idm.
information & data manager

AUGUST-SEPTEMBER 2025

Southeast Asia's Cyber-Scam Industry Booms

What should AI be doing with documents?

Information Governance and Data Governance: Time for a Détente?

GenAI prompts are next Records Management Problem Area

Banking Giant Picks ASC for Teams Compliance

In a significant move to enhance regulatory compliance, one of Australia's leading ASX-listed financial institutions has selected ASC Technologies to provide cloud-based recording services for its Microsoft Teams communications. The multi-year contract will implement ASC's Recording Insights solution across the enterprise.

The financial institution chose ASC based on three key factors: the company's established expertise in regulated markets, native integration capabilities with Microsoft Teams, and a robust, scalable solution built on Microsoft Azure technology. The deal represents a strategic expansion for ASC in the Australia-New Zealand region. Sreekanth Sreevalsam, Vice President of ASC ANZ, highlighted that the engagement "not only strengthens our presence in the ANZ region, but also reinforces our long-standing partnership with Microsoft."

He added that the collaboration empowers financial institutions with enterprise-grade compliance recording and AI data analytics, helping them navigate increasingly complex regulatory environments.

Based in Germany with a global presence spanning 15 locations and partners in over 60 countries, ASC specializes in compliance recording, quality management, and AI-based analytics.

Its solutions help organizations evaluate communications data, meet regulatory requirements, and optimize customer service through real-time AI analysis that can detect compliance violations and assess interaction quality.

Kapish Signs Cloud Contract with UTS

The University of Technology Sydney (UTS) is a leading public research university located in Sydney, Australia. UTS is known for its strong focus on innovation, technology, and industry collaboration.

The university emphasizes practical learning and real-world experience, and its modern, urban campus is situated in the heart of Sydney's central business district. UTS consistently ranks among the top young universities globally and is recognized for its research impact and graduate employability.

The Kapish cloud contract with UTS will support over 1,100 users and 7TB of documents across all business units, UTS will be supported by Kapish Content Manager Cloud, an ISO27001 Cloud eDRMS Platform.

The Kapish Content Manager Cloud contract provides a zero-footprint solution including:

- Content Manager Production Instance
- ISO27001 (Information Security Management) Certification
- Server Management – including Microsoft Patches
- Storage Management

UTS joins, University of New South Wales, CSIRO, University of Newcastle, Victoria University, ACT Education Directorate and Bureau of Meteorology on Content Manager Cloud.

https://kapish.com.au/products/content-manager-cloud/

Data Breach Surge Hits Record High

Australian businesses and government agencies reported an unprecedented 1,113 data breaches in 2024 - the highest annual total since mandatory reporting began in 2018, according to the Office of the Australian Information Commissioner (OAIC).

The latest statistics for July to December 2024 reveal 595 data breaches were reported to the OAIC during this period, contributing to the year's total figure. This represents a significant 25% increase from the 893 notifications recorded in 2023.

"The trends we are observing suggest the threat of data breaches, especially through the efforts of malicious actors, is unlikely to diminish, and the risks to Australians are only likely to increase," warned Australian Privacy Commissioner Carly Kind.

"Businesses and government agencies need to step up privacy and security measures to keep pace."

The Australian experience mirrors global trends identified in Pentera's 2025 State of Pentesting survey, which found that 67% of enterprises worldwide reported security breaches in the past 24 months. The impact of these breaches has been substantial, with 76% of Chief Information Security Officers (CISOs) reporting significant consequences including unplanned downtime (36%), data exposure (30%), and financial loss (28%)

idm.
information & data manager

Publisher/Editor: Bill Dawes
Email: bill@idm.net.au

Web Development & Maintenance: Cordelta

Advertising Phone: 02 90432943
Email: idm@idm.net.au

Published by Transmit Media Pty Ltd
PO Box 392, Paddington NSW 2021, Australia

Data Sharing Law Under Scrutiny

The Australian Government has opened public consultation on the future of its data sharing framework after revealing that only eight agreements have been established under the scheme since its inception three years ago.

The Department of Finance released an Issues Paper last month to guide the statutory review of the Data Availability and Transparency Act 2022 (DAT Act), which was initiated by Finance Minister Senator Katy Gallagher on March 20. The review comes as the legislation approaches a critical sunset clause that would see it automatically expire in April 2027 unless Parliament intervenes.

The Issues Paper reveals that despite establishing a framework designed to facilitate secure data sharing between government bodies and accredited entities, uptake has been minimal. All eight data sharing agreements formed under the scheme relate solely to the National Disability Data Asset project.

"This represents a small fraction of the total current public sector data sharing," the paper notes, revealing that a survey of 19 Commonwealth entities showed they maintained over 11,000 data sharing agreements outside the DAT Act framework.

The review will examine whether the legislation should continue, be amended, or be allowed to sunset, with submissions open until May 30. Dr Stephen King will lead the assessment, focusing on whether the Act has met its objectives of promoting better availability of public sector data while maintaining appropriate privacy and security safeguards.

Dr King is a Commissioner to the Productivity Commission and Professor of Practice at Monash University. His previous roles include Member of the Australian Competition and Consumer Commission, Professor of Economics at the University of Melbourne and Professor of Management (Economics) at the Melbourne Business School.

Key discussion points outlined in the Issues Paper include whether private sector and non-government organizations should be allowed to participate in the scheme, which currently limits accreditation to Commonwealth entities, state and territory entities, and Australian universities.

The paper also questions whether the Act's prohibition on data sharing for enforcement purposes should be reconsidered, potentially broadening use cases beyond the current limitations of government service delivery, research, and policy development.

The Office of the National Data Commissioner, established under the Act with approximately 40 staff and an annual budget of $A16 million, has accredited 34 entities to participate in the scheme to date.

The Productivity Commission's 2017 report, which prompted the legislation, estimated the value of Australian public sector data could range from $A625 million to $A64 billion annually.

The Minister must be provided with a report on the review within 12 months of its commencement, with a copy to be tabled in Parliament within 15 sitting days of the Minister receiving it.

ATO Warns of Identity Theft Surge

The Australian Taxation Office has moved to reassure taxpayers that its systems remain secure following reports of hackers stealing thousands of dollars through fraudulent tax returns, with some victims losing more than $14,000.

The ATO issued a statement denying that its systems had been compromised, describing media reports of a "hack" as incorrect. However, multiple taxpayers have come forward reporting that criminals had infiltrated their myGov accounts, filed bogus tax returns, and redirected refunds to fraudulent bank accounts.

"The ATO's systems are secure, resilient and have not been compromised," the tax office said in its statement. "The safety of taxpayers' information is of the utmost importance to us, and the ATO continues to remain vigilant for new and emerging cyber threats."

The ATO attributed the unusual account activity to identity theft rather than a breach of its own systems, explaining that "identity information can be compromised in a variety of ways, including requests for information by malicious actors, phishing emails, large-scale data breaches, and individual device or home network hacking."

Perth woman Kate Quinn discovered earlier this year that hackers had filed a fraudulent $A8,000 tax return in her name. Her accountant found they were no longer authorised to manage her tax affairs, and her linked bank account details had been changed.

Quinn described how quickly the fraud can occur: "They hack in, they untick 'notify me or notify my tax agent' and change the bank account details," she told The Australian. "[The ATO officer] said it probably takes all of 10 to 15 seconds [to] change the bank account details and the money's gone, and the case is closed and no one's notified."

Melbourne accountant Adrian Raftery reported a similar experience with one of his clients, where hackers successfully filed a new tax return and amended the previous year's return to obtain more than $14,000 in fraudulent refunds.

The sophisticated nature of these attacks has raised concerns about the vulnerability of taxpayer accounts, particularly as tax season approaches and criminals typically increase their targeting of tax-related fraud. In response to the growing threat, the ATO said it activates "stringent security measures" when it suspects a taxpayer's identity may be compromised. The ATO has not confirmed how many Australians have been affected by the fraudulent activity, the total amount of money stolen, or whether any arrests have been made in connection with the schemes.

Musk vs Australia: The Billionaire's Regulatory Battle Down Under

Elon Musk's confrontational approach to regulation has found a formidable opponent in Australia, where his companies X and Starlink are embroiled in multiple battles with government authorities.

Musk's satellite internet company Starlink has drawn the ire of the Australian Communications and Media Authority (ACMA) for repeatedly failing to meet basic reporting requirements. The regulator issued a formal warning in May 2025 after finding that Starlink failed to submit mandatory quarterly complaints reports on four separate occasions between October 2023 and July 2024.

Under Australian telecommunications law, companies with more than 30,000 active services must file complaints data within 30 days of each quarter. With an estimated 200,000+ Australian customers paying upwards of $A99 monthly, Starlink generates over $A237 million annually in the country, making the reporting failures particularly significant.

ACMA member Samantha Yorke said the delays "hampered the ACMA in its role of monitoring whether Starlink is meeting its obligations towards consumers," noting that the complaint data helps identify industry trends and areas needing improvement.

In recent months, X has launched fresh legal action against Australia's eSafety Commissioner, seeking to be exempt from the Relevant Electronic Services Standard (RES Standard) that came into effect in December 2024. The standard targets harmful content including child sexual exploitation material, extreme violence, illegal drugs, and pro-terror content.

X argues it should be governed by the less stringent Social Media Code instead, setting up another courtroom confrontation. The company has also faced a $A610,500 fine for failing to provide adequate information about its efforts to combat child abuse material on the platform - a penalty X unsuccessfully tried to avoid by claiming it was issued to the wrong company name after the Twitter rebrand.

The eSafety Commissioner Showdown began in April 2024 when a knife attack on Bishop Mar Mari Emmanuel at an Assyrian church in Sydney was livestreamed and quickly spread across social media platforms. Australia's eSafety Commissioner Julie Inman Grant ordered social media companies, including Musk's X (formerly Twitter), to remove the graphic footage globally.

While other platforms complied, X initially resisted, leading to a heated war of words between Musk and Australian officials. Prime Minister Anthony Albanese called Musk an "arrogant billionaire," while Musk has previously labelled the Australian government "fascists" over proposed misinformation laws.

The Federal Court initially granted a temporary injunction forcing X to hide the content worldwide, but the company successfully argued that Australia's jurisdiction should not extend beyond its borders. Justice Geoffrey Kennett ultimately declined to extend the injunction, citing concerns about the international implications of allowing one nation's regulator to control global internet content.

A Pattern of Defiance

The regulatory conflicts reflect what critics describe as Musk's broader disregard for local laws and oversight. His companies have shown a pattern of challenging regulatory authority, whether over content moderation, transparency reporting, or basic compliance requirements.

Industry observers note that with Musk's personal wealth in the hundreds of billions, potential fines from Australian regulators amount to "pocket change." This financial reality raises questions about the effectiveness of traditional regulatory tools against global tech giants.

Implications for Digital Sovereignty

The Australian cases have broader implications for how nations assert control over digital platforms and foreign-owned infrastructure. The eSafety Commissioner's attempt to impose global content removal orders represents an ambitious expansion of regulatory reach that other countries are watching closely.

Legal experts suggest the outcome of these battles could set precedents for digital sovereignty worldwide. If Australia succeeds in forcing compliance from Musk's companies, it could embolden other nations to assert similar authority over global internet platforms.

Conversely, successful resistance by X and Starlink might demonstrate the limits of national regulation in the borderless digital economy, potentially weakening regulatory frameworks globally.

Economic and Security Concerns

Beyond the immediate legal battles, Starlink's growing presence in Australia raises broader questions about telecommunications sovereignty. A recent regional telecommunications review highlighted concerns about foreign ownership of critical infrastructure, noting potential data security and sovereign risks.

With Starlink competing directly with Australia's National Broadband Network and gaining popularity in regional areas with poor connectivity, the service's regulatory compliance becomes increasingly important to national telecommunications policy.

The various legal proceedings remain ongoing, with court dates yet to be set for X's challenge to the RES Standard. The eSafety Commissioner continues pursuing the $A610,500 fine against X, while the ACMA monitors Starlink's future compliance with reporting requirements.

Regional Australia Bank Hit with Privacy Breach Finding

Following a two-year investigation, Regional Australia Bank (RAB) has been found liable for a significant privacy breach that saw the personal financial data of up to 197 customers mixed up and potentially disclosed to the wrong people, according to a determination released by Privacy Commissioner Carly Kind.

The breach, which occurred between March and June 2023, involved customer transaction data being "co-mingled" due to a software fault in RAB's Consumer Data Right (CDR) system. In at least one confirmed case, a customer received transaction data belonging to another customer, containing their personal information.

The incident was caused by RAB's contracted service provider, Biza Pty Ltd, which manages the bank's CDR technology platform. Biza had identified and fixed the same software fault for other clients in February 2023 but failed to apply the patch to RAB's system when it was upgraded to production on March 29, 2023.

The Privacy Commissioner found that despite the fault being RAB's contractor's responsibility, the bank remained liable under section 84(2) of the Competition and Consumer Act, which makes companies responsible for their agents' conduct.

"The respondent is liable for any failings by Biza even if it had no knowledge or awareness of those matters and was not in a position to take steps to prevent or address them," Commissioner Kind stated in her determination.

Significant Risk to Customers

The Commissioner emphasised the serious potential consequences of inaccurate financial data, noting it "may cause significant risk for customers" including being wrongly refused credit or given inappropriate credit that could lead to financial hardship.

"Decisions based on inaccurate data could result in individuals being wrongly refused credit, which may affect their immediate access to funds, but also their longer-term credit history," the determination stated.

The breach only came to light when a customer reported receiving wrong transaction data through the CDR Service Management Portal on June 29, 2023. Coincidentally, Biza implemented a broader software update on the same day that included the necessary patch, resolving the issue.

Commissioner Kind found RAB breached Privacy Safeguard 11 by failing to ensure CDR data accuracy, and Privacy Safeguard 1 by not implementing adequate systems to ensure compliance with consumer data right rules.

The bank was ordered to review its contractual agreements with Biza and implement better monitoring processes for third-party CDR services. However, no financial penalties were imposed.

RAB notified 181 affected customers of the incident in accordance with CDR rules, and the Commissioner noted there was currently no evidence that any customers experienced actual loss or damage.

The determination highlighted broader concerns about accountability when financial institutions outsource critical data handling functions to third parties, particularly as the CDR system expands across Australia's banking sector.

Industry Implications

The case represents one of the first major privacy breach determinations involving the Consumer Data Right system, which was introduced to increase competition in banking by allowing customers to safely share their data with other providers.

Commissioner Kind noted the finding "may cause some discomfort for regulated entities" who have sought to shift liability to contracted service providers, and hoped the determination would "clarify the position for outsourcing and outsourced entities."

RAB and Biza did not contest the factual findings in the investigation. The incident was resolved when Biza implemented the software update in June 2023, and stronger processes have since been put in place to prevent similar occurrences.

(The Consumer Data Right framework is co-regulated by the Office of the Australian Information Commissioner (OAIC) and the Australian Competition and Consumer Commission (ACCC).)

Read the full judgement here.

GenAI prompts are next Records Management Problem Area

As generative artificial intelligence tools become ubiquitous in corporate environments, legal experts are urging organisations to overhaul their document preservation and discovery practices to account for AI-generated content that could prove crucial in litigation.

In a new analysis published by Reuters Legal News, three Morgan Lewis attorneys argue that companies using AI tools like ChatGPT face unique challenges in preserving prompts and outputs that may be relevant to legal disputes.

"Generative AI tools hold transformative potential, but they must be carefully evaluated, tested, configured, and used with attention to the creation of potentially relevant documents and data that must be preserved," write Tara Lawler, Matthew Hamilton, and Jeff Niemczura in their commentary.

“It is also imperative for organizations to have information governance policies and trainings in place to account for the use of GAI tools across their business. This includes determining if the GAI-generated prompts and outputs are considered "records" and, if so, updating records retention policies and schedules accordingly. It is essential to have knowledgeable counsel who specialize in the discovery and governance of GAI information to ensure prompts and outputs are retained if/as needed.”

The warning comes as US courts are beginning to grapple with AI-generated evidence. In the 2024 case Tremblay v. OpenAI, a federal judge in California's Northern District ruled that AI prompts created by attorneys reflected their "mental impressions and strategies" and were protected from discovery, while ordering the production of prompts used to generate examples included in court filings.

Unique Preservation Challenges

Unlike traditional documents, AI-generated content presents novel preservation challenges because each tool operates differently in how it creates, stores, and manipulates data.

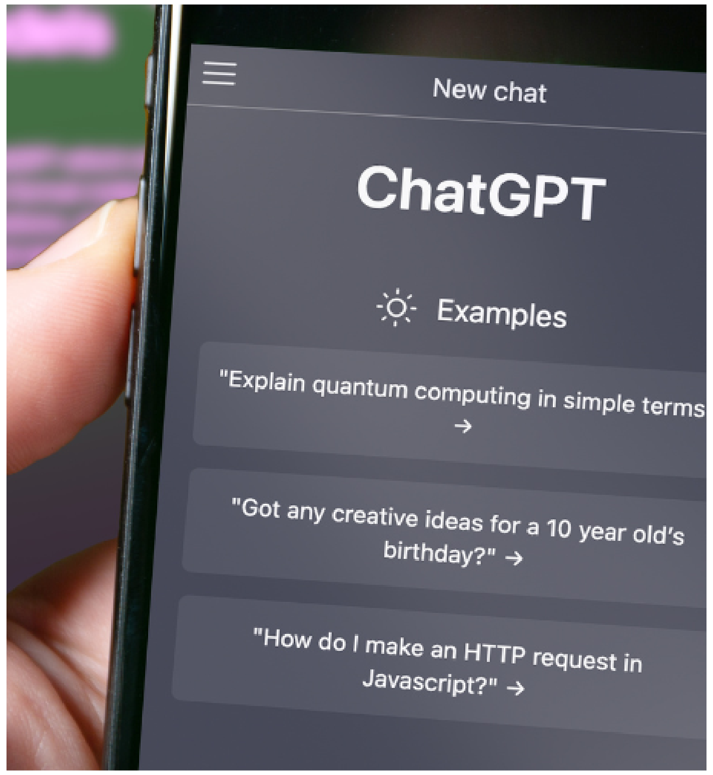
"An application that creates a bullet-point summary of a meeting typically begins by creating a transcript of that meeting, which it then analyses to produce a summary," the lawyers explain. "Will these documents be stored in the meeting organizer's online file storage, integrated into a corporate network, or distributed across the participants' storage?"

“How long will these records be retained? The answers will depend on both technical configurations and the organization's applicable retention policies.”

The lawyers emphasise that organisations cannot preserve relevant data without understanding where AI tools store information and how to retrieve it for discovery purposes.

Best Practices for AI Governance

The Morgan Lewis team recommends several best practices for organizations using AI tools:


New chat
ChatGPT
Examples
"Explain quantum computing in simple terms" →
"Got any creative ideas for a 10 year old's birthday?" →
"How do I make an HTTP request in Javascript?" →

Early Legal Involvement: "Legal and information governance professionals should be considered essential stakeholders to consult when an organization decides to deploy GAI tools," they write.

Understanding Data Flow: Organizations must investigate storage locations and understand what types of documents AI tools create before implementing them.

Policy Updates: Document retention policies may need to be updated to ensure that GAI-generated documents and data are retained for the appropriate duration based on business need and applicable law.

User Training: The lawyers stress that training is "critical" because AI tools can "hallucinate and generate documents and data that may not reflect reality."

"Any AI-generated output must be reviewed and verified before preservation - bullet points, summaries, transcripts, arguments and other GAI outputs must be carefully reviewed and confirmed," they warn.

Growing Legal Implications

The analysis underscores how rapidly AI adoption is outpacing legal frameworks. While generative AI tools have proliferated over the past two years, courts and litigants are only beginning to address their use and outputs in discovery.

"Documents and data created with GAI tools may be relevant to anticipated or ongoing disputes if they pertain to claims and defences and are proportional to the needs of the case," the attorneys note.

The legal experts conclude that organizations must take a "thoughtful and comprehensive approach" to AI integration, balancing the technology's benefits against emerging legal risks and obligations.

The full analysis is available here.

What should AI be doing with documents?

By Duff Johnson

In the 1990s, optical character recognition (OCR) got a lot of attention, enabling search engines to work on scanned documents, providing near-instant access to relevant content without laborious manual indexing. OCR's power was real, but it wasn't a panacea. Recognition errors led to misses or false positives.

These problems were eventually alleviated, in part, by additional software such as language identification and dictionary lookups to improve accuracy. But one fundamental problem was (and remains) harder to solve - complacency. The magic of OCR and search engines inspired far more trust in these systems than the results warranted, leading in some cases to costly mistakes.

Trust in extraordinary technology should not be blindly given, but a key lesson of the information age is that the easier the technology is to use the more readily it gets trusted, even if that trust isn't earned.

Although Artificial Intelligence (AI) is beginning to dramatically transform how users interact with and process documents, weaknesses remain. Even when the training data is tightly quality controlled, AI's results are not necessarily trustworthy.

Although AI is already assisting in authoring, data extraction, and content management, AI tools can only be as good as their inputs and training. If input data is biased, AI models are helpless to resolve - or even detect - the problem, a major source of AI hallucinations. Relying on AI for critical tasks should prompt far more due diligence than their ease of use implies.

It's not the AI's fault - it's what they are fed

While the vast majority of content available for training might be unstructured or poorly semantically structured, this doesn't mean that the semantic information it includes should be ignored.

When proper semantics are present in a document, such as with WAI-ARIA or Tagged PDF, this information becomes a far richer source of trusted knowledge for AI, whereas attempting to retrospectively guess can result in the familiar garbage-in-garbage-out (GIGO) problem.

If AI assistants helped creators to make richly structured documents - and if consuming AIs were equipped to leverage such enriched inputs, including associated machine-readable source data and provenance information, results would evolve to become more trustworthy.

However, document authoring tends to be oriented towards visual consumption, with unstructured or unreliably structured content. Yes, today's AI assistants can help recognise headings and paragraphs and apply these simple semantics for novice users, but the richer semantics of quotes, referencing, indexing, maths, illustrations, etc. do not get the same level of attention.

Even structured source information for tabular data (say, an Excel file) is commonly published in unstructured ways while the associated source data is rarely published at all.

This problem is less acute with HTML, as semantic structures are commonly integrated into the content, offloading the complexities of determining appearance to the browser. PDF is necessarily a more complex format than HTML because it's self-contained. That's why good-quality PDF files and a full PDF parser is essential to extracting anything useful from PDF.

The choice of parser matters, a lot. There are literally thousands of PDF parsers covering a vast array of applications and cases but only a relative few are truly competent at ingesting PDF content in all its variety.

If your parser doesn't support all versions of PDF, uses old Unicode or outdated CMaps, can't understand Tagged PDF, ignores annotations, doesn't process language markers, then inputs into AI will be biased accordingly.

How should AI be integrated for use with documents?

For creators, AI integration should focus on helping content creators to not only draft and refine their content but also to richly structure and contextualise it. Beyond recognising tables and lists and offering to structure them, authoring applications should:

■Identify quotations, and include the source (either visibly or as metadata);

■When pasting content, include the source (either visibly or as metadata);

■Recognise maths, and include MathML, even when equation editors are not used;

■Expose the AI's confidence in AI-generated alt text of images, and ask the author to review;

■Recognise abbreviations and acronyms (does "Dr." mean Doctor or Drive)?

