What Public Sector Leaders May Miss in NIST CSF Assessments

IT Risk & Compliance

2026 Public Sector Seminar

forvis mazars

Agenda

1. What CSF 2.0 changed and who it changed it for
2. Five blind spots that hide inside “good” scores
3. A better way to run the assessment
4. What to do next

01

What CSF 2.0 changed and who it changed it for

CSF 2.0 Changed the Accountability Model

In February 2024, NIST introduced a sixth core function: **Govern**. It covers:

- Risk tolerance and oversight
- Roles and authority
- Policy and accountability
- Supply chain risk

Before	After
Then (implicit): IT-owned framework	Now (explicit): leadership accountability is in-scope
Governance inferred	Govern function is a first-class pillar
Supply chain treated as a topic	Supply chain elevated (GV.SC)

When we say “leadership,” we mean executive, business, financial, and technology leaders collectively - including CIOs, CISOs, and IT leadership - not instead of them.

The Govern Function

- CSF 2.0's Govern function makes leadership accountability explicit (risk tolerance, oversight, roles, supply chain)
- Many leaders still assume CSF is "an IT exercise"
- Result: Govern is often answered by IT (or underscored), so the assessment starts with a hidden gap
- **And that gap cascades** into the other four blind spots you're about to see
- CSF is no longer just an IT framework
- Leadership is now explicitly "in scope"
- Govern is often:
  - Scored on leadership's behalf
  - Or intentionally / unintentionally underscored due to uncertainty

If leadership isn't engaged early, even a thorough CSF assessment can produce scores that feel reassuring—but hide the risks that matter most.

"Who answered the Govern questions in your last CSF assessment?"

"If it wasn't leadership, your assessment may have missed the point."

forvis mazars

Why “Nothing Happens” After So Many CSF Assessments

- Millions spent across on assessments and maturity scoring
- Gaps documented, risk statements written, profiles delivered
- And yet: priorities don’t change, funding doesn’t move, risk persists

What we just discussed explains *why* leadership is in scope. This explains *why sometimes nothing changes anyway*.

This isn’t because assessments are wrong. It’s often because decisions never happened.

Assessments Inform IT. Change Requires Leadership Involvement.

IT's Role

- Run technical programs
- Control maturity and gaps
- Risk scenarios and options
- Program status and trend data

Leadership's Role

- Risk tolerance
- What cannot fail
- What gets funded first
- What gets deferred and why

Reminder: When we say "leadership," we mean executive, business, financial, and technology leaders collectively - including CIOs, CISOs, and IT leadership - not instead of them.

forvis mazars

What This Talk Is (and Is Not) About

Why do we keep doing assessments and still feel exposed?
Because assessment results rarely translate into leadership decisions.

Are we failing because our teams don't understand cybersecurity?
No. Most organizations can identify gaps, the challenge is prioritizing, funding, and validating them.

Is this about more rigor, more controls, or higher scores?
No. Assessments can be done with fewer cycles, earlier decisions, and clearer ownership.

What changed that makes this urgent now?
CSF 2.0 explicitly puts leadership accountability in scope through the Govern function.

> **This is not a technical CSF walkthrough.**
> It's about why assessments don't change outcomes - and how to produce decisions faster, without expanding scope or effort.

