A Resilience Framework for Telecommunications Networks: Methodology, Assessment, and Best Practices

Paul Steinberg
psteinberg@techauditpartners.com
Jim Peterson
jpeterson@techauditpartners.com
Mark Ennis
mennis@techauditpartners.com
Fred Gabbard
fgabbard@techauditpartners.com
Ray Owen
ray.owen@uts.edu.au

***Abstract* - Telecommunications networks are at the core of global digital infrastructure, underpinning critical services for individuals, businesses, and governments. As network outages continue to challenge service providers, the demand for resilient "Always On" network capabilities has never been higher. This paper presents a comprehensive framework for assessing and enhancing telecommunications network resilience, combining industry best practices with a systematic, quantifiable audit methodology. Our approach evaluates the full life cycle of network capabilities, encompassing proactive, reactive, and foundational elements, to identify vulnerabilities, improve operational readiness, and reduce outage impacts. We structure our approach around five key lifecycle pillars: establish, design, implement, operate, and respond, all underpinned by a sixth pillar of encompassing foundational elements. We discuss the structured methodology, attribute-based scoring system, and an evidence-driven audit process that benchmarks providers against industry peers, providing transparency from business strategy down to execution of technical action items.**

Index Terms - Audit framework, network resilience, telecommunications, best practices, proactive capabilities.

I. Introduction

A. Context of Network Resilience

Telecommunications networks are at the heart of today's digital world, supporting critical services for both individuals and enterprises. The concept of resilience has grown significantly in importance as network outages have severe consequences on end-users, businesses, and government functions. The increasing complexity of networks, accelerated by new technologies like Software Defined Networking (SDN), Artificial Intelligence (AI), and cloud-based solutions, although theoretically capable of improving resilience, also introduces complexity and speeds up the propagation of potential issues, making resilience more challenging than ever. These far-reaching and structurally fundamental changes have increased the risk and occurrence of large-scale outages to levels not seen previously.

B. Motivation

The motivation behind this work is to provide a structured, methodical approach to assessing and improving telecom network resilience. This approach draws inspiration from the NIST cybersecurity framework, applying a comparable holistic and lifecycle approach to network resilience. Board members, executive teams, regulators, and customers are all demanding high availability, and outages can significantly damage both trust and business continuity. The goal is to provide a proactive means to minimize the number of outages, their duration, and the associated impacts, by applying a comprehensive framework that provides transparency and continuous improvement.

II. Background

A. Related Work

Previous research has focused on network reliability and the implementation of fault tolerance mechanisms. Reliability refers to the ability of a network to consistently perform its intended function without failure over a specified period. It is typically measured through metrics such as the mean time between failures (MTBF) and mean time to failure (MTTF). In contrast, availability focuses on the proportion of time a

network is operational and accessible, considering both uptime and downtime. Availability is often expressed as a percentage and depends on factors like mean time to repair (MTTR) and the effectiveness of redundancy mechanisms. Together, these metrics provide a holistic understanding of network resilience which we define as the ability of a network to sustain an acceptable level of service, functionality and performance when subjected to disruptions, failures, human error, or other external events. This paper draws upon these efforts and expands them by presenting a comprehensive framework to assess, audit, and benchmark resilience in a way that is actionable from both an executive and engineering perspective.

B. Challenges in Network Resilience

Resilience challenges stem from rapid changes in network architecture, the introduction of new technologies, investment frugality and the increased reliance on third-party systems. Key issues such as SDN misconfigurations, the propagation of software bugs, unanticipated dependencies and human errors are common root causes of major outages. Many network outages result from human error and misconfiguration, supported by several reports from the Uptime Institute [1]. Unfortunately, service disruptions are inevitable, so while prevention is critical, minimization, containment and response are also extremely important. Addressing these challenges requires a holistic framework for proactive assessment, quantification and continuous monitoring.

III. The Resilience Framework

A. Pillars and Attributes

The resilience framework is organized around five key lifecycle pillars: establish, design, implement, operate, and respond, all supported by the sixth pillar of the foundational attributes. Generally, the lifecycle of resilience considerations progresses left to right across the top five pillars from 'Establish' to 'Respond.'