■Suggest improvements to the document's structure and ensure appropriate document navigation;

■Ensure metadata, referencing and cross-referencing all remain meaningful to the content as it is edited;

■Recognise the intentions behind character formatting (are bold words emphasis or defined terms, etc.) and embed those semantics;

■Ensure hyphenation and whitespace is semantically indicated;

■Retain the semantics of common tools such as org-charts, flow-charts, and drawing tools (these are not just lines and words, but represent semantics!)

■In slide decks and document templates, ensure that page "chrome" is semantically identified;

■Ensure that generated PDF files include all this information via Tagged PDF, embedded and associated files, links to structured sources, document and object metadata, ARIA roles and C2PA and digital signatures for provenance and authentication.

At the bare minimum, born-digital documents created using AI assistants, regardless of format, should include the full range of accessibility features such as meaningful alternate text for images, logically arranged headings, and MathML for mathematical equations, to name a few.

They should also provide open data to support any graphs and charts. We already see some of these features today in various modern office suites, but the author-side AIs aren't (yet) necessarily assisting or prompting the authors to make all these enhancements.

As it happens, the exact same features necessary to support accessibility for users with disabilities can also greatly improve results in AI reuse and extraction scenarios. Authoring applications that provide AI writing support but do not thereafter generate Tagged PDF have only implemented half a solution (and are impeding all AIs that consume these documents in the future)!

On the consumption side

AI systems have a massive appetite for both data and computing resources and can consume vast troves of content from many types of systems across many different formats. With an estimated 3 trillion PDF documents on the planet, PDFs are a very attractive source of data.

Even so, AI developers often seem to lack "situational awareness" in terms of recognising when the data fed to their AI is correct and meaningful, and whether the ingestion tools they choose are simply up to the task. The choice of ingestion tool(s) drives the quality of results from content. Is your HTML parser understanding ARIA roles? Does your PDF parser process the full richness of PDF?

As a crude example, there are demonstrable live AI systems today that have "learned" mojibake and "understand" complete gibberish as a Slavic or Asian language! The root cause of such problems often lies in the use of inadequate and outdated technologies that do not support proper text and content extraction from PDF files.

Another approach seen too often is to "dumb everything down" as part of an attempt to support input from pure images of documents (TIFFs, JPEGs, etc). In this case, otherwise rich documents (including, but not limited to PDF) are simply rendered to pixels and then OCR-ed to achieve a form of "consistency" for consumption by the AI engine.

Not only is this computationally expensive, but all existing rich semantics and metadata is ignored and replaced by a guess from the OCR process.

Yet another very serious issue making bad headlines for AI systems arises from their unconsented consumption of Personally Identifiable Information (PII) and copyrighted content. This article doesn't address the ethical or legal issues except to point out that PDF (and other formats) support various means to identify and protect content including encryption, digital signatures, and well-defined metadata.

Conclusion

Today, most AIs are fed with lousy and/or dumbed-down data that contributes to bias and untrustworthy results - and this is all before the problem of malice. To become truly reliable, AIs need schemes for preserving rich semantics and data when they encounter it.

Duff Johnson is CEO of PDF Association. More info: pdfa.org

Agencies Face Critical Challenge to Modernize Legacy Systems: Report

Australian government agencies are spending 80% of their technology budgets maintaining outdated systems, significantly more than their counterparts in banking and finance, according to a new report released by OpenText.

The report, "*Retiring Legacy Applications and Databases: Proven Strategies for Government Agencies*," provides a blueprint for public sector organizations struggling with technology infrastructure that threatens cybersecurity, hampers service delivery, and prevents innovation.

"Government agencies across Australia are under increasing pressure to deliver faster, more secure, and citizen-centric digital services," said George Harb, Vice President-ANZ at OpenText. "This report provides a clear and practical blueprint for transitioning from outdated legacy systems to agile, future-ready platforms."

The findings come at a critical time for Australian public sector organizations. Recent high-profile incidents have highlighted the risks of maintaining outdated systems. The Royal Commission into Defence and Veteran Suicide found that prior to modernization efforts, half of the Department of Veterans' Affairs systems were considered at high risk of failure, with the agency dependent on "niche ICT skills to maintain many of its applications."

Tight Budgets Demand Strong Business Cases

With governments seeking to scale back digital projects and approving fewer major initiatives, agencies must present compelling business cases aligned with core government priorities, the report advises.

The report identifies four core government investment drivers that agencies should target: attending to neglected core services, managing government finances responsibly, anticipating future needs, and growing the economy.

"By retiring legacy systems, resources can be redirected to solutions that improve service delivery or reduce administrative overheads," the report states.

NSW Government Leading the Way

The NSW Government is highlighted as taking a proactive approach through its Whole of Government (WofG) initiative led by Digital NSW. The State of Legacy program offers valuable insights for agencies across Australia, with recommendations for standardizing legacy definitions, measuring impacts, prioritizing high-risk systems, and building skills in legacy and emerging technologies.

"NSW is at a turning point in its digital journey, and legacy technology, or outdated digital solutions, can be a challenge in this progress," the report quotes from NSW Government workshop materials.

Smaller Projects, Better Outcomes

The report strongly advocates for an iterative approach to modernization rather than "big bang" projects. This approach reduces risk, speeds up benefit delivery, and creates opportunities for smaller Australian businesses to participate in government digital transformation.

This recommendation is reinforced by findings from the recent Capability Review of Services Australia, which revealed that 62 percent of internal respondents identified ICT as a critical area for improvement. The review found that an iterative approach to transformation would better support agency objectives.

Modern Archiving Critical for Compliance

A key strategy identified in the report is the deployment of contemporary archiving solutions that help agencies comply with evolving privacy, security, and data management requirements.

Modern archiving solutions can integrate diverse information sources, preserve context, and provide advanced search functionality while maintaining high security standards. These capabilities are essential for agencies dealing with freedom of information requests, maintaining records compliance, and protecting sensitive information.

The report concludes with practical first steps agencies can take to begin their modernization journey, including creating or updating legacy system modernization strategies, developing comprehensive information and data management plans, securing stakeholder buy-in, and leveraging industry expertise.

The full report is available here.

Breaking the 80/20 Rule: Governments Can Escape From Legacy IT Traps

In an era where digital transformation is reshaping both public and private sectors, government agencies face unique challenges in modernizing their IT infrastructure. IDM asked George Harb, Vice President-ANZ at OpenText, what this new report on legacy systems reveals about government agencies' struggle with outdated technology, the risks they face, and strategies for successful modernization that balance fiscal responsibility with service delivery.

OpenText Vice President-ANZ, George Harb

IDM: Your report indicates that government agencies spend 80% of their budget running existing systems - substantially more than banking and finance sectors. What makes government IT infrastructure particularly vulnerable to this imbalance?

GH: This imbalance is a consistent pattern across the public sector, as we've observed through our engagement with all levels of government. It often comes down to scale, complexity, and compliance requirements. Systems in the past have been built bespoke, and as regulations have increased, it's become more difficult for agencies to identify modernization or transformation pathways due to the risks associated with information or systems they must manage.

The risks associated with government information systems have increased, adding to the complexity. In contrast, private enterprises have greater ability to decommission legacy platforms without the restrictions that typically constrain government organizations. That's why you see a disparate level of spending on legacy systems in government versus private sector.

IDM: The white paper outlines several risks of maintaining legacy systems, from cybersecurity vulnerabilities to compliance issues. Based on your conversations with Australian government agencies, which of these risks are most pressing right now?

GH: I think compliance and regulatory risk continues to evolve and increase. Whether it's obligations around privacy, Freedom of Information, or data retention, maintaining legacy systems to support these requirements becomes increasingly complex and expensive.

Many of these legacy systems present cybersecurity risks and vulnerabilities. The more an organization maintains disparate legacy platforms, combined with the departure of subject matter experts, the greater the likelihood these systems won't be maintained properly, creating openings for cybersecurity incidents.

IDM: The report recommends an "unassailable business case" approach aligned with core government investment drivers. Which of these four drivers - attending to neglected core services, managing finances responsibly, anticipating future needs, or growing the economy - have you found resonates most strongly with decision-makers?

GH: The two that have the biggest influence on each other, and which decision-makers often grapple with, are managing finances responsibly while ensuring they attend to neglected core services. Addressing these core services typically requires spending, particularly in areas like health, justice, and social support. The citizen experience can be heavily influenced by the technology being used.

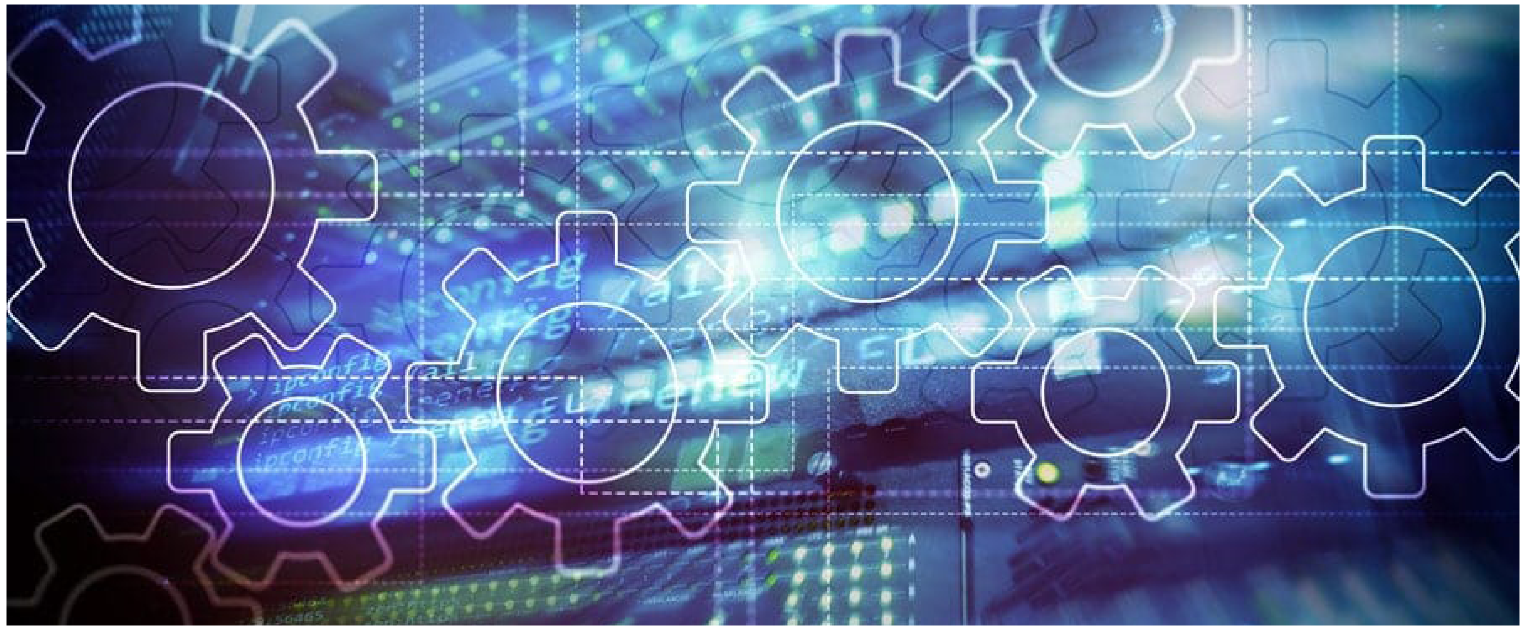
If that technology needs updating, the challenge becomes how to do it while managing finances responsibly. Your sustainment costs need to decline while your investment cost grows, ultimately reaching a point where your technology helps reduce long-term operational costs while still enabling service delivery. It's somewhat of a conflicting scenario, but both aspects are necessary to deliver the outcomes that government seeks.

IDM: You advocate for an iterative approach rather than "big bang" projects. What specific metrics should agencies use to measure success in these smaller, incremental modernization efforts?

GH: It comes down to three areas. First, reducing risk - understanding the existing risks and tracking how they're being addressed through the organization's risk register. Second, user experience uplift - measuring how internal or external users' experiences are being impacted by technological changes. Third, speed to benefit - governments are increasingly concerned with return on investment and how quickly benefits materialize from their investments.

In practical terms, an example would be tracking metrics like critical legacy applications being retired, measuring how that impacts employees' access to data and their ability to serve customers more quickly, and whether the project is being delivered on time. Those are what these metrics mean in layman's terms.

IDM: The NSW Government's State of Legacy program is highlighted as a model approach. What specific elements of this program do you believe other states and the federal government should adopt?



GH: The risk-prioritizing approach, strongly aligned with their overall whole-of-government architecture, is important. Aligning modernization with your strategy and technology roadmap is key.

The program emphasizes standardizing the legacy roadmap, clearly articulating the benefits of moving off legacy platforms, and enabling cross-agency collaboration to capture benefits more broadly. These elements are crucial for creating a legacy retirement or decommissioning plan that can be replicated from a framework perspective.

The structure needs to address questions like: Is it a cloud-first structure? Is it hybrid or modular? How does it align with whole-of-government architecture? That's ultimately where OpenText adds value - providing flexible options for governments to deploy according to their roadmap and whole-of-government architecture.

IDM: You mention that unnecessary encryption wastes capacity, drives up costs, and increases emissions. Can you quantify the environmental impact of poor data management practices in government IT?

GH: It's about eliminating redundant, obsolete, and trivial data. The more data you retain, the more compute power and servers you need, and consequently, the more power required to run those servers.

The more you can consolidate and simplify, the more you reduce costs and enhance performance, while ensuring agencies and users get the information they need quickly. That's how environmental impact can be influenced - by thinking strategically about reducing that footprint.

IDM: Government budgets are tightening, with fewer major digital initiatives being approved. How has this affected the conversations you're having with agencies about modernization?

GH: There's absolutely a shift toward cost justification and value-for-money assessments. Agencies are looking at ways to share infrastructure, leverage cloud environments, and implement multi-SaaS environments that still meet security and regulatory requirements.

Everyone recognizes the need to modernize and understands that modernization impacts how government works. They're seeking low-risk, modular approaches and solutions that can complement current operations while providing a roadmap for future modernization phases. That's where most of our conversations with government agencies are focused.

IDM: The report mentions government employees expecting modern tools similar to what they use in daily life. How significant is this workforce expectation as a driver for modernization compared to other factors?

GH: You want to attract and retain good staff while also appealing to the next generation of workers. Modernization is key, whether in enterprise or government, as driving a better employee experience directly links to employee satisfaction.

The expectation for modern tools exists, and government departments should recognize this as one of the key reasons for modernization - to improve employee experience, help with retention, and ultimately impact customer experience, as the two are clearly linked.

IDM: AI adoption is highlighted as a future need that legacy systems might hinder. How are forward-thinking government agencies preparing their data infrastructure specifically for AI implementation? And how can OpenText help?

GH: Everyone we talk to agrees they need to understand their data and prepare it for eventual wider AI adoption. That's the challenge - to create an AI experience that minimizes errors and "dirty data" requires significant effort, including a proper data governance plan and teams implementing the right algorithms and learning models to augment how employees work today.

The difficulty isn't primarily technological; it's taking the time to assess what you have, what you need, what to retain, and what to discard. This is where a strong enterprise archiving platform helps, enabling organizations to manage legacy information properly going forward.

It's also about having the right content and data management experience - the right platforms, policies, processes, and workflows. If these aren't in place, organizations need to address them through adopting complementary solutions or making wholesale changes to their approach.

It's a significant challenge that requires time, thought, and ultimately a forward-looking plan to fully leverage AI in today's work environment.

Data Readiness Blocks Public Sector AI

Public sector organizations worldwide are rushing to embrace artificial intelligence but lack the foundational data capabilities needed to succeed, according to comprehensive new research that surveyed 350 government agencies across six continents.

The Capgemini Research Institute study exposes a stark disconnect between governmental AI aspirations and execution capabilities. While nine in ten public sector organizations plan to explore agentic AI within the next 2-3 years, fewer than 25% report having the data maturity required to harness AI effectively.

The research reveals that 64% of public sector organizations are already exploring or actively working on generative AI initiatives. Defence agencies lead adoption at 82%, followed by healthcare (75%) and security (70%). However, only 21% have progressed to pilots or deployment stages, and merely 6% have successfully put Gen AI into production.

The data readiness gap is particularly pronounced. Only 21% of surveyed organizations possess the required data to train and fine-tune AI models, while just 12% consider themselves mature in activating data for decision-making.

Australian Government Implementation

Several Australian government agencies demonstrating were cited for successful AI deployment. The Australian Taxation Office (ATO) has leveraged AI to detect $A530 million in unpaid taxes, halt $A2.5 billion in fraudulent claims, and achieve a 90% success rate in identifying superannuation underpayments.

The Australian Federal Police (AFP) has also embraced AI technology, using it to detect deepfakes and problematic content as part of their digital forensics capabilities.

“Data security, privacy, and timely data activation are all critical for public sector organizations,” said Abhijit Gupta, Chief Technology Officer at Environment Protection Authority Victoria (EPA), Australia.

“A secure, modern, scalable, cloud-based infrastructure provides the appropriate foundations for developing this capability. Developing skills across the organization is vital, particularly for business users who need to interact with the data regularly.”

Gupta emphasized the importance of specialized training: “This may include training in prompt engineering and other specialized skills to enable users to effectively access data and generate business value from its use. Finally, strong AI governance will ensure AI models are free from bias, risks have been considered, and data security and privacy are safeguarded.”

Major Barriers to AI Implementation

The study identifies several critical obstacles preventing successful AI deployment:

■ **Security and Trust Concerns:** Data security issues top the list of barriers, cited by 79% of organizations, while 74% express limited trust in AI-generated outputs. These concerns stem from the need to protect sensitive citizen data and ensure AI system accuracy and fairness.

■ **Data Sovereignty Issues:** A significant 64% of organizations express concern about data sovereignty, with 58% worried about cloud sovereignty and 52% about AI sovereignty. This reflects governments’ desire to maintain control over their digital infrastructure and data.

■ **Budget and Infrastructure Limitations:** Some 65% cite budget constraints as a significant barrier, while 77% point to the lack of modern, scalable infrastructure. Only 41% can access data at the speed required for decision-making.

Despite challenges, governments are investing heavily in data and AI leadership. The research shows that 64% of organizations already have a Chief Data Officer (CDO), with another 24% planning appointments. Similarly, 27% have appointed Chief AI Officers (CAIOs), while 41% plan to introduce this role.

“There is a strong focus on data and AI, especially with numerous central government announcements about transforming public sector services through AI,” said Gurpreet Muctor, Chief Data and Technology Officer at Westminster City Council, UK.

“Excellent data management and governance are essential at both local and national government levels.”

Regional Variations and EU Compliance

The study reveals significant regional differences in AI adoption. US government agencies are leading with 72% exploring or piloting Gen AI initiatives, compared to 55% in Europe. The Asia-Pacific region, which includes Australia, represents 14% of the total sample and shows strong practical implementation examples.

However, only 36% of EU-based organizations feel confident about complying with the EU AI Act, despite higher confidence levels for other data regulations.

National agencies outperform local ones, with 76% exploring Gen AI compared to 52% at the local level, suggesting budgetary constraints limit smaller agencies’ AI adoption capabilities.

Data Sharing Challenges Persist

Cross-organizational data sharing remains problematic. While all surveyed organizations either have or plan data sharing initiatives, 65% are still in planning or pilot stages. Only 35% have rolled out or fully deployed data sharing programs, with just 8% achieving full deployment.

“It has become an undeniable truth that very few public sector actors have all the data they need to maximize their AI and data usage potential,” said Peter Kraemer, Director of Data Sovereignty Solutions at Capgemini.

The study recommends a three-pronged approach for bridging the AI ambition-execution gap:

■ **People-Centred Initiatives:** Organizations should ensure clear vision and leadership, foster data-driven culture, and nurture analytical skills, especially among business users.

■ **Process Reinvention:** This includes implementing strong data governance with responsible AI practices and focusing on gradual data landscape modernization.

■ **Technology Foundation:** Investment in robust cloud-based data infrastructure and ensuring interoperability of data and IT systems.

Download the Report here.

"SignalGate" Exposes Critical Gap in Government Records Management

Ephemeral messaging apps are creating significant records management challenges for government agencies and regulated organizations, according to a new report published by the Association for Intelligent Information Management (AIIM).

The report, titled "*When Messages Self-Destruct: The Hidden Risks of Ephemeral Communication for Information Governance*," examines a recent high-profile incident where senior U.S. officials inadvertently invited a journalist into their encrypted Signal group chat containing sensitive military operations details.

Report author John Newton, co-founder of Documentum and Alfresco, describes this "SignalGate" incident as "a wake-up call about the challenges of preserving institutional memory in the age of disappearing messages."

The report emphasizes that while apps like Signal, WhatsApp, and Telegram offer privacy benefits through end-to-end encryption and self-destructing messages, they create major obstacles for proper records management.

"This is great for privacy – but for records management, it's a nightmare," Newton writes. "Traditionally, a 'record' meant an email, memo, or document filed away for future reference. Now, a fleeting chat message might contain a key decision or directive."

"But when an app makes it so easy to bypass the file cabinets (so to speak), it's a recipe for records disappearing. Ephemeral media are redefining how we think about records, forcing records managers to catch up with what "a record" means in 2025."

Newton points out in his white paper, "For leaders in government and regulated industries, the lesson is that we must evolve our practices to meet this reality, without abandoning the principles of accountability. It's not an either/or choice between using secure messaging and maintaining records – it's about finding a way to do both."

The analysis points out that US regulations require federal employees using non-government messaging systems to promptly forward or copy their communications to official accounts. However, ephemeral messaging apps make it easy to bypass these requirements, whether intentionally or through simple convenience.

The Australian Information Commissioner recently found that Australian federal government agencies are regularly using phone-based messaging apps without adequate policies to ensure they meet their legal obligations.

Newton identifies two primary reasons officials use these platforms: convenience in fast-moving situations and deliberate evasion of oversight.

The report cites examples including Homeland Security officials whose text messages from January 6, 2021, were inaccessible due to auto-delete features, and financial industry regulators finding bankers "covertly texting" about trades to avoid compliance monitoring.

To address these challenges, the report recommends organizations implement technological solutions like communications surveillance tools, update policies to explicitly address ephemeral messaging, conduct regular audits, and create accountability measures. It also stresses the importance of leadership modelling proper behaviour.

"Don't get caught thinking a disappearing message leaves no trace," Newton warns. "It might not leave a trace in the app, but it will leave a mark on your organization – for better or worse."

"Vendors in the information management space report an uptick in inquiries from public agencies wanting to retain data from chat apps and collaboration tools .

"This is a positive sign: it means organizations are recognizing the issue and looking for technical fixes to bridge the gap between modern messaging and traditional archiving."