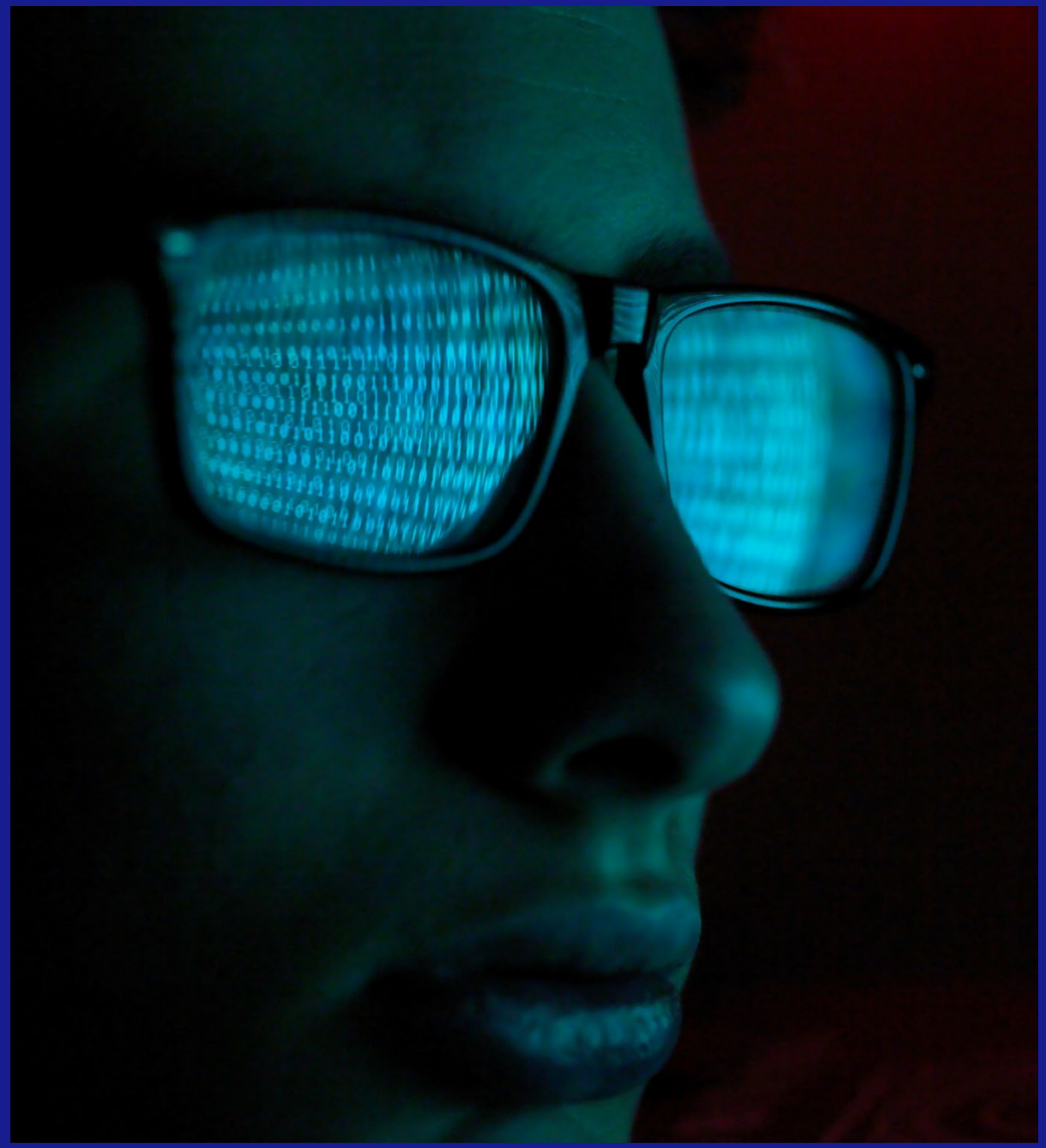
Same framework. Fewer cycles. Earlier decisions.

forvis mazars

Now that leadership is explicitly in scope, here’s what can break when assessments don’t adapt.

