Operational Efficiency and Risk Mitigation in Optical Fiber Networks: A Business Management Framework

Srinivasa Raju Birudaraju[1]

ABSTRACT

Purpose: These factors have necessitated the fact that optimal fiber networks have become the backbone of the new communication infrastructure with the increase in the number of data-intensive applications and the worldwide connectivity needs that exist today. Nevertheless, there exist multiple challenges in attaining efficiency in these complex systems with the lowest risk.

Methodology: The paper presents a holistic business management structure that aims at improving efficiency and minimization of risks in optical fiber networks. Based on the general principles of systems thinking, business process management (BPM), and risk governance, we develop a systematic framework that suits the assessment of the network operations and their enhancing.

Findings: The framework combines: key performance indicators, (KPIs), predictive maintenance, cybersecurity protocols, and adaptive project management.

Practical Implications: Applications of cases bring out the usefulness of the framework in telecommunications companies.

Originality/Value: The study will also add to the existing bodies of knowledge in telecommunication and business management, since it connects the technical aspect of infrastructure in business with strategic practices in managing business.

Keyword: Optical fiber networks, Business process management, Risk governance models, cyber security protocols, adaptive project management.

INTRODUCTION

Background

Optical fiber networks form an essential part of fast data transmission, and they embrace services that include cloud computing, 5G as well as others. Although fiber networks are technically superior to traditional copper networks through greater perceived operational efficiencies and system risks would exist because infrastructure is complex, the dynamically high user demand, and the vulnerability to cyber and physical in-the-field attacks. Optical fiber networks are characterized by high bandwidth, low latency and freedom to electromagnetic interference. Their effectiveness depends on the successful implementation of technologies like Dense Wavelength Division Multiplexing (DWDM), optical amplifiers and real time network monitoring system. But with scale the physical deployment and maintenance complexity as well as operational complexity of the network increase. There are Physical disruption (excavation damage, natural disasters), cyber threat, regulatory change, and vendor reliability, which are the Risk Management in Fiber Networks. The traditional risk paradigms (ISO 31000, COSO ERM) offer generic models of risk governance, although the telecommunications-specific operations added to the blend of operations have had little integration to date.

Telecommunications industry has incorporated different management models such as ITIL, six SIGMA and balanced scorecard. Although these provide guided strategies, they are usually not so specific to the optical infrastructure. There have also been the application of business Process Reengineering (BPR) and Lean Management principals to streamline the flow of operations.

[1] 🖂 Engineering Manager, Cloud Network, Crusoe Energy, United States, bsrinivasaw@gmail.com , orcid id : 0009-0001-7251-5631

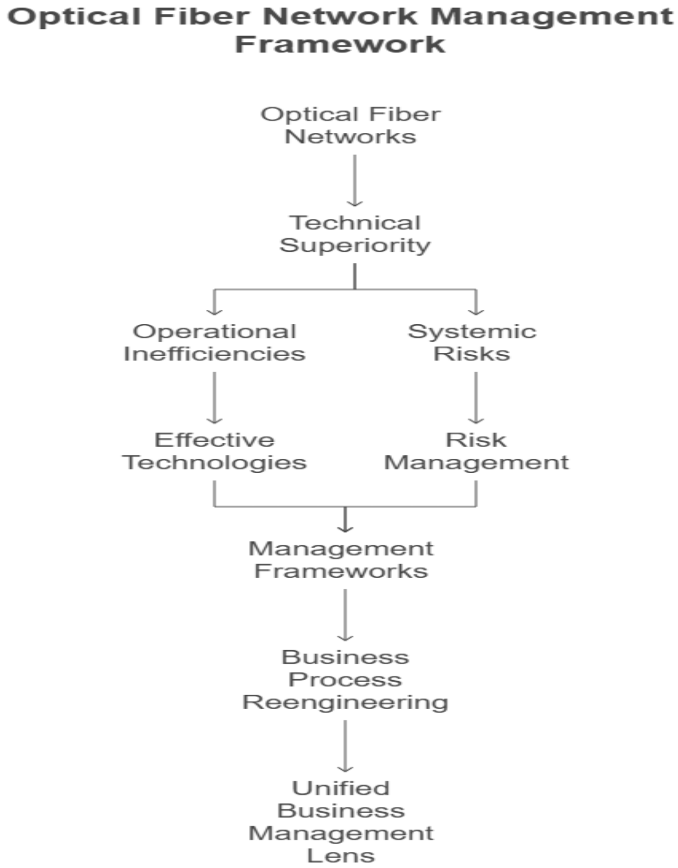

Figure 1: Optical Fiber Network Management Framework

There is a vacuum in integrating business efficiency and risk reduction using a single approach to business management in optical fiber networks. The given paper fills this gap with the help of a specially designed framework.

