WATCO PARTNERS PTY. LTD.
Certified Practising Accountants

44 Tallarook Street (PO Box 286)
Seymour VIC 3660
Phone: 03 5792 2580 | **Email:** admin@watcopartners.com.au
Website: www.watcopartners.com.au

On The Money
September 2026

The information contained in the following articles is up-to-date and covers tax planning and topics that need to be considered in everyday life, or if you are running or starting a business. **The articles included below are**:

- Impersonation scams are on the rise
- Tax Time Checklists
- Does Your Small Business Need to Follow AML Privacy Rules?
- Components of a cyber security plan
- Managing your mental health and wellbeing
- Global companies turn to cost-cutting amid ongoing inflation

Impersonation scams are on the rise

Best defence is to pause – protect your ID and your finances.

Ever received an unexpected call, text or email asking you to ack quickly? We are sure you have.

Small mistakes become big mistakes when we're busy or distracted – sending an email too quickly or clicking a link without thinking twice.

Impersonation scams are common threats we're seeing as we approach the end of the financial year.

These scams can arrive by text message or email and often appear to come from banks, government agencies, or even someone you know – commonly try to create urgency – warning you there's a problem with your account, a missed payment, or a tax issue that needs immediate action.

Scam activity increases at tax time, with common scams related to:-

- tax refunds or outstanding tax payments

Impersonation scams are on the rise

- emails or texts claiming to be from the ATO or myGov
- request to 'confirm' personal or banking details

The safest response is to stop, don't engage, and verify the request through official channels.

Do not engage immediately. Nothing is so important that it cannot wait – days, even weeks.

Put the urgency aside until you are sure it is legitimate.

Tax Time Checklists
Individuals; Company; Trust; Partnership; and Super Funds

These checklists will help us ensure you don't miss any deductions. Simply print, complete and return.

Individuals - 2026

Company Trust Partnership - 2026

Superannuation Funds - 2026

The greatest compliment we receive from our clients is the referral of their friends, family and business colleagues. Thank you for your support and trust.

Does Your Small Business Need to Follow AML Privacy Rules?

Compliance with new anti-money laundering (AML) laws may subject your small business to additional privacy obligations it did not face before.

If your business will be required to comply with the Anti-Money Laundering and Counter Terrorism Financing Act 2006 (AML Act), you also need to consider your privacy obligations when handling personal information. Even if you operate a small business that would normally be exempt from privacy regulation, the new AML laws could change this.

Specifically, businesses that are reporting entities under the AML framework must comply with the Privacy Act 1988 (Privacy Act) when collecting, using, storing or disclosing personal information for AML purposes. This includes businesses with an annual turnover of less than $3 million.

Understanding how these two frameworks interact is important if your business performs customer due diligence, identity verification or transaction monitoring. This article explains how the AML and privacy frameworks interact and what small businesses need to do to comply with both.

When Does the Privacy Act Apply to Your Business?

The Privacy Act generally regulates how organisations handle personal information through the Australian Privacy Principles (APPs). While many small businesses are normally exempt, that exemption does not apply when you handle personal information to meet AML obligations. If your business is a reporting entity under the AML Act, you must comply with the Privacy Act for activities connected with those obligations.

Activities that may trigger privacy obligations include:

- collecting personal information for customer due diligence;
- storing information for AML record-keeping purposes;
- monitoring transactions and reporting suspicious matters; and
- conducting personnel due diligence for employees working in AML roles.

Collecting Personal Information for AML Compliance

To meet your AML obligations, your business will often need to collect personal information about customers, employees or other individuals. Under the APPs, you must limit the information you collect to what is reasonably necessary for your functions and activities. In the AML context, this typically means collecting information required for customer due diligence or risk assessments.

During onboarding, you will commonly collect:

- full name;
- date of birth;
- residential address; and

- identification document details.

However, the requirement to collect information for AML purposes does not give your business unlimited authority to gather any data you want. You should always consider whether the information you are collecting is genuinely necessary for compliance. Collecting excessive or irrelevant information may increase privacy risks and create unnecessary cybersecurity exposure.

Customer Notification

When your business collects personal information, you must notify individuals about how their information will be handled. This is typically done through a collection notice and your privacy policy.

