Affinity Data

M365 Configuration and Risk Assessment

See what you're working with.
Know what to do next.

An assessment of your Microsoft 365 environment to understand and improve your security, compliance, and governance posture.

M365

Table of Contents

Summary

Microsoft 365 is a powerful productivity platform, but its scale and complexity often create blind spots in security and compliance. Organisations are increasingly adopting Microsoft Purview to address these challenges - yet many rush into configuration without fully understanding their current environment or the longer-term governance implications.

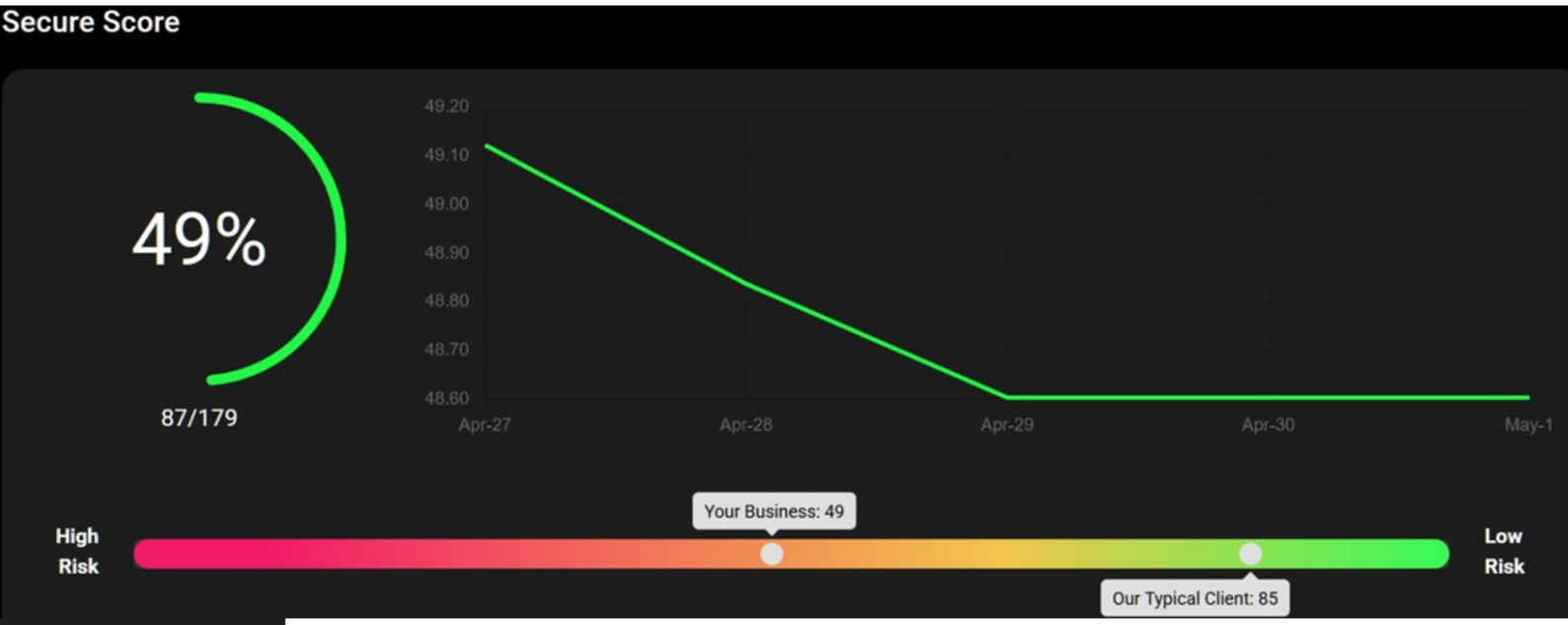
We frequently see organisations enable Purview features such as retention policies, sensitivity labels or Data Loss Prevention in isolation, only to encounter unforeseen outcomes. Policies may conflict with legacy permissions, frustrate users, or fail to meet compliance requirements due to incomplete coverage. Without a baseline assessment, these efforts risk becoming reactive rather than strategic - locking in flawed assumptions and creating technical debt that's difficult to unwind.