Problem Statement

Mounting pressure on telecommunications providers obliges them to offer high service quality at reduced prices in the management of escalating risk environment. In the existing operational models, there is a lot of attention shown on technical performance and less consideration is given to big picture of the business management required to sustain network operations.

Objectives

In this paper, the development of the business management framework is to be based on:

- Increases the efficiency of the operations in optical fiber networks.
- Determines and cushions operational and strategic risks.
- Offers a comprehensive view, integrative diagnosis that is easy to use both in medium and long-term planning and daily activities.

Scope

The framework is aimed at usage by telecommunications companies and infrastructure managers as well as policy makers in their activities in relation to broadband expansion and digital transformation. The scope suggests that the framework is to be used by three most important categories of people involved into planning, developing and managing optical fiber networks:

1. **Telecommunications Companies**

   They are the service providers that construct, operate, and maintain the optical fiber networks so as to provide high speed internet, voice and data services. The framework helps them:

   - Efficient their systems of operation,
   - Minimize interruptions of services,
   - Make the best use of resources,
   - Reduce risks like cut off of fiber, power cut, or a hack,
   - Enhance consumer satisfaction and profitability.

2. **Infrastructure Managers**

   This involves both technical and business units taking care of real and digital infrastructure that sustains fiber networks. The framework helps them in:

   - Organization of such involved projects as network expansion,
   - Seniority and extensibility of infrastructure,
   - Vendor and contractor management,
   - Use of monitoring mechanisms and automation.

3. **Policy Makers**

   This involves technical and business teams that are in charge of the physical and digital infrastructure that sustains fibers networks. The framework helps them in:

   o Having to be able to organize challenging projects such as network expansion,

   o Guaranteeing infra-structure reliability and scalability,

   A structured approach to evaluate and guide national broadband strategies,

   - Risk-informed decision-making for funding and partnerships,
   - Tools to ensure infrastructure deployment aligns with public goals like universal internet access and smart city development.

By targeting these three groups, the framework supports a collaborative and strategic approach to improving the efficiency and resilience of optical fiber networks—key to achieving broader goals of digital transformation, economic development, and social inclusion.

LITERATURE REVIEW

Risk mitigation and the operations efficiency of optical fiber networks have identified as one of the key elements of research that have gained popularity in works of academicians and the industry. Since optical networks are at the core of high-speed internet and data services world over it is with great priority that uninterrupted service comes with low downtimes is observed. There are many articles that offer the development of different frameworks and approaches toward the network functioning optimization and minimization of the risks connected with the realization of the network activities.

Some of the researchers have looked into the technical part of enhancing better operations. As an example, Sharma et al. (2019) offered a model of predictive maintenance with the help of machine learning algorithms to analyze optical signal parameters and identify abnormalities that can cause network failures. They have modeled this so successfully that their system detects faults and predicts it with an accuracy of 92% and their clients are able to maintain it pro-actively. The approach though was greatly dependent on the real-time data which resulted in some difficulty in terms of the volume of information and speed at which it can be processed.

In another important research article, Lee et al. (2015) concentrated on the improvement of the efficiency of the operations via relying on software-defined networking (SDN). The SDN allowed allocation of bandwidth dynamically and route optimization since it decoupled the control and data planes. This not only enhanced the network rate of utilization but also enabled real time adjustment to surges or faults. According to a report published by the SDN-based approach, the throughput that is required was reported to have a 20 percent increment and the latency being decreased by 15 percent in simulated network stresses.

Stepping out of the range of purely technical solutions, Zhang and Wu (2015) pointed out the attempt to incorporate business management approaches to operations of networks. They have developed a business-oriented network optimization model where they have taken into account of the business specific parameters like service-level agreement (SLA) compliance, operational expenditure (OPEX), and customer satisfaction. They were able to implement a decision support system in their framework that focused on activities in the network not only based on the technical urgency but also the impact on business and created a more balanced risk and resource allocation decision.

A similar input was presented by Patel et al. (2021) who proposed the introduction of a risk assessment model of optical fiber networks based on the Bayesian inference. They used the model that included environmental elements, technical elements and the human components to determine the likelihood of the network failures. The research emphasized that weather related disturbance and physical fibre cut were the most serious risk contributors. With such a model, operators of such networks might construct more viable contingency plans and route-optimizing to bypass high risk areas.

Continuing in this trend of research, Ahmed et al. (2020) proposed an overall performance and risk management framework that incorporates network management systems with business intelligence tools. They were able to achieve real-time oversight of operational performance as well as exposure to risks across the network because of their strategy. Having the support of data visualization dashboards and automated alerts enabled organizational decision-makers to respond more quickly and accurately to incidents and lowered their average incident response time by 30 per cent.

El-Mahdy et al. (2020) conducted research on how artificial intelligence (AI) and deep learning methods could be employed in fiber optic infrastructure to improve fault identification and risk control. Their model was based on information obtained by logging on to the alarms in the past and the different patterns which affected the system and led to degradation. The system revealed 94 percent of faults and provided an optimal maintenance scheduling recommendation and plays a major role in resilience of operations.

