Effective Models for IT/OT Collaboration

ISA Calgary OT Cybersecurity Interest Group

January 16, 2025

Introductions

Eric Cosman

- 35+ years experience in industrial information technology
- Founding member and co-chair, ISA99 committee

Norm Runte

- 30+ years as IT auditor
- 25+ years assessing critical infrastructure cybersecurity
- https://www.credly.com/users/norman-runte

Ashif Samnani

- 20+ years in IT OT Cyber Security
- GRC, SecOps and OT

Burt Kim

- 25+ years experience across IT and OT industries
- GRC Consultant

Greg Potter

- 40+ years experience in process control. Last 20 involved in OT cyber
- Senior Automation Advisor

Purpose

- Provide past experiences and opinions on the topic
- Collaborate with industry professionals on the topic
- Share ideas on prior successes and challenges

Convergence vs. Collaboration

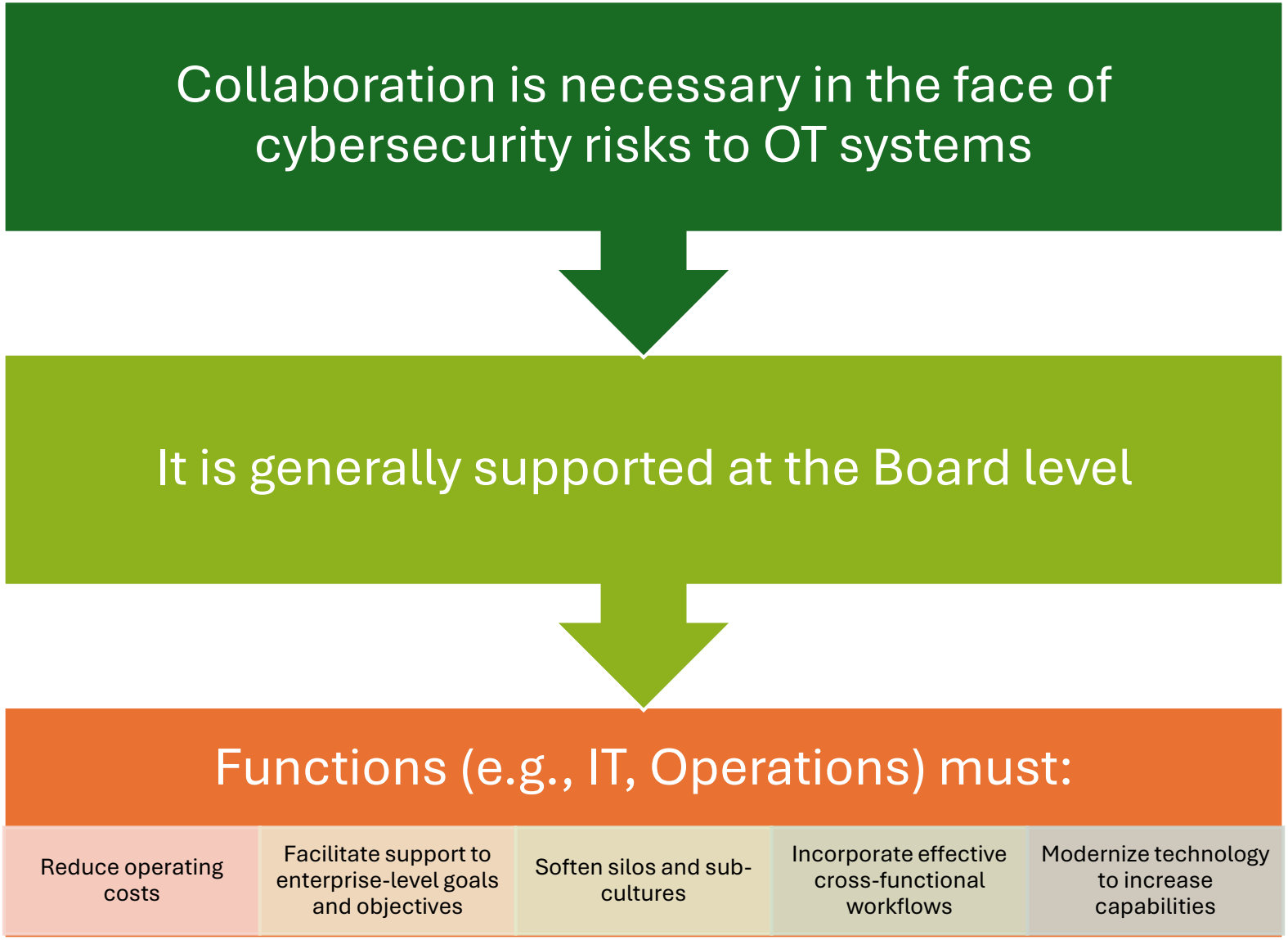
Interpretations:

- Convergence suggests technology focus only.
  - Industry 4.0 acted as a catalyst for IT/OT Convergence
- Collaboration suggests shared accountabilities and responsibilities
- Sharing of resources across people, process, and technology in IT and OT
- Starting with IT suggests OT will integrate with IT
- Operating models that exist at different organization levels
- Collaboration is a methodology to achieve a goal (Enable vs Methodology)

Stakeholders:

- Enterprise (Board)
- Corporate (IT, Finance, HR, Cyber, etc.)
- OT (Operations, Engineering, Maintenance, Risk Management, Process Safety, Physical Security Representatives, etc.)

Business Drivers



Opportunity Statement

Increase IT/OT collaboration to address cybersecurity risk.

Root Causes

Culture Clashes

Differing ideas on Collaboration

Guarding one's territory

Office politics

Competing Priorities

Organizational vs. Shared objectives

CIA versus SAIC – Safety is **paramount** in OT

Misalignment of Governance

Cross-functional teams are reporting up through separate structures

VP's resulting in lack of common vision & collaborative missions

Insufficient engagement from the Board and/or executives

Symptoms

- One department holds their priorities over the other
- Low understanding of the other department's operations
- Initiative is driven without comprehensive requirements
- Shadow IT initiatives – Initiatives outside authorized IT programs
- Enterprise goals and objectives miss targets
- Win / Lose situations

Mitigations

Enterprise goals and objectives:

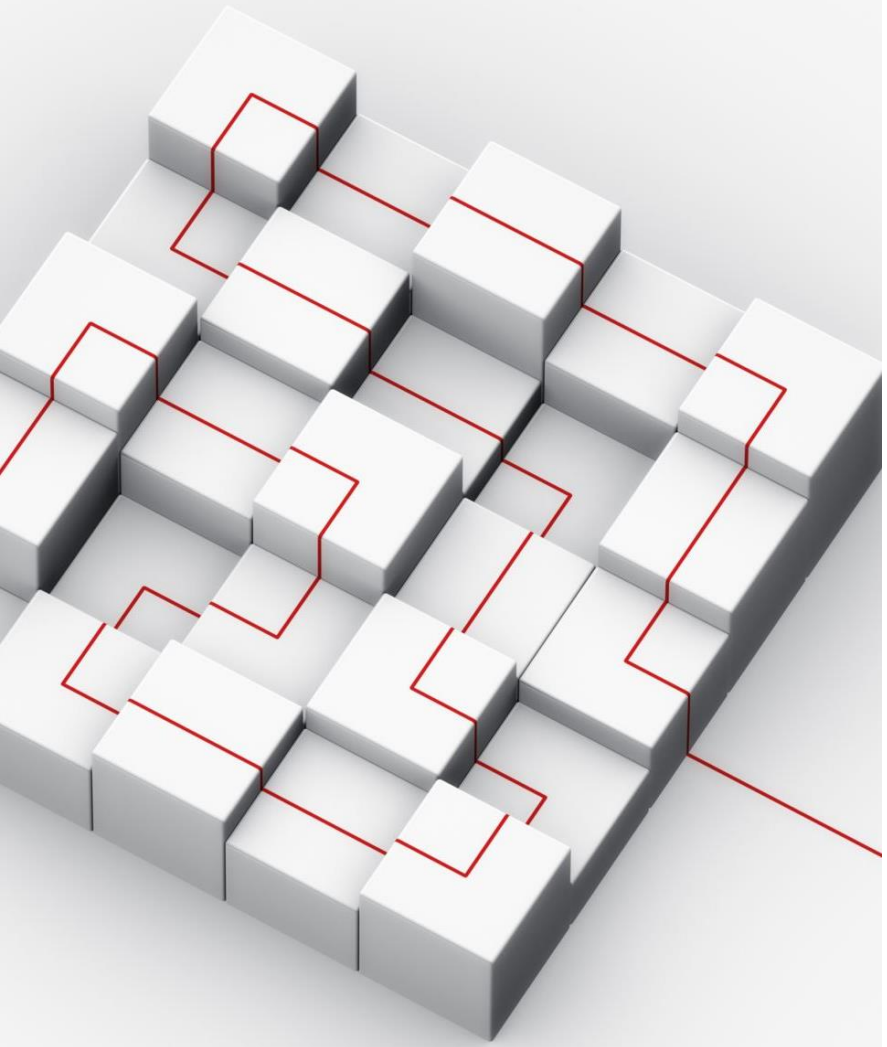
- Formed to IT and OT mission objectives
  - Support objectives with convergence outcomes
- Use a shared risk management program
  - Risk informed decisions

Governance across IT and OT

- Executive support and endorsement
- Update policies where applicable
- Reflect requirements and risks
- Use compliance as a base

