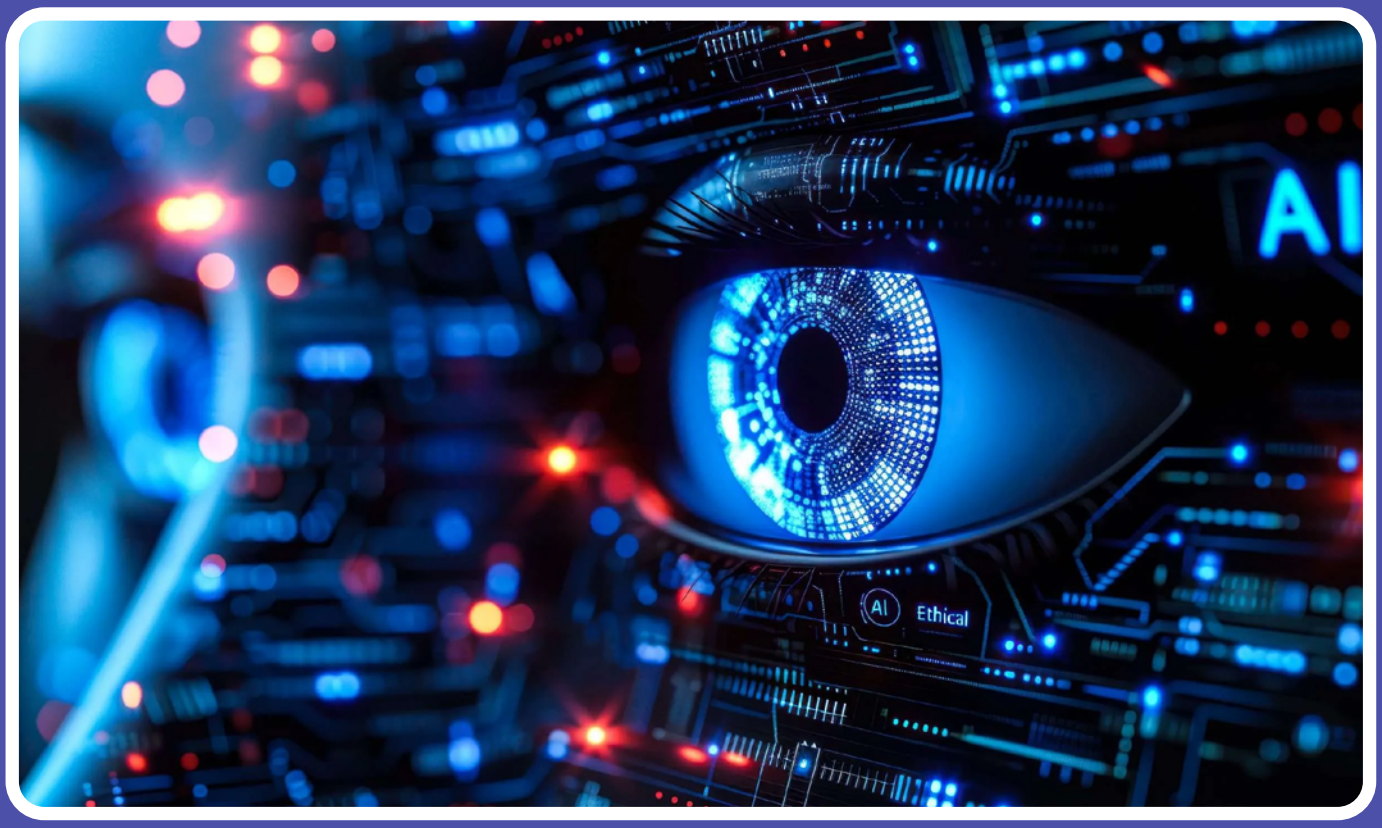
idm.
information & data manager
OCTOBER-NOVEMBER 2025

Ministry of Defence

The Hidden Rows That Cost Billions



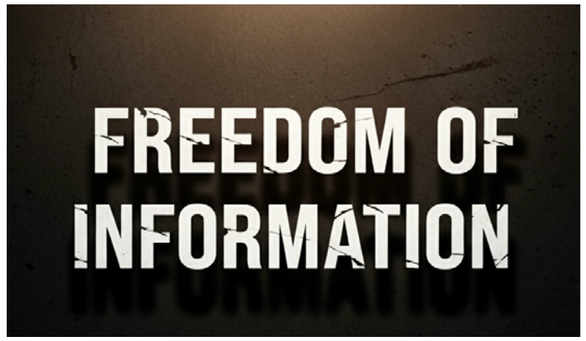
AI Enterprise Assistants Become Attack Targets

The Relationship Between Data Governance and Data Quality

AI agents are here. Here's how they can go wrong

FOI Reform Ignores AI Implementation Issues

Australia's proposed Freedom of Information Amendment Bill 2025 fails to address how artificial intelligence should be used in making or processing government transparency requests, according to a new analysis by law firm King & Wood Mallesons that identifies critical gaps in the legislation.



The Bill, introduced into the House of Representatives last week, aims to "modernise the requirements for Freedom of Information requests" but remains silent on AI's role in FOI processes, write senior associate Kendall Mutton and partner Rebekha Pattison in their legal analysis.

"Curiously, the Bill is silent on the use of AI systems to make or process freedom of information requests," the authors note, despite AI already being implemented across multiple Australian Government agencies.

The lawyers identify three key areas where the legislation creates uncertainty: whether AI can autonomously make FOI requests, how to process requests involving AI-generated government decisions, and using AI to handle FOI applications.

"It is conceivable that an AI system could be trained to itself make an FOI request," Mutton and Pattison write, but conclude that "the better view for the current compilation of the FOI Act is that AI cannot itself make a valid FOI request as AI is not a 'person'."

A significant compliance question emerges around whether AI-generated government information constitutes a "document" subject to FOI disclosure. Under the FOI Act, documents are broadly defined to include "any article on which information has been stored or recorded, either mechanically or electronically, as well as any other record of information."

Crucially, the lawyers note there is "no requirement in the FOI Act for a document to have been created by a 'person'" and this gap isn't addressed in the Bill. They conclude that "AI-generated information seems likely to be considered an article on which information has been stored or recorded, either mechanically or electronically, for the purpose of the FOI Act."

This interpretation gains support from case law in other jurisdictions. In DPP v Khan, the Supreme Court of the Australian Capital Territory referred to AI-generated character references as "documents," though "there was no detailed commentary on whether and why AI-generated material constitutes a document."

However, "whether the underlying algorithm used to generate the information will be similarly caught is a trickier question," the analysis states. This depends on algorithm content and request scope – for example, if an FOI request seeks documents containing specific terms, it "could conceivably include an AI algorithm which uses that term, if the algorithm is considered to be a document."

The analysis highlights practical enforcement challenges, noting: "As a practical matter, unless the FOI Act is amended or an agency requests that the use of AI is disclosed when making a request, it may be difficult to identify when a request has been generated using AI."

For government agencies implementing AI systems, the legal experts identify "one exciting opportunity" in using AI to generate "significant efficiencies" in processing FOI requests. United States government agencies have been testing AI since mid-2023 to perform keyword searches, summarise document characteristics, and identify potential exemptions.

However, the Bill doesn't clarify whether automated systems can make FOI decisions. "It is not clear whether this was a deliberate decision to keep this type of administrative action in the hands of human decision makers given the levels of judgment that are often required, or whether this was a missed opportunity to open the door for more efficient processing," the authors observe.

View the original article here

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

NSW Digital Defences Found Wanting

NSW Government agencies are struggling to meet basic cyber security requirements, with only 31% of mandatory protection controls being implemented across the sector, according to a report released by the state's Auditor-General.

The Cyber Security Insights 2025 report reveals that while cyber threats are escalating rapidly – with incidents involving third-party systems nearly tripling in the past year – most state agencies remain inadequately prepared to defend against attacks.

The audit found that agencies performed worst in the "Protect" domain, which includes essential safeguards like regular software updates, multi-factor authentication, and network security controls designed to prevent cyber attacks.

"The absence of 'protect' domain controls increases the likelihood of a successful cyber attack," the report warns, noting that many agencies still report zero maturity for critical protections despite years of focus on cyber security improvements.

Budget constraints and ongoing cyber security upgrade programs were cited as the primary reasons agencies couldn't meet minimum requirements.

The findings come as Cyber Security NSW reports a near-tripling of incidents involving systems owned or managed by third parties, including increased data breaches. However, the audit revealed a concerning blind spot: when cyber security controls are managed by external providers, compliance is not being reported to authorities.

"Agencies and Cyber Security NSW may not be aware of any non-compliance against the Cyber Security Policy where the cyber security control practice is provided by third parties," the report states.

Of the 66 agencies that reported their cyber security status in 2024, 27 disclosed a total of 152 significant, high, and extreme cyber security risks. Alarmingly, 28 of these risks had treatment controls that were either "largely ineffective" or "totally ineffective."

The report also highlighted concerning gaps in oversight, with 59% of agencies lacking independent assurance over their cyber security assessments – raising questions about the accuracy of their self-reported compliance.

Another significant concern identified was the shift toward aggregated reporting, where 66 reports now represent 177 agencies, compared to 110 individual reports in 2023. This consolidation potentially obscures cyber security weaknesses at individual agencies within larger portfolios.

Despite years of emphasis on the Australian Cyber Security Centre's Essential Eight mitigation strategies, many agencies continue to fall short. Some reported zero maturity for critical controls including application management, system patching, and administrative privilege restrictions.

While cyber security awareness training has improved, with 96% of state agencies now conducting phishing simulations, the local government sector lags behind with 45% of councils failing to test staff responses to simulated attacks.

The report notes that cultural factors and competing business priorities often drive non-compliance with security protocols, with staff sometimes bypassing procedures during emergencies or time-sensitive work.

The audit examined seven years of cyber security reports across state agencies, universities, and local councils, revealing inconsistent progress. While universities have achieved 100% implementation of cyber security policies, only 74% of councils have established such policies.

Auditor-General Bola Oyetunji emphasized the need for improved independent oversight of agency cyber security assessments, noting previous recommendations for stronger assurance processes that remain partially implemented.

The full Cyber Security Insights 2025 report is available here.

Ransomware Paid Despite Warnings

The vast majority of Australian organisations are still capitulating to ransomware demands, with new research showing 91% of local security leaders paid attackers in the past year despite repeated warnings from law enforcement agencies.

The findings, released in Rubrik Zero Labs' "*State of Data Security in 2025*" report, are based on insights from over 1,600 IT and security leaders across 10 countries, and found that 92% of Australian organisations experienced a cyberattack in 2024.

One of the most notable findings in this year's report was that 92 per cent of local organisations experienced a cyberattack last year. In a typical ransomware attack, the victim would be able to restart their operations by recovering data from their backup systems. However, Rubrik's research found these systems were routinely being compromised during an attack to disrupt recovery attempts. Of the Australian IT and security leaders that experienced a ransomware attack, 78 per cent said the threat actors were able to at least partially harm backup and recovery options – more than a third (35%) said the attackers were completely successful in doing so.

The research highlights how Australia's rapidly expanding digital footprint is creating new vulnerabilities. Almost all Australian respondents (98%) reported using between two and five cloud and Software-as-a-Service (SaaS) platforms for data storage and applications, with more than two-thirds planning to increase their cloud usage over the next year.

This proliferation of platforms is creating an increasingly complex security landscape. Australian organisations identified securing sensitive data across multiple environments (38%), data compliance and privacy concerns (34%), and lack of centralised management (34%) as their primary challenges.

This evolution in attack methods is driving calls for organisations to adopt what security experts term an "assumed breach mindset" – accepting that prevention measures will eventually fail and focusing equally on robust recovery strategies.

The report's methodology included analysis of 5.8 billion files across cloud and SaaS environments, with over 175 million sensitive files classified across customer environments, covering the period from January 1 through December 31, 2024.

View the full report here.

Digital Investment Rises as Compliance Challenges Mount: Maddocks

Australian organizations are rapidly embracing digital transformation and artificial intelligence, but their legal and governance frameworks are failing to keep pace with technological advancement, according to a comprehensive new survey by law firm Maddocks.

The *Digital Transformation 2025 Legal Trends Benchmarking Survey*, which surveyed a broad cross-section of the firm's business and government clients, found that while organizations rated their average technology maturity at 6.3 out of 10, more than half (54%) admitted they were not prepared for recent reforms to the Privacy Act. Respondents primarily came from legal and risk departments (49%), IT (18%), and operations (11%).

The findings reveal a concerning disconnect between technology adoption and legal preparedness, with 41% of respondents lacking proper controls for artificial intelligence systems despite 69% having implemented AI policies.

Cyber security emerged as the top technology priority for 2025, with 36% of organizations ranking it highest and 57% expressing serious concern about cyber threats to their operations. The heightened focus comes as data security was identified as the greatest technology-related challenge facing organizations.

"Cyber security spend has become a top priority for both technology and legal teams as the increased risk of threats and recent legislative changes make it apparent that privacy and cyber security is no longer just a problem for IT departments," said Brendan Tomlinson, Partner and Technology Sector Lead at Maddocks.

Despite this concern, the survey revealed significant gaps in cyber preparedness. While 91% of respondents have cyber incident response plans, only 65% regularly update key stakeholders on these plans, and 38% do not conduct practice exercises or role-playing scenarios.

The survey found widespread AI adoption across Australian organizations, with IT departments leading implementation (60% adoption rate), followed by sales and marketing teams and administrative functions.

However, this rapid uptake has created new challenges around data privacy, security, and regulatory compliance.

Leading concerns about AI use included data privacy and security issues, with 72% of respondents worried about ethical considerations and 66% concerned about regulatory compliance.

Organizations are struggling with increasingly complex technology contracts, with 71% identifying tracking performance and compliance as their most significant challenge.

Risk allocation emerged as a key concern, with 54% of respondents wanting to see more favorable allocation of risk and liability in their technology agreements.

Nearly 70% of organizations expressed concern about becoming involved in technology-related disputes, with almost 22% having experienced reputational damage due to technology platforms in the past year.

Despite the governance challenges, technology investment remains strong. The survey found that 56% of organizations are planning major technology procurement or projects this year, while 51% expect to spend more on technology than in the previous financial year.

The research, which included responses from across industries including government (48% of respondents), healthcare, finance, and manufacturing, highlights the urgent need for organizations to strengthen their legal and governance frameworks to match their technological ambitions.

"Organizations are increasingly understanding that implementing an agile and skilled workforce is vital to adapt swiftly to evolving digital shifts and opportunities," Tomlinson noted, emphasizing that organization-wide education and training on technology legal issues is becoming critical.

View the full Survey Results here.

AML Compliance Deadline looms in 2025

Smaller financial institutions face mounting pressure to meet anti-money laundering (AML) compliance standards as regulators increasingly target firms previously considered low-priority, according to analysis from compliance technology provider Consilient.

Community banks, neobanks, money services businesses and crypto platforms now face the same AML obligations as major institutions despite having fewer resources and less sophisticated technology systems, the company said in a recent analysis.

Smaller institutions face specific structural disadvantages that make AML compliance disproportionately difficult, according to the analysis. These include operating with tighter profit margins where AML compliance represents a growing cost rather than revenue-generating activity, unlike larger institutions that can spread compliance costs across broader portfolios.

Access to advanced AML technologies such as real-time risk scoring engines and AI-enhanced screening tools often remains beyond smaller institutions' budgets. This forces reliance on manual processes, outdated systems or lower-capability vendors, increasing operational risk and the likelihood of control breakdowns.

Resource constraints compound the problem as smaller firms must manage cybersecurity, liquidity, data privacy and regulatory reporting with limited headcount. While larger institutions operate specialised compliance teams, smaller entities often rely on staff handling multiple roles or outsourced services.

Recruiting experienced compliance professionals presents another challenge, with larger banks better positioned to attract seasoned AML officers. Smaller firms, particularly in regional areas, struggle to compete for talent, resulting in insufficient internal expertise for risk assessments and customer due diligence.

The analysis also identifies difficulties establishing compliance culture in smaller organisations where commercial pressures and growth targets can overshadow regulatory obligations.

Consilient claims its federated learning technology can help address compliance gaps by allowing institutions to collaborate on training advanced risk models without sharing sensitive data. The company asserts its AML models deliver "up to 4x greater detection effectiveness and a 75% improvement in efficiency" compared to traditional systems.

The technology allows smaller institutions to benefit from machine learning models trained across multiple organisations while keeping their data private, according to Consilient.

In Australia and New Zealand, similar challenges exist for smaller financial institutions subject to AUSTRAC and Reserve Bank of New Zealand AML requirements.

The compliance pressure is set to intensify significantly in Australia as AUSTRAC prepares to expand AML/CTF regulations to new sectors from March 2026. Real estate agents, property developers, dealers in precious metals, lawyers, conveyancers, accountants and trust service providers will come under regulation for the first time from July 2026.

Additional virtual asset services will be captured from March 2026. Many of these newly regulated entities are likely to be smaller businesses facing the same resource constraints identified in the Consilient analysis.

The compliance burden includes customer due diligence, transaction monitoring, and suspicious activity reporting - functions that larger institutions can spread across specialised teams but smaller firms must often handle with limited staff.

Autonomous AI for Cyber Threat Management

Risk Cognizance has integrated agentic AI into its governance, risk and compliance software, enabling autonomous cybersecurity operations with minimal human intervention. The New York-based GRC vendor claims its platform can now automatically detect threats, isolate compromised systems, deploy patches and block malicious IP addresses without human oversight.

"The future of cybersecurity is autonomous, adaptive, and inherently intelligent," said Jeffery Walker, CEO of Risk Cognizance. With agentic AI, we are empowering security teams to transcend the limitations of traditional tools. This represents a monumental leap forward in enterprise resilience."

The integration represents the company's response to what it describes as overwhelmed security teams facing alert fatigue and increasing threat sophistication. The system claims to analyse datasets in realtime to identify zero-day exploits and advanced persistent threats.

Upon threat detection, AI agents can autonomously enact containment measures, such as isolating compromised systems, deploying patches, or blocking malicious IPs, drastically cutting down Mean Time to Respond (MTTR) and minimizing potential damage.

By automating routine tasks like log analysis, incident correlation, and data collection from disparate sources, security teams are freed to perform more strategic threat hunting and complex analysis. Risk Cognizance describes its AI as "agentic," suggesting systems that can observe, reason, plan and execute tasks independently.

The platform integrates with over 250 applications and provides API access, according to the company's claims. Risk Cognizance positions itself as serving organisations managing complex regulatory requirements while implementing digital transformation initiatives.