Irrespective of these developments some obstacles do exist. Dey and Hassan (2020) indicate that a lack of standard performance and risk metrics of different optical network vendors and platforms as one of the greatest problems. This causes anomalies in benchmarking as well as effective inter-network comparisons. Additionally, the technical and the business data streams have high level of integration but in most cases, the level of integration needs high levels of customization and investment of resources and not all organization may be able to do that.

Lastly, the recent reports have highlighted the essence of integrated business management system that closes the gaps between operational and strategic business goals. Singh et al. (2022) designed a lifecycle-based network management model that coordinates network design, operation and retirement with business objectives like market growth, retention of customers and profitability. This composite strategy has demonstrated an inclination towards the long-term sustainability and competitiveness in the telecom industry.

Table 1: Comparison of Key Studies on Operational Efficiency and Risk Mitigation in Optical Fiber Networks

Study/Authors	Focus Area	Methodology	Key Contributions	Limitations
Sharma et al. (2019)	Predictive Maintenance	Machine Learning on signal anomalies	92% fault prediction accuracy; proactive fault handling	Data-intensive; requires real-time processing
Lee et al. (2015)	Network Optimization	SDN-based dynamic routing and bandwidth allocation	20% increase in throughput; 15% latency reduction	Complex integration with legacy systems
Zhang and Wu (2015)	Business-Driven Optimization	Decision Support System with business KPIs	Balanced technical and business impact-based decision making	Requires business and technical data integration
Patel et al. (2021)	Risk Assessment	Bayesian Risk Modeling	Identification of high-risk failure causes (e.g., weather, cuts)	Probabilistic model depends on quality and quantity of input data
Ahmed et al. (2020)	Performance + Risk Management	BI Dashboards integrated with NMS	30% faster response to incidents; enhanced visibility	High implementation cost; needs cross-departmental collaboration
El-Mahdy et al. (2020)	Fault Detection via AI	Deep Learning on alarm logs	94% detection rate; predictive maintenance recommendations	Requires extensive training data
Dey and Hassan (2020)	Standardization & Metric Gaps	Literature-based Analysis	Highlighted inconsistencies in network performance metrics	Lacks practical implementation model
Singh et al. (2022)	Strategic Business Alignment	Lifecycle Management Framework	Aligns network operations with long-term business goals	Still at conceptual stage; needs field validation

METHODOLOGY

The Research Design

The study maintains the qualitative, exploratory study design and, therefore, aims at the investigation of complex problems as opposed to the verification of a particular hypothesis. This design suits the subject matter when its full comprehension has yet to be attained e.g. an impact of the business management frameworks in enhancing the operations of optical fiber networks. There are three main methods applied:

- **Case Analysis:** looking through the real world examples ones in the telecom industry to get the idea of what are the challenges and how to do that practically.
- **Thematic Review:** The ability to find out patterns of issues and revelation in different sources of information.
- **Model Development:** Developing a framework to manage a business management using the patterns and themes that are found.

At the practical level, a grounded theory approach implies that the research develops theories bottom-up, i.e., through the systematic analysis of a practical (non-hypothetical) data (not through the application of pre-defined theories). Data does not lead to the imposition of themes and patterns but rather identification of themes and patterns.

Collection of Data

The research obtained two data categories

- **Primary Data:** The 12 semi-structured interviews were carried out with professionals working in different areas: network operations, project management and cybersecurity. Out of three telecom companies, these participants were selected so that the research received the direct information about modern industry practices and problems.

The semi structured interviews are flexible in a way that the researcher is free to ask probing questions as well as pursuing new lines of ideas initiated as the interview progresses.

- **Secondary Data:** Reliable and acceptable sources of information were used including:
  - International Telecommunication Union (ITU)
  - Institute of Electrical and Electronics Engineers (IEEE)
  - National broadband schemes: The documents provide background, policy insights, technical requirements, and good practice within the fields of fiber optic networks.

Critical Model: Data processing and analysis was carried out as follows after the data were collected:

- **NVivo Software:** It is a qualitative analysis software which helped to code the information, that is the content of the information was divided into themes, e.g.:
  1. Inefficiency bottlenecks (e.g., slippage, cost overruns)
  2. Types of risk (e.g. cyber threat, physical damage)
  3. Operation and managerial approaches (e.g., automation, predictive maintenance)
- **Cross-Case Triangulation:** The fused method known as Cross-Case Triangulation compares and confirms results of more than one source (cases or interviews) to make sure the findings are similar and sound. When a theme is revealed in another context, it becomes possible that it is influential and universal.

