

INDEPENDENT EDUCATIONAL FIELD GUIDE

Your readiness checklist.

A conversation with your team, not a tenant assessment. Mark confirmed facts; leave unknowns open. No production changes are implied.

- ☐ **01** Record the exact license SKU, cloud and tenant rollout status.
- ☐ **02** Check which endpoint, identity, email and cloud app protections are deployed.
- ☐ **03** Confirm ISOC preview eligibility; keep existing Sentinel workspaces and production protections connected.
- ☐ **04** Select the external sources and events the investigation actually needs.
- ☐ **05** Verify workspace, connector, source permissions and data retention requirements.
- ☐ **06** Separate native data access, ingestion, storage, compute and agent capacity.
- ☐ **07** Confirm action ownership, permissions and how results will be checked.
- ☐ **08** Verify current public documentation and tenant availability before changing production.

Purview signals into ISOC

- ☐ **09 Data security** Data loss alerts reach the Defender incident queue with E5 level rights, once an admin turns off the built-in rule that keeps them out.
[Data loss alerts in Defender](#)
- ☐ **10 Insider risk** Insider Risk alerts in Defender are prerelease and need the data sharing setting.
[Insider Risk alerts in Defender](#)
- ☐ **11 Audit log** Audit evidence arrives through an ISOC workspace connector.
[ISOC data and billing](#)

Owner / next check

Public sources

[Microsoft 365 E3, E5 and E7 licensing overview](#)

<https://learn.microsoft.com/en-us/microsoft-365/copilot/microsoft-365-copilot-license-feature-overview>

[ISOC preview eligibility and workspace requirements](#)

<https://learn.microsoft.com/en-us/defender-xdr/isoc-overview>

[Connect Microsoft Sentinel to Microsoft Defender](#)

<https://learn.microsoft.com/en-us/azure/sentinel/microsoft-sentinel-onboard>

[Security Copilot capacity and compute units](#)

<https://learn.microsoft.com/en-us/copilot/security/security-compute-units-capacity>