



How a project manager runs an approval process: who to engage, in what order, and how to answer each reviewer
· spertsuite.com/approval-kit

SPERT® Suite Approval Kit v1.0.0 (Release) · Content reviewed 2026-10-25 · Built 2026-10-26

For: project managers who want to use SPERT® Suite at work and need [ORGANIZATION]'s approval first
Reviewed against: SPERT® Scheduler 0.79.26, SPERT® Story Map 0.53.14, SPERT® Forecaster 0.47.4, SPERT® CFD 0.15.23, GanttApp™ 0.29.8, MyScrumBudget™ 0.44.4; shared backend in the [spert-landing](#) repository 2.7.2 (commit 52b7fbf; Connect AI server 1.14.1); [Terms of Service](#) v1.4 and [Privacy Policy](#) v1.4 (both effective 2026-10-26); [AI Privacy Notice](#) v2.3 (effective 2026-10-26); [AI Connectivity Consent Notice](#) v2.2 (effective 2026-10-26). **Review date:** 2026-10-25.

This guide supports an approval process. It is not legal, compliance or security advice, and it makes no commitments on the operator's behalf beyond those in the published legal documents.

THE SHORT VERSION

Most organizations review any new software that touches work data, even a free tool that runs in a browser. That review is worth doing properly. A reviewer who gets clear, honest answers early is far more likely to say yes than one who finds a surprise late.

Four habits make the difference:

1. **Ask for the smallest thing first.** Request only the apps you need, in local-only mode, as a time-boxed pilot. Cloud storage and Connect AI can be approved later, or not at all.
2. **Bring the evidence.** This kit answers most reviewer questions before they are asked, with sources a reviewer can check.
3. **Be candid about the gaps.** SPERT® Suite has no SOC 2 report, no data processing agreement and no service-level agreement. Saying so up front builds trust; having a reviewer discover it costs you the trust you need.
4. **Position it as a complement.** SPERT® Suite adds probabilistic planning alongside [EXISTING TOOL]; it does not ask [ORGANIZATION] to replace anything.

SPERT® Suite can be approved in three separate tiers. The numbers are labels, not a ladder: tiers 2 and 3 are separate decisions.

Tier	On by default?	What leaves the user's device
1. Local-only use	Yes	Page requests to the web host. SPERT® Scheduler's optional holiday lookup sends a country code and year. No project data.
2. Cloud storage and sharing	No; the user signs in and accepts the Terms	Name, email and saved projects, stored in Google Cloud in the United States
3. Connect AI	No; started by the user, in three apps only	AI edits pass through a relay in Google Cloud. With Read Mode on, a copy of the open project goes to the relay and to the user's chosen AI provider

A reviewer can approve tier 1 alone. The *Architecture Overview* explains each tier with diagrams.

1. WHAT IS IN THE KIT

Document	What it is	Who it is for	Do you fill it in?
This Guide	How to run the approval process	You	No
Reviewer Summary	Two pages: what SPERT® Suite is, the three tiers, key facts and gaps, where to read more	Every reviewer, as the first thing you send	Placeholders only
Approval Pathway Checklist (template)	Every step, owner and date in one place	You and your sponsor	Yes
Value Brief (template)	Why you want it, how it fits with [EXISTING TOOL], what it costs, how you would stop	Your sponsor, manager, procurement	Yes
Information Security Profile (template)	One summary of controls, gaps and the approval scope	Information security, privacy	Yes
Data Flow Diagram with AI Connectivity (template)	The four diagrams, the flows, and space for [ORGANIZATION]'s side	Architecture, information security, AI governance	Yes
Reviewer FAQ (template)	Short answers to the questions each reviewer asks	All reviewers	Light edits
Architecture Overview	Components, data flows and trust boundaries in detail	Architecture, information security, privacy	Placeholders only
Security Questionnaire Answer Sheet	Ready-made answers to a typical security questionnaire, for SPERT® Scheduler only	Information security	Copy answers into [ORGANIZATION]'s form
Connect AI Data Explainer	What SPERT® Scheduler's Connect AI sends, and to whom	Privacy, AI governance	Placeholders only

Contacting the operator. Security reports and suspected account misuse: security@spertsuite.com, or GitHub private vulnerability reporting on any public SPERT® repository. Privacy questions, and requests to access, correct or delete data: privacy@spertsuite.com. Everything else, including the data-flow summary for IT review that the [AI Privacy Notice](#) (§7) offers: contact@spertsuite.com. The security policy is at <https://spertsuite.com/security>. The legal documents give the same addresses.