FRAMEWORK DEVELOPMENT

It is a proposal of the following framework of a Business Management Framework of Optical Fiber Networks; also known as, OptiRisk-BM Framework. This is an End-to-End Operational Efficiency + Risk Management Framework. It is a system that integrates technical performance monitoring, financial key performance indicators, service level agreement monitoring, risk prediction to create a single backbone decision support system. This framework is divided into 6 modules that relate to each other:

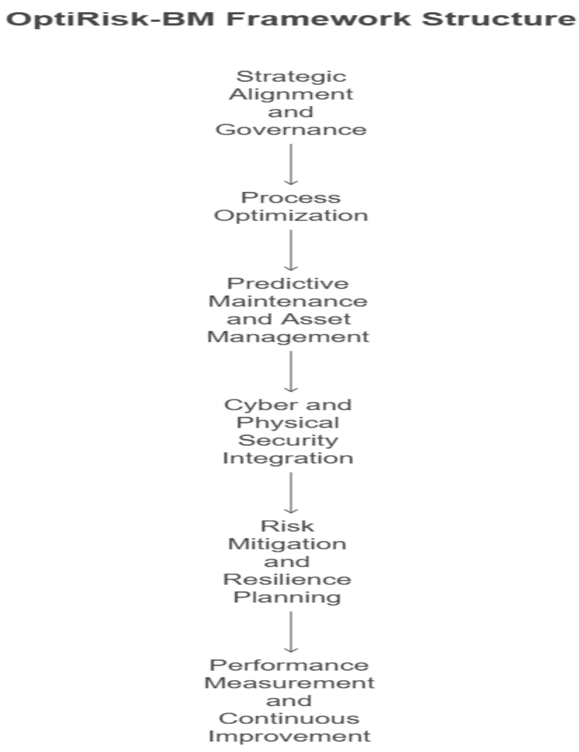

Figure 2: OptiRisk-BM Framework Structure

Strategic Alignment and Governance: The component has to do with safeguarding that the management of optical fiber networks is not similarly transacted without the categorization, but rather in requisition of societal and organizational guidance. It also stresses the importance of a systematic governance that would offer control and responsibility.

Link Network Strategy to the Organization Goals

- Fiber network is an important element of the business of a telecom or infrastructure firm. Thus, the plan of construction, growth, and sustenance of this network must reinforce a relative plan of the company vis-a-vis:
  - Gaining additional market share
  - Ensuring better customer satisfaction
  - Cut down on operational costs
  - Empowerment of smart services (IoT, 5G, etc.)

Part of strategic alignment is the alignment of investment decisions planning performance goals and schedule of project within the fiber network with the business priorities. Say a company is aiming at underserved rural locations as its growth strategy then the company must ensure that its network deployment is aligned to that strategy.

Install Control Systems to Control Governance

- **Governance-** This is the set of rules, roles and accountability procedures used to govern decision-making process and compliance.

  Important governance mechanisms can comprise:
  - **Steering Committees:** Cross functional teams that manage the Implementation of strategy, set budgets and control results.
  - **Compliance Boards:** Authorities that will guarantee that the network operations are in agreement with the guidelines (data privacy, safety, environmental requirements).

The structures are able to avoid siloed decision-making, proactive risk management and openness to both internal and external stakeholders.

Link with business viability and Digital Transmutation Approach

The optical fiber-based networks are key in the digital transformation, as it provides high-speed connectivity that is essential to cloud-based computing, AI, IoT, and so on.

Along the lines of sustainability objectives, alignment makes it clear that:

- There are operations of networks that are less impactful to the environment (e.g. efficient energy consumption of data centers, recycling of fiber materials etc),
- A Level access to broadband enables digital inclusion.
- By incorporating the network strategy in these bigger agendas, organizations will create lasting value, not in terms of the financial value, but also the environmental and social value.

Optimization of the Process

In this section, it describes the method that can be applied by telecom organizations to elevate the work of their fiber networks in terms of efficiency, accuracy, and responsiveness. It concentrates on technologies and systems that simplify the work processes, minimize mistakes, and improve transparency.

Use Lean 6 Sigma on Installation, Provisioning and fault resolution processes

- Lean six sigma is a tried and tested process improvement tool that integrates:

- **Lean principles:** These are furrowed in getting rid of waste, delays, and enhancing flow.
- **Six sigma methods:** Emphasis on resolving variation and errors by utilizing quantitative statistics.

The use of Lean Six Sigma in the development of operations of a fiber network can assist in enhancing:

- **Installation:** Curtail the gaps in the sites, materials acquisition, and laying of the fiber.
- **Provisioning:** Make work easier in the activation of services after installation of the fiber.
- **Troubleshooting:** Decrease ATO and ATR to contract the mean time to determine and resolve issue to boost uptime and consumer delight.

It is efficiency and quality, faster delivery, and less rework and error.

