Sharing Resources in CIP Programs

For GRC and Cybersecurity Programs

April 25, 2025

Introduction

- NERC developed the Critical Infrastructure Protection (CIP) regulations
- Implementing and operating CIP programs requires multiple departments and cross-functional teams
- Siloed and integrated CIP programs hold different risks that must be managed
- Sharing resources in CIP programs can:
  - reduce some risks and introduce new risks
  - lower operating costs
  - increase collaboration
  - make more resources available
  - impact sub-cultures

Compliance Scenarios

Scenario 1: Minimum Compliance

- CIP programs are built for minimum compliance
- Interpret the requirements and implement the program
- Improvements are only necessary if non-compliance event occur
- Reactive versus proactive
- Years of minimum compliance will vary with organizations

Scenario 2: Program Integration

- Multiple compliance programs exist
- Commonalities are implemented across programs
- Internal audit is an active stakeholder
- Organizational requirements are required
- Common among matured programs and organizations

Scenario 3: Hybrid of Scenario 1 and 2

- Compliance maturity falls between minimum and program integration
- Resource availability (budget, SME, time, etc) is usually an indicator of where the organization falls on the scale

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

SIMPLI GRC

Common Functions for CIP Programs

Common Scenarios

- CIP requirements mandate the application of information security and cyber security across people, process, and technologies
- The feasibility of a few teams operating and maintaining a full CIP program is possible but improbable.
- Most CIP programs require representation from many functional teams to implement and operate.

Common Functional Teams

- Network and Firewalls
- Cyber security
- Servers / Infrastructure
- Application
- Middleware
- Corporate / Physical Security
- Engineers (Automation / Protection / SCADA)
- Operators (Plant / Control Center)
- Plant Managers
- Internal Audit
- Analysts (Compliance / Business / Technical)
- Legal
- Human Resources
- Leadership

CIP Program Challenges & Examples

Challenges	Examples
Conflicting Operating Models	
Functional teams may be required to follow multiple policies	Reporting to a CIP Senior Manager that is outside of the SME's department
Existing portfolio of services and requirements which may conflict with CIP	Compliance with other regulations, frameworks or standards
Resource constraints to include additional CIP tasks	The addition of CIP assets may introduce additional resources required to operate
Teams developed their methods to execute activities and tasks and the impact of change requires assessment with many stakeholders	Risk management is sometimes team-based and may not align with risk-based activities in CIP programs
Teams are required to follow CIP processes to execute their functional tasks	Patching within 35 days or follow the exception process may be new to patching teams
Culture Clash	
Sub-cultures can impact expected outcomes of a CIP program	The sub-culture of a network / firewall team may require decisions from the experienced team lead versus the CIP compliance team
Resistance to change, unwillingness to adapt to CIP requirements	Changing or adopting delivery times for reviewing SIEM events
Competing Priorities	
Sharing resources in different teams with different leaders will most likely experience competing priorities	A physical security team resource may prioritize other physical sites due to performance objectives
Team leadership may have opposing objectives	The control center is required to monitor non-CIP assets where the IT cyber security team requires CIP to be prioritized

Indicators to Share Resources

Business Goals and Objectives

- Organization requires alignment with mission objectives
- Restructuring of the organization

Resource Constraints

- Limited compliance budgets are less than compliance metrics
- Functional SMEs in different teams have other priorities
- Deadlines are constantly missing target dates
- Culture compatibilities are not improving

Compliance Risks are Not Improving

- Sub-cultures impact expected outcomes of a CIP program
- Resistance to change, unwillingness to adapt to CIP requirements

Necessary Skills are Missing

- Compliance team members are executing tasks outside of their core competency
- Personnel retention is inconsistent
- CIP requirements are misunderstood

Benefits to Share Resources

Cost Controls

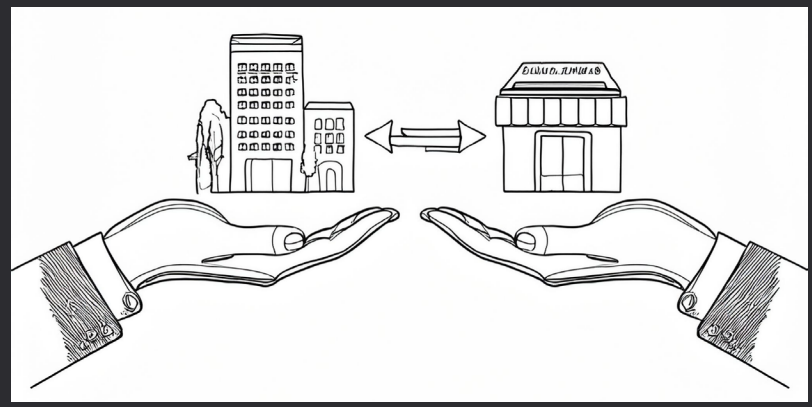
- Use resources from other teams as needed versus onboarding all the necessary people, process, and technology

Instilling Institutional Knowledge

- Siloed CIP program holds risk of key SMEs leaving the organization with the knowledge they gained
- Cross-functional teams and cross-training help to retain knowledge in the organization and program
- Promotes a positive culture

Stronger Risk Management

- One risk management program and operation reduces conflicts
- Greater visibility for the organization



Considerations

Appropriately Assess Challenges

- CIP does not state requirements for the mentioned challenges but they are inherent for compliance success
- The processes and results are the critical measures to meeting the requirements
- Assess for cultural impacts

Knowledge Retention

- Build required knowledge base to remain with the organization
- Retain and improve upon existing knowledge

Unify Multiple Programs

- CIP programs are usually siloed, unless the organization is matured, to reduce compliance risk
- Many environments deem it necessary to silo the CIP program due to incompatibilities with other program requirements
- Unify components of different programs where it generates value

How SimpliGRC Can Support

- Implementing and assessing NERC, ARS, and MRS CIP Programs
- Successfully completed several NIST CSF, CIP, CIS, and ISO assessments and audits
- Softening silos and sub-cultures to achieve enterprise or project goals
- Experienced in Business Impact Analysis and Risk Assessments
- Senior analysis and project management services
- IT / OT convergence services in complex environments
- Strategy development and implementation
- Process development and re-engineering
- The managing directors deliver the services to offer the direct experience and competencies
- Local to Calgary and Edmonton in Alberta, Canada

THANK YOU

info@simpligrc.com

https://simpligrc.com/about/contact/

Visit our blog about risks in CIP programs
https://simpligrc.com/2025/03/25/identifying-risks-in-cip-programs/