Navigating New Cybersecurity Regulations

Charting a Course to Success

Terri Khalil

September 16, 2023
BSides 2023 – St. Pete

Navigating New Cybersecurity Regulations: Charting a Course to Success

Description

We'll dive into the surf of dealing with new cybersecurity regulations, just like a seasoned beachcomber navigating the ever-changing tides and shifting sands. Many companies find themselves new to the sea of cybersecurity regulations. We'll explore how these regulations may impact both IT and industrial control systems. The beach offers us valuable lessons on resilience, and as we build sandcastles of compliance, we'll uncover strategies to leverage these regulations to not only meet requirements but to strengthen our security posture like fortified sand walls against the tide. We'll discover that like every seashell along the shore, the regulations can hold the secrets of enhancing our cybersecurity resilience.

Cyber beach takeaways:

Attendees will leave the seashore equipped with a treasure trove of planning considerations for crafting an effective cybersecurity-related compliance program.

- With our beach chairs set up for this cybersecurity adventure, we'll **establish governance structures, key stakeholders, and communication channels** to ensure everyone charts the course together.
- We'll then hoist our compliance sails, catching the wind of **interpretation and scoping** to set a clear direction for our journey.
- Along the way, we'll learn **to manage the evidence** like beachgoers collecting seashells, making sure we have everything we need to stay on course.
- The tides of compliance ebb and flow, but we'll prepare for the **day-to-day operations**.
- We'll learn to surf the waves of **audits** and ensure our sandcastles of compliance remain resilient.
- And if we happen to encounter **non-compliance**, we'll report it like a diligent beach patrol, ensuring the safety of our digital shore.
- Our final destination will be **sustainabilit**y, where we'll anchor our compliance efforts for long-term success.

So, whether you're a seasoned beachcomber of cybersecurity compliance or a new adventurer, join us as we embrace the shoreline of success, discovering valuable insights and charting a course towards cybersecurity resilience.

Snippet from Conference Agenda for context.

Terri Khalil

Founder - CyberKaleidoscope, LLC

Senior Consultant - Ampere Industrial Security, Inc.

- Former IT Director at Tampa Electric Company - IT Compliance & Assurance, PMO, IT AM/VM, Benchmarking & Metrics, Security Awareness
- Experience in electric and gas industries
- Certs: CISSP, CISA, CISM, CRISC, ITIL Foundations
- Career break - the carpool mom
- Range of InfoSec roles in global accounting firm
- Began career in retail point-of-sale systems for small home improvement chain.

http://www.linkedin.com/in/terrikhalil/

Terri@CyberKaleidoscope.com

- USF Corporate Mentor Program
- BS, Management Information Systems, University of South Florida
- MBA, USF (only 4 years ago)

Agenda

DISCOVERY THAT YOU ARE IN SCOPE

GOVERNANCE STRUCTURE

STAKEHOLDER IDENTIFICATION

UNDERSTANDING OF ACCOUNTABILITY

UNDERSTANDING THE “WHY” & MINIMIZING THE “FEAR FACTOR”

[COMMUNICATIONS]

INTERPRETATION & SCOPING

IMPLEMENTATION PLANNING

REPORTING

NON-COMPLIANCE

RESILIENCE & SUSTAINABILITY

Discovery that Your Company is in Scope

- Timing depends upon compliance effective dates.
- Considerations if you have to move quickly:
  - Communications deep and wide as soon as you find out: High-level list of the most impactful (effort, costs, technology implementations) based on your initial review
  - A first pass at governance, stakeholders, communications
- Ideal state: proactively set up a compliance program for a well-known standard if you haven’t already. Get ahead before mandated.

- Recommendation (if not following any standard) – start with the CISA Compliance Performance Goals (CPGs).
- Cover the basics such as:
  - Buy only “trusted” hardware, software, services
  - Know all cyber assets in your environment
  - Know the security posture for all cyber assets
  - Segment and restrict access (e.g., MFA, zero trust)
  - Monitoring and detection at asset & network level
  - Strong incident response capability
  - Strong recovery capability
- Aligns with guidelines, regulation, executive orders, national security memos etc. in critical infrastructure sectors

Governance Structure

Leverage existing elements in your company, such as:

- Business Code of Conduct
- Company-level Compliance Department
- Corporate Compliance Committee
- Regulatory Affairs Department and associated Internal Compliance Program

Program Approaches

- Existing Governance, Risk and Compliance (GRC) team
- Security Team
- Business Area

Sample Structure

- Executive/Senior Leadership (Senior Sponsorship or Executive Committee)
- Steering Committee - Director-level
- Working Group (or xREG Team)
  - Managers/Leads ("Performance Coaches")
  - Subject Matter Experts