The Affinity Data Microsoft 365 configuration and risk assessment helps avoid this trap. It delivers a clear, actionable view of your current posture, revealing hidden gaps in identity controls, access governance, external sharing, data protection and threat management. Findings are benchmarked against frameworks including the Australian **Essential Eight, NIST, CIS and APRA CPS 234** - helping you align governance practices with both internal objectives and external obligations.

By addressing these issues early, organisations reduce risk exposure, avoid compliance failures and build a roadmap that ensures Purview's features are deployed effectively and sustainably. This assessment is more than a technical review - it's a strategic first step in building clarity, confidence and control across your Microsoft 365 environment.

STRATEGIC FIRST STEP

What the Microsoft 365 risk assessment covers - and why it matters



CRITICAL INSIGHTS

A Microsoft 365 risk and configuration assessment delivered by Affinity Data is a short, high-impact engagement that reveals how your cloud environment aligns to security, compliance and governance best practices. It combines automated analysis with expert interpretation to provide a clear picture of where your risks lie and how to address them.

Unlike a surface-level review, the assessment covers all the critical layers that influence cloud governance outcomes:

Identity and access controls

The assessment examines how access is granted, managed and secured. It identifies excessive administrative privileges, dormant or unmonitored accounts, gaps in multi-factor authentication, and whether legacy authentication is still permitted. These findings are crucial - credential misuse remains a leading cause of cloud breaches.

Device trust and endpoint visibility

We evaluate device compliance and how well your policies are enforced across company-owned and BYO devices. This includes inactive or unmanaged endpoints, which often introduce unseen vulnerabilities, and highlights whether conditional access is applied effectively.

Collaboration and external sharing

The review includes guest access across Teams and SharePoint, link-sharing policies, and the sprawl of external collaboration. Many tenants are unaware of the extent to which external parties retain access - a common and often overlooked risk.

Compliance configurations

This includes existing Purview capabilities such as retention labels, sensitivity labelling, DLP and audit logging. We assess how well these are implemented, where coverage is inconsistent, and where configuration gaps may leave sensitive data exposed.

Threat protection and security policies

We look at policies and protections within Microsoft Defender, anti-phishing configurations, Safe Links/Safe Attachments, and how well your environment detects and responds to common threats. These are benchmarked against frameworks such as CIS Controls and Microsoft's Secure Score.

Licensing alignment and cost efficiency

The assessment also reveals potential savings and improvements by highlighting unused or misaligned licenses, but without exposing your cost structure or business model. Rather than showing how to save money, we demonstrate where strategic license adjustments can fund better security or compliance outcomes.

