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

2022 Fall Technical Forum
SCTE • CABLELABS • NCTA

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

A Technical Paper prepared for SCTE by

Mike Gala
Executive Director
Comcast
1701 John F. Kennedy Blvd, Philadelphia, PA 19103
(215) 286-8937
mulchand_gala@comcast.com

Andrew Yun
Director
Comcast
1701 John F. Kennedy Blvd, Philadelphia, PA 19103
(215) 605-0722
andrew_yun@comcast.com

Table of Contents

List of Figures

List of Tables

1. Introduction

Network security has been one of the top priorities for the industry since the transition from analog to digital. It is a combination of prevention, mitigation, remediation, and customer notification technologies that help reduce the risk of data loss, theft, and sabotage. [1] The landscape has also changed drastically recently due to the pandemic, geo-political instability, and evolving federal and state regulatory requirements and standards. Network security threats are constantly evolving as well with threat actors looking to exploit vulnerabilities to gain the initial access required to laterally move across the network, and ultimately exfiltrate sensitive information or impact the environment. The recent CISA alert AA22-158A [2] of state-sponsored cyber actors exploits of network providers and devices is an example of such threats potentially targeting modern networks. These actors exploited known vulnerabilities, primarily common vulnerabilities, and exposures (CVEs) associated with network devices to target and compromise major telecommunications companies and network service providers since 2020.

Often the response to widely impacting cyber threats is to deploy additional security safeguards across the network and its devices; initially at the perimeter and down through its many additional security layers (network, endpoint, application, and data) as well as externally to the subscriber premise devices. Patching and end-of-life infrastructure replacement can also be conducted, but these are usually reactive measures to exploits that are already utilized and potentially costly to remediate.

A security controls framework approach facilitates the proactive measurement of existing and implemented protections required to minimize risks across an organization's people, processes, and technologies safeguarding a 10G network. Network security threats such as DDoS attacks, fraud and phishing, and data breaches are top priorities for any organization requiring the ability to continuously measure control effectiveness and risks with an automated and scalable solution. The design and implementation of continuous monitoring for security controls is often a complex and challenging task requiring subject matter expertise, alignment across multiple organizations, and data aggregation and correlation to enable effective risk management. This whitepaper will elaborate on a unique strategy that showcases the best practices for design, implementation, and operation of a controls framework for a 10G network aligned with a risk management approach.

2. Methodology

To establish the continuous measurement and monitoring of security controls requires the implementation of a controls framework that is adaptable and customizable to the technologies, processes, policies and standards, and expertise of each individual organization. Many security frameworks exist where an assessment is required to determine the best fit in alignment to organizational cybersecurity goals and its risk management strategy.

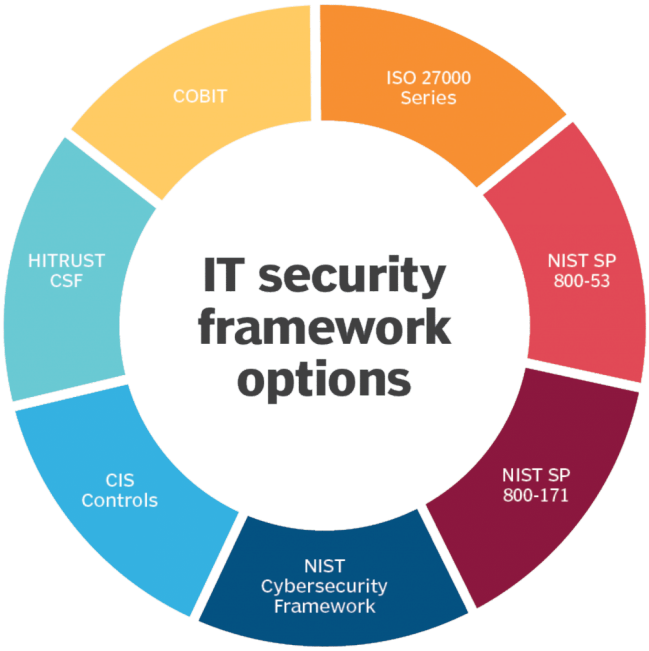

Figure 1 – Common Cybersecurity Control Frameworks

The cybersecurity framework utilized in this whitepaper to illustrate the design and implementation of continuous controls monitoring is NIST SP 800-53 [3]. The National Institute of Standards and Technology (NIST) is a non-regulatory agency of the United States Department of Commerce, where the NIST Cybersecurity framework was introduced in 2014 with revisions released to domains, controls, and enhancements (currently in Revision 5). The NIST Cybersecurity Framework is centered around five essential domains:

- **Identify (ID):** Determines an organization's critical functions and the risks that could disrupt those functions. Identifying organizational systems and assets, information types, policies and procedures, risk management strategy, and roles and responsibilities are essential elements of this domain.
- **Protect (PR):** Defines the relevant safeguards required to deliver critical protective services by establishing priorities and cybersecurity efforts. Protection of organizational systems, assets, and information via access controls, awareness and training, data security, information protection processes and procedures, maintenance, and protective technology management are essential elements of this domain.
- **Detect (DE):** Implementation of an organization's detective capabilities to promptly identify cyber risks and incidents. Event logging, anomalous activity detection, security continuous monitoring, and detection processes are essential elements of this domain.
- **Respond (RS):** Execution of measures related to a detected cybersecurity incident and an organization's ability to manage its impact. Response planning, communication strategy, analysis procedures, mitigation, and application of improvements are essential elements for this domain.
- **Recover (RC):** Restorative capabilities to impacted systems and services as the consequence of a cybersecurity incident. Recovery processes and procedures, application of improvements, and cross organization collaboration are essential elements of this domain.