A collection notice should explain:

- your organisation's identity and contact details;
- why you are collecting the information;
- whether the collection is required by law;
- how the information may be used or disclosed; and
- the consequences if the information is not provided.

In the AML context, this may include explaining that information is collected to comply with the AML Act. However, you do not need to provide a collection notice where doing so would be inconsistent with your tipping off obligations under the AML Act.

Using and Disclosing Personal Information

Under the APPs, personal information should generally only be used or disclosed for the primary purpose for which it was collected. For AML activities, this may include:

- verifying a customer's identity;
- assessing money laundering or terrorism financing risks; and
- meeting reporting obligations.

In some situations, your business may also be required to disclose personal information to regulators.

For example, reporting entities must submit suspicious matter reports to AUSTRAC when certain conditions are met. Because these disclosures are authorised by law, they are permitted under the Privacy Act even if the individual has not provided consent for these disclosures.

If you disclose personal information overseas (including to a third party service provider), you must generally take reasonable steps to ensure that the overseas recipient does not breach the APPs. However, exceptions apply where the disclosure is required or authorised by the AML Act.

Protecting Personal Information

Businesses that handle AML data often hold large volumes of sensitive personal information. This can make them attractive targets for cybercriminals. Under the APPs, you must take reasonable steps to protect personal information from misuse, interference, loss or unauthorised access.

Practical security measures include:

- using strong password policies and multi-factor authentication;
- restricting staff access to personal information;
- keeping software and systems updated;

- monitoring system activity with audit logs; and
- implementing a data breach response plan.

Having a clear response plan ensures your business can act quickly if a data breach occurs.

Retaining and Destroying Personal Information

Under the Privacy Act, businesses must take reasonable steps to destroy or de-identify personal information once it is no longer required. However, the AML Act requires certain records to be kept for specified periods to demonstrate compliance. This means your business must retain AML records when required by law. Once the retention period expires and there is no other reason to keep the data, you should securely delete or de-identify it.

Key Statistics

1) $3 million: the annual turnover threshold below which a business is normally Privacy Act exempt, an exemption that does not apply where the business is an AML/CTF reporting entity.
2) Close to 100,000: businesses will be regulated by AUSTRAC once the reforms take effect on 1 July 2026, up from around 19,000 today.
3) Fewer than 5%: of Australian businesses meet the threshold that would bring them within the Privacy Act's scope under the current small business exemption.

Sources

1) OAIC (April 2026)
2) AUSTRAC (March 2026)
3) Attorney-General's Department, Privacy Act Review Report 2022 (February 2023)

Key Takeaways

If your business is a reporting entity under the AML regime, you must comply with the Privacy Act when handling personal information for those obligations. This applies even to small businesses that would otherwise be exempt from privacy regulation.

To comply with both frameworks, your business should only collect information that is reasonably necessary, provide clear privacy notices, protect personal data with appropriate security measures, and retain information only for as long as required. Taking these steps will help you meet your AML obligations while maintaining strong privacy practices and protecting the personal information entrusted to your business.

The greatest compliment we receive from our clients is the referral of their friends, family and business colleagues. Thank you for your support and trust.

Components of a cyber security plan

What is a cyber security risk plan?

A cyber security risk management plan is a strategic blueprint that outlines how an organization identifies, evaluates, and mitigates threats to its digital assets. It aligns security controls with business objectives to protect the confidentiality, integrity, and availability of information systems against breaches or attacks.

Key Components

A comprehensive cyber security plan goes beyond basic IT by integrating specific policies, strategies, and actions into day-to-day operations:

- **Asset Identification:** Cataloguing and prioritising all critical data, hardware, and software systems.
- **Risk Assessment:** Systematically analysing vulnerabilities and estimating the likelihood and financial impact of potential cyber-attacks (e.g., ransomware, phishing).
- **Mitigation Strategies:** Implementing defensive measures to reduce, accept, transfer, or avoid identified risks.
- **Data Breach Response:** Outlining exactly who is responsible, when to trigger the protocol, how to contain the threat, and who to notify (customers, legal teams).
- **Ongoing Monitoring:** Continuously scanning for new vulnerabilities and reviewing controls to adapt to an evolving threat landscape.

