Creating Infinite Possibilities.

SCTE
a subsidiary of CableLabs

Design and Implementation of a Controls Framework to Secure a 10G Network

Mike Gala

Executive Director – Cybersecurity Governance, Risk and Compliance
Comcast

SCTE CABLE-TEC EXPO 22
SEPTEMBER 19-22 • PHILADELPHIA, PA

2022 Fall Technical Forum
SCTE • CABLELABS • NCTA

Agenda

10G Security
- Controls Framework Methodology

Control Design
- Identify Risks
- Identify Framework and Controls
- Principles for Control Monitoring
- 3 Lines of Defense Risk Management

Measurement and Reporting
- Defining Control Metric and Thresholds
- Identifying Sources of Reliable and Scalable Data
- 1st line and 2nd Line of Defense Dashboards
- Accountability Summary and Responsibility Views

Onboarding and Continuous Monitoring
- Approach to Onboarding
- Control Knowledgebase
- Control Trial Implementation
- Control Lifecycle
- Continuous Monitoring

Takeaway
- Adopting Continuous Monitoring for Security Controls for the 10G Network at your Organization

10G Security

Prevention, mitigation, remediation and customer notification technologies

“What problems are we solving?

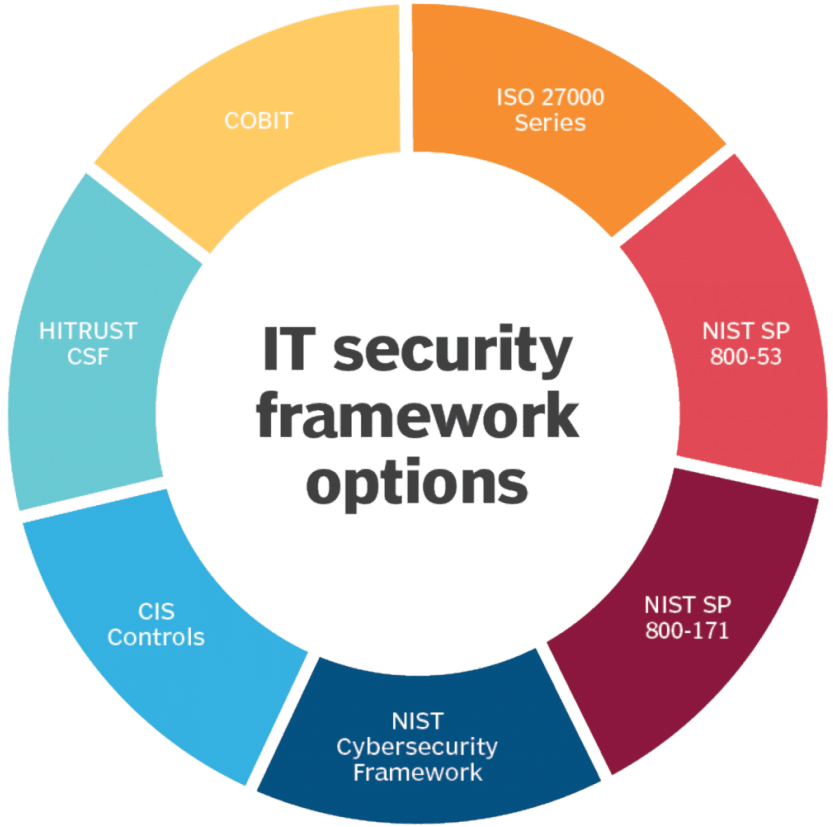
Many security considerations, including DDoS attacks, fraud/phishing and data breaches, stem from two main sources: unsecured Internet of Things (IoT) devices (think a baby monitor or webcam) and inadequate network security controls. Although we cannot stop every hacker from seeking out and exploiting these vulnerabilities all the time, we can make it extremely difficult to do so by implementing advanced access control, network monitoring and management technologies, as well as meaningful industry-wide policy changes. Security is often compared to a never-ending arms race, where good people must always out-smart, or in our case, out-invent the bad.”

Source: https://www.cablelabs.com/10g/security

Methodology

Establishing the continuous measurement and monitoring of security controls requires implementation of a controls framework that is adaptable and customizable to organizational technologies, processes, policies, and expertise.

