Regs to Resilience

Energizing the Cybersecurity Compliance Journey

Terri Khalil

March 28, 2024

Can You Set It & Forget It?

How many of you have an IT and/or ICS environment that never changes?

- Where the equipment never changes?
- Where the technology never changes?
- Where the technology never touches IT or corporate or external networks?
- Where the business needs/requirements never change?
- Where the team members never change?
- Where the standards never change?

Compliance Landscape

Electric Sector and Critical Infrastructure

National Security

- Executive Orders, National Security Memo. & 1st 100 Days
- National Sec. Strategy & Impl. Plan
- CISA Cybersecurity Strategic Plan 2024-2026
- DFARS 252.204-7012 Safeguarding Covered Defense Info. & Cyber Inc. Rptg. & CMMC - contractual/federal

Critical Infrastructure

- NERC Critical Infrastructure Protection (CIP) - electric
- DHS CISA Cross-Sector Cyber Performance Goals
- DHS TSA Pipeline Safety Guidelines & Security Directives
- API 1164 Pipeline Control Systems Cybersecurity
- Cybersecurity Baselines for Electric Distribution Systems and DER
- Cyber Incident Reporting for Critical Infrastructure Act

ICS Cybersecurity

- NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations
- NIST SP 800-82 Guide to Industrial Control Systems (ICS) Security
- ISA/IEC 62443 Automation and Control Systems Cybersecurity Standards
- Consequence-driven Cyber-Informed Engineering
- Failure Mode and Effects Analysis (FMEA)
- NIST Risk Management Framework and Authorization Concepts

CyberKaleidoscope, LLC

AMPERE Industrial Security

How to Get Started

Leverage Existing Company Governance Models

- Code of Business Conduct
- Company-level Compliance Department/Committee
- Regulatory Affairs

Build

- Executive/Senior Sponsorship
- Director-level Steering
- Working Group – Subject Matter Experts(SMEs)/Leads/Managers

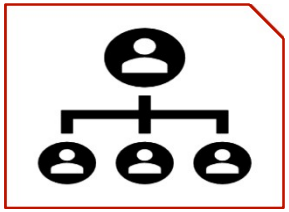
Set up a Charter – review and agree amongst the stakeholders

- Mission
- Purpose
- Responsibilities
- Scope
- Guidelines
- Relation to other internal governance structures
- Leadership Sponsor
- Agendas/Minutes/distribution for review
- Meeting frequency and attendance
- Annual review

Stakeholders

Anyone that can affect or be affected by the compliance program

- Who performs the ICS Security Compliance work?
- Who manages the ICS Security Compliance work?
- Who makes decisions about the ICS Security Compliance work and program?
- Who needs to know about the ICS Security Compliance program?
- Who can benefit from the success of the ICS Security Compliance program?
- Who can be harmed from the failure of the ICS Security Compliance program?
- Who can influence the ICS Security Compliance culture?



ORGANIZATION

Functional Areas

GEOGRAPHY

Multi-sites: city, state, nation, multi-affiliates and/or territories

KEY DECISION MAKERS

KEY INFLUENCERS

Subject Matter Opinion Leader

INVOLVEMENT ASPECTS

RACI

ONGOING ENGAGEMENT PLAN

Organizational Change Mgmt, Dept. Goals

Accountability

Getting to Ownership

Responsibility	Requirement Owner	Requirement Owner Manger	Requirement Owner Director	Cyber Asset SME	Cyber Asset SME Manager	Cyber Asset SME Direcotr	Compliance analyst	Compliance management
Develop and maintain relevant NERC CIP programs, processes, procedures, and forms.	R	R	A	C, I	C, I	I	C	
Perform relevant NERC CIP operational procedures, adhering to processes and programs.	R	R	R	R	R	A	C	
Review administrative updates to programs, processes, procedures, and forms							R	A
Inform compliance team of potential non-compliance issues	R	R	R	R	R	R	R	R