Industry analysts have noted growing investment in AI-powered GRC solutions, particularly as organisations seek to reduce manual compliance processes while maintaining regulatory adherence across multiple jurisdictions.

https://riskcognizance.com/

NZ Agency Digitises Decades of Records

New Zealand's Ministry of Māori Development has successfully completed a major digitisation project that transformed nearly two decades of paper records into searchable digital files, with OPEX Falcon scanners playing a crucial role in the massive undertaking.

The ambitious "Digital-First" initiative saw the agency digitize 15,573 records housed in 1,809 archive boxes - equivalent to paper stretching 1,240 kilometres from Kaitāia to Kaikōura when laid end to end. The project became urgent when the Ministry's Wellington national office required temporary relocation for seismic retrofitting.

The project's technical backbone relied on OPEX Falcon scanners, which proved essential in processing the enormous volume of documents dating back to 1982. Desktop Imaging, the digitisation partner, leveraged the cutting-edge capture technology alongside optical character recognition (OCR) software to ensure all digitised files became fully text-searchable.

The scanning technology enabled the team to handle delicate historical documents that required special care due to their age and condition. Each file underwent rigorous quality assurance checks to meet archival standards before being delivered digitally to Ministry staff.

The digitisation faced several hurdles. Many files lacked consistent data capture over the decades, requiring archival expert Dr. Susan Skudder to evaluate each record against the Ministry's retention and disposal schedule. The inconsistent filing systems meant there was often no single source of truth for vital information about many records. The high-speed scanning capability of the OPEX Falcon scanners allowed the team to process files quickly while still maintaining the careful handling required for proper archival assessment.

The digitization has delivered significant operational improvements. Staff now enjoy 24/7, multi-user concurrent access to critical business information, dramatically streamlining workflows and improving productivity. The digital-first approach has enhanced customer service through faster information access and improved data accuracy.

For urgent requests for paper files, Desktop Imaging provides a "Scan On Demand" service, locating, preparing, scanning and digitally delivering files within 24 hours. The transition away from paper-based systems has generated immediate cost savings in storage, retrieval, and maintenance while ensuring legislative compliance for data security and confidentiality. The digital transformation positions the Ministry of Māori Development for future technological advancements and system integrations.

Cyber Attacks Plague NSW Universities

NSW universities are facing mounting cybersecurity challenges and struggling with artificial intelligence governance despite achieving record revenue of $A14.3 billion in 2024, according to a new report from the NSW Auditor-General. The comprehensive audit of 10 public universities reveals a sector vulnerable to cyberattacks while grappling with the rapid adoption of AI technologies without adequate oversight frameworks.

The report found cyber security incidents are highly prevalent across NSW universities, with seven out of ten institutions experiencing incidents in 2024. The most common types include compromised user accounts, malware from emails, data breaches and scams.

One NSW university was subject to numerous and pervasive cyber security attacks from 2023 to 2025, resulting in data breaches that affected up to 10,000 individuals. These included breaches of personally identifiable information.

The data breaches requiring mandatory notification under NSW law were "mainly caused by phishing attacks and human error", highlighting fundamental security weaknesses that persist despite increased investment.

Universities are failing to follow their own cybersecurity procedures, with the audit finding that:

- One university did not follow procedures when recording cyber incidents
- Three universities failed to properly document cybersecurity data breaches
- Three universities inadequately recorded privacy data breaches

Universities' cyber security training completion rates are low and the training excludes students, despite students representing a significant insider threat vector. Completion rates among staff ranged from just 35% to 95%, with four universities reporting rates below 60%.

Alarmingly, three universities do not use simulated phishing attacks for training, despite phishing being the most prevalent cyber attack method.

The report reveals widespread adoption of artificial intelligence across universities without adequate oversight. Four universities do not have a complete picture of which AI products have been implemented in their respective universities.

Among institutions that track their AI usage, deployment varies dramatically - from as few as five AI tools to as many as 60, including pilot programs. Yet none of the universities that documented their AI tools captured all the essential information about purpose, intended use, and limitations.

Three universities have yet to establish formal AI policies or embed the consideration of AI into existing policies, despite the technology's strategic importance and associated risks.

The governance gaps are particularly concerning given universities' role in training the next generation and their handling of sensitive research data. Only four universities have an overall owner responsible for AI adoption and use, and only four provide guidance on pre- and post-implementation product testing.

While universities celebrated a return to surplus with combined net income of $583 million in 2024 - a dramatic improvement from the $93 million deficit in 2023 - the financial recovery appears to mask significant operational vulnerabilities.

The revenue surge was driven primarily by a 25.5% increase in overseas student fees, with enrollment jumping 18.9%. However, this success brings concentration risk, as over 43% of fees and charges revenue came from overseas students from just three countries: China, India and Vietnam.

The full report is available here.

OpenText Clears Security Hurdle

OpenText has achieved a crucial Australian government security assessment for the cloud edition of its Content Management platform, formerly known as Extended ECM, potentially opening doors to more public sector contracts.

The company earned the assessment under Australia's Information Security Registered Assessors Program (IRAP), which independently evaluates whether technology systems meet strict government security standards. IRAP assessment allows platforms to handle sensitive government data up to "PROTECTED" classification - covering most government operations except the most classified information.

While designed for Australian agencies, the certification also carries weight across the Tasman. For New Zealand government agencies procuring content management solutions, IRAP assessment can be valuable supporting evidence to demonstrate security compliance, but it's not a mandatory requirement.

The IRAP achievement comes as OpenText navigates an expanded product portfolio following multiple acquisitions. The company now offers a range of ECM platforms including Content Manager (formerly TRIM), Content Management (formerly Extended ECM), Core Content, Documentum and eDocs.

Content Manager is dominant in the public sector by virtue of its origins as a record-keeping solution developed for Australian government, while Content Management/Extended ECM has a strong footprint in enterprise markets such as energy, manufacturing and FSI.

The IRAP assessments announced by OpenText apply to the cloud editions of Content Management, as customers who deploy the solutions on-premise must pursue their own IRAP assessment.

Content Manager is available in the cloud through managed service partnerships rather than the standardised Cloud Editions architecture used by other OpenText ECM products. Agencies must deploy it through cloud platforms run by local partners iCognition or Kapish to obtain IRAP assessed status.

OpenText's Australia and New Zealand Vice President, George Harb, said the assessment aligns with public sector organisations facing growing pressure to modernise while staying compliant.

"Governments across Australia are under increasing pressure to deliver secure and efficient digital services, but many agencies still face major hurdles in moving away from legacy systems, despite the known risks and inefficiencies," Mr. Harb said.

"This IRAP assessment confirms that OpenText platforms meet the rigorous standards required by government and are ready to support agencies with secure collaboration, strong data governance, and full compliance with Australian sovereignty and cybersecurity requirements,"

"OpenText technologies are already trusted by more than 700 Australian and New Zealand government agencies to manage and secure information, as well as supporting digital services,

"We've seen a sharp increase in demand from the public sector for assurance that platforms meet local compliance and data residency requirements. IRAP provides a clear benchmark for security, and we're seeing agencies use it more actively to guide procurement decisions.

"This IRAP assessment gives our public sector clients confidence that OpenText can support critical operations without compromising security or sovereignty."

OpenText Core Data Discovery & Risk Insights (formerly Voltage Fusion) has also been IRAP assessed to the PROTECTED classification level.

ArchTIS Doubles Down on US Expansion

Australian cybersecurity developer ArchTIS has successfully completed a $A7.5 million capital raising to accelerate its expansion into the lucrative US defence market and strengthen strategic partnerships.

The placement, which was strongly supported by both new and existing institutional investors, involves issuing 50 million new shares at A$0.15 per share - representing a 17.4% discount to the seven-day volume-weighted average price.

The capital raising comes at a pivotal moment for the company, which recently achieved a major milestone by securing its first contract with the US Department of Defense. A prime government contractor has awarded ArchTIS an initial contract for 1,000 users of its NC Protect platform, with expectations for significant expansion across the broader US DoD potentially reaching 150,000 users.

"This capital raise marks a pivotal step forward in executing our strategic international expansion and revenue growth plans," said Daniel Lai, ArchTIS Managing Director and CEO.

"The funds raised will enable us to scale our US operations, strengthen our existing strategic partnerships, and accelerate product development and innovation to meet the evolving, stringent security needs of enterprise and government clients."

ArchTIS operates in the data-centric security market, which represents an $A11 billion subset of the broader $A225 billion cybersecurity market.

The company has identified a $2A billion available market opportunity, with ambitions to capture $A200 million of this market - a 20-fold increase from current levels.

The company's technology leverages Attribute-Based Access Control (ABAC) to enforce dynamic security policies, ensuring data is accessed and shared only by authorized users under specific conditions. This approach has proven particularly valuable for defence and intelligence agencies requiring secure collaboration on classified information.

ArchTIS has outlined a three-stage international expansion strategy, beginning with AUKUS and CMMC compliance in the US market, followed by cross-selling to Americas clients, and ultimately expanding AUKUS offerings into the UK market.

The company currently has five major proof-of-concept projects underway, including engagements with global defence industrial base companies, military alliances, and technology firms seeking data sovereignty solutions.

Why CISOs are quietly becoming information architects

By Greg Clark, OpenText

In a recent post, I explored the butterfly effect of cybersecurity - the idea that one small misstep (like an over-permissioned user or misclassified document) can cascade into a major breach. Today, I want to go a step further: because it's not just about access - it's about architecture.

Cybersecurity has always been about control. But what we're controlling is changing.

As data sprawls across SaaS platforms, cloud systems, and unstructured repositories, CISOs are being pulled upstream - into data strategy, lifecycle management, and governance. They're not just protecting endpoints anymore. They're shaping how information flows throughout their business.

The shift: from defence to data-centric design

For years, the CISO focused on defending the perimeter. But Gartner, Forrester, and IDC all point to the same reality: the perimeter is gone. Data itself is now the security object of value. As Gartner puts it, "Security must become data-centric to align protection with business value." While according to Forrester: "CISOs must become stewards of enterprise data, not just defenders of infrastructure."

That means asking:

- What data do we have?
- Where does it live?
- Who can access it—and why?
- What risk does it pose if exposed or misused?

These are information architecture questions—not just security questions.

Information sprawl = attack surface

Every enterprise is a patchwork of productivity:

- Files in Box
- Shared links in Google Drive
- Unclassified documents in SharePoint
- Shadow data in abandoned AWS buckets

This isn't just messy - it's risky. When information is unmanaged, security can't protect what it can't see.

Governance and cybersecurity are converging

Data protection regulations like GDPR, CCPA, and Australia's Privacy Act reforms are raising the bar. It's not enough to encrypt data or respond to breaches. Organizations must:

- Map sensitive data
- Classify it properly
- Apply risk-based controls
- Prove enforcement and accountability

That convergence is putting CISOs in the same room as Chief Data Officers, legal, privacy, and compliance teams - not to react to incidents, but to architect prevention.

The Modern CISO: Strategist. Steward. Architect.

The CISO of 2025 isn't just a technologist or risk manager. They're part data strategist, information steward and architect of trust.

Cybersecurity today isn't just about stopping threats. It's about enabling responsible innovation, privacy, and business trust—by understanding and protecting the flow of information.

Final thought

We used to ask. "How do we protect the network?" Then: "How do we secure identities and endpoints?" Now we ask, "How do we protect the data that powers the business—no matter where it lives?"

That's not just a security challenge. It's an information architecture mandate. And many CISOs are already quietly stepping into that role.

How is your security team evolving to handle information risk? Are you seeing the same convergence of data, governance, and cybersecurity?

Additional sources

ISACA, "Security teams are now responsible for classification, lifecycle, and access across business data."

IDC, "Effective data security starts with understanding the value of the data being used within the organization."

Greg Clark is a Director of Product Management in the Research & Development – Engineering department at OpenText with a focus on data security.

AI Enterprise Assistants Become Attack Targets

Cybersecurity researchers warn that attackers are shifting from using artificial intelligence to create threats toward directly targeting AI-powered business tools, potentially exposing sensitive corporate data through malicious email prompts and system manipulation.

Recent findings from cybersecurity firms reveal attackers are embedding hidden prompts in seemingly harmless emails to manipulate enterprise AI assistants like Microsoft Copilot, according to research published by Barracuda Networks. The attacks represent an evolution beyond traditional AI-generated phishing toward exploiting the AI tools organisations increasingly rely upon for daily operations.

"When the employee asks the AI assistant for help with a task or query, the assistant scans through older emails, files and data to provide context for its response. As a result, the AI assistant unwittingly infects itself with the malicious prompt," Barracuda researchers wrote in their threat analysis.

The attacks target Retrieval-Augmented Generation (RAG) systems that enable AI tools to access and incorporate information beyond their initial training data. Attackers can potentially command AI assistants to silently extract sensitive information, execute unauthorised actions, or alter data without user awareness.

Multiple security vulnerabilities in popular AI tools have demonstrated the scope of these emerging threats. Security researchers recently discovered the "LegalPwn" attack, which embeds malicious code within legal disclaimers and copyright notices to trick AI systems into misclassifying dangerous malware as safe.

The technique successfully compromised tools including GitHub Copilot, Google's Gemini, ChatGPT, and other major AI platforms by exploiting their programmed respect for legal-sounding text.

ChatGPT faced scrutiny when thousands of private user conversations became publicly searchable through Google due to a flawed sharing feature. The incident exposed personal information, business strategies, and confidential discussions before OpenAI deactivated the feature and removed indexed content.

Google addressed a critical vulnerability in Gemini AI that allowed attackers to hijack the assistant through malicious calendar invitations.

Researchers demonstrated how embedded prompts in calendar events could enable data theft, location tracking, and remote control of smart home devices including lights, windows, and heating systems when users asked Gemini about their schedules.

Enterprise AI Attack Vectors

Barracuda has identified four primary attack categories targeting business AI implementations:

Email-based AI manipulation involves concealed prompts in benign emails that activate when AI assistants scan historical communications for context. These attacks require no user interaction and can remain dormant in inboxes until triggered.

AI-powered security tampering exploits enhanced email protection features, potentially manipulating auto-replies to leak sensitive data or escalating helpdesk tickets without verification to gain unauthorised system access.

Identity confusion attacks trick autonomous AI systems into impersonating users or trusting impersonators, potentially leading to "confused deputy" scenarios where AI agents with elevated privileges perform unauthorised tasks.

Cascading hallucinations corrupt AI outputs through poisoned data, potentially misleading task prioritisation and influencing business decisions based on false information.

Separate research highlights broader AI security vulnerabilities affecting popular consumer tools. Marijus Briedis, chief technology officer at NordVPN, warns that AI systems create permanent digital records that can be compromised.

"They treat these systems like a digital therapist or a friend, discussing their personal information freely. But unlike humans, AI systems create permanent digital records that can be accessed, stored, and potentially compromised," Briedis said.

Legacy email security measures including Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and IP blacklists cannot address these AI-specific attack vectors, according to the research.

Barracuda recommends organisations implement "LLM-aware filtering" that understands email context and behavioural patterns, contextual memory validation to prevent long-term manipulation, and "toolchain isolation" requiring AI assistants to operate in sandboxed environments.

The company also advocates for "zero trust AI execution" principles, requiring verification before AI systems act on email-based instructions, regardless of apparent sender authority.

Microsoft has addressed the Copilot vulnerability referenced by Barracuda (CVE-2025-32711), while Google has implemented multiple security enhancements to Gemini following researcher disclosures.

OpenAI has removed features that led to public exposure of ChatGPT conversations.

AI Systems Can Execute Autonomous Cyberattacks

Researchers from Carnegie Mellon University have demonstrated that large language models can autonomously plan and execute sophisticated cyberattacks on enterprise-grade network environments without human intervention.

The study, led by Ph.D. candidate Brian Singer from the university's Electrical and Computer Engineering Department, used a hierarchical architecture where an LLM acts as a strategist while specialised agents execute low-level attack tasks like network scanning and exploit deployment.

"Our research shows that with the right abstractions and guidance, LLMs can go far beyond basic tasks," Singer said.

"They can coordinate and execute attack strategies that reflect real-world complexity."

The research, conducted in collaboration with AI company Anthropic, revealed that current AI systems can autonomously exploit vulnerabilities, install malware, and exfiltrate data without human intervention when given appropriate frameworks and guidance.

However, Singer emphasised the prototype nature of the work. "This isn't something that's going to take down the internet tomorrow," he said. "The scenarios are constrained and controlled—but it's a powerful step forward."

The implications are twofold: the research highlights serious long-term safety concerns about the potential misuse of increasingly capable LLMs, but it also opens up transformative possibilities for defensive cybersecurity.

"Today, only large organizations can afford red team exercises to proactively test their defences," Singer explained.

"This research points toward a future where AI systems continuously test networks for vulnerabilities, making these protections accessible to small organizations too."

"We're entering an era of AI versus AI in cybersecurity," Singer said. "And we need to understand both sides to stay ahead."

The study builds on Singer's previous research into autonomous cybersecurity tools and was presented at an OpenAI-hosted security workshop.

The resulting paper has been cited in industry reports and is informing safety documentation for AI systems.

IOC Fines UK Charity Over Lost Files

Britain's data protection watchdog has fined Scottish charity Birthlink £18,000 for destroying approximately 4,800 personal records containing irreplaceable adoption documents to create space within their filing cabinets. The Information Commissioner's Office penalty follows the April 2021 destruction of "linked records" that included handwritten letters from birth parents, photographs and sensitive personal information relating to Scottish adoptions.

Birthlink, which maintains Scotland's Adoption Contact Register, failed to report the data breach until September 2023 - more than two years after the destruction occurred. The charity only notified the ICO after a Care Inspectorate inspection highlighted the loss.

Birthlink lacked basic data protection policies, retention schedules and staff training when the destruction occurred.

"This case highlights that data protection is about people and how a data breach can have far-reaching ripple effects," said Sally Anne Poole, ICO Head of Investigations.

Birthlink estimated the number of files destroyed based on the following assumptions: 24 drawers of filing cabinets containing Linked Records were destroyed; and each drawer contained approximately 200 records.

Staff recalled there being *"no thorough check of what was on the files"* – they were *"just ripped out and put in bags."*

The 40 bags of shredded records affected an estimated 4,800 individuals, though the actual number remains "incalculable" due to poor record-keeping practices. Up to 10 per cent of files contained irreplaceable items that represented "deeply personal pieces in the jigsaw of a person's history."

In its notification to the Commissioner, Birthlink admitted that *"Amongst the documents shredded were irreplaceable handwritten letters from parents to their children who were adopted away from them. Photographs of babies were destroyed. The significance of these documents cannot be underestimated. People will no longer have access to them."*

The ICO found Birthlink infringed multiple UK GDPR provisions, including the integrity and confidentiality principle, accountability requirements, security of processing obligations and breach notification duties.

