TSA Governance & Compliance Framework

November 5, 2024

SIMPLI GRC

Current Situation

- **Issue:** Align and integrate existing TSA cybersecurity compliance into your organization's cybersecurity program
  - Need an organization's TSA compliance solution – not another company's program
  - Need strong governance, risk management and compliance processes built on management preferences and culture
- **Issue:** Per TSA requirements, corporate and OT cybersecurity programs need to work together effectively
  - Need processes for the effective communication of threats, vulnerabilities and potential risks
  - Need a coordinated incident response plan to effectively operate
- **Issue:** TSA compliance reporting of both the corporate and OT environments
  - Program needs to show secure, risk managed environments for pipeline operations
- **Issue:** Compliance evidence & personnel need to be ready for a TSA audit by operations transition

TSA General Guidance

Organizations are permitted to develop their own document management & risk management methodologies for compliance with TSA directive

TSA wants evidence of regular monitoring of both organization changes & TSA Security Directives changes to ensure risk is effectively managed

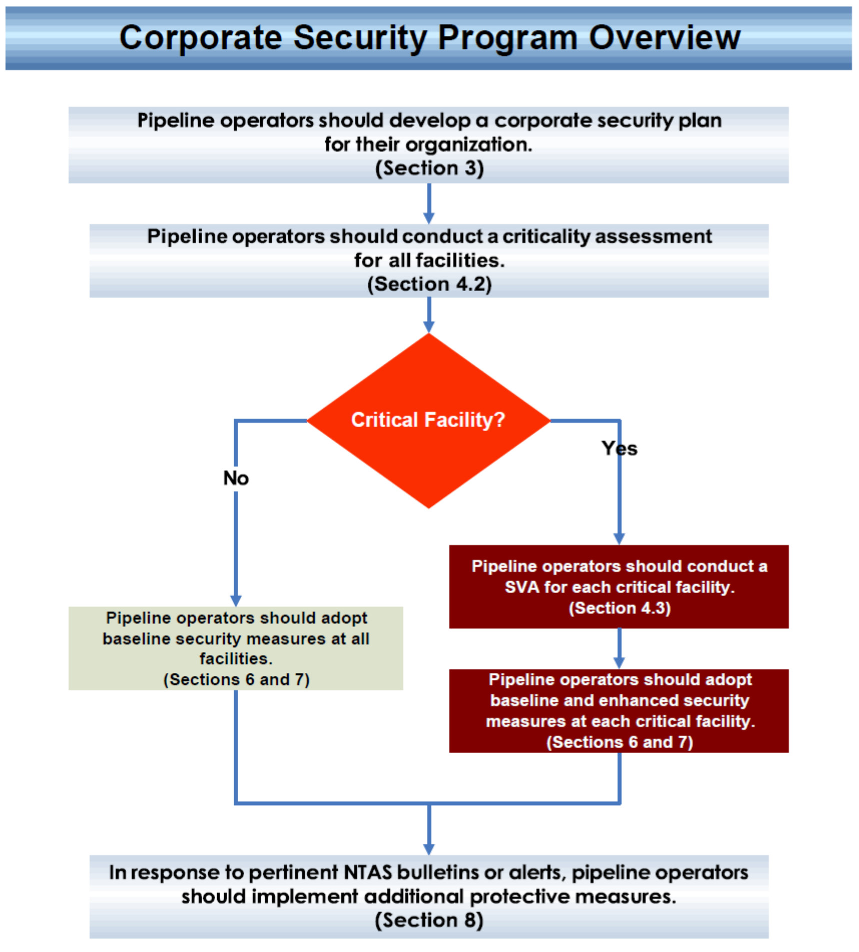
TSA will look for formal documentation for:

- Identifying & implementing new or changed requirements contained within the TSA Security Directive
- Formal and continuous threat-vulnerability-risk assessments of critical facilities
- A comprehensive and well-tested incident response plan
- A business recovery/continuity plan for pipeline operations
- Formal approval by senior management
- Communication of changes throughout the organization
- A formal annual assurance plan
- Collecting and securing TSA sensitive information and evidence

SIMPLI GRC

Overview of Core TSA Requirements

- Enterprise / Corporate Security Program
- Corporate / OT Security Plan consisting of:
  - Implementation and improvements plan
  - Incident management plan
- Facility Security Measures
  - Structured around critical and non-critical pipeline facilities
  - Asset collection and categorization
- Asset Risk Analysis
  - Threat-vulnerability analysis
  - People (focus on awareness, training & competencies)
  - Processes (heavy on documentation and management approval)
- Cyber Asset Security Compliance Measures
  - Controls implemented
  - Monitoring and measurement
  - Evidence capture and reporting
- Protective Measures for NTAS Alerts



Corporate Security Program Overview

Pipeline operators should develop a corporate security plan for their organization. (Section 3)

Pipeline operators should conduct a criticality assessment for all facilities. (Section 4.2)

Pipeline operators should adopt baseline security measures at all facilities. (Sections 6 and 7)

Pipeline operators should conduct a SVA for each critical facility. (Section 4.3)

