What Should an AI Agent Be Allowed to Do in Your Business?

BUSINESS RISK, COMPLIANCE & GOVERNANCE • Issue 3 learning theme: Permissions, Authority and Oversight

Illustrative figures are not actual client results.

The business problem

A customer service AI assistant can read approved FAQs, but someone also connected it to customer billing records and payment settings.

What business owners need to understand

An AI tool that drafts a response is different from an agent that changes records, sends messages or approves transactions. Grant the minimum necessary permissions and require human approval for sensitive actions.

How to apply it

1. Inventory each AI-connected system and the data it can access.

2. Separate permissions into read, create, change, send, approve and delete.

3. Prohibit unauthorized financial transfers, bank changes and deletion of records.

4. Log actions, assign a human owner and test an emergency shutdown procedure.

Work through the numbers

Assume access controls and review cost $180/month. That is a $2,160 annual operating expense before setup. The direct EBITDA impact is negative until measurable operating benefits or avoided costs are realized. Risk reduction can still justify the expense, but do not present a hypothetical prevented fraud loss as guaranteed ROI.

Annual recurring control cost = monthly operating cost × 12. Evaluate risk using plausible impact and likelihood ranges, not a single unsupported probability.

What the financial statements reveal

Income statement: check recognized sales, direct costs, operating expenses and EBITDA. Balance sheet: check cash, receivables, payables and obligations created by the decision. Cash flow: verify when money actually arrives or leaves. A positive EBITDA change does not guarantee positive cash flow.

The CEO decision

Review cash controls, separation of duties, incident response, contractual obligations, privacy, data retention and audit logs. Security decisions should not depend solely on short-term EBITDA.

Apply it to your business

Choose one AI tool. Write its permitted actions, prohibited actions, required approvals and the person accountable for monitoring.

Your quick review

☐ What is the baseline measure?

☐ What will change and who owns it?

☐ What is the monthly cost?

☐ What is the expected EBITDA effect?

☐ What happens to cash, customer experience and risk?

Continue learning

Explore The Scaling Edge and the Across the Table Business Learning Center for more practical lessons on strategy, financial decisions, AI and business systems.

Read and connect with Across the Table

Across the Table website: https://acrossthetable.biz/

The Scaling Edge newsletter: https://acrossthetablebiz.substack.com/

Across the Table: https://acrossthetable.biz/ | The Scaling Edge: https://acrossthetablebiz.substack.com/