

TRAFFIC LIGHTS

Governance Kit

Design, operate and report on supervised AI processes

For process owners, risk and compliance leaders, auditors and implementation partners.

Version 1.0 · October 2026

About the frameworks - This kit uses the structure of the COSO Internal Control – Integrated Framework, business process management practice and the APQC Process Classification Framework. Processes designed with it are COSO-structured; whether your controls are sufficient is determined by your auditors. COSO is a trademark of the Committee of Sponsoring Organizations of the Treadway Commission; Traffic Lights is not affiliated with or endorsed by COSO.

Contents

1. How to use this kit.....	3
2. Part 1 · Design a governed process.....	4
3. The frameworks in brief	4
4. How the seven steps map	4
5. The worksheet	5
6. Part 2 · Operate: from design to evidence	10
7. From worksheet to live process	10
8. What is recorded on every run	10
9. Part 3 · Report: what to show management or the board.....	11
10. Question 1 · What are your AI agents doing?.....	11
11. Question 2 · Who approved what, and when?	11
12. Question 3 · What rules govern your agents?	12
13. Question 4 · What happens when something goes wrong?	12
14. Question 5 · How are you improving over time?	12
15. Which design step answers which board question	13
16. Appendix A · Sample board report	14
17. Executive summary	14
18. 1. What are our AI agents doing?	14
19. 2. Who approved what, and when?	15
20. 3. What rules govern our agents?.....	15
21. 4. What happened when things went wrong?.....	16
22. 5. How are we improving?	16
23. Board attestation.....	16

How to use this kit

Supervised autonomy works when three things line up: a process designed with the right controls, a platform that records what happens, and evidence your board and auditors can read. This kit follows that lifecycle.

Part	Question it answers	When to use it
1. Design	How do I design a process that will stand up to scrutiny?	Before you build, ideally before you sign in
2. Operate	What does Traffic Lights record while the process runs?	While configuring and running the process
3. Report	What will the board, auditor or regulator ask, and can I answer it?	Before every governance review
Appendix A	What does a finished board report look like?	As a model for your own

Designed answers become evidence - Every question in Part 1 produces something the platform records, and every board question in Part 3 is answered from those records. The table in Part 3 shows which design step answers which board question.

Part 1 • Design a governed process

Three frameworks shape the design. Each plays a different role, and none of them is reproduced here; the descriptions below are our summaries.

The frameworks in brief

- **COSO Internal Control – Integrated Framework.** The standard structure for internal control in regulated organizations: control environment, risk assessment, control activities, information and communication, and monitoring. It gives the design its governance questions.
- **COSO guidance on generative AI.** COSO has published guidance on applying internal control to generative AI. The AI-specific questions in this kit (named accountability for AI outputs, model change, approver context) reflect that direction; confirm specific expectations against the publication itself.
- **Business process management (BPM).** The discover, design, manage and improve lifecycle. It gives the design its order: what the process does before what controls govern it.
- **APQC Process Classification Framework (PCF).** A shared vocabulary for classifying processes (for example, 9. Manage Financial Resources). It is used for classification only.

How the seven steps map

Step	Focus	Framework basis
1 • Identify the process	Name the process, what it is for, who owns it, and whether AI takes part	Business process management (discover) · APQC process classification
2 • Control environment	Who holds authority over the process, and how changes to it are governed	COSO component 1: control environment
3 • Risk assessment	What could go wrong, how much it matters, and whether it can be undone	COSO component 2: risk assessment · BPM assess
4 • Control activities	The steps of the process, who or what performs each, and where a person must decide	COSO component 3: control activities · BPM design
5 • Information and communication	Who is told what, through which channel, and how fast they must act	COSO component 4: information and communication

Step	Focus	Framework basis
6 · Monitoring	How you will know the process is healthy, and how it reaches your oversight body	COSO component 5: monitoring activities · BPM manage
7 · Improvement and ratification	How the process changes over time, and who approves each change	COSO component 5 (continuous) · BPM improve

The same seven steps in the product - Traffic Lights' process wizard asks these questions in this order. Completing this worksheet first means the process is ready before you open the wizard, and the answers carry straight across. You can also complete the same interview with an AI assistant connected to Traffic Lights.

The worksheet

Fields marked * are required in the wizard. "Recommended" values are Traffic Lights' guidance, not framework requirements.

Step 1 · Identify the process

Business process management (discover) · APQC process classification

Name the process, what it is for, who owns it, and whether AI takes part. Everything after this builds on these answers.

