

Cybersecurity Maturity Models Explained



Maturity models give CISO, GRC, audit, and consulting roles a shared vocabulary



Not a certificate, not an audit opinion, not a score that proves security



Control framework: what to do.
Capability model: what you must be able to do



Maturity model: how well capability is performed, repeated, and improved



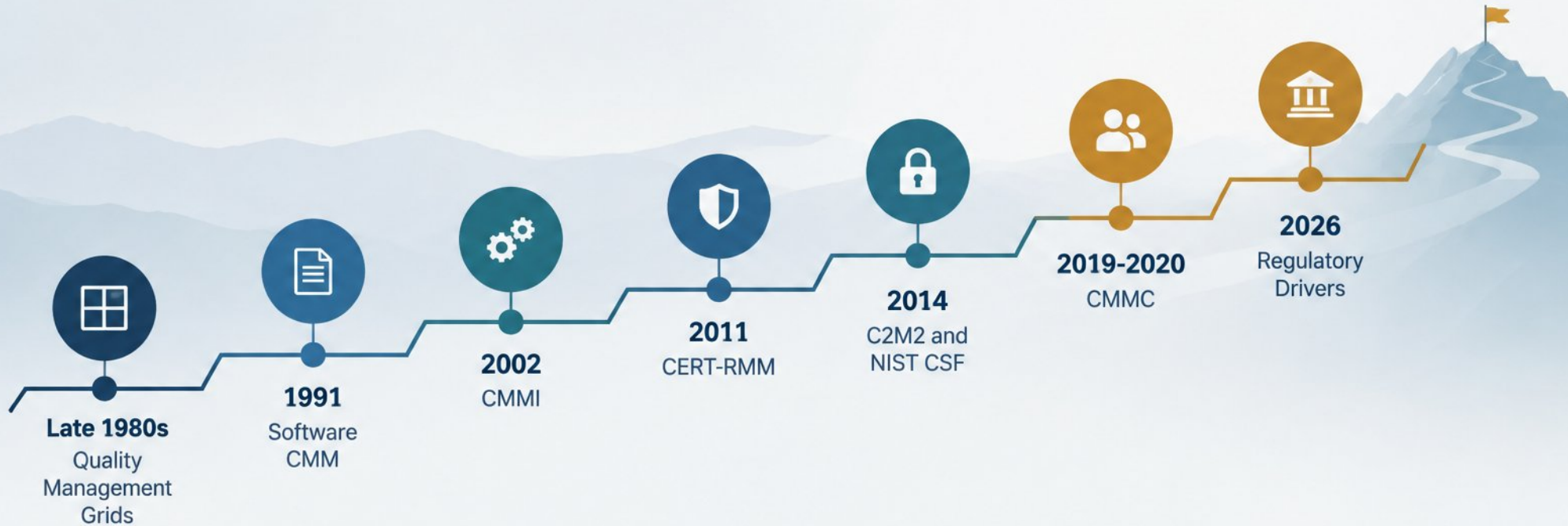
Why now: 89% of boards approve risk appetite; 63% use cyber risk data



Course roadmap: origins, scoring, frameworks, evidence, mapping, roadmaps, pitfalls