Taking into consideration an organization's goals, policies and standards, technologies, and processes are key in the successful implementation of a control monitoring framework. An organization's goals define its objectives, policies and standards provide governance and management, technologies illustrate its capabilities, and processes allow enablement. The domains in NIST 800-53 serve as the guidelines to be implemented concurrently to form an operational culture that addresses cyber risk. Within the domains are controls that provides the protective measures for systems, organizations, and individuals. The controls allow specification and customization to an organization's objectives allowing enablement of a continuous controls monitoring culture.

Table 1 illustrates how a series of controls can be customized to the specificity of a 10G network.

Table 1 – Example of NIST 800-53 Controls for a 10G Network

ID	10G Network Specific Controls
ID.AM	Network Inventory Management in defined source system, automated discovery, completeness of key attributes like Serial Numbers, Location for all key assets that encompass the 10G Network.
ID.BE	Alignment of the organization's mission, objectives, stakeholders, and activities with cybersecurity roles, responsibilities, and risk management of the 10G Network.
ID.GV	The policies, procedures, and processes alignment with regulatory, legal, risk, environmental, and operational requirements for the 10G Network.
ID.RA	Understanding of the 10G Network related cybersecurity risk to operations (including mission, functions, image, or reputation), organizational assets, and individuals.
ID.RM	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions as they relate to the 10G Network.
PR.AC	Identity Management, Authentication and Access Control for physical and logical assets and associated facilities for authorized users managing and monitoring the 10G Network.
PR.AT	Providing personnel and partners the cybersecurity awareness education to perform their cybersecurity-related duties and responsibilities for the 10G Network.
PR.DS	Protecting Information and records (data) in transit and at rest in 10G Network against data leaks separating production and test environments.
PR.IP	Processes are in place for Software Development Lifecycle (SDLC), secure configuration, backups, vulnerability management and incident response for the 10G Network.
PR.MA	Maintenance and repairs of industrial control and information system components of the 10G Network are performed consistent with policies and procedures.
PR.PT	Audit Logging, media protection, control plane protection, load balancing are in place to ensure security and resiliency of the 10G Network.
DE.AE	Detecting Anomalous activity against a baseline and creating incidents for necessary events by correlating from multiple sources and sensors within the 10G Network.
DE.CM	Continuous monitoring and vulnerability scanning to identify cybersecurity events, malicious code, unauthorized access etc.
DE.DP	Detection processes and procedures are maintained and tested to ensure awareness of anomalous network events.
RS.RP	Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.

RS.CO	Response activities are coordinated with internal and external stakeholders (e.g., external support from law enforcement agencies, vendors, etc.).
RS.AN	Analysis and forensics are conducted to ensure effective response and support the network recovery activities.
RS.MI	Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the network incident.
RS.IM	Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.
RC.RP	Recovery processes and procedures are executed and maintained for restoration of 10G network sub-systems or assets affected by cybersecurity incidents.
RC.IM	Recovery planning and processes are improved by incorporating lessons learned into future activities.
RC.CO	Restoration activities are coordinated with coordinating centers, Internet Service Providers, owners of attacking systems, victims, and vendors).

The rest of the whitepaper will discuss the process of designing the controls mentioned above, implementing related KPIs that can be matured over time, onboarding various teams running the parts of the 10G network, and setting up continuous monitoring of these controls aligned with a risk management approach.

3. Control Design

The number of devices connected to a subscribers' network continues to increase across variety of industries (e.g., healthcare, education, private and public sectors, etc.) requiring connectivity to reliable network services. Speed, capacity, reduced latency, enhanced reliable and security are all advancements that make 10G transformational in how people and industries operate in a multi-gigabit reality. "The 10G platform is a combination of technologies that will deliver symmetric multi-gigabit Internet speeds with a vision toward enabling symmetric 10 gigabits per second (Gbps) services. 10G will be significantly faster than what most consumers currently experience, and will offer lower latencies, enhanced security, and greater reliability" [4].

These advancements are examples of organizational 10G goals that are foundational to control design and the successful implementation of a security controls framework. The definition of these business objectives enables an organization to establish its scope of controls, prioritization of related security efforts, organizational adoption, and the measurability of control performance. With the organization objectives defined, an iterative approach to control design can be applied to establish a framework that is aligned to organizational goals, policies and standards, technologies, and processes.

3.1. Identify Risks

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. Identifying organizational systems and assets, information types, policies and procedures, risk management strategy, and roles and responsibilities are essential elements for a risk managed network.

