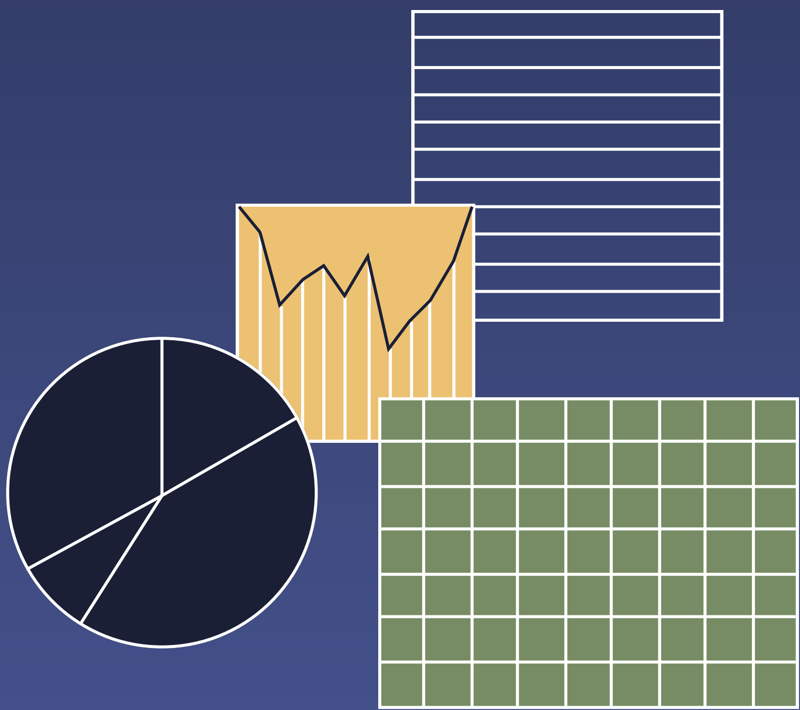
The Australia Business Email Report 2025:

Insights from 1,000+ IT Leaders



Exclaimer

2025

Executive summary

Email holds everything together. But control is slipping.

Throughout Australia, email remains the central system for business-critical communication. It's how contracts are shared, compliance notices are delivered, and internal policies are distributed. It's formal, traceable, and trusted—especially in industries like legal, finance, education, and healthcare.

Yet despite how vital it is, email remains one of the most overlooked parts of the IT stack.

Insights from 1,000 Australian IT leaders show that most organisations still depend on manual signature updates. Disclaimers are inconsistently applied. Brand formatting breaks between departments. And responsibility is divided across IT, compliance, HR, and marketing—with no shared platform or process to manage it.

IT is tasked with keeping this core infrastructure secure and compliant, despite fragmented systems and limited visibility.

Email isn't falling apart. But it's under pressure. And as usage scales without governance, the risk only grows.

This report reveals how Australian organisations are managing business email in 2025—and where gaps in compliance, branding, and IT control are starting to show.

Executive summary

Key insights

1. Email is still the backbone of business communication

- **94%** of Australian IT leaders say email is important or very important for business operations—the highest across all surveyed regions.
- Finance, legal, education, and healthcare teams rate it as mission-critical for auditability, documentation, and compliance.
- Over **82%** say more than half of their internal and external communication runs through direct one-to-one email.

2. Email signatures matter, yet are still managed manually

- **93%** of respondents agree professional email signatures build trust and credibility.
- Signature updates remain a top time sink in sectors like legal, retail, and education—where compliance and consistency are non-negotiable.
- Yet only **19%** use any form of centralised signature management.

3. Security incidents are common, and oversight is limited

- **71%** of organisations experienced an email-related security incident in the last 12 months.
- Only **18%** of respondents say they're very confident in their organisation's compliance posture.
- Common threats include phishing, spoofing, and unauthorised access.

Executive summary

4. Responsibility is shared with no ownership

- IT still manages the infrastructure—but legal needs disclaimers enforced, HR wants consistency in onboarding, and marketing owns branding.
- Without a centralised system, control is fragmented and updates become reactive.

5. Automation is in demand—but readiness is low

- **62%** of IT leaders want to automate elements of email governance, including email signatures, compliance workflows, and branding.
- Only **16%** say they're ready to implement automation as they're held back by budget constraints, migration complexity, and lack of integrated tooling.