Background: From Software Process Maturity to Cyber Maturity

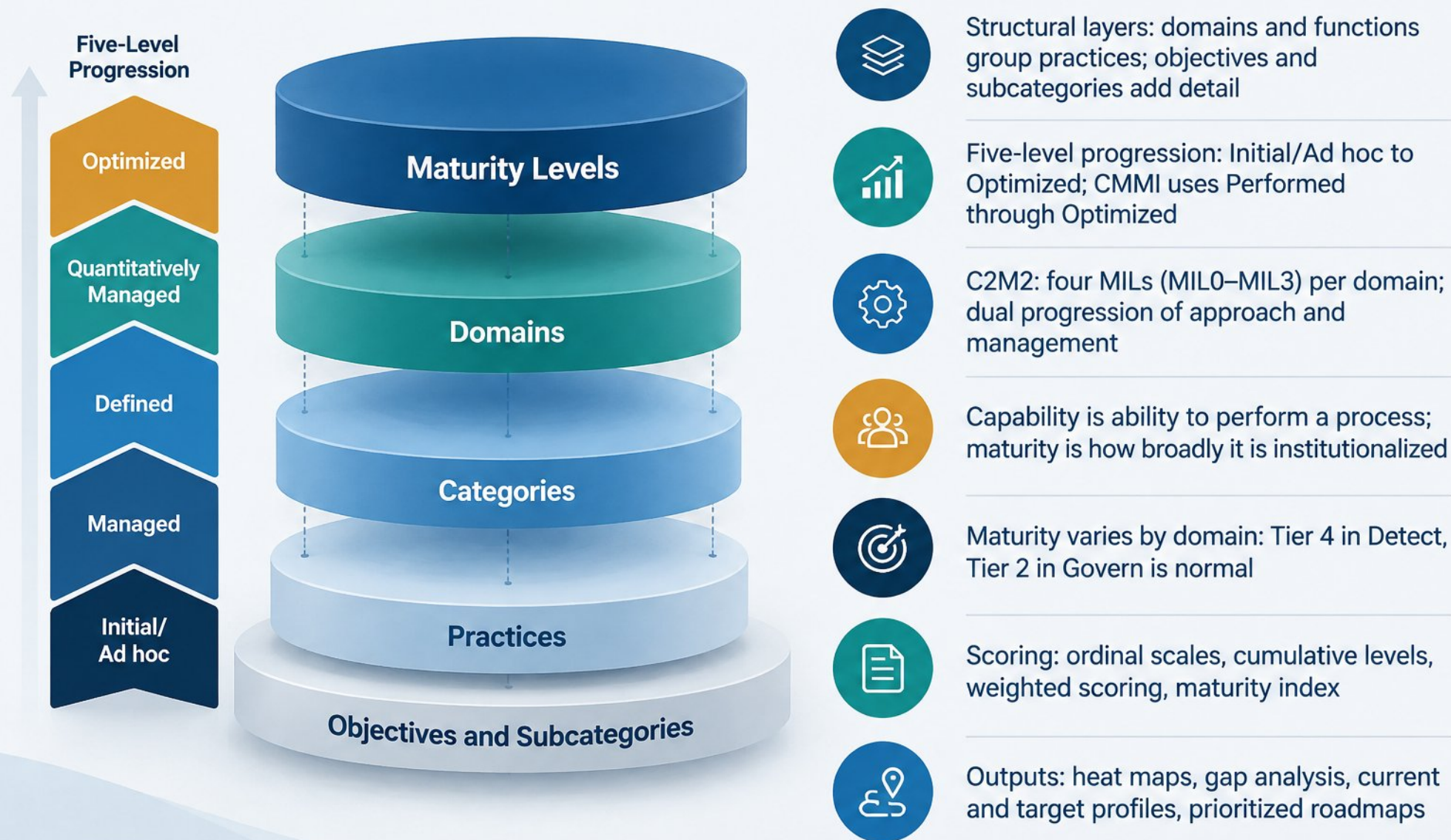


No content available for this page yet.

Core Concepts and Model Anatomy

FROM STRUCTURE TO INSIGHT

PEOPLE | PROCESS | STRONGER OUTCOMES



Leading Frameworks: NIST CSF 2.0, C2M2, CMMC 2.0, and ISO

Different origins. Aligned goals. A stronger, more resilient organization.

PEOPLE
PROCESS
TECHNOLOGY
GREATER RESILIENCE

NIST CSF 2.0



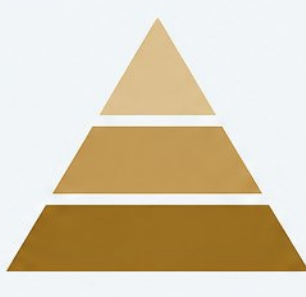
- NIST CSF 2.0: six functions, 22 categories, 106 subcategories; Govern added in 2024
- CSF Tiers are not maturity levels—Tier 4 is not a universal goal

C2M2



- C2M2: 10 domains, 356 practices, four MILs; self-evaluated, strong for OT and ICS