Every document comes as a PDF to read or forward and a Word file to edit. Fill in the highlighted [PLACEHOLDERS] in the Word file, then save it as PDF to send it on. Do not change the facts to make them sound better: reviewers can and do check them against the source code and the legal documents.

2. BEFORE YOU START: FOUR DECISIONS

Which apps. SPERT® Suite is six separate apps. Ask only for the ones you will use in the pilot. The *Security Questionnaire Answer Sheet* covers SPERT® Scheduler only, because that app and the shared backend received the most recent security hardening (2026-10-24 and 25). A suite-wide self-review was completed on 2026-10-25; its fixes are being released in stages. If you need cloud storage in another app, ask the operator (contact@spertsuite.com) for its status.

App	What it is for	Connect AI
SPERT® Scheduler	Build and maintain a project schedule that accounts for uncertainty	Write and Read

App	What it is for	Connect AI
SPERT® Story Map	Map and size release scope before the first sprint	Write and Read
SPERT® Forecaster	Forecast release dates and how confident to be in them	Read only
SPERT® CFD	See where work is piling up (cumulative flow)	Not offered
GanttApp™	Build and share a project timeline with uncertainty included	Not offered
MyScrumBudget™	Plan and reforecast a project or team budget	Not offered

Which tiers. Start with tier 1. It needs no account and sends no project data anywhere. Add tier 2 only if people must share projects or work across devices. Add tier 3 only if [ORGANIZATION] already allows an AI assistant such as [AI PLATFORM], and you have a clear use for it. Tier 3 does not need tier 2: Connect AI needs no account and works with projects stored locally. Many organizations find tier 3 in Write Mode only the easier second step, because existing project data is not uploaded ([AI Privacy Notice](#) §2.1).

What data. Find [ORGANIZATION]'s data classification scheme and decide which level of planning data you will put in the apps. The [Terms of Service](#) (§5.3) prohibit storing third-party personal information, protected health information, payment card data, government identification numbers "or other sensitive or regulated data" in cloud storage, and recommend cloud storage "be used only for non-sensitive planning metadata such as effort estimates, story point counts, sprint dates, task names, and similar project management data". Propose a classification at or below that line: [DATA CLASSIFICATION].

Who sponsors it. A manager or portfolio lead who wants the outcome makes every later conversation easier. Your sponsor does not need to understand the technology; they need to say the pilot is worth the reviewers' time. Then find [ORGANIZATION]'s intake route: a software request form, an architecture review board, a vendor-risk process, or a conversation with the service desk. [INTAKE ROUTE]. Use it, even for a free browser tool. The [Terms of Service](#) put the responsibility for approval on the user: a person using the apps for an employer represents that their use complies with the organization's policies, and "The Operator assumes no liability arising from your failure to obtain required organizational approvals" ([ToS](#) §5.5 for cloud storage, §5A.4 for Connect AI). Do not put work data into the apps until you have approval.

Approving a tier is a policy, not a setting

Approving tier 1 only is a policy decision. SPERT® Suite has no administrator switch, so nothing in the apps stops a member of staff from turning on cloud storage or Connect AI anyway. Write the approved tiers into the conditions of use and tell pilot users which ones they may use (*Approval Pathway Checklist*, section D).

If [ORGANIZATION] also wants a technical control, these are the options. **None of them has been tested**, by the operator or for this kit, so [ORGANIZATION]'s IT team should test any block it relies on.

- **Stop cloud sign-in (tier 2):** block `spert-suite.firebaseio.com`, the operator's Firebase sign-in handler. Untested, including what happens to a user who is already signed in.
- **Stop Connect AI from starting (tier 3):** block `us-central1-spert-suite.cloudfunctions.net/generatePairingCode`, the pairing function, or that whole host, which also stops sharing invitations. Blocking one path needs a web proxy that inspects HTTPS. Untested. Blocking the Connect AI server (`mcp.spertsuite.com`) does not work, because the AI provider's servers call it, not the user's device.
- **Use [AI PLATFORM]'s own connector controls (tier 3):** where the AI platform lets administrators restrict which custom connectors users may add, this is the most effective control, because it acts where the connection is made.

3. WHO TO ENGAGE, AND IN WHAT ORDER

Organizations differ, but this order works in most. Steps 3 to 6 can often run in parallel. Legal and procurement come later because their questions depend on the scope the others agree.