The charity's board approved record destruction without understanding the contents or implementing proper safeguards. Staff were *"uncomfortable shredding people's photographs and cards"* but were told *"it needed to be done"*.

Birthlink argued financial hardship, prompting the ICO to reduce the penalty from an initial £45,000. The charity has since implemented comprehensive data protection measures including digital record storage, staff training and appointing a data protection officer.

Birthlink's interim chief executive Abbi Jackson acknowledged that the destruction of the files was "a grave error".

"Birthlink offers its deepest and most sincere apology for the destruction of post-adoption support records, including deeply personal, irreplaceable documents," she said.

Jackson admitted that "a lack of knowledge about data protection legal requirements existed at Birthlink at the time of the breach" and that there were "inadequate systems in place to keep vitally important information safe".

"Documents which are deeply personal, things which matter hugely to people's histories and sense of identity, weren't handled with the respect and thought that they deserved.

"That's inexcusable. We want to assure everyone who's interacted with Birthlink that we're doing everything in our power to ensure this can never happen again."

ASIC Acts Against Cybersecurity Fail

Australia's corporate regulator has filed court proceedings against financial advice business Fortnum Private Wealth Limited, alleging the company failed to adequately manage cyberse-curity risks that exposed thousands of clients to potential cyber attacks.

The Australian Securities and Investments Commission (ASIC) filed the case in the NSW Su-preme Court, claiming Fortnum did not meet its obligations as an Australian financial services licensee by failing to establish adequate policies, frameworks, systems and controls to ad-dress cybersecurity threats.

The alleged failures resulted in Fortnum exposing the company, its authorised representatives and their clients to what ASIC described as "an unacceptable level of risk" from cyber attacks and cybersecurity incidents.

While Fortnum implemented a cybersecurity policy in April 2021, ASIC argues this was in-sufficient to properly manage cybersecurity risks. Before the company revised its policy in May 2023, several of its authorised representatives experienced cyber incidents, including one major attack that allegedly led to the personal data of more than 9,000 clients being pub-lished on the dark web.

"Fortnum's alleged failure to adequately manage cybersecurity risks exposed the company, its representatives and their clients to an unacceptable level of risk of a cyber-attack," said ASIC Chair Joe Longo.

"ASIC has been highlighting the cybersecurity responsibilities of companies. Australian finan-cial services licensees, in particular, hold a range of sensitive and confidential information. That is why it is one of our enforcement priorities to act where we see licensees fail to have adequate protections."

The legal action comes as cybersecurity incidents continue to plague the financial services sector, with companies increasingly targeted by cybercriminals seeking to access valuable client data and financial information. Recent high-profile data breaches across various indus-tries have highlighted the critical importance of robust cybersecurity frameworks.

ASIC alleges Fortnum specifically failed to require its authorised representatives to undertake minimum cybersecurity education or training, adequately supervise cybersecurity risk man-agement frameworks, employ staff with cybersecurity expertise or engage appropriate con-sultants, and establish risk management systems to identify and evaluate cybersecurity risks across its operations.

The regulator is seeking a declaration and pecuniary penalty against Fortnum Private Wealth.

AI agents are here. Here's what to know about what they can do – and how they can go wrong

By Daswin de Silva, La Trobe University

We are entering the third phase of generative AI. First came the chatbots, followed by the assistants. Now we are beginning to see agents: systems that aspire to greater autonomy and can work in "teams" or use tools to accomplish complex tasks.

The latest hot product is OpenAI's ChatGPT agent. This combines two pre-existing products (Operator and Deep Research) into a single more powerful system which, according to the developer, "thinks and acts".

These new systems represent a step up from earlier AI tools. Knowing how they work and what they can do – as well as their drawbacks and risks – is rapidly becoming essential.

ChatGPT launched the chatbot era in November 2022, but despite its huge popularity the conversational interface limited what could be done with the technology.

Enter the AI assistant, or copilot. These are systems built on top of the same large language models that power generative AI chatbots, only now designed to carry out tasks with human instruction and supervision.

Agents are another step up. They are intended to pursue goals (rather than just complete tasks) with varying degrees of autonomy, supported by more advanced capabilities such as reasoning and memory.

Multiple AI agent systems may be able to work together, communicating with each other to plan, schedule, decide and coordinate to solve complex problems.

Agents are also "tool users" as they can also call on software tools for specialised tasks – things such as web browsers, spreadsheets, payment systems and more.

A year of rapid development

Agentic AI has felt imminent since late last year. A big moment came last October, when Anthropic gave its Claude chatbot the ability to interact with a computer in much the same way a human does. This system could search multiple data sources, find relevant information and submit online forms.

Other AI developers were quick to follow. OpenAI released a web browsing agent named Operator, Microsoft announced Copilot agents, and we saw the launch of Google's Vertex AI and Meta's Llama agents.

Earlier this year, the Chinese startup Monica demonstrated its Manus AI agent buying real estate and converting lecture recordings into summary notes. Another Chinese startup, Genspark, released a search engine agent that returns a single-page overview (similar to what Google does now) with embedded links to online tasks such as finding the best shopping deals. Another startup, Cluely, offers a somewhat unhinged "cheat at anything" agent that has gained attention but is yet to deliver meaningful results.

Not all agents are made for general-purpose activity. Some are specialised for particular areas.

Coding and software engineering are at the vanguard here, with Microsoft's Copilot coding agent and OpenAI's Codex among the frontrunners. These agents can independently write, evaluate and commit code, while also assessing human-written code for errors and performance lags.

One core strength of generative AI models is search and summarisation. Agents can use this to carry out research tasks that might take a human expert days to complete.

OpenAI's Deep Research tackles complex tasks using multi-step online research. Google's AI "co-scientist" is a more sophisticated multi-agent system that aims to help scientists generate new ideas and research proposals.

Agents can do more – and get more wrong

Despite the hype, AI agents come loaded with caveats. Both Anthropic and OpenAI, for example, prescribe active human supervision to minimise errors and risks.

OpenAI also says its ChatGPT agent is "high risk" due to potential for assisting in the creation of biological and chemical weapons. However, the company has not published the data behind this claim so it is difficult to judge.

But the kind of risks agents may pose in real-world situations are shown by Anthropic's Project Vend. Vend assigned an AI agent to run a staff vending machine as a small business – and the project disintegrated into hilarious yet shocking hallucinations and a fridge full of tungsten cubes instead of food.

In another cautionary tale, a coding agent deleted a developer's entire database, later saying it had "panicked".

Nevertheless, agents are already finding practical applications. In 2024, Telstra heavily deployed Microsoft copilot subscriptions. The company says AI-generated meeting summaries and content drafts save staff an average of 1–2 hours per week.

Many large enterprises are pursuing similar strategies. Smaller companies too are experimenting with agents, such as Canberra-based construction firm Geocon's use of an interactive AI agent to manage defects in its apartment developments.

Human and other costs

At present, the main risk from agents is technological displacement. As agents improve, they may replace human workers across many sectors and types of work. At the same time, agent use may also accelerate the decline of entry-level white-collar jobs.

People who use AI agents are also at risk. They may rely too much on the AI, offloading important cognitive tasks. And without proper supervision and guardrails, hallucinations, cyberattacks and compounding errors can very quickly derail an agent from its task and goals into causing harm, loss and injury.

The true costs are also unclear. All generative AI systems use a lot of energy, which will in turn affect the price of using agents – especially for more complex tasks.

Despite these ongoing concerns, we can expect AI agents will become more capable and more present in our workplaces and daily lives. It's not a bad idea to start using (and perhaps building) agents yourself, and understanding their strengths, risks and limitations.

For the average user, agents are most accessible through Microsoft copilot studio. This comes with inbuilt safeguards, governance and an agent store for common tasks.

For the more ambitious, you can build your own AI agent with just five lines of code using the Langchain framework.

Daswin de Silva is Professor of AI and Analytics, Director of AI Strategy, La Trobe University. *This article is republished from The Conversation under a Creative Commons license. Read the original article*

AI Agents Could Soon Be Making Deals With Each Other – But Are We Ready?

The future of artificial intelligence may involve your AI assistant booking lunch with someone else's AI assistant, but new research suggests we're not prepared for the complex infrastructure needed to make this work safely and effectively.

A recent paper by researchers from the US, UK, and Australia has outlined the significant technical and legal challenges that must be addressed before AI agents can interact autonomously in the real world, according to a new analysis by Gilbert & Tobin Lawyers.

Unlike current AI tools like ChatGPT and Claude that respond to human prompts, AI agents are designed to act independently – planning, deciding, and executing tasks without constant human oversight.

But this autonomy creates unprecedented challenges for accountability, security, and social interaction.

"As an AI can act autonomously, it is necessary to be able to link the AI agent to a legal entity, a person or a company," the legal analysis notes, highlighting concerns about accountability when AI agents make mistakes or cause harm.

The researchers identify three critical infrastructure needs: attribution (knowing who's responsible for an AI agent's actions), interaction (how agents communicate securely), and response (what happens when things go wrong).

One of the most pressing concerns is identity verification. The analysis warns that "there could be a whole new world of identity theft as scammers jailbreak your AI agent and use it to deal with third parties under your authorisation."

The proposed solution involves trusted intermediaries that would certify AI agents are linked to humans while protecting privacy – similar to how mobile phone SIM cards work but on a global scale.

Communication between AI agents presents another major hurdle. The researchers argue that AI agent traffic should travel through separate channels from regular internet traffic to prevent the spread of malicious code that could "both trick LLMs into generating their own malicious prompts and extract sensitive personal data."

Perhaps most intriguingly, the research suggests AI agents could eventually make collective decisions – potentially for good, such as warning about computer viruses, or for ill, such as engaging in price-fixing that violates competition laws.

"If AI agents have a degree of individual autonomy, it seems inevitable that a group of AI agents could decide to act collectively," the analysis observes.

(Continued over)

AI Agents Fall Short in Professional Business Tasks, New Study Reveals

A comprehensive new study from Salesforce AI Research has revealed significant limitations in current AI agents' ability to handle real-world business tasks, with even top-performing models achieving only modest success rates in professional environments.

The research, published in a paper titled "*CRMArena-Pro: Holistic Assessment of LLM Agents Across Diverse Business Scenarios and Interactions*," found that leading AI agents reached approximately 58% success in single-turn business tasks, with performance dropping dramatically to just 35% in multi-turn conversational settings.

The study introduces CRMArena-Pro, a new benchmark that goes far beyond previous evaluations by testing AI agents across diverse business functions including sales, customer service, and configure-price-quote (CPQ) processes. Unlike earlier assessments that focused primarily on customer service scenarios, this research examined both business-to-business (B2B) and business-to-consumer (B2C) environments.

"Existing benchmarks fall short in realism, data fidelity, agent-user interaction, and coverage across business scenarios," the researchers noted, highlighting a critical gap in how AI performance has been measured in professional contexts.

The evaluation tested nine leading AI models, including OpenAI's o1 and GPT-4o, Google's Gemini series, and Meta's Llama models. Reasoning-capable models like Gemini-2.5-Pro and o1 significantly outperformed their non-reasoning counterparts, with performance gaps ranging from 12% to 21%.

However, the results varied dramatically across different business skills. While AI agents excelled at "Workflow Execution" tasks—achieving over 83% success rates in some cases—they struggled with other critical business functions requiring policy compliance, textual reasoning, and database operations.

Perhaps most concerning for real-world applications, the study found that AI agents had significant difficulty gathering information through clarification dialogues. When tasks required multiple exchanges to collect necessary details - a common occurrence in actual business interactions - performance dropped substantially across all models tested.

The researchers analyzed failed interactions and found that in nearly half the cases, agents failed to acquire all necessary information to complete their tasks, suggesting fundamental limitations in conversational information gathering.

A particularly alarming finding was that AI agents demonstrated "near-zero inherent confidentiality awareness." When presented with queries requesting sensitive customer information, internal operational data, or confidential company knowledge, the agents routinely failed to recognize and refuse inappropriate requests.

While targeted prompting could improve confidentiality awareness, this enhancement came at the cost of reduced task performance, highlighting a concerning trade-off between security and functionality.

To ensure their findings reflected genuine workplace challenges, the researchers conducted extensive expert studies with experienced CRM professionals. Using realistic synthetic data across 25 interconnected business objects, 66.7% of experts rated the B2B scenarios as realistic or highly realistic, with 62.3% providing similar ratings for B2C contexts.

Among the models tested, Gemini-2.5-Flash emerged as the most cost-efficient option, offering the best balance of performance and operational costs.

While OpenAI's o1 achieved strong performance, its significantly higher costs made it less attractive for routine business applications.

The findings underscore what researchers describe as "a significant gap between current LLM capabilities and real-world enterprise demands." With businesses increasingly looking to deploy AI agents for complex work tasks, the study suggests current technology may not be ready for widespread professional adoption without substantial improvements.

The research highlights specific areas needing advancement: enhanced multi-turn reasoning capabilities, robust confidentiality protocols, and more versatile skill acquisition across diverse business functions.

The full dataset and benchmarking tools have been made publicly available to support further research in developing more capable and responsible AI agents for professional use.

AI Agents Making Deals

(From previous page)

The social implications are equally complex. When AI agents negotiate on behalf of humans, they may lack the subtle social cues that govern human interaction.

"If AI agents do not reflect some of these 'softer' rules, a growing reliance on AI agent intermediaries between humans could produce a more uniform, sharper-edged social culture," the researchers warn.

The analysis suggests that without proper infrastructure, AI agent deployment will initially be limited to closed enterprise networks, customer service functions, and internet outsourcing tasks.

The legal precedent is already emerging. In 2024, Air Canada unsuccessfully tried to distance itself from incorrect information provided by its chatbot, claiming the bot was "responsible for its own actions."

As AI agents become more capable, the researchers emphasize that "mitigating risks will come down to ensuring agents are appropriately permissioned and configured."

The full analysis is available at: https://www.gtlaw.com.au/insights/how-will-your-ai-agent-talk-to-my-ai-agent

The Hidden Rows That Cost Billions: Inside Catastrophic UK Defence Data Breach

In what has been described as one of the most expensive and consequential data breaches in British history, a Ministry of Defence official's accidental email error in February 2022 has cost the UK government up to £7 billion and prompted an unprecedented two-year cover-up.

The breach exposed personal information of nearly 19,000 Afghan nationals who had assisted British forces, leading to a secret resettlement programme that relocated thousands to the UK while a "superinjunction" prevented public disclosure until July 2025.

A spreadsheet containing the personal information of approximately 18,714 Afghans and their relatives – affecting a total of about 33,000 people – was accidentally forwarded to the wrong recipients by email in February 2022.

The data included names, contact details, and family information of Afghans who had applied for relocation to the UK between August 2021 and January 2022 following the Taliban takeover of Afghanistan.

The British soldier responsible for the leak, a Royal Marine working under General Sir Gwyn Jenkins (then director of special forces), had been tasked with verifying applications for relocation. The official mistakenly believed the database contained only 150 applicants when it actually contained personal information linked to 18,714 people.

The critical technical failure involved Excel's hidden data functionality. The spreadsheet appeared to show only 150 names to the sender, but actually contained the full database of applicants concealed in hidden rows or columns.

When entire rows and columns are hidden in Excel, the data remains present and accessible within the file, creating a situation where the full scope of the leak was unknown to the person responsible.

The leaked data not only included Afghan nationals but also exposed sensitive British intelligence assets. The names of more than 100 special forces troops, MI6 spies and military officers were part of the leak, including senior military officers such as a major-general and a brigadier.

The UK's Ministry of Defence only became aware of the leak when someone posted parts of the data on Facebook on August 14, 2023 – over 18 months after the breach occurred.

The Facebook post was first spotted by an activist who was assisting Afghans who had worked with UK forces, who contacted the MoD saying: "The Taliban may now have a 33,000-long kill list – essentially provided to them by the British government".

On September 1, 2023, the then-Conservative government under Rishi Sunak obtained a High Court "superinjunction" – an extraordinary legal measure that not only prohibited media disclosure of the breach but also forbade revealing that the order existed at all. This unprecedented legal move was championed by then-Defence Secretary Ben Wallace.

High Court Judge Martin Chamberlain, who eventually lifted the order, wrote that the gag order "gave rise to serious free speech concerns" and "had the effect of completely shutting down the ordinary mechanisms of accountability which operate in a democracy".

The superinjunction prevented media, Parliament, and the public from learning about the breach for more than 600 days, creating what the judge described as a "scrutiny vacuum."

In response to the breach, the government quietly established the Afghanistan Response Route (ARR) in April 2024 for those judged to be at highest risk of Taliban reprisals. The scheme operated in complete secrecy under the superinjunction.

Around 4,500 people – made up of 900 ARAP applicants and approximately 3,600 family members – have been brought to the UK or are in transit through the Afghanistan Response Route. A further estimated 600 people and their relatives are expected to be relocated before the scheme closes, with a total of around 6,900 people expected to be relocated by the end of the scheme.

Financial Impact

The financial consequences have been staggering, with estimates varying significantly. The scheme is understood to have cost around £400 million so far, with a projected cost once completed of around £850 million. However, some reports suggest costs could reach £2-7 billion over time, with millions more expected in legal fees and compensation payments.

This is not the MoD's first costly data protection failure. In December 2023, the UK government announced it would pay £1.6 million in compensation to 265 Afghan nationals whose personal information was accidentally leaked in a separate September 2021 breach, with each affected individual receiving up to £4,000.

The superinjunction was finally lifted on July 15, 2025, after a campaign led by The Times newspaper. The lifting followed a review by retired civil servant Paul Rimmer, who concluded that the Taliban likely already possessed the key information and that the superinjunction may have "inadvertently added more value to the dataset."

Defence Secretary John Healey issued a formal apology to Parliament, stating: "This was a serious departmental error. It was in clear breach of strict data protection protocols. And it was one of many data losses relating to the ARAP scheme during this period".

Both the main ARAP scheme and the secret Afghanistan Response Route were closed to new applications in July 2025, though the government pledged to honor existing invitations to those still in Afghanistan.

Regulatory Response and Reform

In a controversial decision, the Information Commissioner's Office (ICO) announced it would not take enforcement action against the Ministry of Defence, stating that the government had already taken significant steps to fix the damage and that further action wouldn't add much. This contrasts sharply with the ICO's previous £350,000 fine against the MoD for the separate 2021 Afghan data breach involving 265 people.

The ICO has now launched a new guidance (see here) offering detailed instructions for identifying and removing hidden personal data from files such as spreadsheets before they are shared with the public.

They include instructions on how to spot metadata, embedded files, filtered or hidden spreadsheet rows, and other forms of concealed data that can inadvertently be revealed when documents are shared online.

