

Every failure is a missing control — not a malicious model

What goes wrong without AI control, in business terms — and the control that prevents it.

IF THIS HAPPENS	THE BUSINESS CONSEQUENCE	THE MISSING CONTROL
Unknown / shadow AI use	You can't govern what you can't see: unmanaged exposure, failed audits	Inventory & Classification (07)
Vendor AI enabled silently	Enterprise data processed & retained without review — contract & privacy breach	Vendor review (07) · Data Boundary (09)
Excessive AI data access	AI reaches far beyond its need; one prompt can exfiltrate	Identity & Access (08) · Data Boundary (09)
Unauthorised RAG retrieval	Users see documents they were never entitled to — confidentiality breach	Data Boundary Control (09)
Prompt injection via content	Untrusted content hijacks the model into leaking or acting	Input Control (10) · Tool & Action (12)
Recommendation becomes decision	A consequential decision with nobody accountable to a regulator	Output & Decision (11) · Human Accountability (13)
An agent that cannot be stopped	No kill-switch; damage continues while you scramble	Tool & Action (12) · Containment (16)
Incident cannot be reconstructed	You can't prove what the AI saw or did — no defensible audit trail	Monitoring & Evidence (15)
Exception becomes permanent	A temporary risk acceptance quietly becomes standing exposure	Assurance & Governance (14)
Failure has no recovery path	An irreversible action with no rollback or compensation	Containment & Recovery (16)