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. From the virtualization of the cable modem termination system (CMTS) to the delivery of broadband signals across the network to the subscriber premise, the traditional approach to protect physical assets and key infrastructure has now expanded to the virtual environment.

Figure 2 illustrates an example of a virtualized CMTS network. *[5] (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)*

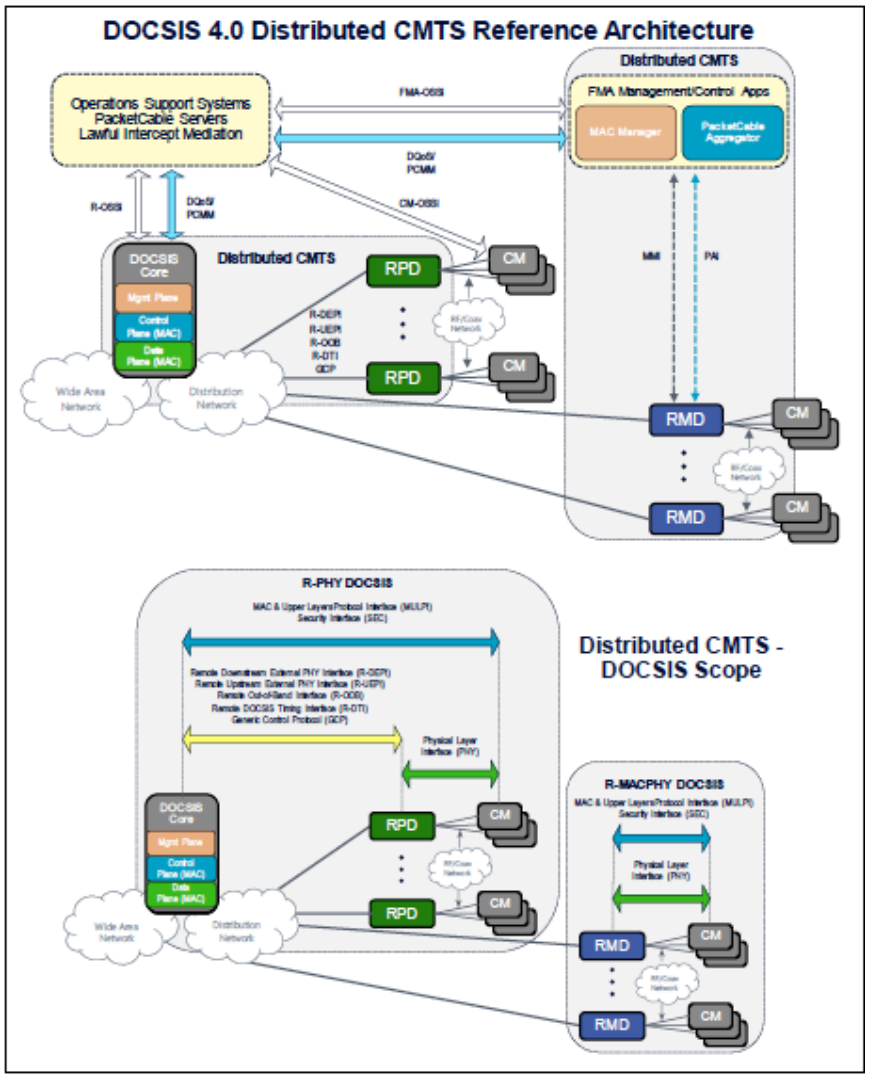

Figure 2 – DOCSIS 4.0 Distributed CMTS Reference Architecture [5]

Therefore, controls such as asset identification should be expanded to ensure coverage of the virtual environment, along with the design and implementation of policies and standards relevant to the security of a 10G network to ensure broader risk coverage. Similarly, with further reliance on automation to manage distributed and virtualized environments, traditional identity and access management risks should

be expanded to ensure appropriate coverage. Risks related to change management are also important to consider ensuring various teams involved in building and operating the 10G network are appropriately reviewing and approving deployments. Version control tools are appropriately configured and managed in alignment to organizational standards, along with the secure storage of secrets in organizational vaulting solutions and not present in source code.

Risk assessment and third-party management are additional critical aspects of risk identification in a 10G network. These areas allow a 10G network provider to understand the cybersecurity risks to organizational operations, priorities, and risk tolerance.

- **Risk Assessment:** Asset vulnerabilities to core 10G infrastructure are identified and documented; Cyber threat intelligence is received potentially impacting network providers (e.g., implementation of a Threat Intelligence Platform); Potential business impacts and likelihoods are identified; Threats, vulnerabilities, likelihoods, and impacts are used to determine risk; Risk responses are identified and prioritized
- **Third Party Management:** Cyber third party risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders and network management teams; Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed; Contracts with suppliers and third party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program; suppliers and third party partners are routinely audited to confirm they are meeting contractual obligations

3.2. Identify Framework and Controls

Identified internal and external risks require the implementation of controls within a framework that aligns best to organizational objectives. Frameworks such NIST 800-53, NIST CSF, ISO 27001, etc. provide specific scope and functions where the selection may be based on various frameworks that align to the organization's goals and regulatory requirements (e.g., GDPR, CCPA, PCI DSS, etc.). Often, the legal team within the organization provides consultation on the framework selection to ensure appropriate coverage is provided to identified risks and specific regulatory requirements. Once the approach to framework selection is completed, the process to control identification can begin mapped to the identified risks.

