NIST CSF 2.0 Unleashed: *Get Past the Gaps and Boost Your Results*

Meet the Team

Aaron Pritz

CEO, Co-Founder, Partner

Chris Adickes

Consulting Director

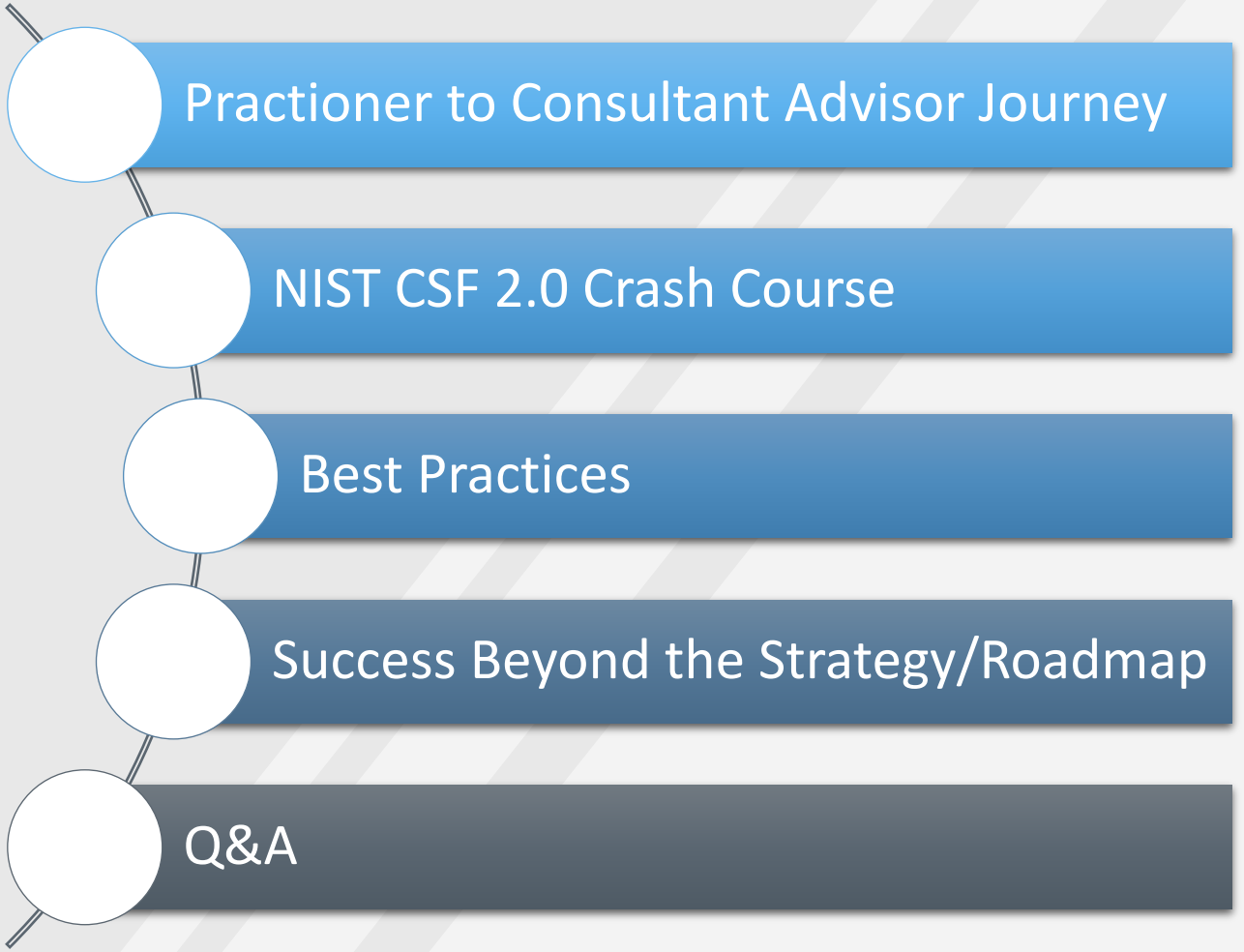
Michael Milroy

Senior Consultant

Eugene Korolyov

Senior Consultant

Agenda


Practioner to Consultant Advisor Journey
NIST CSF 2.0 Crash Course
Best Practices
Success Beyond the Strategy/Roadmap
Q&A