	SME Manager	SME	Additional SME Managers	Additional SMEs
CIP-007 R2	Ron Jon	Surfin' Joe	Kirk, Uhura, Jean-Luc	Spock, Scotty, Soran
CIP-007 R2.1	Ron Jon	Surfin' Joe	Kirk, Uhura, Jean-Luc	Spock, Scotty, Soran
CIP-007 R2.2	Ron Jon	Surfin' Joe	Kirk	Spock

RESPONSIBILITIES – Org Chart, RACI, Process

CODE OF CONDUCT ≠ Goals & Performance Review

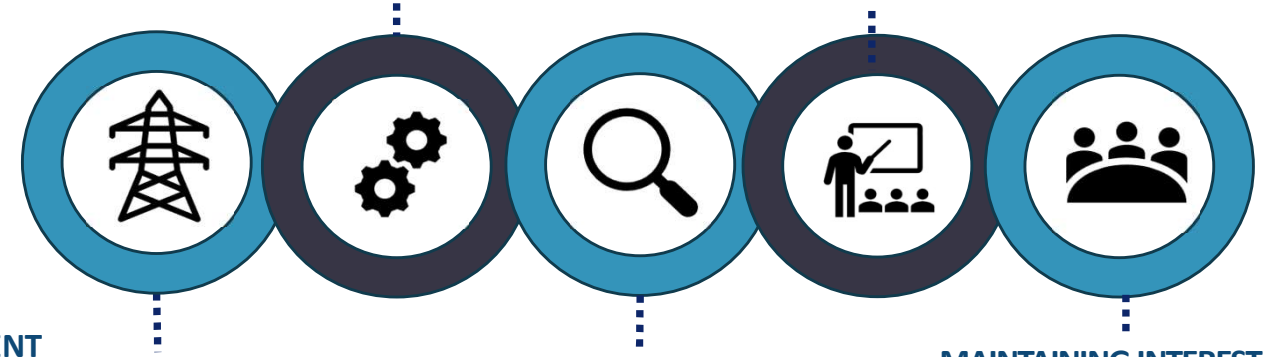
Unintended Consequences of Positive Discipline

OCM & Culture Change

- AWARENESS
- DESIRE
- KNOWLEDGE
- ABILITY
- REINFORCEMENT

HOW DO WE DO IT?
SME Collaboration
SME Training
Ongoing: New SME Orientation

VARIED LEARNING APPROACHES & POLICY
Process training/courses (record/store on LMS)
Lunch & Learns, 1-1s, Surveys
Policy Review/Update (e.g., annual)
End-to-end process reviews,
Assessments/Mock audits



WHY ARE WE DOING THIS & WHY IS IT IMPORTANT?
What's in it for me?
What are we really protecting?
Why we can't just check the compliance box.
"Awaring" isn't Caring → Pathos ← Use Stories

WHERE CAN I FIND MORE INFORMATION?
Program/Process/Procedures location/evidence site
Regulation/standards website
Your GRC or Compliance team

MAINTAINING INTEREST
What's going on in the world of cybersecurit
that the SMEs may want to know about?
REINFORCE: Validate processes/ & controls

Upcoming standards
Local workshops

DIMENSIONS OF SECURITY CULTURE
Carpenter/Roer

- Attitudes
- Behaviors
- Cognition
- Communications
- Compliance
- Norms
- Responsibilities

Interpretation:

Ensure Understanding of Standards & Requirements

- Content of the standards and requirements (and intent) vs. how your company does business.
- Processes, programs, and procedures → business-focused
- Compliance narrative → how you comply.

REQUIREMENTS

Review and carefully pay attention to every NOUN and VERB in the standard requirements.

TERMINOLOGY & GUIDANCE

Research every term in the standards and treat any defined terms as part of the requirements. Also review available guidance from the regulator and/or framework author.

