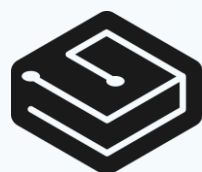


Leading Through Uncertainty:

AI Governance, Cyber Risk and
Organizational Resilience



LAYER9
IT MANAGEMENT



ORGANIZATIONAL READINESS

The Foundation for Secure AI Adoption

People

Clear expectations, training and accountability

Process

Approved use cases and consistent review

Data

Defined access, privacy and protection

Technology

Secure tools, integrations and vendors

AI readiness is an organizational capability



A REAL-WORLD EXAMPLE

AI Adoption Often Begins Without a Launch



WHAT LEADERSHIP BELIEVED

“We are preparing to explore AI.”

WHAT THE ASSESSMENT REVEALED

Adoption was already underway

Visibility gives leadership a starting point.

AUDIENCE CHECK

Where Is Your Organization Today?

Choose the statement that best reflects your current approach to AI.



KEEP IN MIND:

Different departments may be at different stages

The Visibility Gap

Formal approval and actual organizational behavior do not always match.

WHAT LEADERSHIP MAY SEE

“We have not formally adopted AI.”

“Our approved vendors are controlled.”

“Sensitive data stays in approved systems.”

“IT knows which applications are in use.”



WHAT MAY ACTUALLY BE HAPPENING

Employees may already use public tools.

Existing platforms may have added new AI features

Information may be copied into AI prompts.

Browser tools may sit outside the normal review process

You cannot govern what you cannot see

AI Creates Opportunity but Adds Responsibility

THE OPPORTUNITY

15.9%

less time working in notes

Clinicians using an AI scribe

- Reduce administrative burden
- Give staff time back
- Support a better patient experience

Source: Pearlman et al., JAMA Network Open, 2025

THE RESPONSIBILITY

Secure adoption creates the conditions for innovation to succeed

- 01 Protect the data**
Use approved tools and control what information they can access.
- 02 Validate the output**
Review important information before it influences care or action.
- 03 Preserve accountability**
A person owns the decision, even when AI supports the work.

AI Also Creates Opportunity for Bad Actors

AI makes familiar fraud easier to personalize and harder to recognize.

DEEPPFAKE ATTACK EXPOSURE

62% of organizations were hit by a deepfake attack in the previous 12 months.

IMAGES

CLONED VOICES

VIDEO

ONLY 40%

Of healthcare professionals said their security awareness training addressed emerging threats such as deepfakes

Three Steps Leaders Can Take Now

A simple way to reduce risk while supporting responsible AI use.

STEP

01

SEE IT

Discover the AI tools and features already in use.

COMPLETE A SHADOW IT SCAN

STEP

02

GUIDE IT

Define approved tools, data boundaries and human review.

CREATE AN AI USAGE POLICY

STEP

03

VERIFY IT

Validate important output and confirm sensitive requests.

REQUIRE INDEPENDENT VERIFICATION

These steps reduce hidden use and make responsible AI adoption easier.

STEP 1: SEE IT

Know what is already happening.

Leadership should be able to answer:



Which AI tools are employees using?



Which existing vendors have added AI features?



What information is being entered or accessed?



What problems are employees trying to solve?



Practical action

Conduct a short employee survey or Shadow IT Scan



STEP 2: GUIDE IT

Create a safe path for responsible experimentation.

Clear guidance gives employees the confidence to innovate while keeping your organization and your data protected.



Approved tools

Where can AI be used?



Data boundaries

What information cannot be entered?



Human ownership

Who must review and approve the result?



PRACTICAL ACTION

Publish a one-page AI acceptable-use guide.

Make the safe path easier to understand and easier to follow.



Verify before you act.

For AI-generated information:

-  Confirm important facts using a trusted source.
-  Require human review based on potential impact.
-  Document who owns the final decision.

For suspicious requests:

-  Call a known number.
-  Use a second communication channel.
-  Require secondary approval for sensitive actions.
-  Never use contact information supplied in the request itself.



Practical action

Establish a verification rule for high-risk requests.

Stop. Confirm. Then act.



FROM INSIGHT TO ACTION

How to Get Started Today

A practical 30-day plan for secure AI adoption.

1

Week 1

See It

Understand what is already happening.



Survey employees on current AI use.



Inventory vendors with AI-enabled features.



Identify the problems employees are trying to solve.



Flag any use involving sensitive or patient information.

2

Week 2

Guide It

Create simple rules before creating complex governance.



Name an executive owner for AI.



Define approved and unapproved tools.



Establish basic data boundaries.



Publish a simple AI usage policy.

3

Weeks 3–4

Verify It

Build the behavior into the organization.



Train employees on **Stop. Confirm. Then act.**



Establish verification rules for high-risk requests.



Define when human review is required.



Select one controlled AI pilot and measure the outcome.



You do not need a complete AI strategy to get started.

You need visibility, clear boundaries, and one safe place to begin.

SEE IT. GUIDE IT. VERIFY IT.

PEOPLE

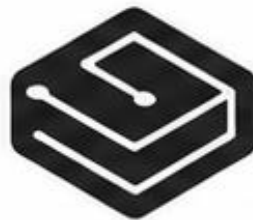
PROCESS

TECHNOLOGY

A SAFER
TOMORROW

Q&A

Questions, discussion, or next steps?



LAYER 9
IT MANAGEMENT

Let us build your AI Strategy