NFP RISKS AND COMPLIANCE

GAAP Consulting
advice • training • risk management • information

Authored by Colin Parker and edited by Stephen Downes

Edition 42: July – September 2024

IN THIS ISSUE

GOVERNANCE

Critical insights into financial management

The latest *Not for Profit Leader's Report on Financial Management* by HLB Mann Judd Sydney provides leaders with industry findings, insights, and best-practice solutions to help organisations achieve long-term sustainability.

More than 80 NFP leaders were surveyed about financial management – 52 per cent led charities, 19 per cent were from clubs and peak-body organisations, 9 per cent religious organisations, 8 per cent schools and training providers, 5 per cent social enterprises, and 5 per cent foundations. Two per cent led 'other' institutions.

Key findings included:

- Loss of major funding was the top financial risk for 59 per cent of respondents
- Sixty-eight per cent reported that their financial performances had worsened in the current economic climate
- Rising operational costs were the biggest financial challenge for 85 per cent
- Data security, automation, and integration were ranked as the most important finance-related technologies
- Budget constraints and limited resources were the primary barriers to technology investment
- Turnover within finance teams was at 60 per cent, which affected output
- Forty-three per cent were looking to outsource some of their finance processes, payroll most likely
- Eighty-four per cent had little understanding of AI and 14 per cent strong understanding – near identical findings with the previous report, and
- Sixty-four per cent were 'confident' in their systems, 14 per cent 'not confident' and 22 per cent 'unsure'. There was a notable decline in confidence to prevent and detect fraud compared with the previous survey. The percentage of respondents expressing confidence was 72 per cent in 2023.

Payday super progresses

While most employers do the right thing, the Australian Taxation Office estimates that $3.6 billion worth of super went unpaid in 2020–21.

From 1 July next year, employers must pay their employees' super simultaneously with salaries and wages.

The federal government has announced details aimed to 'incentivise' compliance and ensure that employees are compensated for delays in receiving their super, including:

- An updated 'super-guarantee' charge will ensure that employees are fully compensated for any delay in receiving their super, incentives for employers to catch up on any missed payments quickly, and an increase in the severity of consequences for employers that deliberately or repeatedly do the wrong thing
- Businesses will become liable for the charge if super contributions are not received by their employees' funds within seven days of payday. This allows time for payment processing to occur as well as for swift action to be taken against employers that are not meeting their obligations, and
- Revised choice of fund rules that will make it easier for employees to nominate their fund when starting a new job, reducing unintended duplicate accounts, and giving employers more timely and accurate details.

Legislative drafting will continue until the end of the year ahead of draft legislation's being released for consultation.

AI

More guidance needed on AI

Australian businesses need more guidance in adopting safe and responsible artificial-intelligence practices, a new report finds.

Commissioned by the National AI Centre, the *Responsible AI Index 2024* shows that Australian businesses consistently overestimate their ability to use AI responsibly.

It found that 78 per cent of Australian businesses believed that they were implementing AI safely and responsibly but in only 29 per cent of cases was this correct.

The index surveyed 413 executive decision-makers responsible for AI development across financial services, government, health, education, telecommunications, retail, hospitality, utilities, and transport.

Businesses were assessed on thirty-eight 'responsible' AI practices across five topics:

- Accountability and oversight
- Safety and resilience
- Fairness
- Transparency and explainability, and
- Contestability.

The index found that, on average, Australian organisations were adopting only 12 out of 38 of the practices.

Voluntary AI safety standard released

The federal government has released *Voluntary AI Safety Standard*, which guides high-risk AI businesses on best practice. Details on the standard are available at industry.gov.au/VAISS.

The standard gives businesses certainty ahead of implementing mandatory guardrails. Consultation on a *Proposals Paper for Introducing Mandatory Guardrails for AI in High-Risk Settings* closed on 4 October. For more information on the proposals paper go to consult.industry.gov.au/ai-regulatory-guardrails.

OIAC issues guides on using AI

Two new guides from the Office of the Australian Information Commissioner show how Australian privacy law applies to artificial intelligence. They set out the regulator's expectations.

The first guide will make it easier for businesses to comply with privacy obligations when using commercially available AI products and help them to select an appropriate one. The second provides guidance on privacy and developing and training generative AI models.