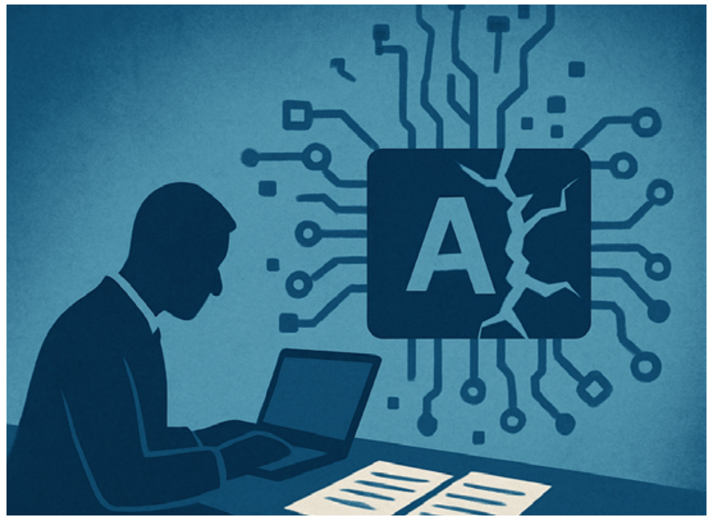
As government agencies and regulated industries continue adopting new communication technologies, Newton concludes that the core principles of transparency, accountability, and compliance must be maintained, even as the tools evolve: "The tools may change, but our duty to maintain a truthful record endures."

"Transparency, accountability, and compliance are cornerstones that organizations must uphold, even as the channels we use transform. The recent Signal fiasco underscores that neglecting those values – even accidentally – can lead to serious breaches of trust and legal peril.

"Conversely, those organizations that adapt and reinforce their records management in creative ways will not only avoid scandals, they'll be stronger and more trusted for it."

Global Survey reveals Data Quality Dilemma

In today's data-driven economy, the gap between organizations effectively managing their information assets and those struggling with data integrity continues to widen dramatically. New research from information management giant Iron Mountain reveals Australian companies are both benefiting from good data practices and paying a steep price for poor ones.



The comprehensive study of 500 large organizations worldwide found that Australian companies are particularly focused on extracting better insights from their data, with 50% identifying this as their top strategic priority - significantly outpacing global counterparts including the United Kingdom (44%) and United States (39%). This intensified focus appears justified, as data integrity flaws cost organizations an average of $A493,000 over the past year, contributing to a staggering $A22 billion global loss. For Australian firms, the consequences are especially severe, with 48% reporting lost competitive advantage from poor data - the highest percentage among all markets surveyed and substantially above the 29% global average.

Despite these challenges, Australian organizations are seeing remarkable returns when they get data management right. An impressive 84% of Australian respondents reported revenue and profitability growth directly attributable to their information management practices, contributing to what researchers call a "good data dividend" worth $A115 trillion globally.

"With the rise of open-source and specialized AI models, data integrity, transparency and trust are more critical than ever," said Narasimha Goli, Chief Technology Officer at Iron Mountain.

"At Iron Mountain, we are investing in solutions such as our Iron Mountain InSight Digital Experience Platform (DXP) to help our customers get their information ready for use in generative AI and other AI-powered applications.

"This enables organisations to illuminate dark, unstructured data by automating the processes for extracting and organising metadata at speed and scale, and with a high degree of accuracy.

"By leveraging technology like this to ensure their data is being sourced responsibly, organisations can harness the full potential of their information to drive intelligent decision-making and unlock new growth opportunities."

The research identified a clear blueprint from leading organizations that are successfully navigating the AI frontier. These top performers universally implement processes for eliminating redundant, obsolete or trivial (ROT) and automating data extraction, while 96% use AI dashboards to explain outcomes and data lineage to non-technical stakeholders. However, significant hurdles remain. Workforce AI literacy emerged as a major concern for 42% of Australian organizations - substantially higher than the global average of 28%. This skills gap threatens to undermine otherwise promising AI initiatives.

Half (50%) of Australian organisations surveyed say improving data insight extraction will be key to achieving their strategic ambitions over the next 12 months – making it the most cited focus area in the country. This is 37% higher than the global average, and surpasses countries such as the United Kingdom (U.K.) (44%) and the United States (U.S.) (39%).

Over a third of respondents (36%) identified AI-ready data as the information management focus area that will have the greatest impact on achieving their organisation's strategic ambitions over the next 12 months.

Download the Executive Summary report

Australia Laser Focussed on Data Integrity

New research from information management giant Iron Mountain reveals Australian companies are both benefiting from good data practices and paying a steep price for poor ones. IDM asked Greg Lever, Iron Mountain's Senior Vice President, Asia-Pacific what the survey revealed about the local market.

Iron Mountain's Senior Vice President, Asia-Pacific,Greg Lever

IDM: The research reveals Australian organisations are prioritizing data insight extraction 37% higher than the global average. What unique factors in the Australian business landscape are driving this stronger focus on data utilisation?

GL: The research we commissioned shows that 50% of large Australian organisations are placing greater focus on improving data insight extraction to help them achieve strategic goals over the next 12 months. Australia's strong business culture around digital transformation, together with government initiatives that support data-driven decision-making, further fuel this focus. For businesses of any size - from large enterprises to the small businesses and start-ups that make up much of Australia's business landscape - innovation and actionable data insights are critical to maintaining a competitive edge.

IDM: Your study found that AI literacy is a top challenge for 42% of Australian businesses—significantly higher than the global average of 28%. What specific skills gaps are you observing in the Australian workforce, and how might this impact the country's AI competitiveness?

GL: Australia's skills gap is a well-known, ongoing business issue. For AI, businesses attribute the source of this issue as lack of advanced technical knowledge, insufficient training in AI tools and limited understanding of AI ethics and applications. Often these gaps create obstacles to the effective implementation of AI initiatives, reducing Australia's global competitiveness. Addressing these gaps through targeted education and training will be crucial for enhancing AI literacy and ROI from businesses' investments in these emerging technologies.

IDM: Nearly half of Australian organisations (48%) identify loss of competitive advantage as the main consequence of data integrity flaws - the highest among markets surveyed. Why do you think Australian businesses are particularly sensitive to this risk compared to other regions?

GL: It's around 19% higher than the global average of 29% - Australian businesses are highly sensitive to data integrity issues due to their reliance on accurate data as part of strategy development, decision-making and innovation initiatives. The highly competitive market and regulatory environment further amplifies the impact of data flaws on business performance. Australia, for example, has a high cost for data breaches, and the need for compliance due to stringent data protection regulations contributes to this heightened sensitivity.

IDM: The research indicates organisations globally gained an average revenue growth of A$3.4 billion from effective information management. Are Australian companies seeing comparable financial benefits, or are there differences in the "good data dividend" here?

GL: Australian companies are indeed seeing comparable financial benefits, with 84% reporting revenue and profitability growth when information management practices are governed well. This aligns closely with the global average, highlighting the universal value of good data management. The focus on leveraging data for competitive advantage and innovation drives these financial gains. The 'good data dividend' equated to a total average global revenue gain of A$115 trillion.

IDM: While 92% of Australian organisations report benefits from AI readiness strategies, 58% admit their AI initiatives lack consistency. What are the main stumbling blocks preventing more systematic implementation?

GL: Inconsistent data quality, lack of standardised processes, and insufficient integration of AI tools across business functions are the key stumbling blocks for Australian businesses. Addressing these issues requires a more cohesive approach to AI strategy and implementation, and getting your data in order is number one. Businesses can then leverage tools like Iron Mountain's Digital Experience Platform (DXP) to ensure that data is not only secure and compliant, but also accessible and actionable.

IDM: Your research identified "leaders" with exemplary AI-ready data practices. How do Australian organisations compare to these global leaders, and what specific areas should they prioritise to close any gaps?

GL: The key focus areas for Australian organisations are eliminating redundant, obsolete and trivial (ROT) data, automating data extraction, and using AI dashboards for transparency to build AI-ready data resources. Prioritising these areas will help close gaps with global stakeholders: 96% of "leaders" are using AI dashboards to explain outcomes and data lineage to non-technical stakeholders. Investing in advanced data management tools and fostering a data-driven culture are also essential steps.

IDM: The report mentions organisations lost approximately A$493,000 over the past year due to data integrity flaws. What are the most common data integrity issues you're seeing in Australian businesses, and how can they be addressed?

GL: Data integrity flaws have led to an approximate A$22 billion average loss globally according to our research with common issues including duplicate data, outdated information, and lack of proper data governance. Addressing these requires implementing robust data management practices, regular audits, and leveraging AI tools for data accuracy. Establishing clear data governance frameworks and training employees on best practices can also mitigate these issues, not least using software which helps keep your data in check.

IDM: How are regulatory differences in Australia affecting organisations' approach to responsible AI and data management compared to other markets like the U.S. or EU?

GL: Australia's regulations around data management emphasise privacy and data protection, which in turn impacts how businesses locally approach AI and data management. Compared to the U.S. and EU, Australian regulations require more stringent compliance which has a direct influence on data handling practices, which in turn results in a greater focus on ethical AI and transparency in Australia. For example, the Privacy Act locally sets clear rules for business requirements in managing and protecting personal information.

IDM: Looking ahead, what timeline do you envision for Australian businesses to overcome their AI literacy challenges, and what role does Iron Mountain plan to play in supporting this transition?

GL: Close to all (92%) Australian organisations are aware that AI readiness strategies have benefited their companies to date, but our research also finds that 42% of Australian organisations view AI literacy as a major barrier – well above the global average – and upskilling our workforce is now an urgent need which even with focused efforts, could take three to five years to achieve.

Iron Mountain is actively supporting this transition through its InSight DXP platform which helps businesses structure and prepare data for AI, while also guiding on responsible data practices and offering strategic insights for sustainable AI adoption.

What Librarians Know About Organizing Information (That Tech Should Borrow)

The Royal Library of Ashurbanipal, named after Ashurbanipal, the last great king of the Assyrian Empire, is a collection of more than 30,000 clay tablets and fragments containing texts of all kinds from the 7th century BC.

Librarianship is over 4,000 years old—we've been building systems to make knowledge usable since the Library of Ashurbanipal. (That's clay tablets, not cloud drives.) And weirdly enough, a lot of what worked back then still works now.

Whether you call it knowledge management, content strategy, or just "trying to get SharePoint under control," the core problem is the same: how do we make information findable, usable, and not overwhelming?

If your team's knowledge base feels more like a junk drawer than a resource anyone trusts, here's what librarians—and knowledge managers—tend to get right.

1. Organize around how people search, not how creators file

People rarely remember file names or folder paths. They remember vibes. "That one slide deck from early spring 2023," or "the doc with the blue graph." Librarians plan for this.

We build systems that support multiple ways in—keywords, subjects, filters, context clues. Because the goal isn't just to store information. It's to help people actually find it.

KM principle: User-centered design. Organize it based on how people think—not how it looked in your project folder.

2. Use consistent, human-friendly tags and vocabularies

Tags are only helpful if everyone uses the same ones. Otherwise, you end up with "hiring," "recruitment," "staffing-docs," and "old resumes" all pointing to the same thing—sort of. Librarians avoid this mess by using shared, standardized vocabularies. It's not fancy. It just works.

KM principle: Governance. A system only works if people speak the same language—literally and structurally.

3. Build for discovery, not just storage

Uploading documents isn't knowledge management. Making it easy for someone to stumble into the right thing at the right time—that's where the magic is.

Good systems support browsing, related content, context cues, and next steps. Librarians think in paths, not just piles.

KM principle: Findability. If no one can find it, it doesn't exist.

4. Maintain it like a garden—weeding never stops

Every content system eventually turns into digital clutter—unless someone plans for maintenance. Librarians do. We build in review cycles. We retire outdated stuff. We check links.

Yes, we even get rid of books. Not because they weren't good—but because we know that clarity, trust, and usefulness depend on letting go of what no longer serves.

There's no final form. You just keep it tidy enough to be useful.

KM principle: Lifecycle management. Content has a shelf life. Make room for pruning.

What's the Takeaway?

■The tools may change.

■The platforms may get flashier.

■But the people who know how to structure, label, and sustain useful information?

■We've been here the whole time.

If your SharePoint site is more confusing than helpful, maybe don't reinvent the wheel.

Just ask a librarian.

Originally published here.

Southeast Asia’s Cyber-Scam Industry Booms, Triggering Global Alarm

A report by the United Nations Office on Drugs and Crime (UNODC) has uncovered the dramatic expansion of the cyber-scam industry in Southeast Asia, revealing a complex web of transnational organized crime that’s generating tens of billions of dollars in illicit profits annually.

The report, titled “*Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia*,” paints a disturbing picture of an industry that has rapidly evolved from scattered fraud operations to sophisticated, large-scale criminal enterprises.

These syndicates, according to the UNODC, often operate under the guise of legitimate businesses, infiltrating sectors such as industrial and science and technology parks, casinos, and hotels. The industry’s growth is fuelled by massive illicit capital inflows, with criminals exploiting gaps in governance and regulations across the region.

This exploitation has led to the proliferation of scam centres, particularly in the Mekong subregion, which has become a breeding ground for these criminal networks.

The report highlights the syndicates’ ability to quickly adapt and adopt new technologies to facilitate their crimes. These include including blockchain, cloud computing, generative artificial intelligence, and machine learning, among others, and sophisticated online platforms that function as illicit online marketplaces.

These platforms provide other criminals with the tools and services necessary for cyber fraud, money laundering, and other illicit activities.

“As a growing number of governments intensify their efforts against cyber-enabled fraud and scam centres in the region, organized crime has responded by hedging both within and beyond it,” the report concludes

“It is now increasingly clear that a potentially irreversible spillover has taken place in Southeast Asia, leaving criminal groups free to pick, choose, and move jurisdictions, operations, and value as needed, 3 Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia with the resulting situation rapidly outpacing the capacity of governments to contain it.

“More than this, the region has emerged as a key testing ground for organized crime, which is reflected in increasing linkages to criminal ecosystems in other parts of the world facing similar vulnerabilities and challenges.

The problem extends far beyond Southeast Asia, with the report detailing the increasing presence of these crime networks in Africa, the Pacific Islands, South America, and other regions.

In the United States alone, authorities reported more than $US5.6 billion in financial losses to cryptocurrency scams in 2023, with an estimated $US4.4 billion attributed to so-called ‘pig butchering’ schemes most prevalent in Southeast Asia.

This global expansion has allowed the syndicates to target a wider range of victims, increase their illicit profits, and establish a stronger foothold in the international criminal landscape.

Key Findings of the Report:

Operational Adaptation and Evolution: Cyber-enabled fraud and scam centres have taken on industrial proportions, driven by billions in illicit capital.

Geographic Shifts and Spillover: Crime networks are expanding beyond Southeast Asia, exploiting vulnerabilities in other regions.

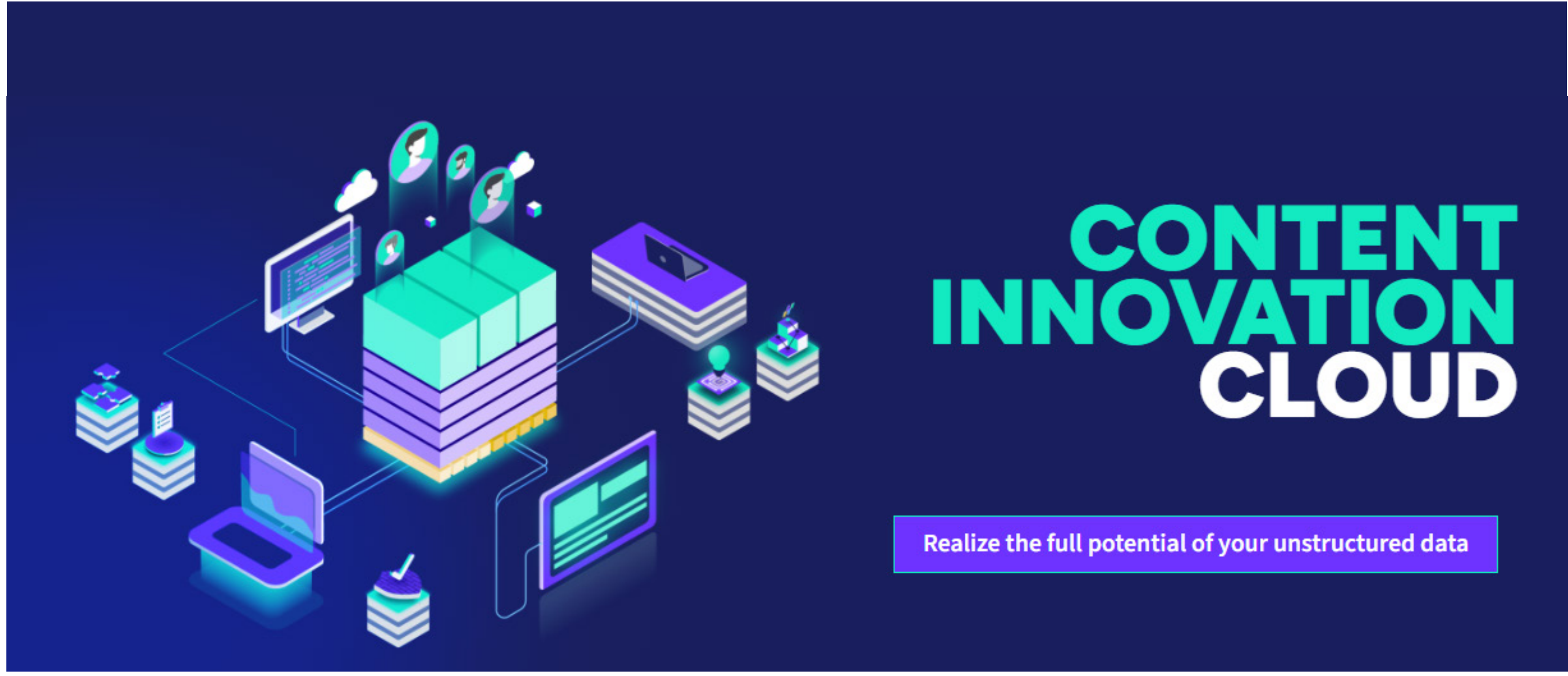
Emergence of Illicit Online Marketplaces: Platforms like Huione Guarantee (Haowang) have revolutionized transnational organized crime, providing a marketplace for fraud tools and services.   Headquartered in Phnom Penh, Cambodia, the predominantly Chinese language platform has grown to more than 970,000 users and has “become a one-stop-shop for illicit actors sourcing the technology, infrastructure, data, and other resources needed to conduct cyber-enabled fraud and cybercrime, as well as large-scale money laundering and sanctions evasion,” according to the report.

Integrated Money Laundering Services: These platforms often include integrated cryptocurrency and other financial services, further complicating efforts to track and disrupt illicit financial flows.

The UNODC report calls for urgent and coordinated international action to address this escalating crisis. It emphasizes the need for increased awareness, improved policies, enhanced capacity building, strengthening regulatory frameworks and stronger cooperation between countries in Southeast Asia and their international partners.

The report warns that failure to take decisive action will have “unprecedented consequences,” allowing these crime syndicates to further entrench themselves and expand their operations globally.

The UNODC report is available here.



Most people use AI regularly at work but global survey finds concerns

By Nicole Gillespie and Steven Lockey, Melbourne Business School

Have you ever used ChatGPT to draft a work email? Perhaps to summarise a report, research a topic or analyse data in a spreadsheet? If so, you certainly aren't alone.

Artificial intelligence (AI) tools are rapidly transforming the world of work. Released today, our global study of more than 32,000 workers from 47 countries shows that 58% of employees intentionally use AI at work – with a third using it weekly or daily.

Most employees who use it say they've gained some real productivity and performance benefits from adopting AI tools.

However, a concerning number are using AI in highly risky ways – such as uploading sensitive information into public tools, relying on AI answers without checking them, and hiding their use of it.

There's an urgent need for policies, training and governance on responsible use of AI, to ensure it enhances – not undermines – how work is done.

Our research

We surveyed 32,352 employees in 47 countries, covering all global geographical regions and occupational groups.

Most employees report performance benefits from AI adoption at work. These include improvements in:

- efficiency (67%)
- information access (61%)
- innovation (59%)
- work quality (58%).

These findings echo prior research demonstrating AI can drive productivity gains for employees and organisations.

We found general-purpose generative AI tools, such as ChatGPT, are by far the most widely used.

About 70% of employees rely on free, public tools, rather than AI solutions provided by their employer (42%).

However, almost half the employees we surveyed who use AI say they have done so in ways that could be considered inappropriate (47%) and even more (63%) have seen other employees using AI inappropriately.

Sensitive information

One key concern surrounding AI tools in the workplace is the handling of sensitive company information – such as financial, sales or customer information.

Nearly half (48%) of employees have uploaded sensitive company or customer information into public generative AI tools, and 44% admit to having used AI at work in ways that go against organisational policies.

This aligns with other research showing 27% of content put into AI tools by employees is sensitive.

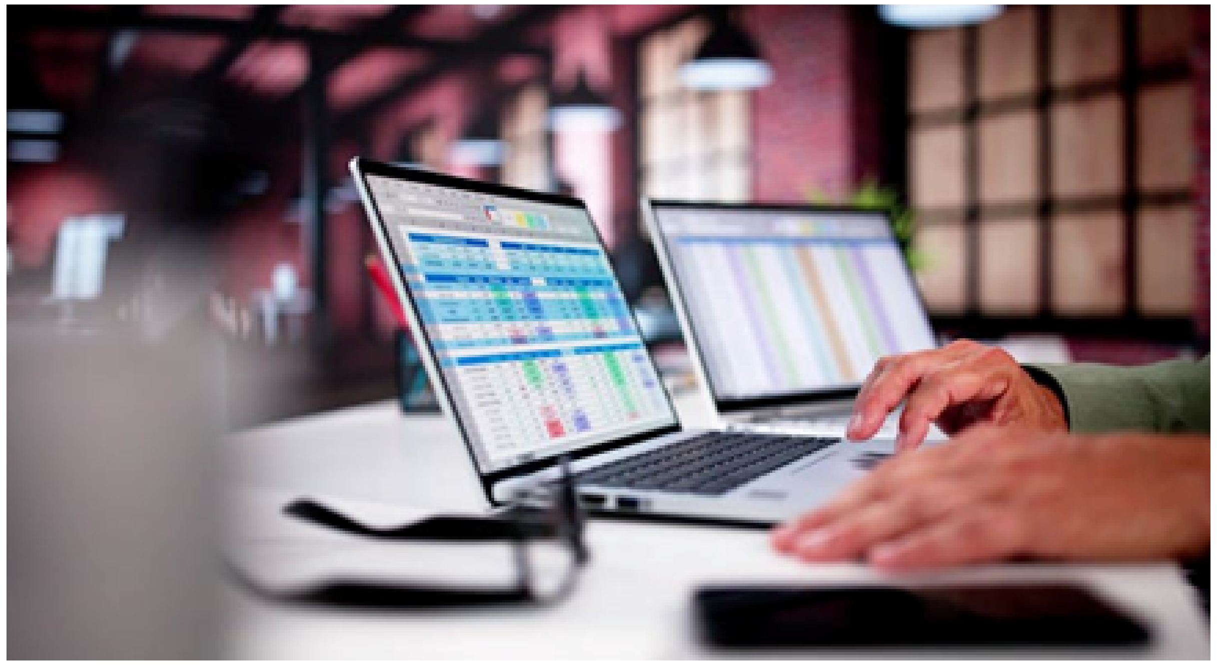
Check your answer

We found complacent use of AI is also widespread, with 66% of respondents saying they have relied on AI output without evaluating it. It is unsurprising then that a majority (56%) have made mistakes in their work due to AI.