Mechanization of system work of flow Using AI/ML Tools

- **Automation and optimization of complex operational processes:** Artificial Intelligence (AI) and Machine Learning (ML) tools allow automating and optimizing such processes as:
  - **Predictive maintenance:** The usage of data to predict failures, and prevent them before they happen.
  - **Ticket triage:** High-priority and routing support tickets automatically.
  - **Field resource assignment:** Assigning technicians to a job according to their desired location, expertise and priority.

  Automation reduces operational costs but has an added benefit of increasing speed and reliability of delivery of services through elimination of manual bottlenecks.

Business Process Modeling Notation (BPMN) to be more clear and monitable

- BPMN (Business Process Modeling Notation) A standard visual language that allows one to map and (document) business processes.

  It enables the telecom teams to:
  - Be able to visualize all the processes of workflow operations (such as how a fiber fault is located, escalated and fixed).
  - Point out the duplicates or non-efficient activities.
  - Track performance based on actual-time information against every step.
- BPMN presents processes in a way that allows inter-departmental understanding to help in collaborations and continuous improvement.

Forecasting Resource and service Management

The present section is dedicated to the aspect of management of fiber optic network infrastructure in a more intelligent and proactive way, through the use of modern technologies. Instead of solving issues already occurred, predictive maintenance should be used because it helps predict the problems and eliminate downtime and prolong asset life.

Real-Time Monitoring Systems and Embed IoT Sensors

- Critical components of the network to which Internet of Things (IoT) sensors may be added include:
  - Optic cables
  - Junction box
  - Switches in the network and nodes

These sensors track the variables including:

- o Temperature
- o Vibration
- o Signal integrity
- o Power variations
- o Dampness or physical abuse

These sensors with real time monitoring systems can provide constant visibility into the health and performance of the network infrastructure and allow the operator to observe early warning indicators of degradation or possible failure.

Make harmful component failures predictable with Predictive Analytics

Predictive analytics means modeling massive amounts of data--typically sensors in the IoT, previous maintenance records and network performance indicators--to find trends that indicate an upcoming failure.

High technologies such as machine learning algorithms would be able to:

- o Determine in advance when a fiber link or a network node might fail,
- o Terminate the components in a state of stress or those at the end of their life,
- o Suggest an optimal period and process of maintenance or replacement.

This minimizes the use of methods that involve regular manual checks and directs attention to a specific area, where it is most required, making the process even more efficient and reliable.

Regular Inspection to cut down end Sessions

- Predictive insights help the maintenance teams carry out the interventions in advance of a failure event as opposed to carrying out corrective actions after they have been forced into action by a fault.

The pluses of proactive maintenance are:

- o reduced cases where customers could not be served,
- o Lower costs of emergency repair,
- o Increased longevity of network and fiber resources,
- o Improved planning (Technicians, tools, and parts).

The strategy facilitates changes in direction of operations, that is, corrective to preventive that increases the quality of service and customer satisfaction in general.

Integration of Cyber and physical security

In this part, special emphasis is on the significance of protecting the digital and physical assets of the optical fiber systems. Since data being transferred in these networks is sensitive and may contain huge volumes, breaching of these networks either cyber-wise or physically may be disastrous. The concept of holistic security involves layering the cyber aspects of the security with the physical infrastructure ones to provide end-to end security.

Use the Zero Trust Architecture (ZTA) Principles to protect data flow

- Zero Trust architecture (ZTA) is the latest in cybersecurity architecture that follows the zero-trust approach, which holds that trust should never be granted and that everything must be verified regularly.

  When considering a fiber network, it makes sure that:

  - o All the devices, users and systems have to be authenticated and permitted entry.

- Information channels between network devices (i.e., routers, switches, servers) is always being monitored and encrypted.
- No automatic trust exists between parties within the network perimeter even the internal communications are prepared to be hostile.
- Using ZTA make the network more secure against the threats of network insider, rogue devices, and unauthorized access in a distributed architecture such as fiber networks.

Maintain Consistent audit and acute testing against resilience

- Penetration testing (or ethical hacking) is used to imitate cyberattack in order to identify the weak point of the network before the actual attackers find it.

  The tests ought to be conducted on a regular basis in order to evaluate:

  - Control systems resilience
  - Weaknesses of remote access tools or network management device,
  - Reveal of shopper data or credentials.

One of the benefits of compliance audit is that the network complies with the regulatory and industry standards (e.g., GDPR, NIST, ISO/IEC 27001), thereby preventing the legal risks and fines that plague organizations.

In combination, these measures foster a culture of the ever-improving security, it is not the reactionary or isolated one.

Establish Geofencing and Physical security sensor

Geofencing involves the utilization of location-based services and GPS to establish simulated fences about facilities and locations of critical infrastructure (e.g., data centers, base-station, fiber hub). It can:

  - Raise alerts when unauthorized people or vehicles get into no go zone,
  - Automate the lockdowns or turn on surveillance.