NIST Cybersecurity Framework 2 (Draft) – GOVERN Section

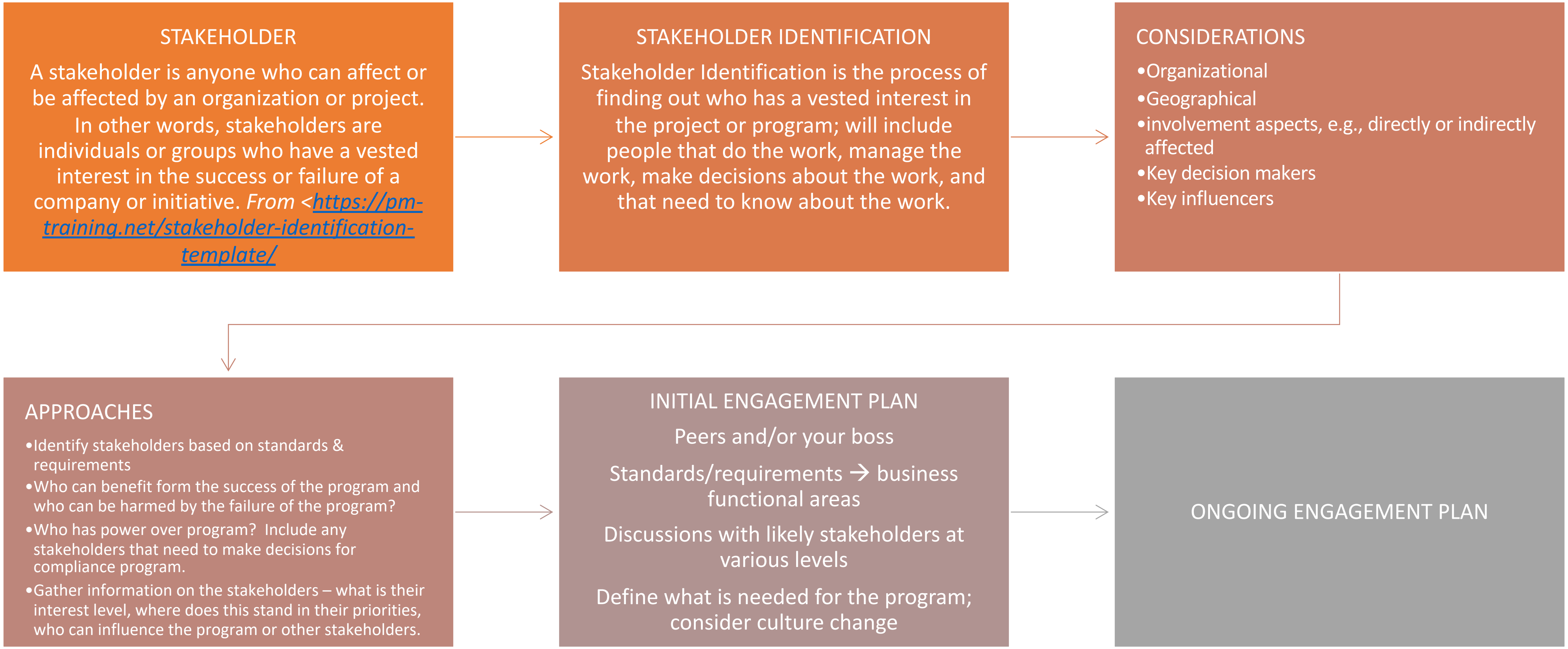
- Establish and monitor the organization’s cybersecurity risk management strategy, expectations, and policy.
- **How an organization will achieve and prioritize the outcomes** of the other five Functions in the context of its mission and stakeholder expectations.
- **Roles, responsibilities, and authorities; policies, processes, and procedures; and the oversight of cybersecurity strategy**.
- *COBIT, Other

Why do I really need to attend?

Governance Structure (Steering Committee) Elements

- Mission/Driver
- Purpose/Description
- Goals
- Responsibilities of the Steering Committee
- Scope
- Guidelines
- 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

Stakeholder Identification



STAKEHOLDER

A stakeholder is anyone who can affect or be affected by an organization or project. In other words, stakeholders are individuals or groups who have a vested interest in the success or failure of a company or initiative. *From <https://pm-training.net/stakeholder-identification-template/*

STAKEHOLDER IDENTIFICATION

Stakeholder Identification is the process of finding out who has a vested interest in the project or program; will include people that do the work, manage the work, make decisions about the work, and that need to know about the work.

