

MCP security and compliance review checklist

Review executable code, delegated access, data paths and incident controls before rollout.

Updated October 29, 2026

Treat an MCP server as an access path to tools and data. Local servers can execute code with the process account's permissions. Remote services can receive data and credentials. Review both paths.

Before a pilot

- Confirm the package publisher and repository. Inspect the exact version and licence.
- Use a test account with the smallest useful scope. Keep production secrets out of copied configuration examples.
- List data sent to the server, upstream service, model provider and logs.
- Check how a remote endpoint validates identity and token audience.
- Define who can approve writes and who can revoke access.

The MCP security best-practices document discusses token passthrough, confused-deputy attacks, session handling and server-side request forgery. Read the current guidance for your architecture. Do not assume that using OAuth alone resolves these risks.

Test the boundary

Ask the server to access a resource the test user cannot read. Try an expired credential and a revoked connection. Check that errors do not expose tokens or private payloads. Test suspicious content in a retrieved document. External text must not become an instruction to grant more access.

For remote deployments, inspect endpoint configuration, allowed destinations and redirect handling. For local deployments, review filesystem mounts, network access and inherited credentials. Restrict the execution account. Pin packages and review updates before broad rollout.

Ask for compliance evidence

Request the data-processing agreement, subprocessor list, retention policy and incident-notification terms. If the vendor presents an audit, confirm the audited entity, service scope, reporting period and exceptions. An audit is evidence to review. It is not a guarantee that your workflow is compliant.

Record a release decision

Keep the evidence link, review date, reviewer, unresolved risk and mitigation. Document the steps to disable the connection and rotate affected credentials. Repeat the review when permissions, data types or deployment change. This checklist supports an internal review; it does not certify a vendor or replace legal advice.

Sources

- [MCP specification: Security best practices, revision 2025-06-18](#). Fetched 2026-10-29.
- [MCP specification: Authorization, revision 2025-06-18](#). Fetched 2026-10-29.
- [MCP specification: Transports, revision 2025-06-18](#). Fetched 2026-10-29.

Frequently asked questions

Does OAuth alone prove that a connection is secure?

No. Review identity mapping, token handling, data paths, permissions and revocation. Test the actual boundary.