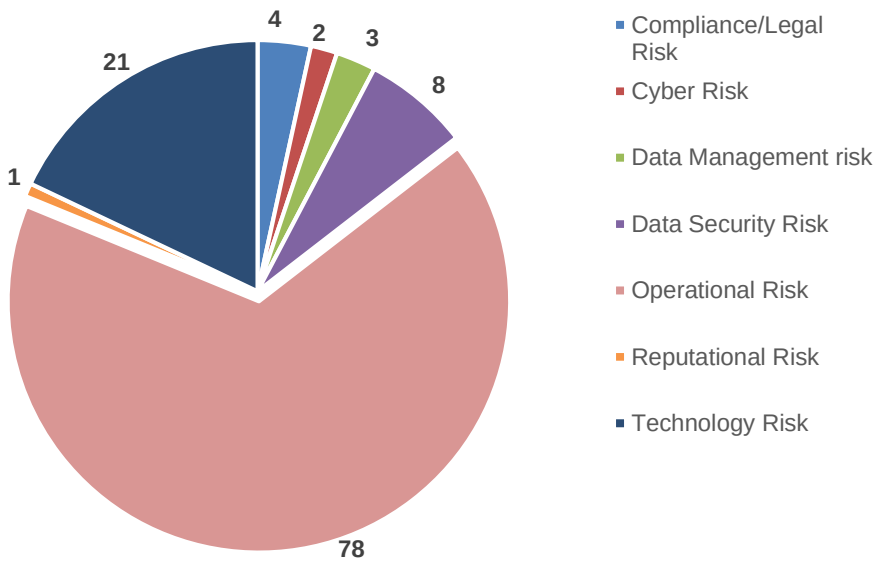
Technology Risk
Third party providers lack the necessary infrastructure, policies, or procedures to protect information and intellectual property from unauthorized access, modification, destruction, disclosure or misuse, potentially resulting in financial and reputational loss or legal or regulatory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

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

Data Security Risk/Cyber Risk
Third party provider fails to protect the clients digital assets and safeguard their organisational security, customer data and security controls

Sources of risk identified through deviations in third party control reports



Key questions:

- What are the sources of these deviations and risks? Have you assessed trends and root causes?
- Is the design of your controls appropriate to mitigate these risks? If not, why are you falling behind the improving trend?
- Do you seek guidance from your auditors on changes to controls throughout the year?

4. Timeliness of reporting has improved compared to last year, with average days to issue an opinion decreasing to 47 days