Field	What to decide	Your answer
Process name *	A short name people will recognize on the Control Tower.	
Business purpose *	One to three sentences: what the process achieves and for whom.	
Process family	The APQC Process Classification category it belongs to (for example, 9. Manage Financial Resources).	
Regulatory and framework context	Regulators or frameworks that apply (for example SOX, SEC, GDPR, COSO, SOC 2). Context only; it does not change the platform's behavior.	
Process owner and backup *	The person accountable for the process and outcomes, and who covers when they are away. Chosen from your team.	
Is AI involved? *	Does any step have an AI agent propose, generate or act? If yes, the AI-specific questions in later steps apply.	

Step 2 • Control environment

COSO component 1: control environment

Who holds authority over the process, and how changes to it are governed.

Field	What to decide	Your answer
Ratification authority *	The person who must approve any change to the process's rules.	
Separation of duties *	Must the person who starts a run be different from the person who approves its outcome? Recommended: yes for financially material processes.	
Accountable for AI outputs	If AI is involved, the named person accountable for its outputs. A person, not a team.	
Oversight committee or function	For example, Risk Committee, CFO or Chief Compliance Officer.	
Review frequency *	How often the process and its rules are reviewed.	
Change documentation *	Must every rule or threshold change carry a written reason? Recommended: yes.	

Step 3 • Risk assessment

COSO component 2: risk assessment • BPM assess

What could go wrong, how much it matters, and whether it can be undone.

Field	What to decide	Your answer
What the step does *	What the agent or system does in plain words.	
Consequence of approval *	What happens downstream once the outcome is accepted.	
Reversible? *	Yes, no or partially. Irreversible actions call for stronger gates.	
Worst case if wrong	The realistic worst outcome.	
Risk rating *	Low, medium, high or critical.	

Field	What to decide	Your answer
AI-specific risks	If AI is involved: how likely a confident but wrong output is, and whether the model may change between reviews.	
Regulatory sensitivity	Which obligations an error would touch.	

Step 4 · Control activities

COSO component 3: control activities · BPM design

The steps of the process, who or what performs each, and where a person must decide.

Field	What to decide	Your answer
Steps and their types *	For each step: machine, agent, agent with human review, or human sign-off.	
Escalation threshold *	What sends an outcome to a person, for example an amount over \$500 or a result below a confidence level.	
When review adds no value *	Complete: "A human review adds no value when ...". This is the justification for anything that proceeds automatically.	
Approval checklist	For each human gate: the items the approver must answer before Approve is available (confirmations, choices, numbers, dates, text). Recommended for high and critical risk.	
Independent corroboration	Should an agent's output be checked against an independent record before the process continues? For example, a proposed value checked against a custodian statement.	
Separation of duties enforced	If yes, the person who starts a run cannot approve it.	

Step 5 · Information and communication

COSO component 4: information and communication

Who is told what, through which channel, and how fast they must act.

Field	What to decide	Your answer
Notification channels *	Email, Microsoft Teams or Slack.	

Field	What to decide	Your answer
Primary and backup approver *	Named people, chosen from your team.	
Response window *	How long an approver has before the task turns amber, and when it escalates.	
Context shown to the approver *	What the approver must see to decide well: the agent's output, source data, downstream consequence.	
Severity that notifies	Which outcomes notify (for example warnings and errors, or every completion).	

Step 6 • Monitoring

COSO component 5: monitoring activities · BPM manage

How you will know the process is healthy, and how it reaches your oversight body.

Field	What to decide	Your answer
Process SLA *	The end-to-end time target.	
Yellow and red thresholds *	When the process turns amber (for example at 80% of its SLA) and red (when breached).	
Expected review rate	Roughly what share of outcomes you expect a person to review. A useful baseline for later.	
Reporting cadence *	Weekly, monthly or quarterly.	
Board reporting *	Should this process appear in the board's governance report? Recommended: yes for high and critical risk.	

Step 7 • Improvement and ratification

COSO component 5 (continuous) · BPM improve

How the process changes over time, and who approves each change.

Field	What to decide	Your answer
First review *	When the first review happens. Recommended: after 30 days for any new process.	
Ongoing review *	Monthly, quarterly or annually. Higher risk calls for more frequent review.	

Field	What to decide	Your answer
Change trigger *	What prompts an unscheduled review, for example “more than 85% of escalations approved unchanged for three months”.	
Model change review	If AI is involved: does a change to the underlying model trigger a review? Recommended: yes.	
Ratification evidence *	Must the ratifying authority give a written reason for every change? Recommended: always.	
Post-change monitoring	How long to watch outcomes after a change before considering it stable, for example 30 days.	

PRIVATE AND CONFIDENTIAL

Part 2 • Operate: from design to evidence

Once designed, the process runs inside Traffic Lights. Every step produces a record, and the record is what you report from.