COMPLIANCE MATH

Watch out for "compliance math" – it isn't always as straightforward as it might initially appear.

Planning for Implementation

Compliance Documentation Management

Establish:

- Documentation and Evidence Artifact Storage Sites for policies, standards, procedures, programs, processes, procedures
- Templates
- Naming Conventions
- Approval Processes
- Deviations from Standards (Exceptions/Risk Register)
- Compliance Tracking, Notification, and Escalation Methodology and Tool(s)

Planning for Implementation

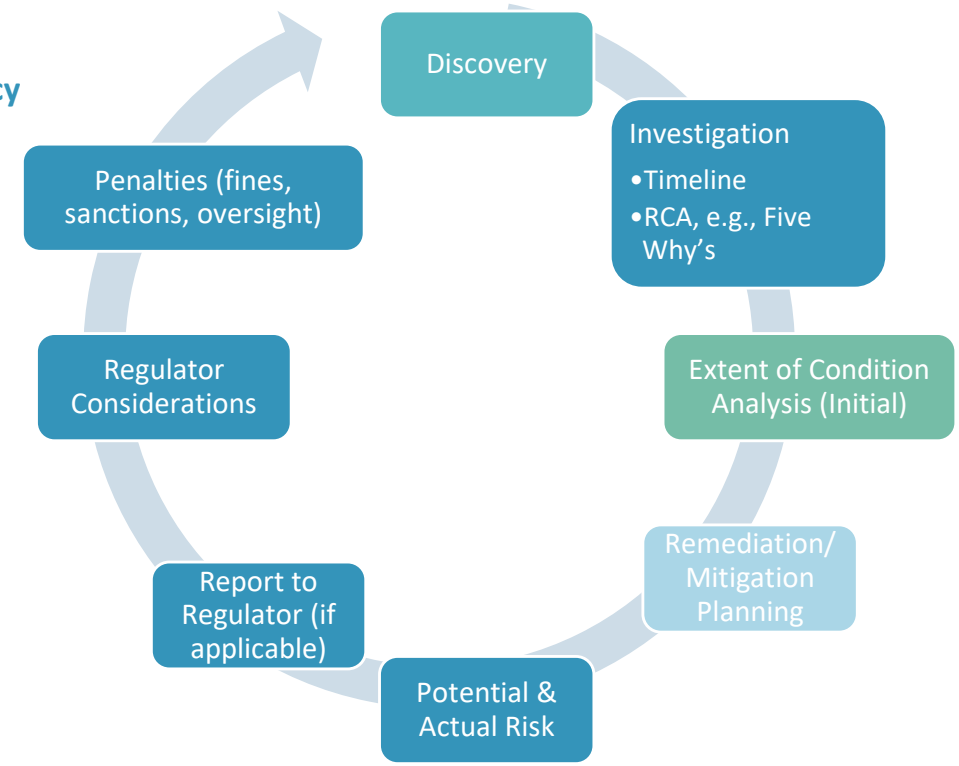
High-level Project Activities Leading to Establishing the Compliance Program

- Document/confirm/review scope, interpretation, and SMEs
- Determine gaps between current posture and the regulation/standards
- Determine relevant people, processes, and technology needed as well as budget
- Start grouping activities logically by function and/or by SME Teams and design workshops to be held to determine approaches and make decisions (requires a core person or small team to get this started)
- **Hold workshops with key SMEs or all relevant SMEs and document decisions made, approaches, etc., and any additional decisions needed**
- Design internal Controls to help stay compliant (preventive/detective)*
- Perform the work to meet the requirements; in parallel, begin writing the programs, processes and procedures..
- Plan for operationalization of the requirements.
- Set up tracking for periodic requirements, reminders, escalation
- **Establish Evidence & Documentation Management - Programs, processes, procedures, performance evidence e.g., forms, attestations, review/approval process**
- Train team members for reminders, escalation and evidence management
- Train SMEs on the processes