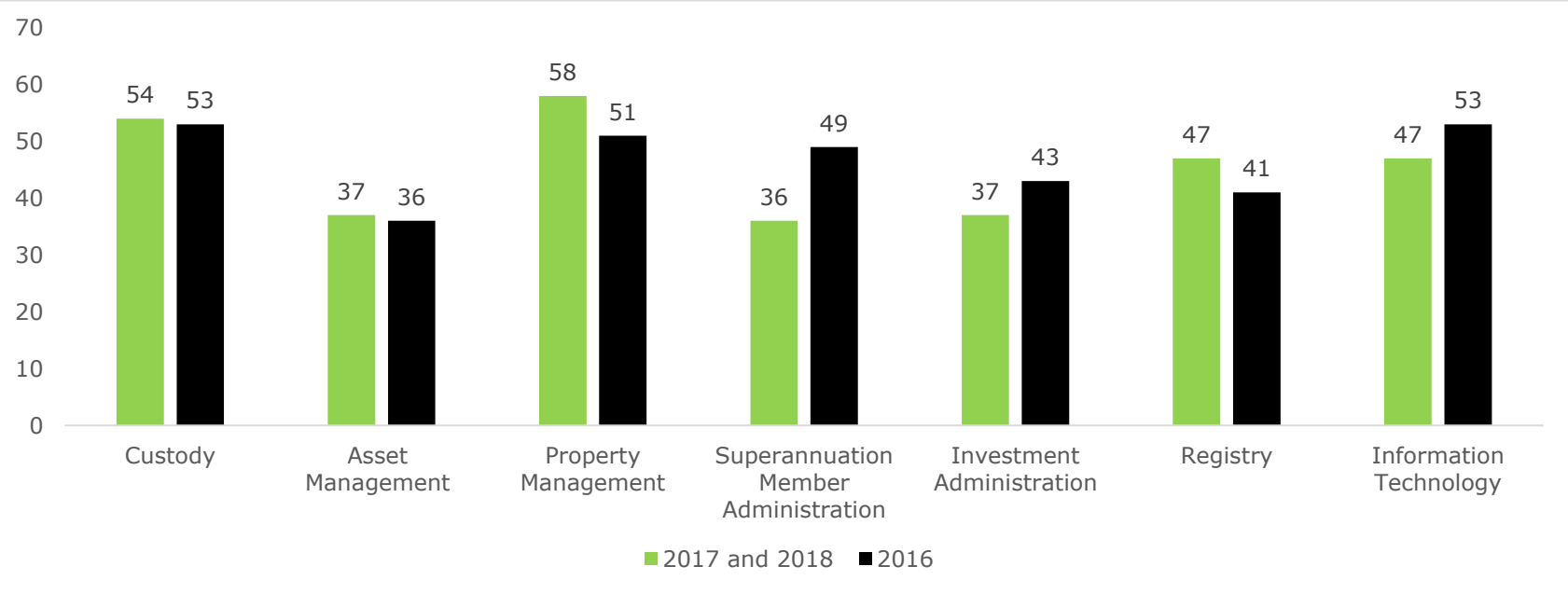
Average Days Elapsed Overall by Year

In FY 2017 and 2018, control reports were issued on average within 47 days from the year end date. The timeliness has improved from last year for 2 reasons. Firstly less deviations and qualifications has reduced the reporting timeframes. Secondly, organisations are more proactive with planning and executing reviews within required timeframes.

Key question:

- Are you doing what you can upfront in order to meet your deadline? Starting the review of your controls earlier in the year can speed up the process.

Average days elapsed after balance date per sector



5. Manual controls continued to be significantly higher than automated controls, showing that there is still a high reliance on people to manually prevent and manage risks.

