New-MSP 90-day onboarding checklist

Free from CIO Support (cio.support). No form or sign-up. Version 2026-11-10.

How to use it

The checklist (the Checklist tab in Excel; the pages after this one in the PDF) has one row for each onboarding step and each piece of checkpoint evidence on the CIO Support page it accompanies. Work through it with your new managed IT provider. For each row, fill in who owns it (your company, the provider, or both), when it is due, what evidence you received, and whether it is done. These four columns are left blank for you: agree the owners and dates with your provider and, where you can, write them into the contract.

Groups: Days 1 to 30 (take control safely), Days 31 to 60 (close the urgent gaps), Days 61 to 90 (stabilize and plan), Co-managed IT (only if your own IT staff stay on), and the evidence to ask for at the day 30, day 60 and day 90 checkpoints.

Where each row comes from

Every row quotes its source. 'This page' means the CIO Support answer 'What should the first 90 days with a new MSP look like?' (https://cio.support/managed-it/msp-onboarding-first-90-days/), by section heading. Some rows also quote CISA et al. Advisory AA22-131A: Protecting Against Cyber Threats to Managed Service Providers and their Customers (https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-131a), which the page cites. The 'Step or evidence' wording is ours; the quoted text is the source's own.

The page also covers warning signs, what to get from the old provider, questions to ask your new provider and log retention guidance from CISA and its partners. Read it alongside this checklist.

What this checklist does not do

It does not set response times, service levels, prices or deadlines, and the page's phases are a guide, not a contractual timetable. Larger or more complex environments take longer. Compare what a provider offers with what your business needs.

It is general guidance, not legal advice, and it is not published or endorsed by CISA or Microsoft.

About

CIO Support is an executive technology library published by LAN Service Group, Inc., an IT management, cybersecurity, compliance and AI services firm headquartered in San Ramon in the San Francisco Bay Area, serving clients across the United States and in major international cities. LAN Service Group works as a fully outsourced IT department or as a co-managed partner alongside in-house IT staff.

#	Step or evidence	Source (quoted)	Owner	Due	Evidence received	Done
1	**Days 1 to 30** Inventory users, devices, licenses, domains, cloud services and vendor contracts.	This page, 'Days 1 to 30: take control safely': “Inventory users, devices, licenses, domains, cloud services and vendor contracts.”				
2	**Days 1 to 30** Confirm that your company owns the Microsoft 365 tenant, the domain registrar account and key vendor accounts.	This page, 'Days 1 to 30: take control safely': “Confirm you, the customer, own the Microsoft 365 tenant, domain registrar and key vendor accounts.”				
3	**Days 1 to 30** Create two cloud-only emergency access accounts protected by passkeys or certificate-based authentication, and store their credentials safely.	This page, 'Days 1 to 30: take control safely': “Create two cloud-only emergency access accounts protected by passkeys or certificate-based authentication, as Microsoft recommends, and store their credentials safely.”				
4	**Days 1 to 30** Give the new provider least-privilege, time-bound access (for example Microsoft's granular delegated admin privileges, GDAP), not shared Global Admin passwords.	This page, 'Days 1 to 30: take control safely': “Grant the MSP least-privilege, time-bound access, for example through Microsoft's granular delegated admin privileges (GDAP), rather than shared Global Admin passwords.”				
5	**Days 1 to 30** Remove or disable the previous provider's accounts, tools and remote-access agents.	This page, 'Days 1 to 30: take control safely': “Remove or disable the previous provider's accounts, tools and remote-access agents.” AA22-131A: “Customers should be sure to disable MSP accounts that are no longer managing infrastructure. Note: disabling MSP accounts can be overlooked when a contract terminates.”				
6	**Days 1 to 30** Deploy monitoring and endpoint protection, and start the help desk.	This page, 'Days 1 to 30: take control safely': “Deploy monitoring and endpoint protection, and start the help desk.”				
7	**Days 31 to 60** Enforce MFA for every user and every technician account that touches your environment, starting with admins.	This page, 'Days 31 to 60: close the urgent gaps': “Enforce MFA for every user and every technician account that touches your environment, starting with admins.” AA22-131A: “Contracts should also require MFA to be enforced on all MSP accounts used to access customer environments.”				
8	**Days 31 to 60** Verify backups by restoring real data, including Microsoft 365 mailboxes and files.	This page, 'Days 31 to 60: close the urgent gaps': “Verify backups by restoring real data, including Microsoft 365 mailboxes and files.”				
9	**Days 31 to 60** Bring operating systems, firmware and key applications up to a supported, patched state.	This page, 'Days 31 to 60: close the urgent gaps': “Bring operating systems, firmware and key applications up to a supported, patched state.” AA22-131A: “Organizations should update software, including operating systems, applications, and firmware.”				
10	**Days 31 to 60** Turn on logging and alerting, and agree how long logs are kept.	This page, 'Days 31 to 60: close the urgent gaps': “Turn on logging and alerting, and agree how long logs are kept.”				
11	**Days 31 to 60** Get a ranked report of the risks found so far, showing what is fixed and what needs a decision.	This page, 'Days 31 to 60: close the urgent gaps': “Report the risks found so far, ranked, with what is fixed and what needs a decision.”				