'How businesses should be approaching AI and what good AI governance looks like is one of the top issues of interest and challenge for industry right now', said privacy commissioner Carly Kind.

'Our new guides should remove any doubt about how Australia's existing privacy law applies to AI, make compliance easier, and help businesses follow privacy best practice. AI products should not be used simply because they are available.

'Robust privacy governance and safeguards are essential for businesses to gain advantage from AI and build trust and confidence in the community.

'Addressing privacy risks arising from AI, including the effects of powerful generative AI capabilities being increasingly accessible across the economy, is high among our priorities', said Ms Kind.

'The community and the OAIC expect organisations seeking to use AI to take a cautious approach, assess risks and make sure privacy is a key consideration. The OAIC reserves the right to take action where it is not.'

Paper explores AI and consumer law

A new discussion paper explores the application of Australian consumer law to AI enabled goods and services.

It's part of the federal government's ongoing work to strengthen existing laws to address AI's risks and potential harms. Being considered are mandatory 'guardrails' for high-risk settings.

The paper seeks stakeholder views on:

- The appropriateness of existing consumer protections under ACL for consumers of AI enabled goods and services
- The application of existing ACL provisions to new and emerging AI enabled goods and services, and
- Remedies for consumers and liability for suppliers and manufacturers of AI enabled goods and services when things go wrong.

CYBER SECURITY

Data breaches highest since 2020

New statistics from the Office of the Australian Information Commissioner show that data breaches notified to the regulator in the first half of 2024 were the highest in three-and-a-half years.

The OAIC was notified of 527 data breaches between January and June, according to the latest *Notifiable data breaches* report, the highest number since July to December 2020 and an increase of 9 per cent from the second half of 2023.

Privacy commissioner Carly Kind said that the high number was evidence of significant threats to Australians' privacy.

Ms Kind said: 'Almost every day, my office is notified of data breaches where Australians are at likely risk of serious harm. This harm can range from an increase in scams and the risk of identity theft to emotional distress and even physical harm.

'Privacy and security measures are not keeping up with the threats facing Australians' personal information, and addressing this must be a priority.'

A MediSecure data breach affected about 12.9 million Australians – the highest number since the Notifiable Data Breaches scheme came into effect.

Like previous reports, malicious and criminal attacks were the main source of breaches (67 per cent), 57 per cent of them being cyber-security incidents.

The health sector and the federal government notified the most data breaches (19 per cent and 12 per cent), highlighting the vulnerability of both private and public sectors.

Commissioner Kind said six years on from the launching of the scheme, the OAIC had high expectations of organisations.

'The Notifiable Data Breaches scheme is now mature, and we are moving into a new era in which our expectations of entities are higher', she said.

'Our recent enforcement action, including against Medibank and Australian Clinical Labs, should send a strong message that keeping personal information secure and meeting the requirements of the scheme when a data breach occurs must be priorities for organisations.'

The OAIC will continue to take a proportionate approach to enforcement and is focused on providing guidance to help organisations comply with their obligations.

An eligible (notifiable) data breach occurs when personal information has been lost or accessed or disclosed without authorisation and that it is likely to result in serious harm to one or more individuals. A breach is notifiable when an organisation has not been able to prevent the likely risk of serious harm.

The *Privacy Act* requires organisations to take reasonable steps to conduct a data-breach assessment within 30 days of becoming aware that there are grounds to suspect that one has occurred. They must notify affected individuals and the OAIC as soon as practicable.

Australian privacy principle 11 requires organisations to take reasonable steps to protect personal information from misuse, interference, and loss, as well as unauthorised access, modification or disclosure, and to destroy or de-identify the information when it is no longer required.

The OAIC has published guidance on securing personal information and data-breach preparation and response as well as advice for individuals on data-breach responding.

Privacy bill introduced

The OAIC has welcomed the first tranche of privacy reforms with the introduction of the *Privacy and Other Legislation Amendment Bill 2024*.

The bill strengthens the OAIC's enforcement tools, including through an enhanced civil-penalty regime and infringement-notice powers.