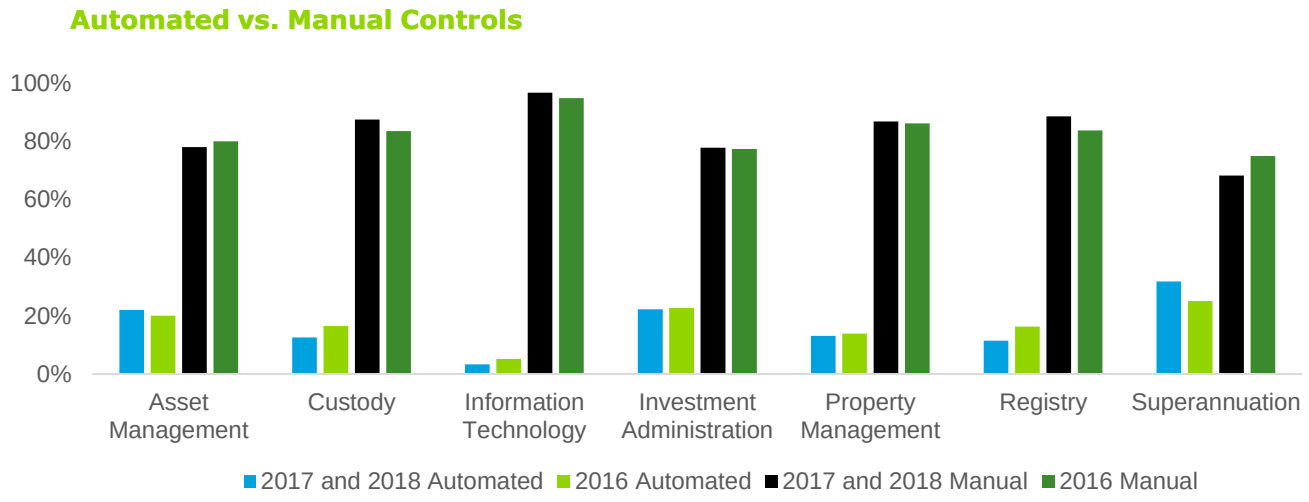
Automated vs Manual Controls

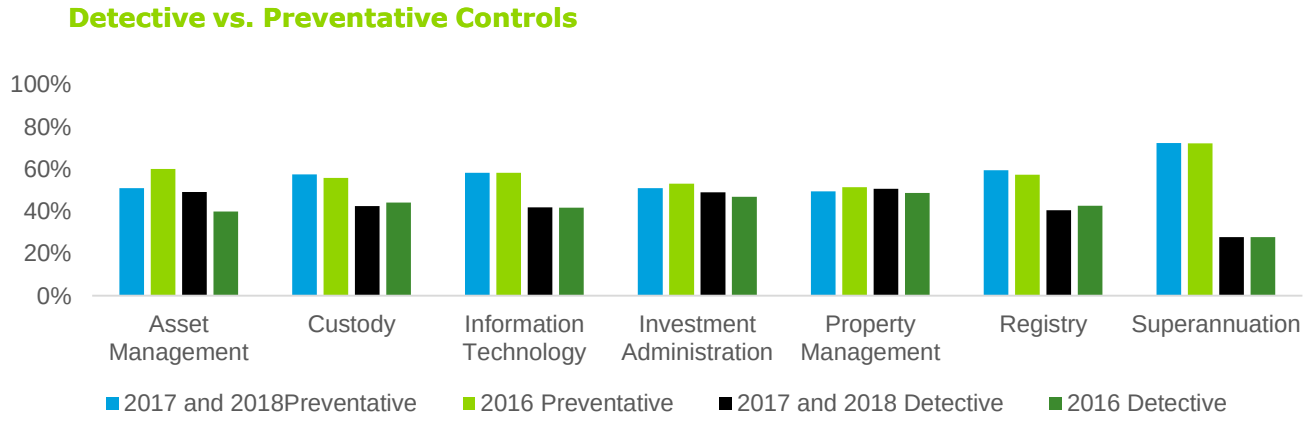
Across all sectors including Information Technology denoted a greater reliance on manual controls rather than automated controls. In fact, the Property Management and Registry Services showed a very large proportion of manual controls (96% and 90% respectively). Examples of manual controls related to Registry Services are: client set up, transactions entered in the registry system, review of redemption requests, reconciliation, review of unit prices.

Preventative vs Detective Controls

We saw a relatively consistent split and pleasingly a marginally higher proportion of preventative controls as compared to detective controls.

The Information Technology sector had the highest proportion of preventative controls (76%).






Technical update

Regulatory focus on data management leading to increased monitoring of third party service providers

1. European Union (EU) General Data Protection Regulation (GDPR)

What is the GDPR?

The European Union (EU) General Data Protection Regulation (GDPR) comes into effect on 25 May 2018 and will introduce stringent privacy and data protection requirements on businesses. All Australian businesses of any size will be impacted by the GDPR that holds, controls or processes personal data of individuals located in the EU. The GDPR applies to data controllers (e.g. trustees of superannuation funds and employers), but also to organisations that process data on behalf of the controller (such as administrators and payroll processors). The consequences of non-compliance are severe with fines of up to €20 million per infringement or 4% of global annual turnover (whichever is greater) and the risk of reputational damage, class actions and other regulatory attention.

Going forward it is important for organisations to understand how ***they and their service providers*** manage and protect personal data assets including how ***robust data protection measures and processes including breach identification and response processes.***

2. CPS 234 Information Security

This Prudential Standard aims to ensure that an APRA-regulated entity takes measures to be resilient against information security incidents (including cyberattacks) by maintaining an information security capability that is commensurate with information security vulnerabilities and threats.

A key objective is to minimise the likelihood and impact of information security incidents on the confidentiality, integrity, or availability of information assets, including information assets managed by ***related parties or third parties.***

How will this impact your organisation?

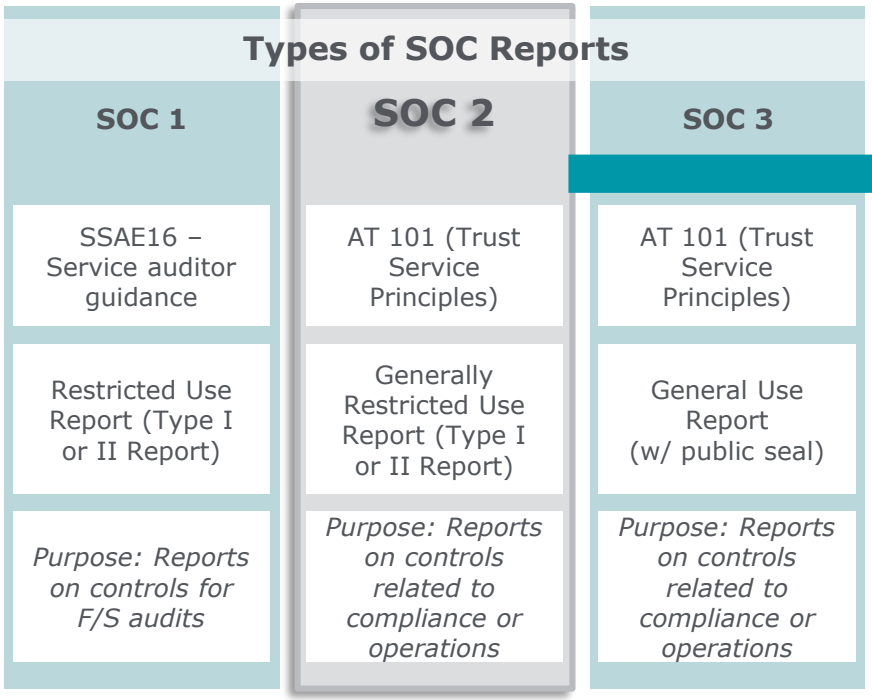
You can expect increased monitoring of third party and subservice organisations to ensure effective processes and controls exists to manage the personal data and information assets.