Younger employees (aged 18-34 years) are more likely to engage in inappropriate and complacent use than older employees (aged 35 or older).

This carries serious risks for organisations and employees. Such mistakes have already led to well-documented cases of financial loss, reputational damage and privacy breaches.

About a third (35%) of employees say the use of AI tools in their workplace has increased privacy and compliance risks.



Almost half of respondents who use AI said they had uploaded company financial, sales or customer information into public AI tools. Andrey_Popov/Shutterstock

'Shadow' AI use

When employees aren't transparent about how they use AI, the risks become even more challenging to manage.

We found most employees have avoided revealing when they use AI (61%), presented AI-generated content as their own (55%), and used AI tools without knowing if it is allowed (66%).

This invisible or "shadow AI" use doesn't just exacerbate risks – it also severely hampers an organisation's ability to detect, manage and mitigate risks.

A lack of training, guidance and governance appears to be fuelling this complacent use. Despite their prevalence, only a third of employees (34%) say their organisation has a policy guiding the use of generative AI tools, with 6% saying their organisation bans it.

Pressure to adopt AI may also fuel complacent use, with half of employees fearing they will be left behind if they do not.

Better literacy and oversight

Collectively, our findings reveal a significant gap in the governance of AI tools and an urgent need for organisations to guide and manage how employees use them in their everyday work. Addressing this will require a proactive and deliberate approach.

Investing in responsible AI training and developing employees' AI literacy is key. Our modelling shows self-reported AI literacy – including training, knowledge, and efficacy – predicts not only whether employees adopt AI tools but also whether they critically engage with them.

This includes how well they verify the tools' output, and consider their limitations before making decisions.

We found AI literacy is also associated with greater trust in AI use at work and more performance benefits from its use.

Despite this, less than half of employees (47%) report having received AI training or related education.

Organisations also need to put in place clear policies, guidelines and guardrails, systems of accountability and oversight, and data privacy and security measures.

There are many resources to help organisations develop robust AI governance systems and support responsible AI use.

The right culture

On top of this, it's crucial to create a psychologically safe work environment, where employees feel comfortable to share how and when they are using AI tools.

The benefits of such a culture go beyond better oversight and risk management.

It is also central to developing a culture of shared learning and experimentation that supports responsible diffusion of AI use and innovation.

AI has the potential to improve the way we work. But it takes an AI-literate workforce, robust governance and clear guidance, and a culture that supports safe, transparent and accountable use.

Without these elements, AI becomes just another unmanaged liability.

Nicole Gillespie is Professor of Management; Chair in Trust, Melbourne Business School and Steven Lockey, Postdoctoral Research Fellow, Melbourne Business School, This article is republished from The Conversation under a Creative Commons license. Read the original article.

GenAI a growing threat to information systems

Research in the rapidly expanding field of artificial intelligence is not only focused on the development of innovative new models and efforts to reduce the carbon footprint of GPUs: AI has also created a host of new opportunities for cyber criminals and a wide range of challenges for cybersecurity experts.

Among the research teams who are already at work on systems to combat ill-intentioned hackers, scientists at Los Alamos National Laboratory recently presented a ground-breaking defence method to shield AI from adversarial attacks, which make use of near-invisible tweaks to data inputs that can fool models into making incorrect decisions.

"It is not unusual to see hackers who aim to make malicious use of generative AI exchanging information on models and tactics on dark web networks," points out Vivien Mura, Global CTO for Orange Cyberdefense.

Reports on artificial-intelligence vulnerabilities are also alarming: according to a May 2024 survey conducted by the Capgemini Research Institute, 97% of organizations had encountered breaches or security issues related to the use of GenAI in the preceding 12 months.

New risks have emerged, notably data leaks caused by employees who unwittingly upload information to GenAI tools

How hackers make use of generative AI

Generative AI can accelerate several aspects of hacking including the production of malicious code.

"It can expedite the work of reconnaissance ahead of the launch of an attack by collecting data that enables hackers to determine the ideal point of entry, that is to say an individual within a company who has permission to access sensitive data and a suitably vulnerable profile," said Mura.

Along with shorter timeframes for the preparation of attacks, "New risks have emerged, notably data leaks caused by employees who unwittingly upload information to GenAI tools."

Last but not least, there are risks inherent in the configuration of services for artificial intelligence: "AI users do not control the entire chain of third-party suppliers, hosting providers and application developers must also take charge of their responsibilities."

With multi-agent systems deployed over interfaces that are not fully standardised, agentic AI may also be targeted: "System interfaces inevitably have vulnerabilities that can be exploited to hijack AI agents for malicious purposes."

"There is a growing likelihood of attacks that aim to steal models and context information memorised in response to user prompts, because they contain more and more sensitive data," said Mura.

Big Tech’s Information Management Crisis: Why US Solutions Don’t Work

By Scott Brown

The fundamental divide between US and Australian approaches to records management means that information Management solutions that come out of the US (i.e. Microsoft) cannot be taken seriously by Australian Government and regulated industries

Information falls into two categories: structured data (databases with specific functions) and unstructured data (everything else: Office documents, emails, network files, SharePoint content). While structured data largely manages itself, unstructured data requires deliberate organization.

In Australia, Electronic Document and Records Management Systems (EDRMS) solve this by structuring unstructured data through systematic container titling based on the AFDA Express V2 classification system, organizing information by Function-Activity-Descriptor.

The AFDA is issued by National Archives for Federal Government. State Governments and Territories create their own Retention and Disposal Schedules.

American information management fundamentally differs from Australian practices. We discovered this in the late 90s when I was working at TOWER Software, making and implementing TRIM (Content Manager – an EDRMS). Americans practice document management, not records management.

They would pass documents around, attach further documents to the original document if necessary, and when finished, put the documents in a box. Finding information was called the “paper-chase”, not “where is the File”. With the evolution to electronic document management, the concept remained the same and they workflow individual electronic information.

This cultural difference persists today. US companies have no concept of managing information at the collection level, creating what industry experts call “information chaos.”

Microsoft SharePoint: A Recipe for Disaster

SharePoint exemplifies these problems through three mechanisms:

- **Folder Proliferation:** The Windows Explorer paradigm creates confusing “rabbit holes” that only make sense to their creators, who may leave the organization over time.
- **Security Fragmentation:** Each folder requires individual access permissions, violating corporate information governance and creating orphaned content when staff depart.
- **Uncontrolled Sprawl:** Anyone can create new SharePoint or Teams sites with custom permissions, making central management impossible.

The real crisis emerges during information disposal. Microsoft’s object-centric approach embeds metadata within documents - when content is deleted, all evidence of its existence disappears.

Australian government and regulated industries must retain metadata while removing content to prove proper disposal under retention schedules. This protects organizations during Freedom of Information requests and legal proceedings.

EDRMS systems handle this correctly through metadata-centric relational databases. Object-centric solutions like SharePoint make compliance impossible - once the object is gone, there’s no proof it ever existed.

Privacy Act Complications

The Privacy Act’s APP 11.2 requires destroying personal information once it’s no longer needed for business purposes, unless it’s a Commonwealth Record (which EDRMS content is). Organizations using SharePoint face an impossible choice: over-retain information indefinitely or risk compliance violations.

Tech giants now promote AI as the solution to information chaos. However, AI requires the very structure and context that proper records management provides - something US companies lack. The fundamental approach remains flawed.

The first thing that AI needs is structure and context – which is Records Management – which the US doesn’t have. AI needs Records Management, but Records Management does not need AI.

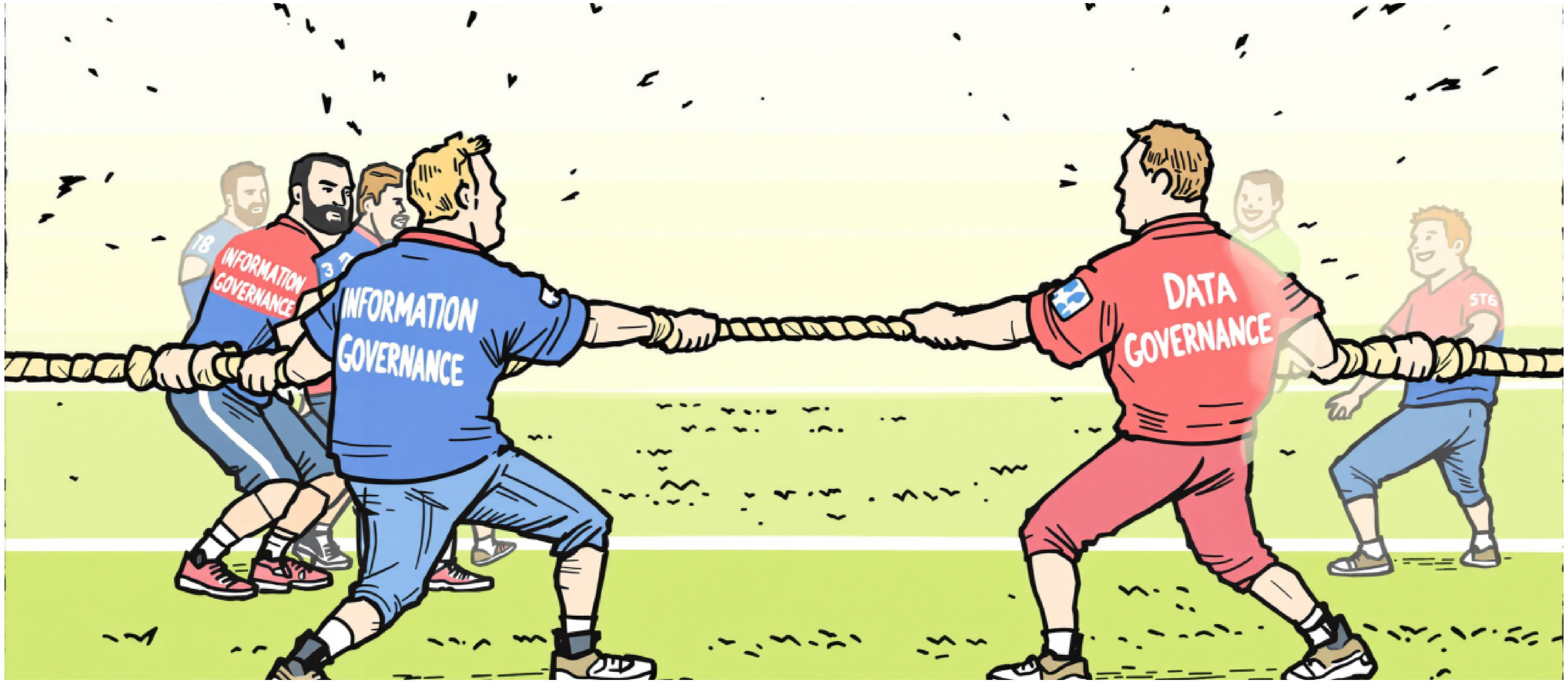
Purview, Microsoft’s compliance solution, actually violates records management principles by applying retention labels at document level without aggregation, then deleting information from folders at different times.

The Path Forward

Australian organizations should resist following US tech giants down this path. The rules governing information management haven’t changed in decades: organize information by subject (Function-Activity-Descriptor) at the container (File/folder) level.

This simple principle, which big tech doesn’t understand, forms the foundation of effective information management. There’s no need for the world to abandon proven records management practices just because the US never adopted them.

Scott Brown is an Information and Records Specialist contracting to Government and Regulated Industry



Information Governance and Data Governance: Time for a Détente?

By Rob Gerbrandt

In today's hyper-connected business environment, the governance of organizational information assets has become a critical strategic concern. Two frameworks have emerged as dominant approaches: Information Governance and Data Governance. While both aim to optimize the value of an organization's information assets, they have evolved as distinct, sometimes competing disciplines. This artificial separation raises an important question: Is it time for a détente between these two domains?

Information Governance emerged from records management and legal compliance traditions, focusing on risk mitigation, retention policies, and regulatory adherence across all information assets. Meanwhile, Data Governance grew from database management practices, emphasizing data quality, structure, and analytics to drive business value.

This bifurcation wasn't accidental. It reflects the historical separation between IT departments (stewarding structured data) and legal/compliance teams (managing documents and records).

As digital transformation accelerated, however, these once-clear boundaries have blurred considerably.

Organizations today face a paradox, simultaneously implementing Information Governance programs to manage risk and Data Governance initiatives to extract value—often with overlapping tools, processes, and stakeholders.

Quantifying the Cost of Division

The maintenance of parallel governance structures creates substantial inefficiencies. Research from the Information Governance Initiative suggests that large enterprises typically allocate 7-12% of their IT budgets toward governance initiatives. Organizations with separate governance frameworks report 30-40% duplication in technology investments and staffing resources.

Beyond financial implications, this division creates operational friction with significant challenges in cross-functional coordination between Information and Data Governance teams. This fragmentation leads to contradictory policies, inconsistent metadata standards, and competing priorities.

The Convergence Imperative

Several market forces are now compelling organizations to reconsider this artificial division:

- **The Dissolving Data Dichotomy** - The distinction between structured and unstructured information is rapidly evaporating. Modern analytics platforms can extract insights from documents, emails, and social media just as effectively as from databases. Machine learning algorithms don't distinguish between information types—they process all available inputs to generate value.
- **Holistic Regulatory Requirements** - Recent regulatory frameworks like GDPR, CCPA, and industry-specific regulations don't differentiate between structured data and unstructured information. They mandate comprehensive protection and management of all personal information regardless of format or storage location.
- **Cross-functional Decision Making** - Effective organizational decision-making increasingly requires a unified view of information assets. When governance is fragmented, executives receive incomplete or contradictory guidance, hampering their ability to make informed strategic choices.

The Integration Opportunity

Forward-thinking organizations are beginning to implement integrated governance frameworks that combine the strengths of both approaches. This integrated model:

- Aligns governance objectives with overall business strategy
- Creates unified metadata standards and taxonomies
- Establishes consistent policies across all information types
- Implements coordinated technology architectures
- Develops cross-functional governance teams with diverse expertise

The Path to Détente: Three Critical Steps

Organizations seeking to bridge the governance divide should consider three foundational steps:

- Establish Unified Leadership - Successful integration requires executive sponsorship that transcends traditional silos. Progressive organizations are creating new leadership roles—such as Chief Information Asset Officer—with authority spanning both domains. This leadership must balance the risk-mitigation focus of Information Governance with the value-creation emphasis of Data Governance.
- Develop Integrated Policies and Standards - Rather than maintaining separate frameworks, organizations should create comprehensive governance policies addressing information assets throughout their lifecycle. These policies should incorporate both compliance requirements and value optimization objectives. For example, healthcare providers are routinely developing an integrated information taxonomy that supports both regulatory compliance and analytics initiatives. This unified approach has the potential to reduce their policy maintenance effort by 35% while improving cross-functional collaboration.
- Align Technology Investments - Perhaps the most tangible benefit of governance integration comes through technology rationalization. By evaluating governance tools against comprehensive requirements, organizations can eliminate redundant systems while ensuring consistent metadata and policy enforcement.

The Organizational Transformation Challenge

While the benefits of integration are compelling, significant organizational barriers remain. Governance integration initiatives fail most often due to entrenched stakeholder interests rather than technical challenges.

The governance détente requires cultural transformation, not just process redesign. Information and data professionals have developed distinct vocabularies, methodologies, and professional identities. Bringing these communities together requires careful change management.

Successful organizations approach this transformation incrementally, identifying specific business problems that require integrated governance and using these as catalyst projects to demonstrate value.

Conclusion: The Imperative for Integration

The artificial separation between Information Governance and Data Governance made sense in an era when structured data and unstructured information existed in separate domains with distinct management challenges. Today's digital business environment demands a more unified approach.

Organizations that continue to maintain parallel governance structures face escalating costs, inconsistent policy enforcement, and missed opportunities to leverage their information assets fully.

Those that successfully bridge this divide position themselves to simultaneously reduce information-related risks and maximize information-driven value creation.

The time for détente between Information and Data Governance has arrived. Forward-thinking executives must now lead their organizations beyond artificial divisions toward truly integrated information asset management.

In doing so, they will transform governance from a fragmented compliance function into a unified strategic capability.

Rob Gerbrandt is Global Head of Information Governance at Iron Mountain.

AI-Powered Information Management powers NZ OAIC Requests

Microsoft New Zealand has announced the successful implementation of AI and low code solutions transforming the way local and central government agencies manage Official Information Act (OIA) and Local Government Official Information Act (LGOIMA) requests.

In a new report, titled "Optimising official information management with AI," it details how government agencies are leveraging AI technology to address longstanding challenges.

According to the report, New Zealand government agencies collectively handle approximately 38,000 requests every six months, up from 26,000 two years ago, with responses taking an average of 13 days.

The implementation of AI solutions aims to dramatically reduce this timeframe to just four days, while simultaneously improving accuracy and reducing complaints.

The report highlights several critical challenges faced by public sector agencies in managing official information requests, including resource constraints, complex processes, fragmented data, manual processing, and sensitive data risks.

Multi-layered approval processes and difficulties in routing requests to appropriate departments further complicate the landscape.

One government agency reported having "multiple ministerial teams, up to 1000 instances of ministerial correspondence and 300+ briefings per month," equating to thousands of hours spent on OIA response management through primarily manual processes.

AI-Powered Request Routing and Response

The first case study features a collaboration between Microsoft and partner Arinco to implement an "Official Information Routing & Response Agents" solution. This system utilizes Copilot Studio or Azure Open AI Agent integrated with existing email, document store, and CRM systems.

The solution expedites triage and routing of incoming requests using Retrieval Assisted Generation (RAG) technology, automatically directing inquiries to appropriate business units.

It then automates response drafting by reviewing questions against previous responses and augmenting drafts with relevant information from internal knowledge bases.

A government agency implementing this solution reported significant improvements, stating, "We removed a manual, time-consuming process with automated retrieval of relevant information using AI, reducing time and effort required to respond."

Benefits included improved response times, enhanced accuracy and consistency, simpler request lifecycle management, and stronger data privacy protections through layered access controls. The agency highlighted that implementation took just weeks and was highly customizable to their specific needs.

Lifecycle Management Application

The report's second example showcases an "Official Information Lifecycle Manager Apps" solution built on Model Driven Power Apps or D365 Customer Service with Power Automate & Power BI. This approach integrates with existing document stores, CRM systems, and data warehouses.

This solution provides an overall view for information managers while enabling participants to see relevant subsections of the process. It includes tools for ensuring consistency in responses, streamlining approval processes, and generating detailed reports to improve efficiency.

One agency reporting a 70% reduction in both hours spent on reporting and request allocation time.
Other benefits included improved visibility through operational dashboards, reduced manual effort through automation of administrative tasks, and significantly enhanced user satisfaction.

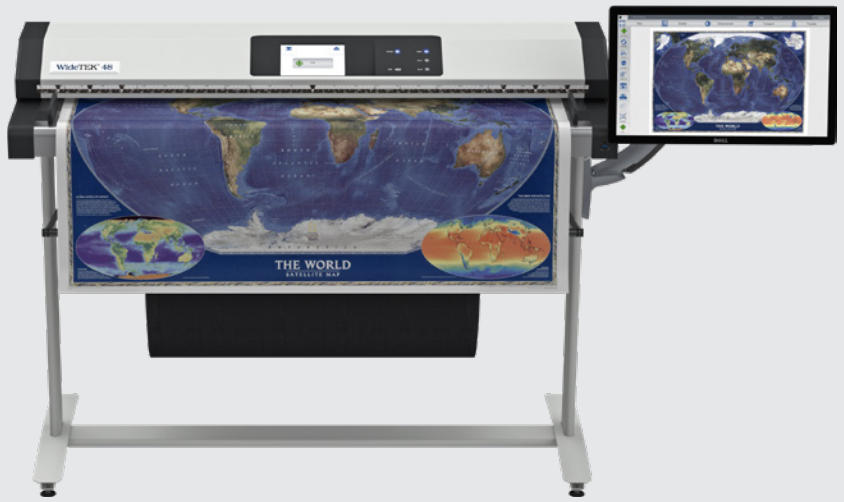
Microsoft's report concludes with ambitious goals for the future of official information management in New Zealand's public sector.

Beyond reducing response times to just 4 days, it aims to decrease the approximately 6,500 requests annually that are transferred or refused because information is already publicly available or meant for other departments.

The report also targets reducing the approximately 610 annual complaints about OIA handling to under 100 through improved accuracy and expedience. Finally, it suggests expanding these successful AI approaches to other areas with similar challenges, such as Data Privacy requests.

"We know the public service is focused on driving value for money and delivering the services New Zealanders want," said Vanessa Sorenson, Managing Director of Microsoft New Zealand.

"Responding to official information requests in a timely way is an important part of that, while also improving efficiency – including on agency reporting requirements – and freeing up public servants for other work. At its core democracy is about communication between citizens and government and we're proud to support that."



Five Years of Warnings Ignored as Government Record Crisis Spirals

A damning new audit has revealed widespread failures in Australian government record-keeping, with missing meeting minutes, lost procurement documents, and collapsed IT systems undermining public accountability across federal agencies.

The Australian National Audit Office's latest report found that more than 90% of government performance audits conducted over the past five years identified serious deficiencies in records management, with all 45 audits conducted in 2023-24 flagging problems.

The scale of the crisis has prompted warnings that poor record-keeping is not just an administrative failing but a fundamental threat to democratic accountability and public trust.

Among the most serious cases uncovered was the Department of Climate Change, Energy, the Environment and Water, where 31% of weekly senior executive meeting records disappeared following IT system changes. The department, formed in 2022 to lead the government's climate commitments, lost critical documentation of decisions and action items during a crucial period.

Tourism Australia was found storing key procurement records in individual email accounts, with documentation for one major contract becoming irretrievable when the responsible employee left the organisation.

The Australian Institute for Teaching and School Leadership was criticised for using basic network drives that failed to meet National Archives standards, leading to inconsistent documentation of stakeholder communications and project changes.

Procurement activities emerged as a particular area of concern, with 88% of procurement audits in 2023-24 identifying records management problems. The findings raise serious questions about transparency in government spending and contract management.

The Bureau of Meteorology was flagged for records management deficiencies that contributed to errors in measuring revenue, leases, and property valuations in its financial statements, though the agency has since implemented improvements.

Systemic technology failures

The audit revealed that many agencies are still relying on inadequate systems, with some using basic network drives that cannot meet legal requirements under the Archives Act 1983. The shift to digital communications has created new compliance blind spots, with official business conducted through informal platforms often going unrecorded.

Email records containing critical business information are frequently stored outside official systems, creating risks when staff leave or systems change. The report notes that all digital information created since January 2016 must be managed digitally, but many agencies are failing to meet this basic requirement.

The audit identified machinery of government changes - when departments are restructured or merged - as particularly high-risk periods for records management. Poor planning during these transitions has led to incompatible systems, lost documents, and breaks in institutional knowledge.

The Department of Climate Change, Energy, the Environment and Water case study highlighted how inadequate preparation can result in records being scattered across multiple systems without proper governance, severely impacting business continuity.

