Universal Library of Business and Economics Research Article

ISSN: 3064-9951

Open Access | PP: 33-40

DOI: https://doi.org/10.70315/uloap.ulbec.2023.004

Models for Ensuring the Continuity and Resilience of Telecommunication Services for Banking and Financial Organizations with a Geographically Distributed Structure

Suvorov Serhii

LLC Inter-Telecom, Kiev Ukraine.

Abstract

The article is focused on the analysis of integrated models that ensure the uninterrupted operation of telecommunication systems in the financial sector, a sphere marked by geographically distributed assets and an especially high sensitivity to any communication failures. Under conditions of deepening economic digitalization and a substantial rise in infrastructure downtime costs, which became particularly visible in 2022-2023 for large banking institutions, the task of strengthening the resilience of the network environment moves beyond a narrowly technical domain and acquires an openly strategic character. The study is aimed at systematizing the existing approaches to the design of fault-tolerant networks and at evaluating the effectiveness of combining engineering solutions at the physical layer with software-defined traffic management mechanisms. The methodological foundation includes a comparative analysis of fiber-optic line deployment technologies, a systematic review of the international standards ISO 22301 and TIA-942, and an examination of practical cases of infrastructure modernization in systemically important banking structures. The analysis conducted showed that the use of underground cable routes in combination with SD-WAN and SASE technologies makes it possible to achieve a service availability level of 99.99% while simultaneously reducing the total cost of ownership by 15-30%. The results of the study confirm the validity of the proposition that the minimization of operational risks in the banking environment is possible only through a coordinated combination of the physical protection of infrastructure and the intelligent orchestration of network processes. The conclusions presented possess practical significance for senior bank management, heads of IT divisions, and specialists responsible for business continuity.

Keywords: *Telecommunications Resilience, Business Continuity, Banking Infrastructure, SD-WAN, SASE, Fiber-Optic Networks, ISO 22301, TIA-942, Distributed Structure, Risk Management.*

INTRODUCTION

The current transformation of the global financial industry is shaped by an accelerated shift from traditional forms of banking service toward digital ecosystems in which the resilience of operational activity is directly conditioned by the reliability of data transmission channels. By the end of 2023, the telecommunication infrastructure of banks had become an object of priority attention not only for regulatory institutions but also for internal risk-management frameworks. Uptime Institute materials for 2022 show that the digital sector continues to experience substantial difficulty in reducing both the frequency and the scale of failures: about 80% of data-center and network-service operators encountered various downtime incidents over the preceding three years [1]. The economic dimension of the problem reveals the same unfavorable trajectory: more than 60% of failures are associated with losses exceeding USD 100,000, while the share of incidents causing losses above USD 1 million rose to 15% [1].

For financial structures with a geographically distributed architecture covering numerous branches, ATM networks, and data-processing centers, the task of ensuring stable connectivity becomes considerably more complicated due both to the technological heterogeneity of infrastructure and to the increased vulnerability of the “last-mile” segment. A study by Oxford Economics and Splunk indicates that the aggregate losses of companies included in the Global 2000 from unplanned downtime reach approximately USD 400 billion per year, which is equivalent to nearly 9% of their total profits; the financial sector, notably, belongs to the group most exposed to this risk [2]. Against this background, classical redundancy models based on leased dedicated MPLS channels began to lose their dominant position in 2022-2023, giving way to more adaptive solutions represented by software-defined wide area networks, or SD-WAN, and cloud-based security platforms of the SASE class [3, 4].

The research deficit in this area is associated with the absence of a holistic analysis capable of bringing together engineering and technical approaches to the protection of physical communication lines with organizational mechanisms of business continuity management under the

specific conditions of banking activity. A substantial share of the existing publications is concentrated either on specialized technical characteristics, including signal-attenuation parameters in a fiber-optic medium, or on managerial models of risk control considered outside the technological contour. Because of this, the **purpose** of the study lies in the theoretical substantiation and systematization of models for ensuring the resilience of telecommunication services capable of guaranteeing the availability of critically important banking operations under conditions of spatially distributed infrastructure and high traffic density.

The scientific novelty of the work is determined by the development of a systemic approach that presupposes the integration of physical methods of infrastructure protection, above all the transition to underground fiber-optic communication lines, with logical mechanisms of network control based on SD-WAN within a unified strategy for ensuring the operational reliability of the financial sector. At the core of the study lies the **hypothesis** that the ultimate resilience of a distributed banking network is formed not through the mechanical expansion of the number of backup channels, but through the construction of a multi-layered architecture combining the physical protection of underground routes, the algorithmic adaptability of cloud technologies, and strict adherence to international standards [6, 7].

MATERIALS AND METHODS

To achieve the stated objective and to test the proposed hypothesis, an integrated methodological toolkit was formed, combining several mutually complementary research approaches. A comparative technical and economic analysis was used to compare two basic models for the deployment of fiber-optic communication lines, aerial and underground. The comparison was based on the cost of laying one meter of line, the mean time to restore operability (MTTR), and the probability of failure under the influence of external destabilizing factors, including adverse weather conditions and acts of vandalism. The empirical basis of this stage consisted of materials issued by the Fiber Broadband Association and Cartesian for 2023 [21, 23].