Figure 1: Resilience Framework Structure

Within these pillars are more detailed attributes that contribute to the resilience of the network; the existence and application of attributes are assessed and scored. Each attribute (approximately 60 comprise the framework) is defined by a set of specific, capability-based considerations (approximately 215 total considerations across the framework).

- **Establish**: The purpose of this pillar is to set the foundation for resilience by establishing a strong governance framework and strategy. This includes defining roles, responsibilities, and resilience objectives, and ensuring that the overall vision is aligned with business requirements. Key attributes assessed in this pillar include leadership involvement, investment adjudication, clear ownership, and accountability. Effective internal and external communication practices are also evaluated to ensure alignment across all levels.
- **Design**: This pillar focuses on designing the network architecture with resilience as a core principle. This involves incorporating redundancy, risk assessments, and diversity into the design. The goal is to build systems that can handle failures without causing significant service interruptions. Assessment includes evaluating redundancy plans, supplier dependencies, blast-zone containment, and the robustness of architecture and design methodologies to minimize single points of failure.
- **Implement**: The implementation pillar ensures that the network is built in accordance with the design specifications, adhering to resilience standards. Proper configuration management, supplier management, compliance with standards, and implementing best practices are critical to ensuring that resilience is effectively embedded during deployment. This phase assesses how well configuration management is performed, how well the implementation adheres to standards, and the effectiveness of resilience practices, such as testing and verification.
- **Operate**: Operation of the network includes monitoring, maintaining, configuring, and optimizing the network on a day-to-day basis. This pillar assesses the ability to maintain high availability through proactive monitoring, maintenance, and performance evaluation. Key components assessed include routine health checks, maintenance protocols, change management, real-time monitoring systems, and effective incident detection processes. The purpose is to ensure that there are operational processes in place that have a high probability of identifying potential issues.
- **Respond:** The respond pillar is critical in minimizing the impact of outages when they do occur. This pillar involves having a well-defined response plan that includes rapid detection, containment, communication, fault identification and restoration of services. Assessment of this pillar focuses on the effectiveness of incident response processes, the speed of restoration activities, and the ability to learn from incidents through post-incident reviews and implementing lessons learned.
- **Foundations**: These foundational enablers are essential for the consistent application of the five pillars. Foundational elements include governance, Key Performance Indicators (KPIs), metrics and data-driven

decision-making, learning and continuous improvement, and fostering a resilient organizational culture. These elements ensure that resilience is not just about technology but is embedded in the organization's processes, culture, and decision-making. Specific attributes assessed include governance processes, leadership support, the effectiveness of data-driven metrics for resilience, and processes for learning and continuous improvement.

A. Framework Structure

Each attribute in the framework is assessed through a structured process involving data collection, interviews, and evidence-based analysis, with the result of the assessment being a numeric score indicating how closely the implementation of the pillar approaches the ideal. Attribute scores are aggregated into pillar scores, providing an overall resilience score for the network. This scoring system allows for both internal tracking and benchmarking against industry peers.

IV. Methodology for Assessing Telecom Network Resilience

A. Audit Process

The resilience audit follows a systematic process, including the following phases:

- **Pre-Engagement**: Establish the audit scope, assemble the team of experienced telecommunications engineers who are trained in the network resilience framework to conduct the assessment and gather initial data from stakeholders.
- **Planning**: In collaboration with interview sponsors within the organization being assessed, define the interview strategy and create a schedule for data collection, interviews and stakeholder engagements. Since no two service providers are the same (organizationally, structure, business strategy, regulatory perception, technical maturity, etc.), it is important to establish the interview strategy to ensure that the audit is focused properly and navigates the realities of the service provider's current context.
- **Data Gathering**: Gather information through documents, reports, surveys, and interviews to enable evidentiary analysis of resilience attributes.
- **Findings Development**: Identify key observations, develop findings, and score attributes based on evidence gathered.
- **Recommendations**: Develop targeted recommendations to improve resilience based on identified gaps and weaknesses.