Culture and leadership failures

Beyond technical problems, the audit found fundamental cultural issues, with records management not valued as a strategic priority. Many agencies lack chief information governance officers, fail to include record-keeping in staff performance agreements, and provide inadequate training on compliance requirements.

The report noted that Treasury stood out as a positive example, receiving an "advanced" maturity rating for its comprehensive approach to performance reporting and records management, including strong oversight and documented methodologies.

Records management is required under multiple pieces of legislation, including the *Public Governance, Performance and Accountability Act 2013* and the *Archives Act 1983*. The failures identified could potentially breach legal obligations and undermine parliamentary oversight.

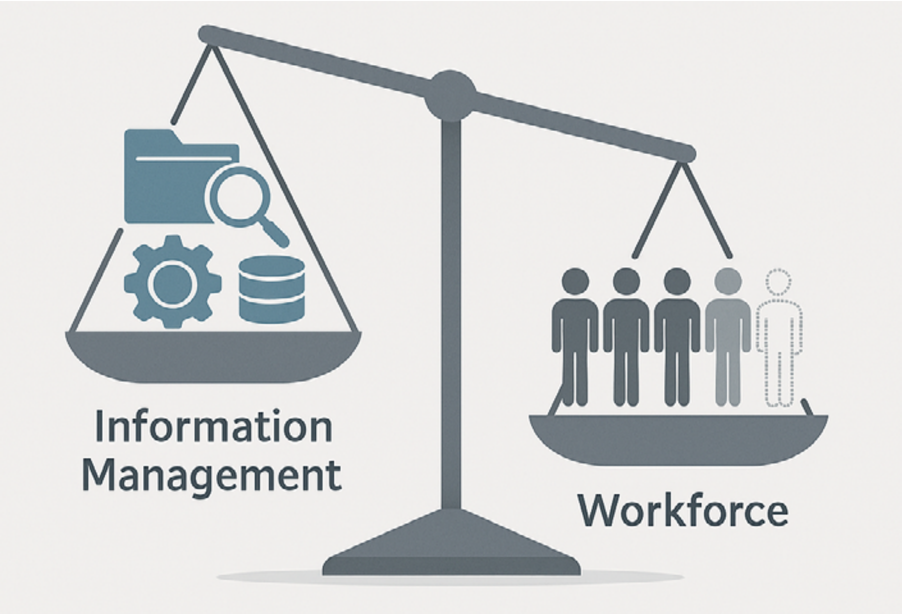
The audit office noted that when records are incomplete or inaccessible, governments lose the ability to provide evidence for decisions, maintain business continuity during crises, and demonstrate accountability to Parliament and the public.

The report documented 41 specific recommendations related to records management made across recent audits, with the majority focusing on basic governance issues and the creation of necessary documentation. The persistence of similar problems across multiple audits suggests many agencies are failing to implement recommended improvements.

The audit office has called for urgent action to establish proper information governance frameworks, invest in compliant systems, and embed records management into business processes. Without significant reform, the report warns, public sector efficiency and democratic accountability will continue to deteriorate.

The full ANAO "Records Management: Audit Lessons" report is available at https://www.anao.gov.au/work/insights/records-management

Staff Cuts Threaten NZ Government Record-keeping Progress



New data from Archives New Zealand reveals both improvements and ongoing challenges in government record-keeping practices across New Zealand's public sector.

In the recently released "*Report on the State of Government Recordkeeping 2023/2024*," Chief Archivist Anahera Morehu describes the current situation as "two steps forward and one step back for IM [information management] across the sector."

The report, based on a survey of 174 public sector organizations and an audit of 23 agencies, highlights several key trends in information management practices.

The number of governance groups with information management oversight has increased, with 48% of organizations now having governance groups that include IM as part of their mandate, up from previous years.

Public offices are also showing improved practices in authorized destruction of records. The percentage of organizations reporting authorized destruction of physical information rose from 51% in 2022 to 68% in 2024, while digital information destruction increased from 34% to 50%.

Although the report concludes more work needs to be done in building IM requirements into new business systems. Only 21% of organisations survey reported that all their systems meet minimum requirements.

Workforce Reductions

After several years of modest growth in information management personnel across the public sector, numbers have declined from 677.2 staff in 2022 to 573.46 in 2024. Many organizations reported plans to further reduce their IM workforce.

"Since 2020, there has been an increase in IM staff, but this trend is sadly reversing with many organisations telling us that there would be further reductions of their IM workforce later in the year," the report notes.

The audit program, which assesses the maturity of information management practices, revealed that most audited organizations are still operating below expected standards.

Out of 23 organizations featured in the report, only 7 (30%) were rated at the required 'Managing' level or higher in at least half of the 20 assessment areas.

However, there were standout performers, with the Inland Revenue Department and the Reserve Bank of New Zealand achieving high ratings, with most of their assessment topics rated at "Maturing" or "Optimising" levels.

Response to Royal Commission Findings

A significant focus for Archives New Zealand has been addressing record-keeping improvements in response to the Royal Commission of Inquiry into Historical Abuse in State Care. In April 2024, the Chief Archivist issued a Temporary Care Records Protection Instruction to protect care records while allowing agencies to carry out their wider disposal responsibilities.

The organization has also undertaken a substantial project to improve access to care records, with staff listing more than 40,000 cards for people under care and protection, indexing various registers and logbooks, and completing the listing of over 2,300 boxes of patient records from hospitals in Auckland.

Archives New Zealand is developing guidance and tools to support public sector organizations in managing records created or affected by artificial intelligence, and has resumed sector webinars to share information management best practices across government.

As public sector organizations continue to navigate organizational and fiscal changes following the change of government in 2023, Archives New Zealand is actively advising on maintaining proper record-keeping during periods of transition.

The report underscores the critical role of proper information management in supporting trusted, open, and accountable government, with the Chief Archivist emphasizing that improvements are both necessary and possible.

The full report is available here.

Ensuring Data Security in the Age of AI

By Janine Morris

Organisations across Australia and New Zealand (ANZ) face unprecedented challenges in managing and securing their most valuable asset — data. What we're hearing is that data is the new gold — valuable, worth hoarding, and something to be mined for insights. But it could also be viewed as uranium: powerful but potentially dangerous, requiring careful handling, and something you only want to keep in the amounts you absolutely need.

As organisations increasingly rely on AI to drive innovation and efficiency, they must also address the unique security challenges that come with it. In 2024, 95% of organisations faced challenges in AI implementation, primarily due to data readiness and information security. Organisations most vulnerable to attacks often hold years of accumulated data — every piece of data you store is a potential target for cyberthreat or insider risk.

Managing vast amounts of data requires robust lifecycle management and ensuring compliance with legislative requirements like Public Records Acts, Australia's Privacy Act 1988, New Zealand's Privacy Act 2020, and industry-specific regulations like Australian Prudential Regulation Authority (APRA). Organisations must adopt proactive data security posture management (DSPM) to safeguard sensitive information and mitigate risks.

This blog covers a new approach to information security that addresses the unique challenges presented by AI technologies.

The Critical Intersection of Data Security and Information Management

According to Forrester, 60% of Asia Pacific firms will localise AI with regionally trained language models reshaped by diverse customer needs, regulatory challenges, and linguistic barriers.

Organisations with a more mature information management strategy are 1.5x more likely to realise the early advantages of AI implementation compared to those with a less robust approach.

Information management provides the foundation for effective data security by establishing policies, procedures, and systems for creating, using, sharing, and disposing of information assets.

In fact, the Office of the Australian Information Commissioner (OAIC) Notifiable Data Breaches Report Australian Cyber Security Centre's (ACSC) Annual Cyber Threat Report 2023-2024 received 527 data breach notifications from January to June 2024, the highest number of notifications received in three and a half years.

Malicious and criminal attacks were the primary source of breaches (67%), with 57% of those being cybersecurity incidents. This highlights the increasing reliance on digital tools and the sophistication of cybercriminals using emerging technologies like AI to bypass traditional defence measures.

In addition, the regulatory requirements under the upcoming Privacy Act reforms in ANZ impose strict obligations to protect against data breaches. Here are some key changes in Australia's Privacy Act reforms responding to growing digital privacy concerns and aligning with international standards:

Increased penalties: Significantly higher fines for serious privacy breaches (up to 10% of annual turnover)

Expanded definition of personal information: Explicitly includes technical data and online identifiers

Stricter consent requirements: Demands clear, specific, and timely consent for data collection

Enhanced individual rights: Includes broader rights to access, correct, and delete personal information

Mandatory data breach notification: Tighter timelines and reporting requirements

Privacy by design: Requires embedding of privacy protection in systems and processes from inception

New Zealand has similarly updated its Privacy Act framework, building on the 2020 Privacy Act reforms with additional measures:

Strengthened cross-border data protection: Implements new restrictions on international data transfers

Additional regulatory powers: Expands authority for the Privacy Commissioner

New risk assessment: Mandatory evaluations for high-risk data processing activities

Enhanced accountability measures: Includes more detailed record-keeping requirements

ANZ organisations must now review and update privacy policies, data collection practices, and security measures to ensure compliance with the stricter requirements. This underscores the intrinsic link between AI and data security, highlighting why information management matters.

Managing Data Sensitivity in AI Environments

Today's customers and workforce expect security by design. AI systems process vast amounts of sensitive data, from personal information to confidential business intelligence. We've seen large-scale data breaches with organisations like MediSecure, an Australian health organisation that holds sensitive medical information and dispenses e-prescriptions. The breach affected nearly half of the Australian population, and the company had to seek government assistance to manage its affairs, assets, and liabilities.

The incident reinforces the potential impact of cyberattacks that go beyond privacy concerns and financial implications. Targeting a healthcare sector that provides essential and time-sensitive services in which downtime can cause operational disruption is a stark reminder that no organisation is immune. It's not a question of "if" but "when."

As AI systems become more sophisticated, so must business strategies to protect sensitive information. Effective DSPM enables organisations to:

Identify and classify sensitive data across all storage locations

Apply appropriate security controls based on data sensitivity

Monitor access patterns and detect anomalies

Enforce compliance with regulatory requirements

Automate security responses to potential threats

By implementing DSPM solutions, ANZ organisations can gain visibility into their sensitive data landscape and proactively address security risks before they result in breaches.

Emerging Security Roles and Continuous Conversations

The rise of AI has introduced new security roles within organisations. These roles focus on analysing risk exposure and managing data security without making changes like adding tags or modifying permissions. Security leaders must prioritise resilient data security to prevent data loss or breaches, leveraging new tools and technologies to gain a deeper understanding of the risks within their organisation.

These specialists analyse risk exposure across AI systems focusing on evaluating AI model vulnerabilities, developing AI-specific security policies, and coordinating response to AI security incidents.

As the threat landscape constantly evolves, organisations must engage in continuous security conversations to stay ahead of potential risks.

This involves regularly assessing the security posture, identifying risk acceptance criteria or tolerance levels, and reallocating resources for security initiatives and compliance with evolving regulatory requirements. By fostering a culture of security, organisations can ensure that their AI initiatives are resilient and beyond secure.

For executives in ANZ organisations, these new security capabilities are not merely a cost centre but a strategic investment. By maintaining continuous dialogue around security concerns, organisations can develop a shared understanding of risks and align security initiatives with broader business objectives.

Automating Data Security for Scale and Efficiency

Manual approaches to data security cannot keep pace with the volume of data in AI environments. Automation has become essential for effective protection.

According to Cybersecurity Ventures, there has been a 35% increase in the adoption of advanced threat detection tools. Gartner also predicted that 70% of organisations will have integrated AI-driven threat intelligence systems by 2025, enhancing their ability to identify and mitigate threats before they manifest into major incidents.

Organisations can run risk assessments to identify who has access to sensitive data, whether they have accessed it, and if any external entities pose a threat.

By aggregating highly exposed content with sensitive information types, organisations can present a heatmap of at-risk data across their systems.

This enables rapid and efficient resolution of data visibility concerns, ensuring that sensitive information is protected.

These automated capabilities allow security teams to focus on strategic initiatives rather than routine monitoring, significantly enhancing operational efficiency.

Strengthening Data Security Through Quality and Governance

AI systems rely on accurate and up-to-date data to generate meaningful insights. However, outdated or obsolete data can lead to incorrect recommendations and decisions.

Organisations must automatically identify and act on outdated content to maintain the accuracy of AI recommendations. This involves archiving or deleting obsolete data and ensuring that AI systems have access to high-quality, relevant information.

According to Gartner, poor data quality costs organisations an average of $14.2 million annually, accounting for approximately 30% of security-related costs.

- To enhance data security, organisations should:
- Implement automated data quality checks.
- Establish clear data governance frameworks.
- Create metadata management systems.
- Develop lifecycle management policies.

By prioritising data quality and governance, organisations create a security foundation that significantly reduces their attack surface while enabling AI systems to operate within defined security parameters.

This approach transforms lifecycle management from a support function into a strategic security asset directly contributing to the organisation's cyber resilience.

A Holistic Approach to AI Data Security

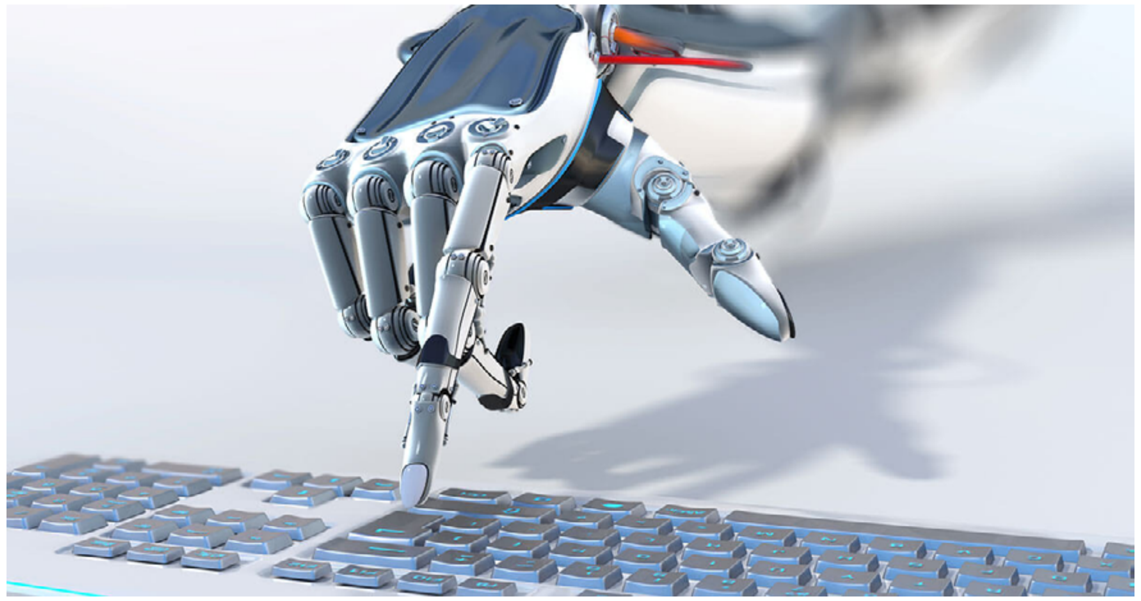
As AI adoption accelerates across ANZ, security challenges will continue to change. Organisations that take a holistic approach – integrating information management, data sensitivity governance, and data readiness – will be best positioned to harness AI's benefits while mitigating its risks.

The journey toward comprehensive data security in the age of AI requires ongoing commitment, investment, and adaptation. By prioritising these key areas, ANZ organisations can build the foundation for secure and responsible AI deployment.

Discover how AvePoint's Confidence Platform can help your organisation implement robust data security and information management practices to support your AI initiatives.

Janine Morris is Industry Engagement and Strategy Lead at AvePoint.

Bots Overtake Humans: AI-Powered Traffic Now Dominates the Internet



In a significant shift in global internet usage patterns, automated bot traffic has surpassed human-generated activity for the first time in a decade, according to the 2025 Imperva Bad Bot Report.

The 12th annual research study reveals that bots now account for 51% of all web traffic, with malicious bots making up 37% of internet traffic - a concerning increase from 32% in 2023. This marks the sixth consecutive year of growth in bad bot activity.

"The surge in AI-driven bot creation has serious implications for businesses worldwide," said Tim Chang, General Manager of Application Security at Thales, which recently acquired Imperva.

"As automated traffic accounts for more than half of all web activity, organizations face heightened risks from bad bots, which are becoming more prolific every day."

AI Lowers Barriers for Cybercriminals

The report attributes this dramatic shift to the rise of generative artificial intelligence and Large Language Models (LLMs), which have significantly reduced the technical barriers for creating sophisticated bots. These accessible AI tools enable less skilled actors to launch more frequent and widespread attacks.

Researchers identified several AI platforms being exploited for malicious purposes, with ByteSpider Bot responsible for 54% of all AI-enabled attacks. Other significant contributors include AppleBot (26%), ClaudeBot (13%), and ChatGPT User Bot (6%).

The travel industry has become the most targeted sector, accounting for 27% of all bot attacks in 2024, up from 21% in 2023 The report notes a shift from sophisticated to simpler attacks in this sector, with advanced bot attacks declining from 61% to 41%, while simple bot attacks increased from 34% to 52%.

API Business Logic Under Attack

One of the most concerning trends highlighted in the report is the surge in API-directed attacks, with 44% of advanced bot traffic now targeting APIs. Rather than simply overwhelming API endpoints, these attacks exploit vulnerabilities in the business logic that defines how APIs operate.

"The business logic inherent to APIs is powerful, but it also creates unique vulnerabilities that malicious actors are eager to exploit," Chang warned. "As organizations embrace cloud-based services and microservices architectures, it's vital to understand that the very features that make APIs essential can also leave them susceptible to risk of fraud and data breaches."

Financial Services Most Vulnerable to Account Takeovers

The financial services sector emerged as the most targeted industry for account takeover (ATO) attacks, accounting for 22% of all incidents, followed by Telecoms and ISPs (18%) and Computing & IT (17%).

The report explains that financial institutions remain prime targets due to the high value of accounts and sensitive data they manage. The proliferation of APIs within the industry has broadened the attack surface, allowing cybercriminals to exploit vulnerabilities such as weak authentication and authorization methods.

A Growing Bots-as-a-Service Ecosystem

The report also notes the emergence of a growing Bots-as-a-Service (BaaS) ecosystem, where commercialized bot services make sophisticated attack capabilities available to less technical actors. This democratization of attack tools, combined with AI's ability to help attackers learn from failed attempts, creates a rapidly evolving threat landscape.

"In this rapidly changing environment, businesses must evolve their strategies," Chang emphasized. "It's crucial to adopt an adaptive and proactive approach, leveraging sophisticated bot detection tools and comprehensive cybersecurity management solutions to build a resilient defense against the ever-shifting landscape of bot-related threats."

The 12th Annual Imperva Bad Bot Report analyzed data collected from across Thales' global network in 2024, including the blocking of 13 trillion bad bot requests across thousands of domains and industries.

Download THE 2025 Bad Bot Report here.

Hacktivist Groups Target Critical Infrastructure

Hacktivist groups are rapidly evolving beyond traditional disruptive activities into more sophisticated and destructive cyberattacks targeting critical infrastructure and deploying ransomware, according to a new report from cybersecurity firm Cyble. The report, which analyzes hacktivist activities during the first quarter of 2025, reveals that hacktivism has "transformed into a complex instrument of hybrid warfare" with some groups now employing advanced techniques previously associated primarily with nation-state actors and financially motivated criminal organizations.

Pro-Russian hacktivist groups, including NoName057(16), Hacktivist Sandworm, Z-pentest, Sector 16, and Overflame, were identified as the most active in Q1 2025. These groups primarily targeted NATO-aligned nations and countries supporting Ukraine, with a concerning 50% surge in attacks on Industrial Control Systems (ICS) and Operational Technology (OT) in March alone.

"Hacktivism is no longer confined to fringe ideological outbursts," the Cyble report states. "It is now a decentralized cyber insurgency apparatus, capable of shaping geopolitical narratives, destabilizing critical systems, and directly engaging in global conflicts through the digital domain."

The sectors most frequently targeted include government and law enforcement agencies, banking and financial services, telecommunications companies, and energy and utilities. The latter was particularly singled out for ICS attacks, with notable incidents affecting energy distribution and water utilities.

Geographically, India experienced the highest number of incidents in January, while Israel remained a persistent target throughout the quarter with a major spike in March, driven largely by pro-Palestinian hacktivist groups.

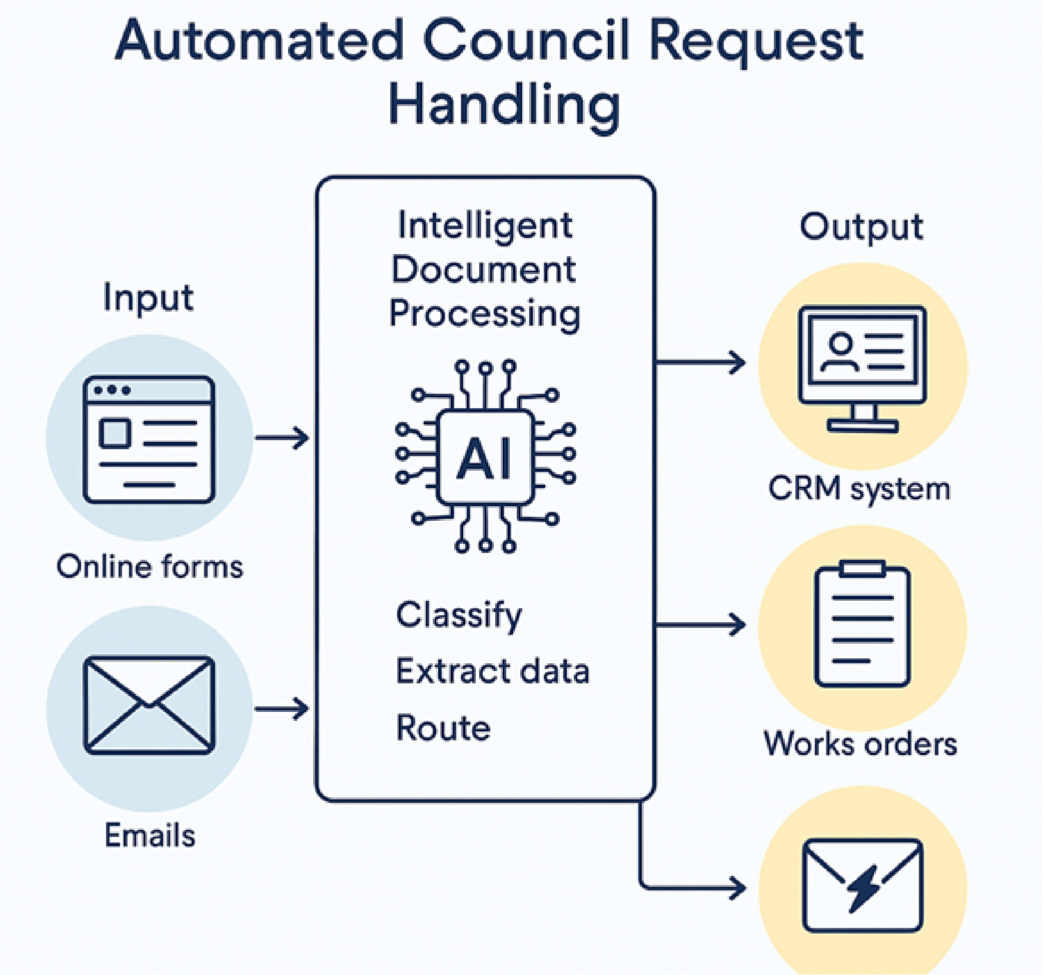
The United States saw an increase in attacks in March, which Cyble correlates with early actions by the new Trump Administration, including military strikes in Yemen and the implementation of import tariffs.

