ICS CYBER SECURITY CONFERENCE

SECURITYWEEK
CYBERSECURITY NEWS, INSIGHTS & ANALYSIS

Can You Set It and Forget it? Establishing an ICS Cybersecurity Compliance Program

By Terri Khalil

OCTOBER 23-26, 2023 | ATLANTA

Can You Set it and Forget It?

How many of you have an 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

Signaling is Clear

National Security

- Executive Orders, National Security Memo. & 1st 100 Days
- National Security Strategy & Impl. Plan
- CISA Cybersecurity Strategic Plan 2024-2026
- DFARS 252.204-7012 Safeguarding Covered Defense Information & Cyber Incident Reporting. & Cybersecurity Maturity Model Certification (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

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

Other Related

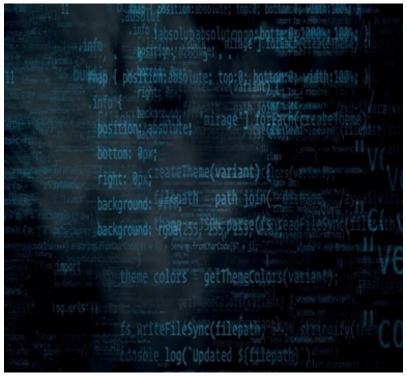
- NIST Risk Management Framework and Authorization Concepts
- NIS2 (EU)
- Consequence-driven Cyber-Informed Engineering
- Failure Mode and Effects Analysis (FMEA)

GOVERNANCE STRUCTURE

Compliance Project – Evolves to – Compliance Program

LEVERAGE EXISTING

- Code of Business Conduct
- Company-level compliance dept/committee
- Regulatory Affairs



BUILD

Executive/Senior Sponsorship

Director-level Steering

Working Group
(SMEs/Leads/Managers)

Charter

ICS Cybersecurity Program

The program charter can start out as a project charter and evolve over time.

- ✓ **Mission**
- ✓ **Purpose**
- ✓ **Responsibilities**
- ✓ **Scope**
- ✓ **Guidelines**

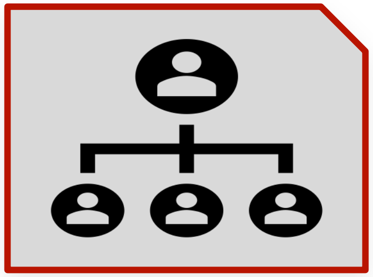
http://www.website.com

- Relation to other internal governance structures
- Leadership Sponsor
- Minutes – documented, responsibility (e.g., chair), distribution for review
- Meeting frequency and attendance
- Agendas
- Annual review
- Common responsibilities across major roles

STAKEHOLDERS

Anyone that can affect or be affected by the compliance program

- Who does 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 within city, state, and/or nation, multi-affiliates and/or territories