B. Attribute-Based Scoring

The attribute scoring methodology employs both quantitative and qualitative assessments for each attribute. Quantitative assessments are based on a series of specific and measurable considerations for each attribute that can be scored. Qualitative input, on the other hand, is derived from the overall strength of the responses to these questions; this can be used to modulate the recommendations developed from the scoring. Scores are assigned from 1 to 5, reflecting the level of resilience maturity based upon the following rubric.

Score	Assessment Criteria	
N/A	Not applicable to this case	
0	Nothing in place	Red
1	Observed but minimal, immature and in localized pockets	Red
2	Observed partially across the organization, some good practices to expand	Yellow
3	Observed systemically but needs further improvement (e.g., budget/resourcing too limited, practices out of date, performance not meeting expectations, etc.)	Yellow
4	Enacted systemically with expected rigor and repeatability	Green
5	Learning/Reinforcement and optimization of widely deployed and effective practices	Green

The aggregated scores are used to generate a series of detailed comparative charts including a top-level resilience radar chart that visually represents the network resilience strengths and weaknesses. This scoring helps organizations understand their current resilience posture and areas requiring attention, as well as allows for benchmarking against best-in-class peers.

As an example, a score for an operator might result in the evaluation depicted below.

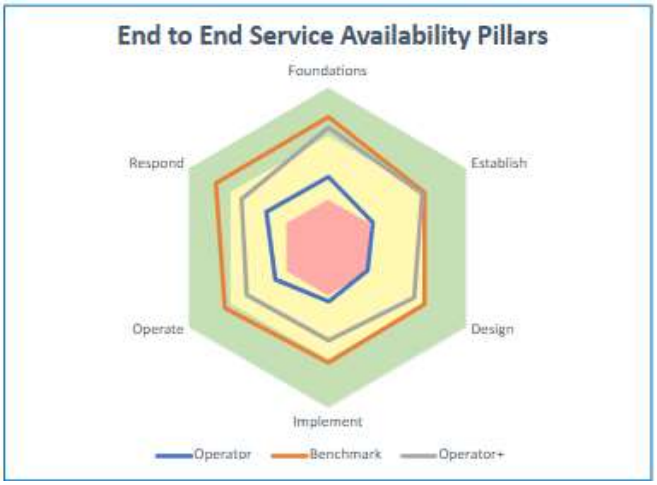

Figure 2: Framework Audit Sample Results

In this evaluation, the blue scores (Operator) represent the current assessment of the network being evaluated, and the orange (Benchmark) depicts a "best in class" network derived from data accumulated from the audits of other networks. The gray (Operator+) line represents a possible improved state for the network under assessment after a specific set of recommendations are successfully implemented.

Figure 3: Sample of individual attribute pillar scoring

Scores at the Pillar level as depicted in Figure 2 provide a high-level dashboard but it is important to look deeper within each pillar. Figure 3 provides an example of how detailed scoring is depicted for one sample pillar (Design) and how the capabilities of the attributes within each pillar vary exposing specifics strengths and concerns more granularly to enable remediation.

C. Audit Results and Benchmarking

The audit model evaluates resilience through comprehensive assessments that yield primarily quantitative results, with qualitative observations a by-product of the quantitative analysis. Results are categorized into risk levels using a **Red/Yellow/Green (R/Y/G)** framework as shown in Figures 2 and 3, allowing for easy visualization of resilience performance against industry benchmarks.