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

- Mapping of controls to policies and standards, assets, risks, owners, and organizational data allows the ability to successfully design a control for implementation and measurement
- The management of controls is best accomplished utilizing domains (e.g., asset management, risk management, identity & access management, etc.) with mapping to controls for an organized implementation which avoids duplication of controls
- Each control should be paired with a specific process owner that has defined the scope of the control, designed and implemented the control, continuously supports the control and its system and users, and can accurately report on control performance
- Control design logic and requirements should be formally documented and continuously maintained with updates and changes. Additionally, a control maturity model should be considered and formally documented as the selection and implementation of a control may require multiple phases based on enhancements by the process owners

Another key aspect in the selection, design, and implementation of a control is the organization's data. The availability of control data allows the ability to measure control performance, identify risks, and enables the business to establish a continuously control monitoring culture. A data strategy should be designed based on organizational capabilities to ensure data ingestion, quality, transformation, analytics, sharing, and governance is appropriately and efficiently conducted.

Figure 3 illustrates both the upstream and downstream control mapping based on organizational data.

Figure 3 – Organizational Data Mapping to Controls [6]

3.3. Principles for Control Monitoring

Establishing principles for control monitoring is essential to ensure the implementation of controls meets the objectives for a 10G network. Following a set of defined and agreed upon principles allow the implementation, adoption, and support of the controls to be sustainable with roles and responsibilities clearly defined in the controls end-to-end process.

Figure 4 defines a set of principles that can be utilized to meet an organization's control monitoring objectives and requirements.

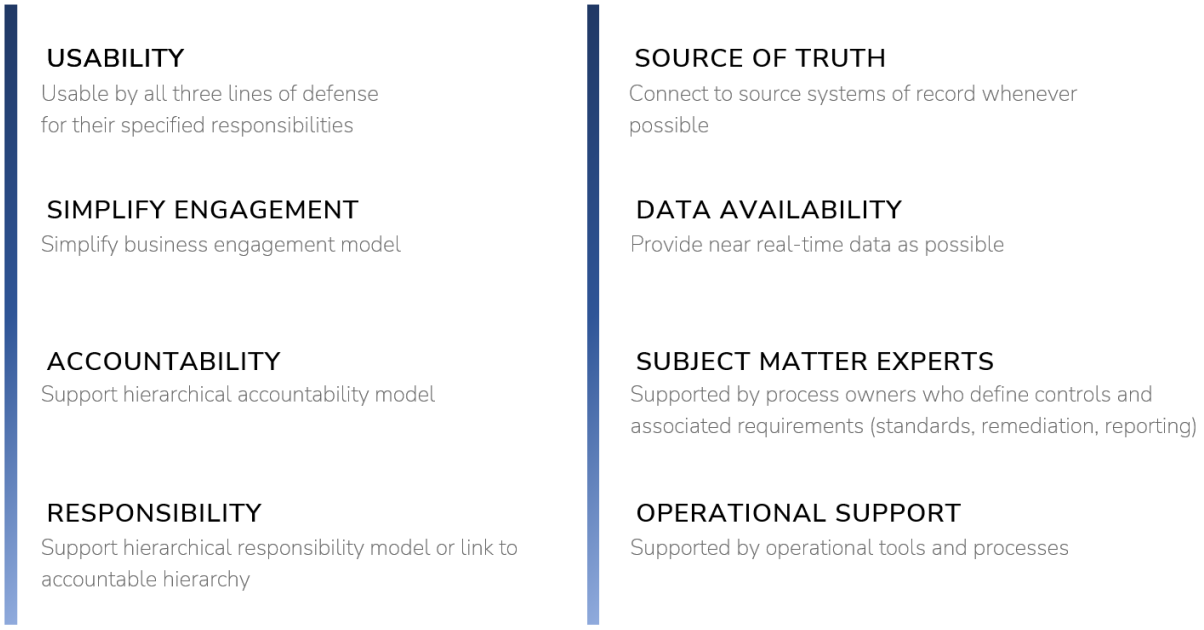

Figure 4 – Principles for Control Implementation and Monitoring

3.4. 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.

Figure 5 illustrates and details the 3 lines of defense and their responsibilities across an organization.