14

SOC Overview: Positioning of SOC2 to address the increased and new regulatory focus for data management

The American Institute of Certified Public Accountants (AICPA) created the SOC 2 reporting standards to gain assurance over internal controls related to Information Technology based on the Trust Principles of Security, Availability, Integrity of processing, Confidentiality and Privacy.

Latest trends in the US are a good indicator for global markets, including Australia, to consider what may be emerging globally. One such emerging trend is the growing use of SOC2 and SOC2+ reports resulting from increased outsourcing and growing regulatory focus on information technology and data management.



SOC 2

- Covers business areas outside of financial reporting for example security, privacy, processing integrity, availability or confidentiality
- Applied for regulatory or non-regulatory purposes, across industries and business sectors
- Can be distributed to user entities and specified parties.

SOC 2 reports focusing on the OSP's controls that are relevant to AICPA AT 101 Trust Service Principles (TSPs):

• **Security**: The system is protected against unauthorised access (both physical and logical). The security TSP serves as the basis for all SOC 2 reports and is commonly referred to as the Common Criteria.
• **Availability**: The system is available for operation and use as committed or agreed.
• **Processing integrity**: System processing is complete, accurate, timely, and authorized.
• **Confidentiality**: Information designated as confidential is protected as committed or agreed.
• **Privacy**: Personal information is collected, used, retained, disclosed, and destroyed in conformity.

Moving from SSAE 16 to SSAE 18

The SSAE 16, also called Statement on Standards for Attestation Engagements 16, is a regulation created by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA) to provide assurance on controls at the service and sub-service organisation. Effective May 1st 2017, the SSAE16 standard was replaced by SSAE18. The updated attestation standards emphasis on controls related to monitoring effectiveness of controls at the service and subservice organisation.

Global markets, including Australia, should consider whether their local third party assurance report should encompass these changes as they strengthen reputation and demonstrate increased transparency, and commitment to continually enhance internal control environments and reporting. The key changes are described below.

1 Monitoring the effectiveness of controls at subservice organizations

"The updated standards emphasizes that 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**."

2 Identifying complementary subservice organization controls

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

3 Clarification of complementary user entity control considerations (CUECCs)

"The updated standards **clarify** that the **CUECCs** should ***only*** **include** those controls and procedures that are **relevant** to achieve the **control objectives** within the service organization's report."

4 Evaluating the reliability of information produced by the service organization

"The revised standard **requires** that the **auditor evaluate** whether the **information provided** by the service organization is **"sufficiently reliable"** for the service auditor's purposes. "

5 Assessing the risk of material misstatement

"The updated standard place **emphasis** on the **service auditor** to **consider risks** and likely sources of **misstatement**, including those related to fraud at planning or during the course of the examination. "

Classifying vendors and sub-service organizations

The scope of the SSAE 18 report covers monitoring the effectiveness of internal controls at sub-service organization. Therefore, accurately identifying vendor and sub-service organizations is a critical component of the SSAE18 framework.

Sub-service organizations

A subservice organization is "a service organization used by another service organization to perform some of the services provided to user entities that are likely to be relevant to those user entities' internal control over financial reporting." As part of making that determination, management considers whether controls over the functions performed by the entity from which it has contracted services are likely to be relevant to the user entities' internal control over financial reporting.

- **Carve-out the subservice organization from the report.**
- **Identify Complementary Subservice Organization Controls (CSOCs)**
- **Include monitoring controls performed by the service organization over the sub-service organization in Section III of the report.**

- **Include the subservice-organization in scope, and expand report/controls. (Inclusive method)**

Vendor

Organizations that provide services to a service organization that are not considered subservice organizations are referred to as *vendors***.** This distinction is important because if an organization that provides services to a service organization is not a subservice organization, than an SSAE18 would not be applicable. (As per *AT-C Section 320*.)

If the client's controls alone are sufficient to meet the needs of the user entity's internal control over financial reporting (that is, achievement of the control objectives is not dependent on the entity's controls), management may conclude that the entity is not a subservice organization


Contact us

Contact our third party assurance specialist team

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

Ally MacLeod
Financial Services and Information Technology – Risk Advisory
Tel: +61 (0) 2 9322 7499
Email: amacleod@deloitte.com.au

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

Janice Scott (Sydney)
Financial Services and Information Technology – Assurance & Advisory
Tel: +61 (0) 2 9322 3737
Email: janscott@deloitte.com.au

19

Deloitte.