It would also provide important clarification on the scope of existing security obligations by amending privacy principle 11 to require organisations to implement technical and organisational measures (such as encrypting data, securing access to systems and premises, and undertaking staff training) to address information-security risks.

The amendment aims to assist in clarifying the OAIC's expectations about the scope of measures that organisations should consider when protecting personal information.

COMPLIANCE

Sham contracts exploited workers with disabilities

The Fair Work Ombudsman has secured $197,000 in court-ordered penalties against a Sydney health-and-wellness research company for contraventions, including sham contracting involving workers with disabilities.

The Federal Court imposed the penalties against Doll House Training Pty Ltd, which researched robotics, coding, and artificial intelligence and their application to the health-and-wellness industry.

Doll House Training breached the Fair Work Act after it terminated or threatened to terminate three workers' employment and to re-engage them as independent contractors to perform substantially the same work.

The company also misrepresented to the workers that they were or would be engaged as independent contractors, when in fact they continued to be employees.

In October 2020, Doll House Training emailed each worker a 'new contract' titled Independent Contractor Agreement, which included several terms indicative of its being a contract of employment. Doll House also represented to the workers that they had to provide Australian business numbers and submit invoices.

Justice Scott Goodman considered the terms of the ICA and found them to be 'contracts of employment' for several reasons, including that the 'rights and obligations' suggested that the workers 'were contracted to work for Doll House's business rather than any business of their own'.

Judge Goodman found that there was a 'clear power imbalance' for two of the workers who signed the contract because they felt that they had 'no alternative'.

Doll House Training also failed to pay the workers in full at least monthly during their employment and failed to comply with a notice to produce issued by a fair-work inspector that required it to provide specified records or documents, including those about the terms of engagement and duties performed by the workers.

Judge Goodman considered the situation the workers were in, being 'persons with disabilities, who had been searching for work and who were owed payments equivalent to the minimum wage'.

He found that the company's 'disregard' of the notice to produce hindered the FWO's investigations and that there was no evidence of any contrition, which further warranted penalties that would ensure both general and specific deterrence.

Fair Work Ombudsman Anna Booth said that the substantial penalties sent a clear message that sham contracting is serious and would not be tolerated in Australian workplaces.

'We treat sham contracting particularly seriously', she said.

'We will pursue any employer who thinks they can take advantage of the power imbalance they have over workers, including those with disabilities as in this matter, some of whom felt that they had no alternative but to accept a sham contract or be jobless.'

The underpayments were rectified in full after the FWO began its investigation.

FINANCIAL-REPORTING INSIGHTS

AASB issues annual-improvements standard

The Australian Accounting Standards Board has issued AASB 2024-3 *Amendments to Australian Accounting Standards – Annual Improvements Volume 11*.

The standard amends AASB 1 *First-time Adoption of Australian Accounting Standards*, AASB 7 *Financial Instruments: Disclosures*, AASB 9 *Financial Instruments*, AASB 10 *Consolidated Financial Statements*, and AASB 107 *Statement of Cash Flows*.

It applies to annual periods beginning on or after 1 January 2026, earlier application of amendments to individual standards permitted.

In **GAAPinar No.12** on Tuesday 17 December Carmen Ridley and Colin Parker are covering *Reporting and auditing considerations for 31 December reporters.*

SUSTAINABILITY REPORTING

AASB S1 sustainability disclosure is voluntary

The AASB has published a voluntary AASB S1 *General Requirements for Disclosure of Sustainability-related Financial Information* and mandatory AASB S2 *Climate-related Disclosures*.

They apply to annual reporting periods beginning on or after 1 January next year. Earlier application is permitted.

AASB S1 is intended to be used by entities that voluntarily disclose information about their sustainability-related risks and opportunities in general-purpose financial reports.

An entity electing to voluntarily apply AASB S1 discloses information about sustainability-related risks and opportunities that could reasonably be expected to affect its cash flows, access to finance and cost of capital over the short, medium, and long terms.

AASB S1 applies to reporting sustainability-related financial information across a range of possible sustainability topics, including climate-related financial disclosures.