Step	Who	Why at this point	Give them
1	Your sponsor	Agrees the pilot is worth doing and sets its scope	<i>Value Brief</i>
2	Intake (service desk or software request)	Opens the formal request and routes it	<i>Value Brief, Approval Pathway Checklist</i>
3	Information security	Decides whether the controls are acceptable for the data	<i>Information Security Profile, Security Questionnaire Answer Sheet, Architecture Overview</i>
4	Privacy or data protection	Decides on personal data, retention and transfers	<i>Information Security Profile, Data Flow Diagram</i>
5	Enterprise architecture	Checks fit with the existing landscape	<i>Architecture Overview, Data Flow Diagram, Value Brief</i>
6	AI governance (tier 3 only)	Decides whether Connect AI may be used, and with which AI	<i>Connect AI Data Explainer, Data Flow Diagram</i>
7	Legal	Reviews the Terms of Service the user would accept	The four legal documents, <i>Reviewer FAQ</i>
8	Procurement or vendor management	Records a no-cost supplier and any onboarding steps	<i>Value Brief, Reviewer FAQ</i>
9	The decision-maker	Approves, with conditions, per tier	<i>Information Security Profile (decision block), Approval Pathway Checklist</i>
10	Your pilot users	Use it within the conditions, then report back	The conditions of approval

The sections below say what each reviewer usually asks, and what the honest answer is today.

Information security

They will ask: where it is hosted; how data is encrypted; how users sign in; what the known weaknesses are; whether there is a SOC 2 report or a penetration test; how vulnerabilities are reported; what is logged; how incidents are handled.

What to tell them:

- In tier 1 the planning calculations and storage happen in the user's browser. The web pages come from Vercel. There is no application server holding project data.
- In tier 2 data is stored in Google Cloud Firestore in the United States, behind Firebase Authentication and Firestore security rules. Sign-in is through Google or Microsoft only, including Microsoft Entra ID work accounts, so [ORGANIZATION]'s own MFA and conditional access apply. There are no passwords.
- The source code is public under GPL-3.0, so they can read the code that runs. GitHub Dependabot alerts, CodeQL code scanning, secret scanning and private vulnerability reporting are on for every public SPERT[®] repository (since 2026-10-25). Vulnerabilities can be reported to security@spertsuite.com; the operator's Security page aims to acknowledge reports within 3 business days.

- **Microsoft sign-in may need an administrator first.** The SPERT® Suite sign-in app is not yet a Microsoft "verified publisher". If [ORGANIZATION]'s Entra ID lets users consent only to apps from verified publishers, staff see "Need admin approval" at their first Microsoft sign-in, and an Entra administrator must grant consent to the app. The alternatives are Google sign-in or tier 1 only (operator's statement, 2026-10-25).
- **The gaps:** no SOC 2, ISO 27001 or independent penetration test; security reviews are the developer's own; no customer-facing audit log; no 24×7 monitoring or response commitment.
- **If they want to scan the live apps, raise it first.** The [Terms of Service](#) (§4) forbid attempting "to probe, scan, test, or circumvent the security or authentication measures of the Apps". A reviewer can read the public source instead, run their own copy, or ask the operator in writing (security@spertsuite.com) before any test.

Privacy

They will ask: what personal data is collected; where it is stored and for how long; how it is deleted; who else receives it; whether the operator will sign a data processing agreement.

What to tell them:

- Tier 1: the operator collects no data from local-only use other than the standard request data the web host receives ([Privacy Policy](#) §1, §2.4).
- Tier 2: name, email and profile-photo link from the sign-in provider, a record of which Terms were accepted (with the sign-in provider and the first app used), the projects the user saves, and technical data such as IP address ([Privacy Policy](#) §2.1 to §2.3). Data at rest is in the United States (Firestore multi-region nam5); operational logs are kept 30 days in a location "not restricted to a specific country or region" (§2.3, §9).
- Deletion is done by the operator on request, "not to exceed thirty (30) days under normal circumstances"; backup copies expire within 98 days, and Google's Firebase Authentication may keep a deleted account's sign-in information for up to 180 days (§6). There is no self-service delete-account control.
- **The gaps:** no data processing agreement is offered; under the [Privacy Policy](#) the operator is the data controller (§7.6), not a processor for [ORGANIZATION]. There is no separate subprocessor list; the service providers are named in [Privacy Policy](#) §4. SPERT® Scheduler's holiday lookup service (Nager.Date) receives only a country code and year; [Privacy Policy](#) §1 describes it.