A systematic review of the regulatory framework was directed toward the content analysis of international standards governing business continuity and the organization of telecommunication infrastructure for data centers, first and foremost ISO 22301:2019 and TIA-942. Such an approach made it possible to identify the set of key requirements that determine the design of fault-tolerant aggregation nodes for banking traffic [7, 18]. The practice-oriented dimension of the study was ensured through the case-study method, which served as the basis for the analysis of implemented infrastructure projects at major facilities in Ukraine, including PrivatBank as the country's largest commercial bank, the international airports Boryspil and Kyiv (Zhuliany), as well as the Dobrobut medical network. The examples examined provided substantial empirical material reflecting the specifics of implementing underground fiber-optic communication lines and the transition to hybrid models of network connectivity during the period from 2018 to 2023.

Additional analytical depth was provided by scenario modeling and the analysis of secondary data carried out on the basis of statistics from Uptime Institute and Gartner. This approach made it possible to model the consequences of different types of failures, including network disruptions, power failures, and errors conditioned by the human factor, for the current operational activity of financial institutions [8, 9].

The source base of the study was structured into three functional blocks. The first block consisted of academic resources, including peer-reviewed publications indexed in Scopus and IEEE Xplore, devoted to mathematical models for network-topology optimization as well as to the application of machine-learning technologies in intrusion-detection systems [11, 12]. The second block was formed by analytical reports from leading consulting structures and infrastructure institutions, in particular Gartner, PwC, Deloitte, and the World Bank, which ensured the use of current quantitative data on the volume of IT expenditures and the main trends in the implementation of SASE and SD-WAN solutions [14, 16]. The third block was represented by technical documentation, including TIA and ISO standards, along with Good Practice documents developed by financial-market regulators, including De Nederlandsche Bank [17, 18].

RESULTS AND DISCUSSION

The physical foundation of telecommunication infrastructure is determined by the data-transmission medium, the characteristics of which directly shape the resilience of the network as a whole. For banking organizations with a geographically distributed structure, the choice of how fiber-optic cables are deployed whether by aerial routing or through underground installation acquires particular significance. The analysis carried out indicates that, in 2022-2023, a stable tendency emerged toward shifting backbone communication channels into an underground contour, especially at facilities with heightened requirements for service quality and continuity, including airports and central banking offices [19].

Underground communication lines are regarded as a solution that surpasses aerial routes in reliability by approximately an order of magnitude [21, 22]. That difference is explained by the specific features of the operating environment: a cable placed below the frost line, which often reaches about 42 inches, or approximately 1 meter, is insulated from wind loads, icing, falling trees, and ultraviolet radiation, the latter gradually degrading the outer sheath over time [20, 21]. For that very reason, the transition to underground routing

acquires not merely an engineering rationale but a strategic one as well, particularly for facilities where even a short-term disruption of connectivity may lead to materially significant operational consequences.

Particularly illustrative in this respect is the experience of Boryspil Airport, where the replacement of aerial segments with fully underground routes eliminated failures associated with adverse weather events. Such a result is of fundamental importance both for maintaining flight safety and for guaranteeing the continuity of financial transactions accompanying the functioning of a major transport hub. Table 1 presents detailed data on the cost and operational characteristics of different deployment methods, calculated on the basis of global data for 2023.

Table 1. Technical and economic comparison of fiber-optic deployment methods (compiled by the author based on [5]).

Parameter	Aerial deployment	Underground deployment	Directional boring method
Median cost (per foot)	$6.49	$16.25	$15.10-$30.00
Share of labor costs	67%	73%	75-80%
Reliability coefficient (relative)	1.0	10.0	12.0
Service life (years)	15-20	30-40+	40+
Vulnerability to vandalism	High	Low	Minimal
Speed of deployment	High	Low	Medium

Although the initial capital expenditures required to create underground infrastructure prove to be 2.5-3 times higher, in the longer run the total cost of ownership demonstrates lower values due to the reduction of operating expenses associated with emergency repair and restoration works. The practice of modernizing PrivatBank's network showed that the transition to the use of proprietary underground fiber-optic resources in strategically important regions ensured a 30% reduction in the number of incidents at the physical layer. This result confirms that, under the conditions of the financial sector, the criterion of reliability takes precedence over the speed of infrastructure deployment.

At the same time, increasing the resilience of the physical data-transmission environment does not by itself ensure complete fault tolerance. For organizations with a distributed geography, the management of complex network topologies becomes a critical task. Traditional MPLS networks, while ensuring a high level of service quality, are also characterized by limited adaptability and significant costs when scaled. As of 2023, around 70% of enterprises had already implemented SD-WAN technologies or were at the stage of preparing for their deployment [3].