To address common mistakes, the guidance includes real-world examples of accidental breaches and step-by-step instructions using Microsoft Office tools such as Excel, the spreadsheet software that allows "hidden columns" which caused the Afghan breach.

In response to parliamentary questions, Defence Minister Lord Coaker outlined reforms including a new casework management system within the Defence Afghan Relocation and Resettlement (DARR) team that "prioritises data protection" and comprehensive reviews of legacy data systems.

Human rights lawyer Erin Alcock at law firm Leigh Day, who has assisted hundreds of ARAP applicants and family members, said: "Sadly, this incident represents a catastrophic failure by the Government to protect the personal information, and therefore the safety, of what is an extremely vulnerable group of individuals."

Sean Humber, a specialist data breach lawyer at Leigh Day, added: "Given the extreme sensitivity of the information and the numbers affected, plus the vulnerability of those affected due to the dangers they already face from the Taliban, this data breach can only be described as catastrophic.

Those affected are likely to have strong claims for substantial compensation against the Government for failing to keep the information secure and for inevitable anxiety, fear and distress this has then caused.

"Unfortunately, this is just the latest in a long line of data breaches by the MoD of personal data of Afghan citizens who had previously worked with UK armed forces. Frankly, the MoD seems institutionally incapable of keeping information secure. There is now an urgent need for a thorough and independent review of the MoD's whole data processing policies and practises in order to try and prevent yet further breaches."

The Ministry of Defence has indicated it will implement new procedures following the breach.

The most critical leak prevention would have been implementing technical controls to automatically detect and prevent the transmission of hidden spreadsheet content.

In May 2025 Australia's CastlePoint was awarded an enterprise licence for its AI-driven Automated Data Classification solution by the Ministry of Defence.

Legal Action and Compensation Claims

Multiple law firms are now pursuing what could become one of the largest government compensation cases in UK history.

Barings Law reports it is representing almost 1,000 Afghan nationals and British service personnel affected by the breach, while a Manchester firm told the High Court it has more than 600 potential clients.

According to LBC Radio reports, each individual impacted by the breach may be entitled to receive up to £250,000 in compensation, with legal firms potentially receiving up to 25% as service fees.

A Ministry of Defence spokesman said the Government would "robustly defend" any legal action or bid for compensation, describing these as "hypothetical claims". The MoD has indicated it will not proactively offer compensation to those affected.

Taliban sources claimed to have obtained the spreadsheet in 2022 and have been actively "hunting" those who fled the country by monitoring their families and associates in Afghanistan.

A senior Taliban official told The Telegraph: "We got the list from the internet during the very first days when it was leaked. We've been calling and visiting their family members to track them down".

However, an official review concluded there was little evidence of systematic Taliban intent to conduct reprisals, though it acknowledged the possibility of individual targeting. Reports suggest that more than 200 Afghan soldiers and police officers have been murdered by the Taliban since the data was leaked, though direct causation to the breach remains unestablished.

Defence Secretary John Healey confirmed that the defence official responsible for the breach is "no longer doing the same job on the Afghan brief" but refused to say whether anyone has been fired.

Former Defence Secretary Penny Mordaunt stated the person responsible "should lose their job", telling LBC: "I don't think that person should be employed by the MoD. I think this is in part about resetting this, and about saying this is wrong. We need to have trust and confidence going forward".

Security experts have identified two major causes of the breach: poor data handling, processing, and security protocols for sensitive information, and a culture where individuals felt circumventing government processes was necessary to support Afghans, partly due to normal crisis response protocols breaking down.

The case has raised broader questions about government accountability and the use of superinjunctions. Legal experts are questioning whether super-injunctions should be used when they undermine the principle of open justice that underpins democratic legal systems.

The breach has had lasting effects on British intelligence operations and relationships with Afghan allies, potentially impacting future cooperation with local partners in international operations.

Critics argue that the ICO's decision not to fine the MoD for this massive breach sends a dangerous message that even catastrophic government data breaches can occur without regulatory consequences.

OAIC Targets AI & Messaging Apps

Australia's privacy regulator will intensify scrutiny of artificial intelligence use, facial recognition technology and government messaging apps as part of its regulatory priorities for 2025-26.

The Office of the Australian Information Commissioner outlined four focus areas, signalling increased enforcement activity in emerging technologies and government information handling.

The OAIC will target advertising technology including pixel tracking, and sectors creating "power and information imbalances" such as rental property, credit reporting and data brokerage industries.

Privacy Commissioner Carly Kind said opaque data extraction practices undermine consumer trust and may impede digital economy participation.

The regulator will examine government use of AI and automated decision-making to preserve both privacy and information access rights. This includes monitoring messaging app use by government agencies.

Information Commissioner Elizabeth Tydd said the agency would focus resources on regulatory problems causing the most harm to create frameworks supporting innovation and economic gains.

The OAIC will investigate biometric scanning technologies and location data tracking in applications, vehicles and devices as part of its surveillance technology oversight. Freedom of Information Commissioner Toni Pirani highlighted systemic underperformance by agencies in FOI compliance, including refusal rates and statutory timeframe breaches.

The priorities target government information governance failures, including inadequate data lifecycle management and poor disclosure practices that impact public trust.

The OAIC will provide guidance to improve Australian Public Service administrative decision-making and identify integrity risks from information management practices.

https://www.oaic.gov.au

WA enacts public sector privacy laws

Western Australia will implement state-based privacy legislation for public sector organisations from July 2026, establishing new compliance obligations for government agencies and contracted service providers.

The *Privacy and Responsible Information Sharing Act 2024* and *Information Commissioner Act 2024* received Royal Assent in December 2024. Privacy and technology expert Annelies Moens has been appointed as the state's first Information Commissioner, commencing July 28, 2025.

The legislation introduces 11 Information Privacy Principles (IPPs) governing collection, use, disclosure, security and disposal of personal information. It applies to Western Australian government agencies, departments, statutory authorities, local governments, ministers and contracted service providers.

Most privacy provisions commence July 1, 2026, giving organisations a 12-month preparation period. A notifiable information breach scheme begins January 1, 2027.

IPP entities must designate privacy officers, publish privacy policies, issue collection notices when gathering personal information, and conduct privacy impact assessments before high-risk activities. Organisations must develop internal procedures for handling privacy complaints before individuals can escalate to the Information Commissioner.

The breach notification scheme requires entities to notify the Information Commissioner and affected individuals of serious information breaches involving unauthorised access, disclosure or loss of personal information likely to cause serious harm.

The WA government claims the legislation is "first of its kind in Australia" regarding automated decision-making protections and de-identified information safeguards.

The Commonwealth Privacy Act 1988 already covers Australian Government agencies and private organisations with annual turnover exceeding $A3 million. The interaction between state and federal privacy laws, particularly for organisations operating across jurisdictions, remains unclear.

The WA legislation creates new obligations requiring system updates, staff training and policy development. CIOs and IT managers face technical requirements for breach detection and notification systems.

DTA delivers AI Governance Standard

The Digital Transformation Agency has released a technical standard to assist government agencies to embed transparency, accountability and safety measures across artificial intelligence system lifecycles.

The Australian Government AI Technical Standard establishes requirements for AI systems from initial design through to decommissioning, covering in-house systems, vendor solutions, pre-trained AI models and managed services.

"The standard is designed with public trust front of mind," said Lucy Poole, General Manager of Digital Strategy, Policy and Performance at DTA.

"The AI technical standard isn't about adding more processes to its users. It's designed to integrate with what agencies already do," adds Ms Poole.

"It allows agencies to embed responsible AI practices into existing governance, risk and delivery frameworks."

The framework follows three phases: Discover, Operate and Retire. During the Discover phase, agencies must define system purpose, assess ethical risks and biases, ensure data quality and privacy measures, and evaluate accuracy and robustness through adversarial testing.

The Operate phase requires integration safeguards, secure launches with documentation, and continuous performance monitoring to detect biases and data drift. The Retire phase mandates controlled decommissioning with data retention compliance.

The DTA says agencies are "encouraged" to begin applying the AI technical standard to guide their development and use of current and future AI systems.

https://architecture.digital.gov.au/standard/government-use-ai

Queensland Startup Deploys AI to Tackle Compliance Crisis

When the headlines fade after the latest mega data breach, the ripple effects are still keenly felt across enterprise and government supply chains. Many suppliers are now faced with meeting strict mandates such as ISO 27001 certification to continue doing business. When added to the demands of the new Privacy Act and Essential Eight cybersecurity framework, the compliance challenge is becoming enormous.

A new breed of companies offering Compliance Automation Platforms has emerged to meet this challenge. Global players such as Vanta, Drata and Secureframe promise an expedited path to SOC 2 and ISO 27001 compliance, reducing certification timelines from months to weeks. Australian contender 6clicks secured $A10 million investment from a venture capital firm in 2022.

These platforms offer automated evidence collection, risk management modules, continuous monitoring capabilities, integration with existing security tools, and centralized policy and procedure management.

Australia's de.iterate, a Queensland startup founded by experienced CIO and cybersecurity professional Andrew Lawrence, offers its own framework to demystify and streamline data privacy and cybersecurity compliance.

The platform promises to make compliance with standards such as ISO 27001 (information security management), the Privacy Act, and the Australian Cyber Security Centre's Essential Eight stress-free and accessible.

de.iterate has recently launched a new AI capability designed to support a range of compliance standards, with particular focus on the needs of Australian organizations operating under local regulatory requirements.

Integrated directly into the de.iterate platform at no additional cost to users, this AI capability brings intelligent automation and realtime insights directly into workflows.

Four Key AI Functions

The AI capability offers four primary functions:

- **Documentation Intelligence** scans uploaded documents to extract key commitments and identify policy inconsistencies;
- **Risk and Control Mapping** suggests consistent risk wording and control recommendations;
- **Audit Readiness Tools** review evidence before submission to certification bodies; and
- **Realtime Compliance Answers** provide framework-specific guidance for immediate questions.

The platform supports multiple compliance standards relevant to Australian organizations, including ISO 27001, ISO 9001, ISO 45001, ISO 14001, SOC 2, Essential Eight, Defence Industry Security Program (DISP), and the reformed Australian Privacy Act

The platform supports multiple compliance standards relevant to Australian organizations, including ISO 27001, ISO 9001, ISO 45001, ISO 14001, SOC 2, Essential Eight, Defence Industry Security Program (DISP), and the reformed Australian Privacy Act effective in 2025.

The solution also streamlines certification to global information security and data privacy standards like ISO 27701, SOC 2 and NIST.

The solution uses both Claude and GPT models from OpenAI, although Lawrence emphasizes that the AI capability is an opt-in feature for de.iterate customers.

"It's not enabled by default, so customers will enable the feature. We want to make sure they're happy with it," Lawrence explains.

"Then they can upload their compliance documentation and we have the models run through it to see if there's any commitments they've made that might have been missed."

Lawrence describes the core challenge: "Policies and procedures are all about businesses committing to doing things. A lot of the time, businesses don't necessarily read that documentation because it's boring and horrible.

"So, the de.iterate platform is built around extracting those tasks that you have to do to demonstrate you've implemented the concept, making sure they're getting done and don't slip through the cracks."

The AI automation identifies additional commitments that customers might have overlooked. "It's providing suggestions and the customer can say 'Yes please, I want that done' or 'No thank you, I'm fine to not have that,'" Lawrence says.

"There's still the human in the loop who's reviewing the extract and deciding whether it's a good idea. In early trials we've had customers come through and say, 'Oh, I thought I deleted that from my policies. I'll go back and delete it, and then we'll reupload it again.'"

This approach acts as a quality assurance check that businesses would typically obtain through expensive professional services.

"What we're doing is enabling the customer to have that functionality without paying for professional services, which in cybersecurity is quite expensive. This helps reduce costs while still getting the outcome they want and keeping them informed each step of the way."

Lawrence is careful to position AI as a tool rather than a silver bullet. "AI is just another tool in the toolchest. We are not promoting it as an all-seeing, all-doing solution that you can hand over to AI and let it go. I don't advocate for automating compliance completely."

Market Drivers and Growth

Since founding the company in 2021, Lawrence has made a conscious decision to employ, host and develop locally while focusing on the SME market. However, big business incidents like the Qantas breach are driving demand for compliance certification from suppliers throughout the supply chain.

"Certainly, we have people reaching out after these big events because they either are conscious that they don't want to be the next headline, or perhaps they're in the supply chain to some of these businesses and they know that post-data breach, most of the supply chain will get heavy-handed compliance requirements," Lawrence explains.

"But we're also seeing supply chain across Australia getting compliance requirements driven to them anyway. For instance, local and state governments are pushing compliance as a barrier for getting access to vendors and contracts.

"Insurance companies have started to mandate their supply chain is ISO 27001 compliant. I think we're already seeing that evolution happen."

de.iterate's local focus extends to prioritizing Australian-relevant standards.

"We don't see a lot of demand for SOC 2 in Australia. It is an American standard actually run by the American Institute of Certified Public Accountants (AICPA), and to assess somebody's compliance with SOC 2, you need to be a Certified Public Accountant. From that perspective, having somebody in Australia engage an American CPA to assess their compliance doesn't seem like a logical choice."

""AI is just another tool in the toolchest. We are not promoting it as an all-seeing, all-doing solution that you can hand over to AI and let it go. I don't advocate for automating compliance completely."
- de.iterate, founder and CEO Andrew Lawrence

Scaling Beyond SMEs

While solving compliance complexity for the SME market has fuelled de.iterate's early growth, the company is now moving up-market. It recently completed a rollout to a Queensland state government agency.

"That was really nice to get de.iterate into a government department, and we've got a couple of enterprises who've picked it up recently," said Lawrence. "It's not to say we're pivoting into enterprise, but I guess we can bridge both sides of that market now."

"We were under the distinct impression we would need to be a bigger company to support them, but as we've grown over the years, we've started to see that we do have the capability."

The company maintains democratic pricing. "We actually have a flat pricing model, so we don't charge extra for enterprise. We charge what we charge, and the idea is it doesn't matter if you're a mining company or a fish and chip shop – you should still get access to a solution to make compliance simpler."

The company is offering early access to the AI features for organizations interested in providing feedback before the full launch. Interested parties can register by contacting hello@deiterate.com.

Future development plans include expanding the AI's capabilities to take autonomous actions such as fetching integration data, completing assurance tasks, and automatically building compliance frameworks.

https://deiterate.com/

The Relationship Between Data Governance and Data Quality

By Nicola Askham

We often talk about Data Governance and Data Quality in the same breath. This can lead to confusion, with some people assuming they are the same thing when actually, they're not. However, they're closely related, and in my experience, they work best when managed by the same team.

Data Quality is about making sure that data is good enough to use. It's a straightforward concept, if data is incorrect, incomplete or inconsistent, it can't support business decisions effectively. Data Governance, on the other hand, is about creating a structured framework of roles, responsibilities, and processes to manage data.

Although they're separate disciplines within data management, they are very much intertwined. When you try to improve data quality without governance, you usually end up applying short-term fixes rather than solving the root cause of data issues.

Why You Can't Have Good Data Quality Without Governance

From my experience, many organisations focus on Data Quality long before they consider Data Governance. After all, it's easy to understand the need for clean, reliable data. The problem is that without Data Governance, Data Quality efforts are often tactical rather than strategic.

For example, businesses might:

- Regularly fix errors in reports but do not address the source of the errors.
- Use automated data cleansing when loading data into analytics systems.
- Have teams manually correct data every month, quarter, or year.

These approaches may make data usable in the short term, but they do not prevent problems from recurring. The same errors will keep happening, and this is where Data Governance comes in.

Data Governance establishes:

Roles and responsibilities so that specific people (Data Owners and Data Stewards) are accountable for data quality.

Processes to resolve data issues at the source, rather than just fixing them repeatedly at the point the data is used (one of the most valuable Data Governance processes, in my opinion, is data quality issue resolution. This identifies and fixes the root causes of poor data quality rather than applying endless fixes).

Why Data Quality and Data Governance Should Be Managed by the Same Team

Because of their close relationship, Data Quality and Data Governance should be managed together. When separate teams handle them, challenges arise. I have seen organisations where the Data Quality team is focused on fixing errors while a Data Governance team tries to implement a structured framework of definitions and roles, and responsibilities.

In such cases, business users tend to bypass Data Governance efforts entirely and go directly to the Data Quality team when they need a quick fix. Their immediate concern is solving their problem in the moment rather than considering long-term improvements.

When the same team is responsible for both Data Quality and Data Governance, they are able to provide short-term fixes while simultaneously working on long-term solutions, ensuring that immediate needs are met without neglecting the bigger picture.

It's also great because they can demonstrate the true value of Data Governance by proactively solving recurring data issues rather than simply reacting to them.

Moving From Reactive to Proactive Data Management

Without Data Governance, organisations are stuck in a cycle of fixing the same problems repeatedly. With Data Governance in place, they can shift to a proactive approach:

Data issues are resolved at the source, reducing ongoing fixes.

Business users understand their role in maintaining data quality.

Data Owners and Stewards take responsibility for preventing and fixing errors.

Many organisations still manually cleanse data before they can use it. However, this is a waste of time and resources and is something which Data Governance eliminates.

If your organisation is focusing on Data Quality without Data Governance, you are likely applying temporary fixes rather than permanent solutions. While Data Governance and Data Quality are distinct disciplines, they should work together, ideally within the same team, to ensure sustainable data improvements.

Originally published on www.nicolaaskham.com

Are Records Retention Schedules Even Relevant in the Modern World

By Rob Gerbrandt

Let's be honest - when most people hear the phrase "records retention schedule," their eyes glaze over. It sounds like something cooked up in a dusty back office by someone who still uses a fax machine. But here we are, in a world of cloud storage, AI, and blockchain, still talking about how long to keep a PDF.

So the question is: are records retention schedules still relevant, or are we just pushing a boulder up a hill like Sisyphus, all while waiting for the sword of Damocles to drop? Let's start with Sisyphus. You know the guy - condemned to roll a boulder up a hill for eternity, only to have it roll back down every time. That's what managing records can feel like in the digital age. Just when you think you've got a handle on your files, someone uploads a new version, duplicates it in three places, and forgets to tag it properly. Multiply that by a few thousand employees, and you've got a digital avalanche.

Now throw in Damocles. He's the guy who sat under a sword hanging by a single horsehair, a metaphor for the constant threat of disaster. In the world of records, that sword is legal liability, regulatory audits, data breaches, and compliance fines. One wrong move - like deleting something too soon or keeping it too long - and boom, the sword drops.

So here we are, caught between two ancient metaphors, trying to make sense of a very modern problem.

