

AI Agent Control Matrix

Tools, permissions, human authority and evidence for agentic systems.

INTELLIGENT SYSTEMS. PRACTICAL RESULTS.

How this asset operates

Funnel stage	Commercial investigation to build
Audience	Product, engineering, security, privacy, risk and operations leaders
Trigger	An agent will access tools, data or actions
Objective	Make authority and control decisions explicit before implementation
Primary CTA	Complete the matrix before architecture approval
Delivery method	PDF architecture and governance worksheet
CRM action	Attach to opportunity or project control evidence
Follow-up	Security and architecture review
Compliance	Does not replace legal, privacy, security or regulatory review.
KPI	Agents with least privilege, explicit approvals, auditability and tested failure controls

Create one row for every tool or material action. "The agent needs access" is not a control decision.

System identity

Agent / system name

Workflow

Operating owner

Technical owner

Risk owner

Environment

Authority matrix

Tool / action	Purpose	Data	Permission	Human approval	Audit record	Revoke / rollback

Control questions

- ☐ Least privilege is documented
- ☐ External content is treated as untrusted
- ☐ Prompt / instruction hierarchy is protected
- ☐ Outputs are validated before material use
- ☐ High-risk actions require human authority
- ☐ Rate, cost and action limits exist
- ☐ Secrets are not exposed to the model unnecessarily
- ☐ Logging excludes prohibited sensitive data
- ☐ Incident response and shutdown are tested
- ☐ Model / tool changes trigger regression testing

Approval

Open risks

Conditions before release

Approval owner

Date

Next review

Decision record and limitations

Decision or conclusion

Evidence supporting the decision

Material limitations and assumptions

Accountable owner

Review date

Important

Does not replace legal, privacy, security or regulatory review.

PlanckCyber resources are general planning tools. They do not create a client relationship or substitute for qualified legal, privacy, security, financial, accounting, engineering, regulatory or procurement review.