02

Five blind spots that hide inside “good” scores

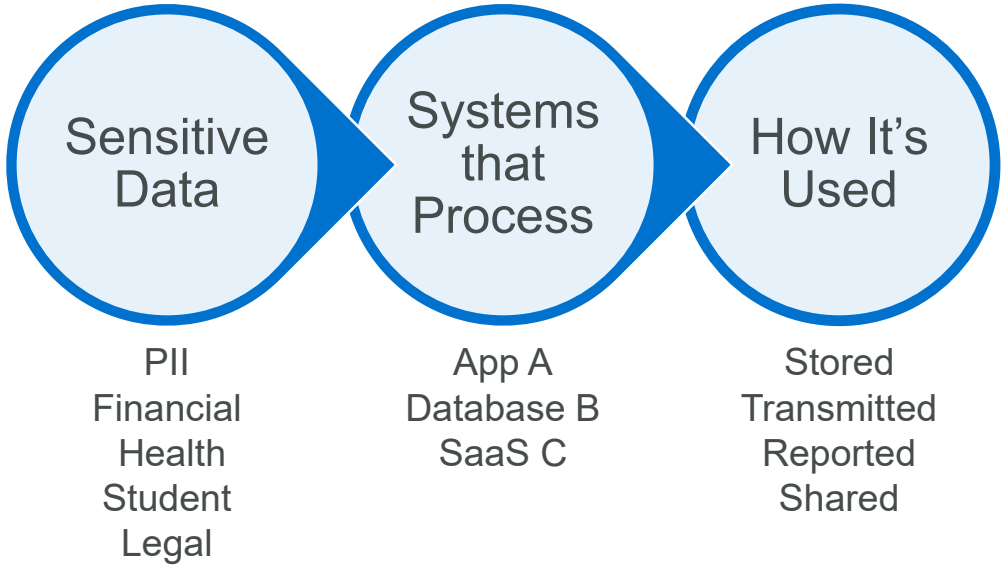


1. Assessments Don’t Start with a Documented Data Inventory

Theme: Data visibility failure

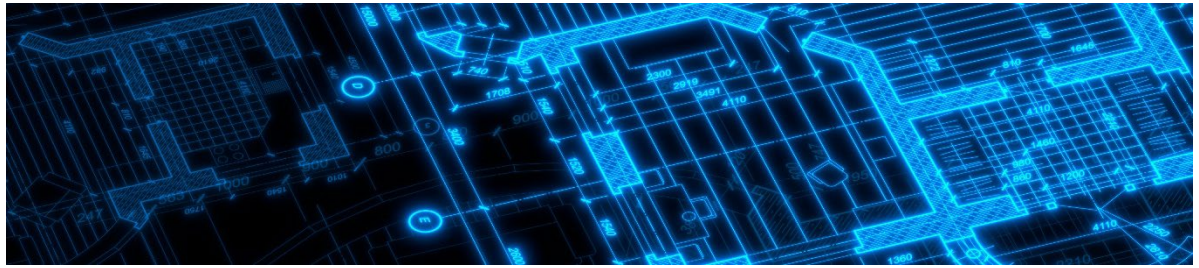
- Many CSF assessments are conducted without knowing:
  - Data types and sensitivity
  - Data locations, movement, and use
  - Regulatory requirements based on data types
- In practice, sensitive data is often not fully identified, tracked, and analyzed

If you don’t understand the data, you can’t accurately assess cyber risk.



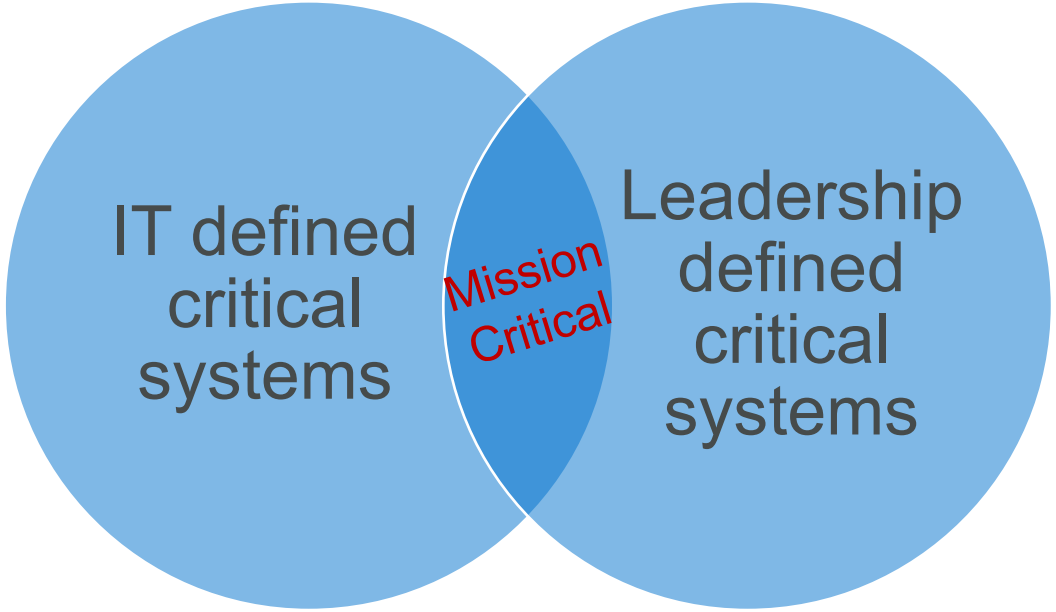
2. Critical Systems Are Often Poorly Identified or Disagreed Upon