Journey From:
Practitioner to Consultant Advisor

NIST CSF 2.0

NIST Cybersecurity Framework (CSF): Context

History

- CSF 1.0
- CSF 1.1
- CSF 2.0

Objective

- Guidance
- Outcomes

Approach

- Understand
- Assess
- Prioritize
- Communicate

NIST CSF: Structure

Profiles

- Organizational
- Community

Tiers

- 1: Partial
- 2: Risk Informed
- 3: Repeatable
- 4: Adaptive

Implementation

- Concise Examples
- Action-Oriented

NIST CSF: Structure

Profiles

- Organizational
- Community

Tiers

CMMI

- 1: Initial
- 2: Managed
- 3: Defined
- 4: Quantitatively Managed
- 5: Optimizing

Implementation

- Concise Examples
- Action-Oriented

NIST CSF: Functions and Objectives

Govern

Drive standards

Identify

Find vulnerabilities

Protect

Be proactive

Detect

Find threats

Respond

Take action

Recover

Fix and learn

NIST CSF 2.0: Biggest Functional Changes

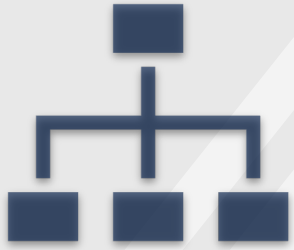
Govern

- New function
- Intentional connection to enterprise risk strategy
- Supply Chain

Identify

- Improvement category

Protect



- Distributed to other functions
- Platform Security
- Infrastucture Resilience

Respond & Recover

- Initiation criteria
- Magnitude
- Backup integrity

NIST Maturity Journey

Investment Hurdle

Can require substantial resource investment, training, and potentially new technologies.
Investment is not 1:1 maturity outcome.

Control Coverage

Key component is breadth of coverage.
Exceptions or special cases are reduced to minimal edge cases.

Technology Investments

Technology takes time to install, configure, and tune.
Technology, in addition to process or policy, supports most controls.

Organizational Growth

Security control requirements grow along with organization.
Organizational changes include security from the beginning.

Lessons Learned

Tips & Tricks

- Start with most critical areas.
- Small progress is still progress.
- Maintain a program, don't just do assessments.

Pitfalls to Avoid

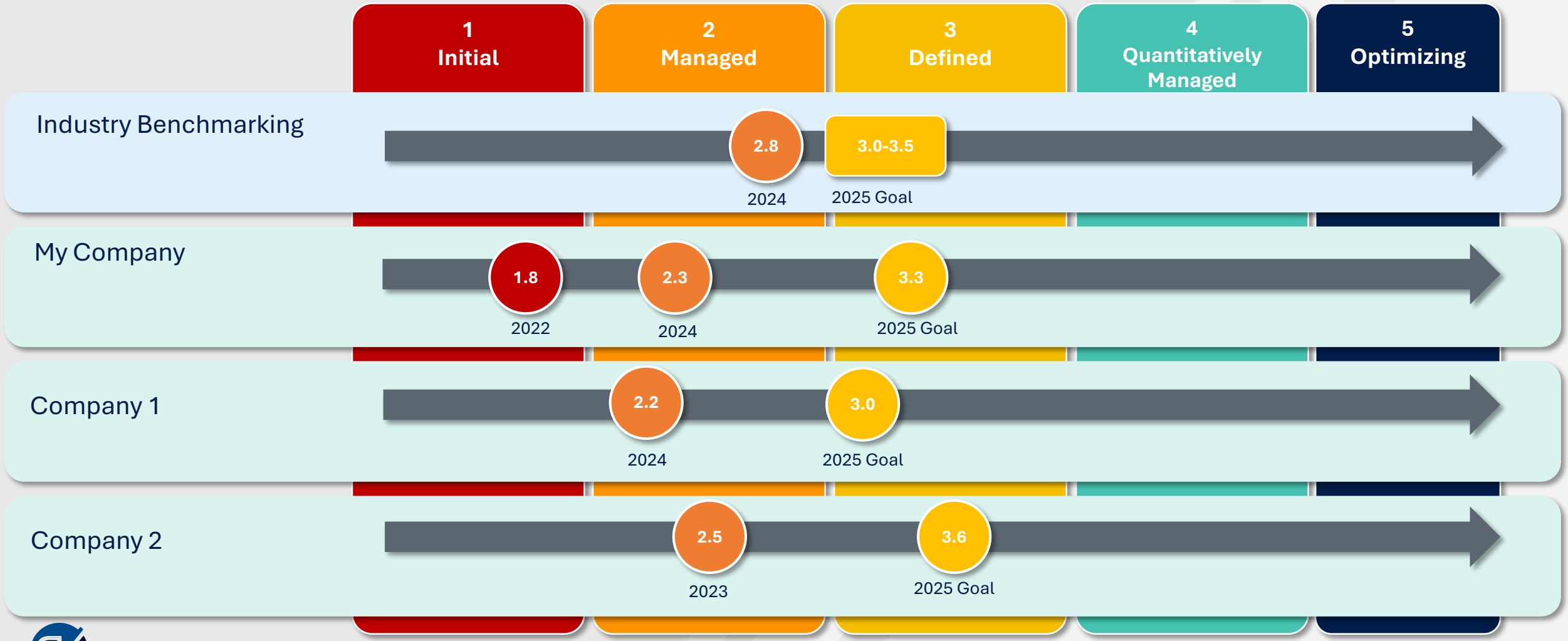
- Don't build a program to a single framework.
- Compliance does not equal Security.