CMMC 2.0



- CMMC 2.0: three levels; Level 2 = 110 NIST SP 800-171 controls, C3PAO assessed

ISO/IEC 27001:2022



- ISO/IEC 27001:2022: certifiable ISMS, 93 Annex A controls; ISO 21827 legacy



CIS Controls v8.1

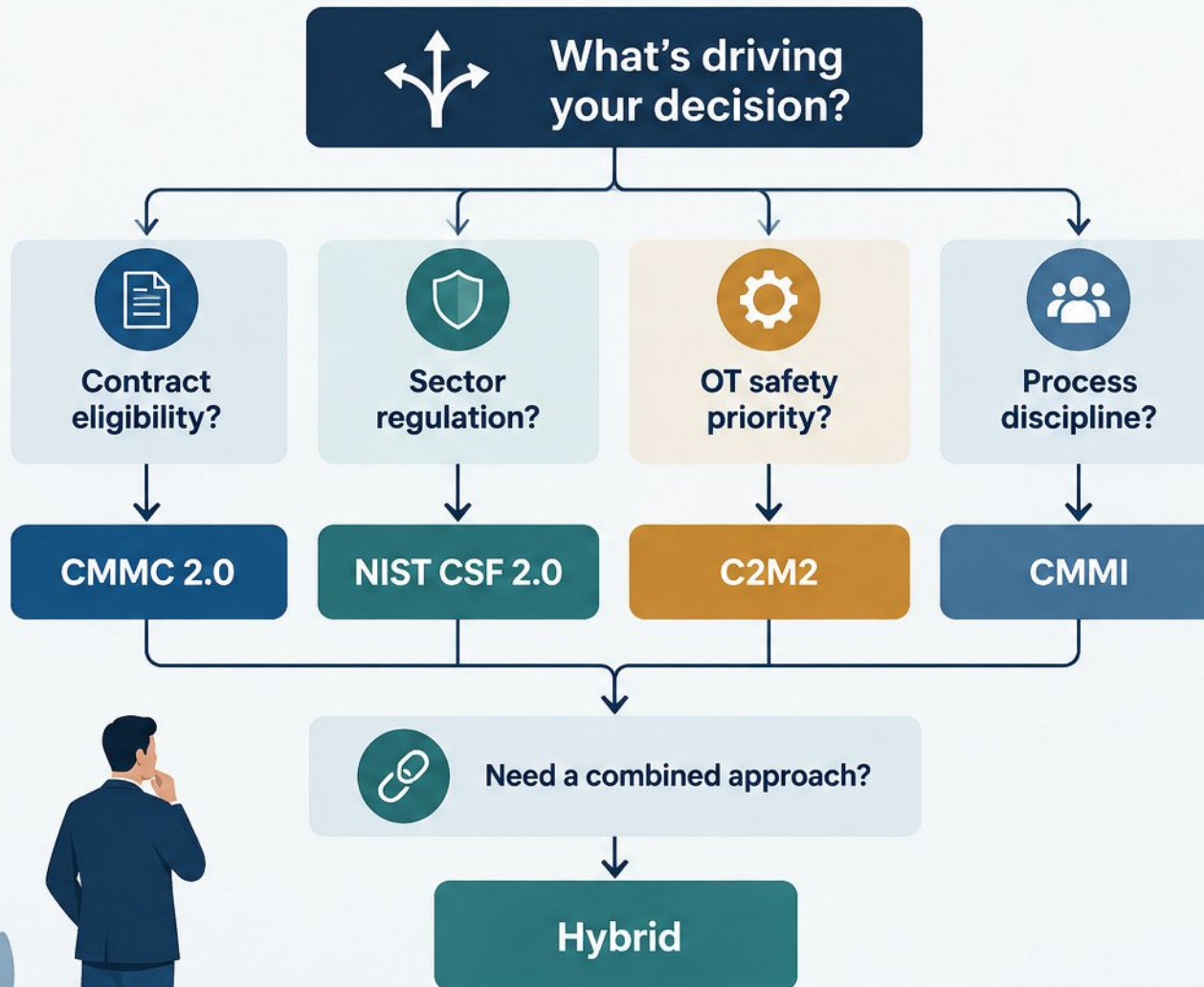
- CIS Controls v8.1: prioritized safeguards with Implementation Groups for tactical gains

COMMON FRAMEWORKS.
STRONGER OUTCOMES.