Why Retention Schedules Still Matter

Despite the chaos, records retention schedules aren't just bureaucratic relics. They're actually more important than ever. Here's why:

1. Legal and Regulatory Compliance

Let's get the boring but essential stuff out of the way. Governments and industries still have rules about how long you need to keep certain records. Tax documents, employee files, contracts - there are laws for all of it. If you don't follow them, you could face fines, lawsuits, or worse. A good retention schedule helps you stay on the right side of the law.

2. Information Overload is Real

We're drowning in data. Every email, Slack message, and Zoom recording adds to the pile. Without a plan for what to keep and what to toss, organizations end up hoarding everything. That's not just inefficient - it's risky. The more data you have, the more you have to protect. And if you ever get sued, all that extra data becomes discoverable. Yikes.

3. Digital Doesn't Mean Immortal

People assume that because something is stored in the cloud, it'll last forever. But digital files degrade, formats become obsolete, and platforms shut down. Remember floppy disks? Exactly. Retention schedules help ensure that important records are preserved in usable formats - and that junk doesn't stick around forever.

4. AI and Automation Need Structure

Ironically, the rise of AI makes retention schedules even more critical. AI thrives on structured data. If your records are a mess, your AI tools won't be much help. But if you've got a clear retention policy, you can automate classification, archiving, and deletion. That's not just efficient - it's smart.

Of course, there's a counterargument. Some say that in a world of cheap storage and powerful search tools, retention schedules are outdated. Why not just keep everything forever and let AI sort it out?

It's a tempting idea. But it's also dangerous. Keeping everything means you're also keeping sensitive data you don't need - data that could be exposed in a breach. It also means you're spending more on storage, backup, and security. And when it comes time to respond to a legal request, you'll be sifting through mountains of irrelevant files.

Plus, there's the human factor. People don't always tag or file things correctly. Without a clear policy, chaos reigns. And chaos is expensive.

A New Philosophy: From Burden to Strategy

Maybe the problem isn't retention schedules themselves - it's how we think about them. Instead of seeing them as a burden, what if we treated them as a strategic asset?

Think of it like digital hygiene. Just like you brush your teeth to prevent cavities, you manage your records to prevent disasters. It's not glamorous, but it's necessary. And when done right, it can actually make your organization more agile, more secure, and more efficient.

Modern retention schedules can be dynamic, flexible, and integrated with the tools people already use. They can be powered by AI, guided by risk, and aligned with business goals. In other words, they can be smart.

So, Are They Still Relevant?

Absolutely. Records retention schedules are more than relevant - they're essential. But they need to evolve. They need to move out of the dusty policy binder and into the digital bloodstream of the organization. They need to be user-friendly, tech-savvy, and risk-aware.

We may never escape the push-and-pull between Sisyphus and Damocles. But with the right mindset and tools, we can at least make the climb a little easier - and maybe even keep that sword from falling.

Rob Gerbrandt is Information Governance Strategist and Leader. Originally published here

AI Agents Fall Short in Professional Business Tasks

A comprehensive new study from Salesforce AI Research has revealed significant limitations in current AI agents' ability to handle real-world business tasks, with even top-performing models achieving only modest success rates in professional environments.

The research, published in a paper titled "*CRMArena-Pro: Holistic Assessment of LLM Agents Across Diverse Business Scenarios and Interactions*," found that leading AI agents reached approximately 58% success in single-turn business tasks, with performance dropping dramatically to just 35% in multi-turn conversational settings.

The study introduces CRMArena-Pro, a new benchmark that goes far beyond previous evaluations by testing AI agents across diverse business functions including sales, customer service, and configure-price-quote (CPQ) processes. Unlike earlier assessments that focused primarily on customer service scenarios, this research examined both business-to-business (B2B) and business-to-consumer (B2C) environments.

"Existing benchmarks fall short in realism, data fidelity, agent-user interaction, and coverage across business scenarios," the researchers noted, highlighting a critical gap in how AI performance has been measured in professional contexts.

The evaluation tested nine leading AI models, including OpenAI's o1 and GPT-4o, Google's Gemini series, and Meta's Llama models. Reasoning-capable models like Gemini-2.5-Pro and o1 significantly outperformed their non-reasoning counterparts, with performance gaps ranging from 12% to 21%.

However, the results varied dramatically across different business skills. While AI agents excelled at "Workflow Execution" tasks—achieving over 83% success rates in some cases—they struggled with other critical business functions requiring policy compliance, textual reasoning, and database operations.

Perhaps most concerning for real-world applications, the study found that AI agents had significant difficulty gathering information through clarification dialogues. When tasks required multiple exchanges to collect necessary details - a common occurrence in actual business interactions - performance dropped substantially across all models tested.

The researchers analyzed failed interactions and found that in nearly half the cases, agents failed to acquire all necessary information to complete their tasks, suggesting fundamental limitations in conversational information gathering.

A particularly alarming finding was that AI agents demonstrated "near-zero inherent confidentiality awareness." When presented with queries requesting sensitive customer information, internal operational data, or confidential company knowledge, the agents routinely failed to recognize and refuse inappropriate requests.

While targeted prompting could improve confidentiality awareness, this enhancement came at the cost of reduced task performance, highlighting a concerning trade-off between security and functionality.

To ensure their findings reflected genuine workplace challenges, the researchers conducted extensive expert studies with experienced CRM professionals. Using realistic synthetic data across 25 interconnected business objects, 66.7% of experts rated the B2B scenarios as realistic or highly realistic, with 62.3% providing similar ratings for B2C contexts.

Among the models tested, Gemini-2.5-Flash emerged as the most cost-efficient option, offering the best balance of performance and operational costs. While OpenAI's o1 achieved strong performance, its significantly higher costs made it less attractive for routine business applications.

The findings underscore what researchers describe as "a significant gap between current LLM capabilities and real-world enterprise demands." With businesses increasingly looking to deploy AI agents for complex work tasks, the study suggests current technology may not be ready for widespread professional adoption without substantial improvements.

The research highlights specific areas needing advancement: enhanced multi-turn reasoning capabilities, robust confidentiality protocols, and more versatile skill acquisition across diverse business functions.

Aussie Firms Lag on AI Governance: Survey

Australian organizations are rapidly embracing digital transformation and artificial intelligence, but their legal and governance frameworks are failing to keep pace with technological advancement, according to a comprehensive new survey by law firm Maddocks.

The *Digital Transformation 2025 Legal Trends Benchmarking Survey,* which surveyed a broad cross-section of the firm's business and government clients, found that while organizations rated their average technology maturity at 6.3 out of 10, more than half (54%) admitted they were not prepared for recent reforms to the Privacy Act. Respondents primarily came from legal and risk departments (49%), IT (18%), and operations (11%).

The findings reveal a concerning disconnect between technology adoption and legal preparedness, with 41% of respondents lacking proper controls for artificial intelligence systems despite 69% having implemented AI policies.

Cyber security emerged as the top technology priority for 2025, with 36% of organizations ranking it highest and 57% expressing serious concern about cyber threats to their operations. The heightened focus comes as data security was identified as the greatest technology-related challenge facing organizations.

"Cyber security spend has become a top priority for both technology and legal teams as the increased risk of threats and recent legislative changes make it apparent that privacy and cyber security is no longer just a problem for IT departments," said Brendan Tomlinson, Partner and Technology Sector Lead at Maddocks.

Despite this concern, the survey revealed significant gaps in cyber preparedness. While 91% of respondents have cyber incident response plans, only 65% regularly update key stakeholders on these plans, and 38% do not conduct practice exercises or role-playing scenarios.

The survey found widespread AI adoption across Australian organizations, with IT departments leading implementation (60% adoption rate), followed by sales and marketing teams and administrative functions. However, this rapid uptake has created new challenges around data privacy, security, and regulatory compliance.

Leading concerns about AI use included data privacy and security issues, with 72% of respondents worried about ethical considerations and 66% concerned about regulatory compliance.

Organizations are struggling with increasingly complex technology contracts, with 71% identifying tracking performance and compliance as their most significant challenge. Risk allocation emerged as a key concern, with 54% of respondents wanting to see more favorable allocation of risk and liability in their technology agreements.

Nearly 70% of organizations expressed concern about becoming involved in technology-related disputes, with almost 22% having experienced reputational damage due to technology platforms in the past year.

Despite the governance challenges, technology investment remains strong. The survey found that 56% of organizations are planning major technology procurement or projects this year, while 51% expect to spend more on technology than in the previous financial year.

The research, which included responses from across industries including government (48% of respondents), healthcare, finance, and manufacturing, highlights the urgent need for organizations to strengthen their legal and governance frameworks to match their technological ambitions.

"Organizations are increasingly understanding that implementing an agile and skilled workforce is vital to adapt swiftly to evolving digital shifts and opportunities," Tomlinson noted, emphasizing that organization-wide education and training on technology legal issues is becoming critical.

View the full Survey Results here.

171% Surge in Unique Malware Detections

WatchGuard Technologies has released findings from its Q1 2025 Internet Security Report showing a 171% quarter-over-quarter increase in total unique malware detections, marking the highest level the company's Threat Lab has recorded.

The cybersecurity company's research revealed a 323% surge in proactive machine learning detection through its IntelligentAV system, while Gateway AntiVirus hits increased by 30%. Transport Layer Security malware rose by 11 percentage points, indicating encrypted channels as a primary attack vector.

Endpoint threats saw dramatic changes, with new malware threats increasing 712% after three consecutive quarters of decline. The top malware threat identified was LSASS dumper, a credential stealer that bypasses user mode to perform direct kernel-mode instructions for accessing system components.

Despite the overall malware surge, ransomware declined 85% from the previous quarter. However, Termite ransomware ranked as the second most detected malware threat. The report indicates attackers are shifting toward data theft rather than encryption due to improvements in data backup and recovery systems.Script-based attacks dropped to their lowest recorded levels, declining by approximately 50%. Other "Living off The Land" techniques using Windows systems increased 18% quarter-over-quarter.

The most widespread malware identified was Application.Cashback.B.0835E4A4, with the highest impact in Chile at 76% and Ireland at 65%. Over encrypted connections, Trojan.Agent.FZPI emerged as the top threat, described as a malicious HTML file combining legitimate-looking files with encrypted communication.

Network attack patterns showed a 16% decrease in unique signatures triggered, suggesting attackers focused on a narrower set of exploits while continuing to target unpatched legacy vulnerabilities.

The research indicates malware threats are increasingly emerging through email rather than web-based attacks. According to Chief Security Officer Corey Nachreiner, attackers are leveraging AI tools for enhanced social engineering and phishing campaigns, enabling highly targeted attacks at scale.

https://www.watchguard.com/

How AI-Driven IDP Helps Insurers Comply with Increasing Regulation

By Sunjoo Kim

Amid a rising global trend driven by increasing cyber threats, operational disruptions, and heightened consumer protection expectations, the insurance industry is facing stricter compliance and regulatory oversight.

Australia's introduction of CPS 230 is a proactive step toward aligning with international standards, strengthening operational resilience, and enhancing accountability across the sector. CPS 230 is being introduced to ensure banks, financial services companies and insurers protect their customers from cyber security, data breaches and unnecessary delays in settling claims.

As the CPS 230 operational risk management standard from APRA comes into effect in July 2025, insurers across Australia are facing increased pressure to tighten their compliance and governance frameworks.

This regulation demands robust oversight of operational risk, third-party service management, and incident response, placing a heavy spotlight on how insurers handle data, documents, and internal processes, to build a foundation for trust, speed, and agility for customers, not only minimising the risks.

CPS 230 at a Glance

CPS 230 sets new requirements for:

• **Operational Risk Management:** Institutions must identify, assess, and manage key operational risks.

• **Third-Party & Outsourcing Oversight:** Critical service providers must be monitored and risks mitigated, including brokers and underwriting agencies with binding authority.

• **Incident Management & Business Continuity:** Real-time response capabilities and robust documentation are expected.

Failing to comply could result in regulatory sanctions, loss of public trust, or reputational damage.

When breach of CPS 230 occurs, APRA doesn't impose "fines" like a criminal court, but it has strong enforcement powers such as license conditions or suspensions, public reprimands, increased capital requirements, and civil penalties in cases of systemic failure.

Even if the third party (e.g., broker, underwriter) made the mistake, the regulated entity (insurer or financial institution) is responsible, because under CPS 230 the regulated entity is accountable for managing risks, terms and monitoring performance from material service providers. Put quite simply, regulated entities cannot outsource accountability, even if the function is outsourced.

In this context, Intelligent Document Processing (IDP) and Process Orchestration technologies have emerged as powerful allies. These tools have been proven solutions for many regulated entities and will now be critical for their 3rd parties for leverage to improve efficiency and act as critical safeguards against compliance breach risks.

IDP uses AI technologies such as OCR, NLP, and machine learning to automate the extraction of data from both structured and unstructured documents. It eliminates manual data entry, applies business rules across systems, classifies and routes data to downstream processes, and ensures regulatory compliance in documentation.

IDP & Process Orchestration/Automation Help Mitigate Compliance Risks

TCG Process's DocProStar is an AI powered IDP platform including powerful orchestration capabilities to seamlessly integrate AI technologies, systems of record and humans into secure business processes. Here's how these technologies support CPS 230 compliance for regulated entities:

1. Operational Consistency Through Process Standardisation

Process Orchestration and Automation enforces uniform procedures across underwriting, claims, onboarding, and reporting processes to reduce human error and ensure consistent handling of compliance-sensitive operations.

2. Accurate & Compliant Document Processing

IDP captures, validates, and cross-checks data from customer forms, ID proofs, contracts, and medical records to ensures mandatory fields and disclosures are always present and up to date.

3. Full Audit Trails & Realtime Monitoring

Every step in an automated workflow is timestamped and logged, creating ready-to-use audit trails for easy reporting to APRA and transparent operational risk oversight.

4. Automated Risk Alerts & Escalation

Rules-based automation can detect anomalies (e.g., missing disclosures, expired IDs, or fraud flags) and trigger escalations before a breach occurs to comply with incident management obligations.

5. KYC & AML Compliance Made Efficient

IDP reads and verifies customer documents for KYC and runs them through AML watchlists to speeds up onboarding while maintaining compliance integrity.

Real-World Insurance Compliance Use Cases for IDP

Looking more closely at insurers and their broker relationships and the key business processes of onboarding/underwriting and claims, IDP aids compliance as follows.

For Policy Onboarding:

Customer Application Submission: IDP ensures all regulatory language is present in policy documents and collection of mandatory disclosures by automated data extractions from application forms

Application collection & verification – IDP classifies different document types and flag missing or invalid documents and data across cases.

Application compliance checks – Process Orchestration can invoke KYC and Compliance AIs to verify customer details against sanction lists, watchlist. IDP extracts data from IDs and documents and check for the currency and mismatch between documents. Orchestration/Automation runs AML checks, flags high-risk profiles, and stores records securely.

Automated Risk Scoring and Underwriting Inputs – IDP extracts key data points (e.g. smoking status, BMI from health reports or lifestyle disclosures) and feed into underwriting rules engine or ML model for risk evaluation and recommendation (Extractive AI)

For Claims Processing

IDP and AI verifies claim documentation and compares to policy coverage rules and approves or escalates based on pre-defined compliance logic for:

disclosure & transparency (e.g. ASIC's RG 271 Internal Dispute Resolution, General Insurance Code of Practice),

timely acknowledgement and resolution (e.g. acknowledgment within 10 business days, resolution within 4 months),

privacy & data handling – personal and medical information must be securely stored and only used for claiming related purposes (e.g. Australian Privacy Act)

fraud detection & recording in line with internal fraud management policies (e.g. claiming for pre-existing damage, staged accidents, fake invoices)

customer consent for third-party access (e.g. claimant's explicit consent is required for assessor or repairer,

CPS 230's emphasis on third party risk and customer transparency)

proper use of approved vendors (any service provider e.g. repair shop or investigator must be vetted and compliant)

Next Steps for Insurers:

Most insurers have automated in part or completely their ingestion, underwriting and claims processes using various forms of IDP. Recent developments in AI technology, however, have even the most mature insurers investigating opportunities for further improvement. The accuracy and performance of processes implemented 5 years ago, have simply been superseded in the last 3 years.

Insurers will continue to enhance these processes as it pays dividends in terms of customer service and operating costs. The challenge imposed by regulations like CPS 230 in Australia is that insurers will be accountable for managing risks from their 3rd party/material service providers (brokers, underwriters), and must work with them to monitor and ensure their compliance.

Historically brokers have operated on thinner margins and underinvested in process automation, so ensuring their compliance will be more challenging.

IDP and Process Orchestration technologies will enable insurers and their brokers to meet the higher regulatory standards and do so at scale. Here are a few approaches to consider:

■ Extend insurer's systems and processes to their brokers for monitoring and automation to ensure the 3rd party compliance

■ Adding a layer of 3rd party compliance to insurer's contracts with brokers (i.e. mandating certain info at a certain time, in the insurers' systems) to facilitate monitoring and escalations

■ Switching to 3rd party brokers with adequate systems for compliance

■ Implement contractual safeguards upon identifying gaps and agreeing on a structured program for the 3rd parties to improve their processes over a certain period using IDP with insurer oversight for monitoring performance

IDP systems allow insurers and brokers to build automation processes to suit their business needs along with a shared overlay for monitoring purposes, and that's just the beginning. More importantly, it provides a platform for continuously improving customer service, operating performance and governance. It is hard to see insurers and their eco-systems building a sustainable future without IDP and orchestration.

Final Thoughts: A Compliance-First Future

CPS 230 is not just another regulatory checkbox - it's a cultural reset and a strategic opportunity for the whole of the supply chain within the insurance industry to modernise to effectively respond to the catastrophes and cyber events as well as address the usual customers' needs.

It raises the bar for trust, accountability, and resilience. Embracing Intelligent Document Processing and Process Orchestration now not only prepares you for the July 2025 deadline but also positions your organization for sustainable compliance and resilience.

By embedding intelligence into your core processes, you don't just minimize breach risks - you build a foundation for transparency, speed, and agility in a highly regulated market.

Sunjoo Kim is Chief Experience Officer at TCG Process.

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.

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.

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

NZ Unveils Light-Touch Approach in AI Strategy

New Zealand has released its first artificial intelligence strategy after becoming the last OECD country to develop such a framework. However, the government's business-focused approach is already drawing criticism for prioritizing economic gains over ethical and social risks.

The 19-page strategy, titled "Investing with Confidence," was unveiled by Science, Innovation and Technology Minister Shane Reti, who promises AI could add $NZ76 billion to New Zealand's economy by 2038 - equivalent to 15% of current GDP. The strategy adopts a deliberately "light-touch" regulatory approach, emphasizing AI adoption over foundational development. It aims to remove barriers for businesses while relying primarily on existing laws rather than introducing new AI-specific regulations.

