

The PMO Generative AI Approved- Use Checklist

Before a project team uses Generative AI for any task, it should be able to answer five questions about the tool, the use case, the data, the reviewer and the approval path. This checklist turns those questions into practical rules that PMO leaders, project managers and project teams can apply every day. It is a template: adapt the tool names, data categories and approval roles to your organization's own policies and legal requirements.

Educational template only. It does not replace your organization's policies or legal, security or compliance advice. All examples are illustrative.

How to Use This Checklist

The checklist is designed to be used at three moments:

- **Before starting a new AI use case:** work through the five quick-start questions and the approved-use table
- **Before entering project information into an AI tool:** check the data-sharing rules
- **Before using or sharing AI-generated content:** apply the review level that matches its risk

Who it is for

- **PMO leaders:** to set standards and monitor adoption across projects

- **Project and program managers:** to decide day to day what AI can be used for
- **Business and delivery teams:** to understand what they may and may not enter into AI tools
- **IT, security, legal and compliance:** to confirm that the rules match their requirements

How to adopt it

1. Replace the example tool names and data categories with your own
2. Have security, legal and compliance review the rules once
3. Share it with all project teams and make it part of project onboarding
4. Review it every quarter, and whenever a new tool or regulation changes the picture

The traffic-light system used throughout

Color	Meaning	What to do
Green	Allowed within the stated conditions	Proceed, and apply the review level

Amber	Allowed only with approval or in an approved tool	Get approval first
Red	Not allowed	Do not proceed

Quick-Start: The Five Questions Before You Use AI

If the answer to any question is “no” or “I don’t know,” stop and check before continuing.

1. **Is the tool approved?** Only use AI tools on the organization’s approved list. Free consumer tools and personal accounts are not approved by default.
2. **Is this an approved use case?** The task should appear in the approved-use table below, or have been approved separately.
3. **Is the data safe to enter?** Nothing in the input should be in the red data category, and amber data should go only into approved tools.
4. **Who will review the output?** A named person must review the result before it is used, with a level of review that matches the risk.
5. **Is extra approval needed?** New tools, new data types, external-facing outputs and AI agents with system access all need sign-off.

Example: applying the five questions

A project manager wants to ask an AI tool to turn raw meeting notes into action items.

- Tool: the organization's approved enterprise AI assistant (yes)
- Use case: summarizing internal meeting notes (approved with review)
- Data: the notes contain project names and task owners, but no personal or client confidential data (amber, fine in an approved tool)
- Reviewer: the project manager checks every action item against the meeting
- Extra approval: not needed

Result: green, proceed with review.

Now suppose the notes contain a client's contract pricing and a team member's performance concerns. The data is red, so the answer changes to stop: remove that content or do not use AI for this task.

Approved and Restricted Use Cases

Not every project task carries the same risk. The table below shows an example classification. Treat it as a starting point and adjust it to your organization.

Use case	Status	Conditions

Drafting a weekly status report from approved project data	Green	Reviewer verifies every date, cost and milestone against the project system
Summarizing internal meeting notes	Green	No red data in the notes; reviewer checks action items and owners
Suggesting items for a risk register	Green	Suggestions are inputs only; the project manager assesses and approves each risk
Drafting stakeholder emails or presentations	Green	Reviewed and edited by the sender before it goes out
Creating a first draft of a project plan or work breakdown structure	Amber	Approved tool only; the team validates durations, dependencies and resources
Analyzing project data for trends or forecasts	Amber	Data must be approved for AI use; results validated against the source
Sending any communication outside the organization without review	Red	Not permitted; a person must review and send

Changing budgets, schedules, contracts or resource assignments	Red	Human decision only; AI may offer analysis but may not act
Evaluating, ranking or making decisions about individual employees	Red	Prohibited
Entering client confidential or personal data into an unapproved tool	Red	Prohibited

Worked examples

Example 1: weekly status report (green). A project manager pastes approved milestone and budget figures into the approved assistant and asks: *“Draft a one-page weekly status report with sections for progress, risks, upcoming milestones and decisions needed. Use only the data provided.”* The draft is accurate except that it describes a delayed milestone as “on track.” The reviewer catches the error, corrects it and approves the report. The AI saved drafting time, and the human ensured accuracy.

Example 2: draft project plan (amber). A team asks the assistant for a draft work breakdown structure for a software rollout. The draft looks tidy but omits a security review and assumes two-week testing for a system that normally takes six. Because this is an amber use case, the project manager and technical lead validate the plan, add the missing tasks and correct the durations before it is shared.