Many frameworks exists when an assessment is required to determine the best fit in alignment to organizational cybersecurity goals and its risk management strategy.



Common Cybersecurity Control Frameworks

Controls Framework Customized to a 10G Network

A controls framework can be customized based on an organization's goals, policies and standards, technologies, and processes.

Asset Management

Network Inventory Management in defined source system, automated discovery, completeness of key attributes like Serial Numbers, Location for all key assets that encompass the network

Risk Management Strategy

The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support network operational risk decisions

Identity & Access Management

Identity Management, Authentication and Access Control for physical and logical assets and associated facilities for authorized users managing and monitoring the network

Data Security

Protecting Information and records (data) in transit and at rest against data leaks separating production and test environments

Maintenance & Repairs

Maintenance and repairs of industrial control and information system components of the network are performed consistent with policies and procedures

Protective Technologies

Audit logging, media protection, control plane protection, load balancing are in place to ensure security and resiliency of the network

Anomalies & Threat Detection

Detecting anomalous activity against a baseline and creating incidents for necessary events by correlating from multiple sources and sensors across the network

Security Continuous Monitoring

Continuous monitoring and vulnerability scanning to identify cybersecurity events, malicious code, unauthorized access etc.

Recovery Planning

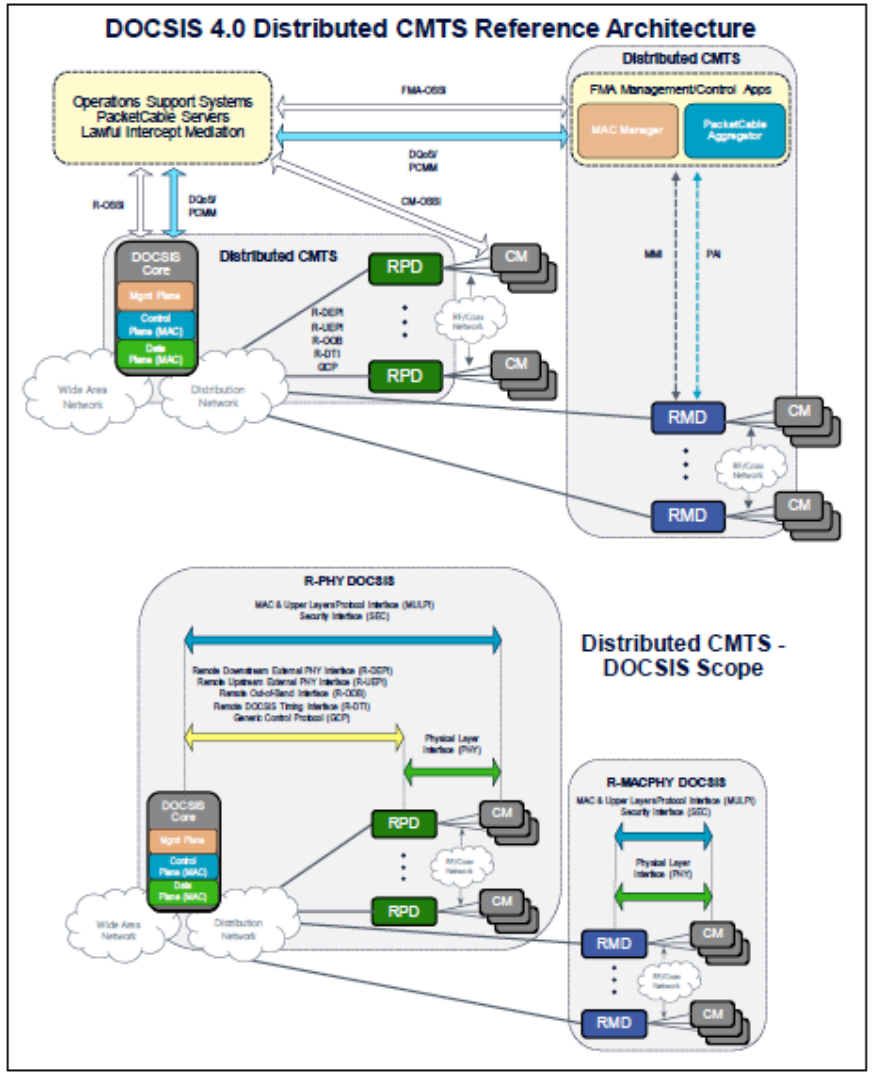
Recovery processes and procedures are executed and maintained for restoration of network sub-systems or assets affected by cybersecurity incidents

Control Design

Identify Risk

Development of the organization's holistic view of critical business functions starts with the identification of its assets, risks, policies, and owners. Identification of these aspects determines an organization's critical functions and the risks that could cause disruption to key network components or infrastructure.

