EINPRESSWIRE

TECHOM Systems launches IT Audit & Health Check with AI-driven threat intelligence to secure businesses and cut IT costs

□□□□□□ □□□□□□□ □□ □□□□□ □□□□□ □□□□□□□□□□ □□□□□□□□□□ □□□□□□□□ □□□□□, □□□□□□ □□ □□□□□, □□□ □□□□ □□□□□□□□ □□□ □□□□□□, □□□□□□□□□ □□□□□□ □□□□ □□ □□□□□□□□

TECHOM Systems launches IT Audit & Health Check with AI-driven threat intelligence to secure businesses and cut IT costs

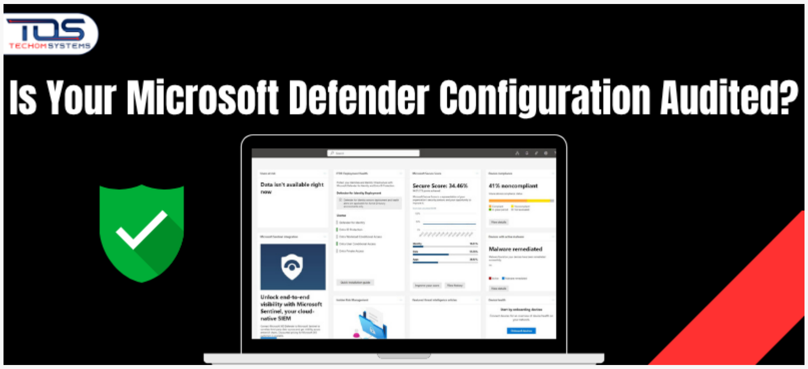
Microsoft 365 Admin Center Audit

MELBOURNE, VICTORIA, AUSTRALIA, June 5, 2025 /EINPresswire.com/ -- □□ □□□□□□□’□ □□□□□□□□□□□□□□□□ □□□□□□□□□□□- □□□□□□□ □□□□□□□□□□ Australian businesses rely on technology more than ever before. Yet behind the scenes many companies bleed money each year on unused software overlapping subscriptions and □□□□□□□□□□□□□□□□ □□ □□□□□□□□□□□□□. At the same time, they remain exposed to costly cyber threats fuelled by □□-□□□□□□□□□ □□□□□□□□□□ and □□□□□□□□□□□ □□□□□□ □□□□□□□□□□□□□□□□□□□□□□. According to the □□□□□□□□□□□□□□ □□□□□□□ □□□□□□□□□□□ □□□□□□□□□ (□□□□□□) a cyber incident is reported roughly every six minutes, but most business owners lack clarity on whether their systems are protected properly backed up or compliant with evolving regulations.

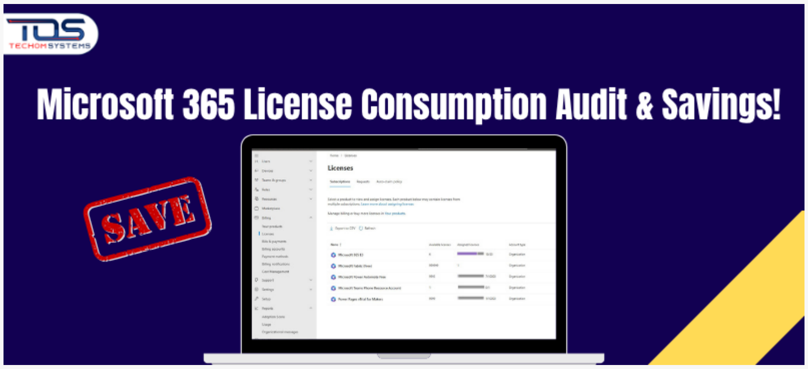
Imagine discovering only after a breach that you had never enabled multi-factor authentication for critical accounts that backups had not run correctly for weeks or that your monthly □□□□□□□□□□□□ □□□□ □□□□□□□□□ included licenses for former employees. These invisible risks and expenses can cripple growth damage reputations and erode customer confidence. Business leaders juggling limited resources often have little time to dig into their own IT environment and answer questions such as “□□□ □□ □□□□□□□□ □□□□ □□□□□□ □□□□□□□□ □□□□□? □□ □□□□ □□□□□□□ □□□□□

□□□□□□□ □□□□□□? □□□□ □□ □□□□□□□
□□ □□ □□-□□□□□□□ □□□□□□□□ □□□□□□
□□ □□□□□□□□□□ □□□□ □□□□□□□□□?”