The main principles and guidance relate to:

- Identifying the objective of sustainability-related financial information
- Setting out the conceptual foundations for sustainability-related financial information to help ensure that its relevance and that the information disclosed is a faithful representation of what it purports to represent
- Materiality
- The core content that would be expected to be disclosed about a particular sustainability topic, including on governance, strategy, risk management, metrics, and targets
- Sources of guidance on disclosing sustainability-related financial information
- The location of sustainability-related financial-information disclosures
- Their timing
- The disclosure of comparative information in the sustainability report, and
- Judgements, uncertainties, and errors affecting sustainability-related financial information.

AASB S1 is a voluntary standard consistent with federal-government policy, which is to mandate for the time being only climate-related disclosures.

Mandatory-disclosure requirements for other sustainability-related topics might be developed, which might result in either revisions to or replacement of S1, potentially including its becoming mandatory.

Hear more sustainability and climate change reporting in **GAAPinar No.4** on Thursday 14 November *New legislation and AASB standards on climate risk disclosures* with Carmen Ridley and Colin Parker

AASB S2 *Climate-related Disclosures* is mandatory

The AASB's separate, mandatory standard on climate-related financial disclosures, AASB S2 *Climate-related Disclosures*, applies to annual reporting periods beginning on or after 1 January. Earlier application is permitted.

The *Corporations Act 2001* sets out the entities that are required to comply with the standard and specifies three application dates (financial years beginning on or after 1 January next year and in two subsequent years) for the various classes of entity.

AASB S2 requires an entity to disclose information about climate-related risks and opportunities that could reasonably be expected to affect its cash flows, access to finance and cost of capital over short, medium, and long terms.

The standard sets out disclosure requirements to provide useful information to primary users of an entity's general-purpose financial reports about climate-related risks and opportunities that could reasonably be expected to affect it.

The main climate-related financial disclosure requirements relate to governance, strategy, risk management, metrics, and targets, including information about scenario analysis and scopes 1, 2, and 3 greenhouse-gas emissions.

AASB S2 incorporates content from S1 to make it stand alone for climate-related financial disclosures. The content is included in S2's appendix D. General requirements include conceptual foundations for reporting such information, the location of disclosures, the timing of reporting, and disclosures on judgements, uncertainties, and errors.

Appendix D applies only to climate-related financial information and not broader sustainability-related financial information covered by S1. An entity may refer to AASB S1 for guidance in complying with the requirements in appendix D.

Entities may apply S1 in preparing sustainability reports.

ACNC ACTIVITIES

Applying external-conduct standards

More than 6 per cent of Australian charities operate overseas in the Philippines, Indonesia, Kenya, Papua New Guinea, and India, the five most-preferred countries.

All but basic religious charities must comply with the Australian Charities and Not-for profits Commission's governance standards. Charities operating outside Australia (including those that simply send funds overseas) must also comply with the ACNC's external-conduct standards.

The latter set reasonable expectations of oversight and governance rather than detailed, specific requirements. They cover four key areas of a charity's overseas operations:

- Activities and control of resources
- Annual review and record-keeping
- Anti-fraud and anti-corruption, and
- The protection of vulnerable individuals.

The external standards were introduced in 2019 with the aim of promoting greater transparency about operations overseas and to provide the public with confidence that resources and services reached legitimate overseas beneficiaries and were used for legitimate charitable purposes.

Charities must be able to provide evidence that they are meeting the standards if the ACNC asks them to do so.

The commission advised that good record-keeping was a key way that charities could show they were meeting the standards. They revealed a clear trail of accountability, which was vital in the context of money-laundering and terrorism-financing.

With global events driving the need for humanitarian aid, it is more important than ever for charities to adhere to these standards. The commissions updated advice on donating money for humanitarian relief emphasises the need for due diligence and proper oversight to help ensure funds are used appropriately.

Adhering to external-conduct standards allowed charities to make a positive impact on the global stage while maintaining the trust and confidence of the Australian community.

Don't be scammed

The ACNC is sounding the alarm on fake charity scams – Scamwatch has revealed that nearly 360 had been received in 2024 so far.

Between 1 January and 21 August:

- Scamwatch received 358 reports of fake charity scams, losses amounting to more than $107,000
- The most common contact mode was phone (117 reports), social networking and online forums (31 reports) and email (93 reports), and
- People aged 65 and over reported the highest total losses ($45,700), followed by people aged 55-64 ($20,103) and 25-34 ($19,318).