CONSIDERATIONS

- Organizational
- Geographical
- involvement aspects, e.g., directly or indirectly affected
- Key decision makers
- Key influencers

APPROACHES

- Identify stakeholders based on standards & requirements
- Who can benefit form the success of the program and who can be harmed by the failure of the program?
- Who has power over program? Include any stakeholders that need to make decisions for compliance program.
- Gather information on the stakeholders – what is their interest level, where does this stand in their priorities, who can influence the program or other stakeholders.

INITIAL ENGAGEMENT PLAN

Peers and/or your boss

Standards/requirements → business functional areas

Discussions with likely stakeholders at various levels

Define what is needed for the program; consider culture change

ONGOING ENGAGEMENT PLAN

Understanding of Accountability

Getting to Ownership

- Responsibilities
  - RACI Matrices
  - Role Descriptions
  - Process Roles & Responsibilities Section
- Code of Conduct ≠ Goals & Performance Review
- Ins/Outs (Unintended Consequences) of "Positive Discipline“

Subject Matter Expert (SME) List & Modified RACI

- Approaches to SME List
  - Org Chart – helpful for orientations for new stakeholders and for presentations to a regulator
  - Modified RACI – by Standard Requirement/Sub-requirement - helpful for clarity of who does what
  - Outlook Distribution list – great for meeting invites and news

- Considerations:
  - All methods need frequent updating (recommendation: minimum quarterly)
  - Who facilitates amongst the cyber asset SMEs for a given requirement? Example: Patching Program owner vs. patching a Linux asset, a windows desktop, a windows server, a switch, a firewall, etc.

Sample RACI – *note these may be different in every organization*

Responsibility	Reuqirement 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
Facilitate process to ensure investigation of non-compliance								
Fill out non-compliance and perform root cause analysis, identify corrective steps, and identify new preventive controls								

Roles	Role Description
R – Responsible	This role is in charge of completing that activity - the one doing the work – or better, the one *responsible* to do the work. Try not to have more than one person responsible; may need to make the task more granular.
A – Accountable	This role indicates the person who *owns the outcome* of the activity, i.e., "being held accountable" - the person who will bear the consequences if the activity is completed or not, or if the activity has a good outcome or not. So, the accountable person must ensure the responsible person has everything s/he needs to do the work. If the responsible person is not getting things done, the accountable person generally has the authority to replace the responsible person. In short, the accountable person does not do the work, but people will go to him/her rather than the *responsible*. There is only one accountable person.
C – Consulted	This role is consulted while performing the activity. Mainly, it is the responsible or accountable person who goes to the consulted person to ask for *advice and validation*. Depending on the organization and project, the consulted role may have more or less power over the outcome of the project.
I - Informed	This role is for people who must be informed on the status of an activity. It will be the duty of responsible and accountable to inform them, generally with emails, newsletters, and meetings.

Sample Modified RACI

	SME Manager	SME	Additional SME Managers	Additional SMEs
CIP-007 R2 Patching	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
CIP-007 R2.3				
CIP-007 R2.4				
CIP-007 R3				
CIP-007 R3.1				
CIP-007 R3.2				
CIP-007 R3.3				

Understand the "Why" & Minimizing the Fear Factor

Address the Fear Factor: I don't want to work on *compliance* – I don't want to get a violation

Why are we doing this and why is it important?

____

Above/beyond the regs- what we are really protecting and why we can't just check the compliance box

What's in it for me?

How do we do it ?

____

The processes – have SMEs been trained, do they know where to locate the documentation?

What about new SMEs? New to company, dept – orientation?

Where can I find more information?

____

Your evidence site and Program/Process/Procedure documentation

Regulation website

Your GRC or IT compliance team

Other?

Varied Learning Approaches

____

Process Training (recorded and stored on LMS)

Course (s) & Lunch n learns

1-1s/Hallway Conversations

Surveys

Orientations

End-to-end process reviews

Mock audits

Maintaining Interest –

What's going on in the world that the SMEs may want to know about?

____

Upcoming standards

Local workshops

Conferences

Ambassadors/Champions

News via our cyber resources that we see that our SMEs may not be seeing

Teach * Communicate * Learn

"Awaring" isn't Caring → Pathos ← Use Stories

Organizational Change Management PROSCI/ADKAR): Awareness * Desire * Knowledge * Ability * Reinforcement [Reduce Resistance|Increase Desire]

Carpenter/Roer: Seven Dimensions of Security Culture – Attitudes, Behaviors, Cognition, Communications, Compliance, Norms, Responsibilities