Theme: Scope & prioritization failure

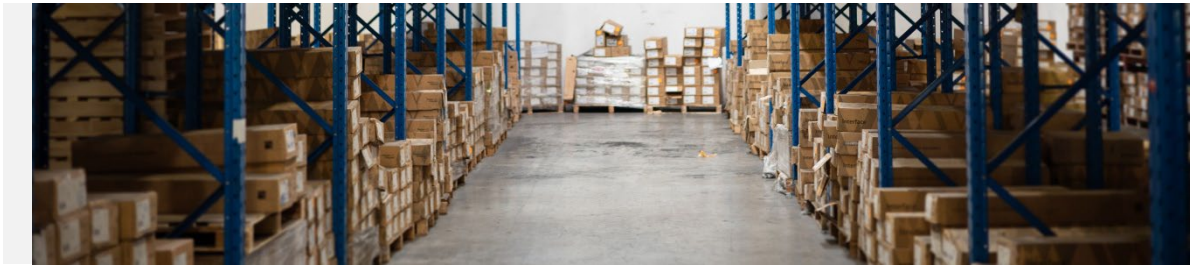


- CSF assumes organizations agree on what systems are truly mission-critical
- In practice, IT and leadership often define “critical” very differently
- When “critical” isn’t agreed, control scores lose operational meaning

Technically accurate scores can still misrepresent real operational risk.



3. Third-Party and Supply Chain Risk Is Often Underscored
Theme: Boundary failure



- CSF 2.0 elevated supply chain risk (GV.SC) for a reason
- Public sector environments are:
  - Highly vendor dependent
  - Heavily shared and outsourced
- Yet supply chain often scores as low risk

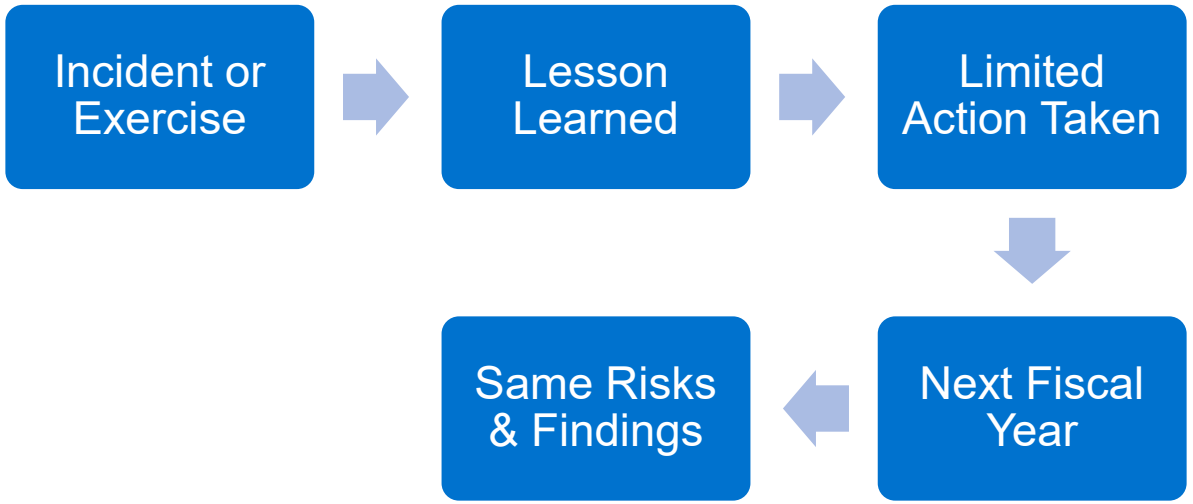
Your greatest exposure may not be inside your firewall.

Vendor Type	Dependency	Data	Operational	Contract	Owner
Tech					
Cloud					
Data					
Legal					
Cyber					
Materials					

4. Incidents, Exercises, and Near Misses Don’t Change Priorities

Theme: Lessons learned failure

- Organizations investigate incidents, conduct tabletop exercises, and document near misses
- After-action reports and lessons learned are produced
- But outcomes sometimes do not translate into:
  - Funding changes, ownership decisions, timelines for remediation
- Operations often return to “normal” with the same risk profile