Scams are usually under-reported, and the actual figures are likely to be higher.

If you've been the victim of a scam or are suspicious of a donation request, report it to Scamwatch. Your reports help the National Anti-Scam Centre warn others about scams, monitor trends, and disrupt scammers.

To ensure that donations go to legitimate causes, always check the charity.

The ACNC recommends these simple precautions:

- Don't click on links in text messages, emails, and social-media posts
- Never disclose personal information or banking details to unknown callers
- Use the Charity Register
- Find contact information on the register such as a purported charity's website, and
- Donate direct to the charity using the methods given on the website.

Charities also need to be vigilant and should review and upgrade cyber-security measures to avoid becoming an easy target for criminals.

Federal Court dismisses PBI appeal

The Federal Court's full court has dismissed an appeal by Equality Australia Ltd to be registered as a public benevolent institution.

ACNC Commissioner Sue Woodward said: 'The term "Public Benevolent Institution" is not defined in legislation. We welcome judicial consideration of [it] and will be considering the judgment in the coming days'.

The Federal Court decision does not alter Equality Australia's charitable status – it remains a registered charity.

It has been registered with the ACNC since 2016. Its subtype is 'advancing public debate'. In 2020, it applied to the ACNC to change to PBI.

The ACNC refused to register Equality Australia as a PBI because it considered that the charity had an independent, non-benevolent purpose. (It agitates for law reform and social change, and this purpose did not amount to benevolent relief to people in need.)

The Administrative Appeals Tribunal later upheld, by a 2-1 majority, the ACNC's decision to refuse PBI registration. The AAT determined that it was not a PBI because of an insufficient connection between its activities and the benevolent ends it pursues.

Equality Australia then appealed to the full court of the Federal Court.

Hear about NFPs in **GAAPinar No.11** on Tuesday 17 December *Latest NFP and ACNC developments and insights* with Carmen Ridley and Colin Parker

NDIS

Jail time for NDIS rorters

Two men and a woman have been jailed in New South Wales for their roles in a multi-million-dollar defrauding of the National Disability Insurance Scheme.

The sentencing is the result of an investigation into several suspected fraudulent providers in western Sydney. It followed an investigation by the Australian Federal Police, the National Disability Insurance Agency, the Australian Transaction Reports and Analysis Centre, and Services Australia that uncovered more than $5.8 million in fraud.

Two other men were jailed in 2022 as part of the investigation.

Each of the three pleaded guilty to charges of dishonesty against the commonwealth.

- A Lidcombe man who pleaded guilty to two counts of dishonestly obtaining a gain from the commonwealth and one count of dealing with property reasonably suspected of being proceeds of crime, was sentenced to six years and six months imprisonment. A reparation order of $328,420.28 is to be repaid to the commonwealth
- A Lakemba woman who pleaded guilty to one count of dishonestly obtaining a gain from the commonwealth was sentenced to three years and five months imprisonment. A reparation order of $96,070.90 is to be repaid to the commonwealth, and
- A Ryde man who pleaded guilty to one count of dishonestly obtaining a gain from the commonwealth was sentenced to two years and 11 months imprisonment and a reparation order of $150,783.76.

Almost 1000 disability service providers have had payment of claims locked within recent months as the NDIA and Fraud Fusion Taskforce continue to target providers.

Crackdown continues on NDIS rorting

Three people have faced court for defrauding the National Disability Insurance Scheme while another provider awaits sentencing as the Fraud Fusion Taskforce clamps down on the scheme's exploiters.

An $83.9 million *Crack Down on Fraud* program has already yielded results, more than $75 million in payments having been stopped since July.

The most recent court cases have seen four people – from three separate matters across two states – face court and plead guilty to charges of exploiting the NDIS.

They include:

- A North-West Sydney NDIS provider pleading guilty to fraud-related offences totalling more than $1 million. She will be sentenced in coming months
- A Western Sydney male sentenced to 10 months' jail for dealing with proceeds of crime to the value of $69,000. The man had been an NDIS participant before having his access to the scheme revoked. It was found that he had colluded with family members – who had been operating as disability providers – to defraud the NDIS. Family members will face sentencing in coming months, and
- Two people in Gippsland sentenced to community correction and work orders for creating false invoices to defraud an NDIS plan.