Example 3: automatic budget change (red). An AI agent connected to the finance system proposes moving 10% of a project’s contingency to another work package. The proposal may be a useful input, but the agent may not make the change. The project manager and sponsor review the proposal and decide, and the decision is recorded.

Checklist: before starting any use case

- ☐ The use case is listed as green or amber in the approved-use table, or has been approved
- ☐ The conditions for that use case are understood
- ☐ A reviewer has been named
- ☐ The team knows which data is allowed

Data-Sharing Rules

What goes into an AI tool matters as much as what comes out. Many AI risks start with the wrong data in the prompt.

Category	Examples	Rule
Green: can be used	Public information, approved templates, generic project terminology, publicly available standards	May be used with approved tools

Amber: approved tools only	Internal project plans, internal schedules, non-sensitive meeting notes, internal status information	Only in tools approved for internal data; remove unnecessary detail
Red: never enter	Personal data about employees or customers, client confidential information, contract terms and pricing, credentials and access keys, unreleased financial results, legally restricted information	Never enter into AI tools unless a specific, documented approval exists

Preparing data before use

- ☐ Remove names, email addresses and other identifiers that are not needed for the task
- ☐ Replace client names with generic labels, such as “Client A”
- ☐ Remove prices, contract terms and account numbers
- ☐ Provide only the minimum information the task needs
- ☐ Confirm the tool’s data retention and training settings with IT or security
- ☐ Never paste passwords, access keys or confidential credentials

Example: a safer prompt

Risky version: “Summarize this email thread with Ravi Menon at BlueRiver Bank about the \$2.4 million contract renewal and his concerns about our delivery team’s performance.”

Safer version: “Summarize the following email thread. The client has raised concerns about delivery timelines and wants a revised plan. Identify the main concerns, the requested actions and the deadlines.” The text provided is stripped of names, amounts and performance comments about individuals.

The second version still gives the project manager a useful summary and avoids exposing personal and commercial information.

Questions to ask when unsure

- Would this information cause harm or embarrassment if it became public?
- Does it identify a person, a client or a contract?
- Is it covered by a confidentiality agreement or a regulation?
- Is the tool approved to receive this category of data?

If any answer is yes or unclear, treat the data as red until security, legal or compliance says otherwise.

Human Review Requirements

AI-generated content can be fluent and wrong at the same time. A human reviewer is the control that prevents errors from becoming project decisions. The level of review should match the impact of the output.

Review level	When it applies	What the reviewer does
Light review	Internal drafts, personal working notes, brainstorming	Read for sense, correct obvious errors, do not circulate unchecked
Standard review	Status reports, meeting summaries, stakeholder communications, risk suggestions	Verify facts and figures against source systems, check tone and context, edit and approve
Senior review	Anything affecting budget, schedule baselines, contracts, regulatory commitments or external parties	Independent verification by a second qualified person, documented approval before use

What reviewers must check

- **Accuracy:** do dates, costs, names, percentages and milestones match the source?

- **Completeness:** is anything important missing, such as a dependency or a risk?
- **Invented content:** are there statements, references or figures with no source?
- **Context:** does the output reflect how this project actually works?
- **Tone and audience:** is it suitable for the people who will read it?
- **Data exposure:** does the output reveal anything that should not be shared?

Reviewer checklist

- ☐ Every number and date checked against the project system
- ☐ Every named person, vendor or system confirmed to be correct
- ☐ Assumptions identified and either confirmed or removed
- ☐ Missing tasks, risks or stakeholders added
- ☐ Wording edited so that it sounds like the project manager, not like a generic template
- ☐ Final version approved by the named owner

Example: reviewing an AI-generated risk list

An assistant suggests eight risks for a data migration project. The project manager reviews each one:

- Three are relevant and become risks in the register
- Two are generic (“stakeholders may disagree”) and are rewritten with project-specific detail
- One is wrong, because it describes a system the project does not use
- One is a duplicate of an existing risk
- One reveals a new concern about a dependency on a vendor delivery date, which the team had missed

The AI widened the thinking, and the human judged what mattered. Neither alone would have produced as good a result.

Keeping accountability clear

- The person who approves AI-assisted content is responsible for it, in the same way as for work done by a team member
- “The AI wrote it” is never an acceptable explanation for an error
- Record who reviewed important AI-assisted deliverables, especially senior review items

Approval and Escalation Triggers

Some situations always need more than the project manager’s judgment. Pause and seek approval when any of the following applies.