93%
say email signatures build trust

71%
experienced an email-related security incident in the last year

18%
are confident in their companies compliance posture

Trend 1: Email is still the foundation for high-trust business communication

In Australia, email continues to serve as the communication channel of record. When accuracy matters—when legal, regulatory, or contractual details need to be clearly documented—it's email that organisations rely on. No other tool offers the same level of traceability, formality, and audit-readiness.

This is especially true in sectors where compliance is non-negotiable. IT leaders in **finance (94%), legal (94%), healthcare (92%), and education (93%)** rate email as the most important communication method in their organisations. Despite the rise of Teams, Slack, and other messaging platforms, email remains the one channel that spans departments, devices, and documentation standards.

And the volume backs it up. In legal and finance, employees send more than **20 emails per day**, far exceeding usage of other communication tools. The more formal or regulated the interaction, the more likely it is to be delivered by email.

How Australia compares globally

Australia stands out globally for its overwhelming reliance on direct one-to-one email. **94%** of Australian IT leaders say email is essential to their operations, compared to **86%** in the U.S.

While collaboration tools are gaining ground, they haven't replaced email. In industries like retail and education, instant messaging may support quick coordination, but the official message still goes through the inbox.

The trust placed in email isn't just cultural—it's practical. It scales, it logs, and it keeps a record when a record matters.

Trend 1: Email is still the foundation for high-trust business communication

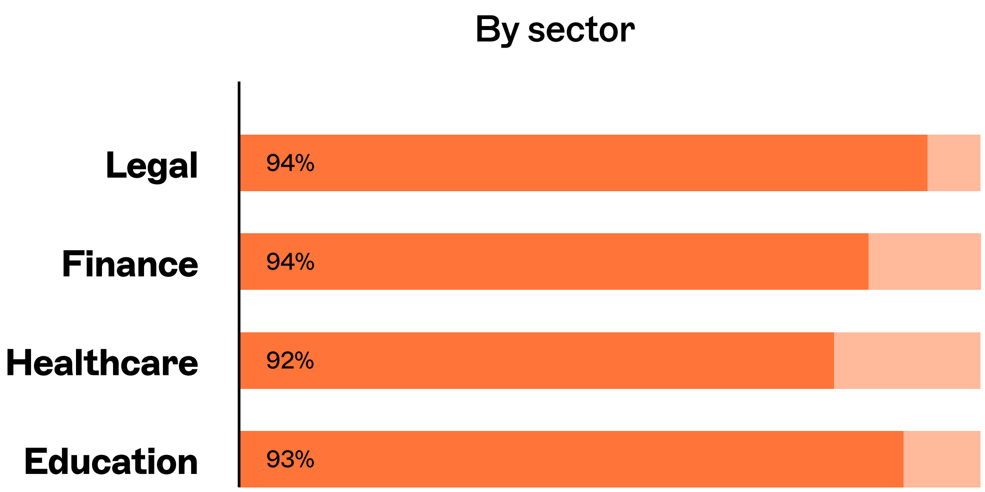
What this means for IT

IT leaders in Australia are managing a tool that's as mission-critical as it is under-managed. The infrastructure may be relied on daily, but the processes around it often lag behind.

Email governance—disclaimer logic, sender formatting, signature updates—is still handled manually or inconsistently across many organisations. These gaps aren't always visible, but they can introduce significant risk: brand exposure, non-compliance, and audit failures.

Treating email as core infrastructure means modernising how it's managed—not just the message content, but what surrounds it. That includes automation, oversight, and the ability to enforce standards across every user, every department, and every device.

% who say email is mission critical



Trend 2: **Email signature management is still too manual**

Email signatures should be simple. But for most Australian organisations, managing them is anything but. It remains one of the most overlooked admin burdens placed on IT teams—despite being one of the most visible parts of the business.

In sectors like legal, retail, and education, signature updates consume disproportionate amounts of time. IT teams are tasked with maintaining disclaimers, formatting sender details, and enforcing brand consistency—often across dozens of departments and hundreds of users.

The belief is there. **93% of IT leaders** in Australia say well-managed email signatures contribute to brand trust and professionalism. But the way they're managed tells a different story.

- Only **19%** of organisations use a centralised signature management tool.
- **66%** say signature updates are one of the most time-consuming tasks for IT.
- In sectors like legal and retail, inconsistent formatting and missed disclaimers are common pain points.
- Nearly half of all organisations rely on employees to manage their own email signatures manually.