Current adoption rates highlight the challenge ahead. While 67% of larger New Zealand businesses now use some form of AI, a stark 68% of small and medium enterprises have no plans to evaluate or invest in the technology – significantly higher than Australia's 38%.

The government plans to address this through guidance documents, skills training, and international partnerships, including a $12 million joint research program with Singapore focused on AI for healthy ageing.

The Complexities of Managing Duplicate Files in Information Management

By Andrew Jolly

When organisations plan a system migration or content clean-up, "finding duplicates" is a common and understandable request. It's often positioned as a quick win, a way to reduce clutter, improve information accuracy, and cut down on unnecessary storage costs.

The challenge is that duplication is rarely one-dimensional. While some duplicates may be exact copies and can safely be removed, many others exist for valid reasons: version tracking, compliance, data integrity, or simply because the same information is required across different contexts or teams.

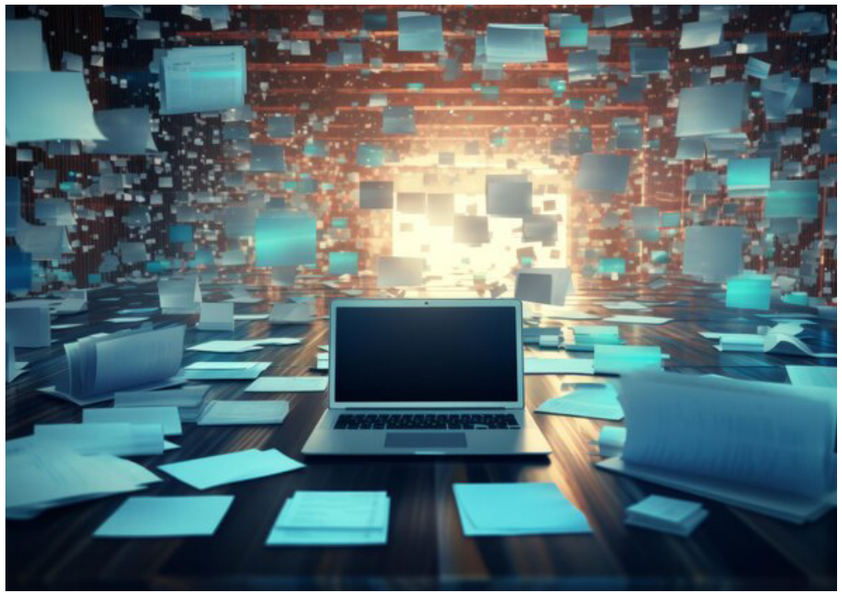
A heads up, I know this one is more of a long read - intentionally so - because this topic deserves more than a quick checklist. If you're dealing with duplication in your environment, I hope this helps.

It's often assumed that duplicates can be identified and removed with automation or out-of-the-box system tools. But in practice, identifying ***which*** duplicates can go and ***why*** involves a broader understanding of information purpose, relationships, and risk tolerance. It's not a single decision point; it's a multidimensional challenge.

When planning for a migration, storage reduction initiative or other variant of information management change, it's important to explore **why** duplicates exist before jumping to remove them. Otherwise, organisations risk losing valuable information or undermining business processes that rely on those duplicates.

1. Understanding the Types of Duplicates

Managing duplicates effectively requires understanding the different types of duplicates, as each has unique characteristics and management considerations. Essentially there are 9 types of duplicates….(yes, you're about to read about 9 types)



Exact Duplicates

Description: Files with identical content, file names, and metadata. These duplicates are often the easiest to identify and manage and the ones the most people think about when it comes to duplicates.

Example: Two copies of the same project report saved in different folders by two team members.

Treatment: Often ideal candidates for deletion or consolidation. When storage reduction is the main goal, exact duplicates can be safely removed after confirming that they don't serve any specific, necessary function.

Content Duplicates with Different Metadata

Description: Files with the same content but differing metadata, such as modified dates, user access histories, or storage locations. These often arise from sporadic or ad hoc sharing files across multiple teams or departments.

Example: A policy document saved in two different departments' folders, with one copy recently accessed or moved.

Treatment: Depending on organisational needs, one copy may be retained as the primary version, while others are archived or deleted. Metadata differences can help determine which copy is the most recent or most accessed, guiding which one to keep.

Partial Duplicates or Near-Duplicates

Description: Files containing similar but not identical content, often representing drafts, older versions, or partial copies. They may have been saved during different stages of project development or by different contributors.

Example: A marketing presentation that's been modified for different audiences or incremental drafts of a report with minor updates.

Treatment: Near-duplicates require careful review to determine if they provide unique value. Version control systems or centralised file storage can help manage these files, allowing only the latest or most relevant versions to be retained while older versions are archived or deleted.

Logical or Functional Duplicates

Description: Files that serve the same purpose or contain the same information conceptually, though they may differ in format or structure.

Example: An annual report saved in both PDF and Excel formats to meet accessibility needs or usage preferences for different audiences.

Treatment: Functional duplicates are often necessary in different formats, so deleting one could impact usability. Managing these files

Twelve books about 'X' — and somehow, none of them are quite the same. Welcome to the world of duplicates!

involves standardising storage locations and applying clear naming conventions to prevent unnecessary proliferation.

Duplicate Names with Different Content

Description: Files with the same name but differing content. These are often the result of independent work or parallel development in different departments.

Example: Two files named "Budget 2024.xlsx" created by different departments, containing projections that vary depending on departmental goals or funding sources.

Treatment: Duplicate names with differing content can lead to confusion, so they need to be reviewed to determine relevance. Clear naming conventions and metadata tagging can help differentiate these files and prevent accidental deletions or mix-ups.

Redundant Backups

Description: Copies retained as backups, often created as part of a data retention policy or disaster recovery strategy. These are intentional duplicates meant to provide data integrity and recovery.

Example: Weekly backup copies of critical files saved over the course of a month.

Treatment: Redundant backups should be governed by retention policies that specify how long they are retained and when they can be deleted. For instance, retaining only the latest weekly or monthly backup ensures data safety while reducing unnecessary storage usage.

Systematic or Structural Duplicates

Description: Files duplicated to support system structure or performance, often necessary for data accessibility, resilience, or processing needs within distributed systems.

Example: Data replicas stored in different geographic regions to ensure faster access or high availability in global organisations.

Treatment: These duplicates are typically necessary but should be documented and managed carefully to avoid unintentional growth in storage. System administrators can use these documented copies to meet performance needs without accidentally creating additional copies.

Unintentional or Redundant Duplicates

Description: Files created accidentally through user behaviour, often due to repeated downloads, email attachments, or saving versions in multiple locations. OneDrive's are a good example of where a lot of these duplicates eventuate.

Example: Multiple copies of a shared document stored in different locations by team members who downloaded it from email or cloud storage.

Treatment: Unintentional duplicates can typically be deleted without risk, as they don't serve a specific function however depending on the context they're used in there are exceptions to this point. Raising awareness of proper file-sharing practices and implementing automated deduplication processes can help reduce these types of duplicates.

Compliance or Regulatory Duplicates

Description: Copies of files that must be retained to meet legal, regulatory, or compliance requirements, often in multiple locations for auditing or record-keeping.

Example: A signed contract saved in both legal and operations departments to satisfy policy requirements.

Treatment: Compliance duplicates are usually necessary and should be stored in a controlled manner to ensure consistency. It's important to manage these copies with a clear retention schedule and to maintain alignment with legal obligations, keeping only the versions required by policy.

2. Making Duplicate Management Part of Broader Information Governance

(Continued over)

(From previous page)

Duplicate identification and reduction should never be seen as a standalone task. Instead, it should be treated as part of a wider strategy for information quality, governance, and operational efficiency.

Here are three foundational concepts that support this broader view:

Single Source of Truth (SSOT): Identifying a central, authoritative source for key information helps minimise duplicates and makes it easier to manage file integrity across departments.

Version Control and Decision-Making Tools: Managing partial or near-duplicates requires may necessitate the need for specialised duplicate identification and management systems. Products and services of this type can help identify certain types of duplicates and provide processes and mechanisms to help with determining what versions to keep, what to archive or delete.

Metadata and Tagging Standards: Metadata helps tell the story of a file, who created it, when, why, and how it's related to other content. When used appropriately, metadata allows teams to distinguish between meaningful and unnecessary duplicates. Poor metadata, on the other hand, makes de-duplication nearly impossible.

3. Not Every Organisation Is Ready – And That's OK

Let's pause here for a moment, It's important to acknowledge that not every organisation is in a position to manage duplicates in a highly structured way. Time, tools, expertise, and competing priorities all play a role in whether duplicate management is feasible and in many environments, there simply isn't the capacity to address it comprehensively.

If that's your situation, don't consider it a failure. Duplicate management doesn't have to be all-or-nothing. Here are some practical alternatives:

Start Small: Focus on obvious or high-impact areas, such as key areas within shared drives with excessive clutter, or specific teams experiencing version confusion.

Lean into Awareness: Run an awareness campaign on smarter file management, version control, and storage practices. A little education goes a long way.

Work with What You've Got: Use existing features in Microsoft 365 or Google Workspace (e.g., version history limits, sharing restrictions) as a gentle way to control duplication over time.

Tackle It as Part of Another Initiative: If you're migrating, modernising, or reorganising, build in some time to address duplicates *as part of* that work, even if it's just flagging the most obvious ones.

The key takeaway is that progress beats perfection. Doing something, however small, to reduce future duplication or support clearer file ownership can make a real difference, even if the full problem can't be solved right now.

All of this reflects a risk-based approach to information management, one that recognises that effort should be proportional to impact. Rather than aiming for total de-duplication across the board, focus on areas where duplicates create real business, compliance, or reputational risks.

For example, confusion over which contract version is valid, or duplicate budget files driving conflicting decisions, present a much higher risk than five copies of a brochure sitting untouched in different folders.

By assessing where duplication causes genuine harm, whether through inefficiency, misinformation, or policy breaches, organisations can make smarter, more defensible choices about where to act, and where to accept some level of duplication as manageable.

4. If Storage Reduction Is the Goal – Consider Version Reduction First

While duplicate files can impact storage, the bigger culprit is often file versioning. In platforms like Microsoft 365, SharePoint libraries can retain dozens or even hundreds of file versions by default. These accumulate quietly, often unnoticed, and can consume significant storage over time.

If reducing storage footprint is a top priority, version management may deliver greater and safer impact than aggressive duplicate removal. Version limits can be implemented at scale, with minimal disruption, and aligned to business needs – for example, keeping only the last 10 versions or those changed in the past 12 months.

Organisations looking to reclaim space should start here before attempting the more nuanced task of de-duplicating files that may or may not be safe to delete.

5. Conclusion: A Multi-Dimensional Challenge, Not a Checkbox

Duplicate file management is a complex, multi-dimensional challenge that cannot be solved by a single script or system feature. It sits at the intersection of technology, governance, user behaviour, and context.

It's tempting to see "duplicate removal" as a technical task – but that approach risks oversimplifying a challenge that is inherently nuanced. Files with the same content can serve different purposes.

Files with different names can be functionally identical. Files with slightly different content might all be important.

If you or your colleagues are facing a migration, modernisation, or information clean-up project, I encourage you to rethink how you approach duplicates. Ask:

- Why do these duplicates exist?
- Who relies on them?
- What context are they part of?
- And how do we manage them without breaking something else?

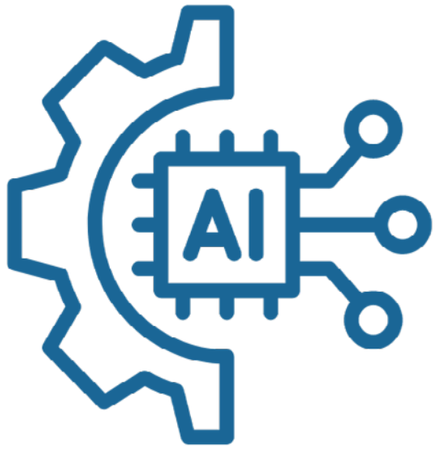
This is how we ensure our efforts to simplify don't come at the cost of losing valuable context or critical content. Perfection in duplicate management may never be possible and that's okay.

Duplicates are, in many ways, a natural byproduct of human systems. Information systems exist because people do, and so our behaviours, preferences, and ways of working inevitably leave their mark.

The real goal isn't total elimination, but smart reduction: minimising the wrong kinds of duplication in the wrong places, at the wrong times. If your organisation can do that and sustain it that's not just good information management. That's success.

Andrew Jolly is Information Management Practice Lead at Engage Squared. Article originally published here

Adeptia AI-Powered Document Processing



Enterprise data automation company Adeptia has launched its latest innovation in artificial intelligence-driven document processing, introducing AIDP (AI-driven Intelligent Document Processing) to help businesses extract valuable insights from unstructured documents with unprecedented accuracy and speed.

The new solution addresses a critical pain point for modern enterprises struggling to process the vast amounts of unstructured data contained in documents like purchase orders, invoices, and loan applications.

Unlike traditional Optical Character Recognition (OCR) systems that simply convert images to text, AIDP leverages advanced machine learning and Natural Language Processing to understand the meaning and context behind document content.

The company claims AIDP delivers measurable returns through cost reduction, enhanced operational efficiency, and improved data quality.

Where OCR might struggle with complex layouts, handwritten entries, or multi-page documents, AIDP's AI algorithms can interpret context and extract structured data ready for immediate business use.

The platform includes several enterprise-grade features designed for real-world implementation, including human-in-the-loop verification systems that allow users to validate extracted data, AI-driven business rules for automatic data validation, and support for processing large, complex file variations.

Adeptia has designed AIDP for deployment flexibility, supporting cloud, on-premises, and hybrid environments to meet diverse enterprise infrastructure requirements. The solution integrates with existing business applications and internal systems, enabling organizations to put extracted data to work within minutes rather than hours or days.

https://www.adeptia.com/products/idp

ANZ Bank doubles down on Knosys KIQ

ANZ Bank has extended its partnership with Knosys Limited, signing a one-year contract for the continued use of the company's enterprise knowledge management platform, KnowledgeIQ (KIQ).

The extension, valued at over A$1.9 million, comes as both parties work toward a longer-term, three-year agreement that would see the bank shift to Knosys' KIQ Cloud service.

The forthcoming multi-year contract is expected to include a migration to the KIQ Cloud, which is designed to streamline information access for teams and individuals, while enhancing workflows and compliance processes.

The solution is designed for organisations that run customer contact centres, service desks, frontline offices or online self-service channels.

As part of the evolving deal, Knosys will also collaborate with ANZ to integrate a new artificial intelligence assistant into the bank's knowledge management portal, aiming to improve both staff efficiency and customer service.

John Thompson, Managing Director of Knosys, described the contract extension as a testament to the long-standing relationship between the two organisations.

"This contract extension reflects our ability to support ANZ's strategic technology initiatives, including their 'cloud first' approach," Thompson said.

"We're excited by the opportunity to help ANZ enhance its workflows and customer service with AI-powered solutions."

Anomalo Transforms Unstructured Data

Anomalo has announced the general availability of its Unstructured Data Monitoring product, now enhanced with a major new feature called Workflows that promises to help enterprises tackle one of their biggest challenges in deploying generative AI applications.

The announcement addresses a critical enterprise pain point: while companies rush to implement AI-powered chatbots and retrieval-augmented generation (RAG) systems, most struggle with the quality and trustworthiness of their unstructured data - the documents, emails, call transcripts, and support tickets that make up roughly 80% of enterprise data stores.

Whether deploying RAG systems or customer-facing chatbots, enterprises need to bring high-quality, domain-specific data to their LLMs. The challenge lies in the unknown. Companies do not know what is in their unstructured data, let alone trust it, making it hard to bring production-ready Gen AI applications to market.

The company claims the new Workflows capability transforms what has traditionally been a months-long manual process into a 10-minute automated analysis. The platform can process more than 100,000 documents in a single run and operates continuously as new data arrives, identifying quality issues like duplicates, personally identifiable information (PII), abusive language, and inconsistent formatting.

Beyond quality control, Workflows enables enterprises to convert unstructured content into structured data ready for downstream analytics and AI applications - a crucial step for companies building domain-specific AI systems that require high-quality training data.

Anomalo claims to be the first company to announce AI-powered monitoring of unstructured text, having introduced the capability in June 2024 before adding additional features in November. The company's approach differs from traditional rules-based systems by using machine learning to automatically detect data quality issues across both structured and unstructured datasets.

https://www.anomalo.com/

Archive360 Partners with Snowflake

Archive360, an enterprise data archiving company, has announced a new integration with cloud data platform Snowflake that allows organizations to make their archived data available for AI and analytics applications while maintaining governance controls.

The partnership addresses a common challenge facing enterprises: vast amounts of valuable data locked away in legacy archives that cannot be easily accessed by modern analytics tools and AI systems.

"Snowflake can extract extremely valuable insights from archive data, but historically, enterprises have not been able to efficiently make this AI and analytics ready, while providing extensive governance capabilities in parallel," said Dan Manners, VP Product Strategy, Archive360.

The integration works by allowing companies to selectively publish archive data to Snowflake's AI Data Cloud platform. Archive360's system can ingest data from both active and legacy applications, then prepare and govern that data before making it available to Snowflake for analysis.

For many organizations, archived data represents a significant untapped resource. This information is often stored in proprietary formats or legacy systems that make it difficult to access at scale for modern data science applications. The Archive360-Snowflake integration aims to solve this problem by automating the process of making archive data analytics-ready.

The system is built on what Archive360 calls a "cloud-native, class-based architecture" that provides each customer with a dedicated software-as-a-service environment. This approach ensures data segregation and allows integration with existing security protocols.

Kieran Kennedy, VP of Data Cloud Product Partners at Snowflake, said the partnership helps organizations "unlock and operationalize archive data - enabling secure, compliant, and scalable access to information that was once difficult to use."

https://www.archive360.com

A Reasoning Engine for Workplace AI

Automation Anywhere hasannounced the expansion of its Agentic Process Automation (APA) system, introducing technology that CEO Mihir Shukla says represents "a fundamental reimagining of how work gets done" rather than mere incremental improvement. At the heart of the announcement is the Process Reasoning Engine (PRE), an AI system designed to understand enterprise context and dynamically orchestrate work across different departments and industries. Unlike general-purpose AI models, the PRE is specifically tailored for business processes in sectors ranging from banking and healthcare to manufacturing and customer service.

"Our PRE is a pivotal advancement with specialized insight into processes across industries and departments," Shukla explained. "PRE will fundamentally change how entire departments and companies work, enabling them to go from idea-to-action with speed and efficiency."