KEY DECISION MAKERS

KEY INFLUENCERS

Subject Matter Opinion Leader

INVOLVEMENT ASPECTS

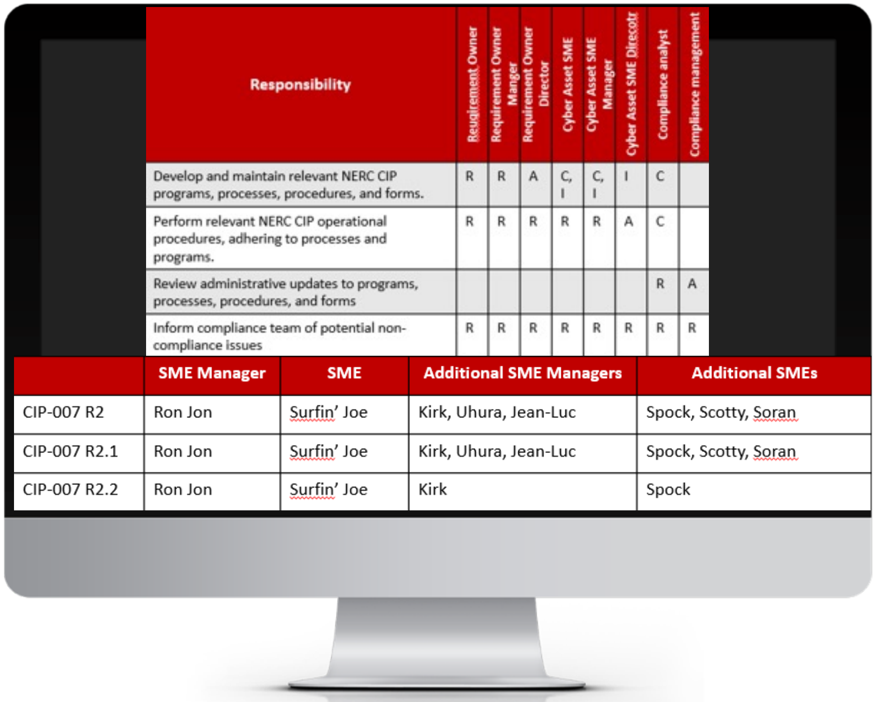
RACI

ONGOING ENGAGEMENT PLAN

Organizational Change Management, Department Goals

ACCOUNTABILITY

Getting to Ownership



Responsibility	Reugirement 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

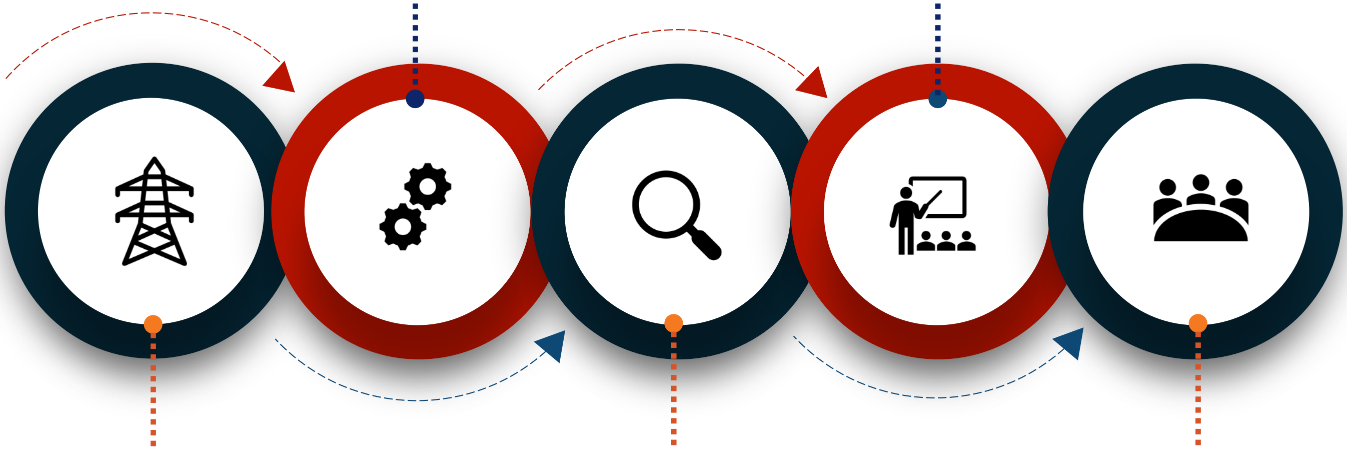
OCM & CULTURE CHANGE

Understanding the "Why" & Minimizing the Fear Factor

ORGANIZATIONAL CHANGE MANAGEMENT (OCM)

Example: PROSCI/ADKAR

- ✓ AWARENESS
- ✓ DESIRE
- ✓ KNOWLEDGE
- ✓ ABILITY
- ✓ REINFORCEMENT



HOW DO WE DO IT?

SME Collaboration
SME Training
Ongoing: New SME Orientation

VARIED LEARNING APPROACHES

Process training/courses (record/store on LMS)
Lunch & Learns
1-1s
Surveys
End-to-end process reviews
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 ICS Security that the SMEs may want to know about?

Upcoming standards
Local workshops

DIMENSIONS OF SECURITY CULTURE

Carpenter/Roer

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

INTERPRETATION

Ensure Understanding of Standards & Requirements

The content of the standards and requirements is not likely to match up to how your company does business. Careful interpretation analysis is required to ensure you are meeting the intent of the standards, especially those that are regulatory. Your processes, programs, and procedures will need to be business-focused, and a compliance narrative can be written to explain 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

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

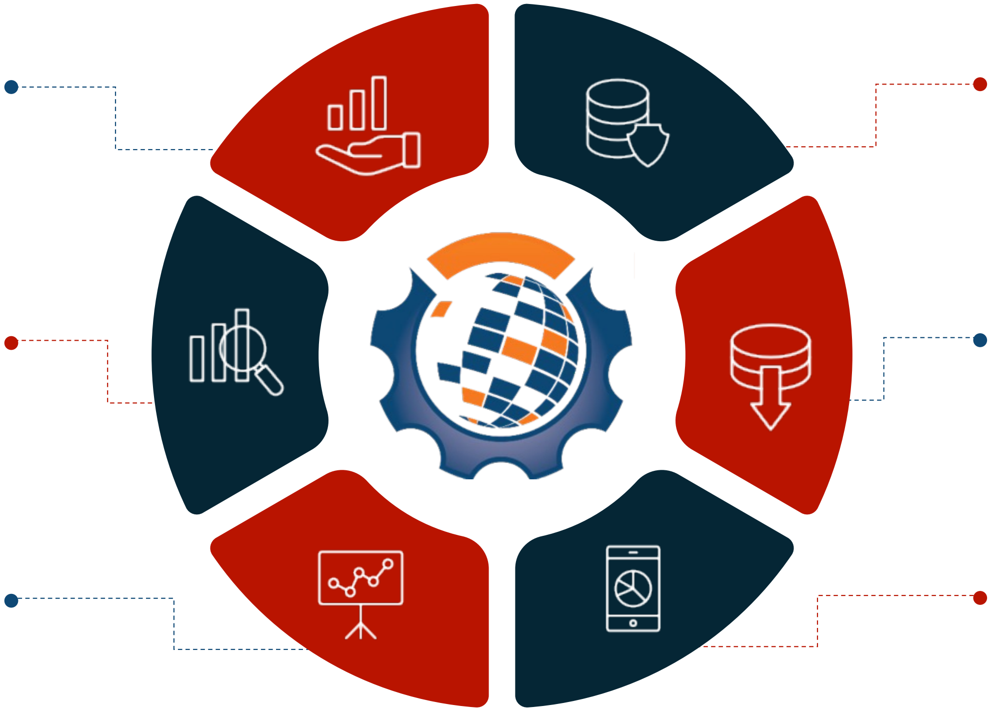
Develop Compliance Narratives and perform final validation on Audit Readiness