Email is a critical communication layer, yet it's still governed by outdated processes.

Trend 2: : Email signature management is still too manual

How Australia compares globally

Australian teams face many of the same email signature challenges as their global peers, but with slightly more shared responsibility.

While U.S. teams report that IT bears the brunt of the burden, Australian organisations are more likely to involve marketing or compliance teams in signature updates. That said, the execution still falls short. Manual processes dominate, and visibility is limited across departments.

Other countries like Germany have higher tooling maturity—**94%** of German respondents say signatures are vital to brand trust—but Australia leads in acknowledging the need for improvement.

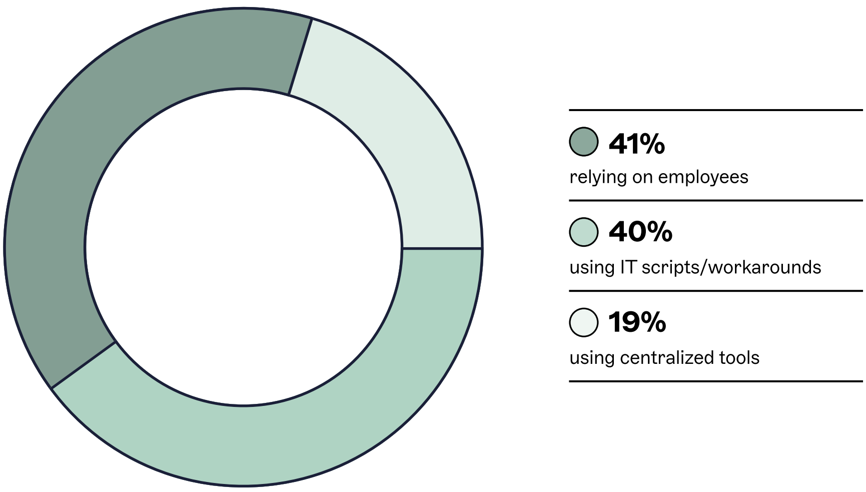
The gap lies not in recognition, but in adoption.

What this means for IT

Email signatures sit at the intersection of branding, legal compliance, and operational consistency. But without the right systems, every change becomes a support ticket. Formatting breaks between devices. Disclaimers are missed. Logos go out of date. And teams lose track of what's been sent and what hasn't.

For IT, this creates unnecessary workload and unnecessary risk.

Centralising email signature management doesn't require a complete overhaul of the email system. But it does require tools that enforce consistency, reduce admin, and allow other teams—like marketing or legal—to make updates without compromising control.



Trend 3: Security threats are rising, and compliance isn't keeping up

Email is still the most targeted communications channel in Australia. It's where sensitive information is shared, credentials are exchanged, and contracts are distributed—making it a natural entry point for phishing, spoofing, and data leakage.

And while security tools have evolved, controls around what gets sent—and *how*—haven't.

The disconnect is clear: security protocols like DMARC, SPF, and DKIM may be in place, but enforcement around sender formatting, disclaimers, and signature content remains patchy.

Industry	% experienced incidents	% very confident in compliance
Finance	67%	42%
Legal	64%	41%
Tech	61%	39%
Education	55%	27%
Retail	48%	32%
Education	42%	25%

Security threats are real and rising. But without centralised controls and better visibility, compliance confidence in Australia remains low.

Trend 3: Security and compliance confidence doesn't match risk exposure

How Australia compares globally

Australia sits near the top of the global scale for email-related security incidents. Like the U.S., **71%** of Australian organisations report at least one email-related issue in the past year. In regulated industries like finance and legal, the rates consistently exceed **60%**, despite high awareness of compliance requirements.

Germany shows similarly high incident levels. The UK reports fewer—though that may reflect limited reporting visibility, not stronger protections. In Australia, IT leaders are clear-eyed about the risks but still lack the centralised tools to manage them.

The result is a growing gap between intent and action.

What this means for IT

Security incidents are rising. Confidence in compliance is falling. That gap signals a growing vulnerability—one where IT is expected to govern a high-risk, high-volume channel with limited oversight.

Email protections are often applied inconsistently. Visibility into sender identity, message formatting, and policy adherence is fragmented across systems. Disclaimers, audit controls, and signature logic vary from one department to the next.

Closing that gap means building compliance into the infrastructure—not just securing the inbox but managing what leaves it.