NDIS minister Bill Shorten said the cases were a timely reminder of the NDIA's enhanced capability to detect and prevent fraud.

'Providers need to understand that they can't be "half honest". If the NDIA suspects something might be dodgy about a submitted claim, the agency won't pay it and will make enquiries', he said.

'If fraudulent activity is detected, its first priority is ensuring participant safety and welfare – meaning the agency will move participants to alternative providers – and may then launch an investigation into the provider.

'Pleasingly, the disability community is playing its part. Tip-offs have more than doubled since we introduced the taskforce, with more than 5000 tip-offs received so far this financial year.'

People can report fraud or non-compliance by filling in the online tip-off form, calling the NDIS helpline on 1800 650 717, or emailing fraudreporting@ndis.gov.au.

Support lists boost clarity for NDIS participants and providers

Minister Shorten has released lists of what NDIS participants can and cannot spend their funding on. The lists will provide much needed clarity and certainty to participants and providers.

They came into effect on 3 October, making it easier for participants to identify what is appropriately funded by the NDIS and what NDIS funding can be used to purchase.

There is also a substitution list that will allow participants to request a replacement support in cases where a standard household item might be able to provide better outcomes and value.

The lists are among amendments to *Getting the NDIS Back on Track Bill No. 1*, which passed parliament in August.

There will be a year-long transition period to ensure that participants aren't penalised for simple mistakes.

The Department of Social Services and the NDIA have worked extensively with the community to obtain feedback. Changes have included:

- The support categories are in language and terms which reflect supports included in plans, pricing arrangements, and how they are claimed
- A single list of support items and another of unsupported items
- A replacement process to access household items and assistive technology that might better meet participants' needs
- Menstrual products
- Participants may use their own funds to get the most cost-effective supports
- Internal and external building modifications to remedy damage arising exclusively from disability-related behaviours or use of NDIS-funded assistive technology are included in the list
- Driver training with a specialised instructor
- Clarification of hair and nail care, and
- Cultural activities support for First Nations participants.

Huge increase in penalties for dodgy NDIS providers

Minister Shorten has announced the second part of NDIS's *Getting it Back on Track Bill*, which will significantly increase protections for scheme participants and workers.

The proposed new law will strengthen the deterrence and compliance powers for the scheme's Quality and Safeguards Commission to take action to lift the quality of NDIS supports and safety for participants.

Penalties for providers will increase from a maximum of $400,000 to more than $15 million when a participant is hurt or injured under a provider's care.

The commission will be able to refer providers for criminal prosecution, for example, where there is a serious failure to comply with registration conditions.

The proposed legislation includes measures to:

- Impose stricter regulatory requirements and stronger penalties and criminal offences for those doing the wrong thing
- Strengthen information-gathering powers to improve monitoring and compliance of NDIS providers and others, and
- Expand the scope and application of banning orders to include people operating in other areas of the NDIS, such as auditing and consulting activities.

INSIDE GAAP CONSULTING

GAAPinar series underway

Our 12 new *GAAPinars* cover the very latest in auditing, financial and sustainability reporting, SMSF, and business risks. Ethical issues are discussed in several sessions.

New sessions focus on the recently released AASB 18 *General Presentation and Disclosure* – the foundation standard that you MUST know. And we'll cover contemporary financial-reporting issues, including climate change and fraud.

We continue the journey on audit quality and group audits.

We also go back-to-basics with sessions on share-based payments, financial instruments, and Australian Financial Services Licences.

Your favourites are back – 'what's new', SMSFs insights, NFPs and charities round-up as well as year-end considerations. And the special focus, as always, is on changes and how they affect the upcoming reporting season.

Let's summarise the sessions and who should participate (see below table).

Many of the topics are inter-related, so it's wise to participate in them all. But if you can't manage that, choose the sessions that best fit your business. And, bearing in mind our GAAPinars' reach, they offer huge value for money.

All sessions are recorded for later viewing.

