START HERE — NO TECHNICAL BACKGROUND REQUIRED

SECURE USE OF AI

AI is already in your firm. **The question is not whether to allow it — it is whether you can show someone how you control it.** This page explains the whole idea in about five minutes.

WHERE AI COMES FROM | FIVE HABITS | THE ONE-PAGE RULE | WHAT TO DO FIRST | ALIGNED TO NIST AI RMF · OWASP · SANS · ISO 42001

WHAT IS THE RISK, REALLY?

AI is a very fast, very confident assistant that **remembers what you tell it** and will happily repeat it. The risk is what your people put in, what comes out unchecked, and criminals using the same tools on you.

WHY DOES IT LAND ON US?

No regulator has written a separate AI rulebook. They did not need to. **Your existing duties already cover it** — supervision, protecting client information, keeping records, and responding to incidents.

WHAT DOES "GOOD" LOOK LIKE?

Not a ban, and not a free-for-all. Good looks like **approved tools, clear rules, a human accountable for output, and a record you can show** if someone asks. That is the entire job.

01 AI GETS INTO YOUR FIRM THREE WAYS

THE BIG IDEA

Most firms think about only the first one. All three are your responsibility, and each needs a different answer.

WAY 01

YOUR PEOPLE USE IT

Staff use ChatGPT, Copilot, Claude, or an AI note-taker to move faster. Usually with good intentions, usually without asking.

WHAT THAT LOOKS LIKE

"I pasted the client's statement in so it could summarize the holdings for me."

THE ANSWER

Give people a short list of approved tools and one hard rule: client information never goes into anything that is not on the list.

WAY 02

YOUR VENDORS ADDED IT

Your CRM, planning software, custodian portal, and email system all switched on AI features. You did not buy them and may not have been told.

WHAT THAT LOOKS LIKE

"Our CRM now writes meeting summaries automatically. Nobody asked where that data goes."

THE ANSWER

Ask every vendor the same few AI questions, and ask again each year — not just when you first sign them up.

WAY 03

CRIMINALS USE IT ON YOU

Attackers have the same tools. They can now copy a voice from a few seconds of audio and write flawless email in your CEO's style.

WHAT THAT LOOKS LIKE

"The client called and authorized the wire himself. I recognized his voice." It was not him.

THE ANSWER

Verify every money movement on a separate channel you start yourself. A voice or a face is no longer proof of who someone is.

02 FIVE HABITS OF A FIRM THAT USES AI SAFELY

WHAT SECURE USE LOOKS LIKE

If your firm does these five things consistently, you have covered the large majority of the risk. Everything else is refinement.

01 APPROVED TOOLS ONLY

A short published list of AI tools the firm has vetted and pays for, plus an easy way for staff to ask for a new one.

WHY IT MATTERS

Personal free accounts leave no record and no protection.

02 NO CLIENT DATA BY DEFAULT

Client names, account numbers, statements, and contracts stay out of AI tools unless the firm has approved that specific use.

WHY IT MATTERS

This is the single most likely way your firm leaks information.

03 A HUMAN SIGNS OFF

AI drafts. People approve. Anything going to a client, a regulator, or a trade gets read by a named person first.

WHY IT MATTERS

AI is fluent, confident, and sometimes flatly wrong.

04 KEEP A RECORD

Know who used AI, for what, and where the resulting record is stored — in the same archive as everything else.

WHY IT MATTERS

Record-keeping rules did not change because a machine helped write it.

05 CHECK YOUR VENDORS

Ask whether they use AI, whether your data trains it, who else touches it, and whether you can turn it off.

WHY IT MATTERS

If they lose your client data, it is still your notification to make.

THIS IS NOT ABOUT SAYING NO

Firms that use AI well are faster at research, drafting, and client service — and firms that use AI in their **security** operations cut roughly **$1.93M off the cost of a breach** and contained incidents **65 days faster** than firms that did not. The goal is not to slow your people down. It is to let them move quickly in a way that holds up when a client, an auditor, or an examiner asks how you did it.

03 THE ONE-PAGE RULE YOU CAN HAND TO STAFF TOMORROW

PRINT AND CIRCULATE

If you adopt nothing else from this overview, adopt this. It is short enough that people will actually remember it.

YES — GO AHEAD

NO APPROVAL NEEDED, USE AN APPROVED TOOL

- ✓ **Research and learning.** Explain a concept, summarize a public article, compare regulations.
- ✓ **Starting a draft.** A first pass at a memo, agenda, job posting, or internal policy — that you then edit.
- ✓ **Rewriting your own words.** Making something you already wrote shorter, clearer, or friendlier.
- ✓ **Internal work with no client data.** Training material, checklists, meeting prep, brainstorming.
- ✓ **Asking how to do something.** Formulas, software steps, "how do I structure this analysis."