- **Comparison to Peers**: The audit framework also enables benchmarking against peers within the telecommunications industry. It is expected that companies that score consistently high on attributes should demonstrate stronger service availability and resilience. The benchmarking process helps highlight gaps where a company's resilience performance falls below industry norms and identifies best practices from peers that can be adopted to improve outcomes.
- **Evaluation of Remediation Action Plans**: It is important to ensure that remediation and improvement efforts are prioritized and provide the maximum resiliency return on investment while addressing the most crucial needs with urgency. The framework can be used to assess various improvement plans by scoring (predicting) the impact of actions to quantify their overall benefit vs. the needs and capabilities of the organization. Figure 2 depicts an example of this where the gray line (Operator+) shows the impact of a successfully executed example improvement plan relative to the currently assessed state shown by the blue line (Operator).
- **Red Flags and Immediate Actions**: During the audit, specific attributes may raise "Red Flags," indicating areas where immediate action is required to prevent potential vulnerabilities from compromising network resilience. These red flags are crucial for guiding attention to critical issues and ensuring that mitigation efforts are prioritized appropriately.

V. Recommendations for Enhancing Network Resilience

A. Proactive and Reactive Measures

Based on the assessment the next step is to determine recommendations to enhance and improve the resiliency of the network. These recommendations are extracted from the pillar analysis and are driven by low-scoring areas. Typically, recommendations will focus on an entire pillar with a low score, or individual attributes with scores noticeably below the mean score across attributes. 'Red flag' items that indicate 'network at risk' conditions should obviously receive priority.

Recommendations generally fall into two types: Proactive and Reactive.

- **Proactive Improvements** focus on actions that will avert or minimize future outages. Examples of proactive improvements are: Implementing redundancy strategies, regularly updating risk assessments, and improving cross-functional collaboration.
- **Reactive Enhancements** address problem areas that have already caused an outage and are known, current weaknesses. Examples include strengthening incident response plans, investing in outage detection tools, and establishing clear communication protocols to manage incidents effectively.

A consideration in creating recommendations is to balance between these two types of recommendations. A network in immediate distress may need more reactive work, where a relatively well-functioning network may benefit from more of the proactive recommendations.

B. Cultural and Foundational Changes

Maintaining a strong corporate culture towards resilience is essential. Governance, leadership support, and effective training programs are key elements for ensuring that resilience is embedded within the organization's DNA. Low attribute scores in the Foundation area are more likely to result in recommendations that address cultural issues.

C. *KPIs*

To ensure the success of network resilience efforts, it is crucial for an operator to have in place Key Performance Indicators (KPIs) that measure both the desired outcomes and operational effectiveness of resilience strategies. The attributes and considerations of the framework thoroughly assess the presence of comprehensive KPIs and metrics as well as how they are collected, measured, employed and operationalized. Specific KPIs and metrics are chosen to measure the effectiveness of initiatives recommended as a result of the scoring. It is particularly important that recommendations include the addition of missing KPIs along

with ongoing action to monitor, analyze, and understand the data from these KPIs.

These KPIs are divided into two primary types: leading indicators and lagging indicators.

- **Leading Indicators**: Leading indicators are proactive metrics that can predict potential resilience issues before they lead to outages. Examples include the number of resilience tests conducted, compliance with maintenance schedules, and early detection rates of vulnerabilities. These indicators help assess the preparedness of the network and the ability to anticipate issues.
- **Lagging Indicators**: Lagging indicators, on the other hand, measure outcomes after events have occurred. These include metrics such as outage duration, mean time to recovery (MTTR), and customer impact during outages. These indicators provide insight into the effectiveness of the response and the overall resilience of the network.

Choosing an effective set of KPIs allows for the Pillar scoring to be tracked and progress monitored against goals.

VI. Discussion

A. Calibration

As we have made use of the framework, we have observed that the scoring can be subjective. A future improvement will be to calibrate scoring across evaluators and projects.

B. Variance across Interviewees

Another observation is that within the same organization there can be significant variation in the internal evaluation across interviewees. While this may at first seem like a concern, in fact it turns out to be a good indicator of where problems exist. Wide variation in internal scoring identifies areas for additional investigation.

C. Adaptation

Not all telecom operators and networks are identical. The framework can be adapted to align with the characteristics of a specific operator. For example, some attributes may not apply to an MVNO.

D. Future Trends in Network Resilience

Future resilience challenges will include handling new paradigms such as AI-driven network optimization, managing SDN architectures, and incorporating cloud-based service integrations. These developments will require continuous adaptation and agile resilience planning and will influence evolution of the framework as well.