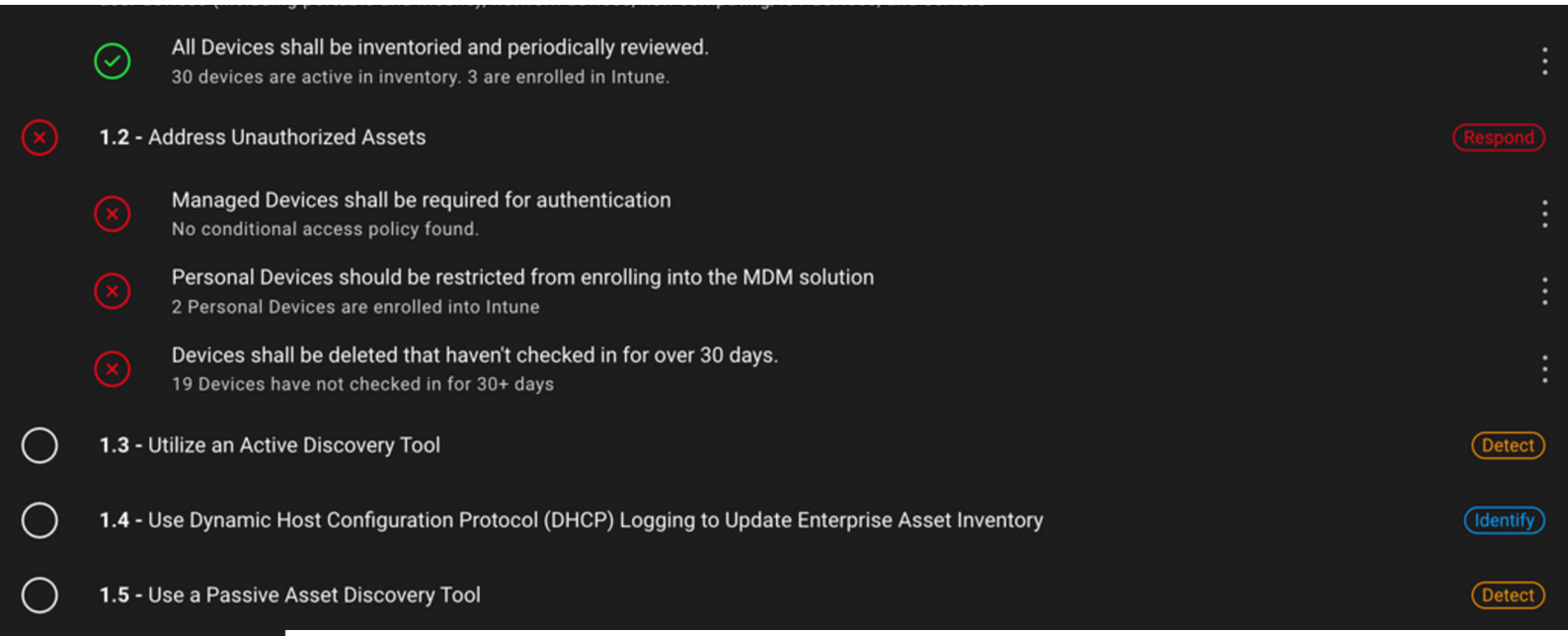
EQUIP DECISION MAKERS

Framework alignment

Our findings are mapped to the Australian Essential Eight, NIST CSF, CIS Controls, and APRA CPS 234 (where relevant). This helps technical teams understand gaps in practical terms and enables compliance or audit stakeholders to track alignment against familiar frameworks.

Each of these areas contributes to a broader objective: equipping decision-makers with the insight needed to strengthen governance, avoid unforced errors, and prepare for a successful rollout or enhancement of Microsoft Purview.

Common issues uncovered by the assessment



DISCOVER RISK

Every Microsoft 365 environment is different, but certain patterns emerge time and again. These issues often go unnoticed until a breach, audit or failed project forces them into the spotlight. The assessment identifies and contextualises these risks so they can be addressed before they become problems.

Multi-factor authentication gaps

One of the most common and high-risk findings is incomplete MFA coverage. While administrators may be protected, standard users often are not. Conditional Access policies may be inconsistently applied, or legacy protocols may still permit logins without strong authentication. This remains one of the most exploited weaknesses in Microsoft 365 environments.

Dormant accounts and privilege sprawl

It is not uncommon to find user accounts that have not logged in for months, yet still have active licences and elevated access. These are often forgotten service accounts or old admin roles that were never removed. They increase your attack surface, consume resources unnecessarily and indicate weak identity governance.

HIGH-IMPACT IMPROVEMENTS

Oversharing and external access risks

Excessive guest access, anonymous sharing links and broadly accessible SharePoint sites are widespread issues. Many tenants have little visibility over how information is shared externally, or who still has access to it. This lack of control can lead to accidental data exposure or breach of contractual and regulatory obligations.

Inconsistent or absent data retention

Some content is kept indefinitely, while other data is deleted arbitrarily. Many organisations lack a formal retention policy for SharePoint, Teams or Exchange content. This creates compliance gaps, increases discovery risk, and contributes to uncontrolled data growth.

Legacy authentication still enabled

Even in tenants that have adopted modern authentication, legacy protocols like IMAP or SMTP Basic Auth are often still permitted. These bypass MFA and are a common path for credential abuse. Their presence undermines any gains made through more advanced security measures.

Shadow IT and ungoverned apps

Third-party applications authorised by users can introduce unmonitored access to mail, files or calendar data. These are often granted high levels of permission without formal approval. The assessment identifies these apps and helps organisations regain control over how data is accessed and used.

