Security Controls Are Financial Controls

Protecting transactions, contracts, and government data

Georgia Fiscal Management Council Annual Training Conference
Savannah, Georgia • September 2026

Why this belongs at FMC

The conference agenda is already about controls, modernization, fraud, and AI.

FISCAL MANAGEMENT

Budget • accounting • audit • procurement • payment integrity

→

SECURITY CONTROLS

Email • identity • contracts • incident reporting • data handling

→

PUBLIC TRUST

Protect the transaction, protect the contract, protect the data

45 minutes allotted: ~35 minutes of content, then time for questions.

The core idea

Cybersecurity is now embedded in the financial control environment.

“If a control protects how money moves, obligations are created, or sensitive or sensitive information is used… it is a financial control.”

Protect the transaction

Email, payment changes, invoice fraud, rapid reporting

Protect the contract

RFP requirements, vendor obligations, audit rights, subcontractors

Protect the data

Approved AI tools, data minimization, human validation

1 • PROTECT THE TRANSACTION

The attack has moved into the business process

An attacker may not need to “break” the the financial system. They may only need to to persuade an authorized employee to use it. use it.

Example: fraudulent invoices, altered ACH instructions, payment redirection

Business email compromise is payment fraud with a keyboard

The risk is not “email” in isolation — it is what the email asks the organization to do.

From: Known Vendor
Subject: Updated ACH instructions

“We recently changed banks. Please use the use the attached updated payment instructions for all future invoices.”

Control trigger: a request to change where money goes

$55.5B

global exposed losses tied to BEC / email account account compromise reported by FBI IC3 data, data, Oct. 2013–Dec. 2023

The control response: move verification outside the email conversation.

Email security as a financial control

Do not rely only on whether a message “looks suspicious.” Ask what business action it requests.

Identify

Requests to change bank details, redirect payments, bypass approvals, or act urgently.

Verify

Use known contacts and established records — not the phone number or link in the email.

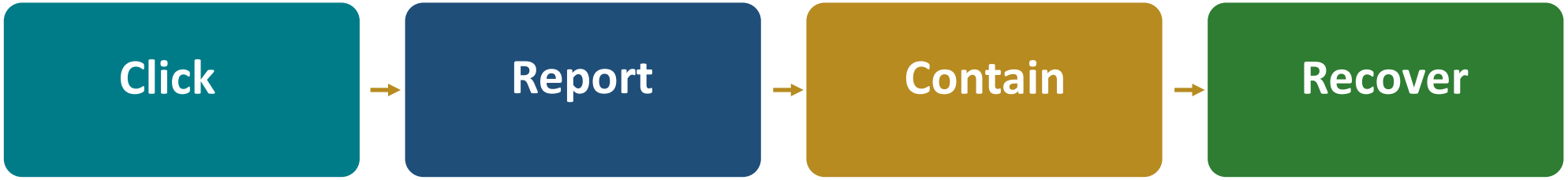
Document

Record who verified, what changed, when it changed, and what evidence supports the change.

An email can initiate a financial process. It should not, by itself, authorize a high-risk change.

If you clicked, report immediately

Fast reporting is not an admission of failure; it is a containment control.



The security team does not need embarrassment. It needs facts: Did credentials get entered? Did entered? Did something download? Did payment information change? Can we stop it now? now?

Finance professionals are part of the security architecture architecture

People are not merely the “weakest link.” Often, they are the last control standing.

Professional skepticism

- Does this request fit the normal process?
- Is the urgency trying to bypass controls?
- Can I verify through records I already trust?
- Would I be comfortable explaining this change to an auditor?

Security translation

- Stop payment redirection
- Report suspicious activity
- Preserve evidence
- Protect public trust

Your judgment may be the control that prevents the loss.

2 • PROTECT THE CONTRACT

The best time to negotiate security is before award

- Before the vendor has your data
- Before the vendor has your money
- Before implementation pressure narrows your options

Weak contract language turns a security incident into a contract dispute.

What belongs in RFPs and contracts

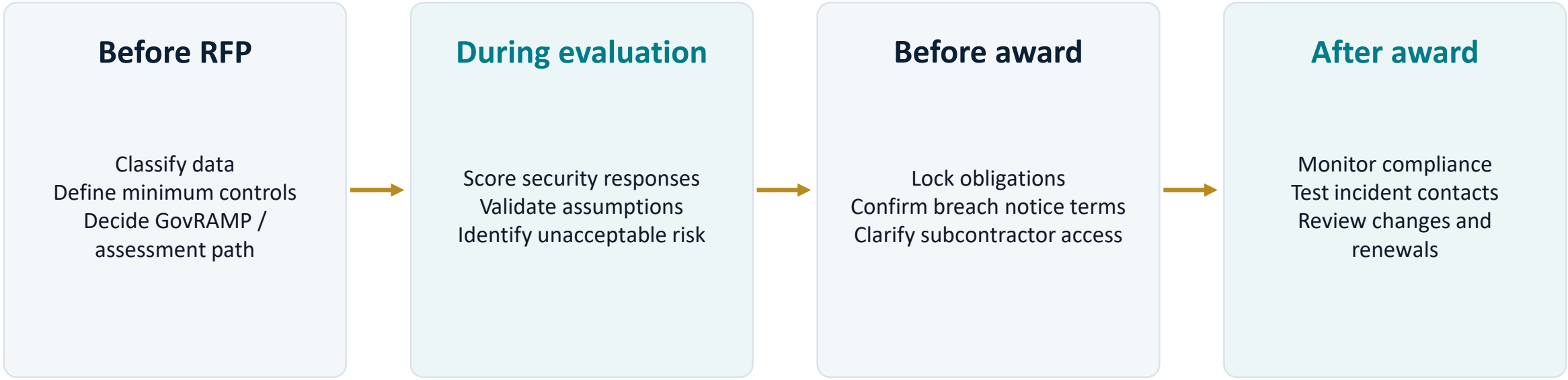
These are security controls, procurement controls, and financial-risk controls.