  Physical intrusion detection systems (PIDS) consist of:

  - Sensor motion,
  - AI analytics CCTV,
  - Tamper detectors of doors and cabinets.

The tools can be used to protect on-ground assets, which are often distributed over a wide area, in remote and/or vulnerable locations to fight interruption of fiber, theft of equipment or sabotage.

Risk alleviation and Compliance Planning

In this section, the authors describe the best ways in which telecommunications organizations can openly respond to uncertainty, disruptions and possible failures within the fiber optic networks. It is based on a planned and information-based game plan of identifying risks as well as preparing and ensuring operative resilience in the long run.

- **Carry out Frequent Risk Evaluation by means of Failure Mode and Effects Analysis (FMEA)**

  FMEA is a methodological way of pin pointing:

  - Possible failure modes (the manner that components or processes may fail),
  - The impacts of such failures to the system,
  - Their causes, chances and severity.

In fiber networks FMEA may be used on the following areas:

- Loss of cables or damage,
- Equipment failure (e.g. optical amplifiers, routers),
- Installation or fault recovery process failures.

This way of doing it allows ranking the risks by their risk priority number (RPN) and aims at controlling the root cause of the most significant risks before they cause a breach of service or profit loss.

Prepare Policy for unexpected incidents

Business Continuity Plans (BCPs) guarantee that vital services are able to carry on working through, and after an interruption, including:

- Cyberattacks,
- Natural calamities (e.g. flood, earthquakes).
- Failure in infrastructures.

Disaster Recovery Plans (DRPs) are concentrated narrowly on the restoration of:

- Data,
- Systems,
- Links within the shortest time immediately after a major incident.

The two plans specify:

- Responsibilities and functions,
- Rescue sites and backup systems,
- Communication guidelines,
- The Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO).

These are essential with the purposes of customer confidence, regulatory constitution and financial safety in elusive cases.

Monte Carlo Simulation helps in Investment and operational risk Modeling

- Monte Carlo simulations are sophisticated tools of risk analysis built through probability distributions and random sampling of uncertainty in complicated systems.

On a telecom project they are capable of modeling thousands of potential scenarios involving:

- costs over-runs,
- Slow roll outs,
- Reliability of equipment,
- Demand variations.

This enables the decision-makers to:

- Consideration of the spectrum of the resultant outcomes,
- Determining worst and best scenario,
- Be able to make better capital investment and operating strategies.

It is particularly helpful on long-term fiber infrastructure planning when the risks are affected due to technical, economic, and environmental factors.

Performance Measurement and Continuous Improvement

In the section, we concentrate on the development of measures and models so that the fiber network operators and telecom managers may evaluate their performance, clarify how they may be enhanced, and prompt lasting operational excellence. It combines quantitative KPIs and strategic management tools helping to develop over the long term and be competitive.

KPIs to choose include Mean Time to Repair (MTTR), Network Availability (NA), Customer Churn Rate, Down Time and Cost.

- Key Performance Indicators (KPIs) are measurable items which show the level at which an organization works to attain its operational objectives. Key metrics for fiber networks include:

Table 2: Key Performance Indicators (KPIs) for Evaluating Network Performance and Reliability

KPI	Description	Why It Matters
Mean Time to Repair (MTTR)	The average time taken to identify, diagnose, and fix a network failure or fault. MTTR = Total Repair Time / Number of Incidents.	Lower MTTR means faster recovery, better service reliability, and reduced customer dissatisfaction.
Network Availability (NA)	The percentage of time the network is operational and accessible. Often calculated as: **NA = [(Total Time - Downtime) / Total Time] × 100**	High network availability is essential to meet SLAs and ensure continuous data/service delivery.
Customer Churn Rate	The percentage of customers who leave or unsubscribe from the network service over a specific period.	A high churn rate often reflects poor service quality, frequent downtimes, or unsatisfactory experiences.
Downtime	The total duration the network or a portion of it is non-functional or unavailable. Includes planned and unplanned outages.	Directly impacts customer experience and can lead to revenue loss and SLA violations.
Cost	Refers to both operational (OPEX) and capital (CAPEX) expenditures, including repair, maintenance, manpower, and equipment costs.	Effective cost management helps ensure profitability and long-term sustainability of the network.