Why It Matters

Without a solid plan, organisations risk operational downtime, severe regulatory penalties, and significant financial or reputational damage. A documented plan ensures that cybersecurity is not just a reactive IT problem, but a proactive, board-level discipline.

Frameworks & Tools

Many organizations base their plans on established standards or guidelines to ensure compliance and industry best practices. Australian organisations frequently align their frameworks with resources from the Australian Cyber Security Centre (ACSC), while global organizations often look to the ISO/IEC 27001 standard or frameworks provided by the National Institute of Standards and Technology (NIST).

To learn more about assessing your own organisational risks, consider reading up on threat modelling using the SANS Institute Glossary or the IBM Cybersecurity Risk Assessment Guide.

The greatest compliment we receive from our clients is the referral of their friends, family and business colleagues. Thank you for your support and trust.

Running a small business has always required grit, creativity and the ability to adapt quickly. However, today's environment brings a level of uncertainty that can present challenges for everyone.

Economic pressures, rising operating costs, shifting customer behaviour and ongoing workforce challenges don't just affect business decisions; they can also affect your mental health and wellbeing.

Here are some practical strategies to help you navigate uncertainty and manage stress.

The hidden stress of running a small business

In recent years, the level of uncertainty facing small business owners has intensified. For many small business owners this creates a persistent sense of being 'on alert', scanning for the next challenge or setback.

This heightened sense is a natural human response to unpredictability. When the brain perceives uncertainty as a threat, it activates the stress response system, preparing the body to react quickly.

In the short term, this can help business owners stay focused and responsive. When uncertainty becomes chronic, the stress response can remain switched on for long periods, taking a significant toll on mental health and wellbeing.

The mental toll of uncertainty

When business owners feel they cannot predict or control what comes next, it becomes harder to make decisions, plan ahead or feel optimistic about the future. Over time, this can take a significant toll.

Small business owners may find themselves imagining worst-case scenarios, replaying concerns late at night or feeling unable to switch off.

This can lead to fatigue, irritability, difficulty concentrating, a sense of being overwhelmed, reduced productivity and anxiety or low mood.

The emotional load of running a business can also lead to isolation. Many small business owners feel they must appear strong for their staff, customers and families. This can make it difficult to acknowledge when they are struggling.

How to stay steady in uncertain times

Without support, stress can accumulate and begin to affect physical health, relationships and decision-making.

While uncertainty is part of running a small business, there are practical ways to protect your mental wellbeing and create more breathing room in the day.

- Remind yourself that unpredictability is a reality of running a business, not a result of anything you've done or not done.
- Focus on what's in your control and list the tasks, decisions or actions you can influence to shift attention away from the unknowns and reduce feelings of helplessness.
- Break down big worries into smaller, solvable pieces – instead of asking 'what if the business doesn't survive?' ask 'what can I adjust this month to improve cash flow?'
- Identify the signs that your stress is building, such as irritability, avoidance or overworking, so that you can intervene early rather than waiting until you're overwhelmed.
- Celebrate the wins (no matter how small) to acknowledge progress to help counterbalance the brain's tendency to fixate on threats and uncertainty.

It's also important to think about your overall wellbeing and the steps you can take to create a calmer mindset. Small consistent habits can make a noticeable difference in how you cope, think and lead.

Useful wellbeing strategies

When feeling overwhelmed, small, practical habits can make a meaningful difference.

- Set boundaries around news and information like checking updates at set times rather than constantly scrolling. This helps reduce mental clutter and keeps the brain from staying in 'threat mode'.
- Take short breaks away from devices. A few minutes of movement, stretching or fresh air can calm your nervous system and improve focus.
- Talking with others whether it's a trusted peer, mentor or a professional support service can help lighten the load and offer perspective.
- Prioritise your sleep and rest. Fatigue magnifies stress. Protecting sleep and building in small moments of rest strengthens resilience and decision-making.
- Practising grounding techniques like simple breathing exercises, mindfulness moments or sensory grounding can help calm the body and bring clarity when things feel chaotic.

These strategies won't remove uncertainty, but they can help you navigate it with more steadiness, clearer thinking and a stronger sense of control.

Reaching out for support

When stress hits, the impulse can be to withdraw, but reaching out for support is a sign of strength.