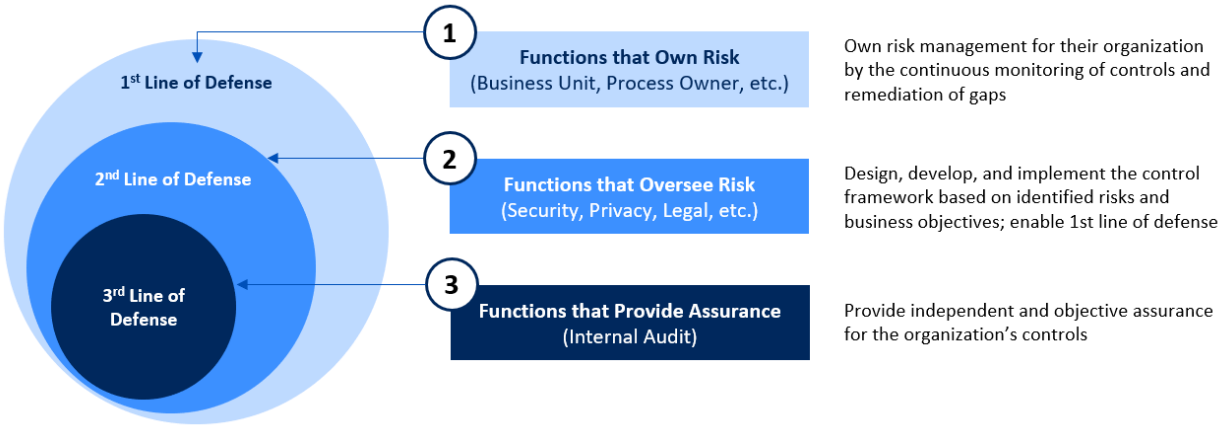

Figure 5 – 3 Lines of Defense

4. Measurement and Reporting

The representation of the control performance and analytics is key in the organizational adoption of the controls framework. The development of the control performance measurement is often accomplished utilizing a visualization tool (e.g., Tableau, Power BI, Splunk, etc.) that best fits organizational capabilities and skills. Prior to development, steps should be taken to gather and define development requirements which includes the determination of control metrics and thresholds, data source identification, and 1st and 2nd line defense views that demonstrate risk and control performance progress.

4.1. Defining Control Metric and Threshholds

Once the controls are defined, attention can be focused on the control metrics. Below are a few principles to consider in building the insights necessary for successful utilization:

- Understand your audience, identify their analytical capabilities and what best complements their visualization needs
- Define the appropriate control numerator and the denominator that provides the risk coverage and measures progress accurately
- Take a risk driven approach to prioritization of control measurements as opposed to easily available metrics in the data set and keep in mind the total risk posture (total attack or risk surface)
- Business Unit actions vs. Process Owner actions to maintain the accountability and responsibility for remediations
- Time-bound activities and their proper representation in the metric to measure SLAs and quarterly breakouts. Also consider the re-certification of a metric after an elapsed time
- "Keeping it simple but effective". This adage still serves well for these metrics that can get very granular and detailed and could take a life of their own
- Ensuring that thresholds are defined in consultation with internal risk management teams and legal teams so internal and external compliance requirements are met

4.2. Identifying sources of reliable and scalable data

Following the control metrics definition, the next step is to look at various systems that source the data and build the data pipelines to integrate into the control monitoring dashboard. A few aspects to consider in this step:

- Secure interfaces and methods to integrate the data at the source
- Determine the frequency of the updates and apply automation where possible
- Ensure quality and accuracy of the data and its useability in the control metrics build out
- Deidentify the data to remove any Personal Information (PI)

Figure 6 illustrates a general inventory of an organization's data required to build the controls metrics dashboard and the lines of defense that utilizes its insights to perform risk identification and mitigation.

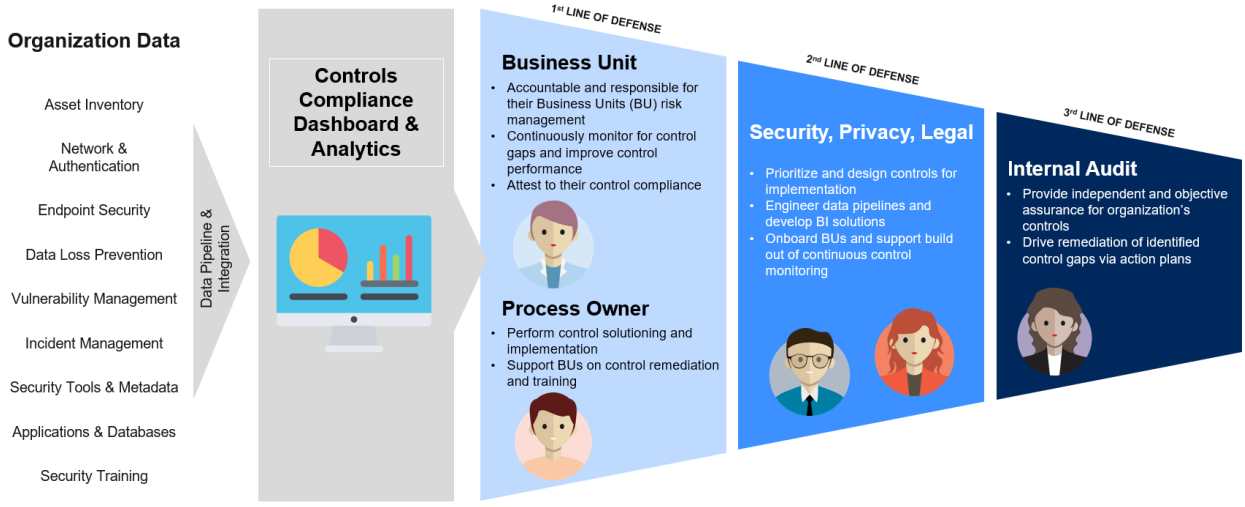

Figure 6 – Identification of Reliable Organizational Data and Insights Utilization

