

NIST Cybersecurity Framework: Components and Application

- ▶ Voluntary, risk-based guidance for managing cybersecurity risks
- ▶ CSF 2.0 expands scope beyond critical infrastructure to all organizations
- ▶ Update introduces a sixth Function: Govern
- ▶ Common language for security leaders, technical teams, and learners
- ▶ This training moves from framework structure to real-world operationalization



What Is the NIST CSF and Why It Matters

- ▶ Voluntary, risk-based guidance first released in 2014
- ▶ CSF 2.0 expands scope to all organizations and sectors
- ▶ Common language for prioritization and board communication
- ▶ Maps existing controls without prescribing specific tools



CSF 2.0 at a Glance: Three Components



- **Core:** taxonomy of high-level, technology-neutral cybersecurity outcomes



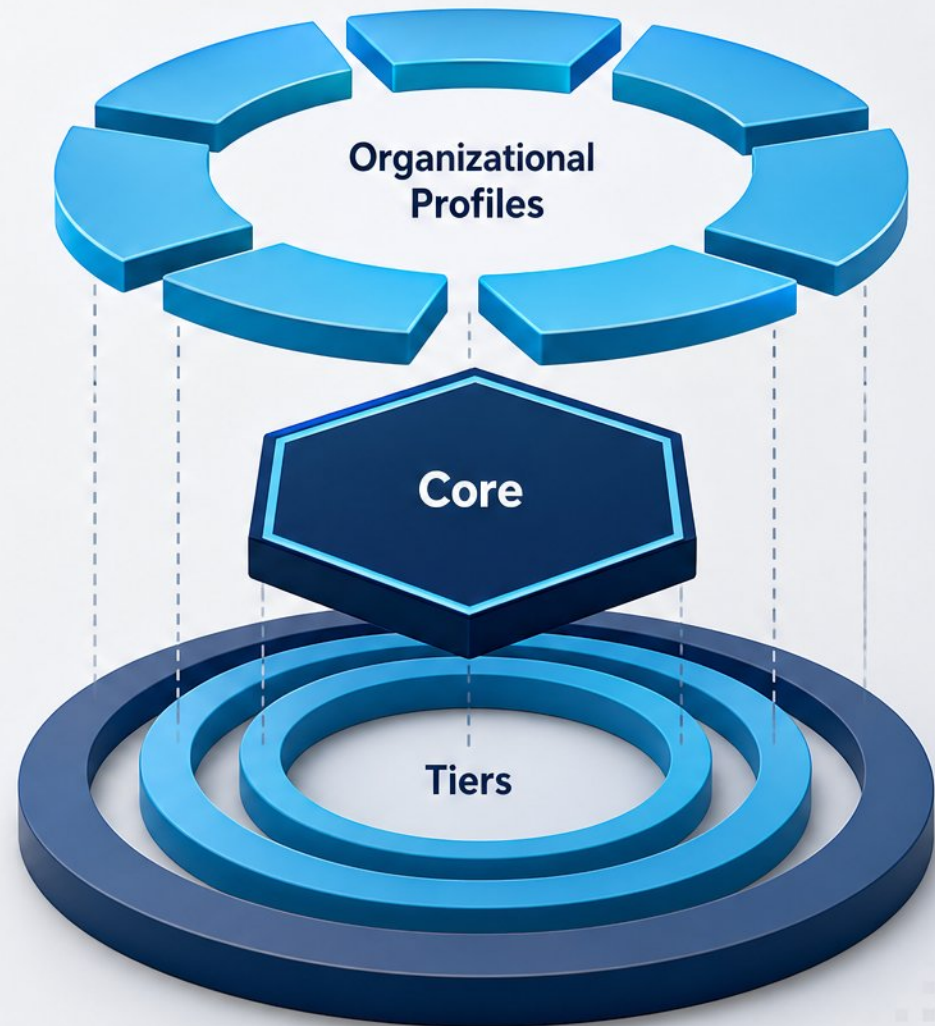
- **Organizational Profiles:** describe current and target cybersecurity posture



