Need to Know Microsoft 365 Webinar February 2026

@directorcia

http://about.me/ciaops

Web cast has started

Web cast is being recorded. Note recording may be made public

If you can’t hear anything check your speaker settings

For questions after the event:

Email : director@ciaops.com

X : @directorcia

https://directorcia.gumroad.com/

directorcia

Your email address

Subscribe

CIAOPS

Copilot

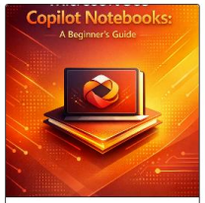
1-6 of 6 products

Sort by

Tags

Contains

Price

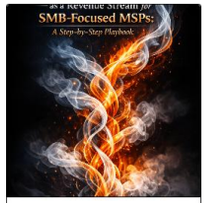


Introduction to Copilot Notebooks

A$9+

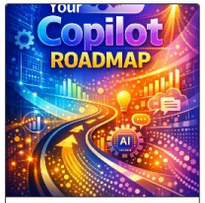
MSP AI Playbooks

A$18+



AI as a Revenue Stream for MSPs

A$9+



Your Copilot Roadmap

A$9+

How to Effectively Use Microsoft 365 Copilot

A$9+

Copilot Readiness Assessent

A$9+

ecurity

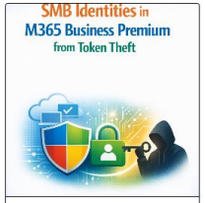
1-6 of 6 products

Sort by

Tags

Contains

Price

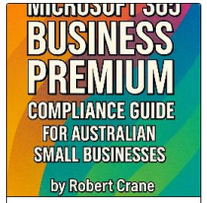


Protecting SMB Identities in M365 Business Premium from Token Theft

A$9+

Cybersecurity Verification Playbook

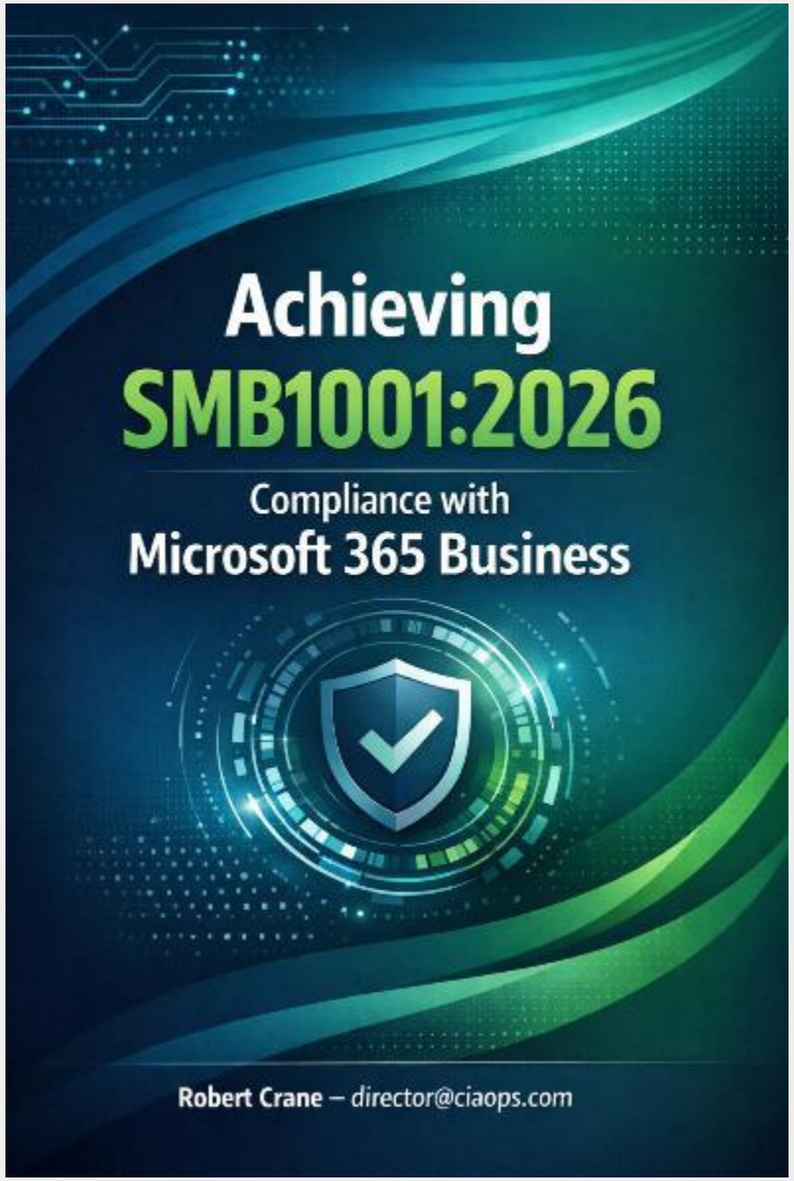
A$9+



Microsoft 365 Business Premium Compliance Guide

A$9+

https://directorcia.gumroad.com/l/smb10012006



https://blog.ciaops.com/2022/07/29/join-my-teams-shared-channel/

Join my free shared Channel

Agenda

-Microsoft 365 Update
-Baseline Security Mode
-Q & A


Microsoft 365 Update

News

- Running OpenClaw safely: identity, isolation, and runtime risk
  - https://www.microsoft.com/en-us/security/blog/2026/02/19/running-openclaw-safely-identity-isolation-runtime-risk/
- Introducing Security Dashboard for AI (Now in Public Preview)
  - https://techcommunity.microsoft.com/blog/microsoft-security-blog/introducing-security-dashboard-for-ai-now-in-public-preview/4494637
- Your Data, Your Choices: Understanding Microsoft's Privacy Commitments
  - https://techcommunity.microsoft.com/blog/microsoft365insiderblog/your-data-your-choices-understanding-microsoft%E2%80%99s-privacy-commitments/4489814
- Microsoft Entra Agent ID explained
  - https://www.youtube.com/watch?v=N-B-kD28P2I
- What's New in Microsoft Intune – January 2026
  - https://techcommunity.microsoft.com/blog/microsoftintuneblog/whats-new-in-microsoft-intune-%E2%80%93-january-2026/4476487
- From runtime risk to real-time defense: Securing AI agents - https://www.microsoft.com/en-us/security/blog/2026/01/23/runtime-risk-realtime-defense-securing-ai-agents/