Topics	Audit team members	Other public practitioners and their team members	Accountants in commerce, industry and NFPs
Auditing			
Further audit-quality lessons for the audit team	●		
Understanding the revised ASA 600 *Audits of a Group Financial Report (Including the Work of Component Auditors)* – Part 2	●		
An introduction to Australian Financial Services Licence regulatory requirements and audit guidance – Part 1	●		
Revisiting the fraud risk – governance and audit perspectives	●		
Financial reporting			
AASB 101 to AASB 18 *General Presentation and Disclosure* – the changes	●	●	●
Refreshing our understanding of share-based payments and employee benefits	●	●	●
Getting back to the basics of financial instruments – Part 1	●	●	●
Self-managed superannuation funds			
Contemporary SMSF compliance and audit issues	●	●	
Business risks			
What's new with accounting, auditing, ethical standards, and the regulators?	●	●	●
New legislation and AASB standards on climate-change reporting	●	●	●
Latest NFP and ACNC developments and insights	●	●	●
Reporting and auditing considerations for 31 December reporters	●	●	●

More training riches on demand

Looking for contemporary training in financial reporting, business risks, ethics, and auditing? Want to hear from the experts – Carmen Ridley, Chanelle Pienaar, Jessica-Anne Saayman, Stephen Newman, Shelley Banton, and Colin Parker?

Check out 'on-demand' sessions in *GAAP Training's* extensive library of more than 110 topics.

Use the *GAAPinars* as a refresher and to bring new members up to speed.

More than 150 CPD hours are just a mouse-click away at www.gaaptraining.com.au.

How we can help

As well as our advisory services on the interpretation of accounting, auditing, and ethics standards, *GAAP Consulting* can help you with:

Financial reporting – implementation of new and revised accounting standards, preparation of accounting policy position papers and pre-issuance reviews of financial statements

Risk management – quality-assurance reviews of audit files and risk-management systems (under auditing and ethical standards rules), engagement quality review and root-cause analysis services, help with enquiries from regulators and accounting bodies, and managing litigation risks

Training – face-to-face and web-based *(GAAPinars)* training on standards, legislative developments, and business risks as well as client briefings on contemporary issues. There is also an extensive library of *GAAPinars* (www.gaaptraining.com.au)

Information services – use of proprietary technical content from *GAAP Alert, Special GAAP Reports,* and *NFP Risks and Compliance* newsletters to enhance the brand awareness and expertise of existing and potential clients

Improving communication skills – we can help you to communicate better, editing and rewriting professionally your tenders, client communications, and internal manuals. They'll be clearer, simpler, more powerful, and easier to read and to understand. We can also help you to prepare formal and informal talks, speeches, and seminars, and

Whistleblowing service – *ReportFraud* is a cutting-edge fraud-protection tool you need to have. It's designed to safeguard your organisation from fraud, bribery, and corruption 24 hours a day, seven days a week. It allows whistleblowers to report unethical activity safely and – most importantly – anonymously (www.reportfraud.org.au).

The *GAAP Consulting* members and their areas of expertise and locations are:

- **Colin Parker** (financial reporting, audit, ethics, and risk management) – Canberra
- **Carmen Ridley** (financial reporting and ethics) – Melbourne
- **Stephen LaGreca** (financial reporting, audit, and risk management) – Sydney
- **Chanelle Pienaar** (audit and risk management) – Brisbane
- **Jessica-Anne Saayman** (audit and risk management) – Brisbane
- **Shelley Banton** (self-managed superannuation funds) – Newcastle
- **Andrew Parker** (training, marketing, and event management) – Melbourne, and
- **Stephen Downes** (client communications) – Melbourne.

We use the services of Stephen Newman, corporate lawyer, Hope Earle, Melbourne, when matters have a legal aspect.

Contact Colin 0421-088-611 or colin@gaap.com.au.

Colin Parker
GAAP Consulting

Contact Us

Should you require any further information about the services provided or our team, please contact:

Colin Parker
Principal, *GAAP Consulting*
Head of the GAAP Consulting Network
Email colin@gaap.com.au
Mobile 0421 088 611
Postal GPO Box 1497, Melbourne, Victoria 3001
Website www.gaap.com.au

GAAP Consulting GAAP Consulting Colin Parker

Sponsored by

ReportFraud

GAAP Consulting

advice • training • risk management • information