From worksheet to live process

- **Wizard.** The worksheet's answers are entered in the guided wizard (or with an AI assistant), saved as a draft as you go.
- **Builder.** The draft is reviewed in the builder: each step's type and parameters, approvers chosen from your team, checklists on human gates, connections with their conditions, and rules such as escalate, notify and retry.
- **Readiness and finalize.** The platform checks the draft before it can go live, and lists anything that must be fixed. Finalizing creates a versioned, live process definition.

What is recorded on every run

Record	What it shows
Run graph	Which paths were taken and which were not, with the reason; loops, with the verdict that caused them; the current step
Story	Each step: who or what acted, the outcome, start and finish, duration and SLA outcome
Events	Every event in order, with severity, filterable and exportable
Evidence	The decisions an auditor reads: approvals, rejections, delegations, challenges and rule actions, each with who, when and the basis given
Approval checklist answers	What the approver was asked (in the wording at the time), what they answered, pre-filled values confirmed or changed, and challenges with their justification
Rule and definition versions	Every change to a rule or process creates a new version; prior versions stay readable

Identity is never self-declared - Every action is recorded under the identity that performed it, derived from the person's sign-in or the system's credential. No sender can name who they are or which organization they act for.

The Traffic Lights User Guide describes each screen in detail.

Part 3 • Report: what to show the board

When a board member, auditor or regulator asks about your AI agents, reassurance is not enough. They need a specific, evidenced answer that is already on record. These are the five questions they ask, the evidence for each, and where it lives in Traffic Lights.

A test for your next review - If any of these answers has to be assembled by hand, that process is the one to bring under governance before the review.

Question 1 • What are your AI agents doing?

A complete picture of agent activity: not a list of tools, but a record of what agents actually did.

Evidence to have ready

- ☐ Every active process, by name and owner, with the business function it supports
- ☐ Each step's type: machine, agent, agent with human review, human
- ☐ Runs in the period, by process, with their outcomes
- ☐ Which outcomes proceeded automatically and which went to a person

Where it is in Traffic Lights: Control Tower (all processes and their health) · Runs (filter by process and date, export) · each run's graph and Story.

What good looks like: *"Our agents took part in 6 governed processes this quarter. Outcomes inside the approved thresholds proceeded automatically; everything above them went to a named reviewer."*

Question 2 • Who approved what, and when?

Every consequential outcome has a named person behind it: who decided, when, and on what basis.

Evidence to have ready

- ☐ Approval history for any process and period, exportable
- ☐ For each decision: who decided, when, the outcome and the reason given
- ☐ For checklist gates: what was asked, what was answered, which pre-filled values were confirmed or changed, and any challenge with its justification
- ☐ For delegated approvals: who handed off to whom

Where it is in Traffic Lights: Approval history (filter by decision, delegated yes/no, decided by) · each run's Evidence tab · Events (export).

What good looks like: *"Here is the approval record for the October month-end close. Every decision names its reviewer and time, and shows the checklist the reviewer answered before approving."*

Question 3 • What rules govern your agents?

Agent behavior is governed by defined, versioned rules that can be shown to a regulator.

Evidence to have ready

- ☐ The current rules for each process and when they took effect
- ☐ Change history: what changed, who changed it, when, and why
- ☐ Each threshold: what proceeds automatically and what escalates
- ☐ Named reviewers and backups for each gate

Where it is in Traffic Lights: Policies (current and prior versions) · the process definition and its version history · Audit tables.

What good looks like: *“Our refund rule is on version 3. On 15 September the threshold rose from \$500 to \$750, ratified by the Finance Controller, with the data that justified it on record.”*

Question 4 • What happens when something goes wrong?

The system recovers, escalates appropriately, and stops a bad outcome from spreading.

Evidence to have ready

- ☐ The escalation path for each process
- ☐ SLA breaches in the period: what breached, what fired, what happened next
- ☐ Runs halted by a rule, a loop bound or an expired approval, with the reason
- ☐ Notifications that failed to deliver, with the reason

Where it is in Traffic Lights: Control Tower (red and amber) · Events (filter by severity = error) · Runs (failed and halted) · each run’s NOW banner and Story SLA column.

What good looks like: *“In Q3 we had 14 SLA breaches. Each escalated automatically to its named owner, and each is on record with how it was resolved.”*

Question 5 • How are you improving over time?

Governance learns: thresholds change on evidence, and human review becomes more targeted, not more burdensome.

Evidence to have ready

- ☐ Threshold change history with the reason and ratifier for each
- ☐ How often escalated outcomes were approved unchanged (a signal a threshold may be too low)
- ☐ Where reviewers changed or challenged pre-filled values (where people add the most value)

Where it is in Traffic Lights: Policy version history · Approval history (decision and checklist outcomes) · each run's Evidence.