Perform early validations of performance evidence in first few months to ensure compliance is maintained

***Utilize Consequence-driven Cyber Informed Engineering (CCE) concepts and Failure Mode Effects Analysis**

Non-Compliance Issues

Ensure both SME & Management Involvement along with Sense of Urgency



Discovery of non-compliance issue

Investigation of non-compliance issue – timeline, Root Cause Analysis (RCA)

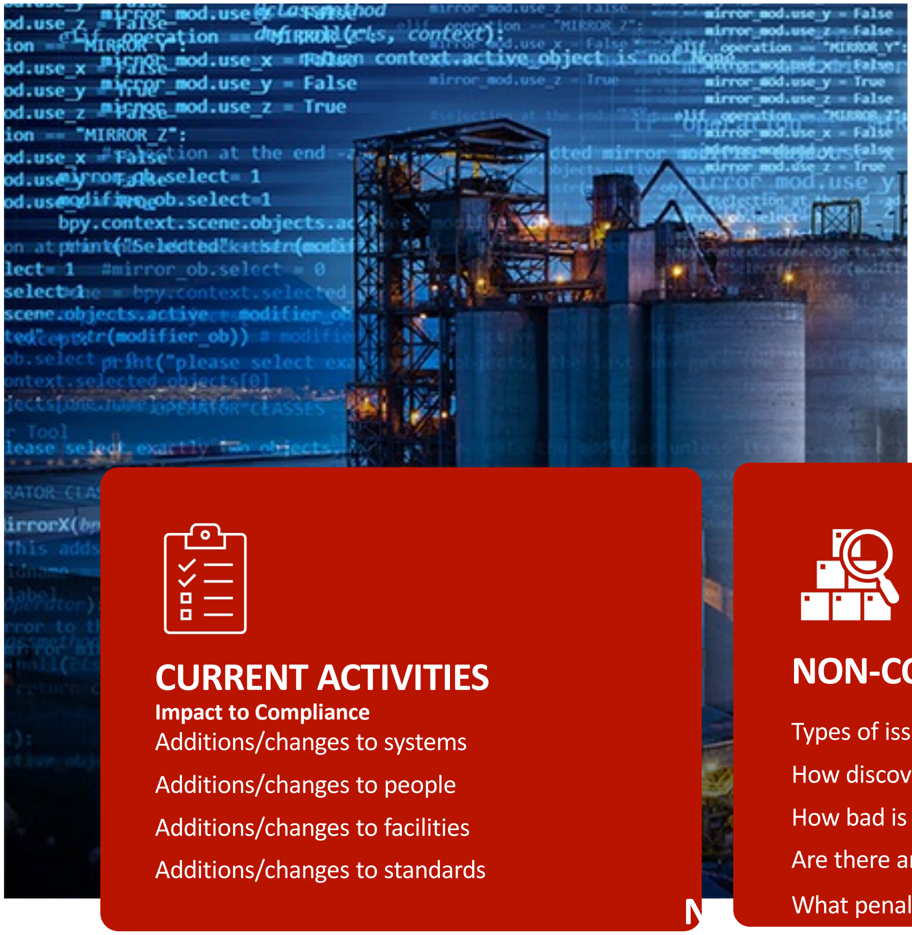
Extent of Condition Analysis

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

Report to the Regulator (if applicable)

Regulator Enforcement Considerations (if applicable), such as settlement and penalties



REPORTING

Tailor Reporting & Measurement to the Audience

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

CURRENT ACTIVITIES

Impact to Compliance

Additions/changes to systems

Additions/changes to people

Additions/changes to facilities

Additions/changes to standards

N

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

ICS CYBER SECURITY CONFERENCE

Questions?

Terri Khalil

✉ tkhalil@amperesec.com

in Terri Khalil | LinkedIn

☎ 813-765-7703

CyberKaleidoscope, LLC

AMPERE