ALIGN
UNDERSTAND
APPLY
BUILD RESILIENCE

Choosing the Right Model: When NIST CSF, CMMC, C2M2, or a Hybrid Fits



- **NIST CSF 2.0:** what you do — voluntary, flexible, rated by coverage and integration
- **CMMC 2.0:** what you must do for DoD contracts — 110 Level 2 practices, no risk acceptance
- **C2M2:** how mature per domain — OT where availability and safety outrank confidentiality
- **CMMI:** how well you run a process — five-level scale for process discipline
- **Hybrid:** CSF 2.0 taxonomy plus documented 1-to-5 capability score per function
- Decide by mandate, certifications, IT vs. OT scope, baseline, and assessment budget

STRONGER CAPABILITIES
GREATER RESILIENCE
LONG-TERM VALUE

Assessment Methods and Evidence

— CONSISTENT METHODS. CREDIBLE EVIDENCE. STRONGER OUTCOMES.



Approaches span self-assessment, facilitated workshops, third-party audit, and formal certification



Evidence hierarchy: simulated testing > configuration review > screenshots > policy statements



Three core methods: examine artifacts, interview personnel, test controls under specified conditions



Anchor scoring definitions per level per category before assessment begins



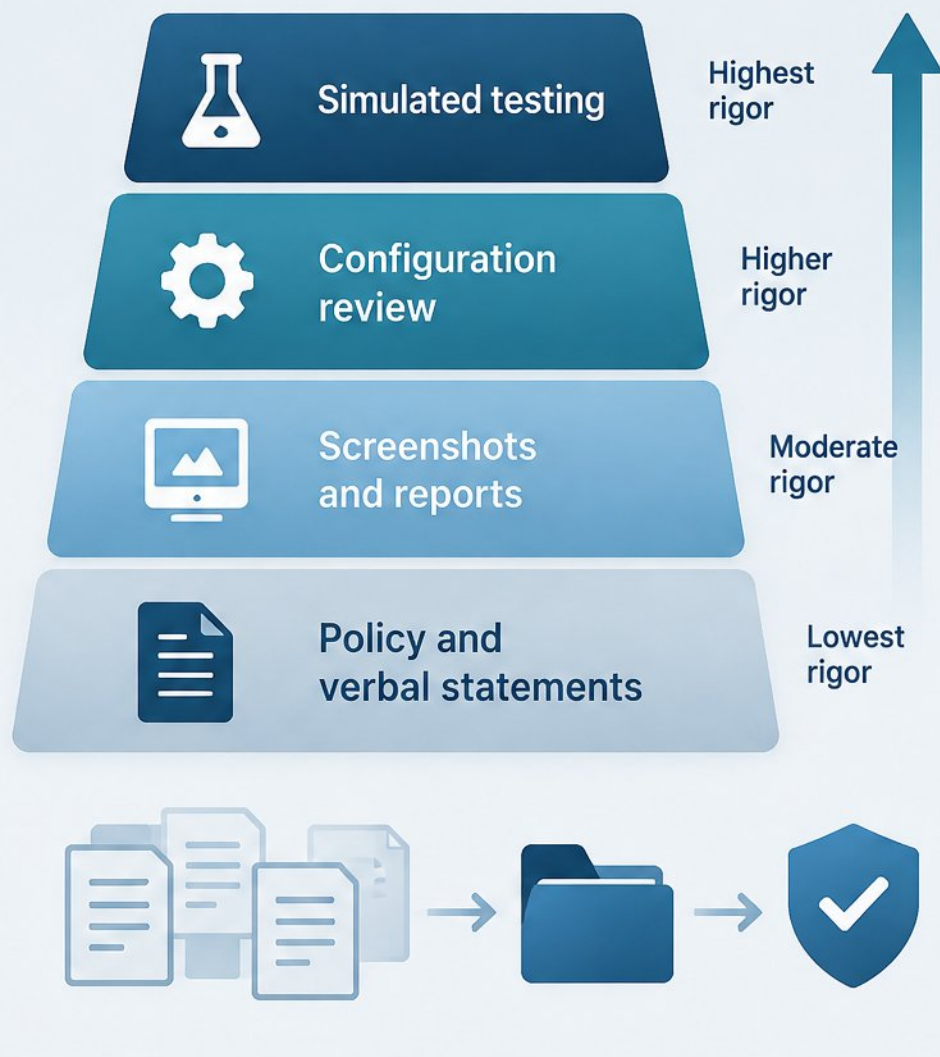
Self-scored maturity inflates roughly one full level on governance and third-party risk