4.3. 1st line and 2nd line of defense dashboards

In line with the risk management framework, it is advisable to create dashboards that serve specific purposes to highlight risk for its intended use. The 1st line of defense dashboards provides the ability to highlight risk for the Business Unit to focus on control performance, gap remediation, and enablement to continuously monitor control performance. Ease of use, data accuracy, and alignment to the analytical capabilities of its audience is key in its adoption to drive enablement for the Business Unit.

The 2nd line of defense dashboards provides a risk view of the network across the entire organization with the ability to focus in on specific control risk areas requiring intervention or support. Also has the capabilities of highlighting the risk management maturity of a Business Unit with the added ability to assess progress via trending and identify additional risk areas. The 3rd line of defense is also able to utilize this view to support internal audits with the benefit of reducing the manual efforts associated to

identifying risks, driving remediation via action plans, and the validation required to confirm risk mitigation.

4.4. Accountability Summary and Responsibility Views

As the controls framework and its controls contain multiple and at times complex metrics, it is recommended to provide separate views that are related to accountability (the executive view) and responsibility (the operational view). The accountability view provides an executive the visibility required to understand control compliance at the organization level, identify escalation needs when control performance is lacking or use for attestation purposes (see section 5.6 for more details on attestations). Adding trending expands the control accountability to

The responsibility view provides the operational visibility required for the remediator to identify their control gaps and perform the corrections required to reduce risk. The responsibility view should provide the details necessary to perform the remediation; data points such as control gaps, insights on risk factors supporting prioritization, distribution by owner to forecast resource demand, and drilldown details are examples of the insights necessary to quickly and easily remediate the control gaps identified.

One of the challenges often experienced is the re-factoring of the dashboards due to organizational changes which may impact the hierarchical ownership of assigned controls and associated risks for the accountability and responsibility views. Associating the business unit roll up to a control metric that can be linked to immutable data objects such as applications and vendors provides a way to keep the dashboards agile and "self-correct" when these changes occur.

5. Onboarding and Continuous Monitoring

The onboarding of users onto the security controls framework and related dashboards is key in the organization's overall risk management strategy. The goal in onboarding of users is to ensure a continuous control monitoring process and culture can be implemented, which improves the organization's security posture and leads to a sustainable model for gap remediation. Sustainability is also central to onboarding as teams are often challenged with priorities and resource capacity, where consultation may be required to build in continuous control monitoring processes into existing workflows.

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.

Figure 7 illustrates the onboarding approach to ensure alignment across key stakeholders and application of corrections or improvements based on feedback for Business Unit (BU) onboarding:

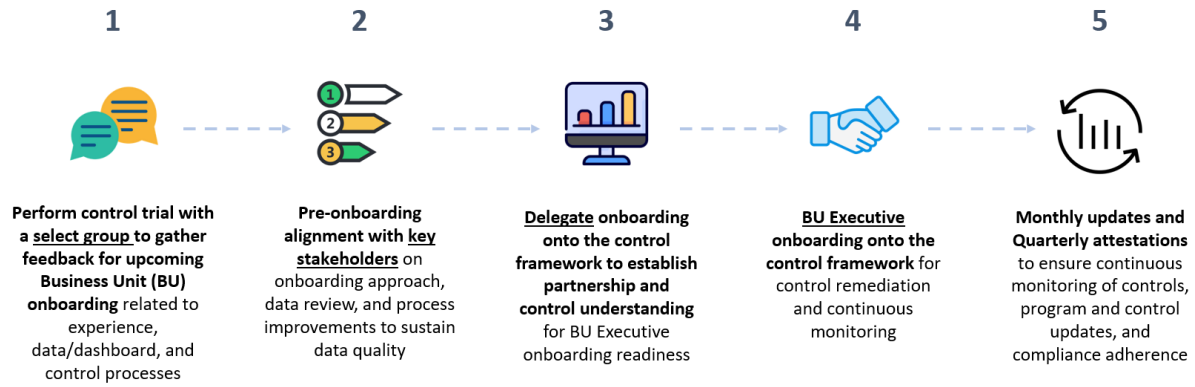

Figure 7 – Business Unit Onboarding Approach

5.1. Knowledgebase

Building a knowledgebase is key in the successful onboarding of users onto an organization's security controls framework. Depending on the size, implemented tools, and structure of the organization; control requirements and related processes may be complex. The ability for a user to understand a control, their responsibilities, and processes related to gap remediation allows the enablement necessary where accountability is taken in alignment to organizational cybersecurity goals and objectives.