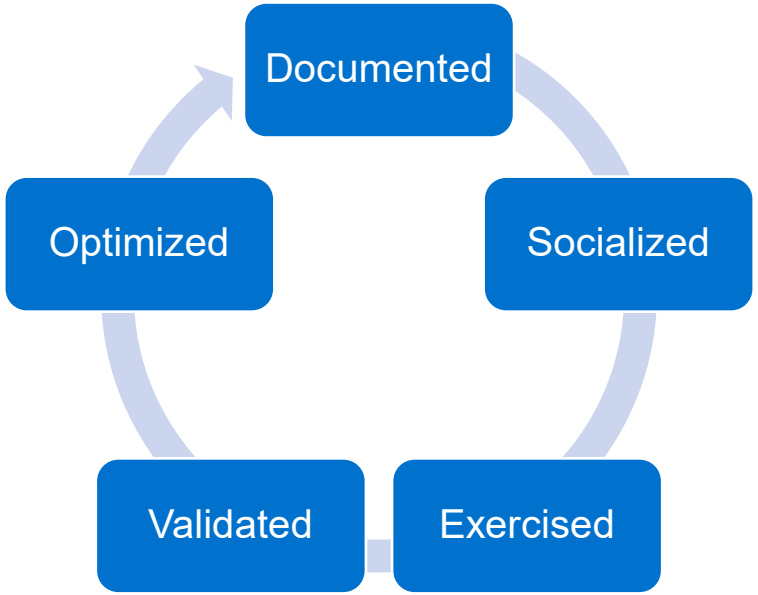
Real signals of risk are observed, but not acted upon.

5. Documentation is Not the Same as Tested Capability

Theme: Capability validation failure

- Incident response plans exist. Have they been exercised?
- Recovery procedures are written. Have they been executed?
- Assessments sometimes accept documentation as evidence

Can we do this when it really matters?



The 5 Blind Spots (and What Each One Breaks)

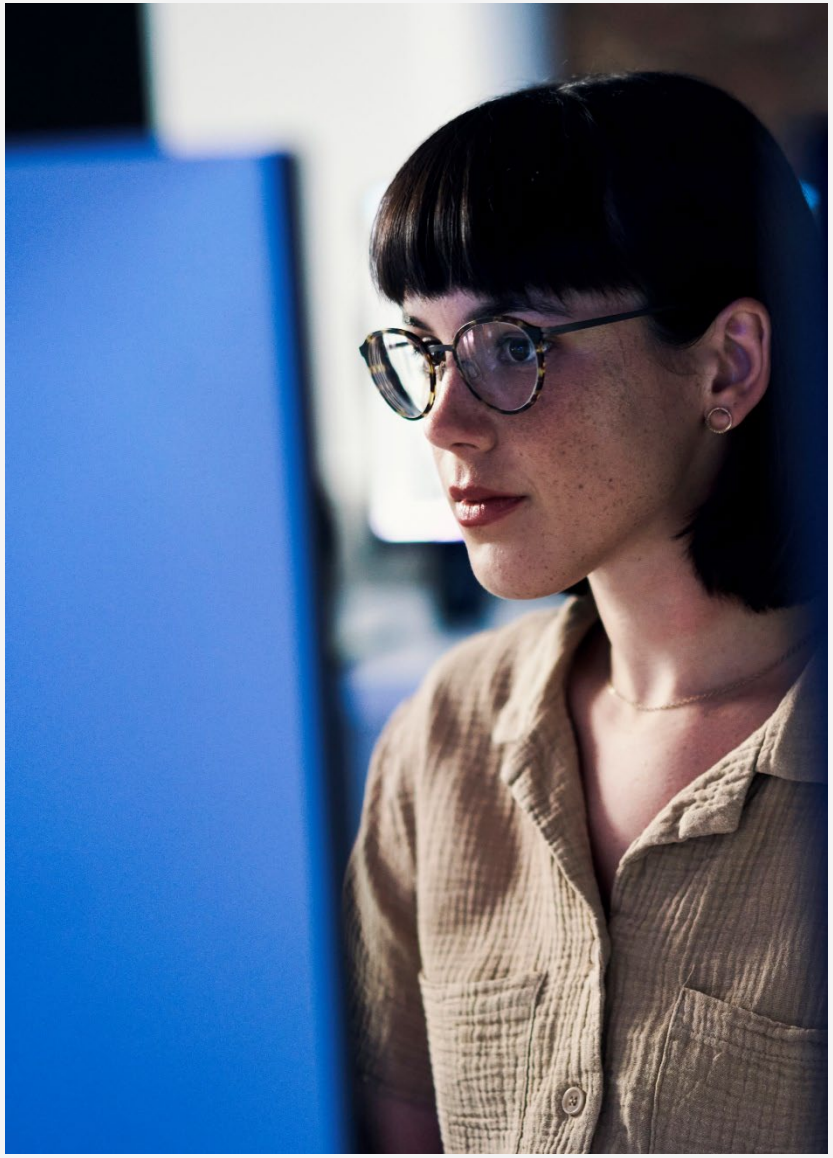
These aren't isolated issues. They are five ways assessment results consistently fail to translate into leadership action.