The path to 10G and its network transformation to a distributed access architecture has required the controls framework to further adapt in the identification of risks in a virtualized and digital environment.



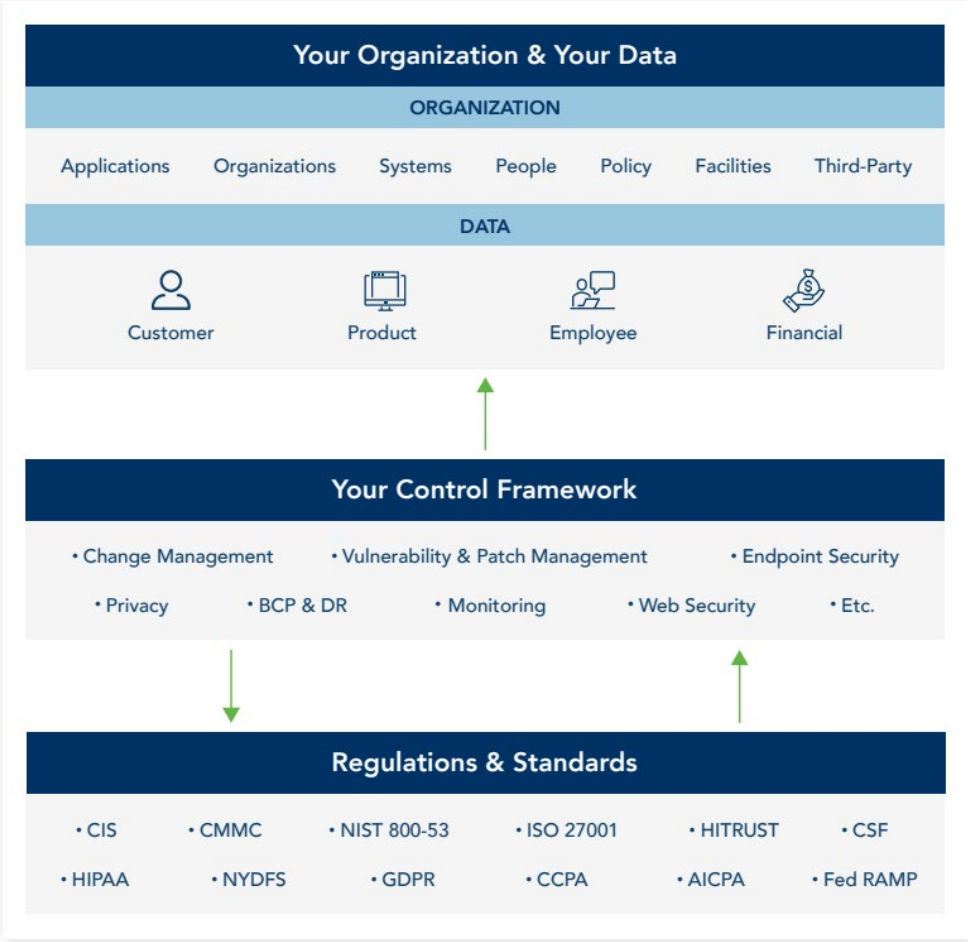
(Source: [Cable Labs Data-Over-Cable Service Interface Specifications for DOCSIS® 4.0, MAC and Upper Layer Protocols Interface Specification CM-SP-MULPIv4.0-I05-220328])

Identify Framework and Controls

Identified internal and external risks require the implementation of controls within a framework that aligns best to organizational objectives.