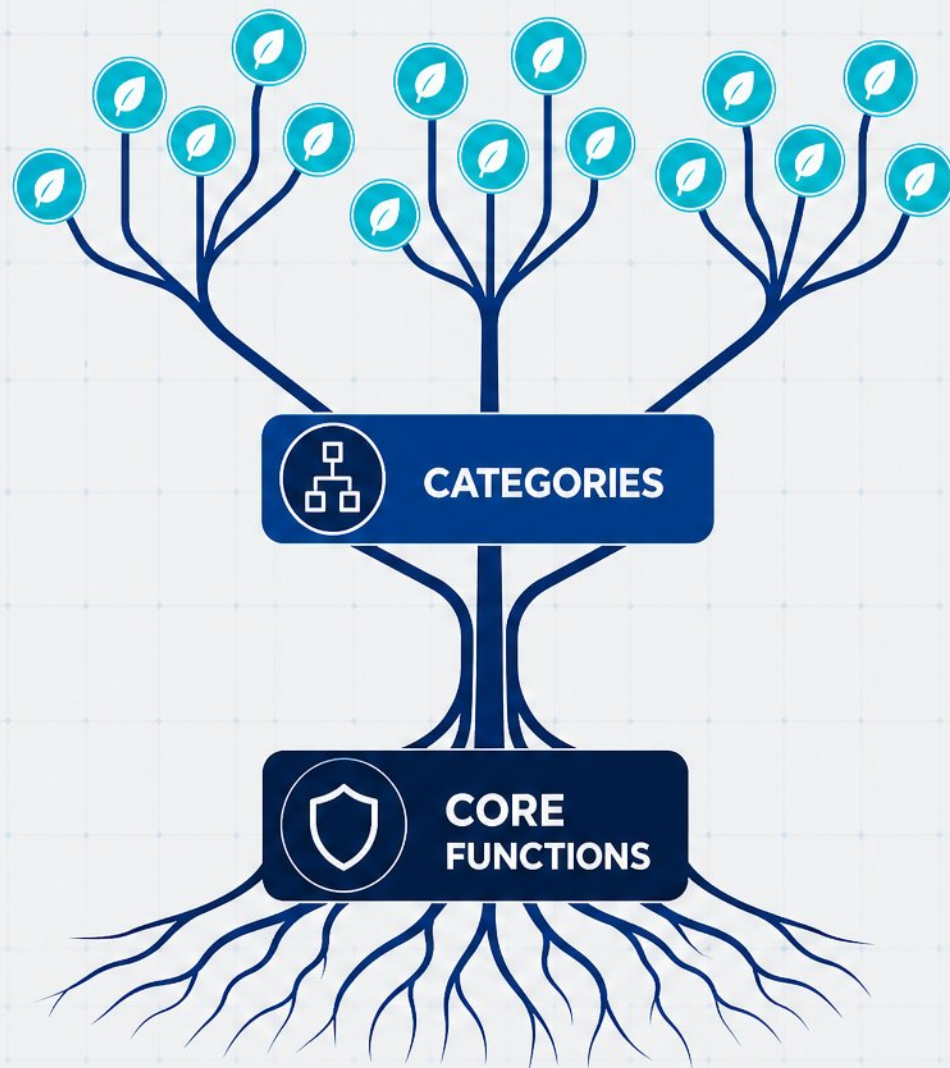
- **Tiers:** characterize rigor of risk governance and management practices



- Tiers apply to Profiles to add context on risk management processes



The Core: Functions, Categories, Subcategories



- **Hierarchy:** Function → Category → Subcategory, each describing specific outcomes



- Sector-, country-, and technology-neutral outcomes, not an action checklist



- Subcategory numbering has intentional gaps from relocated CSF 1.1 content



- Applies to all ICT: IT, IoT, OT, cloud, mobile, and AI systems

The Six Core Functions of CSF 2.0



- **Govern:**
Establishes strategy, expectations, and policy for cybersecurity risk management.



- **Identify:**
Understands assets, risks, and supply chain dependencies.



- **Protect:**
Implements safeguards to manage and reduce cybersecurity risk.



- **Detect:**
Finds and analyzes possible cybersecurity attacks and compromises.



- **Respond:**
Takes action regarding a detected cybersecurity incident.



- **Recover:**
Restores assets and operations affected by an incident.