- **Operationalization: Day-to-day operations turnover**
- **Develop Compliance Narratives and perform final validation on Audit Readiness**
- **Perform early validations of performance evidence in first few months to ensure compliance is maintained**

Non-Compliance

Ensure both SME & Management Involvement along with Sense of Urgency



Remediation/Mitigation Planning:

- Correct initial issue and any extent of condition issues
- address the root cause, implement preventive controls and possibly additional detective controls
- perform training/communication
- update orientation

Reporting

Tailor Reporting & Measurement to the Audience

- Board
- Executives
- Directors
- Business Areas
- Company Compliance Committee and/or Affiliate reporting to parent

CURRENT ACTIVITIES

Impact to Compliance

Additions/changes to systems

Additions/changes to people

Additions/changes to facilities

Additions/changes to standards

NON-COMPLIANCE

Types of issues?

How discovered?

How bad is it (extent of condition

Are there any patterns or trends

What penalties are anticipated?

HORIZON & LONG-TERM FORECAST

New/revised standards

Leveraging frameworks for regulation & vice versa

Sustainability – expanding validation/assurance

Compliance ≠ Security

- Regulatory & Internal Standards Compliance can help security
- Still Need:
  - Cybersecurity Strategy
  - Cybersecurity Roadmap
  - Cybersecurity Operations, Risk Assessments, Vulnerability Assessments
  - And
  - And
  - And everything else….
- What about…?

What is Cyber Resilience?

"The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources." NIST

Developing Cyber-Resilient Systems: A Systems Security Engineering Approach NIST.SP.800-160v2r1.pdf

Cyber Resiliency Goals
- Anticipate
- Withstand
- Recover
- Adapt

Cyber Resiliency Objectives
- Prevent/Avoid
- Prepare
- Continue
- Constrain
- Reconstitute

Managing the Unexpected: Mindful Organizing by Karl Weick, Kathleen M. Sutcliffe
- Preoccupation of Failure
- Reluctance to Simplify
- Sensitivity to Operations
- Commitment to Resilience
- Deference to Expertise

Countering Cyber-Sabotage – Introducing Consequence-driven Cyber-informed Engineering (CCE) by Andrew A. Bochman & Sarah Freeman
- Consequence Prioritization
- System of Systems Analysis
- Consequence-based Targeting
- Mitigations & Protections

Sustaining Sustained Performance: "The ability to deal with a crisis situation is largely dependent upon the structures that have been developed before chaos arrives." Karl Weick

Funding Opportunities to Improve Cybersecurity

Past Grants

- **Clean Energy Infrastructure Funding Opportunity Exchange**
  - Bipartisan Infrastructure Law (BIL) Rural and Municipal Utility Cybersecurity (RMUC) Advanced Cybersecurity Technology Funding Opportunity Announcement (ACT FOA) 3/18/2024
  - Bipartisan Infrastructure Law (BIL) - 40125b Cybersecurity for Research, Development, and Demonstration (RD&D) Pre-app 1/10/2024 and Full app 5/16/2024
- CISA Cyber Grants Oct 2023
- DHS STATE AND LOCAL

New

- Cyber Grants - Florida [Digital Service] **Fiscal Year 23/24 Florida Local Grant Programs**
  - Federal State and Local Cybersecurity Grant Program, 11.9-million-dollar program,
  - Funded by U.S. Department of Homeland Security (DHS), in partnership with Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Emergency Management Agency (FEMA)
  - Florida's administering agency is the Division of Emergency Management
  - Grant application will open after December 2023; Two years of spending eligibility
- Water Sector: EPA's **Clean Water State Revolving Fund** and EPA's Cybersecurity Resources for Drinking Water and Wastewater Systems

Coming Soon! Full 1.5 Day Course

Terri Khalil

tkhalil@amperesec.com

Terri Khalil | LinkedIn

813-765-7703