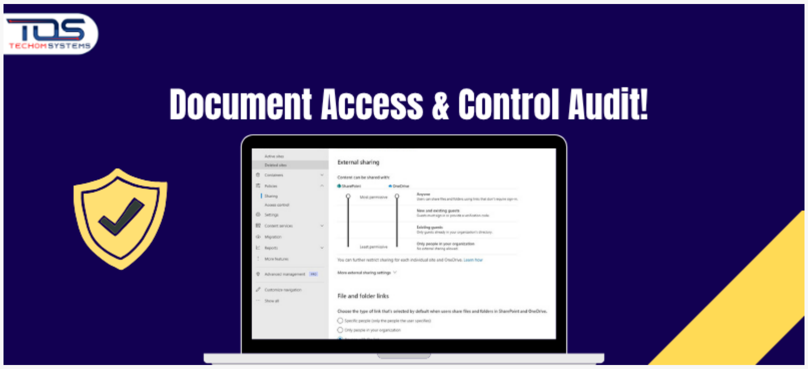
□□□□□□ □□□□□□□ recognized these challenges and has launched a comprehensive IT Audit and Health Check service designed specifically for Australian organisations—especially small to medium-sized businesses and mid-market firms. By combining deep AI-enhanced cybersecurity analysis with a thorough review of software licensing backup reliability and compliance readiness □□□□□□ □□□□□□ □ □□□□□ □□□□□□□□□□ □□□□□□□ to strengthen security reduce waste and prepare for scalable growth. Whether it’s a boutique law firm in Sydney a family-run medical clinic in Brisbane or a fast-growing e-commerce retailer in Melbourne companies can finally gain the transparency they need to manage both risk and cost.



Microsoft Defender Configuration Audit



Microsoft 365 Licence Consumption Audit & Savings



Document Access & Control Audit

With economic pressures mounting and □□□□□ □□□□□□□ □□□□□□□□ daily especially in the Web3 space the time to act is now. This service removes the guesswork and gives business owners the confidence to know exactly where their IT stands so they can sleep easier focus on growth and avoid expensive surprises down the track.

□□□ □□□□□□□□□□ □□□□□□□ □□□□□□□□□□□ □□□□□□□□□□□
Today’s Australian businesses face a perfect storm of technology-related challenges. On one front cybercriminal are becoming more sophisticated launching □□-□□□□□□□ □□□□□□□□□ □□□□□□□□□□□ and data-theft campaigns that target companies of all sizes. The □□□□ reported more than 94,000 cybercrime incidents in the last year with half of those involving medium-sized enterprises. On the other front the explosion of cloud services Web3 platforms and subscription software has created hidden pockets of wasted spending: □□□□□□ □□□□□□□□□ □□□ □□□□□□□□ overlapping backup tools and outdated antivirus platforms that remain on the monthly invoice long after they’re needed.

For many business owners the □□ □□□□□□□□□□ □□□□□ □□□□□□□□□□□□. Someone signs up for a new AI-driven collaboration tool here an ex-employee’s license remains active there and a shiny new Web3-enabled SaaS app is adopted without evaluating whether it overlaps existing tools. These subscription-bloat issues quietly □□□□□ □□□□□□□□□□□ □□□□□□□. Meanwhile outdated or misconfigured security settings weak passwords missing multi-factor authentication unpatched devices and exposure to smart contract risks in Web3 environments leave organizations vulnerable to a breach that can cost anywhere from tens of thousands to millions of dollars in downtime remediation and reputational damage.

A handful of all-too-common scenarios illustrates this gap:
□□• A medium-sized retail chain pays for dozens of Microsoft 365 accounts that staff no longer use costing more than $10,000 per year
□□• A professional services firm discovers its backup system hasn’t run successfully in six weeks only after suffering a hard drive failure
□□• A regional healthcare clinic never enabled multi-factor authentication for its patient-records portal exposing sensitive data to credential-harvesting attacks in a new AI-powered campaign

These problems overlooked because they’re invisible to day-to-day operations—eventually surface as lost revenue angry customers and compliance fines. Australian regulations such as the Privacy Act 1988 and expected alignment with ISO 27001 and ACSC Essential Eight increasingly require formal documentation of cybersecurity controls. Yet most organisations lack the resources or expertise to perform a full IT assessment leaving them at risk.