Enterprise architecture

They will ask: what it duplicates; how it integrates; how identity works; who supports it; what happens if it goes away.

What to tell them:

- Nothing to install. Each app is a web page; projects can be exported to files at any time.
- No integrations or APIs with other enterprise systems: data moves by file export and import.
- Microsoft sign-in may need an Entra administrator to grant consent to the SPERT® Suite app first (see information security above).
- No enterprise administration: no admin console, single-sign-on enforcement, user provisioning or organization-wide export.
- It is positioned as a complement to [EXISTING TOOL], used for the probabilistic planning that [EXISTING TOOL] does not do. Concede the rest: [EXISTING TOOL] remains the system of record.

AI governance (only if tier 3 is in scope)

They will ask: what AI is involved; what data the AI receives; which AI providers; whether [ORGANIZATION] can restrict it; what the AI can change or delete.

What to tell them:

- None of the apps has AI built in. Connect AI lets a user connect an AI assistant they already use, such as [AI PLATFORM], to one open project. It is off unless the user starts it, and only SPERT® Scheduler, SPERT® Story Map and SPERT® Forecaster offer it.
- Write Mode lets the AI send edits and does not upload existing project data. Read Mode uploads a copy of the open project to the relay and on to the AI provider, and "Read Mode uploads a copy of your open project regardless of your storage setting" ([AI Privacy Notice](#) §2.2).
- The AI tools can overwrite names, estimates and descriptions, and remove some links, but no tool deletes an activity, milestone, story-map item or project. SPERT® Forecaster's connection is read-only. The *Data Flow Diagram* template lists every tool.
- **The gaps:** there is no administrator switch to turn Connect AI off for [ORGANIZATION]. The practical controls are an acceptable-use rule and [AI PLATFORM]'s own controls over which connectors users may add. Blocking the Connect AI server (`mcp.spertsuite.com`) on [ORGANIZATION]'s network does not work, because the AI provider's servers call it, not the user's device. Starting Connect AI does need the user's browser to call SPERT® Suite's pairing function at `us-central1-spert-suite.cloudfunctions.net/generatePairingCode`, so blocking that path, or that whole host (which also stops sharing invitations), may stop Connect AI from starting. This is untested, so [ORGANIZATION]'s IT team should test any block it relies on.

Legal

They will ask: what the user agrees to; who carries the risk; whether the terms can be negotiated.

What to point out early (all from [Terms of Service](#) v1.4):

- The relationship is a standard set of online Terms, not a negotiated contract. The Terms say that accessing or using any app means agreeing to them (opening paragraph), and users accept them in a dialog before cloud storage is turned on.
- A person using the apps for an employer "represent[s] that you have authority to bind that organization to these Terms" (§5.5). **Ask legal who may accept the Terms for [ORGANIZATION] before anyone does.**
- The service is provided "AS IS" and "may be modified, suspended, or discontinued at any time without notice" (§2, §8). Liability is capped at the greater of \$25 or fees paid in the past 12 months (§9). The user indemnifies the operator (§10).
- Florida law and Florida courts, with a class action waiver (§17). The Terms can change, with notice by posting an updated version (§16).
- Software rights come from the GPL-3.0 licence with additional terms, which the Terms do not restrict (§3).
- Users who accepted the Terms before October 26, 2026 are asked to accept the updated [Terms of Service](#) and [Privacy Policy](#); a user who is already signed in is signed out once and asked when they sign in again.

Procurement or vendor management

They will ask: what it costs; who the supplier is; whether a contract or supplier record is needed.

What to tell them: "Core application functionality is provided at no charge" ([ToS](#) §2), and no paid tier exists today, so there is nothing to purchase. The operator is famousdavis, LLC, a Florida limited liability company ([ToS](#) §1) run by one person. There is no SLA, support contract or continuity commitment. The exit is simple: export the projects and stop. Some organizations still require a supplier record or vendor-risk assessment for a free tool; follow [ORGANIZATION]'s rule.