Until that's in place, IT teams will remain reactive—fixing issues after they happen, instead of preventing them by design.

Trend 4: : Ownership is shared—but systems haven't kept up

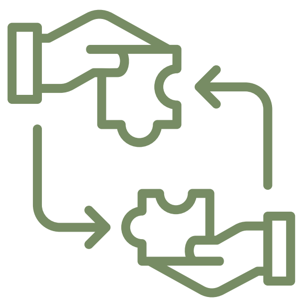
In Australia, IT still leads most email technology decisions. But it's no longer the only team involved. Marketing wants control over branding. Legal needs policy enforcement. HR expects consistency during onboarding. And yet, few organisations have the systems in place to manage that shared responsibility effectively.

This is especially true in industries like tech, finance, and retail, where email signatures carry real operational and reputational weight.

- **Marketing** teams want to run branded campaigns through email banners.
- **Legal and compliance** need disclaimers applied correctly and logged.
- **HR** expects uniform templates and role-based formatting for new joiners.

The inbox has become a cross-functional space, yet the infrastructure behind it hasn't evolved. Marketing might drive campaign strategy but still has to route changes through IT. Legal might request new disclaimers, but has no visibility into how they're applied. And HR rarely has access at all.

Without shared tooling, shared ownership often results in bottlenecks and inconsistencies.



Trend 4: : Ownership is shared—but systems haven't kept up

How Australia compares globally

Australian organisations show slightly better alignment across departments than their U.S. counterparts, but the execution gap remains.

In the U.S., IT shoulders most of the operational burden, even when other teams influence messaging. In Australia, marketing and compliance are more likely to be involved in email signature decisions—but without centralised systems, collaboration often breaks down.

Germany trends IT-heavy, while the UK faces similar decentralisation challenges. Australia falls somewhere in between: more cross-functional intent, but not enough shared control.

What this means for IT

Email tooling is no longer just IT's responsibility. It touches every department that manages branding, policy, or employee experience. But while input is growing, access isn't.

IT teams remain the gatekeepers, responsible for changes they didn't initiate and often without the bandwidth to keep up.

Solving this doesn't mean handing over control. It means implementing infrastructure that supports collaborative governance:

- **Legal** teams lack awareness of available tools
- **Finance** teams face slow procurement cycles
- **Education** teams encounter resistance to change

Without this, IT becomes the bottleneck and the inbox becomes another fragmented system that no one truly owns.

Trend 5: Australian IT teams want automation —but they're not ready

Across Australia, IT leaders are clear on what they need: centralised control, audit-ready infrastructure, and tools that take manual email management off their desks.

But despite that clarity, most still haven't implemented automation—particularly in sectors like education, retail, and healthcare, where resources are tight and priorities compete.

- **62%** of Australian IT leaders say they want to automate parts of their email infrastructure—including signatures, disclaimers, and policy enforcement.
- But only **16%** feel they're ready to do so.
- The biggest blockers? Budget approvals, migration complexity, and limited awareness of available solutions.

Even when the need is obvious, the execution is still out of reach:

- **Legal** teams can't apply disclaimers reliably or track updates centrally.
- **Finance** faces delays from procurement processes and demands audit logs by default.
- **Education** teams still manage signatures manually, often with inconsistent formats.
- **Retail** leaves email signature management to individuals, making brand control nearly impossible.

Each industry has its own goals:

- **Legal and finance:** Centralised policy enforcement, audit history, disclaimer control
- **Tech:** API flexibility, CRM integrations, scalable email signature templates
- **Education and healthcare:** Simpler workflows, auto-provisioning, role-based formatting
- **Retail:** Lightweight rollout, easy branding updates across locations

The need is universal—but without purpose-built tools, most teams are still stuck using manual workarounds and fragmented processes.

Trend 5: Australian IT teams want automation —but they're not ready

How Australia compares globally

Australian IT teams are aligned with peers across the U.S., Germany, and the UK: everyone wants automation. Everyone wants consistency. But very few are truly ready.

Even in sectors like tech and finance—where budgets tend to be higher and digital maturity stronger—email signature automation still falls behind. Migration concerns, approval bottlenecks, and internal complexity continue to block progress.

The issue isn't demand. It's readiness. And that gap between what's needed and what's in place is nearly identical around the world. The solutions exist. The infrastructure doesn't.