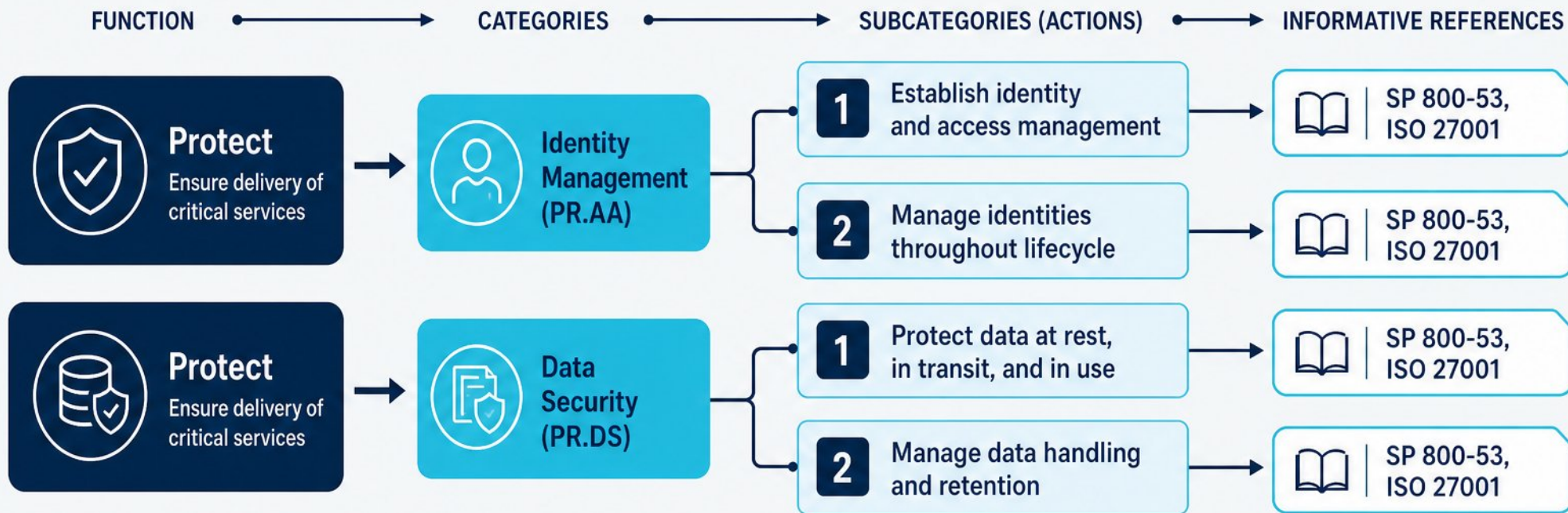


Govern: The New Foundation

- ▶ - New sixth Function in CSF 2.0
- ▶ - Consolidates risk strategy, roles, policy, and oversight
- ▶ - Elevates supply chain risk management visibility
- ▶ - Aligns cybersecurity with enterprise risk and legal obligations
- ▶ - Governance should shape and inform the other five Functions



Categories and Subcategories: From Function to Action



- Functions divide into outcome-oriented Categories
- Subcategories specify technical and management outcomes
- Protect example: Identity Management (PR.AA), Data Security (PR.DS)
- Informative References map Subcategories to standards (SP 800-53, ISO 27001)
- Implementation Examples provide notional steps to achieve outcomes

Informative References and Implementation Examples



- Informative References map CSF outcomes to global standards, guidelines, and regulations



- References are not checklists; organizations select all, some, or none



- Implementation Examples provide concise, action-oriented steps for each outcome