Security monitoring and response gaps

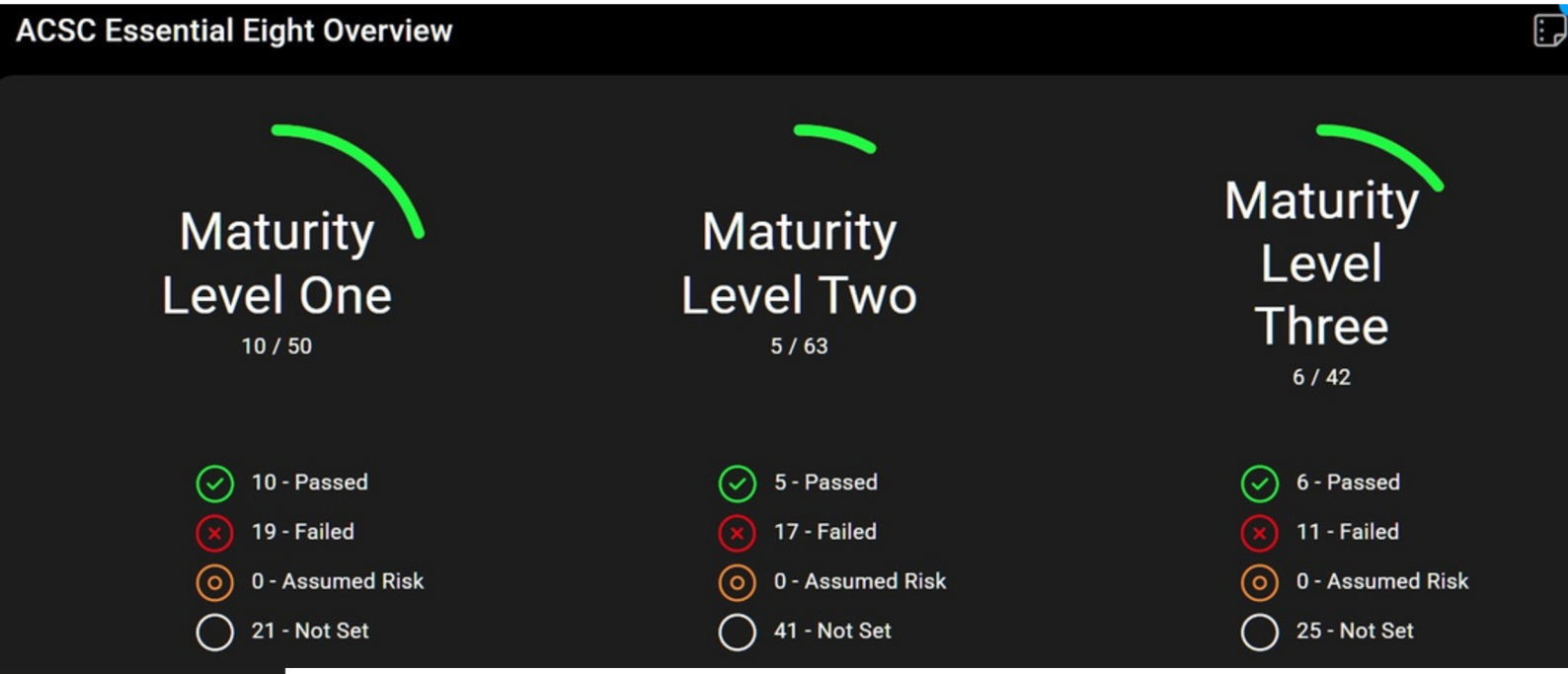
Audit logs may be disabled. Alerts might not be configured. In some cases, high-risk sign-ins have occurred without triggering any response. While the tools exist, they are often not fully enabled or integrated with security operations. The assessment highlights these gaps and recommends simple, high-impact improvements.

Inactive Teams and SharePoint sites

Digital clutter builds over time. Inactive collaboration spaces may still contain sensitive content, with no owners actively managing access. These abandoned sites can pose long-term risks if not reviewed or retired appropriately.

Together, these issues illustrate the governance and security challenges that accumulate in Microsoft 365 over time. The assessment does more than flag problems. It provides practical, targeted recommendations to address them, aligned to your licensing, business model and maturity.