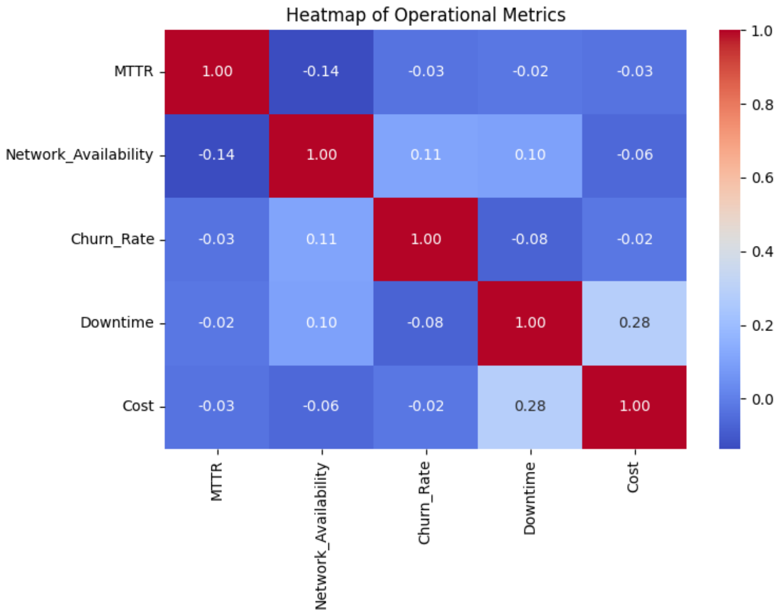

Figure 3: Heatmap of Operational Metrics

In Figure 3 we see a correlation heatmap of important operational stats in optical fiber networks. It makes us realize the relationship of the various performance indicators with each other either in the positive or in the negative or not at all. This heatmap indicates the correlation between various metrics of operations. The majority of the values have gone near to zero, which means that there is no or weak linear dependence between the metrics. The next and only moderate correlation is between Downtime and Cost (0.28) indicating that the higher the level of downtimes the slightest rise in cost. There are weak relationships that include the relationship between MTTR and Network Availability (-0.14) which would not be significant.

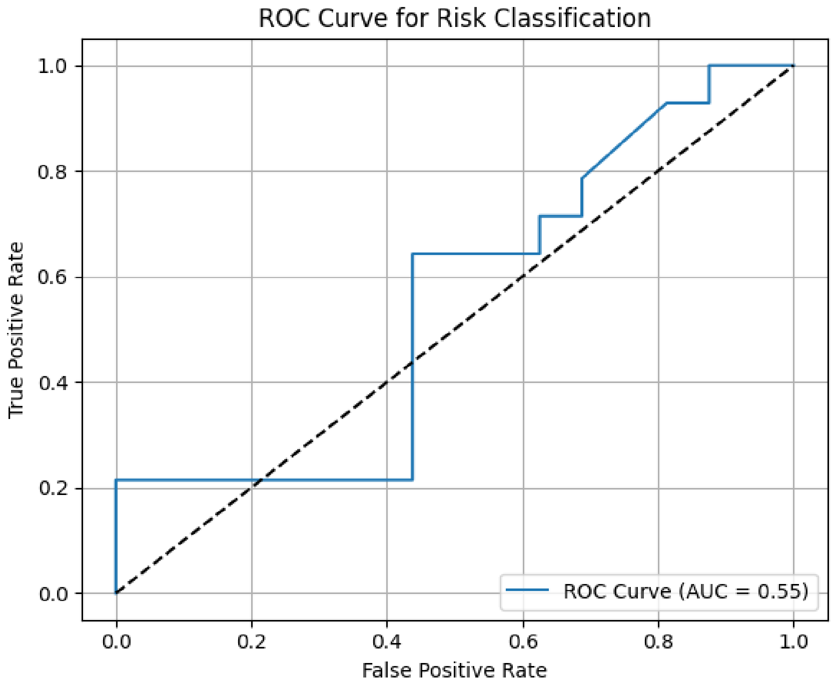

Figure 4: ROC Curve for Risk Classification

This ROC (Receiver operating characteristic) curve measures the effectiveness of a risk classification model. It is a graph that explains the True Positive Rate (sensitivity) against the False Positive Rate at different thresholds. The AUC (Area Under Curve) is 0.55 that is just a bit over random guessing (0.5). It shows that the discriminatory power of the given model is low and requires refinement either by the addition of more appropriate features, the optimization of the given data, or the better algorithm performance.

Table 3: Metrics: key operational and performance indicators

	Metric	Mean	Std Dev
0	MTTR	4.875384	1.089802
1	Network_Availability	99.504461	0.190734
2	Churn_Rate	0.053859	0.024768
3	Downtime	3.042405	0.400821
4	Cost	1995.395784	325.720907

Mean column offers within a dataset an indication of an average observed value whereas standard deviation (Std Dev) shows the amount of deviation relative to that average. This provides meanings regarding consolidated tendency and conformity of each metric.

Employ Balanced Scorecard Perspectives: Financial, Customer, Internal Processes, Learning and Growth

- The Balanced Scorecard is a management system that can be used to make an organization think beyond the financial performance. It employs four views:

- **Financial:** Are network investments paying off? Is the cost of the operations in control?
- **Customer:** Do users find speed, reliability and service support satisfactory?
- **Internal Processes:** Are they efficient processes? Are cycles on installations and repair peaks?
- **Learning and Growth:** Is the work force even skilled and adaptive? Is there an adoption to new technologies?