What good looks like: *"Our review rate fell from 42% to 29% this year, not by lowering standards, but by raising thresholds where the record showed reviewers approving unchanged. Every change is ratified and on record."*

Which design step answers which board question

Board question	Answered by these design steps
1. What are your agents doing?	Step 1 (process, owner, AI involvement) and Step 4 (step types)
2. Who approved what, and when?	Step 2 (authority, separation of duties) and Step 4 (approval checklists)
3. What rules govern your agents?	Step 4 (thresholds) and Step 7 (ratification)
4. What happens when something goes wrong?	Step 3 (risk, reversibility), Step 5 (escalation, response windows) and Step 6 (SLA, thresholds)
5. How are you improving?	Step 6 (baselines) and Step 7 (review triggers, ratification evidence)

Assembling the report - Each answer above comes from records Traffic Lights already keeps. Today the quarterly report is assembled from those screens and exports; a generated board report is planned.

Appendix A · Sample board report

Illustrative sample — fictional data - Every organization, person, number and record in this appendix is invented to show the shape of a finished report. Use it as a model; do not cite its figures.

AI Governance Report · Q3 2026

Human oversight of AI-assisted processes · Prepared for board review

Item	Detail
Organization	[Your organization]
Period	Q3 2026 (1 July – 30 September 2026)
Prepared by	Chief Operating Officer / Risk and Compliance
Classification	Board confidential

Executive summary

Measure	Q3 2026
Governed processes	15
Outcomes produced by agent and machine steps	18,472
Proceeded automatically within ratified thresholds	13,256 (71.8%)
Sent to a named reviewer	5,216 (28.2%)
Decisions recorded	5,201
Approved / rejected / expired	4,267 / 521 / 15
Delegated before decision	413
Runs within SLA	94.3%
Rule changes in the period	7, all ratified by a named authority

Agent-assisted processes produced 18,472 outcomes in Q3. 71.8% proceeded automatically within ratified thresholds, up from 65.2% in Q2, after threshold changes ratified at the Q2 review. Every outcome above a threshold reached a named reviewer, and every decision is on record with the reviewer, the time and the basis given.

1. What are our AI agents doing?

Process	Step types
Month-End Close	Machine, agent, agent with human review, human sign-off
Invoice Reconciliation	Machine, agent
Client Communication Review	Agent with human review
Counterparty Limit Sign-Off	Agent with human review, human sign-off
Vendor Onboarding	Agent, human sign-off
Cash Reconciliation	Machine, agent

Steps typed “agent with human review” always go to a person by design; for those, an automatic rate of 0% is the expected outcome.

2. Who approved what, and when?

Decision	Count
Approved	4,267
Rejected	521
Expired without a decision	15
Delegated before decision	413

Sample decision record

Field	Value
Run	MEC-20260912T044343Z · Month-End Close
Step	NAV controller sign-off
Proposed by	Reconciliation agent
Decided by	R. Okafor, Controller
Checklist	5 items answered; reported NAV pre-filled and confirmed; one item challenged with a written justification
Outcome	Approved, 12 September 2026, 06:14 UTC

The checklist answers are the evidence that the reviewer engaged with what they approved: Approve was not available until the required items were answered.

3. What rules govern our agents?

Rule	Change in Q3	Ratified by
Invoice auto-approval	Threshold raised \$250 → \$500	Finance Controller, 15 July
Counterparty limit	Threshold raised \$1M → \$2M	Risk Manager, 1 September
Vendor onboarding	Confidence threshold 0.85 → 0.80	COO, 1 July

Every change creates a new version and keeps the prior version readable.

4. What happened when things went wrong?

Measure	Q3 2026
SLA breaches	18, each escalated to its named owner
Runs halted by a rule or bound	3
Runs within SLA	94.3%

5. How are we improving?

Quarter	Proceeded automatically
Q1 2026	58.4%
Q2 2026	65.2%
Q3 2026	71.8%

The automatic rate rose because thresholds were raised where the record showed reviewers approving unchanged, not because standards were lowered. Each change was ratified and versioned.

Recommended for Q4: require a backup reviewer on every human-review gate (two Q3 breaches were caused by reviewer absence); review the invoice threshold after 30 more days of data.

Board attestation

- AI-assisted processes ran under versioned rules ratified by named people.
- Every outcome above a ratified threshold was decided by a named person before it was acted on.
- Checklist gates recorded what each reviewer was asked and answered before approving.
- The complete record is available for examination on request.

Chief Operating Officer	Chief Compliance Officer	Chief Risk Officer
Signature:	Signature:	Signature:
Date:	Date:	Date:

PRIVATE AND CONFIDENTIAL