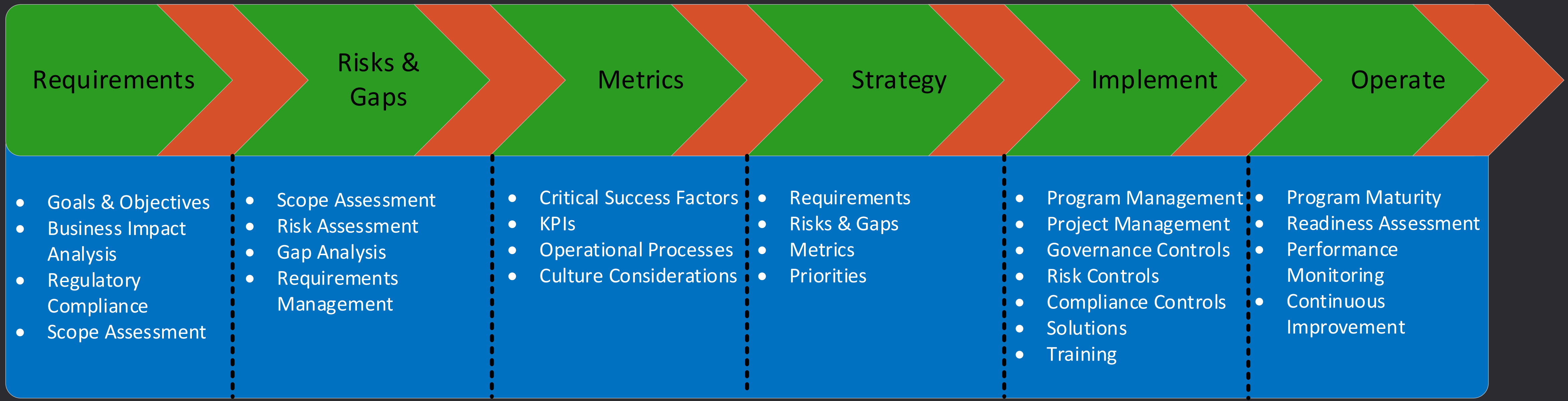
Pipeline operators should adopt baseline and enhanced security measures at each critical facility. (Sections 6 and 7)

In response to pertinent NTAS bulletins or alerts, pipeline operators should implement additional protective measures. (Section 8)

TSA Program Considerations

- Ensure regular consultation with TSA regulator
- Integration of TSA program with organization structure
  - Roles and responsibilities are defined and communicated
  - Accountabilities are accepted and endorsed
  - Appropriate training is provided to operate the GRC & TSA programs
- TSA program management
  - Ensure metrics for governance and compliance
  - Update ERM to accommodate TSA risk management requirements
  - A unified program for both IT and OT reduces compliance risk
- TSA implementation plan
  - Implemented controls are managed, monitored and reported
  - Sensitive evidence collected and access is managed
- TSA annual assurance plan
  - 1/3 of assets need to be reassessed each year

TSA Governance Program Approach



Requirements	Risks & Gaps	Metrics	Strategy	Implement	Operate
• Goals & Objectives • Business Impact Analysis • Regulatory Compliance • Scope Assessment	• Scope Assessment • Risk Assessment • Gap Analysis • Requirements Management	• Critical Success Factors • KPIs • Operational Processes • Culture Considerations	• Requirements • Risks & Gaps • Metrics • Priorities	• Program Management • Project Management • Governance Controls • Risk Controls • Compliance Controls • Solutions • Training	• Program Maturity • Readiness Assessment • Performance Monitoring • Continuous Improvement

SIMPLI GRC

Document Management: Example Processes

Process for identifying new or changed requirements based on current TSA Directive

Ensures TSA requirements are continuously monitored and captured by the organization

Ensures business/operating changes within the organization remain aligned with TSA requirements

Process for creating standardized draft documents capturing the TSA requirement(s):

Requirement(s) & scope stated and understandable by the organization

Proposed control(s) will effectively address requirement(s)

Compliance can be objectively and consistently measured

Evidence collected, stored, & maintained in a manner ensuring confidentiality, integrity & availability

Document change tracking

Process for SME document review document to confirm:

Controls meet requirement(s) and objectives

Applicable evidence is captured & stored appropriately

Process for formal approval of document

Irrefutable proof of approval

(NOTE: approval by senior management is required)

Date of approval

Date of next review/approval

Process for publishing approved documents

Demotion of old documents into an archive

Promotion of approved documents into a public library

Communication of document changes to all relevant parties

SIMPLI GRC

TSA GRC Program

- As a minimum, TSA requires:
  - Continuous monitoring of TSA Security Directives to ensure ongoing compliance
  - Accurate cyber-risk assessment of critical facilities with strong vulnerability management
  - Continuous, objective monitoring and evidence reporting of pipeline security
  - Reliable and responsive incident management
- Organizations examine its "GRC" solution for gaps in meeting TSA Security Directives (SDs)
  - Policies, standards, procedures, processes for effective development controls
  - Capturing, categorizing and prioritizing critical assets based on consistent risk assessments
  - Completing threat-vulnerability-risk assessments
  - Selecting and implementing controls based on risk prioritization
  - Developing metrics, measurement methods and evidence
  - Providing a project management planning and execution for the successful integration of TSA compliance into the applicable IT and OT environments

How SimpliGRC Can Support

- TSA Pipeline experience with two major pipeline firms
- 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/