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

5.2. 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. As controls will evolve and mature over time, feedback is key in ensuring the effectiveness of controls and new features can be tested in alignment to its design and implementation. The trial goals should also be defined for the early adopters and can be targeted to specific goals during the testing period.

Figure 8 illustrates the trial control goals in preparations for a production implementation:

Figure 8 – Trial Goals for Onboarding Readiness

An added benefit of implementing a trial model for future control implementation allows the ability to establish a release strategy following a control development lifecycle from start to end, while allowing the early adopters to address their control gaps early in the control implementation process.

Figure 9 illustrates the control lifecycle for new control implementation and existing control enhancements from intake to production release:

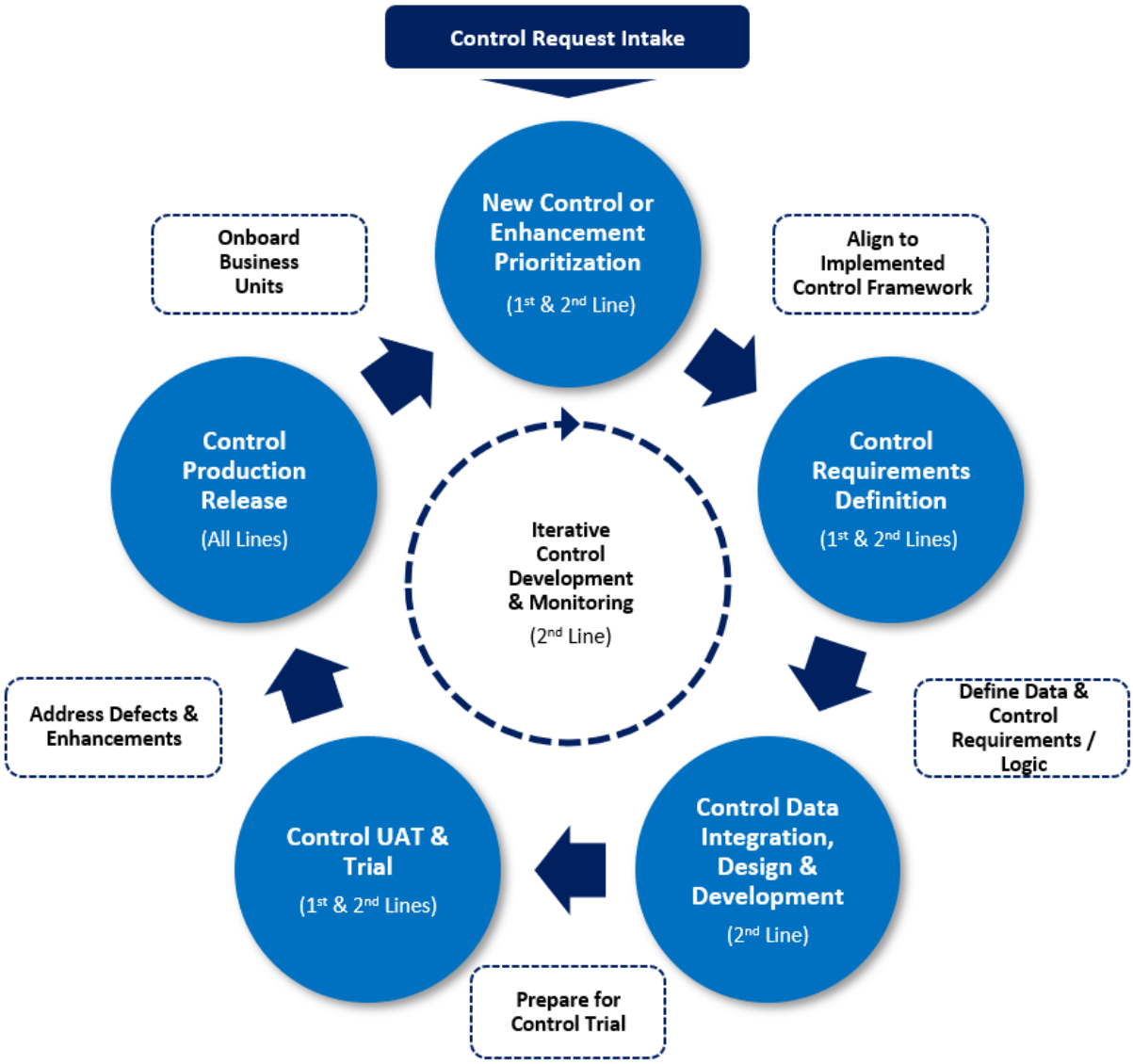

Figure 9 10– Control Lifecycle

5.3. Stakeholder Alignment

A key dependency in the success of a security controls framework implementation is the alignment established between key stakeholders. A 10G network implementation will require partnerships across many teams across engineering, field operations, to customer services. Similarly, a security controls framework requires partnerships with cybersecurity, privacy, and engineering counterparts to ensure the implementation of controls is in alignment to organizational goals and objectives. An example would be the partnership between the network engineering and cybersecurity teams in the establishment of access event logs to critical 10G network components. With access management policies and standards in place, the ability to measure control compliance via access event logs would be critical to proactively identify risks and gaps requiring remediation from both an engineering and process perspective.