Recognising early signs of distress in yourself and others is a proactive step toward preventing burnout or more serious mental health challenges.

Look for the following signs:

- withdrawal or reduced engagement
- irritability or mood changes
- difficulty concentrating
- disrupted sleep
- feeling constantly on edge
- loss of motivation or confidence.

Managing your mental health and wellbeing during times of uncertainty

Services like Beyond Blue's NewAccess for Small Business Owners (NASBO) and Before Blue are designed to help small business owners and their teams navigate stress with practical, evidence-based strategies.

NASBO is a unique, free, confidential mental health coaching program that offers practical tools to manage stress, problem-solve and build coping strategies.

Before Blue (Beyond Blue's workplace wellbeing program) provides counselling, wellbeing support and resources to help employees navigate stress and uncertainty. These services offer a safe space to talk through challenges and develop strategies to protect mental health.

Global companies turn to cost-cutting amid ongoing inflation

Rising operating costs and persistent inflation are placing renewed pressure on businesses worldwide, despite signs that confidence is beginning to recover.

According to the latest Global Economic Conditions Survey conducted by the Institute of Management Accountants (IMA) and the Association of Chartered Certified Accountants (ACCA), a record number of chief financial officers and accountants reported increased costs in the second quarter of 2026.

This underscores the intensifying challenge of managing profit margins amidst geopolitical tensions, supply chain disruptions, and elevated commodity prices.

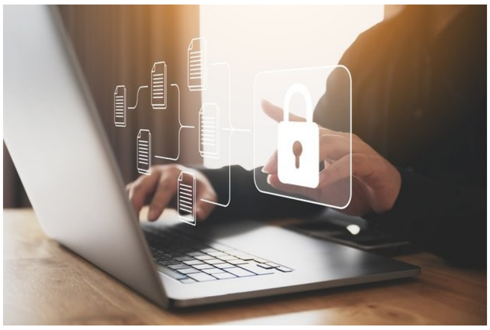
Operating costs have reached unprecedented levels, with 76 per cent of accountants reporting increases that surpass the previous peak recorded after Russia's invasion of Ukraine in 2022. The rise was even more pronounced among chief financial officers, where 83 per cent reported elevated expenses following a surge of over 20 percentage points from the prior quarter.

According to the report, the share of global accountants reporting higher operating expenses grew dramatically in the second quarter, reaching an unprecedented peak.

The greatest compliment we receive from our clients is the referral of their friends, family and business colleagues. Thank you for your support and trust.

Global companies turn to cost-cutting amid ongoing inflation

Researchers connected this growth to surging commodity and energy costs, in addition to supply chain bottlenecks arising from the conflict in the Middle East.



Businesses in North America and Western Europe faced especially intense cost pressures, exacerbated by ongoing supply chain difficulties and increased tariffs.

As profit margins face growing strain, survey participants indicated that numerous organisations are shifting their focus toward cost reduction initiatives. Specifically, over 50 per cent of those surveyed in North America reported that their clients or companies were actively looking for methods to decrease expenses.

These insights demonstrated that controlling operational expenditures has emerged as a primary financial obstacle for companies operating within a highly volatile global market.

Moreover, inflation remained a major concern for finance professionals, with rising commodity prices and geopolitical uncertainty fuelling expectations of further price increases.

The survey found that 72 per cent of accountants and finance professionals expected inflation in their country to increase over the following three months. At the same time, 42 per cent expected interest rates to rise, reflecting growing expectations that central banks would continue tightening monetary policy.

The report noted that higher energy prices following the outbreak of conflict in the Middle East had materially increased headline inflation across many economies.

Those inflationary pressures had already prompted policy responses, including an interest rate increase by the European Central Bank and a more hawkish outlook from the US Federal Reserve.

Researchers warned that developments in the Middle East would remain a key determinant of future inflation trends.

The report indicated that central banks could see inflation risks mitigated if the conflict progresses toward a resolution and oil prices stabilise near pre-war levels.

However, the report cautioned that renewed conflict and another spike in energy prices could force central banks into more aggressive policy action.

For businesses, persistent inflation was expected to remain a key challenge, increasing borrowing costs while adding further pressure to already elevated operating expenses.