Best Practices

Best Practices:
from Theory to Action

- ✓ Scope Alignment
- ✓ Stakeholder Engagement
- ✓ Documentation Review
- ✓ Assessment, not an Audit
- ✓ Iterative Collaboration
- ✓ Scoring Criteria
- ✓ Prioritization
- ✓ External Benchmarking
- ✓ Roadmap

Maturity Scoring Trends with Benchmarks



Best Practices

Assessment Executive Summary

- Assessment Approach / Scope
- Critical Assessment Highlights
- Maturity Rating Overview

Methodology Rating Criteria

- Documentation
- People
- Process
- Technology
- Coverage

Roadmap 1-Pagers

- Initiative Overview
- Resourcing & Cost
- Implementation Approach
- Key Deliverables / Milestones
- In-Flight Initiatives

Beyond the Strategy

The Roadmap… To the Roadmap

Map to Actionable Initiatives

- Link strategy to actionable initiatives.
- The initiatives need to be **prioritized.**
- Capture the initiatives in something "tangible" that can be shared.
- Communicate the strategy to get buy-in.

Execute (Influence!)

- Cyber strategies and their execution do not live in a bubble!
- Get buy-in.
- Address through influencing:
  - Budget constraints.
  - Integration with IT portfolio.
  - Managing competing priorities.
  - Continued operations of strategic improvements.

Driving Buy-In

Testing

- Penetration Testing
- Red Teaming
- Purple Teaming

Tabletop Exercise (TTX)