Regulatory alignment and compliance mapping



COMPLIANCE

One of the most valuable aspects of the Microsoft 365 risk assessment is how it links technical findings to recognised compliance frameworks. For regulated entities, this is critical. It provides clarity on where your tenant stands today and highlights what needs to change to meet evolving obligations.

Affinity Data maps assessment findings to the frameworks that matter most in your jurisdiction and sector, including:

Australian Essential Eight (ACSC)

Widely adopted across the public and private sectors, the Essential Eight provides a practical, outcomes-based guide for improving security maturity. The assessment evaluates relevant controls such as MFA enforcement, administrative privilege management and patch compliance. Each area is rated using the maturity model defined by the Australian Cyber Security Centre, helping organisations track real progress.

STAKEHOLDERS AUDITORS REGULATORS

APRA CPS 234

For financial services and other regulated industries, CPS 234 places specific expectations on information security controls, monitoring and response. The assessment can highlight gaps in areas such as access management, audit logging and incident detection. These findings can then be tied back to CPS 234 requirements to support internal assurance and board-level reporting.

NIST Cybersecurity Framework (CSF)

This globally recognised model allows organisations to measure and communicate their posture across five key areas: Identify, Protect, Detect, Respond and Recover. Our assessment identifies how your Microsoft 365 settings align to these functions. This is especially helpful for CISOs and risk teams who use NIST as a foundation for enterprise-wide security governance.

CIS Microsoft 365 Benchmark and Critical Controls

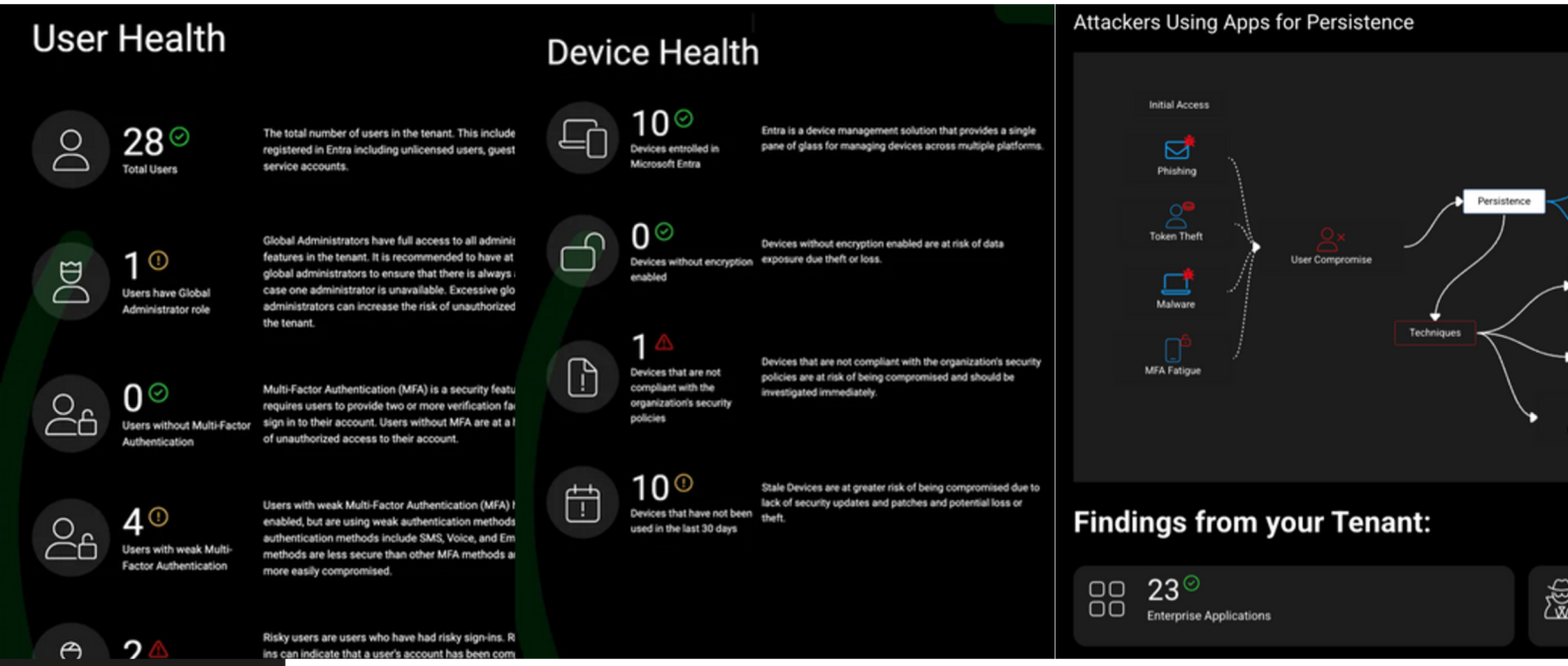
The assessment can compare your configuration against the CIS Microsoft 365 Foundations Benchmark and Critical Controls, identifying which recommendations are in place, partially implemented or absent. This helps create a remediation plan grounded in proven best practice, with actionable steps that your internal teams can follow or use to track improvement over time.