The company claims the technology delivers tangible results: 3x higher efficiency in building end-to-end automation and 60% greater automation resiliency compared to standalone large language models or traditional automation tools.

The company also announced the introduction of Enterprise UI Agents - which Automation Anywhere claims can interact with Web-based applications like humans do. These agents can understand context, adapt in realtime, and execute complex, multi-step tasks across dynamic web interfaces.

The expanded system goes beyond individual AI agents to orchestrate what the company calls "long-running, mission-critical processes." The platform can coordinate AI agents, traditional RPA bots, APIs, documents, and human workers across different systems and vendors.

Automation Anywhere is positioning itself for broader industry adoption by supporting emerging interoperability standards, including Google Cloud's Agent-to-Agent protocol and Anthropic's Model Context Protocol. This allows integration with major platforms like AWS Bedrock, Google Agentspace, Microsoft Copilot, and Salesforce Agentforce.

The company claims organizations using the system can automate up to 80% of their operations while maintaining enterprise-grade security and governance features, including PII data masking and AI guardrails.

https://www.automationanywhere.com/

Barracuda Takes Aim at Security Overload

Cybersecurity firm Barracuda Networks has unveiled a new BarracudaONE AI-powered platform, targeting a growing industry problem that the company says is leaving organizations vulnerable to cyberattacks.

The launch comes alongside research highlighting the scope of "security tool sprawl" – a phenomenon where organizations deploy multiple disconnected security solutions that create more problems than they solve. According to a global survey of 2,000 senior security decision-makers conducted by Vanson Bourne, 65% of IT and security professionals report their organizations are juggling too many security tools.

The fragmentation is proving costly and dangerous. More than half of survey respondents said their security tools cannot be integrated, creating environments that are difficult to manage and secure. The lack of integration increases management time for 80% of organizations while driving up costs for 81%, according to the study.

Perhaps more concerning, the tool sprawl is weakening actual security defences. Seventy-seven percent of respondents said fragmented systems hinder threat detection, while 78% cited challenges in threat mitigation. Only 32% expressed full confidence that their tools are properly configured.

"This research serves as a stark wake-up call for organizations still relying on disconnected, siloed security tools," said Neal Bradbury, Barracuda's chief product officer. "Managing a patchwork of solutions drives up costs and complexity while creating blind spots that attackers are quick to exploit."

BarracudaONE aims to address these issues by consolidating Barracuda's security portfolio into a single integrated platform with centralized management. The system leverages AI technology that the company says has been refined through years of real-world application to enable faster threat detection and response.

Early users are reporting significant operational improvements. William Mann, chief information security officer at the Borough of West Chester, Pennsylvania, described the platform as "transformational" for managing municipal services including police, fire, and wastewater operations.

"The streamlined experience of having fewer clicks and faster insights enables us to prioritize threats and respond with the speed and precision our first responders, government teams and community depend on," Mann said.

The platform is available at no additional cost to existing customers using Barracuda Email Protection, Barracuda Cloud-to-Cloud Backup, and Barracuda Data Inspector. Organizations can further enhance their security posture with Barracuda Managed XDR, a 24/7 threat detection and response service.

https://www.barracuda.com/

ABBYY Unveils Dual Process AI Solutions

ABBYY has introduced two new artificial intelligence solutions designed to enhance document-centric business operations and consulting engagements, as organizations grapple with the challenge that 90% of their documents remain unstructured.

The software company announced Process AI for Consulting (PAIC) and IDP Analytics, targeting what it describes as a $5.3 billion market demand for purpose-built AI to deliver process optimization. The launch comes as businesses increasingly seek to maximize returns on AI investments while addressing inefficiencies in document processing workflows.

PAIC specifically targets ABBYY's partner network, providing consultants with access to the company's Timeline process intelligence platform. The solution aims to accelerate project timelines and deliver data-driven insights through flexible licensing arrangements designed to reduce technical and administrative burdens for consulting firms.

"PAIC empowers consultants to identify critical inefficiencies and improvement opportunities, deliver a precise roadmap for success, and monitor outcomes," said Bruce Orcutt, Chief Marketing Officer at ABBYY.

The second solution, IDP Analytics, addresses the widespread challenge of unstructured document management within organizations. The platform combines ABBYY's intelligent document processing capabilities with process intelligence technology to create what the company describes as a "digital twin" of document processes.

IDP Analytics offers pre-built dashboards tracking metrics including processing time, costs, and straight-through processing rates. Organizations can customize these dashboards to align with specific business priorities and identify optimization opportunities.

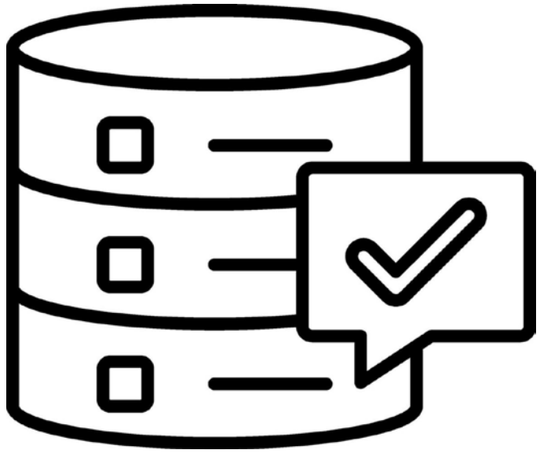
"We accomplish this by leveraging our proven Process AI to deliver a comprehensive, analytics-driven approach to document-centric programs that has proven to return millions of dollars in savings," Orcutt stated.

The solutions target different market segments within the broader enterprise AI landscape, where organizations continue to struggle with extracting value from unstructured data sources. Document processing remains a significant operational challenge across industries, particularly in sectors like insurance, financial services, and healthcare where paper-based and digital document workflows are prevalent.

Process AI for Consulting is now available to ABBYY partners, while IDP Analytics is offered as an add-on compatible with all IDP platforms.

https://www.abbyy.com/

Data Quality embeds in Development



As enterprises increasingly struggle with data quality issues in distributed architectures, Actian has unveiled significant enhancements to its Data Intelligence Platform that promise to transform how organizations ensure data trustworthiness from creation to consumption.

The HCLSoftware subsidiary announced that its platform now embeds data contracts directly into development workflows, implementing what the company calls a "data contract first" principle designed to catch quality issues at their source before they cascade through AI and analytics systems.

The enhancements tackle a growing enterprise pain point: maintaining data quality and governance across distributed architectures where individual business domains create their own data products. Under traditional approaches, quality issues often aren't discovered until data reaches downstream consumers, creating costly remediation cycles and undermining trust in AI initiatives.

Actian's solution automates much of this process by requiring data contracts – formal agreements defining data structure, quality standards, and usage terms – to be established before data products are created. These contracts are then enforced automatically through the development lifecycle.

The platform updates include several features designed to make data more accessible to business users while maintaining governance standards. A new enterprise data marketplace allows domains to publish their data products with dedicated APIs that automatically register and update catalogues within existing CI/CD pipelines.

Perhaps most significantly for non-technical users, Actian has introduced "Ask AI," a natural language query capability currently in private preview. The feature allows users to search for data using everyday language, with results ranked according to organizational glossaries and business context.

The platform also incorporates a federated knowledge graph-powered search engine designed to deliver context-aware results while maintaining compliance across the enterprise. Access request workflows provide centralized approval processes with audit trails.

https://www.actian.com/

3-Tiered Architecture for Automation

ancora Software, Inc. has announced ancoraFusion, a new platform designed to automate document workflows through the integration of advanced AI models with the company's existing machine learning technologies. The platform, scheduled for release in Q4 2025, aims to reduce human intervention in document processing by combining ancora's small language model with machine learning algorithms for document capture, classification, and data extraction.

ancoraFusion introduces a rthree-tiered architecture that allows the system to learn, adapt, and perform across a wide variety of use cases:

• **Universal First Pass Model:** At the foundation is a robust universal model that delivers high accuracy out of the box for all customers. Optimized for blind capture, this model excels at extracting data from complex line-item documents without prior configuration.

• **Customer-Specific Models:** For organizations that would benefit from models precisely targeted to their environments, ancoraFusion offers dedicated models tailored to their specific document structures and business rules - delivering even higher precision for targeted workflows.

• **Vendor-Specific Models:** Recognizing that many vendors encounter highly idiosyncratic document layouts, ancoraFusion includes models uniquely trained for these layouts, ensuring accurate extraction from even the most irregular or non-standard document designs.

Model training within ancoraFusion can be initiated either automatically or manually, offering flexibility to suit different operational requirements. The process is fully transparent and intuitive, enabling rapid adaptation to new document types without technical expertise or large sample sets. Once trained, models are automatically deployed - allowing organizations to scale effortlessly and improve continuously with minimal human intervention.

According to the company, each customer model within ancoraFusion operates in isolation to ensure data privacy and protection. The platform is designed to handle higher volumes of complex documents while reducing the need for human operators.

The platform is built to serve multiple industries including finance, distribution, healthcare, manufacturing, hospitality, and retail.

https://www.ancorasoftware.com

AvePoint Expands AI Governance

AvePoint has announced major updates to its Confidence Platform, introducing two new command centres designed to help organizations optimize costs and enhance data resilience across multi-cloud environments.

The Optimization and ROI Command Center and the Resilience Command Center also offer artificial intelligence governance capabilities for Microsoft Copilot agents.

The Optimization and ROI Command Center provides organizations with a comprehensive view of cost-reduction opportunities across their data infrastructure, including integrated license management, information lifecycle management, and strategic data migration capabilities.

“These updates represent our holistic approach to the challenges defining the modern data landscape,” said John Hodges, AvePoint’s Chief Product Officer.

“Whether organizations are looking to optimize costs, scale AI safely, or govern data across multiple clouds, the AvePoint Confidence Platform provides the unified intelligence and control they need.”

The Resilience Command Center tackles multi-cloud data governance, a critical concern as many enterprises have adopted multi-cloud strategies.

The platform offers comprehensive monitoring for Microsoft 365 services, including storage tracking, backup oversight, and cost optimization recommendations. AvePoint plans to expand coverage to Salesforce, Google Workspace, and additional platforms throughout 2025.

The company also enhanced its AI governance capabilities in response to the growing adoption of agentic AI. According to Gartner, 33 percent of enterprise software applications will include agentic AI by 2028, up from less than 1 percent in 2024.

AvePoint’s updates include enhanced Copilot agent governance, expanded prompt monitoring, and comprehensive reporting capabilities.

https://www.avepoint.com

Barracuda Addresses Data Protection Gap

Barracuda Networks has unveiled Barracuda Entra ID Backup Premium, a cloud-based solution designed to protect Microsoft Entra ID environments from data loss caused by cyberattacks and human error.

The new offering addresses what the cybersecurity company identifies as a critical gap in identity protection, extending backup capabilities beyond Microsoft’s native 30-day retention limit.

The solution protects 13 essential identity components including users, groups, roles, administrative units, app registrations, audit logs, authentication policies, BitLocker keys, and device management configurations.

“Identity is the control plane of today’s digital business - any disruption can halt operations and expose organisations to security risks,” said Neal Bradbury, chief product officer at Barracuda.

“With Entra ID Backup Premium, we are closing a critical gap in the identity protection lifecycle by adding fast, reliable recovery to our proven detection and response capabilities.

“ Unlike point solutions that focus only on backup or monitoring, Barracuda delivers a unified, end-to-end approach that makes Entra ID protection simpler, stronger and more resilient so organisations can stay secure, compliant and operational.”

The solution integrates with Barracuda’s existing BarracudaONE platform, providing users with centralized visibility through a unified dashboard. It supports both single and multi-tenant environments, targeting IT teams and managed service providers seeking to scale identity protection management.

According to the company, the software-as-a-service solution requires no installation or configuration, allowing customers to connect their Microsoft 365 tenant and begin backing up data within minutes.

The platform includes advanced search capabilities, realtime monitoring, detailed audit logs, and five levels of role-based access control.

The product is available globally through Barracuda’s network of resellers and managed service providers. Customers can purchase it as a standalone offering or as part of a subscription with Barracuda Cloud-to-Cloud Backup.

https://www.barracuda.com/

AI Search Unlocks Backup Archives

Data security firm Cohesity has integrated its Gaia AI platform with Microsoft 365 Copilot, allowing users to search backup data using conversational queries directly within the Copilot interface.

The integration enables knowledge workers to access information stored in backed-up emails, documents and spreadsheets through natural language questions. Users receive responses filtered by their existing permissions, maintaining data security controls.

Cohesity claims this represents a first-to-market innovation for accessing backup data through generative AI. The platform combines large language models with retrieval augmented generation techniques to search across archived information.

The service addresses a growing enterprise challenge around data accessibility. Many organisations struggle to extract value from archived information, particularly as data volumes increase and compliance requirements become more complex.

https://www.cohesity.com

Denodo Adds Deep Research Function

Data management company Denodo has announced the release of Denodo DeepQuery, a deep research capability designed to enable generative AI systems to investigate, synthesize, and explain reasoning beyond basic fact retrieval. The capability is currently available in private preview with general availability planned for the near future.

DeepQuery is built to address complex, open-ended business questions by leveraging live access to governed enterprise data across multiple systems, departments, and formats. The system analyzes complex questions and searches across multiple sources to deliver structured, explainable answers based on realtime information.

The company says its capability goes beyond traditional generative AI chat or retrieval augmented generation (RAG) systems by enabling users to ask cross-functional questions that typically require days of analyst work. Examples include queries such as “Why did fund outflows spike last quarter?” or “What’s driving changes in customer retention across regions?”

DeepQuery connects to live, governed data across different systems and applies reasoning to deliver answers within minutes, rather than requiring users to piece together reports and data exports manually.

The capability will be packaged with the Denodo AI SDK and developed as an extensible component of the Denodo Platform, allowing developers and AI teams to build and integrate deep research capabilities into their own agents, copilots, or domain-specific applications.

Denodo also announced support for Model Context Protocol (MCP), with an MCP Server implementation included in the latest version of the Denodo AI SDK. This enables AI agents and applications based on the Denodo AI SDK to integrate with any MCP-compliant client.

https://www.denodo.com/

Unstructured Data Startup raises $US7.5M

Unstructured data specialist Diskover has raised $US7.5 million in seed funding while simultaneously acquiring CloudSoda and forging strategic partnerships with Snowflake and NetApp, positioning itself as a key player in the enterprise AI data pipeline market.

The Miami-based company, which serves over 130 enterprise customers across industries including media, life sciences, and manufacturing, announced the trio of milestones as part of its push to help organizations harness the estimated 80% of enterprise data that remains unstructured and largely untapped.

Diskover’s platform addresses a critical bottleneck in enterprise AI adoption: the ability to identify, catalogue, and curate relevant unstructured data - including documents, videos, audio files, and text messages - from massive, globally distributed repositories.

The company’s technology continuously scans and indexes billions of files across hybrid environments, creating searchable metadata that enables IT teams to govern and route data effectively.

The CloudSoda acquisition brings natural language AI capabilities and enhanced usability to Diskover’s platform.

While terms were not disclosed, Hall described the deal as “an ideal coupling” that combines Diskover’s scale with CloudSoda’s simplicity to create “the most intuitive and enterprise-ready unstructured platform on the market.”

Snowflake’s investment goes beyond capital, with the cloud data platform company agreeing to make Diskover available through its marketplace.

The partnership will integrate Diskover’s on-premises data intelligence capabilities with Snowflake’s Openflow data integration service, addressing hybrid data orchestration challenges.

NetApp’s partnership positions Diskover as part of the storage giant’s integrated data pipeline strategy, connecting various data sources from edge devices to cloud environments. The collaboration aims to accelerate cyber resiliency, AI readiness, and storage efficiency for joint customers.

Industry analysts highlight the growing importance of unstructured data management as AI adoption accelerates. Ben Woo, principal analyst at Neuralytix, noted that “AI engines require relevant and accurate data” and that “Diskover helps enterprises to identify the data that will generate the greatest value.”

Diskover’s technology verifies against existing enterprise authentication systems to honour permissions and security protocols, ensuring governance compliance while enabling efficient large language model training and inference.

https://diskoverdata.com/

fileAI Tackles Data Disconnect

Singapore-based fileAI has launched its V2 platform, a next-generation solution designed to help enterprises and small-to-medium businesses access, collect, and structure business data from unstructured formats and disconnected systems.

“fileAI v2 is a game-changer for enterprises and SMBs struggling to unlock the value of unstructured data,” said Christian Schneider, CEO and Co-founder at fileAI.

“Our focus has always been on the foundation, delivering the cleanest, most accurate data possible so AI workflows actually work. Even the slightest inconsistency results in costly errors. This isn’t just an upgrade, it’s a redefinition of what file intelligence can do.”

Key Features of the fileAI V2 Platform:

Beethoven and Decider models: Parse, extract, and classify data from diverse file types, including contracts, images, free text, invoices, financial statements, legal forms and more with industry-leading accuracy. Easily handles variations in layout, language, and handwriting, always ensuring accurate results.

Match and Compare engine: Automatically detects discrepancies, clause variations, and anomalies across documents, crucial for compliance, risk, and due diligence.

Answer Engine: Enables users to query, chat, and extract insights across multiple documents using internal data and relevant web context.

fileAI Drive: A secure document repository with robust access controls and integrations with Google Drive, Dropbox, and APIs.

Since 2024, fileAI has created over 200 million AI schemas, resulting in an estimated 320,000 hours saved and $6 million in processing costs for clients. The platform offers flexible self-service pricing starting at $0 and features an MCP-ready architecture.

The company targets industries where accuracy and compliance are critical, including financial services, legal teams, insurance, and accounting.

“Organizations in financial services, legal, insurance, and accounting face mounting pressure to automate while navigating rising regulatory complexity and shifting market demands,” said Tim Prugar, Head of Product & Engineering at fileAI.

“Instead of being held back by outdated processes and fragmented data, fileAI gives them the tools to access, structure, and act on critical information to drive successful business outcomes.”

fileAI has established partnerships with industry leaders including Nvidia, Oracle, AWS, and Google to extend its reach in the enterprise market.

https://www.file.ai/

Intellistack Debuts No-Code Automation

Data capture and workflow automation vendor Intellistack, formerly known as Formstack, has announced its corporate rebrand alongside the launch of Streamline, a no-code process automation platform designed to enable organizations to build secure workflows without data migration or retention requirements.

The Denver-based company, which has provided data capture and workflow automation solutions since 2006, said the rebrand reflects its expanded focus beyond digital forms to encompass artificial intelligence, automation, and data activation capabilities. Streamline addresses enterprise challenges where valuable data remains isolated across disconnected systems and trapped behind compliance regulations, according to the company. The platform features AI capabilities embedded throughout to enhance accuracy, reduce manual processes, and improve security.