Program versus Project

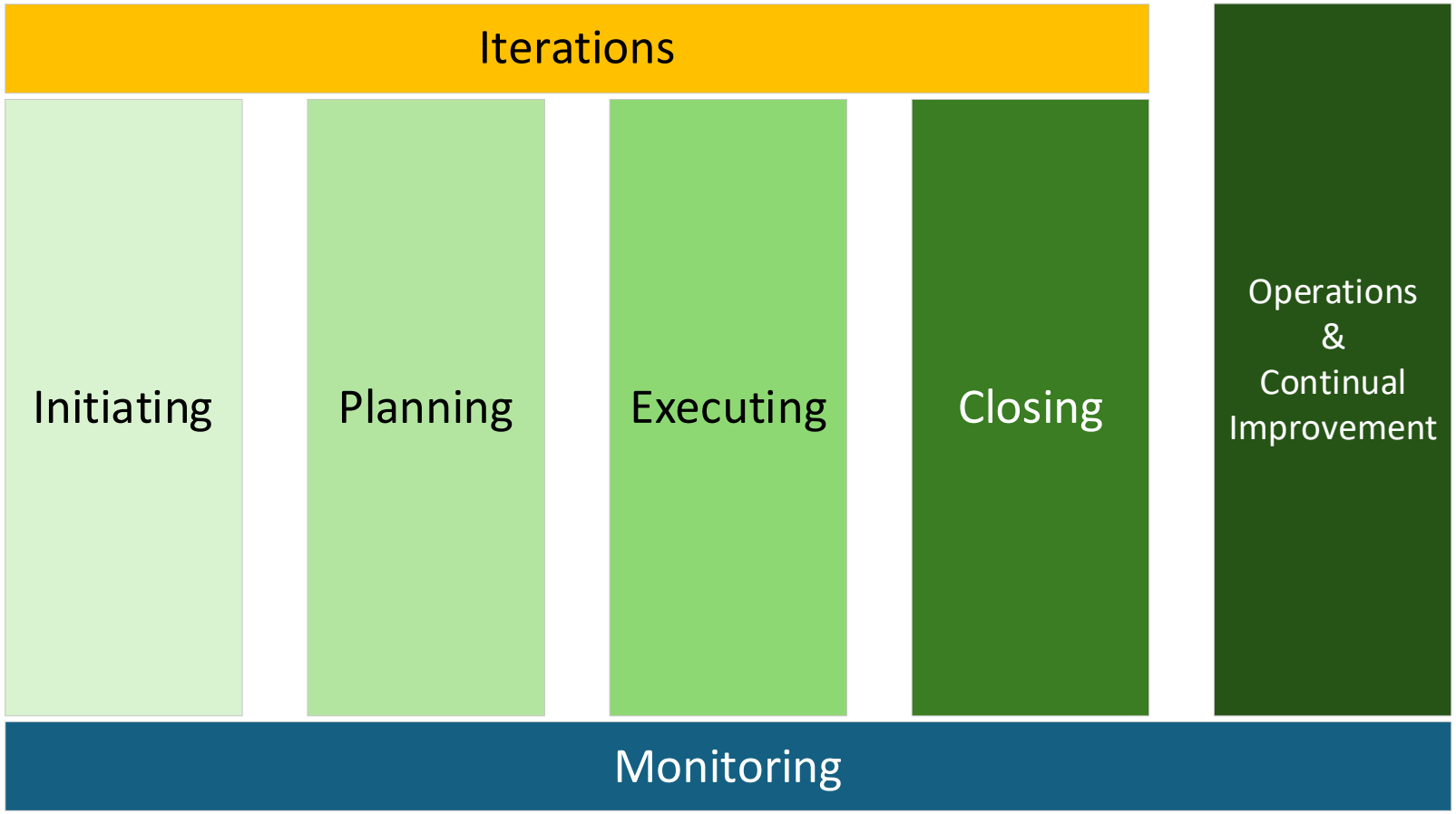
- Continuous and not point-in-time



Ideal Framework

- This framework represents a best-case scenario
  - Prepare for many issues and risks to occur
- Many models will work but they must be tailored to your organization's specific requirements
  - Try using models that are friendly to both environments
    - ISO/IEC 27001, ISO 31000, NIST, PMBOK
  - Additional potential models to integrate:
    - ISA/IEC 62443 in OT & NIST in IT
  - This framework is modeled from a hybrid of PMBOK and ISO/IEC 27001
  - Inject business requirements
  - Use a unified risk management program / process

Ideal Framework



Initiating: Operational & Implementation

Program Development

- Enterprise alignment
- Shared Vision / Shared Mission
- Organization process to initiate a program
- Program sponsorship from executive leadership

Assign a Champion

- Understand and advocate for the mission
- Understand both IT and OT operations
- Ready to actively participate in cross-functional meetings

Collaborative Risk Assessment

- Build a team mentality with interested stakeholders: IT, OT, operations, engineering, maintenance, risk management, process safety, and physical security representatives

Planning: Operational & Implementation

Requirements

- OT Operations, Engineering, Maintenance, Risk Management, Process Safety, and Physical Security Representatives
- Corporate IT and Cyber
- Enterprise
- Regulations
- Laws

Design

- People
- Process
- Technology
- Metrics
- Risk Responses

Plan

- Implementation Plan
- Schedule
- Resources
- Quick Win’s
- Approval Cycles
- Transition
- Operational Metrics
- Deliverables

Executing: Implementation

Program Management

- Progress of Project Execution
- Measure Value to Stakeholders
- Monitoring Executive and Board Level Cyber Risks
- Reporting to Executives and Board
- Support the Champion and Projects

Project Execution

- Implement the PPT Solutions
- RFPs and Procurement
- Process and Procedure Implementation
- Project Management
- Secure Resources
- Implement Risk Responses
- Manage Stakeholders
- Build Deliverables