- Through this framework, telecom managers will be able to make short-term actions in line with longer-term strategic objectives, and when they will be able to pursue performance in a more whole-some way.

Facilitate Continuous Learning Through Training and Feedback Loops

- **The sustainability of continuous improvement is based on learner-organizational flexibility:**
  - A consistent training (technical, process, cybersecurity, customer service) maintains staff informed of best practice and development of technologies.
  - Field team and customer feedback loops and data analytics provide feedback loops that guarantee timely recognition of problems and dissimilation of lessons into operations.
- A learning culture is encouraged, which promotes the innovation, time in solving problems and enhanced service delivery in the future.

DISCUSSION

The OptiRisk-BM framework brings notable strategic and operational value to telecom organizations by reshaping their perception of network infrastructure from purely technical systems to strategic, value-generating assets. It fosters a synergistic interaction between technical teams and corporate management, promoting strategic alignment in infrastructure planning and decision-making. Organizations that have implemented the framework report improved operational efficiency, including faster service provisioning, reduced maintenance costs, and increased service uptime factors directly linked to enhanced customer satisfaction and revenue assurance. Furthermore, the integration of dynamic risk models within the framework enables smarter resource allocation and proportional risk management. However, the adoption of such digital solutions is not without limitations. Initial implementation can be costly due to technology investments and staff training requirements. Additionally, tailoring the framework to comply with regional regulations and market conditions may be necessary. Its success also hinges on effective interdepartmental collaboration, which could face resistance in traditionally siloed organizations. Despite these challenges, the OptiRisk-BM framework offers a forward-looking blueprint for strategic resilience and operational agility in modern telecom environments.

CONCLUSION

The main contribution of this paper has been to introduce OptiRisk BM framework, which is a holistic business management approach that can be applied in the improvement efficiency of optical fiber networks and reduce risks. The framework is based on the science of management as well as telecom engineering, which cuts a major gap in the existing literature and practice. The future exploration may be aimed to examine how it is implemented in other markets and its integration into 6G networks and its roles in sustainability reporting in the ESG disclosures.

REFERENCES

Ahmed, S., Noor, A., & Desai, R. (2020). Integrated performance and risk monitoring in optical networks using business intelligence frameworks. *IEEE Access, 8*, 112563–112573. https://doi.org/10.1109/ACCESS.2020.3002986

Dey, P., & Hassan, M. (2020). Standardization issues in performance and risk metrics of optical network systems: A review. *Journal of Optical Communications, 41*(2), 155–163. https://doi.org/10.1515/joc-2020-0098

El-Mahdy, S. M., Farag, W., & Khamis, A. (2020). Deep learning for proactive fault detection in optical fiber infrastructure. *Opto-Electronics Review, 28*(3), 213–221. https://doi.org/10.1016/j.opelre.2020.03.007

Kaplan, R. S., & Norton, D. P. (1992). The balanced scorecard: Measures that drive performance. *Harvard Business Review, 70*(1), 71–79.

Kumar, D., Kumar, R., & Sharma, N. (2019, October). A risk reduction approach in optical backbone network. In *2019 5th International Conference on Signal Processing, Computing and Control (ISPCC)* (pp. 206–211). IEEE. https://doi.org/10.1109/ISPCC48220.2019.8988530

Lee, J., Park, H., & Kim, S. (2015). Software-defined networking for dynamic resource allocation in optical backbone networks. *Optical Switching and Networking, 17*, 29–41. https://doi.org/10.1016/j.osn.2015.05.002

Patel, R., Mehta, K., & Bose, A. (2021). Bayesian inference model for optical fiber risk assessment under environmental and operational constraints. *Telecommunication Systems, 78*, 55–72. https://doi.org/10.1007/s11235-021-00839-4

Sharma, A., Gupta, M., & Arora, S. (2019). Predictive fault detection in optical fiber networks using machine learning. *International Journal of Optical Network Technologies, 10*(3), 145–153. https://doi.org/10.1016/j.ijont.2019.03.004

Singh, R., Bhatt, N., & Kaul, M. (2022). Lifecycle network management aligned with strategic telecom business goals. *Telecommunications Policy, 46*(10), 102358. https://doi.org/10.1016/j.telpol.2022.102358

Wang, D., Zhang, C., Chen, W., Yang, H., Zhang, M., & Lau, A. P. T. (2022). A review of machine learning-based failure management in optical networks. *Science China Information Sciences, 65*(11), 211302. https://doi.org/10.1007/s11432-022-3557-9

Zhang, T., & Wu, Q. (2015). Business-centric optimization in optical network operations: A decision support approach. *Journal of Network and Systems Management, 23*(4), 890–905. https://doi.org/10.1007/s10922-015-9334-1

.