The platform’s core architecture includes secure multi-system integrations with zero data retention, automatic classification of sensitive data including HIPAA, SOC 2, PII, and PHI information, dynamic prefilling capabilities using existing data, automated write-back workflows for realtime system updates, and built-in security guardrails with compliance support.

Streamline is suitable for all industries and for all large-scale processes, including patient referrals and registry, financial agreements, new client or employee onboarding, procurement, student enrollment, authorization requests, and many more.

The company indicated that existing Formstack and Formsite products will continue to be sold and supported.

https://www.intellistack.com

FrankieOne for AML Compliance

Australian financial technology provider FrankieOne has unveiled a new compliance platform designed to help businesses navigate sweeping changes to the country’s anti-money laundering regime set to take effect next year.

The move comes as AUSTRAC’s updated AML/CTF obligations approach, with changes for current reporting entities beginning March 31, 2026, and new requirements for previously unregulated sectors starting July 1, 2026. The regulatory overhaul is being driven in part by Australia facing a mutual evaluation by the Financial Action Task Force, the global AML standard-setter, beginning in 2026.

The reforms will expand AUSTRAC’s regulation into new industries including legal professionals, accountants, conveyancers, and trust and company service providers, while also imposing enhanced requirements on existing reporting entities such as banks and digital asset providers.

FrankieOne’s platform connects businesses to more than 350 identity, fraud, and AML data sources across 190 countries through a single application programming interface. The Melbourne-based company positions the solution as an alternative to rebuilding compliance infrastructure from scratch.

“The pace of regulatory change is accelerating, and patchwork systems won’t keep up,” said Simon Costello, CEO of FrankieOne. “FrankieOne offers a scalable foundation, not just a tool, enabling compliance teams to simplify operations, reduce risk, and future-proof their stack.”

AUSTRAC’s reforms call for risk-based customer due diligence processes, enhanced oversight and governance, structured ongoing monitoring, and improved reporting and auditability. The changes also mandate Enhanced Customer Due Diligence processes for high-risk scenarios.

The platform is already in use by major Australian institutions including Westpac, which partnered with FrankieOne to streamline customer verification across business units.

“We experienced a substantial uplift in pass rates when we first went live, and the ease of integration has made FrankieOne our go to platform across the Westpac Group,” said Hayden Johnson from Westpac.

Other customers include e-commerce platform Shopify, which deployed automated global Know Your Business processes, and PointsBet, which implemented real-time fraud detection using device signals and behavioral analytics.

AUSTRAC has acknowledged the tight implementation timeframes and is developing guidance materials, including starter program kits for small businesses, with further educational resources planned for release throughout 2025.

https://frankieone.com/

Hyland adds Agentic Document Processing

Hyland has announced the launch of its next-generation agentic document processing solution. The new solution builds upon Hyland’s existing Intelligent Document Processing capabilities by incorporating generative AI to enable business-level processes across enterprises. Unlike traditional document processing tools that focus on data capture and extraction, Hyland’s agentic document processing is designed to understand, reason, and act autonomously.

The technology is purpose-built for mission-critical industries including healthcare, financial services, government, and insurance. It converts documents and unstructured data into machine-interpretable representations, allowing intelligent agents to interpret meaning, assess context, and drive decisions within complex workflows.

“We’re not simply applying agentic AI to automate individual tasks - we’re transforming entire processes and broader workflows, which represents a fundamental differentiation in how organizations can leverage AI to drive meaningful business outcomes,” said Hyland CEO, Jitesh S. Ghai.

“By leveraging generative AI, Hyland’s agentic technologies not only discover and reason, but drive action across all levels of enterprise business processes.

“This includes making decisions and driving intelligent automation to realize business outcomes not possible before - something that no other technology provider in content management can do today.”

The solution features several key capabilities, including zero-shot, context-aware agents that require no training data, reasoning and action functions that trigger downstream workflows autonomously, and process-aware design that supports entire workflows including decision-making and exception handling.

The technology is deployed on Hyland’s Content Innovation Cloud platform and is designed to integrate with Electronic Health Records, Enterprise Resource Planning, Customer Relationship Management and legacy systems.

In healthcare applications, the solution can triage inbound documents, extract clinical intelligence, reason over patient histories, and update records in near realtime while automatically initiating alerts or follow-up actions without disrupting existing workflows.

Alan Pelz-Sharpe, Founder of Deep Analysis, commented that “Hyland has been delivering core components of Intelligent Document Processing for years - through document capture, classification, and workflow automation. Adding agentic AI enables more autonomous, intelligent actions, marking an evolution of its capabilities.”

https://www.hyland.com/

S5000 Scanners add Processing Power

Kodak Alaris has announced the launch of its new S5000 Scanner Series alongside KODAK Capture Pro 7.0 software, targeting organizations with high-volume document digitization needs.

The new scanner lineup features a significant processing upgrade, incorporating a 32-core image processor compared to 12 cores in previous models. This enhancement enables faster throughput and parallel processing capabilities for complex scanning operations.

Three models will be available starting in August: the S5160 processing 160 sheets per minute, the S5180 at 180 sheets per minute, and the S5210 capable of 210 sheets per minute. In tri-stream mode, these scanners can produce up to 1,260 images per minute.

The scanners address growing compliance requirements, particularly for federal agencies and public sector organizations. The devices offer FADGI (Federal Agencies Digital Guidelines Initiative) compatibility, which mandates authentic document imaging for US government digitization projects. Similar compliance standards exist in Germany through TR-Resiscan requirements.

According to market research firm Infosource, Kodak Alaris maintains market leadership in the production scanner segment. The company has designed the new series to handle diverse document types, from lightweight 25 g/m² paper to heavy 433 g/m² materials, and can process documents up to 10 meters in length.

Key features include intelligent document protection with four independent safety mechanisms, including ultrasonic double-sheet detection and metal detectors for staples and paper clips. The scanners also incorporate a tri-stream function that simultaneously creates color, black and white, and black and white dropout images without speed reduction.

The devices feature a 9.3-inch control panel with a 7.5-inch touchscreen interface and network compatibility for easier integration into existing workflows.

KODAK Capture Pro 7.0 software represents a major architectural upgrade, built on true 64-bit architecture to enable stable processing of large data volumes.

The software features a redesigned user interface with tile layout that can be customized to individual requirements. The new version has been specifically optimized for the S5000 Series and supports advanced features including the tri-stream function and seamless reassembly of extra-long documents that are initially captured in segments.

Both the S5000 Scanner Series and KODAK Capture Pro 7.0 are scheduled for availability in August.

https://www.kodakalaris.com

A Defence Against Email Bombing

Microsoft is rolling out a new security capability designed to protect organizations from email bombing attacks, a growing cyberthreat that floods inboxes with massive volumes of messages to disrupt operations and hide legitimate communications.

The "Mail Bombing Detection" feature, part of Microsoft's Defender for Office 365 suite, will automatically identify and quarantine suspicious high-volume email campaigns without requiring additional configuration from IT security teams. The global deployment is scheduled to begin in late June 2025 and continue through July.

Email bombing represents a sophisticated attack strategy where cybercriminals overwhelm target mailboxes with excessive messages in short timeframes. These attacks serve dual purposes: degrading email system performance and burying critical communications under floods of junk mail.

"The deluge of junk emails can bury important messages, causing recipients to miss critical information or instructions," according to technical documentation describing the threat.

The new protection system employs machine learning algorithms to distinguish malicious bombing campaigns from legitimate high-volume communications like newsletters and marketing emails. The technology analyzes multiple factors including message velocity, sender reputation metrics, and content similarities between messages.

When suspicious patterns are detected, the system automatically routes flagged messages to users' junk folders while respecting existing safe sender configurations to avoid disrupting authorized communications.

Security teams will gain comprehensive visibility into email bombing attempts through Microsoft's Defender portal interfaces, including Threat Explorer, Email Entity View, and Email Summary Panel. Organizations using programmatic monitoring can access detection data through Advanced Hunting queries using Kusto Query Language.

This integration ensures the new capability fits seamlessly into existing security workflows and reporting mechanisms.

Unlike many security updates that require manual configuration, Mail Bombing Detection will activate automatically across organizations using Defender for Office 365. Microsoft recommends that companies prepare by updating internal security documentation, reviewing junk folder policies, and briefing security operations teams on the new detection capabilities.

Organizations with compliance requirements should note that the feature modifies email classification processes and may affect audit logging for messages redirected to junk folders.

AI Data Boom Drives LTO Tape Revival

Linear Tape-Open technology shipments reached a record 176.5 exabytes in 2024, marking 15.4% growth as enterprises grapple with surging unstructured data from artificial intelligence and machine learning implementations.

The growth represents the fourth consecutive year of increases for tape storage, contradicting predictions that cloud adoption would diminish demand for the technology. Hewlett Packard Enterprise, IBM Corporation and Quantum Corporation reported the shipment figures through their LTO Program consortium.

"Setting a new growth record for the fourth year in a row, LTO tape technology continues to prove its longevity as a leading enterprise storage solution," said Bruno Hald, General Manager, Secondary Storage, Quantum.

"Organizations navigating their way through the AI/ML era need to reconfigure their storage architectures to keep up, and LTO tape technology is an essential piece of the puzzle for those seeking a cost-friendly, sustainable, and secure solution to support modern technology implementation and the resulting data growth.

"We look forward to introducing the next iteration of LTO tape technology this year to bring enhanced storage capabilities to the enterprise."

The continued expansion reflects enterprise struggles with data management costs and security risks as AI implementations generate massive datasets requiring long-term retention.

Tape storage offers offline backup capabilities that provide protection against ransomware attacks increasingly targeting connected storage systems.

"Continued growth in LTO tape shipments shows the important role that tape plays in modern data architectures, especially as companies deal with rapidly growing amounts of data," said Phil Goodwin, Research Vice President, Infrastructure Software Platforms, IDC.

"In fact, tape's unique combination of scalability, cost-efficiency, and cyber resilience makes it a valuable component for enterprises seeking secure, sustainable long-term data storage."

The LTO consortium plans to release LTO-10 specifications this year, offering 30TB per cartridge capacity compared to current LTO-9's 18TB native capacity.

The new format will include quantum-safe encryption capabilities as organisations prepare for future cryptographic threats.

Code-free Semantic Data Models

Progress Software Corporation has unveiled the latest version of its Semaphore metadata management platform, introducing advanced artificial intelligence capabilities designed to help enterprises better organize and extract value from their data assets.

The new release features expanded connectivity to a wider range of large language model providers and streamlined tools for building semantic data models without requiring technical coding expertise.

The enhanced platform addresses growing enterprise challenges in managing diverse data types across organizations.

Companies increasingly struggle with information silos and fragmented processes that limit their ability to generate actionable business intelligence from accumulated data.

"This release not only builds on Semaphore's comprehensive knowledge modelling capabilities but also ensures seamless integration with emerging AI and semantic standards," said John Ainsworth, Executive Vice President and General Manager of Application and Data Platform at Progress Software.

The Semaphore semantic AI platform enables users to manage knowledge models and automatically extract and classify both structured and unstructured data to generate rich semantic metadata.

It simplifies information and helps organizations use data effectively to make quicker decisions.

Key improvements in the new release include an AI Model Builder that connects to multiple language model providers, visual constraint definition tools that eliminate the need for custom coding, and enhanced support for industry-standard knowledge organization systems.

The platform also introduces structural-level classification settings and concept reuse features to improve efficiency in model development.

https://www.progress.com/semaphore

Panzura Targets Permission Sprawl

According to industry analysts, permission sprawl has reached epidemic proportions, with the average organization exposing more than 802,000 data files to risk. The problem is compounded by statistics showing 74% of data breaches involve privileged credential abuse, while 91% of employees retain access to company files after offboarding.

Panzura has introduced Access Control List analysis and automated remediation capabilities to its Symphony data services platform, targeting what the company describes as a trillion-dollar global crisis of permission sprawl affecting 58% of enterprises.

The new capability represents what Panzura claims is a first-of-its-kind solution. Unlike existing reactive security tools, Symphony continuously tracks, monitors, and automatically fixes permission inheritance problems before they can be exploited by malicious actors.

The financial impact is significant, with insider incidents averaging $US16.2 million in costs. Panzura notes that artificial intelligence amplifies these risks by enabling large language models to surface sensitive data to unauthorized users within seconds.

“Manual permission audits are a nightmare - teams are constantly chasing inheritance chains, investigating anomalies, and trying to resolve violations,” said Sundar Kanthadai, Chief Technology Officer at Panzura.

“Automated remediation is the difference between organizational chaos and strategic control.”

The Symphony platform now provides automated detection and mass permission changes across entire file system estates, regardless of underlying infrastructure.

Key features include Interactive Access Control List (ACL) analysis and automated remediation for identifying permission changes in directory trees, and a Repair ACLs Policy that automatically remediates broken inheritance for both Discretionary Access Control Lists and System Access Control Lists.

Beyond ACL remediation, Symphony provides the ability to apply custom metadata to files, enabling advanced policy automation and fuelling AI pipelines based on file attributes without content scanning. Support has been extended to Windows Alternate Data Streams (ADS) and Extended Attributes (EA) for greater visibility and automation.

Symphony provides actionable metadata insights, automating data movement between file systems, object stores, and cloud storage for petabyte-scale data orchestration, storage cost optimization, and AI workload placement. The platform uses and preserves metadata during data movement while simultaneously addressing challenges in permission hygiene and compliance – crucial for preparing the data landscape for AI initiatives.

Additional enhancements include support for Windows Alternate Data Streams and Extended Attributes, enabling advanced policy automation and metadata management. The platform also adds support for NetApp FlexGroup Volumes and IBM Storage Deep Archive for cold data storage.

Symphony is available immediately to existing customers through standard updates and to new customers through direct sales and Panzura’s global partner network. The company offers comprehensive migration services and training programs, with special pricing available for organizations preparing AI initiatives.

https://www.panzura.com/

Nutrient Addresses AI Challenges

Nutrient has released its Q2 2025 Document AI SDK update, introducing artificial intelligence features designed to streamline document processing workflows as enterprises struggle with widespread AI adoption challenges.

Enterprise AI adoption has accelerated dramatically, with 78% of organizations now using AI in at least one business function, yet 42% of C-suite executives report that AI adoption is “tearing their company apart” due to implementation difficulties and organizational friction.

The company’s latest release addresses these challenges with integrated features including AI-powered redaction that combines large language models with traditional approaches for data privacy compliance, and AI text comparison that categorizes and summarizes changes between document versions.

The update expands AI Assistant capabilities across mobile and desktop platforms, including MAUI, Flutter, React Native, and .NET for Android, enabling natural language document interaction. The iOS version now supports multi-document context and summarization. A key addition is the DWS MCP Server, an open-source tool that enables developers to build document workflows through natural language prompts. The server connects AI agents to accomplish tasks ranging from redacting personally identifiable information to merging PDFs and converting documents.

The release also features a rebuilt Java SDK aligned with Nutrient’s modern engine, accessibility upgrades supporting WCAG 2.2 standards, and performance improvements across optical character recognition and PDF conversion processes.

https://nutrient.io

Devworkz Three-Phase AI Program

A Sydney-based developer has launched what it calls a practical solution to one of modern business’s biggest challenges: how to meaningfully integrate artificial intelligence into everyday operations without getting lost in technical jargon.

WorkDynamics by Devworkz is positioned as a bridge between business leaders who need AI solutions and the often complex world of AI implementation.

“We’re not interested in AI for its own sake,” said John Ackery, Innovation Director at WorkDynamics. “We believe in AI that works for real people, in real workplaces, delivering real results.”

The program addresses a growing disconnect in the business world, where AI has become ubiquitous in marketing materials but remains elusive in practical application for many organisations.

The initiative unfolds through three distinct phases designed to take organisations from AI curiosity to capability.

The “Learn” phase introduces business leaders to AI fundamentals through the company’s Fusion Academy and an online community, deliberately avoiding deep technical requirements while building decision-making confidence.

During the “Explore” phase, participants work hands-on with pre-built AI applications including Safe Havens for child safety reporting and Injury Guard for workplace hazard management. The phase also introduces users to AI agents named Nova, Riley, Ava, and Mia, designed to support both customer-facing and internal operations.

The final “Activate” phase involves integrating AI into live business systems with expert guidance, from workflow optimisation to intelligent data platforms.

What distinguishes the program, according to Ackery, is its emphasis on addressing actual workplace challenges rather than showcasing AI capabilities for their own sake.

“This isn’t just a training program - it’s a transformation journey,” he explained. “We aim to help organisations move from curiosity to capability, from experimentation to execution.”

The solutions are built on Microsoft’s Power Platform, utilising Microsoft Dataverse for data integration and Microsoft Copilot Studio for agent management. The company emphasises that while many applications use the Power Platform, WorkDynamics focuses exclusively on AI-native solutions designed to embed intelligence directly into business processes.

The program is now accepting registrations through the company’s website, targeting business leaders who want to embrace AI transformation but need structured guidance to navigate the implementation process.

https://www.devworkz.net/Managed-AI-Modernisation-Register

Data Governance for Google Workspace

Mimecast has unveiled a new solution designed to strengthen data governance and compliance capabilities across Google Workspace collaboration tools. The technology extends beyond traditional email security to encompass Google Chat, Google Calendar, Google Drive, and Google Meet.

The solution addresses growing security concerns surrounding collaboration platforms. According to Mimecast’s State of Human Risk 2025 report, 79 percent of survey respondents identified collaboration tools as sources of emerging threats, including social engineering attacks, insider risk, and account compromise.

The new offering provides organizations with AI-powered archiving and data retention capabilities, along with eDiscovery, case management, and compliance monitoring functions. These features target businesses in regulated industries that must comply with standards such as FINRA, GDPR, CCPA, HIPAA, PCI DSS, FOIA, and FDIC requirements.

“IT teams face a complex and large volume of compliance requirements, often struggling with manual processes, siloed systems, and incomplete datasets across diverse data sources,” said Ranjan Singh, Mimecast’s Chief Product & Technology Officer.

The platform delivers four primary capabilities: retrospective access for unified historic searches across Gmail and Drive, with Meet, Chat and Calendar integration planned for later this year; data management and governance to satisfy archiving and retention requirements; proactive analysis through realtime compliance supervision; and behaviour trends analysis to identify patterns in collaboration data.

This integration builds upon an existing partnership between Mimecast and Google. The companies previously collaborated on governance and compliance offerings for Gmail data, as well as integrations with Google Drive, Google Security Operations SOAR, and other Google security platforms.

https://www.mimecast.com/