Other frameworks as required

Where necessary, findings can also be mapped to ISO 27001, GDPR, HIPAA or FINRA, depending on your obligations. Affinity Data ensures the assessment output can be used not only to fix technical issues, but also to support internal audits, compliance programs and regulatory engagement.

By interpreting technical risks through a regulatory lens, the assessment provides a clear bridge between IT operations and business accountability. It ensures that your Microsoft 365 posture can be communicated confidently to executive stakeholders, auditors and regulators alike.

Business value and strategic ROI



PREVENT BREACHES

The Microsoft 365 risk assessment is more than a technical health check. It creates tangible business value by reducing risk, strengthening compliance and improving the effectiveness of existing investments.

Improved security posture

By identifying misconfigurations that are often overlooked, such as inactive privileged accounts or legacy authentication, the assessment helps prevent breaches before they occur. These are low-effort, high-impact changes that significantly reduce exposure. In most cases, recommended improvements can be implemented quickly using features your organisation already has.

Greater compliance assurance

For regulated entities, the assessment provides a defensible, framework-aligned record of due diligence. It helps demonstrate to internal and external stakeholders that known risks are being addressed and that Microsoft 365 is being configured in line with current obligations. This can also support a more confident engagement with audits, risk committees and industry regulators.

Better use of licensing and entitlements

Organisations often purchase Microsoft 365 E5 or related add-ons without fully using the capabilities included. The assessment highlights opportunities to reallocate, consolidate or activate existing features rather than procuring additional solutions. It also identifies where licensing may be misaligned with user roles or requirements, providing a pathway to improve efficiency without cutting corners.

Foundation for strategic governance

Perhaps the most important benefit is clarity. The assessment creates a shared understanding of the current state, so that governance decisions are based on facts rather than assumptions. It becomes a catalyst for prioritisation and planning, informing a roadmap for secure collaboration, retention, protection and compliance across Microsoft 365.