Triggers for additional approval

- **A new AI tool or feature** that is not on the approved list, including new plug-ins and integrations
- **A new data type** that has not been approved for AI use, such as financial data or customer data
- **External-facing output**, such as client reports, public content or vendor communications
- **AI agents or automation** that can access systems, use tools or take actions
- **High-impact decisions**, such as those affecting budgets, contracts, safety, legal commitments or people
- **Regulated work**, where specific laws, standards or contract clauses apply

Who approves what

Situation	Typical approver
New use case within an approved tool	PMO lead
New tool, integration or plug-in	IT and security, with PMO sign-off

New data category or personal data	Data protection or privacy officer, legal and compliance
External-facing or regulated output	Legal and compliance, with business owner approval
AI agent with system access	IT, security and PMO, with documented permissions

Example: a request to use an AI agent

A program manager proposes an AI agent that will read project tickets, update status fields and send reminders. The PMO asks for the following before approving:

- Which systems and fields the agent can read and which it can change
- Which actions need human approval first (for example, sending messages to external parties)
- How actions are logged, and who reviews the logs
- How the agent can be switched off quickly if it misbehaves

The agent is approved to read tickets and draft reminders, but not to change status fields or send messages without a person's confirmation.

Reporting an AI error or incident

Report the incident quickly if AI produces a harmful or seriously wrong output, if protected data is entered by mistake, or if a tool behaves unexpectedly. A short incident record should include:

- **Date and reporter**
- **Tool and use case**
- **What happened** (for example, “confidential client pricing was pasted into an unapproved tool”)
- **Data or decisions affected**
- **Immediate action taken**
- **Follow-up owner and date**

Treat reporting as a learning process rather than a blame process. People are more likely to report mistakes early when they know the aim is to fix controls, not punish individuals.

Quick-Reference Do's and Don'ts

Print this page or pin it near your workspace.

Do	Don't

Use only approved tools	Use personal or free AI accounts for project work
Give AI the minimum information it needs	Paste whole documents without checking what they contain
Remove names, prices and identifiers first	Enter personal, client confidential or contract data
Ask for drafts, options and summaries	Let AI make final decisions on budgets, contracts or people
Verify facts, figures and dates against source systems	Copy AI output into official documents unchecked
Name a reviewer for every AI-assisted deliverable	Assume the AI is correct because it sounds confident
Ask for approval when something is new or unclear	Connect AI agents to systems without approval
Report errors and incidents quickly	Hide mistakes or work around controls

Next Steps and Related Resources

This checklist works best as part of a broader governance approach. After adopting it:

1. **Assign an owner** for the checklist, usually the PMO, who updates it as tools and rules change
2. **Add a roles and accountability matrix (RACI)** so that responsibilities for AI use, review and incident handling are clear
3. **Build or review your governance framework** covering policies, risk management, data governance, security, human oversight and monitoring
4. **Train project teams** on the checklist, using real examples from your own projects
5. **Review regularly**, using incident reports, audit findings and team feedback to improve the rules

Building skills

Project professionals do not need to become AI developers, but they should understand AI capabilities, limits, risks and governance principles. GSDC's AI Project Management Certification supports project managers, PMO leaders, program managers and business professionals who manage AI-driven projects, assess AI-related risks, support responsible AI adoption and align AI initiatives with business goals.

This checklist is provided for educational purposes only and should be adapted to your organization's policies, regulatory obligations and risk appetite.

CERTIFICATION IN GENERATIVE AI IN PROJECT MANAGEMENT

LEARN DIRECTLY FROM GLOBAL PRACTITIONERS, GENERATIVE AI SPECIALISTS, AND PROJECT MANAGEMENT LEADERS WHO ARE SHAPING THE FUTURE OF AI-DRIVEN PROJECT MANAGEMENT.



ABOUT GSDC CERTIFICATION



EBOOK

Extensive and exclusive Ebook created by world's experts to help you with understanding core concepts.



EBOOK

Extensive and exclusive Ebook created by world's experts to help you with understanding core concepts.



CREATED BY EXPERTS

GSDC certifications are created and authored by world's leading experts in the field.



LEARNING MATERIALS

Get access to learning materials such as videos, ebooks, templates, and practice exams, which will help you clear the certification exam.

LEARNING OBJECTIVE

- Understand Generative AI fundamentals and its role in modern project management.
- Learn how to use Generative AI to support project initiation, planning, execution, and monitoring.

Enroll now with the code **LEARN20** To avail **20%** discount

Enroll Now



www.gsdcouncil.org