Perhaps most concerning is the adoption of ransomware by hacktivist groups. Cyble identified at least eight hacktivist groups and their allies "embracing ransomware as a tool for ideological disruption" during Q1.

The report also noted that hacktivist groups are increasingly employing more sophisticated website attack methods, including SQL injection, brute-forcing web panels, exploiting OWASP vulnerabilities, and using Dorking techniques to discover exposed databases.

Cyble warns that as the technical capabilities of these ideologically motivated actors continue to advance, the distinction between hacktivists, nation-state actors, and financially motivated threat groups is increasingly blurred, creating heightened risks for organizations in regions experiencing geopolitical tensions.

It is time to Revolutionise Request Handling by Local Government



Local councils across Australia and New Zealand find themselves navigating a constant stream of communication from the residents they serve. Every day brings a fresh wave of requests, applications, and inquiries pouring in through a multitude of channels – emails, website forms, dedicated portals, traditional mail, and even social media interactions.

With increasing cultural diversity many of these councils ingest information through 150+ online form types and 10+ languages.

This diverse influx demands significant effort merely to understand, categorize, and direct each item to the appropriate department for action.

Despite the digital age, many councils grapple with these tasks using traditional, manual methods, leading inevitably to processing bottlenecks, strained resources, and significant, often hidden, operational costs.

The reliance on manual triage, where staff must individually read, interpret, and forward each incoming message, carries a heavy burden.

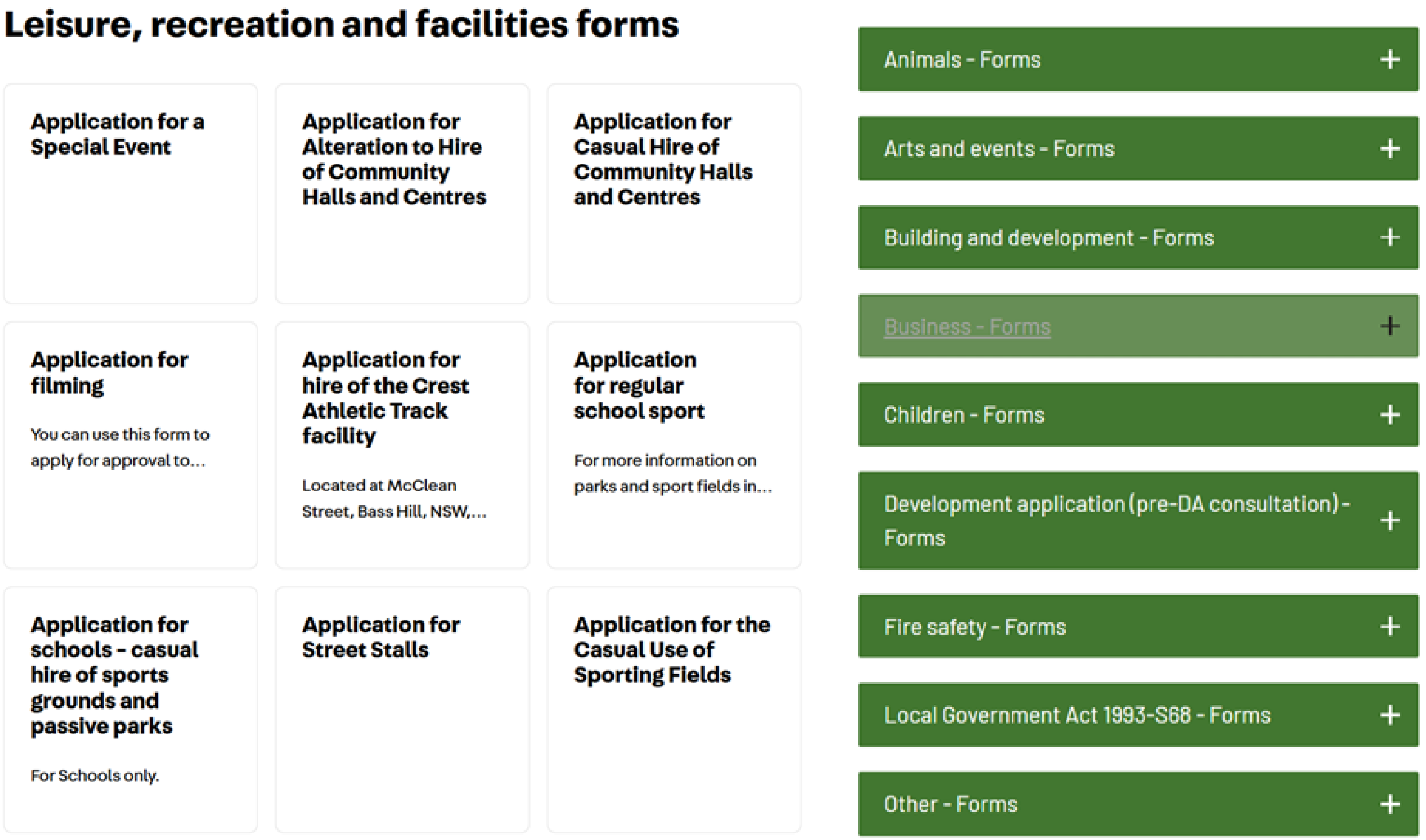
Beyond the direct cost of staff hours spent on this repetitive work, the process is inherently slow, often leading to delays that frustrate residents expecting timely service.

Manual data entry and classification also opens the door to errors, risking misrouted requests and inefficient handling down the line. Furthermore, ensuring consistent communication, tracking response times, and maintaining standards becomes a complex challenge.

Service quality can fluctuate based on workload and staff availability, and the monotonous nature of the task can unfortunately contribute to employee burnout.

Fortunately, technology offers a powerful alternative: AI-powered Intelligent Document Processing, or IDP. This sophisticated approach leverages artificial intelligence, including machine learning, natural language processing, and optical character recognition, to fundamentally change how requests are handled.

Council Size	Population	Emails per Day (Est)	Total Staff (Est)	Public Request Staff (Est)
Small	~10k pop	50 – 200	50 – 150	5 – 15
Mid-sized	~50k pop	200 – 1,000	200 – 500	20 – 50
Large Metro	>100k pop	1,000 – 5,000+	500 – 2,000+	50 – 200+



Leisure, recreation and facilities forms

Application for a Special Event

Application for Alteration to Hire of Community Halls and Centres

Application for Casual Hire of Community Halls and Centres

Application for filming
You can use this form to apply for approval to...

Application for hire of the Crest Athletic Track facility
Located at McClean Street, Bass Hill, NSW,...

Application for regular school sport
For more information on parks and sport fields in...

Application for schools - casual hire of sports grounds and passive parks
For Schools only.

Application for Street Stalls

Application for the Casual Use of Sporting Fields

Animals - Forms +
Arts and events - Forms +
Building and development - Forms +
Business - Forms +
Children - Forms +
Development application (pre-DA consultation) - Forms +
Fire safety - Forms +
Local Government Act 1993-S68 - Forms +
Other - Forms +

IDP systems can automatically ingest and triage incoming communications from various digital sources, in any language or format, intelligently read and understand the content, extract the crucial information, and accurately classify the request type and its urgency.

This allows for immediate, automated routing to the correct team or integration to the ECM and workflow application and can even trigger initial actions like sending acknowledgements, approvals, or updating tracking systems, with little manual intervention.

The response and accuracy to community stakeholders can be improved considerably.

The benefits for councils adopting this technology are substantial and proven, even for handwritten forms and unstructured correspondence.

By automating the initial sorting and routing (triage), IDP dramatically speeds up response times and significantly reduces backlogs.

Fewer requests get lost or delayed, and tracking compliance becomes much more manageable. This efficiency translates directly into lower operational costs and, importantly, frees up valuable council staff from tedious, repetitive tasks.

Typically, the return on investment for such automation projects is achieved in less than 12 months, even within relatively small councils.

Teams become less overburdened and can redirect their efforts towards more complex problem-solving and providing higher-value assistance to the community.

For instance, a council handling around 2,000 emails daily could see 80-90% of the initial classification and routing automated, saving hundreds of staff hours each month.

The scale of this challenge varies – smaller councils might handle 50 to 200 requests daily, while large councils can face upwards of 2,000. These requests span a wide array of services, commonly including waste collection issues, road and park maintenance, planning inquiries, venue bookings, and parking permits, often encompassing over a hundred distinct categories.

The inefficiency of manual intake doesn't just affect one team; it creates friction across the organization, impacting customer service officers on the front lines, records managers ensuring compliance, corporate services integrating information, and the operational units waiting to action the requests.

Depending on the council's size, the team processing public inquiries can range from 5 to over 200 staff members; this scale directly correlates with the potential impact and benefits of implementing process improvements.

In the current climate of tight budgets and high resident expectations for seamless digital experiences, the case for adopting IDP is compelling.

It offers a proven method to maintain or even improve service levels while simultaneously increasing internal efficiency.

Councils can begin by analysing their unique request patterns to identify the areas where automation would yield the greatest benefit, often starting with the highest volume request types.

By embracing AI-powered IDP, councils in Australia and New Zealand can effectively manage the flow of information, reduce administrative burdens, and ultimately, better serve their communities.

TCG Process has specialised in the ingestion of information into teams and business systems since 2006 and has improved processes for many government agencies, local councils, insurers, banks and healthcare providers globally.

If you would like to see a tailored demo on how your council can process requests faster and with half the effort, please contact TCG Process.

For more information visit www.TCGProcess.com or contact info.aus@tcgprocess.com.

Top Challenges Businesses Face with Manual Document Processes

Manual document management is common in many businesses, despite the fact that digital tools can make the process much easier. If your business manages documents manually, you likely face a range of challenges.

1. Process Inefficiencies

Manual processes are often time-consuming and demand a lot of attention from employees. Workers engaging with manual tasks lose opportunities to engage in more valuable tasks, leading to more work than your team can manage.

Every person works at a different pace. If you rely on multiple team members to complete specific tasks or operate with workflows that require one task to be completed before another can begin, you can experience efficiency gaps — workers have mountains of work while others have little to do. The result is inefficient processes that require workers to engage in repetitive, mundane, or less meaningful work.

2. Increased Error Rates in Document Management

Human error is a significant driver of manual document processing mistakes. Data entry errors alone can cost businesses trillions of dollars each year. Several factors, such as fatigue, lack of training, poor lighting, complex instructions, or pressure, can impact employee performance. While mistakes are bound to happen, minimizing their likelihood can boost your business and empower growth.

Mistakes have several adverse impacts on your business, such as:

Cost: If a mistake impacts your resources, budget allocation, customer relationships, or any other element regarding your bottom line, you can find your business at a loss.

Time: Mistakes can be time-consuming to address, especially when one task impacts another. For example, if you discover inaccurate report information, you'll likely need to pull various records and documents and double-check information from multiple sources, taking time away from other tasks.

Reputation: Customers, clients, and partners want to trust the businesses they engage with. If your business appears unreliable or inefficient, you may lose existing relationships or face more roadblocks when trying to forge new ones.

3. Data Retrieval Difficulties

Businesses lose productivity by relying on manual document retrieval. When employees spend hours a day trying to find information, they lose opportunities to engage in other tasks. Slow document retrieval leads to poor customer service, decision-making delays, and other adverse outcomes.

Teams can also experience increasing complexity if your organization lacks a specific retrieval structure. Lacking designated storage spaces or protocols for locating and replacing documents can result in employees misplacing information, potentially losing it permanently.

4. Higher Operational Costs

Another adverse outcome of maintaining manual document processes is the high cost of storing, printing, and handling paper. Physical documents require ink, printers, paper, storage units or filing cabinets, and other expenses that can quickly add up.

Finding, printing, and distributing these materials takes significant time, and losing documents can result in fines or delays that impede financial gain. Factoring in the cost of human mistakes, such as data entry errors, further propels financial losses.

5. Lowered Collaboration

Collaboration can increase efficiency, promote a sense of accomplishment, and reduce the time necessary to complete tasks. However, sharing documents and collaborating on projects is challenging when you rely on manual processes.

It takes a lot of time to print and share documents, and timetables can increase if you also lack proper digital communication tools. Teams that work in different locations can experience hefty wait times during collaboration, and without the ability to make and monitor real time updates, it can be challenging to determine which documents have your latest updates.

6. Lack of Tracking or Visibility

Locating paper documents can be challenging as-is, but improper organization and inadequate management processes reduce visibility and make tracking even more difficult. Manual document handling processes also lack the ability to monitor real-time changes or provide quick navigation.

Team members may not be aware of more updated document versions, use poor data for decision-making, or face significant delay bottlenecks from misplaced or in-use documents. Furthermore, relying on manual processes impedes your scalability. As your business grows, you need a solution that can handle growth periods, but humans alone are limited in the changes they can make to meet these demands.

7. Uninformed Decision-Making

Accurate and reliable data empowers you to identify trends and make decisions based on historical data and future predictions. Manually analyzing historical documents is time-consuming, and workers may not have the experience or understanding to spot trends, especially if they don't know what they're looking for. If your workers make any mistakes during this process, the decision your team makes may not be as impactful as it could have been if your team leveraged correct data.

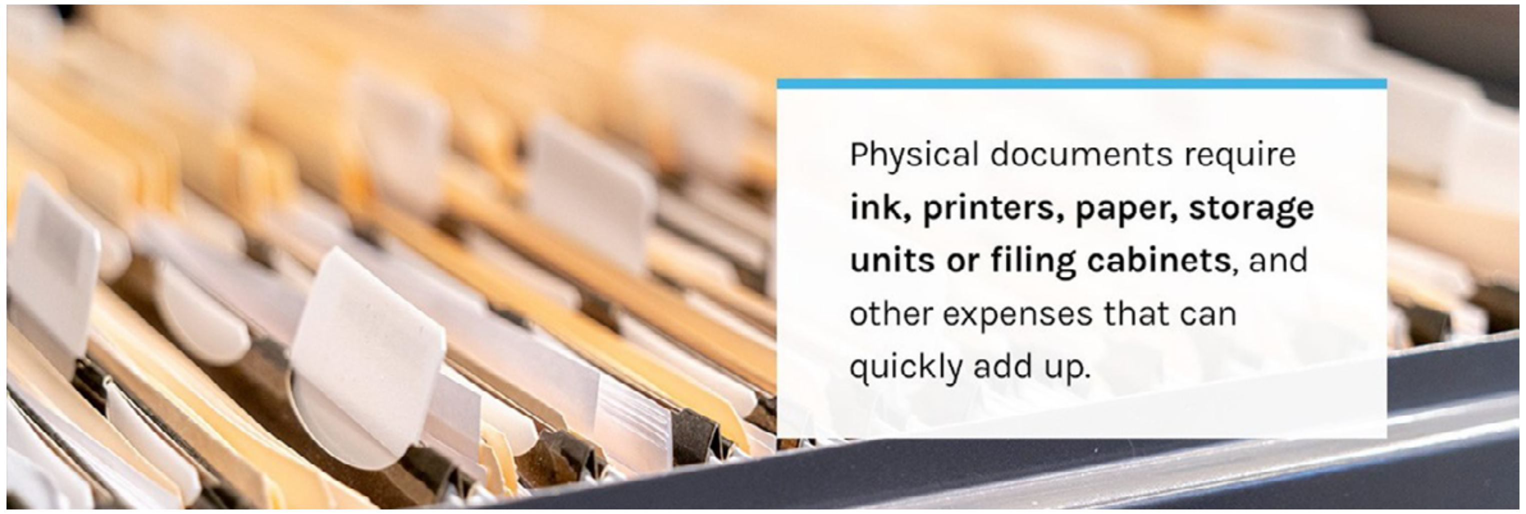
How You Can Improve Workflow With Document Process Automation

There is a solution for navigating the challenges of manual document processes — automation. Today's digital solutions are capable of navigating a variety of document-handling processes, including storing, analyzing, retrieving, and sharing documents. Implementing the right automated solution allows you to:

- **Meet compliance:** Digital automated solutions support uniform processes for document management. This uniformity can help you meet compliance and provide an easier way to navigate compliance changes when they occur.
- **Strengthen security:** Using digital solutions means you always have the information you need, including backups when necessary. You can leverage various security protocols to ensure authorized individuals can access documents while preventing unauthorized access from others.
- **Increase adaptability:** Artificial intelligence and other cutting-edge technologies empower you to scale operations or down as necessary. You can feel confident that your solution will grow with you, providing seamless customer and worker experiences.
- **Reduce costs:** Set rules and train your solutions to provide accurate outputs. These machines and processes can enhance accuracy and reliability while reducing time spent on each task, delivering cost savings all around.
- **Enhance collaboration:** Digital solutions make it easier to share documents and allow you to make real-time updates. Your team can enjoy the simplicity of using digital tools to collaborate on projects and experience the convenience of accessing documents wherever and whenever they need them.
- **Inform decisions:** You can use digital solutions to pull specific reports, request industry predictions, and employ tactics to compare historical data with current information.

Overcome the Impact of Manual Processes on Business Success

OPEX® is the next generation of automation. The OPEX team engineers automated solutions to address your business's most pressing challenges. OPEX document and mail automation allows businesses to increase efficiency, cut costs, reduce manual labor, and gain a competitive edge through innovative technology and scalable operations. For help finding the right automated solution for your business, connect with an OPEX representative today.



Physical documents require **ink, printers, paper, storage units or filing cabinets**, and other expenses that can quickly add up.

EzeScan is one of Australia's most popular production capture applications and software of choice for many Records and Information Managers. This award winning technology has been developed by Outback Imaging, an Australian Research and Development company operating since 2002. Solutions range from centralised records capture, highly automated forms and invoice processing to decentralised enterprise digitisation platforms which uniquely align business processes with digitisation standards, compliance and governance requirements. With advanced indexing functionality and native integration with many ECM/ EDRMS, EzeScan delivers a fast, cost effective method to transform your manual business processes into intelligent digital workflows. EzeScan benefits include: initiate intelligent automated processes; accelerate document delivery; minimise manual document handling; capture critical information on-the-fly; and ensure standards compliance.

www.ezescan.com.au | info@ezescan.com.au | 1300 393 722

Hyland is a leader in providing software solutions for managing content, processes and cases for organisations across the globe. For 30 years, Hyland has enabled more than 16,000 organisations to digitise their workplaces and fundamentally transform their operations. Hyland has been a leader in the Gartner Magic Quadrant for Content Services for the past 12 years and named one of Fortune's Best Companies to Work For® since 2014, Hyland is widely known as both a great company to work for and a great company to do business with. Our solutions are intuitive to use so organisations can focus on what they do best. Managing information doesn't have to be complicated. At Hyland, our mission is to empower efficiency and agility so our customers can grow and innovate with confidence. We help organisations handle their most critical content and processes with flexible, configurable software solutions.

www.hyland.com/en/| info-onbase@onbase.com| 02 9060 6405

DocuVAN is a Distributor and Reseller of higher end scanning equipment, including Ricoh's state-of-the-art scanning solutions in the workgroup, departmental, and production-level scanner categories. Ricoh fi Series Best-in-Class Document Scanners deliver speed, image quality, and great paper handling, along with easy integration and compatibility with document imaging applications. We also represent Image Access in Australia, NZ, Pacific Islands and PNG as the distributor of their suite of Bookeye and WideTEK Scanners. If it is deemed part of your core business, Docuvan can supply, install and train you to operate your own scanning solution. We can help you integrate with a document management system and setup workflow processes to automate most paper based legacy systems. Our solutions are scalable and we offer a wide variety of options to suit most budgets.

www.docuvan.com.au| info@docuvan.com.au | 1300 855 839

OPEX® Corporation is a global leader in Next Generation Automation, providing innovative, unique solutions for warehouse, document and mail automation. With a comprehensive suite of customised, scalable technology solutions, OPEX helps clients transform how they conduct business—improving workflow, reducing costs and driving efficiencies in infrastructure. Since 1975, the family-owned and operated company has served as a trusted partner to clients around the world, with nearly 1,600 employees continuously reimagining automation technology that solves the most significant business challenges of today and in the future. OPEX is headquartered in Moorestown, NJ, with facilities in Pennsauken, NJ; Plano, TX; France; Germany; Switzerland; the United Kingdom; and Australia. The year 2025 marks a significant milestone—the company's 50th anniversary under the multi-generational leadership of the Stevens family.

https://opex.com | info@opex.com

INFORMOTION is an innovative professional services organisation specialising in the design and implementation of modern information management, collaboration and governance solutions – on-premises, in the cloud or hybrid. INFORMOTION's workflow tools, custom user interfaces and utilities seamlessly combine to deliver compliance, collaboration, capture and automation solutions that provide greater business value and security for all stakeholders. We can help you map and successfully execute your digital transformation strategy. Boasting the largest specialist IM&G consulting teams in Australia with experience that spans over twenty years, INFORMOTION consultants have a deep understanding of business and government processes and the regulatory frameworks that constrain major enterprises. Our compliance experience is second-to-none. INFORMOTION is a certified Micro Focus Platinum Partner and global Content Manager implementation leader. We are also an accredited Microsoft Enterprise Business Partner, Ephesoft Platinum Partner and EncompaaS Diamond Partner.

informotion.com.au | info@informotion.com.au | 1300 474 288

Established in 2003, iCognition is a leading Information Management and Governance (IMG) specialist. With over 20 years of customer success stories in delivering IMG services and solutions, we provide managed services for OpenText Content Manager (formerly TRIM) to over 130 government and private sector enterprises across Australia. With information governance at our core, iCognition empowers customers in their digital transformation projects to maximise the value of their information assets. Whether that be on-premises or transitioning to our secure cloud solution, Ingress by iCognition, we enable customers to meet the challenges of managing information across the enterprise. Ingress is a Content Services Platform with OpenText Content Manager at its heart. We can transition your Content Manager system to Ingress or provide a greenfields solution in your cloud or ours. Our Ingress cloud is ISO27001 Information Security Management certified and IRAP assessed to PROTECTED.

www.icognition.com.au | info@icognition.com.au| 1300 4264 00

EncompaaS is a global software company specialising in information management, powered by next-gen AI. Leading corporations, government departments and statutory authorities trust EncompaaS to govern and optimise information that resides within on-premises and multi-cloud environments. Organisations are empowered to solve information complexity, proactively address compliance and privacy risk, and make better use of data to act strategically at pace. EncompaaS is distinguished in the way the platform utilises AI to build a foundation of unparalleled data quality from structured, unstructured and semi-structured data to de-risk every asset. From this foundation of data quality, EncompaaS harnesses AI upstream to unlock knowledge and business value that resides within information. EncompaaS maintains a robust partner ecosystem, including global consulting and advisory firms, technology partners, and resellers to meet the diverse needs of highly regulated organisations.

encompaas.cloud | enquiries@encompaas.cloud | 1300 474 288

Kapish (a Citadel Group Company), established in 2007, is a dynamic organisation delivering secure technology solutions and strategies in Information Management & Governance, Business Transformation and Enterprise Architecture. Kapish is a Tier 1 OpenText Platinum Business Partner, delivering secure cloud-based information governance and records management solutions built around OpenText's Content Manager (formerly TRIM/HPE RM/MICRO FOCUS CM). Kapish's offerings include IRAP-assessed, ISO 27001-certified cloud managed services, data privacy and protection solutions, IM and technical consulting, migration and implementation services, custom product development and software solutions. Our range of integrated software solutions and managed services gives you a complete view of your IT landscape, helping you discover, manage and protect your information assets, meet regulatory compliance, boost user productivity and transform business processes with modern solutions.

kapish.com.au | info@kapish.com.au | 03 9017 4943

Newgen offers a unified digital transformation platform that includes native process automation, content services, and communication management capabilities. Globally, many successful enterprises across various industries rely on the NewgenONE digital transformation platform—a comprehensive and unified cloud-based platform with low code capability for rapid development of content-driven, customer-engaging business applications. The platform can transform and simplify complex business processes. Equipped with cutting-edge technologies, including mobility, social listening/sensing, analytics, cloud, artificial intelligence (AI), machine learning (ML), and robotic process automation (RPA), the NewgenONE platform helps enterprises stay ahead of the curve. From grass-root citizen experience management, dynamic case management to electronic documents and records management, lending to underwriting, the platform solves multiple use cases across various industries, including government, banking, insurance, and others. Furthermore, Newgen has a robust partner ecosystem, including global system integrators, consulting and advisory partners, value-added resellers, and technology partners.

newgensoft.com/home-anz/ | info@newgensoft.com | 02 80466880

Standalone Solution for Process Automation

TCG Process has announced the launch of OCTO, a process automation platform that provides comprehensive orchestration and automation for complete end-to-end business processes.