Momentum and early wins

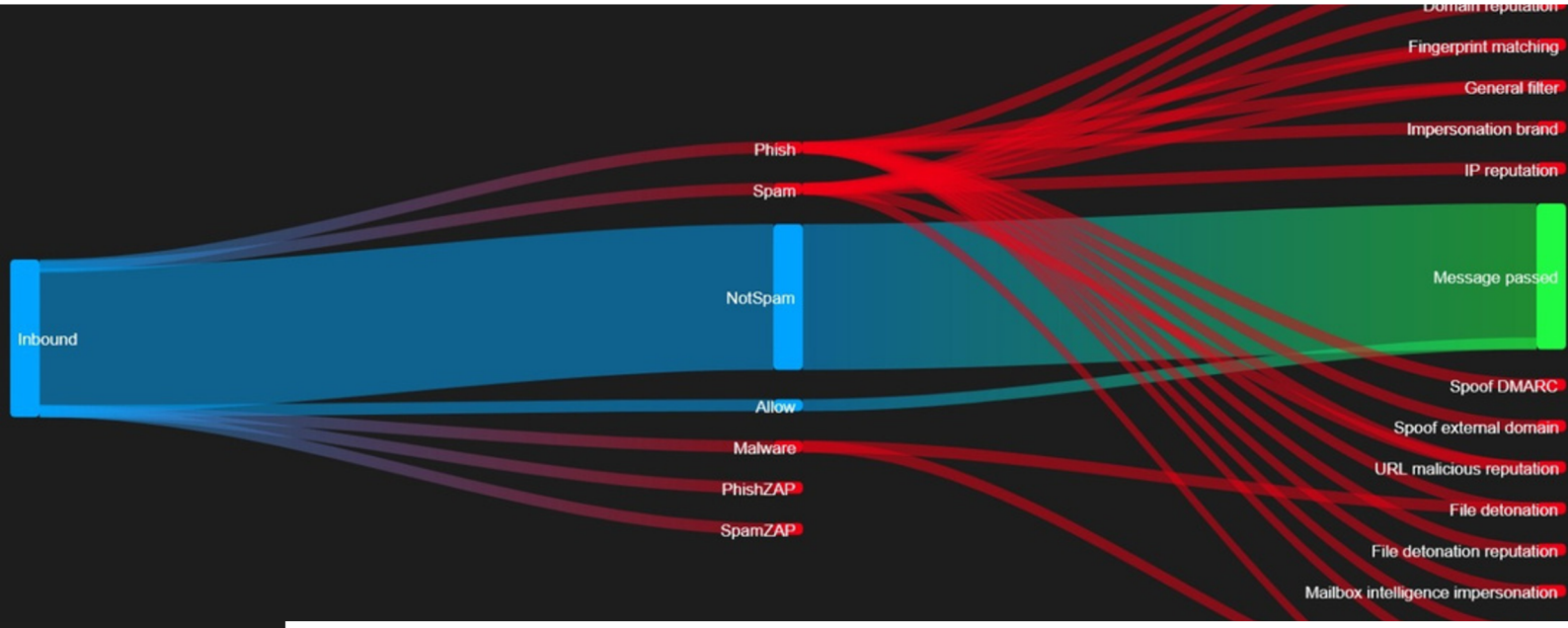
Many organisations face resistance when trying to implement change across cloud platforms. By starting with an assessment, you create a focused improvement program with visible outcomes. Quick wins build internal momentum, while longer-term initiatives can be sequenced logically. This prevents change fatigue and allows governance programs to gain traction across the business.

Support beyond the assessment

Affinity Data works closely with clients throughout the journey. For many, the assessment is just the beginning. Where gaps are identified - especially those involving Microsoft Purview — we can assist with planning, solution design and implementation. Our experience across government, education and regulated sectors ensures that solutions are not only compliant, but practical and sustainable in real-world environments.

In short, the value of the assessment lies in making the invisible visible. It brings structure to an otherwise complex and sprawling environment, allowing your team to move forward with purpose and confidence - with Affinity Data available to assist every step of the way.

Case insights: what real-world assessments uncover



CRITICAL ISSUES

A mid-sized financial services organisation engaged Affinity Data to assess its Microsoft 365 environment. The business had transitioned rapidly to cloud platforms during the pandemic, but lacked a unified governance strategy. Microsoft Purview licensing had been purchased, but little had been implemented beyond default settings.

The assessment revealed several critical issues:

- Multi-factor authentication was applied to administrators but not to regular users, leaving the majority of accounts exposed to credential-based attacks
- Over a dozen global administrator accounts existed, many of which were no longer in active use
- Numerous external users retained access to Teams and SharePoint content from projects that had concluded months earlier
- Retention policies were inconsistent, with some mailboxes kept indefinitely and others relying on user deletion

PRIORITISE REMEDIATION ACTIONS

What made the assessment valuable was not just the visibility it provided, but the clarity of the next steps. Affinity Data worked with the client to prioritise remediation actions, align controls to their APRA CPS 234 obligations, and design a phased roadmap for rolling out Microsoft Purview capabilities.

Within the first 60 days, the organisation enforced MFA for all users, reduced privileged access by more than half, and introduced baseline retention policies across Exchange and SharePoint. By the following quarter, they had deployed sensitivity labels and initiated a program of external sharing reviews.

These changes were not only aligned to compliance expectations - they also improved operational control, reduced cost by reclaiming unused licences, and created the confidence needed to expand their use of Microsoft Purview.

