courant
Keep IT Current

A PRACTICAL FIELD GUIDE

AI Security & Compliance

How businesses can adopt AI without losing control: the risks, the governance, and the questions to ask before you scale.

You don't have to choose
between innovation and control

Governance is not "no AI"
it means intentional, managed use

Most businesses are behind
starting now puts you ahead

01 The Real Risks of Unmanaged AI

MOST IMMEDIATE

Data Exposure

Employees paste client records, financials, and strategy into tools that may train on inputs or retain data far longer than you'd expect.

CLOSE SECOND

Compliance Violations

GDPR, HIPAA, and state privacy laws all apply differently. AI use that breaks them invites fines, legal action, and disruption.

QUIETLY COSTLY

Poor Decisions

AI can be confidently wrong, inheriting bias, hallucinating, missing context. Treating output as infallible is the real risk.

EASY TO OVERLOOK

Vendor & Operational Risk

Not every provider is transparent about security, retention, or compliance. Deploying without vetting leaves you exposed.

02 A Governance Framework Answers Three Questions

? What can AI be used for?

? Who is allowed to use it?

? How do we keep it safe?

1. **Define approved use cases**
   Allowed, needs approval, or off-limits, in writing.
2. **Set data handling rules**
   No sensitive or PII input without explicit approval.
3. **Name a governance lead**
   One owner vets new tools before they're deployed.
4. **Put it all in writing**
   Short, practical, readable by everyone on the team.

> **One policy prevents most incidents: when in doubt, ask.**

03 The AI Use Case Risk Spectrum

Low Risk
Generally approved

- Brainstorming & ideation
- Drafting email templates
- Summarizing internal docs
- Generating marketing copy
- General research questions

Medium Risk
Approval + data rules

- Routine data entry
- Analyzing anonymized data
- Client-facing drafts
- Meeting notes with names
- Reports from internal data

High Risk
Off-limits without review

- Client PII or health records
- Critical financial decisions
- Compliance-related work
- Confidential legal documents
- Anything under HIPAA / GDPR

Always verify AI output before acting. Even low-risk tasks benefit from human review.

04 Before You Sign a Vendor

NON-NEGOTIABLE: MUST HAVE

- Data encrypted in transit and at rest
- Independent security audits, conducted regularly
- Your data is **not** used to train their models, or you can opt out
- Clear retention policy and deletion process
- Financially stable, with a credible track record
- Willing to answer governance and compliance questions

STRONGLY RECOMMENDED

SOC 2 or ISO 27001 certification

Security documentation on request

Data isolation or private deployment option

Tests for bias, hallucinations, and errors

Ability to flag or disable harmful output

Transparent about limits and failure modes

Red flag

A vendor that dismisses your governance questions or resists transparency. Re-score every vendor annually; the standards move fast.

05 Where Does Your Business Stand?

01 Do you have documented policies about which AI uses are approved?

02 Are employees clear on what data they can and can't share with AI?

03 Have you evaluated the vendors behind the tools you already use?

04 Do you understand your compliance obligations around data privacy?

0 YES	1–2 YES	3 YES	4 YES
Starting Out	**In Progress**	**On Track**	**Well Governed**
Build now	Fill the gaps	Almost there	Keep reviewing

Good AI security doesn't require perfection. It requires intention.

We help New Orleans business owners assess their current AI practices, identify compliance gaps, and build a governance framework that fits how they actually work.

Talk to Courant →

gocourant.com
504.454.6373 · New Orleans, LA