Below details the best practices for control selection, design, and implementation:

- Mapping of controls to policies and standards, assets, risks, owners, and organizational data
- The management of controls is best accomplished utilizing domains with mapping to controls
- Each control should be paired with a specific process owner
- Control design logic and requirements should be formally documented and continuously maintained



Principles for Control Monitoring

USABILITY
Usable by all three lines of defense for their specified responsibilities

SIMPLIFY ENGAGEMENT
Simplify business engagement model

ACCOUNTABILITY
Support hierarchical accountability model

RESPONSIBILITY
Support hierarchical responsibility model or link to accountable hierarchy

SOURCE OF TRUTH
Connect to source systems of record whenever possible

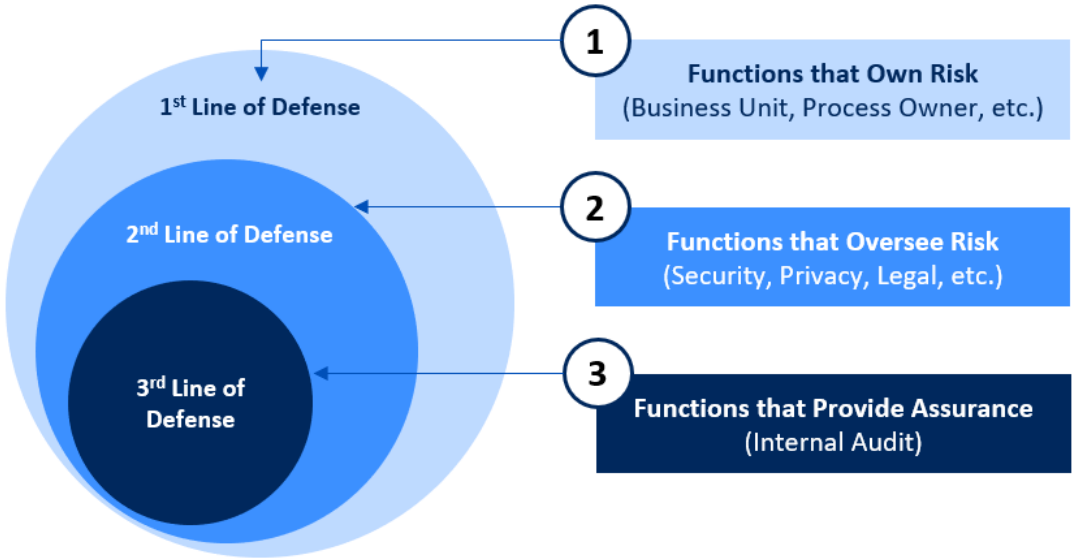
DATA AVAILABILITY
Provide near real-time data as possible

SUBJECT MATTER EXPERTS
Supported by process owners who define controls and associated requirements (standards, remediation, reporting)

OPERATIONAL SUPPORT
Supported by operational tools and processes

3 Lines of Defense Risk Management

The concept of the 3 lines of defense in risk management is a term often utilized in the cybersecurity compliance and audit sector. It is essentially a model that provides guidance for effective risk management and governance for an organization with distinct roles and responsibilities across all 3 lines.



Own risk management for their organization by the continuous monitoring of controls and remediation of gaps

Design, develop, and implement the control framework based on identified risks and business objectives; enable 1st line of defense