This case reflects a common pattern. The environment was not broken, but without a structured review, key risks remained hidden. By starting with a targeted assessment, the organisation gained clarity, built momentum and made real progress on governance in just a few months.

Affinity Data continues to support this client through ongoing strategy and implementation work, ensuring their Microsoft 365 and Purview investment delivers long-term value.

Recommendations and next steps

OUTCOMES

The Microsoft 365 risk and configuration assessment lays the foundation for stronger governance, security and compliance. But its real value comes from what happens next. Based on our experience across government, education and regulated sectors, Affinity Data recommends a structured approach to translating assessment findings into outcomes:

1. Prioritise and act on quick wins

Most assessments reveal critical issues that can be resolved with minimal effort. Enforcing MFA, disabling legacy authentication, reducing privileged roles and cleaning up dormant accounts are changes that deliver immediate risk reduction without requiring new investment.

2. Align with business and compliance priorities

Use the assessment report to engage internal stakeholders. Mapping risks to frameworks like the Essential Eight or CPS 234 gives security and compliance teams

the leverage they need to secure buy-in and resourcing. Framing governance improvements as business enablers also helps shift perceptions from compliance overhead to operational necessity.

3. Plan your Microsoft Purview rollout

The most effective deployments of Purview are those informed by current-state analysis. Rather than switching on labels or policies in isolation, use the assessment to guide where to start, which features to deploy, and how to avoid friction. Whether your focus is on information protection, records management, or insider risk, a targeted plan will improve adoption and reduce unintended consequences.

4. Build internal capability, but don't go it alone

While some organisations are equipped to remediate and configure in-house, many benefit from expert support — particularly when it comes to Purview. Affinity Data helps teams bridge the gap between intent and execution. Whether you need assistance with strategy, deployment or stakeholder engagement, we can provide the experience and clarity to move quickly and with confidence.

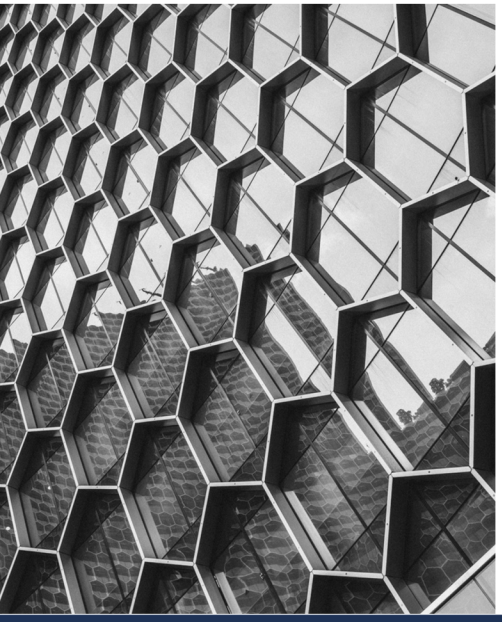
5. Establish governance as an ongoing discipline

Governance is not a one-off project. Policies must evolve as risks shift, user behaviours change and regulations are updated. Use the assessment as the basis for a governance review cycle. Many clients choose to revisit key findings every 6 to 12 months as part of their ongoing cloud risk management.

A well-executed assessment brings visibility, direction and alignment. But it also opens the door to broader improvements that can transform Microsoft 365 from a compliance challenge into a secure, well-governed platform that supports long-term organisational objectives.

Affinity Data is here to help you take the next step - whether that's building a roadmap, enabling Microsoft Purview, or delivering the changes that will keep your environment secure, compliant and future-ready.

Affinity Data



We specialise in governance, security and compliance for Microsoft 365 and Microsoft Purview. Our work is grounded in real-world experience across Australian government, education and regulated industries, and informed by both policy expertise and technical depth.

We don’t just deliver findings. We help you understand what they mean, what to do next, and how to move forward with confidence.

Whether you’re building a roadmap or validating your current state, the Affinity Data Microsoft 365 Configuration and Risk Assessment is the best place to start.

Contact us at info@affinitydata.com.au to request a sample report, book a discovery call or schedule your assessment.