Watch pitfalls: scoring inflation, evidence gaps, scope creep, risk acceptance as justification

Evidence Hierarchy

HIGHER RIGOR AT THE TOP



Mapping Maturity Models to Standards and Regulations

Use control-level mappings to understand alignment, identify gaps, and inform your compliance strategy.

From / To Framework	NIST CSF 2.0	NIST SP 800-53	CMMC Level 2	ISO 27001
NIST CSF 2.0	—	●	●	●
NIST SP 800-53	●	—	●	●
CMMC Level 2	●	●	—	●
ISO 27001	●	●	●	—

● exact ● strong ● partial ● related



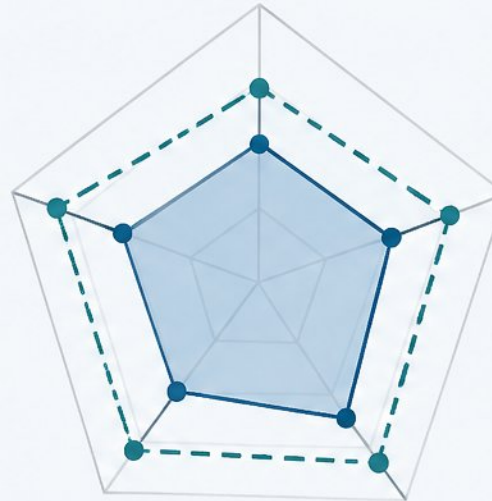
**Mapping clarifies alignment.
Context ensures correct interpretation.**

- NIST publishes official CSF 2.0 informative references at individual control level
- Derived relation mapping uses NIST SP 800-53 as focal document to bridge frameworks
- NIST CSF 2.0 and CMMC Level 2 share 46 of 49 tracked controls
- ISO 27001-certified organizations typically close 60-70% of CMMC Level 2
- Keep honest relationship types: exact, strong, partial, related
- Pitfall: ISO 27001 does not satisfy CMMC; neither replaces NIST SP 800-171

From Assessment to Action: Target Profiles, Roadmaps, and Metrics

- Prioritize initiatives by risk reduction per dollar, regulatory urgency, and business alignment
- Target maturity: 4 on highest-risk categories, 3 elsewhere; 5 everywhere goes unfunded
- Realistic CSF 2.0 program: 12–14 months across four phases for mid-sized firms
- Practical sequence: diagnose, harden identity, build detection, then prevention and governance
- Execution index (on track?), maturity index (improving?), transformational KPIs (impact realized?)
- Board one-pager: outcomes with trend arrows, top risks, owners, aging exceptions
- Report progress with trend data, not point-in-time scores; re-assess annually

Target Profile (Maturity)



—●— Current Profile
- -●- Target Profile

Maturity Index Trend



Key Security Outcomes



Top Risks and Aging Exceptions



Four-Phase Program (12–14 Months)



Common Pitfalls and Critical Perspectives



Maturity theater: scoring for a number, not reducing risk



Static, diagnostic models lack actionability; complexity and one-size-fits-all design undermine adoption