STOP — ASK FIRST

CHECK WITH COMPLIANCE BEFORE YOU DO IT

- × **Anything with client information.** Names, account numbers, statements, tax documents, holdings, balances.
- × **Anything going out the door unread.** Client emails, marketing, or filings that no person reviewed.
- × **Advice, suitability, or trades.** AI does not decide what is right for a client.
- × **A new AI tool or feature.** Including one that appeared inside software you already use.
- × **Anything involving money movement.** No exceptions, no matter who is asking or how urgent it sounds.

04 IF SOMEONE ASKS YOU TO MOVE MONEY

POST THIS WHERE WIRES ARE APPROVED

A voice can now be copied from about three seconds of audio, and nearly half of AI-driven attacks are impersonation. The defense is a habit, not a technology.

VERIFY BEFORE YOU MOVE

EVERY WIRE · EVERY BANKING CHANGE · EVERY TIME · NO EXCEPTIONS FOR EXECUTIVES

1 Slow down.
Urgency is the trick. No real request is ruined by a ten-minute pause — say that out loud.

2 Call back yourself.
Use the number already in your system, never the one in the request. A supplied number rings the criminal.

3 Get a second person.
Two people, and confirmation on a different channel than the one the request came in on.

4 Check the account.
They can fake a voice or a face. They cannot fake the receiving account — match it to your records.

05 WHERE TO START

FIRST STEPS

Three steps, in this order. The first two you can do this month without spending anything.

1 THIS MONTH

- Publish the approved tool list and the one-page rule from section 03
- Brief everyone who touches a wire on the verify habit
- Tell staff how to request a tool, so nobody has a reason to go around you

2 THIS QUARTER

- Write down every AI tool in use, including vendor features you did not buy
- Adopt a short written AI policy and have people sign it
- Add the AI questions to your vendor reviews

3 THIS YEAR

- Have the nine essential controls assessed and scored independently
- Update supervisory procedures and incident response to name AI
- Run one practice scenario, and keep the evidence in one place

ALSO IN THIS SERIES

- **08 · Plain-English Overview**
  You are reading it. The concepts in five minutes — share widely.
- **09 · Secure Use of AI Cheat Sheet**
  Four pages: risk model, use-case tiering, the SEC / FINRA / NYDFS map, twelve-control self-score.
- **10 · The Nine Essential Controls**
  The framework behind our assessment, scored on design, implementation, testing, and evidence.

NOT SURE WHERE YOUR FIRM STANDS?
FIND OUT IN TWO TO THREE WEEKS

Security Basecamp has focused exclusively on cybersecurity for regulated industries since 2013 — no general IT practice and no product-vendor bias. Hundreds of risk assessments, penetration tests, and vendor risk assessments for broker-dealers, RIAs, insurance companies, private equity firms, and FinTech providers. Our mission is to be the most capable cybersecurity firm serving regulated industries, combining deep technical expertise, regulatory fluency, and practical execution.

WHAT WE DO

- **Cybersecurity Risk Assessments**
- **Cloud Security** — AWS, Azure, M365
- **Breach Response & Forensic Analysis**
- **vCISO / CISO Support Services**
- **Vulnerability Mgmt & Penetration Testing**
- **Secure Use of AI**
- **Third-Party & Vendor Risk Assessments**
- **Threat Intelligence & Monitoring Advisory**

CISSP | SECURITY+ | PENTEST+ | GIAC | OSCP | REGULATED INDUSTRIES ONLY

BE SECURE. BE COMPLIANT.

ALIGNED TO NIST AI RMF 1.0 AND GENERATIVE AI PROFILE · OWASP TOP 10 FOR LLM APPLICATIONS · SANS CRITICAL AI SECURITY GUIDELINES · ISO/IEC 42001 · SEC REGULATION S-P AND EXAM PRIORITIES · FINRA NOTICE 24-09 · NYDFS PART 500. BREACH FIGURES: IBM / PONEMON 2026. GENERAL INFORMATION, NOT LEGAL ADVICE.

TALK TO US

WEB securitybasecamp.com
CALL (949) 330-0899
EMAIL info@securitybasecamp.com

A SECURE USE OF AI ASSESSMENT GIVES YOU

- A plain-language picture of where you stand, including AI you did not know about
- Where client information could get out, and what is stopping it
- A prioritized to-do list with owners and dates
- A summary your CCO can present to a board or an examiner

POWERED BY EntrustIQ

EntrustIQ is Security Basecamp's sister company, founded in 2025. **A report is accurate the day it is signed and decays from there.** EntrustIQ keeps your controls, evidence, and scores current between assessments.