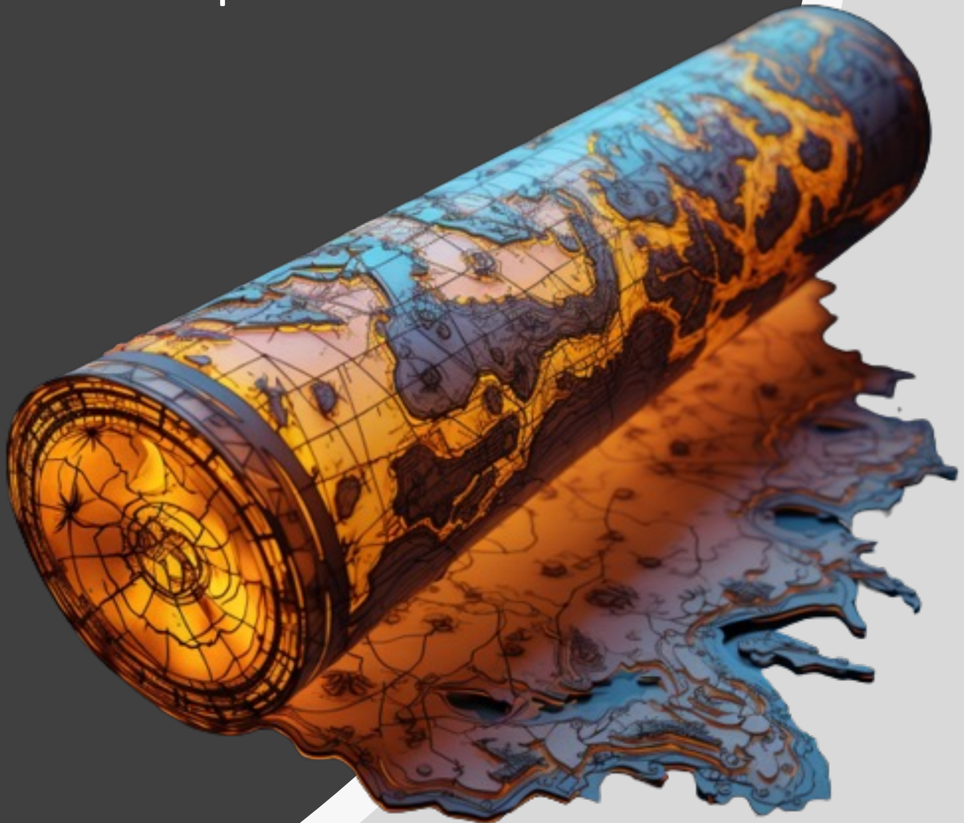
Interpretation & Scoping

Review and carefully pay attention to every NOUN and every VERB in the requirement for each standard

Research terms within the framework

Watch out for “compliance math”

Planning for Implementation



- Document/confirm/review scope 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)
- **Tracking periodic requirements, reminders, escalation**
- **Evidence/Documentation Management**
  - **Programs, processes, procedures, performance evidence e.g., forms, attestations**
  - **Review/approval process**
- Training for reminders, escalation and evidence management
- Training for SMEs on the processes
- Day-to-day operations turnover
- Perform final validation on Audit Readiness
- Perform early validations in first few months to ensure compliance is maintained

Non-compliance

- Discovery
- Investigation – timeline, Root Cause Analysis (RCA)
- Extent of Condition
- Remediation/Mitigation Planning
- Include milestones such as:
    - Correct the issue and the extent of condition issues
    - Address the root cause(s)
    - Implement preventive controls and possible detective controls
    - Train and communicate
    - Update orientation
- Reporting to Regulator

- SME & Management Involvement
- Sense of Urgency
- Enforcement Considerations
- Penalties

Reporting – How are we Doing?

It's been quiet lately – maybe we don't need to have resources on that?

Tailor to your Audience

Board
Executives – CEO and Officers/VPs
Director
Business area
Company Compliance Committee/Group and/or Affiliate reporting to Parent company

Do the business area leaders know about a PNC that occurred in their area?

Content

- Current activities with NERC CIP impacts (risks/challenges/how addressing)
  - Additions/changes to systems – e.g., new asset inventory or discovery tool, new SIEM tool, EMS upgrade, new PACS
  - Additions/changes to people
  - Additions/changes to facilities – new sites, de-NERC'ing a room, NERC'ing a room
  - Additions/changes to standards in progress e.g., BCSI Access Management, Supply Chain for Lows
- Non-compliance
  - What types of issues? How discovered? How bad is it (extent of condition)? Are there any patterns or trends? Are these going to have any penalties?
- The Horizon and Long-term Forecast ($$$)
  - New/Revised Standards (e.g., Virtualization, Supply Chain for Lows)
  - Leveraging NERC CIP regulation to new regulations or internal frameworks if applicable
  - Sustainability – expanding the validation/assurance concepts of CIP-007

Why does this keep happening? How much is this going to cost to remediate and for penalty? Will we have additional regulator oversight? What are we doing about it?

?

Thank you!

FEEDBACK?