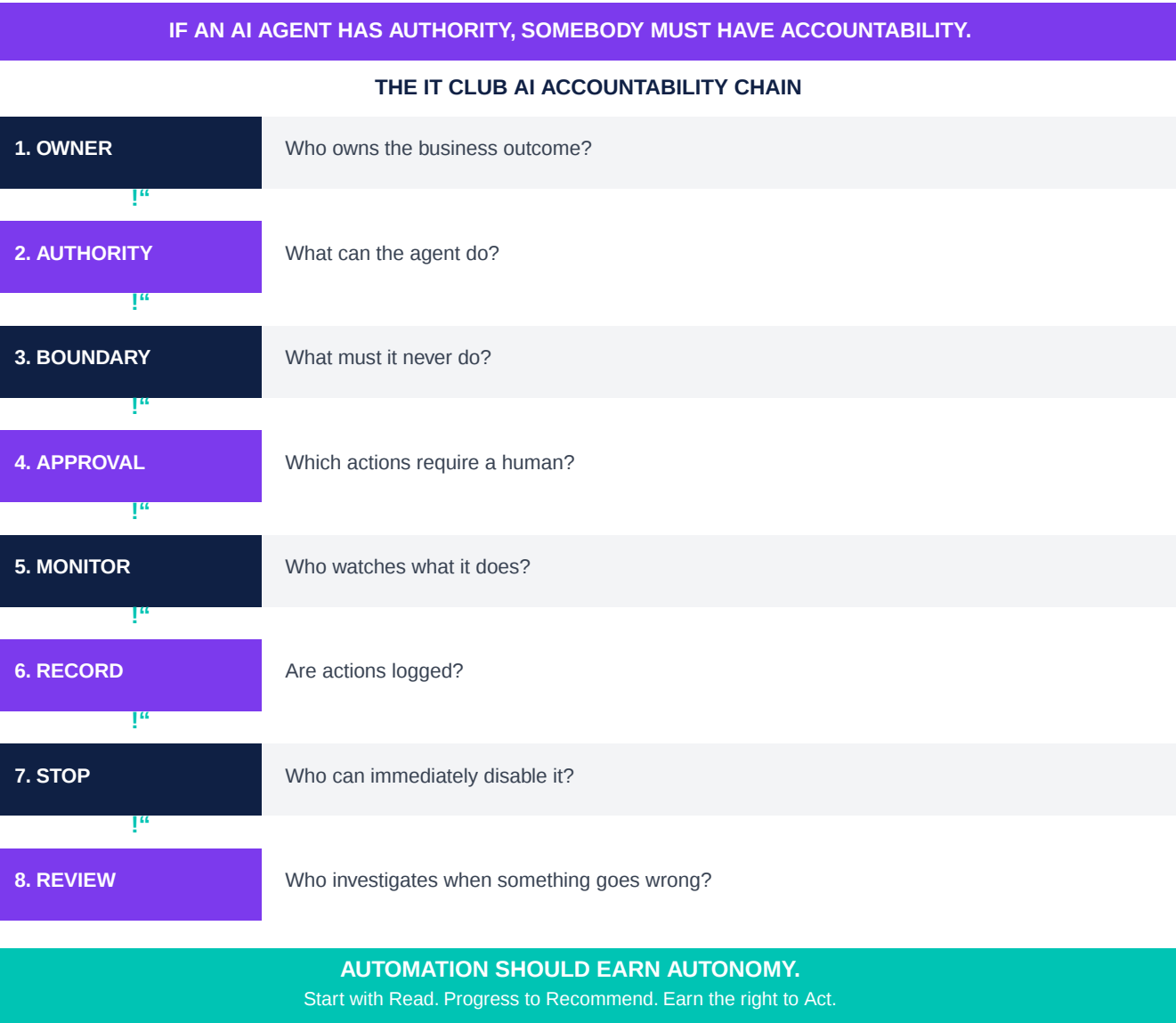


WHO IS RESPONSIBLE

FOR YOUR AI AGENT?

IT Club | AI Governance | itclub.work
Plain-English guidance for business owners



AI Agent Accountability Checklist

OWNERSHIP

- %i Named business owner
- %i Named technical owner
- %i Named risk owner

IDENTITIES

- %i Dedicated identity — not a shared account or employee credentials
- %i Credentials are revocable
- %i Separate test and production access

PERMISSIONS

- %i Least privilege — only the access needed for the defined task
- %i Systems the agent reaches are documented
- %i External actions are limited and understood
- %i Spending limits applied where relevant

HUMAN APPROVAL

- %i High-impact actions require human approval before execution
- %i Exceptions escalate to a named person
- %i Approval-gate process tested before production deployment

LOGGING

- %i Agent actions are logged
- %i Logs are recoverable and retained appropriately
- %i Sensitive data is not unnecessarily captured in logs

SUPPLIER TERMS

- %i AI and platform provider terms reviewed
- %i Data-processing terms understood
- %i Insurance position considered

INCIDENT RESPONSE

- %i Response owner is identified
- %i Evidence retention process understood
- %i Escalation process is defined

KILL MECHANISM

- %i Agent can be disabled immediately
- %i Credentials can be revoked quickly
- %i The process has been tested

REVIEW

- %i Permissions reviewed regularly — not just at deployment
- %i Operational Heartbeat review scheduled
- %i Supplier changes and regulatory updates monitored

AUTOMATION SHOULD EARN AUTONOMY.

Start with Read. Progress to Recommend. Earn the right to Act.