Blind spot	What it breaks (the practical consequence)
1) Assessments don't start with a documented data inventory	Risk impact is misunderstood before prioritization even begins; sensitive data exposure, regulatory impact, and breaches are underestimated.
2) Critical systems are often poorly identified or disagreed upon	Prioritization fails: the assessment treats everything equally, while operations cannot.
3) Third-party and supply chain risk is often underscored	Major exposures sit outside your firewall; vendor dependency isn't managed as mission risk.
4) Incidents, exercises, and near misses don't change priorities	Real warning signs are observed, but not funded owned, or acted upon and the risk persists.
5) Documentation is not the same as tested capability	Plans exist, but performance under pressure is unknown - until the incident.

Common Technical Gaps Leaders Assume Are “Handled”

Technical gaps usually persist not because teams don’t know about the risk, but because of lack of communication, validation, and funding.

- Cyber technical assessments don’t cover full environment (*e.g.*, internal, external, apps)
- Backup and recovery procedures exist, but haven’t been restored in production
- Incident response plans documented, but exercises aren’t related to high-risk scenarios
- Disaster recovery plans in place, but not all business-critical systems have a plan
- Access rights reviews performed, but do not include IT users
- Asset inventory tools exist, but inventory is not complete or up to date
- Enterprise security controls in place, but do not exist at critical systems
- **These are not assessment failures. They’re decision and prioritization failures.**



forvis mazars

03

A better way to run the assessment

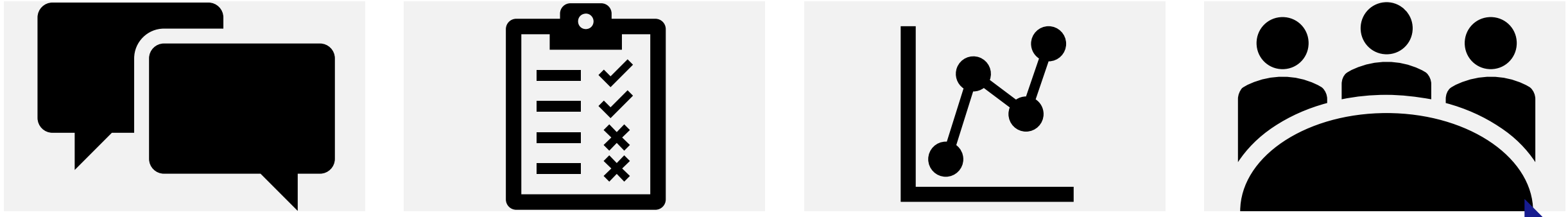
Full Coverage. Less Noise. Better Decisions.

Assessment Principles:

- Maintain full CSF coverage across all six functions (no control areas removed)
- Evaluate real cyber and risk capability, not just documentation (including execution, dependencies, and evidence quality)
- Shift the primary output
  - From documentation completeness
  - To decision-ready insights and tradeoffs
- Design for leadership and technology engagement, not assessment volume

The goal isn't to do more assessment work. It is to get to defensible decisions sooner, without sacrificing CSF coverage.

A Practical Assessment Model That Works



Fewer meetings – Less documentation – Earlier decisions

Kickoff

- IT + executive sponsor align on scope, systems, and intent.
- Alignment upfront avoids weeks of downstream rework.

Questionnaire

- IT + leadership answer the same CSF questions – once.
- No separate executive briefings. No re-interpretation later.