- Both resources are updated regularly via the CSF 2.0 Reference Tool

SUBCATEGORY
OUTCOMES



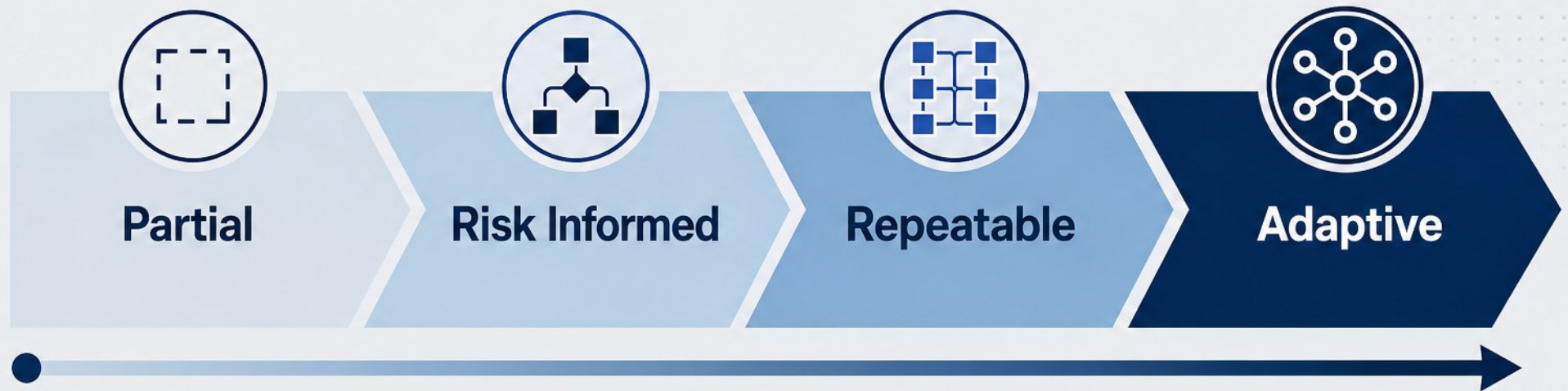
ISO

NIST

CIS



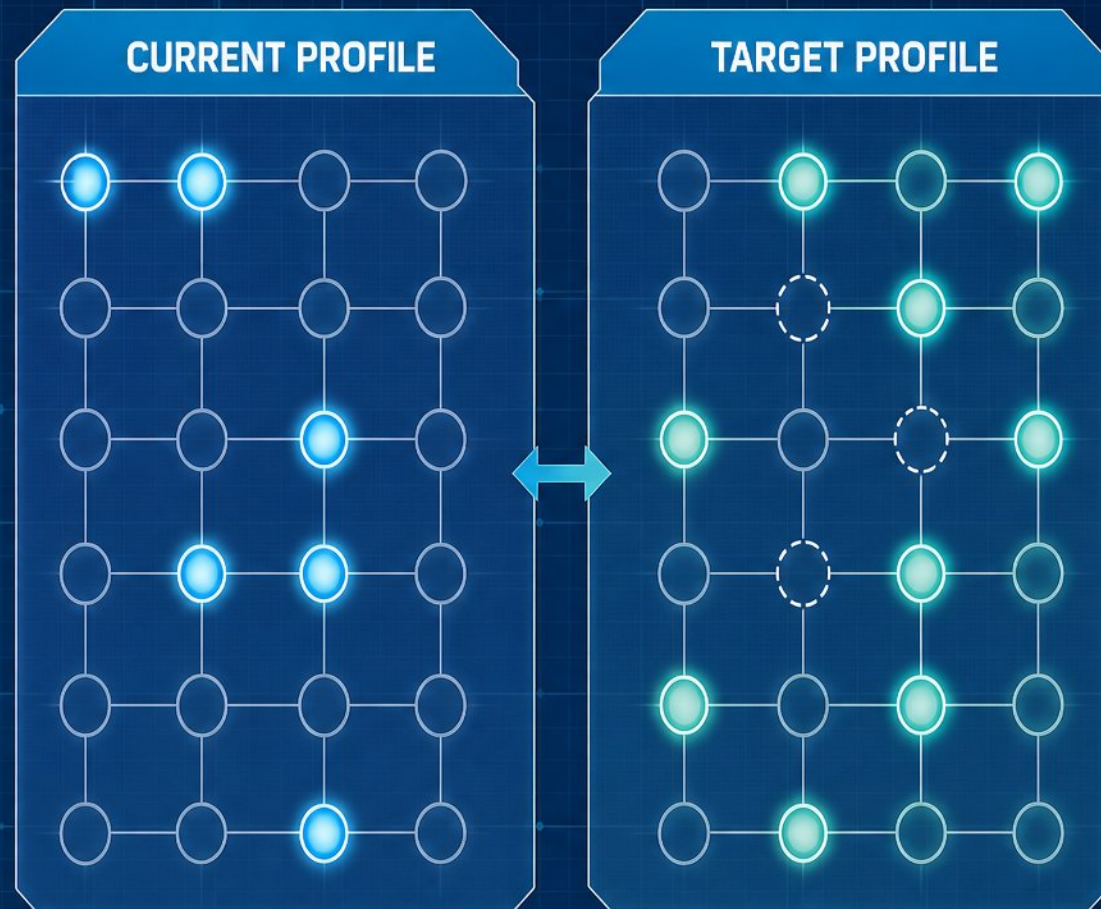
Implementation Tiers: Assessing Your Program



- Four Tiers: Partial, Risk Informed, Repeatable, Adaptive
- Tiers characterize rigor of risk governance and management practices
- Select Tiers at Function or Category level, informed by risk tolerance
- Higher Tiers are not universally better; target depends on context

Building Organizational Profiles

- Documents current and/or target posture using Core outcomes
- Current Profile: outcomes achieved today
- Target Profile: desired future outcomes
- NIST Excel template enables side-by-side gap analysis
- Scoped to mission, stakeholder expectations, and requirements