Baseline Security Mode

In a nutshell

- Additional tenant security options
- Initial options available but will grow
- Appear in admin not security console
- Audit (report) mode available
- No automation options available yet

Setting	Purpose / Effect
Phishing-resistant MFA for admins (Auth)	Enforce strong MFA for all admin accounts, blocking phishing-based compromises of privileged roles.
Block legacy authentication flows (Auth)	Disable outdated auth protocols (POP, IMAP, etc.) that can't enforce MFA, closing common brute-force entry points.
Block basic auth prompts (Auth)	Remove basic username/password login prompts to prevent credential capture via insecure dialogs.
No new password creds for apps (Auth)	Stop adding password-based credentials to Azure AD apps, forcing more secure auth methods (certs, tokens).
Restrict user app consent (Auth)	Users can only consent to apps from your tenant or Microsoft-certified apps, avoiding untrusted applications.
Block basic authentication (Auth)	Fully turn off Basic Auth in Exchange/Office apps, so all clients must use modern auth (prevents legacy login use).
Block insecure file protocols (Auth)	Prevent opening files over insecure links (HTTP/FTP), mitigating man-in-the-middle data theft risks.
Block FrontPage RPC (Auth)	Disable the obsolete FrontPage RPC protocol, removing an outdated vector for remote code execution.
Block SP/OD legacy auth (RPS) (Auth)	Block legacy browser authentication to SharePoint/OneDrive (RPS), forcing modern auth and logging any RPS usage.
Block SP/OD legacy auth (IDCRL) (Auth)	Block legacy client authentication to SharePoint (IDCRL library), ensuring only modern clients connect (with usage reporting).
No new custom scripts in SharePoint (Auth)	Prevent the addition of custom scripts on SharePoint/OneDrive sites, stop ungoverned code, and enhance governance.
Disable SharePoint Store (Auth)	Block end-user access to the SharePoint app store, so apps can't be self-installed without admin oversight.
Disable EWS access org-wide (Auth)	Turn off Exchange Web Services for the org, closing a loophole to mailbox data often exploited by attackers.
Legacy files read-only PV (Files)	Very old Office files only open in Protected View with editing disabled, preventing exploits from ancient formats.

Legacy files in PV + edit (Files)	Old Office files open in Protected View by default (user can enable editing), reducing risk while allowing work.
Block ActiveX in Office (Files)	Prevent any ActiveX controls from running Office documents, blocking a frequent malware mechanism.
Block OLE Graph/OrgChart (Files)	Block legacy OLE Graph and OrgChart embedded objects in Office files, shutting down known exploit techniques.
Block Excel DDE launches (Files)	Stop Excel from using DDE to launch external programs, which protects against a code injection phishing trick.
Block Publisher app (Files)	Prevent Microsoft Publisher from launching, removing a high-risk app (being retired in 2026) from the environment.
No Files access on Teams Rooms (Devices)	Prevent Teams Rooms resource accounts from accessing M365 files, so meeting room devices can't retrieve files.
Only allow managed Teams Rooms (Devices)	Only compliant, IT-managed Teams Room devices can sign in; blocks resource account use on unmanaged devices.
Block resource acct sign-in (Devices)	Completely block resource accounts from signing into any M365 client apps outside their intended device scenario.


DEMO

Take aways

- Opt in
- Audit (report) mode available
- Currently 20 settings
- Policy customisation is available
- Not as granular as Intune security baselines
- Beware of just turning everything on

Resources

- Baseline security mode settings - https://learn.microsoft.com/en-us/microsoft-365/baseline-security-mode/baseline-security-mode-settings?view=o365-worldwide
- New Baseline Security Mode for Microsoft 365 - https://lazyadmin.nl/office-365/baseline-security-mode-for-microsoft-365/
- New Baseline Security Mode in Microsoft 365 Admin Center - https://blog.admindroid.com/baseline-security-mode-in-microsoft-365-admin-center/
- Microsoft Baseline Security Mode: Secure-by-Default for Your Microsoft 365 Tenant - https://www.linkedin.com/pulse/microsoft-baseline-security-mode-securebydefault-your-david-qiibe/
- Ignite'25 Spotlight: Announcing Microsoft Baseline security mode - https://techcommunity.microsoft.com/blog/microsoft_365blog/ignite%E2%80%9925-spotlight-announcing-microsoft-baseline-security-mode/4469709

CIAOPS Resources

- Blog – http://blog.ciaops.com
- Free Office 365, Azure video tutorials – http://www.youtube.com/directorciaops
- Free documents, presentations, etc – https://github.com/directorcia/general/
- Office 365, Azure, Cloud podcast – http://ciaops.podbean.com
- Office 365 and Azure community – http://www.ciaopspatron.com
- Github – https://github.com/directorcia
- Email list – https://bit.ly/cia-email
- Publications – https://directorcia.gumroad.com/

Twitter @directorcia

Facebook https://www.facebook.com/ciaops

Email director@ciaops.com

Teams admin@ciaops365.com

Get access to the latest information by becoming a Patron

http://www.ciaopspatron.com


Questions

That’s all folks!

Thanks for attending