□□□□□□□□□□□ □□□□□□’□ □□ □□□□□ & □□□□□□ □□□□□
□□□□□□ □□□□□□□ an Australian-owned IT consultancy headquartered in Melbourne has designed its new □□ □□□□□ □□□ □□□□□□ □□□□□ □□□□□□□ to address these exact pain points. With certified □□□□□□□□□□□□□□ □□□□□□□□, □□□□□□□□□□ □□□ □□□□□□□□□□□□ and □□ □□□□□□□ on staff TECHOM combines hands-on analysis with □□□□□□□□□□ □□□□□□□□□□□□□ to deliver a complete picture of an organisation’s IT posture. The service promises three core outcomes:

□□□□□□□—A clear easily understandable report on security vulnerabilities including AI-driven threat simulations backup readiness software license usage and compliance gaps
□□□□□□□—Identification of unnecessary subscriptions overlapping tools and underutilized cloud or Web3 services that can be eliminated often reducing IT costs by up to 40 percent
□□□□□□□□□□—A prioritized actionable roadmap that allows business owners and IT managers to implement improvements on day one without expensive guesswork

This all-in-one approach ensures that companies do not have to juggle separate security audits software license reviews or compliance checklists. Instead, they receive a unified assessment tailored to their size industry and budget that not only uncovers risks but also guides them to immediate measurable improvements.

[illegible]

TECHOM’s IT Audit and Health Check comprises eight interlocking components each addressing a critical aspect of an organisation’s digital environment:

[illegible]

• What’s Covered: Firewall configurations antivirus/endpoint protection status multi-factor authentication password policies privileged account access AI-powered penetration testing and potential external attack surfaces (open ports remote desktop)

• Why It Matters: Unpatched firewalls or missing multi-factor authentication can provide attackers a path to pivot internally leading to ransomware or data theft

[illegible] & [illegible]

• What’s Covered: Active versus inactive accounts license tiers mismatched to user needs overlapping third-party add-ons redundant subscription services and underutilized Web3-enabled collaboration tools

• Why It Matters: Businesses can save thousands per year by right-sizing license types consolidating Web3 platforms and removing seats no longer in use

[illegible] & [illegible]

• What’s Covered: Verification of backup schedules storage locations (on-site versus cloud) integrity tests (restore simulations) and overall Recovery Time Objectives (RTO) Recovery Point Objectives (RPO)

• Why It Matters: A backup that has not been tested or is misconfigured can result in data loss costly downtime and regulatory non-compliance

[illegible] & [illegible]

• What’s Covered: Laptops desktops tablets and smartphones—ensuring each device has up-to-date operating systems antivirus disk encryption Mobile Device Management policies and secured endpoints for AI-powered tools

• Why It Matters: An unpatched device or lack of wipe/lock controls on lost smartphones can expose the entire network to breaches

[illegible] & [illegible]

• What’s Covered: Review of SharePoint OneDrive Dropbox Google Drive and other cloud platforms for permission sprawl stale or external sharing links unmanaged guest access and potential Web3 file transfer vulnerabilities

• Why It Matters: Inadvertent public sharing or stale guest links can expose confidential documents to unintended audiences violating privacy regulations

[illegible] & [illegible]

• What’s Covered: Firewall rule audits VLAN segmentation checks VPN configurations secure Wi-Fi settings router firmware updates and assessments of Web3 node or API endpoint security

• Why It Matters: Misconfigured routers or overly permissive firewall rules can give attackers a path to pivot internally once they breach the perimeter

□□□□□□□□□□ □□□ □□□□□□□□□

• What’s Covered: Mapping current practices against ACSC Essential Eight ISO 27001 requirements Privacy Act 1988 obligations and any industry-specific regulations (healthcare legal education) with AI-driven compliance checks
• Why It Matters: Many industries require formal evidence of controls. A compliance gap can mean failed audits insurance denials or hefty fines

□□□□□□□□□□□ □□□□□□□□ & □□□□□□□□□□

• What’s Covered: A plain-English visual report that uses a traffic-light system (red/yellow/green) to highlight critical medium and low-risk items. The roadmap outlines 30 60 and 90-day priorities cost estimates and recommended AI-and-global best-practice solution partners if required
• Why It Matters: Without an actionable plan audit findings often sit unused. TECHOM ensures each recommendation has context priority and a straightforward path to execution