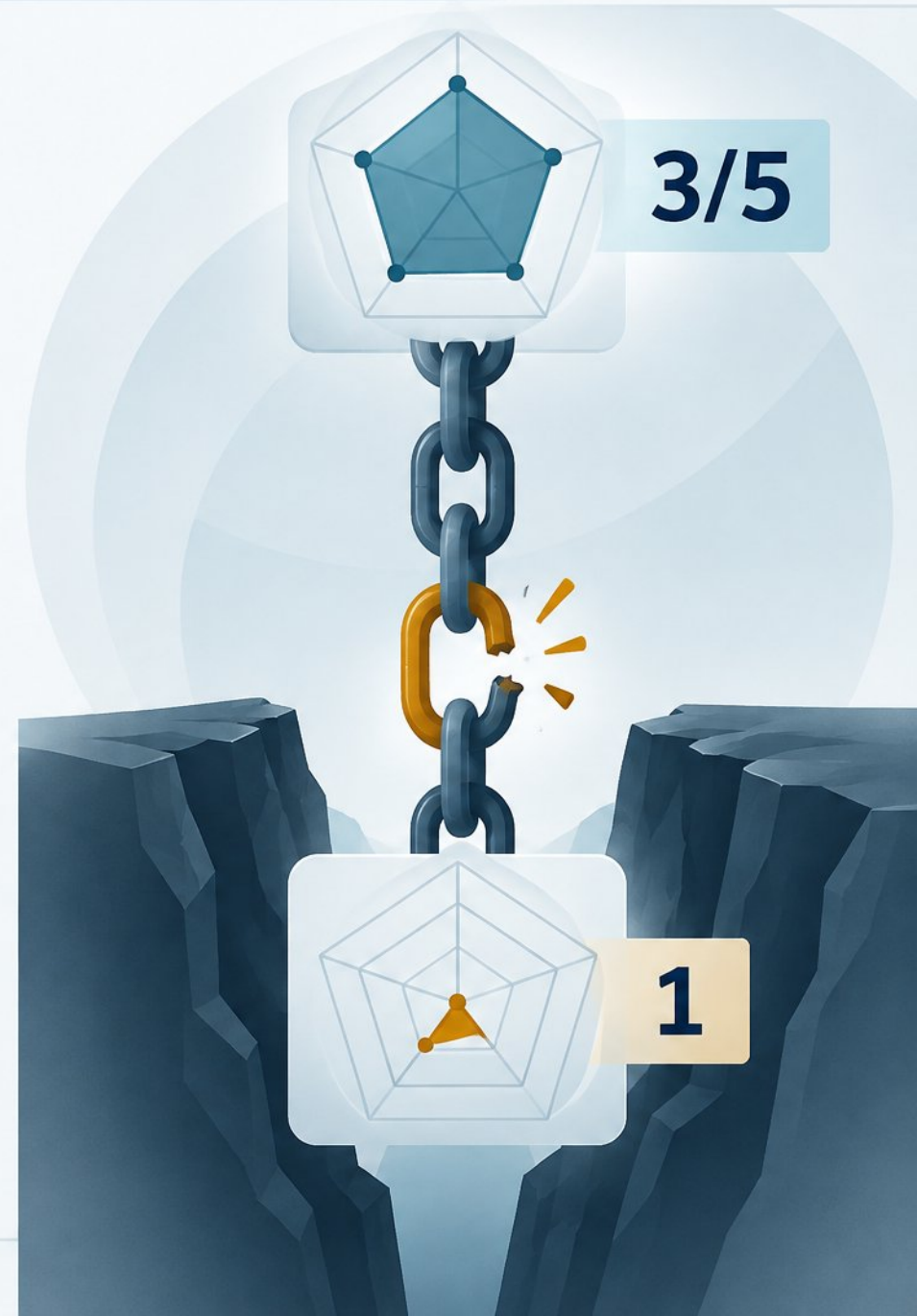
Aggregation hides risk: a 3/5 average masks OT or legacy areas at 1



Self-scored maturity inflates by roughly one full level; reports lack scope and validation context



Assessment is not assurance: under half of findings are fixed, state decays in months



Role-Based Playbooks: CISO, Security PM, GRC, Audit, and Consulting

PEOPLE
PROCESSES
EVIDENCE
STRONGER OUTCOMES



CISO

- CISO: tie maturity ambition to risk appetite; own board narrative in business-risk language