5.4. Compliance Delegate Identification

Champions for a security controls framework implementation are instrumental in ensuring a continuous control monitoring culture can be adopted and implemented across the organization. These champions operate as delegates on behalf of the cybersecurity team, provide guidance on the implementation strategy for their respective teams, provide subject matter expertise to their teams related to control processes, and influence the change necessary to implement a continuous control monitoring mindset. As the delegate function in most situations are not always a part of their defined role, it is important to ensure that professional and personal growth related to this type of role is transparent for their active participation and partnership. This type of role often leads to increased visibility across the organization, with key leadership groups, and the ability to expand their knowledge as a subject matter expert in security.

5.5. Continous Monitoring

The goal in the implementation of an effective security controls framework within an organization is 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. Success should be measured not only in the control performance, but also with an organization's ability to shift security and privacy to the left early on in their internally processes. Only then will the security controls framework become sustainable, built in culturally across the organization, and a mechanism to ensure an initiative such as the design and implementation of a 10G network can be appropriately secured and risks mitigated.

Figure 10 illustrates the comparison between the reactive and proactive approach to control monitoring.

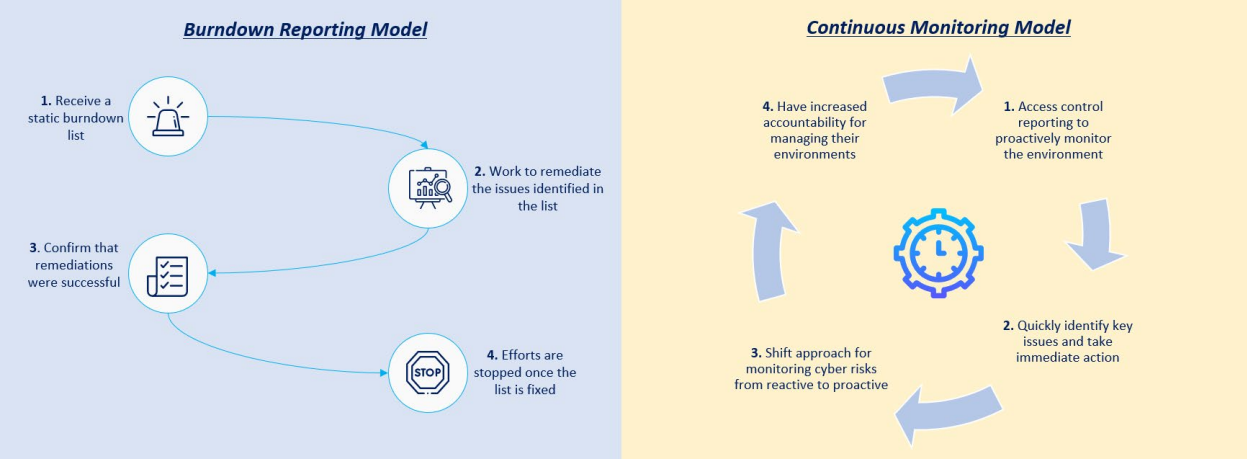

Figure 11 – Shift to Continuous Control Model

The benefits to proactive control monitoring are:

- Provides teams with the tools needed for holistic monitoring of control progress
- Promotes ongoing identification and remediation of cyber risks
- Enables teams to improve processes and go-forward strategy

5.6. Optional Attestation

In the past few years, attestations have grown in popularity to provide assurance over financial, security, and privacy related controls as required by compliance, regulators, or service clients. Adding a layer of formal attestations on quarterly basis provides the ability for companies to now gain confidence in the controls they have implemented in a method that is monitored by the financial, government, and regulatory agencies.

6. Conclusion

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. While it may seem challenging to implement a comprehensive framework such as NIST 800-53, it is possible to take a phased approach focused on risks with the highest impact to the network and organization. Engaging the Cybersecurity, Risk Management, and Compliance teams early on can ensure the appropriate controls are identified aligned to organizational goals and its risk strategy. The insights gained from a successful implementation can also start to showcase the security posture of the various organizational units managing the 10G network, establishing the accountability and responsibility necessary for continuous control monitoring. Securing a network is no small feat, making the right investments in security strategy and ensuring its measurable effectiveness provides the cyber protections necessary to deliver the transformative capabilities of a 10G network.

Abbreviations

GRC	Governance, Risk Management and Compliance
DoS	Denial Of Service
DevSecOps	A portmanteau of “Development” and “Operations”:
Botnet	Robot Network
IAM	Identity and Access Management
PI	Personal Information
NIST	National Institute of Standards and Technology

Bibliography & References

[1] https://www.cablelabs.com/10g/security
[2] https://www.cisa.gov/uscert/ncas/alerts/aa22-158a

[3] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

[4] https://www.cablelabs.com/10g

[5] https://www.cablelabs.com/specifications/CM-SP-SECv4

[6] https://info.processunity.com/rs/638-QKL-150/images/PU_Sustainable_Cybersecurity_WP_Final.pdf