Provide independent and objective assurance for the organization's controls

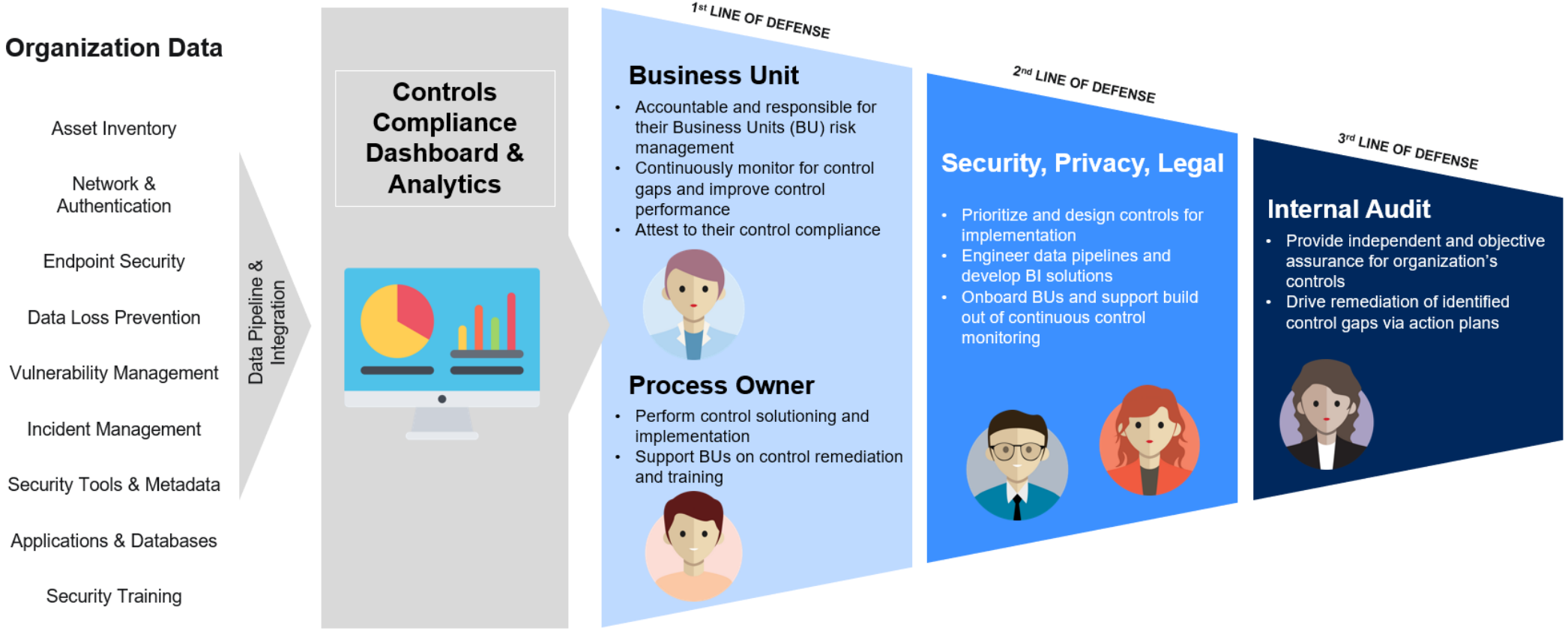
Measurement and Reporting

Defining Control Metric and Thresholds

The representation of the control performance and analytics is key in the organizational adoption of the controls framework.

- Understand your audience
- Define the appropriate control measurement that provides the risk coverage and measures progress
- Take a risk driven approach to prioritization of control measurements
- Business Unit actions vs. Process Owner actions to maintain accountability and responsibility
- Time-bound activities and their proper representation in the metric to measure SLAs and quarterly breakouts
- Keeping it simple but effective
- Ensuring that thresholds are defined in consultation with internal risk management teams and legal teams

Identifying Source of Reliable and Scalable Data



Onboarding and Continuous Monitoring

Approach to Onboarding

Onboarding onto the security controls framework can be methodically accomplished in defined phases to ensure those onboarded are equipped with the knowledge necessary to take ownership of their responsibilities across all lines of defense.

Perform control trial with a select group to gather feedback for upcoming Business Unit (BU) onboarding related to experience, data/dashboard, and control processes

Pre-onboarding alignment with key stakeholders on onboarding approach, data review, and process improvements to sustain data quality

Delegate onboarding onto the control framework to establish partnership and control understanding for BU Executive onboarding readiness

BU Executive onboarding onto the control framework for control remediation and continuous monitoring

Monthly updates and Quarterly attestations to ensure continuous monitoring of controls, program and control updates, and compliance adherence

Control Knowledgebase

Building a knowledgebase is key in the successful onboarding of users onto an organization's security controls framework. A few guidelines can be followed in the development of an enablement focused knowledgebase:

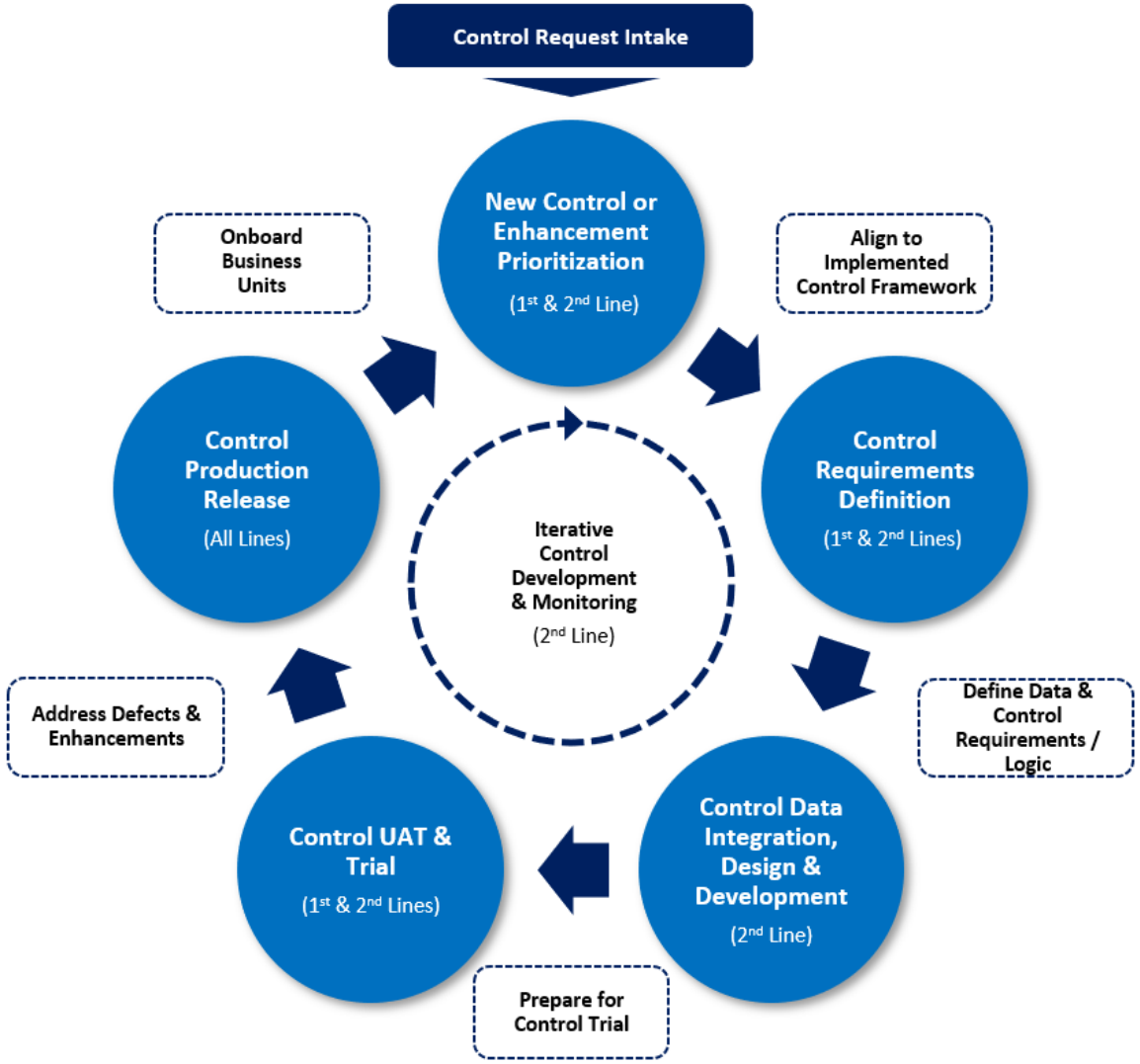
- Accessibility should be considered to ensure it is usable by all users, but secured to ensure access is restricted to only those required in the organization
- Documentation is maintained periodically and expanded over time based on new control implementation, enhancements to existing controls or processes, and repeatedly asked questions
- Management of knowledgebase is simplified to ensure sustainability (e.g., links to policies and standards that can change over time)
- Control responsibilities and helpful tips for remediation are made easily available as it will drive improved adoption and understanding
- Avoid swivel where possible; if dashboards are developed measuring control performance, provide control details and remediation tips directly with the control performance metrics for users to easily address identified gaps

Control Trial Implementation

Similar to the market trials of a 10G network rollout, control implementation should be trialed with a small group of early adopters that can provide feedback on control effectiveness and design.