□□□ □□ □□□□□□□□□ □□□□ □□□□□□□ □□□□□□□

Below are the most common scenarios where TECHOM’s IT Audit and Health Check uncovers hidden issues each of which can have major financial operational or reputational consequences if left unaddressed:

□□□□□□□ □□□□□□:

1. “Paying for Microsoft 365 seats used by ex-employees”
2. “Multiple backup tools costing monthly fees, but none regularly tested”
3. “Overlapping antivirus and endpoint tools that do the same job”
4. “Cloud storage costs keep rising with nobody tracking usage”
5. “Third-party add-ons on our email causing unexpected charges”

□□□□□□□□□ □□□□:

6. “Admin passwords haven’t been changed in over a year”
7. “Employees share the same weak password across multiple services”
8. “Multi-factor authentication is not enforced on critical accounts”
9. “Unpatched laptops on the network expose us to ransomware”
10. “Our firewall has open ports that we don’t actually need”

□□□□□□□□□□□ □□□□□ □□□□□:

11. “No documentation of how we meet the ACSC Essential Eight”
12. “Last external audit flagged our lack of formal policies”
13. “Can’t prove where customer or patient data is stored”
14. “Concerned about Privacy Act 1988 violations but no roadmap”
15. “Insurance renewal is due, but we lack the security evidence required”

□□□□□□□□□□□□ □□□□□□□□□□□□□□□□:

16. “Systems run slow, but we can’t pinpoint the cause”
17. “Half the staff use personal cloud accounts for file sharing”
18. “Don’t know which devices are connected at any given time”
19. “Email system is a patchwork of legacy and cloud solutions”
20. “Integration between critical apps is a nightmare”

□□□□□□□ □□□□□□□□□:
21. “Doubled in size but IT never scaled with us”
22. “Internal IT person left and we have no documentation”
23. “Want to expand interstate but need a stable IT foundation”
24. “Considering ISO 27001 certification but don’t know where to start”
25. “Need to onboard new staff quickly but can’t guarantee a secure device setup”

□□□□□ □□ □□□□ □□□□□:
26. “Experienced a minor breach last year and want to ensure it never happens again”
27. “Tired of firefighting IT problems and want a proactive approach”
28. “Board is pressing for visibility on tech risk, but we lack data”
29. “Want to compete for government contracts requiring formal audits”
30. “Need confidence that IT can support future growth without surprises”

□□□□□□□□□-□□□□□□□□ □□□□□□□□ □□□□□□ □□□□ □□ □□□□□ □□□□□□□

□□□□□□□□□□ & □□□□□□□ □□□□□□□
Clinics practices and allied health providers handle highly sensitive patient data. TECHOM’s audit ensures electronic medical records are encrypted backups are verified and user access is tightly controlled. By aligning with Privacy Act 1988 requirements and hospital-grade standards and assessing AI-powered telehealth tools practices avoid potential fines and protect patient trust.

□□□□□ & □□□□□□□□□ □□□□□□□□
Law firms and accounting practices require airtight confidentiality and audit trails. TECHOM’s service verifies that emails and document shares follow strict permission-based models ensures encryption for client files and confirms that billing and compliance workflows match industry regulations. This readiness can be a decisive factor during external audits or insurance renewals.

□□□□□□□□□□□□ & □□□□□□
Project managers contractors and tradespeople often use shared jobsite devices and cloud storage for blueprints invoicing and scheduling. TECHOM identifies whether these devices have proper endpoint protection ensures secure Wi-Fi on sites and prevents accidental exposure of project plans. A reliable backup strategy means no lost documents even if a laptop is stolen.

□□□□□□□□□ & □□□-□□□-□□□□□□□
Schools training centres and charities typically operate with tight budgets and shared resources.

TECHOM finds and eliminates redundant software subscriptions secures student or donor data in the cloud and provides an easy-to-understand compliance roadmap. Buffering against student data breaches and maintaining grant-mandated security levels are key benefits.

□□□□□□□ & □-□□□□□□□□□

Point-of-sale systems inventory management platforms and customer databases are prime targets for hackers. TECHOM’s audit verifies that POS terminals are segmented cardholder data is encrypted and cloud-based sales tools aren’t exposing customer information. Identifying hidden subscription fees for e-commerce plugins third-party analytics and assessing Web3 payment integrations also reduces monthly overhead.