Closing: Operational & Implementation

Training

- Transition
- Skills and Competencies
- Operation Changes

Documenting

- Policies
- Processes
- Procedures
- Job-Aids
- Diagrams
- As-Builts

Reporting

- Deliverables to Requirements
- Completion Status
- Operation Changes

Monitoring: Operational & Implementation

Key Processes

- Changes in Metrics
- Performance
- Quality Control
- Reporting

Risk Management

- KPIs / KRIs / KCIs
- Projects
- Operational Changes
- External Influences

Communication

- Top-Down, Bottom-Up, Middle-Out
- Cross-functional
- Interviews
- Committees
- Reporting to IT and OT Leadership Simultaneously

Common Issues

- Cultures and sub-cultures
- Competing Priorities (CIA versus AIC / Safety & Reliability)
- Fragmented risk management
- Low understanding of the other department
- Legacy technology / assets
- Understanding and applying standards and frameworks across both environments

Success Factors

Executive willingness to learn is more critical than the SMEs

Active support from executives to implement and sustain

Plan towards the bigger picture (Enterprise goals & objectives)

Measure by business objectives

Conclusion

- Define IT/OT Convergence for your organization
- Stakeholders are in the same boat and under the same banner
- Share the mission objectives
- Customize your program to your requirements and culture – One size does not fit all
- Incorporate risk-based approach with business consequences
- Governance and RACI must be supported by leadership
- Consider impacts of new regulations: e.g. CSA z246.1

MOBIA
TECHNOLOGY INNOVATIONS

SIMPLI GRC

IT OIT Concepts, LLC

"In Operations IT is different."

THANK YOU

ISA Calgary Section

Appendices

Scenario Example 1: Zero to Little OT Cybersecurity

Description:

Operational goals are the priority

OT is accountable and responsible for the assets, including cybersecurity

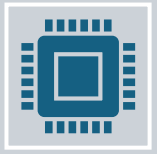
Usually IT provides cyber services when requested

Low culture of collaboration

Drivers for Convergence:

Cost efficiencies

Alignment with enterprise goals



Obstacles:

IT cyber has low understanding of OT

Priorities are misaligned

Different operating models

- Remediations:
  - Develop cross-functional processes
  - Engage stakeholders for all developments
  - Associate consequences to risk responses
  - One change management system or process to facilitate between

Scenario Example 2:
OT Cyber Owned by OT / Serviced by IT

Description:

- OT leverages cyber services from IT cyber
- OT remains the asset owner and budgets for all services on the assets
- Cyber function has a hybrid reporting structure
- Corporate requirements takes priority over operations

Drivers for Convergence:

- Cost efficiencies
- Alignment with enterprise goals
- Cyber security incidents in the industry
- Cyber risks are raised at the board-level

Obstacles:

- Competing priorities over budget allocations
- Tail wagging the dog (IT prioritizes cyber over operations)
- IT cyber has low understanding of OT
- Culture clash
- Decisions made without the other department's engagement

- Remediations:
  - Develop cross-functional processes
  - Engage stakeholders for all developments
  - Analyze the stakeholders
  - One change management system or process to facilitate between
  - Consolidate corporate and operational requirements
  - Prioritize enterprise goals and objectives
  - Unify risk management processes. A technology risk does not always equate to OT risk
  - Leverage process safety
  - Associate consequences to risk responses

Scenario Example 3:
OT Cyber Owned and Managed by OT

Description:

OT operates its own cyber function and is separated from IT cyber

Selective collaboration

Primary requirements are OT focused

Aligns partially with IT requirements

Aligns partially with enterprise requirements

Drivers for Convergence:

Cost efficiencies

Alignment with enterprise goals

Cyber security incidents in the industry

Cyber risks are raised at the board-level

Obstacles:

Competing priorities over budget allocations

IT influence for corporate requirements

IT cyber has low understanding of OT

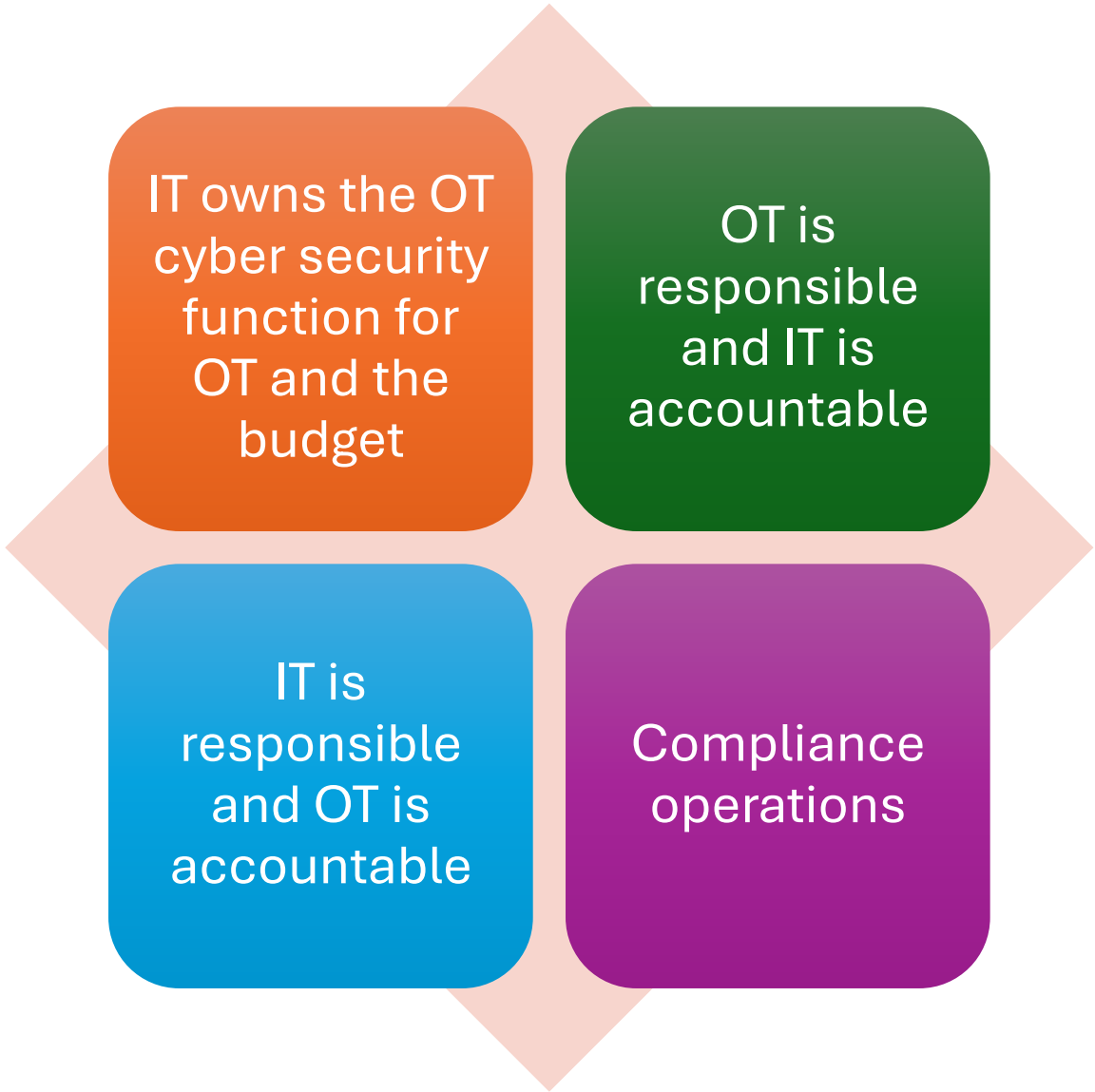
Culture clash

Shadow IT

Increasing resource and operating costs

- Remediations:
  - Analyze the stakeholders
  - Consolidate corporate and operational requirements
  - Prioritize enterprise goals and objectives
  - Leverage process safety
  - Associate consequences to risk responses