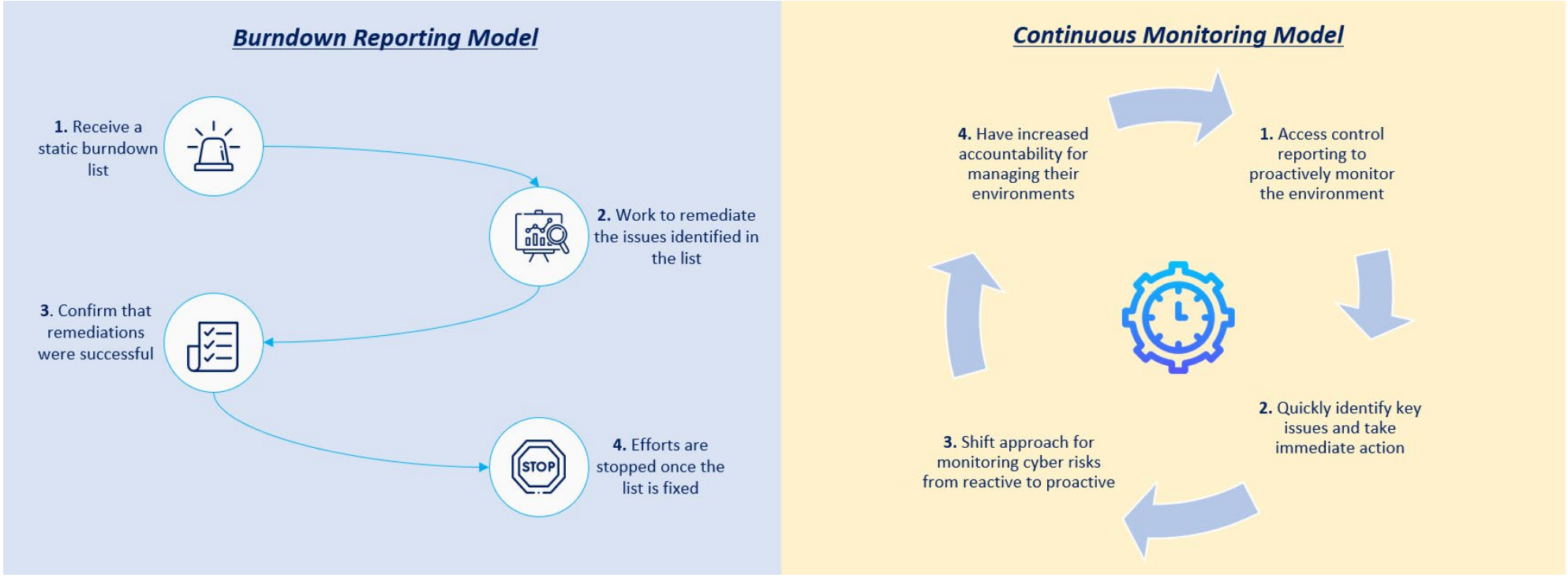
Control Lifecycle

Establishing a control lifecycle for new control implementation and existing control enhancements allows an organization to take a control as code approach, to iteratively develop and release controls to align to goals and objectives.



Continuous Monitoring

Enable the organization to establish a continuous control monitoring process. This requires the ability to shift the cultural mindset from a traditional burndown approach to control gap remediation, to one that is proactive and continuous.



Takeaways

Adopting Continuous Monitoring for Security controls for the 10G Network at your Organization

Establishing the foundations of a security controls framework for a 10G network provides the ability to proactively monitor implemented control effectiveness as well as identify risks in an environment that is continuously changing along with its attack surface. Adopting this approach allows an organization to:

1. Control framework selection to align with 10G Network goals
2. Implementation of a proactive continuous controls monitoring culture
3. Organizational enablement via data and control insights
4. Establishing an accountability and responsibility model throughout the organization

Creating Infinite Possibilities.

Thank You!

Mike Gala

Executive Director – Cybersecurity Governance, Risk and Compliance
Comcast
215.286.8937 | mulchand_gala@comcast.com

Andrew Yun

Director – Cybersecurity and Privacy Compliance
Comcast
215.605.0722 | andrew_yun@comcast.com