- Incident Response Plan TTX (IT/Exec)
- Business Continuity Plan TTX

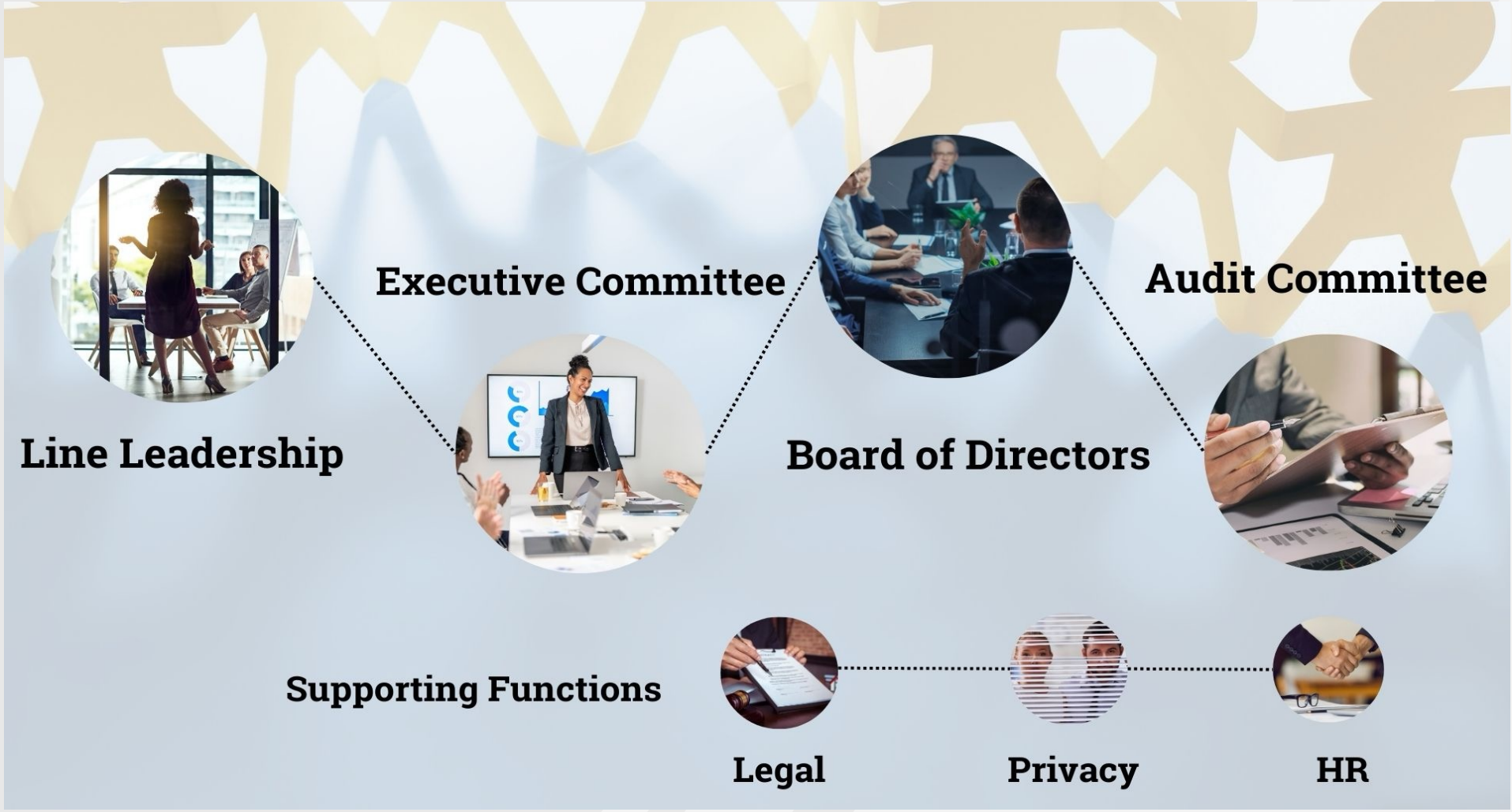
Deep-Dive Assessments

- Process-Specific assessment
- System-Specific Assessment
- Program (Sub-Component) Assessment

Security Events

- Capture key risks and gaps
- Map these to initiatives/update strategy/get buy-in

Navigating the Business, Executive, and Board Landscape



Key Tips for Committee-Level Influence

1. Establish a business-engaged Cyber Governance Steering Committee.

2. Identify embedded champions.

3. Separate business-facing initiatives from back-end technical.
   - Focus on what you need from, whom, by when.

4. Measure progress and success.
   - Gamify a scoreboard to measure results across the business and capture some healthy competition!

Free Resources to Help with Committee Influence and Success

- Audit Committee Board Cybersecurity Insights
- Building Senior Leader Engagement in Cyber Security
- Cybersecurity: A Costly Annoyance or a Differentiating Competitive Advantage
- Empowering Boards for Effective Cybersecurity Oversight: A Director’s Guide
- Making Your Business Fall in Love with Cyber
- Cybersecurity Is Not Best Left to the Experts: A 2024 Business Leader’s Guide

Questions?

Thank you!

Feel free to contact us.

www.revealrisk.com

info@revealrisk.com

317.759.4453

Aaron Pritz

CEO, Co-Founder, Partner

aaron@revealrisk.com

Chris Adickes

Consulting Director

chris@revealrisk.com

Michael Milroy

Senior Consultant | Service Delivery Lead

michaelmilroy@revealrisk.com

Eugene Korolyov

Senior Consultant | GRC & IR Lead

eugenekorolyov@revealrisk.com