Scenario Example X: Different Variations

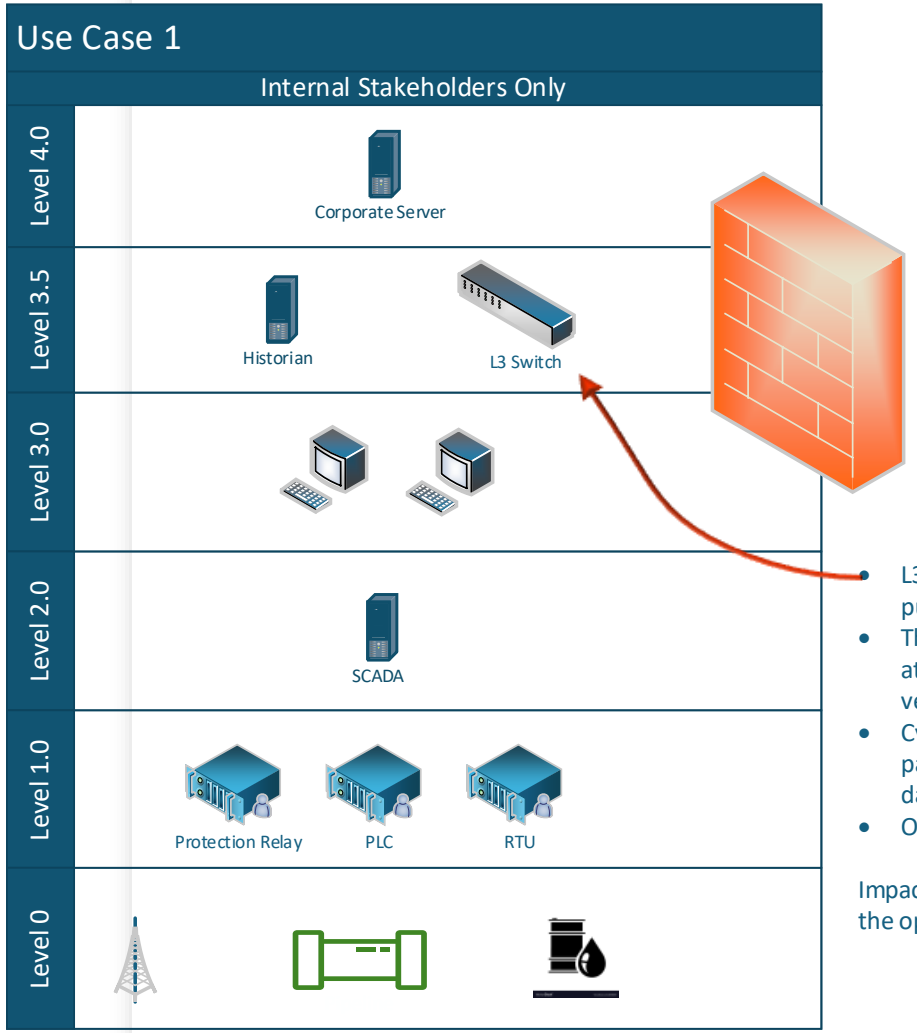


Scenario Observations

- Majority of business drivers apply to all three
- Obstacles and remediations vary for each scenario
- Skills and competency gaps
- Consider collaboration as an enabler versus a methodology
- Unify or connect risk processes

Applying the Same Update in Two Different Scenarios

Internal Stakeholders



- L3 Switch in Level 3.5 is subject to a public vulnerability
- The vulnerability is a man-in the middle attack categorized as critical and the vendor has released a security patch
- Cyber IT policy requires all critical patches be applied within 3 calendar days
- OT policy requires risk assessment

Impact: most likely low impact to interrupt the operations

Applying the Same Update in Two Different Scenarios

External Stakeholders