Analysis

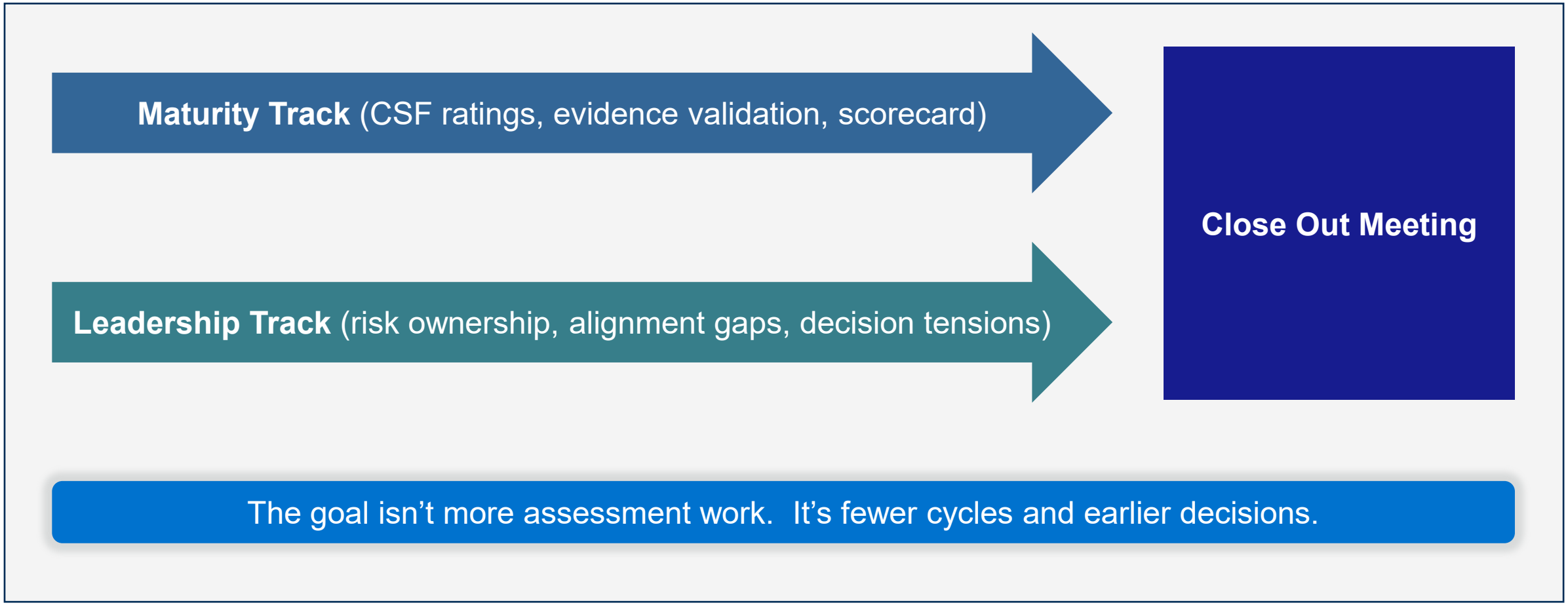
- On top of cybersecurity gaps, include analysis of misalignment, assumptions, weak evidence, and decision-blocking gaps.

Closeout

- Leadership discussion that includes scores and decisions.
- One decision-focused forum can shorten status cycles.

The Most Valuable Output Isn’t Always the Score

Traditional assessments only run the maturity lane; the leadership lane is where outcomes change.



04

What to do next

The Bottom Line

- CSF 2.0 clarified what many practitioners already knew: cybersecurity risk is a leadership responsibility
- Scores are valuable, but can also be misleading
- Design your assessments to produce decisions

The right assessment doesn’t just measure maturity, it creates alignment.

Turning Scores into Action

Expected Outcomes

- Target profile is clearer and leadership owned
- Next steps become logical:
  - Decision register
  - Roadmap development
  - Program build out
  - Control implementation

Skipping these steps often means revisiting the same priorities two budget cycles later.

Target Area	Decision Required	Why it Matters	Owner	Decision Date	Impact if Deferred
Top 5 Mission Critical Systems					
FY Budget Decision Forum + Including Cyber Risk					
IR / Recovery Exercise Cadence					

The Questions to Take Back

After incidents, tabletop exercises, or near misses, did anything actually change … or did operations return to normal?

Do our maturity scores reflect tested capability, or just documented plans?

If IT and leadership listed our top five “cannot fail” systems separately, would the lists match?

If you do nothing else, schedule the decision forum and put owners, dates, and deferrals on the record.

forvis mazars

Contact

Forvis Mazars

Ben Sady
Principal
804.474.1267
ben.sady@us.forvismazars.com