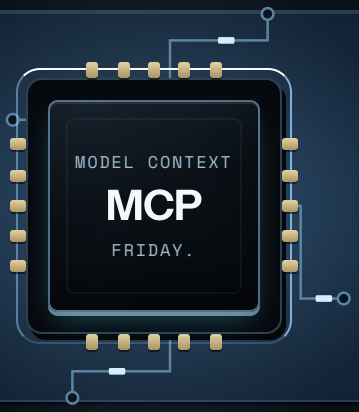
MCP INTEGRATIONS · PDF CHECKLIST

MCP Readiness Checklist

Answer these before you connect an AI assistant to a business tool with the Model Context Protocol. Start with one connection, read-only.

5 SECTIONS · 20 CHECKS · PRINT AND FILL



01 The first connection

6 CHECKS

- **The task:** one question your team asks every week, written in one sentence.
- **The system:** the one tool that holds the answer (CRM, help desk, orders, docs).
- **The access:** you can create an account or token limited to what this task needs.
- **The frequency:** how often it comes up, so you know the connection is worth maintaining.
- **The AI app:** the assistant your team already uses supports MCP connections.
- **The test:** five real questions with known answers to check the results against.

02 Permissions

5 CHECKS

- **Read before write.** Start read-only; add write actions only after the read version works.
- **Each person's permissions.** The AI acts with the signed-in person's access, not a shared admin login.
- **Limit the data, not just the actions.** Restrict which records and fields the server can return.
- **One credential per server.** Never reuse an admin account or share one key across servers.
- **Turn off what you do not use.** Disable tools the task does not need.

03 Approvals

FILL IN

ACTION	DEFAULT	YOUR RULE	WHO APPROVES
Read a record or document	Allowed, logged		
Create a draft or internal note	Allowed, logged		
Send an email or message outside the company	A person approves first		
Payments, refunds, credits	A person approves first		
Delete or bulk-update records	A person approves, or not allowed		

04 Vetting a third-party server

5 CHECKS

- **The publisher:** who maintains it, and is it the tool vendor itself or a known organization?
- **The tool list:** read every tool name and description; reject servers that ask for more than the task needs.
- **The upkeep:** recent updates and a way to report problems.
- **Changes:** re-review tool descriptions whenever the server updates.
- **Separation:** keep servers apart so one cannot read another's data.

05 Records and review

4 CHECKS

- **Log what matters:** which tool ran, for whom, with what inputs and result.
- **Keep secrets out of logs:** redact tokens, passwords and personal data.
- **Watch for hidden instructions:** content from emails, pages or files can try to steer the AI; never let it trigger actions on its own.
- **Review permissions on a schedule** and whenever a person changes role or leaves.

+ Notes for your first connection

WRITE HERE

NEXT STEP

MCP integration services

www.doitwithfriday.com/services/mcp-tools/

Build with Friday →

BASED ON FRIDAY FIELD NOTES

www.doitwithfriday.com/blog/mcp-use-cases-small-business/

www.doitwithfriday.com/blog/mcp-security-permissions/

General guidance, not legal or security advice for your specific setup. Questions: hello@doitwithfriday.com