

Timeline sample: MAS AI evidence pack and approval review

Synthetic test environment. No real firm, system or data. Generated with the open-source CLI timeline 0.2.0 on 23 Oct 2026. Indicative mapping, not legal advice.

The scenario. An accounts-payable agent was approved on 1 Oct 2026 to *read invoices, Singapore entity only, no payment initiation*. Three weeks later a developer connected a payments MCP server to the same agent. No change ticket was raised.

What Timeline shows, in one run:

- The approval is flagged **re-review required** under MAS paras 5.24–5.25(a), with the exact change: a new remote payments server.
- The new server is **not on the firm's approved AI tool list** (paras 2.3–2.5).
- A second approval's evidence **expires in 22 days** (para 4.11).
- The AI inventory (para 4.7) and each agent's accessible tools and guardrails (para 4.8, fn 25) are evidenced from the scan plus the firm's own inventory, including AI inside a SaaS product that a scan cannot see.

Timeline runs inside the firm's environment, reads no secret values (names and locations only) and sends nothing out.

Approval review (2026-10-23)

1 re-review required, 0 evidence expired, 0 to verify, 1 expiring soon, 0 current; 0 unapproved agent(s)

Accounts-payable assistant (Claude Code): re-review required

approved by Chief Risk Officer on 2026-10-01, valid until 2027-10-01; owner Head of Finance Operations

- **capability added:** claude-code/Claude Code (~/.claude/settings.json): unknown-mcp-tool via mcp:payments [MAS AIRM para 5.25(a), 5.24]
- **MCP server added:** claude-code/Claude Code (~/.claude/settings.json): payments (remote, <https://payments-gateway.example>) [MAS AIRM para 5.25(a), 5.24]

Code review agent (CI): expiring soon

approved by Head of Technology Risk on 2026-09-15, valid until 2026-11-14; owner Head of Engineering

- evidence expiring: approval evidence expires on 2026-11-14 [MAS AIRM para 4.11, 2.5(f)]

Indicative mapping, not legal advice. The owner decides whether a change is significant.

AI evidence pack: Example Bank Pte Ltd (synthetic)

Generated by timeline 0.2.0. Indicative mapping, not legal advice. The firm decides whether it complies. No secret values are included.

MAS Guidelines on AI Risk Management (issued 7 Oct 2026)

Sections 3-4 (oversight, identification, inventory, materiality) apply from 7 Oct 2027; sections 5-6 (life-cycle controls) by 7 Oct 2028.

Mapped to paragraph numbers in the issued text.

Ref	Requirement	Status	Evidence
para 4.2, fn 21	Identify AI, including AI in services from material third parties and SaaS not sold as AI	evidenced	2 agent(s) found by local scan; 1 system(s) declared in the inventory.
para 4.7	Inventory with purpose, scope, model type, data, dependencies, status, materiality, review status, owners, documentation	evidenced	All 3 system(s) have the required attributes.
para 4.8, fn 25	For AI agents: the tools and systems the agent can access, and the guardrails applied	evidenced	Tools, systems and guardrails recorded for 2 agent(s) from the scan.
section 4	Risk materiality assessment for each AI use	evidenced	Materiality recorded for all 3 system(s).
para 5.11	The FI stays accountable for third-party AI	partial	Remote (third-party) MCP servers in use: jira, payments. Due diligence on providers is the firm's; Tideline lists them and flags changes (tideline diff).
paras 2.3-2.5	Basic governance: approved AI tool list and process (minimum for every FI)	gap	In use but not on the approved list: payments
paras 5.24-5.25	Significant changes trigger review and re-approval before implementation (applies by 7 Oct 2028)	gap	2 approval(s) checked against the current scan: 1 need re-review, 0 expired, 0 current. Stale: Accounts-payable assistant (Claude Code).

AI inventory

System	Source	Score	Materiality (recorded / suggested)	Owner	Missing attributes
Claude Code	scan	82	medium / high	Head of Finance Operations	none
CI agent (review.yml)	scan	73	medium / high	Head of Engineering	none
CRM email assistant (SaaS)	declared		low / -	Head of Wealth Ops	none

Claude Code

- Tools and systems accessible: aws-credentials-file, filesystem, generic-secret, github, shell-execution, unknown-mcp-tool, workspace-docs
- Guardrails observed: autonomy 0.4 (prompts for actions by default)
- Dependencies (MCP servers): github (local, npx), jira (remote, <https://mcp.atlassian.example>), invoices (local, uvx), payments (remote, <https://payments-gateway.example>)

CI agent (review.yml)

- Tools and systems accessible: ci-secret, repo-write
- Guardrails observed: autonomy 0.9 (runs unattended in CI)
- Dependencies (MCP servers): none