Australian IT teams know what needs to change—but without the right investment, intent doesn't turn into action.

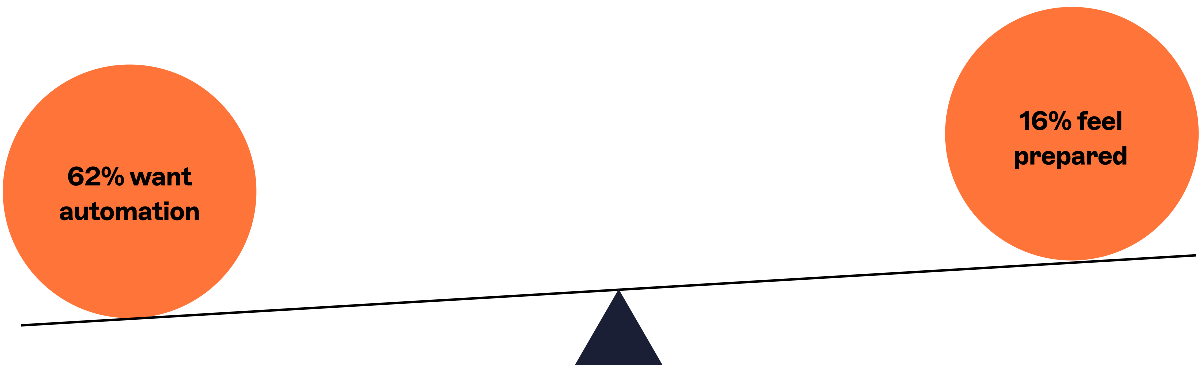
What this means for IT

The case for automation is already made. The challenge now is moving from intent to execution. For Australian IT leaders, that means shifting away from patchwork processes and investing in platforms that:

- **Automate signature updates and branding logic**
- **Apply disclaimers and policies by default**
- **Provide visibility, access controls, and audit tracking**
- **Integrate with Microsoft 365, Google Workspace, and CRM tools**

This isn't about layering on new complexity. It's about removing friction, eliminating unnecessary tickets, and giving other teams the access they need without giving up control.

Until then, IT will remain stuck in reactive mode—managing a critical communications layer manually, long after better options are available.

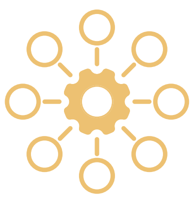


From insight to action: What Australian IT leaders need next

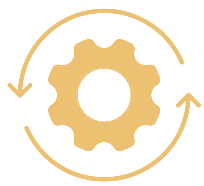
From banking in Sydney to manufacturing in Melbourne to universities in Brisbane, this research highlighted five key priorities:

- **Centralised email signature control**
- **Automated disclaimers and compliance workflows**
- **Cross-functional access for marketing, HR, and legal without losing IT oversight**
- **Integration with Microsoft 365, Google Workspace, and CRM platforms**
- **Audit-ready logs to support legal, risk, and security teams**

The message from Australian IT leaders is consistent: their teams don’t need more tools. They need the right infrastructure—purpose-built for scale, security, and control.

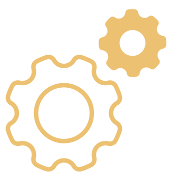


Centralisation



Automation

Access control



Integration

Audit logs

About Exclaimer

Email remains the backbone of business communication—and Exclaimer gives IT leaders the control, consistency, and oversight they need to manage it at scale.

Exclaimer is the global leader in email signature management for Microsoft 365 and Google Workspace. Its cloud platform enables IT teams to centrally manage and automate email signatures, ensuring compliance, brand consistency, and reduced support load.

Built for IT, Exclaimer eliminates manual updates, supports audit readiness, and integrates seamlessly into existing infrastructure.

Key capabilities include:

- **Centralised** control across users, departments, and locations
- **Automated** updates based on role, policy, or business unit
- **Compliance** features with audit-ready logs
- **Integration** with Microsoft 365, Google Workspace, CRM platforms, and security tools

Exclaimer supports more than 70,000 organisations worldwide—managing over 20 billion email signatures every year. Customers include Sony, Mattel, Bank of America, NBC, the Government of Canada, and the BBC.

Learn more at www.exclaimer.com or follow us on LinkedIn, Facebook, and X (formerly Twitter).
For media enquiries: press@exclaimer.com

Book a demo