Board scorecard



Security PM

- Security PM: charter the assessment boundary, run workstreams, track POA&M remediation



Assessment charter



GRC

- GRC: embed maturity in risk registers, control testing, third-party risk, crosswalk maintenance



Control matrix



Auditor

- Auditor: validate evidence at defined rigor, apply scoring anchors, write next-level findings



Evidence request list



Consultant/vCISO

- Consultant/vCISO: advise model selection, run gap assessments, preserve audit independence



Remediation roadmap



RACI

- RACI: who assesses, owns remediation, accepts residual risk, reports to the board



EVIDENCE
INFORMS
CONFIDENCE

Case Exercise: Drafting a Maturity Assessment Scope



Scenario: 1,200-employee health tech firm, CSF 2.0 contract, growing DoD subcontract, lean security staff

1-2

Define boundaries and model



- Define boundaries (IT/OT, cloud, third parties, PHI/CUI)
- Score CSF 2.0 on a 1-5 scale

3-4

Evidence and targeting



- Build an evidence request list
- Target top third fully, middle third partially, bottom third documented as de-prioritized

5-6

Plan and deliver



- Plan a 4-6 week assessment
- Deliver radar charts, gap register, 18-month roadmap, board scorecard



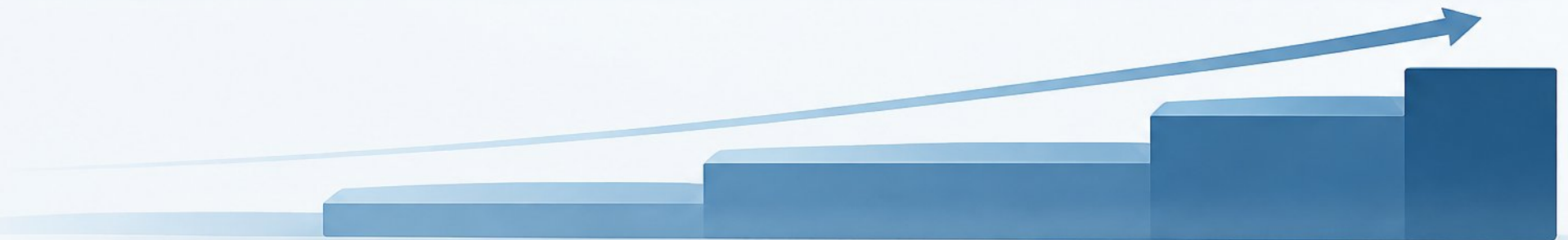
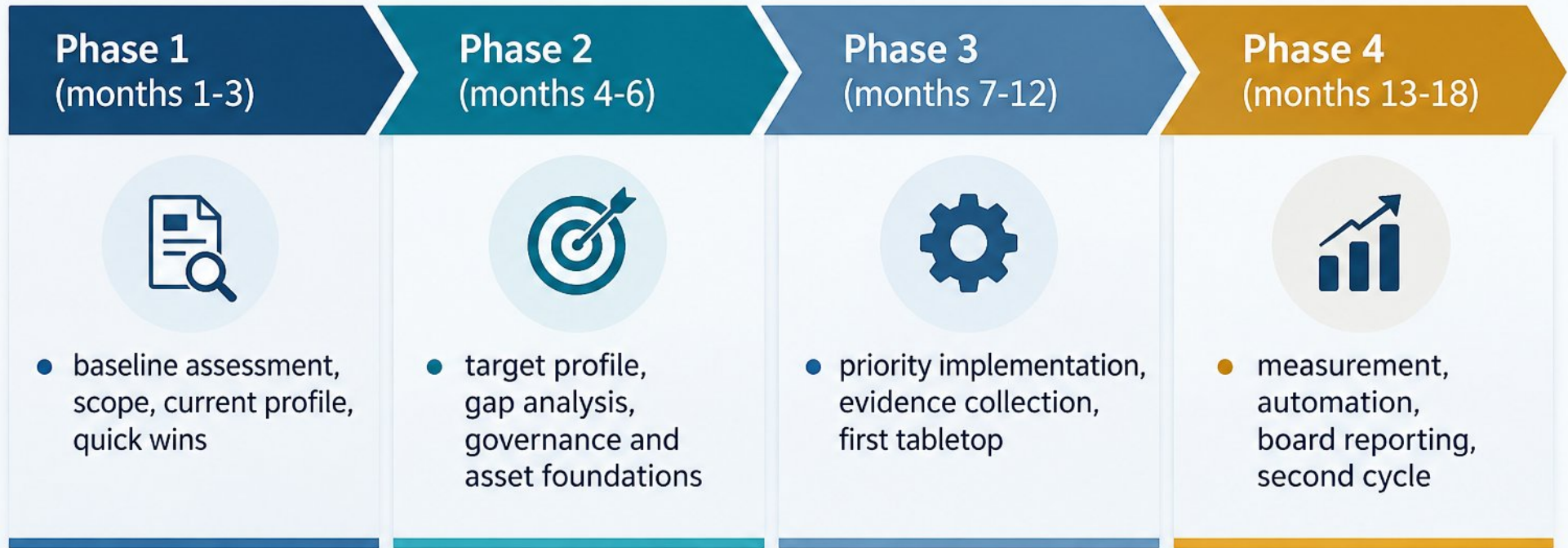
Discuss