4. HANDLING OBJECTIONS

Objection	The honest answer	What you can offer
"It's open source, so no vendor stands behind it."	True. No third party has audited it, and there is no support contract.	The code that runs is public; tier 1 keeps data on the device; a time-boxed pilot with a review date.
"Our data will leave our environment."	Not in tier 1, apart from page requests and Scheduler's optional holiday lookup. Tier 2 stores data in Google Cloud in the US. Tier 3 Read Mode sends one project to the AI provider.	Approve tier 1 only; decline or defer tiers 2 and 3.
"Where are the audit logs?"	There are none for users or administrators.	Keep sensitive work out of scope; export projects as point-in-time records.
"We've never heard of this vendor."	It is a small, single-operator business.	Start small. Local data is unaffected by the operator's fortunes, and the GPL allows self-hosting under a different name.
"What if the AI wrecks a schedule?"	No AI tool can delete an activity, milestone, story-map item or project; overwrites are listed.	Write Mode only, or no Connect AI; export before AI sessions.
"We already have [EXISTING TOOL]."	Agreed, and it stays.	Use SPERT® Suite only for the forecasting question [EXISTING TOOL] does not answer.
"One developer is a continuity risk."	It is. The Terms allow the service to be discontinued without notice.	Treat it as non-critical; export regularly; plan the exit in the <i>Value Brief</i> .
"Our data must stay in [REGION]."	Cloud data is US-only.	Tier 1 only, where data stays on the device.

5. PROPOSING THE PILOT

A pilot with clear conditions is easier to approve than an open-ended request. Propose:

- **Scope:** [APPS REQUESTED], tier [TIERS REQUESTED] only.
- **People:** [NUMBER] named users in [TEAM].
- **Duration:** [PILOT LENGTH], ending with a review on [REVIEW DATE].
- **Data:** planning data classified [DATA CLASSIFICATION] or lower; nothing the [Terms of Service](#) prohibit.
- **Habits:** export projects [EXPORT FREQUENCY]; use assigned devices, or one browser profile per person (local projects belong to the browser profile, not the person); if Connect AI is approved, disconnect when finished, and in SPERT® Story Map before opening a project the AI should not see or change (a Story Map session follows the user to whichever project is open).
- **Success measures:** for example, [MEASURE 1] and [MEASURE 2]. The *Value Brief* has prompts.
- **Exit:** what happens if the pilot stops: export, clear browser data, request deletion of any cloud account ([Privacy Policy](#) §6).

6. IF THE ANSWER IS NO, OR NOT YET

Ask which tier and which concern drove the decision, and write it down. A "no" to Connect AI or cloud storage is often a "yes" to tier 1. If a missing item blocked approval (for example a data processing agreement or an independent audit), record it as a condition for review. The operator says documentation such as a security overview and a subprocessor list is in preparation; it is not published yet, so do not promise it, but you can ask the operator (contact@spertsuite.com) about its status. Do not use the apps for work data in the meantime.

7. WHAT NOT TO DO

- **Don't promise what the legal documents don't.** No SLA, DPA, support hours, certification or notification deadline exists beyond what the Terms and [Privacy Policy](#) say.
- **Don't edit facts in the templates** to make them sound better. Fill in the placeholders and leave the facts alone, or correct them with a source.
- **Don't start with work data** before approval, and never store data the [Terms of Service](#) prohibit.
- **Don't turn on Read Mode** with an AI account [ORGANIZATION] has not approved. AI providers' retention and training practices vary by account type ([AI Privacy Notice](#) §3).
- **Don't scan or test the live apps** without the operator's agreement ([ToS](#) §4).

8. KEEPING THE APPROVAL CURRENT

The operator gives notice of changes by posting updated legal documents with a new version and effective date ([ToS](#) §16; [Privacy Policy](#) §11; [AI Privacy Notice](#) §10), and has said it will give notice before changing where cloud data is stored ([Privacy Policy](#) §9). Agree with [REVIEWING TEAM] what should trigger a fresh look, for example:

- a new version of any of the four legal documents;
- a new app offering Connect AI, or a change in the modes an app offers ([AI Privacy Notice](#) §2.3);
- a change in data location;
- a scope change at [ORGANIZATION], such as a new tier or a higher data classification;
- the scheduled review date: [REVIEW INTERVAL].

Each kit document shows its version and review date under the title. The current kit is published at spertsuite.com/approval-kit; check it for a newer version before you submit.

9. SCOPE AND LIMITS OF THIS GUIDE

Facts here are drawn from the kit's other documents, re-checked against each app's source at the versions above and against the current legal documents (read 2026-10-25). Not verified: live security headers of each app, the export formats of each running app, and Google Cloud's and Vercel's current certifications, which reviewers should read from those providers directly. Organizations' approval processes vary; adapt the order in section 3 to [ORGANIZATION]'s own.