#	Step or evidence	Source (quoted)	Owner	Due	Evidence received	Done
12	**Days 61 to 90** Get written documentation: network diagram, asset list, admin-account list, backup scope and recovery steps.	This page, 'Days 61 to 90: stabilize and plan': “Deliver written documentation: network diagram, asset list, admin-account list, backup scope and recovery steps.”				
13	**Days 61 to 90** Agree the incident response plan, including who calls whom and how the provider notifies you.	This page, 'Days 61 to 90: stabilize and plan': “Agree the incident response plan, including who calls whom and how the MSP notifies you.” AA22-131A: “Note: contracts should detail how and when MSPs notify the customer of an incident affecting the customer's environment.”				
14	**Days 61 to 90** Review ticket trends to find recurring problems worth fixing at the root.	This page, 'Days 61 to 90: stabilize and plan': “Review ticket trends to find recurring problems worth fixing at the root.”				
15	**Days 61 to 90** Get a 12-month roadmap and budget covering hardware refresh, licensing, security and projects.	This page, 'Days 61 to 90: stabilize and plan': “Present a 12-month roadmap and budget covering hardware refresh, licensing, security and projects.”				
16	**Days 61 to 90** Hold a 90-day review against the service levels in your contract.	This page, 'Days 61 to 90: stabilize and plan': “Hold a 90-day review against the contract's service levels.”				
17	**Co-managed IT** Write a responsibility matrix between your internal IT staff and the provider covering help desk tiers, patching, security alerts, user changes and projects.	This page, 'If you are moving to co-managed IT': “When internal IT staff remain, onboarding also means drawing the line between teams.” This page, 'If you are moving to co-managed IT': “Write a responsibility matrix covering help desk tiers, patching, security alerts, user changes and projects”				
18	**Co-managed IT** Agree how tickets move between your internal IT staff and the provider.	This page, 'If you are moving to co-managed IT': “and agree how tickets move between you.”				
19	**Co-managed IT** Check that the contract states who owns hardening, detection and incident response.	This page, 'If you are moving to co-managed IT': “CISA's joint advisory on MSP risk emphasizes that contracts should state who owns hardening, detection and incident response, which applies just as much when two teams share the work.” AA22-131A: “their contract specifies whether the MSP or the customer owns specific responsibilities, such as hardening, detection, and incident response.”				
20	**Evidence at day 30** The inventory of users, devices, licenses and contracts.	This page, 'What evidence to ask for at each checkpoint': “Day 30: the inventory of users, devices, licenses and contracts”				
21	**Evidence at day 30** The list of administrator accounts, including your emergency access accounts.	This page, 'What evidence to ask for at each checkpoint': “the list of administrator accounts, including your emergency access accounts”				
22	**Evidence at day 30** Confirmation that the previous provider's access and tools are removed.	This page, 'What evidence to ask for at each checkpoint': “and confirmation that the previous provider's access and tools are removed.”				
23	**Evidence at day 60** An MFA report covering every user and technician account.	This page, 'What evidence to ask for at each checkpoint': “Day 60: an MFA report covering every user and technician account”				

#	Step or evidence	Source (quoted)	Owner	Due	Evidence received	Done
24	**Evidence at day 60** A record of a real restore test.	This page, 'What evidence to ask for at each checkpoint': “a record of a real restore test”				
25	**Evidence at day 60** Patch status, with exceptions.	This page, 'What evidence to ask for at each checkpoint': “patch status with exceptions”				
26	**Evidence at day 60** The agreed log retention settings.	This page, 'What evidence to ask for at each checkpoint': “and the agreed log retention settings.”				
27	**Evidence at day 90** The documentation set.	This page, 'What evidence to ask for at each checkpoint': “Day 90: the documentation set”				
28	**Evidence at day 90** The agreed incident response plan.	This page, 'What evidence to ask for at each checkpoint': “the agreed incident response plan”				
29	**Evidence at day 90** The 12-month roadmap and budget.	This page, 'What evidence to ask for at each checkpoint': “the 12-month roadmap and budget”				
30	**Evidence at day 90** A service-level review against the contract.	This page, 'What evidence to ask for at each checkpoint': “and a service-level review against the contract.”				