Previously a key part of DocProStar, TCG's intelligent document processing solution, OCTO is now being offered as a standalone solution for generic end-to-end business process automation.

The product name derives from the Latin word for eight, reflecting OCTO's 8 major capabilities: Orchestration, Process Management, Intelligent Automation, Security/Compliance, Integration, Scalability, Flexible UI and Embracing AI.

Key features of OCTO include:

- Easy and secure integration of AI technologies directly into critical operational workflows.
- Information is delivered in an optimized and ergonomically designed UX to enhance human roles.
- A scalable architecture, ensuring adaptable performance that aligns with evolving business demands.
- Rapid process creation and deployment, leveraging AI-driven natural language modeling and no/low-code tools.

“OCTO is a game-changer for businesses looking to stay ahead in an increasingly fast- paced and competitive environment,” said Arnold von Bueren, CEO of TCG Process.

“We're not just offering a tool, we're delivering a strategic advantage. OCTO's ability to provide timely process bottleneck resolution and end-to-end workflow automation makes it an essential part of any modern organization's tech stack.”

The platform is already helping customers in claims processing automation, onboarding workflows, email triage and more. As part of the TCG Process suite of automation solutions, OCTO integrates seamlessly with both legacy systems and newer cloud-based services and applications, offering smooth implementation and immediate results.

Patrick Ulrich, TCG Process CTO, said, “OCTO is able to do more than just extract data from a claims process for instance and trigger the next step in the workflow. Octo is able to link to multiple legacy systems and present the user with all the relevant information that they need to make a decision on a claim or an application.

“So, a knowledge worker is able to visualize all the relevant information in OCTO and close the case in our platform instead of going back and forth between different systems.

Pacific Commerce, a business process outsourcing (BPO) firm, has already seen measurable improvements using the new solution.

“Using OCTO and DocProStar has transformed how we connect and manage data between our customers' ERP systems. We can quickly build and deploy integrated

Connectors - without any specialized coding skills - and reliably orchestrate the flow of accurate information between multiple platforms,” said Dimitri Margaritis, CEO, Pacific Commerce.

“This flexible, no-code approach allows us to validate and process invoice data on the fly, streamlining our workflows and improving both the customer and employee experience.

“OCTO has always been a no code solution to allow business users to build processes without requiring coding. We are able to extend OCTO with low code capabilities if it's needed in a customer installation that has special requirements not already included,” said Ulrich.

For more information visit www.TCGProcess.com or contact info.aus@tcgprocess.com

ABBYY' API removes Data Extraction Headaches

ABBYY has launched a new self-service application programming interface (API) designed to help developers extract accurate data from business documents with minimal coding effort.

Known as ABBYY Document AI, the API addresses growing challenges faced by developers who need to transform unstructured business documents into structured, reliable data. According to ABBYY, the solution allows users to integrate powerful optical character recognition (OCR) and intelligent document processing (IDP) capabilities using just a few lines of code.

“As a vanguard of OCR, ABBYY has long had a vibrant community of cutting-edge developers creating transformational solutions with our advanced document AI,” Nick Hyatt, Vice President of Engineering R&D at ABBYY.

“We are providing them a new API with minimal setup, access to ample community resources, and pre-trained models for building proof-of-concepts.”

Nuix Takes Aim at AI's Biggest Blind Spot

Nuix, in the Australian developer of investigative analytics and intelligent software, has announced the launch of a solution designed to transform complex unstructured data into high-quality, AI-ready information assets, Neo AI Data Curator.

The company's new offering aims to address what it describes as the most critical yet often overlooked prerequisite for successful generative AI implementation: quality data preparation.

Roland Slee, VP of Nuix Ventures, told IDM, “In dialogue with customers, it's become very clear that businesses everywhere are looking to leverage artificial intelligence and especially generative AI.”

Slee explained that many organizations with early AI proof-of-concept projects have discovered that “in order to get the best from AI, you need to train large language models on corporate data,” and that “the quality of outcome that you can get depends very greatly on the quality of that input.”

“So, in order to get the best return on investment from AI focused projects, you need the first curate your data in order to ensure that you're training large language models on a set of information which represents the gold standard view of the enterprise.

“That is a function which the NEO platform is able to support, and we've made some further investments in functionality and features to enable this and are now promoting our solution as Nuix Neo AI Data Curator.”

The core intellectual property of Nuix and the foundation for the company's success has been its data engine which still sits at the heart of the NEO platform which also includes a range of other capabilities, some of which have been engineered in-house by Nuix and some the result of acquisitions.

The acquisition of Topos Labs in 2016 provided NLP technology that has been integrated into the NEO platform and is today providing Cognitive AI capability. Similarly, Nuix made an acquisition of a company called Rampiva in 2023 which provided a workflow engine which has been rebranded as Nuix Automate and is now part of the NEO platform.

“In 2025, we're more looking to promote the business solutions that are available on the platform and progressively to expand that range of solutions,” said Slee.

“The way to think about Nuix today is that NEO is our platform for the processing of unstructured data and leveraging artificial intelligence,” said

According to Nuix, unstructured data makes up over 90 percent of all enterprise information and is inherently difficult to manage. The company warns that even sophisticated AI systems will fail to deliver valuable outcomes if fed with inaccurate, irrelevant, or poor-quality data.

The Neo AI Data Curator builds on Nuix's 25 years of forensic-grade data analytics experience and handles the entire unstructured data processing workflow - from cleansing and normalization to vectorization, enrichment, prioritization, and redaction.

A case study highlighted in the company's fact sheet describes how a major legal sector client initially struggled with their AI implementation. The client attempted to build a document filtering system powered by a fine-tuned LLM but encountered significant challenges. After three months of unsuccessful experiments, they discovered that 90 percent of their dataset was irrelevant or detrimental to training the model.

After implementing Nuix Neo AI Data Curator, the client was able to rapidly identify data anomalies and processing errors, determine the fitness of their dataset for AI applications, and avoid time-consuming iterations of fine-tuning and data cleaning.

“Nuix's engine gives us the ability to very deeply inspect the content of unstructured data and to do that at scale with great efficiency.,” said Slee.

The solution features a five-step process that includes collection, transformation, enrichment, fortification, and promotion of data. The Nuix platform can connect to enterprise data across various storage systems, normalize over a thousand file types, and process terabytes of information in hours.

A notable capability of the Neo platform is its ability to analyse multi-layered documents. Slee provided an example where the system can process an email with a zip file attachment containing multiple documents, including embedded files, and still identify sensitive information like a driver's license number hidden several layers deep.

Nuix is positioning its Neo AI Data Curator as essential for both public and private organizations with complex or messy datasets that want their generative AI initiatives to deliver accurate, scalable, reliable, and explainable results.

As organizations continue to invest in AI technologies, the focus on data quality and preparation appears to be gaining recognition as a critical success factor, with Nuix quoting Oracle co-founder Larry Ellison: “Unless you get your data properly organized, you can't use AI. It becomes utterly useless.”

The intelligent document processing market is experiencing significant growth, with IDC projecting an expansion from $US2.4 billion in 2023 to $US10.5 billion by 2028, representing a 34.9% compound annual growth rate. This growth is attributed to increasing cloud adoption, AI maturation, and expanded document AI use cases.

Amy Machado, Senior Research Manager at IDC, noted that OCR is experiencing a "true renaissance" in the age of AI. However, developers using general large language models for document processing often encounter challenges such as hallucinations, data inconsistencies, and errors, particularly when dealing with multiple languages, handwriting recognition, and complex document structures.

The ABBYY Document AI API, initially available as a technical preview, offers pre-trained models to extract data from documents and accelerate automation for complex business processes including KYC (Know Your Customer), account openings, customs clearance, invoice processing, expense management, and order processing.

A key feature of the new API is its ability to preserve a document's logical structure, providing AI-ready data that can be used for generating insights in generative AI applications and retrieval augmented generation (RAG) systems, or for training language models.

The company has made comprehensive software development kits (SDKs) available for Python, C#, JavaScript, and Java. Developers interested in early access can join the preview list through ABBYY's website.

PROTECTED Status for E-Signatures

Adobe has announced that its e-signature solution, Adobe Acrobat Sign, has successfully completed Australia's Infosec Registered Assessors Program (IRAP) assessment at the PROTECTED level as of March 2025.

This certification enables Australian government agencies at federal, state, and local levels to adopt Adobe's e-signature platform while meeting stringent security requirements for handling classified information.

The announcement comes as demand for secure digital services continues to grow in the public sector. Recent Adobe research has identified a direct correlation between reliable, accessible, and secure public services and higher citizen usage rates.

"This IRAP assessment reaffirms our commitment to providing enhanced yet trusted digital citizen experiences while maintaining the highest security standards," said an Adobe spokesperson.

The PROTECTED level certification verifies that Adobe Acrobat Sign aligns with the control requirements outlined in the Australian Information Security Manual (ISM), a cyber security framework established by the Australian Signals Directorate (ASD). The assessment follows Adobe Experience Manager Gov Cloud Australia's IRAP certification at the same level in March 2024.

Adobe Acrobat Sign provides end-to-end digital experiences for various signing workflows, enabling government agencies to securely manage large volumes of online signature processes, including identity management, authentication, access control, document integrity certification, and audit trails.

The platform also supports remote digital signatures backed by digital certificates from trust service providers with verified Cloud Signature Consortium integrations.

Adobe's security approach is built on its Common Controls Framework (CCF), which aligns with globally recognized standards including SOC2, ISO/IEC 27001:2013, ISO 22301:2019, PCI DSS, and FedRAMP.

Government agencies interested in learning more about the IRAP assessment can access the assessment letter through the Adobe Trust Centre.

Automate PDF Accessibility Workflow

In an era of increasing digital accessibility requirements, PDFix has launched a new solution aimed at streamlining the often complex and time-consuming process of making PDF documents compliant with accessibility standards.

The company's latest offering, PDFix Pipeline, allows organizations to automate their PDF accessibility workflows through a customizable, JSON-driven system that consolidates multiple tasks into a single process.

According to PDFix, the solution can reduce document processing time by up to 90% while eliminating costly manual errors that often plague traditional PDF remediation efforts.

"Every organization faces unique document challenges, and the demand for accessible PDFs has never been greater," a company spokesperson said.

"With strict standards like WCAG and PDF/UA, businesses must ensure compliance while managing complex document workflows. Yet, achieving this often requires multiple specialized tools, leading to slow, costly, and error-prone manual remediation. "

The software features a modular architecture that allows users to combine actions from different vendors and works across major platforms including Windows, MacOS, and Linux.

Its JSON-based configuration means organizations can create tailored document processing sequences without requiring coding expertise.

PDFix Pipeline is available now, with the company offering a free trial of its SDK for interested organizations.

https://pdfix.net/products/pdfix-sdk/

Unlock Archived Data for AI Apps

Archive360, a data archiving company, has launched what it claims is the first modern archive platform specifically designed to support artificial intelligence and analytics applications across enterprises and government agencies.

The company says its newly released Archive360 Platform represents a significant departure from traditional archiving approaches by creating what the company calls a "governed AI ready data cloud."

Unlike conventional archiving systems that primarily focus on long-term storage and compliance, this platform actively prepares archived data for AI consumption while maintaining strict governance and security controls.

The platform addresses growing concerns about AI data governance by enabling organizations to control precisely how artificial intelligence systems access archived information. This capability is particularly crucial as companies seek to leverage AI for applications ranging from fraud detection to workforce planning while avoiding the risks of exposing sensitive or regulated data.

Archive360's solution ingests data from various enterprise sources, including modern communications platforms, legacy ERP systems, and enterprise databases such as SAP, Oracle, and SQL Server. The platform then creates what the company describes as a "data agnostic, compliant active archive" that feeds both AI applications and traditional analytics tools.

The system includes built-in connectors to major analytics and AI platforms including Snowflake, Power BI, ChatGPT, and OpenAI, streamlining the process of making archived data available for analysis.

The platform is deployed using cloud-native architecture, providing each customer with a dedicated SaaS environment. This approach allows organizations to maintain complete data segregation while retaining administrative access and integration capabilities with existing security protocols.

Archive360 positions this launch as part of a broader shift from application-centric to data-centric archiving. Rather than managing multiple disconnected solutions for different types of applications, the platform offers a unified approach that the company says reduces technical debt and accelerates AI readiness.

The announcement comes as organizations across sectors struggle to balance the potential of AI applications with the need to maintain data governance and regulatory compliance. Archive360's platform aims to resolve this tension by providing controlled access to historical data alongside current information.

https://www.archive360.com/unified-data-governance

Successor for Cloud Identity Service

Delinea has announced a strategic partnership with Microsoft to support customers affected by the upcoming retirement of Microsoft Entra Permissions Management. The collaboration aims to provide a seamless transition path for enterprises seeking continued cloud identity protection after the service discontinues on October 1, 2025.

Delinea's Privilege Control for Cloud Entitlements (PCCE) solution will serve as the recommended alternative, offering comprehensive Cloud Infrastructure Entitlement Management (CIEM) capabilities across multiple cloud environments including Microsoft Azure, AWS, and Google Cloud Platform.

"The introduction of AI has led to an explosion of human and machine identities at a time when public cloud environments are growing increasingly complex," said Art Gilliland, CEO at Delinea, highlighting the critical nature of managing cloud privileges in today's security landscape.

The partnership builds on an existing relationship between the two companies focused on identity security.

Microsoft's VP of Product Management, Joseph Dadzie, expressed confidence in Delinea's solution as "a scalable, innovative approach to identity security" and "an effective successor" for current Entra Permissions Management customers.

Delinea's PCCE solution provides continuous discovery of identities, AI-powered analytics, and enforcement of least privilege principles to reduce risks associated with overprivileged accounts and misconfigured identity settings. This approach gives administrators greater visibility into cloud and identity usage patterns..

https://delinea.com/

Enterprise AI's Biggest Security Challenge

Confidencial.io, a data protection company with roots in DARPA-funded research at SRI, has announced a new AI data governance solution. The product aims to address one of the most critical challenges facing enterprise AI adoption: protecting sensitive information while enabling AI innovation.

The solution embeds a cryptographic security layer directly into AI pipelines and document repositories, allowing organizations to safely use their unstructured data - such as documents, transcripts, and images - for AI applications without risking data leaks or compliance violations.

"We're addressing the unsustainable model of fragmented systems that can't talk to each other," said Karim Eldefrawy, Co-Founder and CTO at Confidencial.

"One of the biggest barriers to deploying AI in the enterprise is ensuring consistent data protection, governance, and control across the entire AI pipeline, regardless of where or how that information is accessed."

The company cites surveys showing 61% of Chief Information Security Officers identify intellectual property leakage as their primary concern when implementing AI systems, while 59% worry about customer data exposure. These concerns have led many organizations to implement multiple disconnected protection tools, creating security gaps where sensitive data remains vulnerable.

Confidencial.io's solution takes a unified approach by applying data-centric Zero Trust principles at the object level, securing only the most critical information. This targeted protection also helps organizations reduce computing costs while maintaining compliance with NIST and ISO AI and Cybersecurity Frameworks.

The company also recently launched Cloud Protector, a next-generation Data Security Posture Management (DSPM) solution. Their new AI governance product extends this protection framework to cover both traditional and AI-driven data environments.

"Unstructured data is the fuel powering modern AI, and adoption is picking up serious momentum, especially with the rise of tools like Microsoft Markitdown and IBM Docling that convert files into text for LLMs and text analysis pipelines," said Eldefrawy.

"Confidencial is the only solution that can find and cryptographically protect sensitive information within these converted files, at a granular level, before they enter AI workflows and systems. This provably ensures enterprise-grade cryptographic security and compliance while enabling organizations to safely and cost-effectively unlock more of their data for AI training and innovation."

https://www.confidencial.io/

VAST unveils AI OS

Data infrastructure company VAST Data has announced the launch of its AI Operating System, a platform designed to power large-scale artificial intelligence workflows, as the firm reported reaching $US2 billion in cumulative bookings faster than any data company in history.

The New York-based company said it achieved nearly five-fold year-over-year growth in the first quarter compared to the same period last year, while maintaining a cash-flow positive business model. The milestone underscores growing enterprise demand for AI infrastructure capable of operating at unprecedented scale.

The VAST AI Operating System represents nearly a decade of development work aimed at creating what the company calls an "intelligent platform architecture" capable of harnessing AI supercomputing resources. Built on VAST's proprietary Disaggregated Shared-Everything (DASE) architecture, the system enables complete parallelization of AI and analytics workloads across distributed computing environments.

"This isn't a product release - it's a milestone in the evolution of computing," said Renen Hallak, VAST Data's founder and CEO.

"We've spent the past decade reimagining how data and intelligence converge. Today, we're proud to unveil the AI Operating System for a world that is no longer built around applications - but around agents."

The platform includes comprehensive distributed system components: a kernel for running platform services across private and public clouds, a runtime for deploying AI agents, realtime event processing infrastructure, messaging systems, and distributed file and database storage for real-time data capture and analytics.

Central to the new offering is the VAST AgentEngine, an auto-scaling AI agent deployment runtime that provides a low-code environment for building intelligent workflows. The system allows users to select reasoning models, define agent tools, and operationalize AI reasoning processes.

Building on the company's 2024 preview of InsightEngine - a service that extracts context from unstructured data using AI embedding tools - AgentEngine represents the next phase of VAST's AI strategy. While InsightEngine prepares data for AI consumption, AgentEngine enables AI agents to interact with that data in real-time.

The AgentEngine features an AI agent tool server supporting Model Context Protocol (MCP)-compatible tools, allowing agents to invoke data, metadata, functions, web search capabilities, or other agents. The platform enables agents to assume multiple personas with different purposes and security credentials while providing secure, realtime tool access.

The system's scheduler and fault-tolerant queuing mechanisms ensure agent resilience against machine or service failures. VAST also introduced what it calls "massively-scalable agentic workflow observability" through parallel, distributed tracing capabilities that provide developers with unified visibility into complex agentic pipelines.

VAST plans to release a set of open-source agents through AgentEngine, with one new agent launching monthly to accelerate adoption of AI computing. The agents will include both industry-specific personal assistants and general-purpose tools.

https://www.vastdata.com/

AI Document Processing Platform

San Francisco-based LlamaIndex has secured minority equity investments from data and AI company Databricks and professional services giant KPMG LLP. The funding will accelerate development of LlamaIndex's enterprise AI tools that help companies build intelligent agents capable of processing complex documents.

LlamaIndex specializes in helping organizations implement Retrieval-Augmented Generation (RAG) systems and document-based AI workflows. Their flagship products include LlamaParse, which extracts information from complex document formats, and LlamaCloud, a secure platform for document ingestion and retrieval.

LlamaIndex's suite of services enables organizations to efficiently connect their proprietary data to large language models (LLMs), solving one of the most significant challenges in enterprise AI adoption.

The company's flagship offerings include LlamaParse, which provides state-of-the-art parsing for complex documents with embedded tables and figures, and LlamaCloud, a managed ingestion and retrieval service that dramatically simplifies RAG (Retrieval Augmented Generation) implementations.

"Databricks and LlamaIndex share a common vision of democratizing access to AI by making it easier for organizations to harness the power of their data," said Patrick Wendell, Co-Founder & VP Engineering at Databricks.

"LlamaIndex's technology addresses a critical need in the enterprise AI stack, enabling companies to quickly build production-ready AI applications that leverage their proprietary data. This investment aligns perfectly with our mission to help customers drive innovation through data intelligence."

"As we continue to innovate and push boundaries in applied AI, a robust data foundation is essential for building effective AI systems, particularly sophisticated knowledge assistants and agentic solutions," said Swami Chandrasekaran, Principal and AI & Data Labs Leader at KPMG.

"LlamaCloud and LlamaIndex provide the frameworks necessary to access, curate, and ingest data at-scale, enabling KPMG to develop differentiated, industry-specific solutions that deliver measurable business outcomes for our clients."

The investment from Databricks comes through its Databricks Ventures' AI Fund, which was established to support innovative startups utilizing or enabling AI in conjunction with the Databricks Data Intelligence Platform.

This move follows Databricks' recent investments in other AI-focused companies including Mistral AI, Perplexity, and Cleanlab.

KPMG's investment is spearheaded by KPMG Ventures, which is dedicated to collaborating with and investing in early-stage start-ups in areas like agentic AI, data infrastructure, cybersecurity, and more. KPMG Venture's minority equity investment follows recent investments in other AI-driven startups including Ema, Wokelo and Rhino.AI.

"We're excited to work with industry leaders like Databricks and KPMG to bring enterprise-grade LLM infrastructure to more organizations worldwide," said Jerry Liu, Co-Founder and CEO of LlamaIndex.

Customers including Cemex and Carlyle Group have reported significant productivity gains using LlamaIndex's technology. Daniel G Zapata, Senior Data Scientist at Cemex, noted that tasks "that used to drag on for weeks now ship in days" thanks to LlamaIndex's solutions.

"As the Applied AI Lead at Carlyle, one of Databricks' enterprise clients, I've evaluated numerous document processing solutions for our AI initiatives. LlamaIndex's LlamaParse stands out as the premier solution for integrating complex documents into our advanced analytics pipeline," said Dean Barr, MD, Head of Applied AI and Data Scientist at The Carlyle Group.