VII. Conclusion

A. Summary of Key Findings

This paper presented a comprehensive resilience framework designed for telecom networks. The framework includes five lifecycle pillars: establish, design, implement, operate, and respond, supported by foundational elements to ensure service providers meet reliability expectations amidst increasing network complexity.

B. Implications for Industry

The adoption of resilience audits and periodic benchmarking is essential for improving operational readiness, reducing the risk of outages, and maintaining customer trust. As networks evolve, resilience frameworks must also adapt to changing technological landscapes.

VIII. Acknowledgements

The authors wish to thank Technology Audit Partners and industry stakeholders for their contributions and insights in shaping the resilience framework.

IX. References

[1] The Japan Times, “NTT DOCOMO suffers outage leaving 1.3 million users unable to make calls, send texts,” Dec. 26, 2018. [Online]. Available: https://www.japantimes.co.jp/news/2018/12/26/business/ntt-docomo-suffers-outage-leaving-1-3-million-users-unable-make-calls-send-text/

[2] ZDNet, “Telstra suffers nationwide outage, blames third party,” [Online]. Available: https://www.zdnet.com/article/telstra-suffers-nationwide-outage-blames-third-party

[3] National Institute of Standards and Technology, “Framework for Improving Critical Infrastructure Cybersecurity,” Version 1.1, Apr. 16, 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf doi: 10.6028/NIST.CSWP.04162018

[4] R.Owen, A. Bryant, L. Finch, D. Franklin, "Resilience in the IP Era: Navigating the Fragility of Modern Telecommunications Networks & the Sovereign Functions," TechRxiv, Preprint, 2023. [Online]. Available: https://www.techrxiv.org/articles/preprint/

[5] “The Rising Need for Strong Network Resiliency,” White Paper. [Online]. Available: https://img1.wsimg.com/blobby/go/90526c83-8429-464d-8025-a3ba5a28a84f/Rising%20Need%20for%20Strong%20Network%20Resiliency%20Fram.pdf

X. Author Information

Paul Steinberg, Distinguished Technical Advisor, Paul Steinberg, is an accomplished telecommunications executive with extensive experience in wireless communications solutions for government, commercial, and mission-critical applications. Formerly Motorola Solutions’ Chief

Technology Officer and Senior Vice President of Technology, he led technology strategy, standards, venture capital investing and intellectual property initiatives. Paul holds 17 US patents, has served on the executive boards of TIA and NSC, and has been a member of the FCC's TAC and CSRIC.

Jim Peterson, Distinguished Technical Advisor, Jim Peterson, specializes in systems-level thinking, modeling, and performance analysis of complex products. With over 25 years in telecommunications at companies like AT&T Bell Labs, Motorola, and Lucent Technologies, he has held leadership roles in systems engineering and architecture. Jim has also taught Systems Engineering and Computer Science and holds a PhD in Computer Science from the University of Illinois.

Fred Gabbard, Managing Partner at Technology Audit Partners, Fred Gabbard brings extensive expertise in network migrations, product management, and network resiliency consulting for Tier 1 operators. Formerly a VP at Motorola, he led global product management for wireless technologies. He also served as Senior VP of Engineering at WMS Gaming, driving significant operational improvements.

Mark Ennis is a Managing Partner at Technology Audit Partners, Mark Ennis specializes in program and portfolio management, with expertise in product development and process improvement. A former Executive Director at Motorola and Nokia Networks, Mark has implemented large-scale organizational changes and received a CEO Quality Award for his impact on product turnarounds. He holds a BS in Computer Science, an MBA, and is PMP and Prosci ADKAR certified.

Ray Owen, Professor at the University of Technology Sydney, Ray Owen leads the Telecom Research Unit, advancing telecommunications innovation and industry collaboration. He consults globally on network resilience and operations and has served on various boards, including the Australian Mobile Telecommunications Association and UTS advisory boards. Ray holds a PhD in Electrical and Electronic Engineering and has over 19 patents, emphasizing STEM diversity and industry-driven research.