Community Profiles for Shared Outcomes



- Baseline of CSF outcomes for a shared sector, technology, or threat use case



- Copy a Community Profile as your starting Target Profile



- Includes priorities, rationale, and applicable Informative References



- Lifecycle: Plan, Develop, Use, Maintain

FIELD GUIDE PLATE

HEALTHCARE



MANUFACTURING



CLOUD



RANSOMWARE



ORGANS OF AN ORGANIZATION



PLAN



DEVELOP

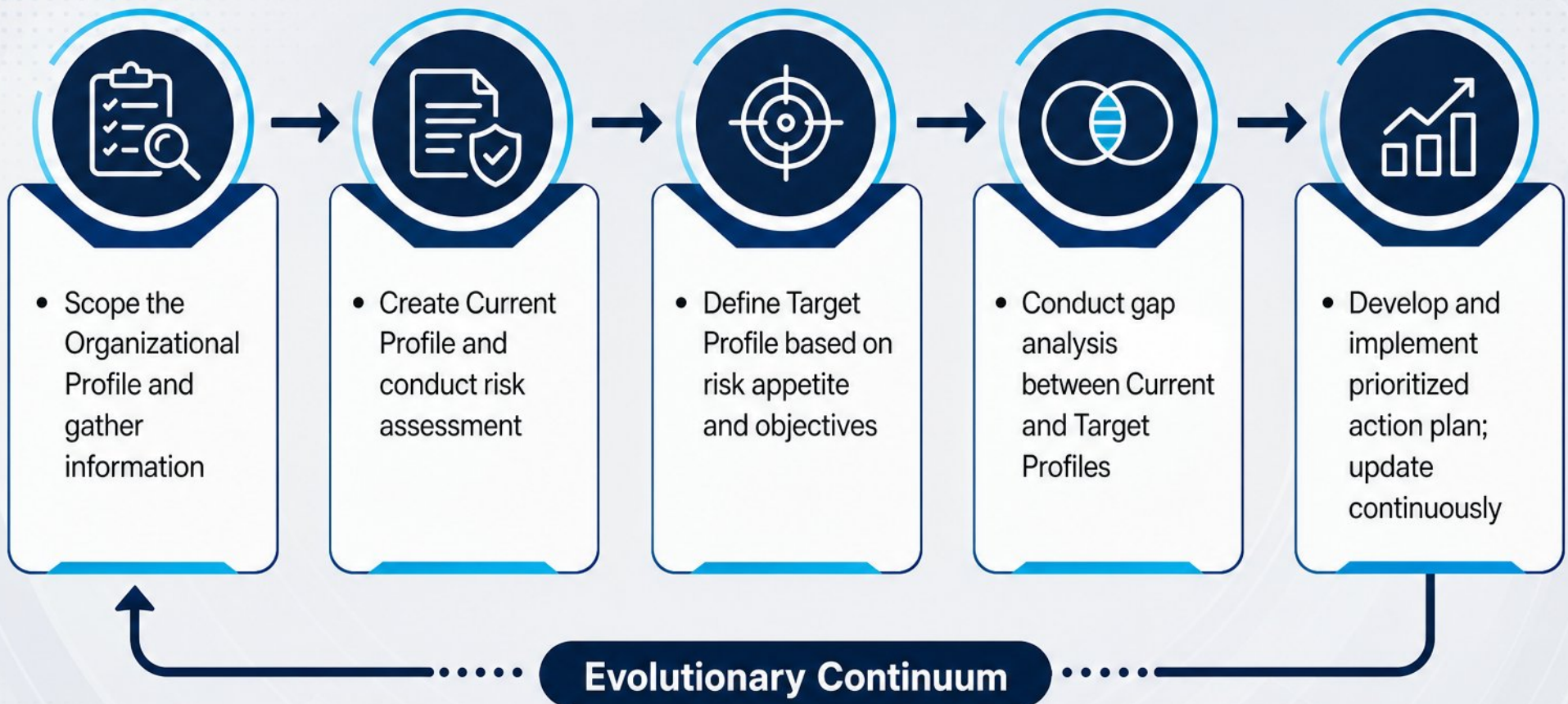


USE



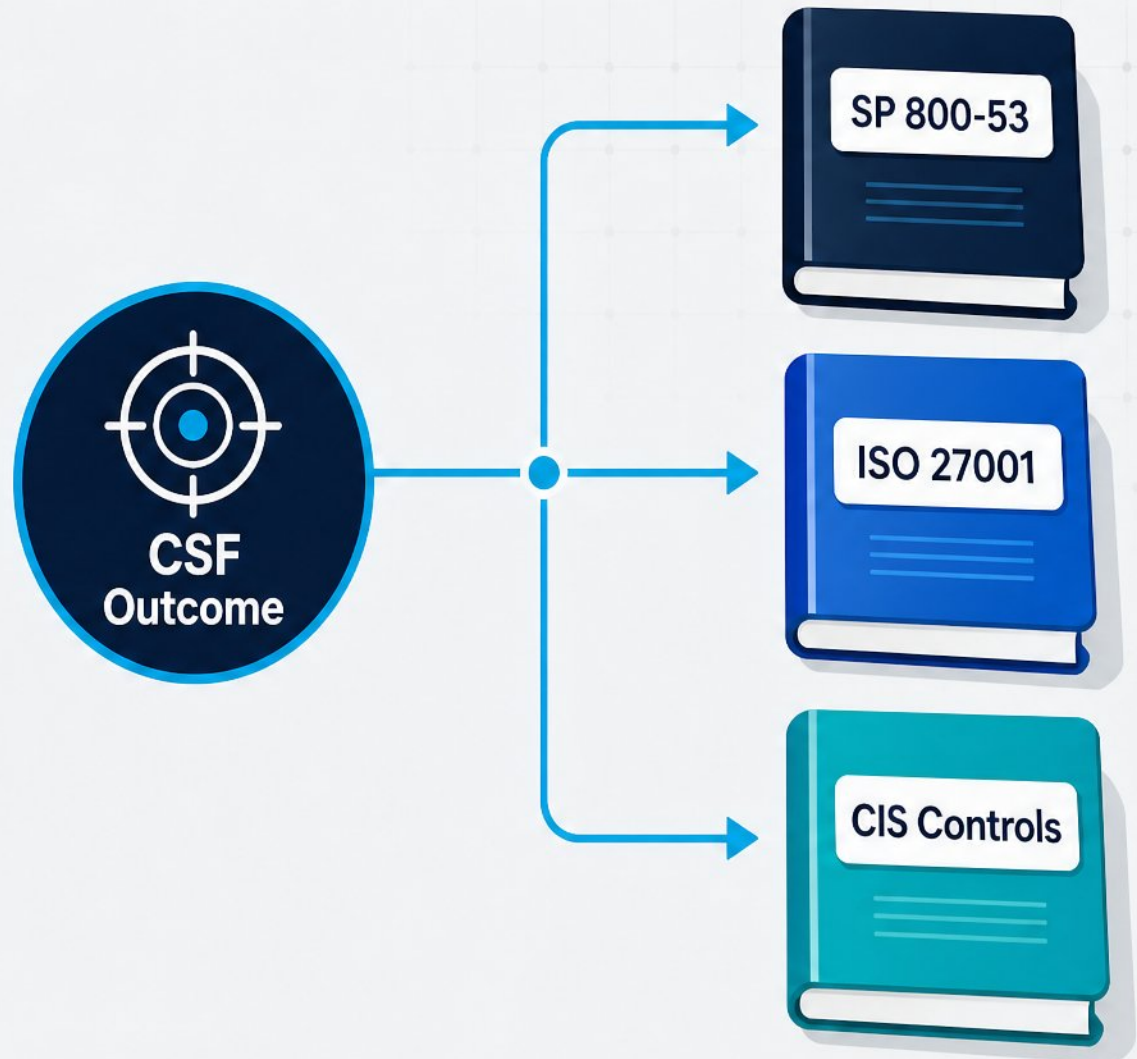
MAINTAIN

Applying the CSF: Step-by-Step Approach



Mapping the CSF to Other Standards

- Informative References map outcomes to SP 800-53, ISO 27001, CIS Controls
- CSF serves as a translation layer between frameworks and regulations
- Mapping is outcome-based, not one-to-one substitution; depth differs
- Use official crosswalks and the NIST CSF 2.0 Reference Tool



Common Adoption Challenges and Practical Guidance



- Avoid checklist-driven implementation that ignores risk context



- Use Quick Start Guides for small and medium organizations



- Keep Profiles and Tiers current as the organization evolves



- Communicate results to executives in business language and metrics



- Leverage NIST supplementary resources, templates, and workforce materials



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/ad820b0e/public