"Its exceptional handling of nested tables, complex layouts, and image extraction has been instrumental in our data-driven investment strategies, particularly when combined with Databricks' powerful data processing capabilities."

Financial terms of the investments were not disclosed.

https://www.llamaindex.ai/

Nintex Employee Onboarding Solution

Process automation company Nintex has unveiled a new pre-built solution designed to address what research shows is a costly problem for employers: poor employee onboarding that drives early departures and wastes thousands of dollars per hire.

The company's new Nintex Employee Onboarding platform aims to streamline the complex, multi-departmental process that often leaves new hires frustrated and employers scrambling to coordinate between HR, IT, and finance teams.

According to studies cited by Nintex, 80% of employees who experience poor onboarding plan to leave their jobs soon after starting, while 17% of new hires actually do quit within their first 90 days.

With the average cost to onboard a single employee reaching $US1,500, the financial impact adds up quickly. For a company hiring 100 people, that translates to $25,500 wasted on the 17 employees who leave within three months due to onboarding problems.

"Employee onboarding touches every employee that enters an organization," said Niranjan Vijayaragavan, Chief Product Officer at Nintex. "Getting it right isn't only important for employee experience and retention, but delays and disruptions throughout onboarding can negatively impact a business's bottom line."

The challenge stems from onboarding's complexity. While many organizations have automated core HR functions through applicant tracking and human resources information systems, the onboarding process typically requires coordination across multiple departments and systems, often leaving critical workflows manual and prone to delays.

Nintex's solution attempts to solve this by providing a centralized platform that integrates with existing HR systems while eliminating the need for multiple bolt-on applications. The system allows HR teams to create branded portals where new hires can complete tasks through self-service interfaces, while automatically importing employee data to reduce redundant entry work.

Key features include customizable approval workflows, document management with electronic signatures, and role-specific onboarding paths. An internal operations portal gives administrators a single view to track progress and manage the entire process.

The employee onboarding solution was built using Nintex's Solution Studio platform and represents the company's expanding focus on pre-built industry solutions. The Bellevue-based company, which serves more than 8,000 organizations across 90 countries, previously launched a licensing and permitting solution for government agencies.

Nintex is now expanding that government solution to the Asia-Pacific region after initially rolling it out to U.S. state and local agencies in 2024.

IBM Unlocking Unstructured Data for Generative AI

Unstructured data – buried in contracts, spreadsheets, and presentations – is one of the most valuable but underutilized resources in the enterprise. IBM is evolving watsonx.data to help organizations activate this data to drive more accurate, effective AI.

TIBM says its evolution of watsonx.data will bring together an open data lakehouse with data fabric capabilities – like data lineage tracking and governance – to help clients unify, govern, and activate data across silos, formats, and clouds. Enterprises will be able to connect their AI apps and agents with their unstructured data using watsonx. data, which tests show can lead to 40% more accurate AI than conventional RAG.

IBM is also introducing watsonx.data integration, a single-interface tool for orchestrating data across formats and pipelines, and watsonx.data intelligence, which uses AI-powered technology to extract deep insights from unstructured data. They will be available as standalone products, with select capabilities also available through watsonx.data – maximizing client choice and modularity.

To complement these products, IBM recently announced its intent to acquire DataStax, which excels at harnessing unstructured data for generative AI. With DataStax, clients can access additional vector search capabilities. Further, watsonx is now integrated as an API provider within Meta's Llama Stack, enhancing enterprises' ability to deploy generative AI at scale and with openness at the core.

Edward Calvesbert, Vice President, Product Management, watsonx Platform, writes, "Enterprises are facing a major barrier to accurate and performant generative AI - especially agentic AI. But the barrier is not what most business leaders think.

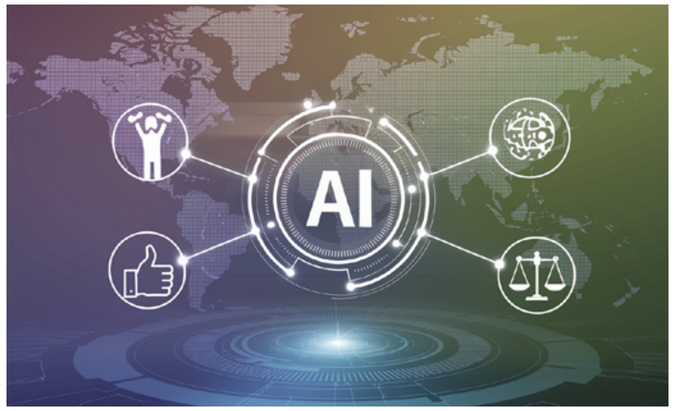
"The problem is not inference costs or the elusive "perfect" model. The problem is data.

"Organizations need trusted, company-specific data for agentic AI to truly create value - the unstructured data inside emails, documents, presentations, and videos. It is estimated that in 2022, 90% of data generated by enterprises was unstructured, but IBM projects only 1% is accounted for in LLMs.

"Unstructured data can be immensely difficult to harness. It is highly distributed and dynamic, locked inside diverse formats, lacks neat labels, and often needs additional context to fully interpret. Conventional Retrieval-Augmented Generation (RAG) is ineffective at extracting its value and cannot properly combine unstructured and structured data.

"IBM's new capabilities will enable organizations to ingest, govern and retrieve unstructured (and structured) data—and from there, scale accurate, performant generative AI."

Dataminr Announces Agentic AI Plans



Dataminr has unveiled its first Agentic AI capability with the launch of Intel Agents, an autonomous system designed to independently generate critical contextual information during unfolding events.

The new technology represents the initial phase of the company's broader Agentic AI roadmap, which aims to transform how organizations process realtime information and respond to emerging threats.

"Intel Agents fundamentally changes how organizations can process realtime information," said Ted Bailey, Dataminr's Founder and CEO.

"This technology gives our clients the surrounding context they need to respond faster and more effectively to emerging events."

Building upon their 2024 ReGenAI technology, which automatically updates event briefs in realtime, Intel Agents add an additional layer of context through autonomous analysis. The system continuously evaluates new developments and updates relevant information without human intervention.

Alex Jaimes, Dataminr's Chief AI Officer, explained that the technology works by having agents determine what additional context is needed, locate that information, and synthesize findings into concise, actionable intelligence.

The company emphasized that Intel Agents run exclusively on Dataminr's proprietary large language models (LLMs), which have been trained on the company's 15-year archive of data and events.

The initial deployment will focus on cybersecurity through Dataminr Pulse for Cyber Risk, with the capability already being piloted to generate enhanced realtime threat intelligence. The company plans to expand the technology across its platform in the coming months.

Looking further ahead, Dataminr outlined two major upcoming developments: Client-Tailored Context, which will customize information based on specific client operations and risk profiles, and PreGenAI, scheduled for 2026, which aims to predict future scenarios as events unfold.

Dataminr has positioned itself as an early adopter in the AI space, having integrated LLMs into its products since 2020. The company processes massive amounts of multi-modal data across 220+ countries and 150+ languages, with an AI system that performs the equivalent work of what would require 30,000 people working around the clock.

Intel Agents are currently available in private beta with general availability expected in early Q3 2025.

https://www.dataminr.com/

Informatica Unveils AI-Enhanced Data Management Tools

Informatica has announced new capabilities designed to streamline access to AI-ready data across organizations. The enhancements to its Intelligent Data Management Cloud (IDMC) platform leverage the company's CLAIRE AI engine to ensure data is more accessible, reliable, and appropriate for AI initiatives.

Among the key innovations are CLAIRE Copilot for data integration and iPaaS (Integration Platform as a Service), both currently in preview. These tools enable users to generate data pipelines using natural language, create complex multi-step integration processes, and automate documentation, potentially saving hours of development time.

"By integrating CLAIRE AI capabilities across our Intelligent Data Management Cloud, we're empowering organizations to manage their data with unprecedented efficiency," said Pratik Parekh, Senior Vice President and General Manager at Informatica.

"These new features boost developer productivity, enable new use cases and democratize data access which helps enterprises accelerate their AI initiatives and governance. Our commitment remains focused on helping businesses unlock the full potential of their data assets in today's AI-driven landscape."

The company has also introduced unstructured data processing capabilities with AI-powered intelligent parsing and transformation features, along with pre-built GenAI integration templates for popular platforms including Amazon Bedrock, Azure OpenAI, and Google Cloud Vertex AI. For Master Data Management (MDM), Informatica has integrated CLAIRE GPT to enable natural language-based search and metadata exploration, while also automatically generating glossary descriptions to improve data understanding across teams.

"By integrating CLAIRE AI capabilities across our Intelligent Data Management Cloud, we're empowering organizations to manage their data with unprecedented efficiency," said Pratik Parekh, Senior Vice President and General Manager at Informatica.

While the CLAIRE Copilot capabilities remain in preview, Informatica announced that other features will be globally available by April 2025.

https://www.informatica.com/

Is your organisation ready for Microsoft's "New Outlook"?

"New Outlook" is a refreshed version of the Outlook for Windows app, offering a more modern and simplified user experience. Designed to be more agile, deliver features faster and provide a consistent experience across Windows, it's not a replacement for the classic desktop program – rather an evolution!

Microsoft has announced a progressive roll-out of the "New Outlook", allowing organisations to manage the transition to this new experience across the enterprise. Many organisations are already transitioning to the "New Outlook", others planning the move over the coming months. Microsoft has advised that "New Outlook on Windows aims to unify the extensibility experience across all Outlook platforms. To provide a more reliable and stable add-in experience, VSTO and COM add-ins aren't supported on the new Outlook on Windows".

Microsoft is focusing on a new platform for Outlook add-ins based on Office add-ins, which utilises technologies such as HTML, CSS and JavaScript. To continue using add-in in the "New Outlook", VSTO add-ins need to be migrated to this new Office add-ins platform.

The team at OpenText has been preparing for this change and now offers an alternative integration add-in for Content Manager that leverages the modern, Office add-ins platform. This integration, known as the Zero Footprint (ZFP) Integration, allows the user to integrate Content Manager with Zero FootPrint (ZFP) Office applications, Teams, and Outlook.

Kapish can assist your organisation to deploy the new Content Manager ZFP Integration as your organization transitions to the "New Outlook".

Contact Kapish today to future-proof your Content Manager Outlook Integration.

Klippa's DocHorizon Platform Launches

Dutch technology company Klippa has secured its first strategic partnership in Australia, marking a significant expansion for the document automation specialist into the Asia-Pacific region.

The Amsterdam-based firm announced has partnered with Ben Accord Business Solutions, an established consulting firm specialising in SAP HANA implementations and financial business transformation. The collaboration represents Klippa's inaugural entry into the Australian market after building a presence across Europe with over 1,000 clients.

The partnership centres on integrating Klippa's DocHorizon platform, which uses artificial intelligence to automate document processing workflows. The technology can scan, read, sort, extract, anonymise and verify documents at scale through APIs and software development kits."

Ben Accord brings more than 40 years of combined experience in SAP implementations and deep expertise in enterprise resource planning systems. The Melbourne-based consultancy works with clients across various industries to streamline processes and improve profitability through best practices and automation tools.

Initially, the collaboration will focus on optimising document processing for businesses seeking more efficient and cost-effective solutions. As the partnership develops, there are plans to introduce Klippa's SpendControl platform, which helps companies manage expenses and invoice processing.

The partnership offers Australian businesses access to software-as-a-service alternatives to traditional packaged software, allowing organisations to modernise without rebuilding legacy systems. The collaboration aims to help companies automate administrative workflows while preserving their unique requirements.

https://benaccord.com/

Metomic Closes AI Security Gaps

Metomic has unveiled a new AI Data Protection Solution aimed at enterprise customers. The security platform is designed to prevent confidential business information from being inadvertently leaked through popular AI systems like ChatGPT, Microsoft Copilot, Glean, Notion AI, Box AI, and others.

According to recent industry research, 81% of Chief Information Security Officers express significant concern about sensitive data being unintentionally accessed by AI tools, workflows, or training sets. This worry comes as AI and machine learning integration tops the priority list for Chief Information Officers in 2025.

"AI tools are rapidly becoming integral to enterprise operations, but they also introduce new vectors for data leakage," said Ben van Enckevort, Co-Founder and CTO of Metomic.

The platform utilizes advanced algorithms to identify and classify sensitive business data across platforms like Slack, Google Drive, Notion, GitHub, Salesforce, M365, Box, and Jira, while continuously monitoring data interactions with AI tools, providing instant alerts.

Granular Access Controls provide precise access permissions to ensure that only authorized AI tools and users can interact with sensitive business data.

Metomic is a data security platform designed to protect sensitive business data across SaaS, GenAI, and cloud applications.

https://www.metomic.io/

Backdoor Attack Exploits Teams

Cybersecurity firm ReliaQuest has uncovered a sophisticated attack campaign that uses Microsoft Teams to deploy a previously unknown backdoor malware. The attacks, which began in March 2025, specifically target female executives in the finance and professional services sectors.

The attack chain begins with carefully timed phishing messages sent through Microsoft Teams from accounts posing as technical support staff. Once victims are convinced to launch Windows' built-in "Quick Assist" tool, attackers gain access to their systems and implement a novel persistence technique called TypeLib hijacking.

"This is the first time we've seen TypeLib hijacking used in the wild," said Hayden Evans, the primary author of the ReliaQuest report. "Attackers are modifying Windows Registry entries to redirect legitimate COM objects to malicious scripts hosted on Google Drive."

The technique ensures that the malware, a sophisticated PowerShell backdoor, is automatically downloaded and executed whenever the system restarts. According to ReliaQuest, the backdoor contains extensive "junk code" designed to evade detection, with several space-themed keywords like "Galaxy," "Cosmos," and "Orion."

Analysis of the attack infrastructure suggests the malware has been in development since January 2025, with early versions deployed through malicious Bing advertisements. The report notes that Telegram bot logs associated with the malware contained Russian text, indicating the developer is likely from a Russian-speaking country.

ReliaQuest believes the attackers may be connected to Storm-1811, a threat group known for deploying Black Basta ransomware. However, the report suggests several possibilities: either Black Basta has adopted new techniques, the group has splintered, or an entirely different group has begun using similar initial access tactics.

To protect against these attacks, ReliaQuest recommends disabling external communication in Microsoft Teams, blocking specific domains at the network edge, disabling JScript via Group Policy, and implementing Windows Defender Application Control to restrict PowerShell functionality.

The report highlights a concerning trend in cybersecurity: increasingly targeted attacks that exploit legitimate collaboration tools to bypass traditional security measures. With Microsoft Teams now a standard communication platform in many organizations, security experts warn that similar tactics will likely become more common.

Data Management for AI Apps

Nextdata has launched a unified platform designed to simplify and automate data management across organizations, Nextdata OS.

The platform introduces autonomous data products that simplify and streamline data management for AI agents, analytics and applications by encapsulating complexity and standardizing and automating data product management across heterogeneous data stacks in complex organizations.

According to Nextdata, enterprises currently struggle with inefficient data management due to centralized data teams and fragmented technology stacks. The company claims these bottlenecks result in costly replatforming projects and ongoing maintenance burdens that consume operating budgets.

Nextdata's approach uses "data product containers" that encapsulate the entire data supply chain, from ingestion to quality enforcement. These containerized products continuously monitor their environment and dependencies to automatically orchestrate data processing, access control, and compliance.

"We've reimagined data management as autonomous, decentralized, self-governing data products - built to work with your systems and for you," said Nextdata founder and CEO Zhamak Dehghani

The platform provides self-service features allowing independent teams to build, share, and discover autonomous data products, which the company says reduces manual tasks and cross-functional dependencies typically found in centralized data operations.

Unlike traditional data catalogs, Nextdata OS incorporates automated governance and security features that enforce policies throughout the data lifecycle. The system works with various data types and formats, integrates with existing data stacks, and offers enterprise-wide visibility into data product health and utilization.

https://www.nextdata.com/

AI Assistant to Generate Workflows

Nintex has unveiled a suite of new generative AI capabilities designed to help businesses create automation solutions faster and with less technical expertise. The new features enable users to generate processes, workflows, forms, and custom integrations using simple language prompts.

The company's latest AI tools are built into the Nintex Automation CE platform and aim to reduce the time and resources needed to design and deploy automation projects. These new capabilities include an AI Process Generator, AI Forms Assistant, AI Workflow Generator, and AI Xtensions Generator.

The AI Process Generator allows users to create new processes within Nintex Process Manager, while the AI Forms Assistant enables users of all technical skill levels to build sophisticated forms through conversational interaction.

The AI Workflow Generator helps users create simple to complex workflows from natural language prompts, and the AI Xtensions Generator builds custom connectors between core business systems and Nintex Workflow.

Nintex Xtensions are used to create API connections required for workflow actions to integrate with third-party services, enabling them to perform actions such as retrieving data, sending notifications, or updating records from the external applications and services.

Nintex has also announced Nintex DocGen for Salesforce, which allows Salesforce users to generate and manage documents using AI agents directly within Salesforce, connecting generated documents to records.

Nintex DocGen® for Salesforce is currently available on AppExchange at www.appexchange.com/.

https://www.nintex.com/

AI-Powered LGA Planning Platform

ASX-listed Objective Corporation is set to launch a new planning technology platform designed specifically for Australian local councils, addressing widespread challenges with development approval backlogs and resource constraints across the sector.

The platform represents a year-long collaboration with councils and planners nationwide to reimagine statutory planning processes.

"We've spent the last year working hand-in-hand with councils and their planners across Australia to reimagine how statutory planning can work efficiently, transparently, and without the admin grind," said Andrea Breen, VP Local Government Solutions at Objective.

The new platform addresses a critical pain point for Australian councils, which face mounting pressure to approve more housing developments while operating with fewer resources and outdated planning systems. Many councils currently rely on what industry insiders describe as a "patchwork of processes" that weren't designed for current demands.

The solution includes smart workflow automation aimed at speeding up approvals and reducing delays, alongside AI-powered tools that surface relevant past decisions to improve consistency across planning decisions. The platform also offers end-to-end compliance visibility with integration to the NSW Planning Portal.

For management oversight, the system provides customisable reporting and real-time dashboards designed for team leaders and executives to monitor planning operations.

"This is about more than just tech," Breen explained. "It's about giving planners the time, tools, and trust they need to focus on what they were trained to do - shape great communities."

The announcement comes as councils across Australia grapple with approval backlogs and planner burnout, issues that have become increasingly prominent as housing demand outpaces supply in many regions.

Objective Corporation trades on the ASX under the code OCL and provides enterprise information management solutions to government and corporate clients across Australia and internationally.

iWorkplace Elements launches in Australia

IT solution provider Professional Advantage is launching iWorkplace Elements in Australia, a self-service solution that transforms digital workspaces.

Developed by New Zealand-based IT company Information Leadership, it addresses issues typically experienced in out-of-the-box Microsoft 365 deployments by many small to mid-sized businesses.

Andrew MacKenzie, Modern Work Practice Lead at Professional Advantage, said "While SharePoint and Teams have provided valuable collaboration features, SMBs often struggle with self-managing their environments. Additionally, enterprise customers face scaling challenges."

"We all need to do better with our retention and disposal of content; the Privacy Act tells us so, and the recent uplift to the Privacy Act in Australia (September 2024) means information protection and compliance are even more relevant to small and large businesses alike," continued MacKenzie.

"Microsoft offers some great controls with Purview, but it can be an expensive step up if clients do not have E5 licensing.

"Purview also requires IT admins or consultants to configure and maintain the controls. iWorkplace Elements bridges this gap by offering a user-friendly solution that empowers businesses to take control of their digital workspace," he said.

iWorkplace Elements features include:

■ Seamless integration with SharePoint, Teams, and Azure;

■ Customisable workflows to meet specific business needs;

■ Advanced security to protect sensitive information and ensure compliance with regulations; and

■ Metadata-driven search to enhance information retrieval for better compliance and management.

The core offering, iWorkplace Elements Essentials + Preview, delivers modern document management and automated workflows. It is a self-deployable solution, supported by Professional Advantage's experts, that enables your team to set up a modern digital workplace in days.

Additional modules cater to specific business needs, including Policies and Procedures, Search, Employee Files, Contract Management, and more.

As the sole strategic partner of Information Leadership in Australia, iWorkplace Elements is exclusively available at Professional Advantage.

Visit pa.com.au/iworkplace to book a demo.

AI-Powered Data Governance on Google Cloud

Striim has announced two governance AI agents powered by Google Cloud's Vertex AI platform to help organizations detect, tag, and safeguard sensitive data in motion, reducing exposure risks, avoiding penalties and reputational damage, and supporting compliance in a continuous, ongoing manner.

Sentinel AI and Sherlock AI are designed to assist enterprises face an emerging challenge: how to maintain control over sensitive data as it traverses data estates, domains, and systems without violating regulatory policies or disrupting operations.

Before businesses can manage sensitive data effectively, they need visibility into where the data resides. Sherlock AI provides transparency by identifying sensitive data within datasets prior to sharing or moving the data through integration or streaming pipelines in enterprise data stores as well as third-party-managed databases and SaaS environments.

This helps organizations assess potential risks and apply the appropriate governance measures proactively.

"Smart AI and Analytics require data integration and sharing. Data governance starts with knowing where your sensitive information is," said Alok Pareek, co-founder and Executive Vice President of Engineering and Products at Striim.

"The new AI-based Sherlock agent eliminates blind spots by discovering sensitive data prior to data sharing or movement, helping businesses reduce risk before it ever becomes a problem.

But since data doesn't stay in one place, Striim's Sentinel AI agent complements Sherlock by protecting sensitive information as it moves through enterprise data pipelines in real time."

Once data is in motion, Sentinel AI continuously analyses live data streams to detect and protect sensitive information as it moves - automating encryption, masking, and compliance enforcement in realtime.

Using Google Cloud's Vertex AI, it detects sensitive data anywhere in the pipeline events, even if misplaced or mislabelled - something rules-based controls can easily miss.

Therefore, it automatically prevents exposure and helps businesses meet GDPR, CCPA, and HIPAA-related data governance requirements without adding complexity.

https://www.striim.com/

Mobile Scanning Platform for Freight Documentation

Transflo, a supply chain software solutions provider, has released version 6.0 of its Transflo Mobile+ app, featuring a completely redesigned document scanning engine that promises to streamline operations for truck drivers and carriers.

The company, which has been in the document digitization business for over 30 years, has rebuilt both the frontend and backend of its scanning technology.

The new version introduces an intuitive "Snap, Tap, and Done" user experience, alongside significant improvements to image optimization, Optical Character Recognition (OCR) performance, and compression capabilities.

"This release of Transflo Mobile+ makes it easier and faster for drivers to capture their documents and connect more seamlessly to back-office workflows," said Renee Krug, CEO of Transflo.

With more than three million downloads and processing nearly a billion documents annually, the app now includes enhanced automatic features like capture, de-skewing, and edge detection to reduce friction in daily supply chain documentation tasks.

Justin King, Transflo's Chief Product Officer, noted that the improvements resulted from "countless hours of detailed user feedback from carriers and drivers," emphasizing the company's commitment to solving fundamental user problems.

Beyond the scanning engine, version 6.0 also offers UI enhancements, support for additional third-party app deep links, and improved in-app performance.

The update is available on both the Apple App Store and Google Play.

https://www.transflo.com/