Breach notification	When does the clock start, and who must must be notified?
Audit rights	How do we verify performance against the contract?
Encryption	How is data protected in transit and at rest?
Subcontractors	Who else touches the service or data?
MFA	What prevents a stolen password from becoming access?
Data ownership	What can the vendor do with government information?
Incident response	Will the vendor preserve evidence, logs, and cooperation?

Procurement should not buy the risk first and negotiate the control later.

A procurement control model

Security should be built into the lifecycle, not bolted on after vendor selection.



Cybersecurity diligence belongs where procurement risk decisions are made.

3 • PROTECT THE DATA

AI starts with one question

“Am I authorized to give this this information to this system?” system?”

The tool may be useful and still be the wrong wrong place for particular government information.

Information that should make you stop before using AI

AI

Especially with unapproved or personal AI tools.

Financial

Banking info
ACH files
Tax data
Payment records

Personnel

Employee records
Salary details
Benefits data
Performance info

Procurement

Confidential bids
Evaluation notes
Vendor pricing
Negotiation strategy

Citizen / offender offender

PII
Benefits cases
Health data
Justice information

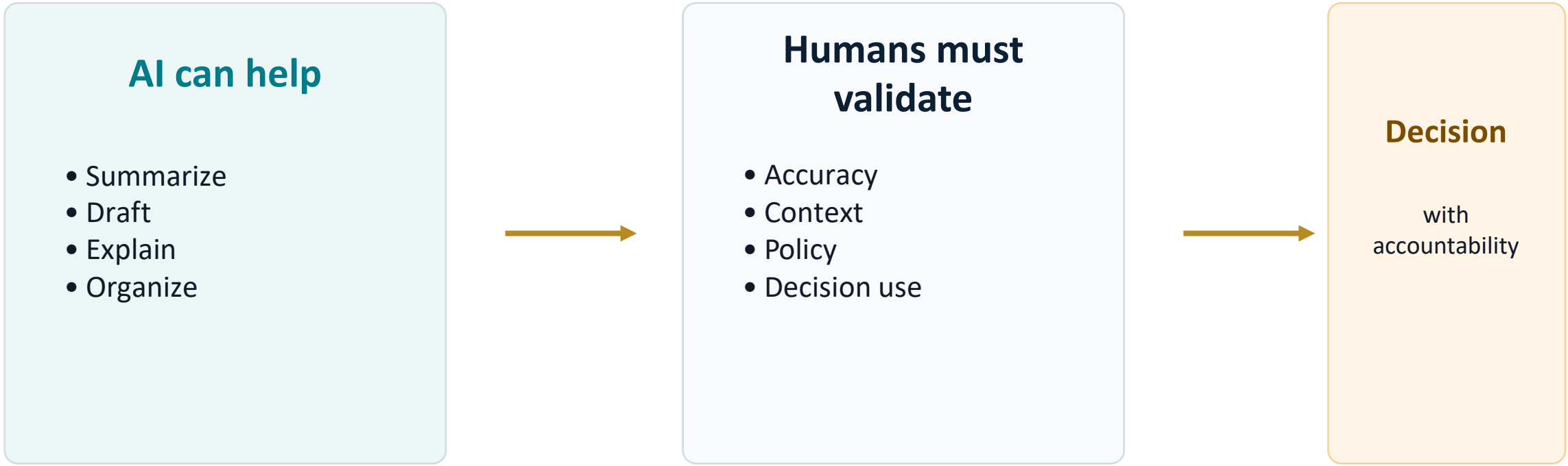
Security

Passwords
Network diagrams
Findings
Incident details

If you would not send it to an unknown outside company, do not paste it into an unapproved AI tool. unapproved AI tool.

AI output is draft work, not final authority

Automation changes how work is performed. It does not eliminate accountability.



Do not turn a draft into an official decision without review.

The control crossover

Different vocabulary, same control objective.

Cybersecurity control	Financial-control objective
MFA	Prevents stolen credentials from authorizing access or payment changes
Encryption	Protects records, files, and payment data from unauthorized disclosure
Incident reporting	Creates early detection and limits loss when something goes wrong
Audit rights	Lets the State verify vendor performance and evidence of control
Data ownership terms	Preserves authority over government information
Human AI review	Prevents unverified output from becoming an official decision

Five questions to take back to your agency

These quickly reveal where cyber risk has become financial risk.

1. **Can one email change where our money goes?**
2. **Do employees know exactly how to report a cybersecurity mistake?**
3. **Are security requirements defined before procurement begins?**
4. **Do our contracts say what vendors can do with our data?**
5. **Do employees know which AI tools are approved and what data may be used?**

What I’m asking of finance leaders

Bring your control discipline into the cybersecurity conversation.

Pause

Treat payment-change requests as as control events.

Verify

Use trusted records, records, not the channel requesting requesting the change.

Involve

Bring security and privacy in before procurement decisions are locked.

Limit

Use approved AI tools and minimize sensitive data.

Report

Escalate suspicious activity quickly and without fear.

The goal is not more friction. The goal is stronger assurance before public money or public or public data moves.

Questions

Security controls are financial controls.

Thank you.