□□□ □□□□□□□ □□□□□□□□ □□ □□□□□□□

TECHOM Systems stands apart because it combines deep local expertise with global best practices:

□□□□□□□□□□-□□□□□□ □□□□□□□□□□ □□□□: All consultants operate from Melbourne Sydney Canberra Brisbane Perth and Adelaide ensuring rapid response and an understanding of local regulations

□□□ □□□□□□ & □□□ □□□□□ □□□□□□□□□□□: Rigorous internal processes guarantee consistent quality security and confidentiality for every audit

□□□□□□□-□□□□□□□□ □□□□□□□: TECHOM does not sell hardware or push specific software recommendations focus purely on business needs without commissions

□□□□□□□□□□□□ □□□□□□ □□□□ □□□□□□□□: Organisations know the exact cost up front without hidden fees

□□□□□□□-□□□□□□□□ □□□□□□□□□□: Every finding includes context priority level and a clear next step so audit findings drive real improvements rather than just more documentation

Consulting firms often provide a dry list of vulnerabilities, but TECHOM delivers a practical prioritized roadmap that empowers organisations to act immediately.

□□□ □□□□ □□ □□□□□□ □□□□ □□□□□□□□□□□□ □□□□□□

□□□□□□□□□□ □□□□□□□□: A consultation (on-site or remote) identifies business objectives reviews preliminary documentation and outlines key concerns
□□□□□ □□□□□□□□□□: With permission TECHOM performs remote scans of server’s endpoints and cloud environments collects billing records and interviews key staff to clarify usage patterns
□□□□□□□□□ & □□□□□□□□□□□□□□: The team analyses scan results manually review configurations tests backup restores and investigates account permissions. Any critical vulnerabilities are flagged immediately
□□□□□□□ & □□□□□-□□□□□□□□: Within two weeks a detailed plain-English report highlights security

risks subscription waste compliance gaps and device health. A walkthrough meeting (remote or on-site) explains findings and answers questions
□□□□□□□□□□□□ □□□□□□□□: The final deliverable is a 30/60 and 90-day plan prioritizing fixes by risk level and cost complete with recommendations for technology improvements or partner selection if needed

□□ □□□□□□□□□□ □□□□□□□□ □□□□□□□□□□□□ □ □□□□□□ □□□□□ □□ □□□□□□□□□ □□□□□□□□□□ □□□□ □□□□□□□ □□ □□□□□□.

□□□□□□□□□□□□ □□□□□□ & □□□□□□□□□□□□□
“Too many Australian businesses operate in the dark when it comes to their IT” says □□□□□□ □□□□□□□, □□□□□□□□□ □□□□□□□ □□□□□□□□. “Our new [□□ □□□□□□ and □□□□□□□ □□□□□□]() service changes that is turning uncertainty into clarity. Whether fixing a vulnerable backup eliminating redundant subscriptions or □□□□□□□□□ □□□□□□□□□□□□ with the latest standards we provide business owners with the insight needed to make confident cost-effective decisions. □□ □□□□□ □□□□ □□□□□□□ □□□□□□□□□□□ □□ □□□□□□□□□□□□ □□□□□ □□□□ □□ □□□□□□□□□□ □□ □□□□□ □□ □□□□□□□□□□□.”

□□□□□ □□ □□ □□ □□□□ □□□□□□□□□□□□□?
Organisations interested in □□□□□□□□□□□□□□□ their □□□□□□□□□□□□□□□ □□□□□□□□ and eliminating □□□□□□□ □□ □□□□□□ are invited to arrange a □□□□□□□□□□□□□□□ □□□□□□□□□□□ □□□l with □□□□□□□ □□□□□□□□.
For more information or to schedule a Discovery Call:
• □□□□□□: □□□□□□://□□□.□□□□□□□□□□□□□□□.□□□□.□□/□□-□□□□□□-□□□□□□□□□□□-□□□□□□□□□
• □□□□□□: □□□□□□□@□□□□□□□□□□□□□□□.□□□□.□□
• □□□□□: □□□□□ □□□□ □□□□
Availability for these complimentary consultations is limited so interested parties are encouraged to book promptly to secure a preferred time slot.

Pradeep Singh
TECHOM SYSTEMS
+61 1800 867 669
hello@techomsystems.com.au
Visit us on social media:
LinkedIn
Instagram
Facebook
YouTube
X

This press release can be viewed online at: https://www.einpresswire.com/article/819291159