- Assessment owner
- Independence
- Scoring disagreements
- Re-assessment triggers

Control-to-Framework Mapping

ASSESS
PRIORITIZE
STRENGTHEN
ADVANCE

Adoption Roadmap: A Phased 12-18 Month Plan



Build vs. buy: internal context and ownership versus independent credibility



Sequence foundations first, then select the model via a decision matrix

Key Takeaways and Next Steps

FROM ASSESSMENT
TO PROGRESS



A maturity model is a management system, not a certificate



Choose by question: coverage (CSF), contracts (CMMC), OT (C2M2), process (CMMI)



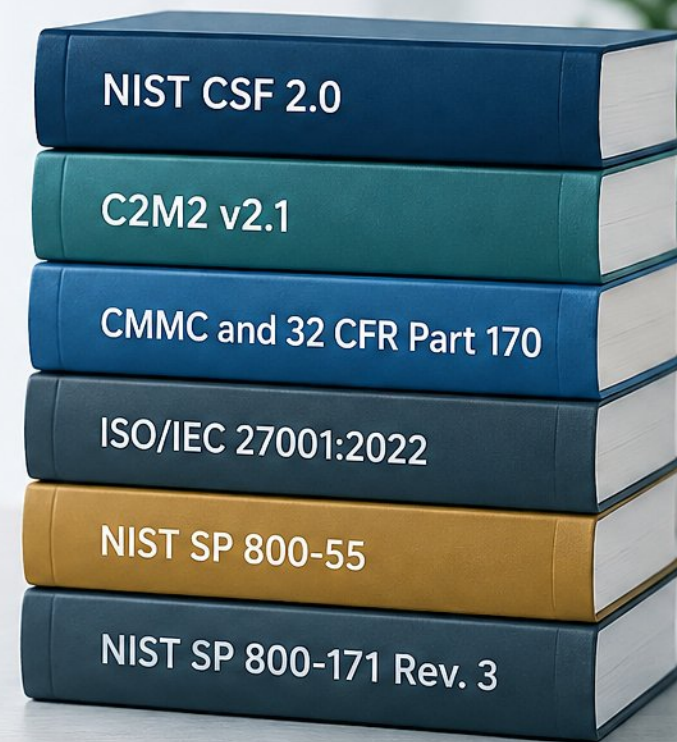
Anchor scores to evidence; lead with radar shape, not one average



The roadmap is the deliverable; the score is its title



Next 60–90 days: baseline, brief leadership, resource first wave, report quarterly



Next
60–90 days



Baseline



Brief leadership



Resource first wave



Report quarterly

PersonWise.

PersonWise • AI digital-human course platform



Scan the code or click anywhere to watch this course live, with voice Q&A

personwise.ai/t/2b3d7e24/public