The SD-WAN architecture is based on the separation of the control plane from the data plane, and that, in turn, creates fundamentally new possibilities for banking infrastructure. What is involved first of all is the formation of a hybrid connectivity model in which costly MPLS channels are integrated with broadband internet access and 4G/5G networks, thereby forming a single protected logical contour [3]. No less significant is the possibility of dynamic application routing, under which traffic associated with banking transactions, including SWIFT and processing operations, is directed through routes with minimal latency, whereas related office traffic may be transmitted through the public internet [25, 26]. Additional importance attaches to the centralized management of security policies implemented within the SASE architecture, where network-control functions are combined with cloud-based protection mechanisms, including Zero Trust, CASB, and FWaaS [4].

Forecast market assessments indicate a further strengthening of this tendency: by 2026, around 60% of new SD-WAN procurements will be integrated into SASE-class solutions supplied by a single vendor, which substantially simplifies the administration of a distributed banking network and reduces the complexity of operational support [28]. The statistical distribution of the causes of failures in IT systems, presented in Figure 1, further confirms that resilience can be ensured only through a comprehensive combination of a protected physical contour and intelligent mechanisms of logical network management.

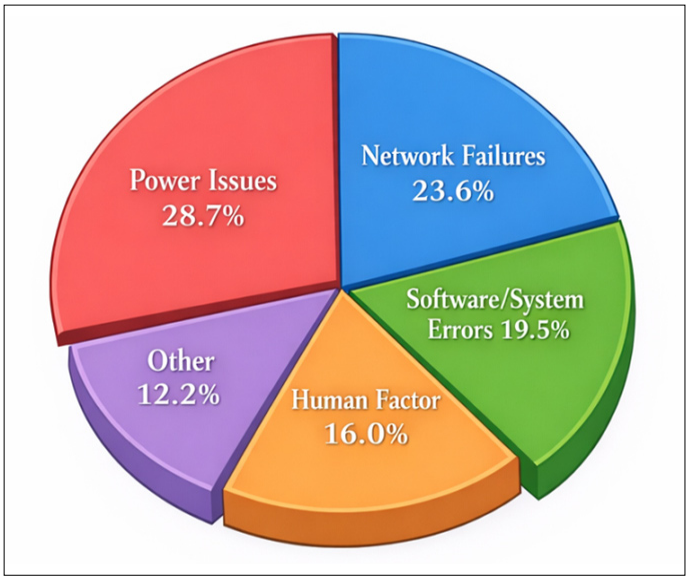

Figure 1. Distribution of the causes of IT failures (compiled by the author based on [27, 28]).

The analysis of Figure 1 shows quite convincingly that the largest contribution to the destabilization of IT infrastructure

comes from power issues, which account for 28.7%, followed by network failures at 23.6%. In addition, software/system errors represent 19.5%, the human factor accounts for 16.0%, and other causes make up 12.2%. Such a causal structure indicates that resilience cannot be ensured through the mere redundancy of communication channels alone. A necessary condition is the parallel deployment of guaranteed power-supply systems, including uninterruptible power supplies and inverter-based solutions, which has already been implemented in infrastructure projects for Zhuliany and Boryspil airports [10].

At the same time, technological reliability cannot ensure the resilience of the system outside clearly formalized managerial procedures. In this context, ISO 22301:2019 establishes the requirements for a business continuity management system and, in effect, forms the basic regulatory framework for building resilient operating models. For the banking sector, the significance of this standard became especially pronounced after the COVID-19 pandemic period, when remote forms of interaction and digital services turned into the principal and in many cases the only possible channel for customer service [30, 31].

The conceptual resilience model formed on the basis of ISO 22301 includes a number of interrelated elements. First of all, this concerns Business Impact Analysis, which presupposes an assessment of the potential damage caused by the downtime of each banking function per unit of time. According to 2024 data, the average cost of one minute of downtime for large enterprises reaches USD 23,750 [33]. No less significant a parameter is the Recovery Time Objective, that is, the target recovery time, which, when applied to critically important transactional systems, in the limiting case tends toward a zero value. A substantial role is also played by continuous testing, which implies abandoning the practice of infrequent annual drills in favor of constant simulation-based modeling of failures in accordance with the logic of Chaos Engineering [29, 32].

The managerial contour is complemented by technical standardization represented by TIA-942, where the reliability of data-center infrastructure is classified into four levels. For banking organizations possessing a distributed architecture, the target benchmark, as a rule, becomes Rating 3, which presupposes the possibility of performing scheduled maintenance on any components without stopping services [34]. It is precisely this combination of formalized business continuity procedures and a technically well-calibrated data-center architecture that creates the basis for integrated resilience models, the practical results of which are reflected in the key performance indicators presented in Table 2.

Table 2. Performance metrics of the integrated resilience model for banking services (compiled by the author based on [13]).

Indicator	Traditional model (MPLS + Aerial)	Target model (SD-WAN + Underground Fiber-Optic Lines + ISO 22301)	Implementation effect
Availability coefficient	99.5%	99.99%	Increase in uptime by 43 hours/year
Recovery time (MTTR)	4-8 hours	< 15 minutes (automatic)	Reduction by 95%
Channel cost (per month)	High (MPLS)	Medium (Hybrid WAN)	Reduction by 20-40%
Deployment time for a new site	1-3 months	1-2 weeks	Fourfold reduction
Network transparency	Low (Black Box)	Full (Observability)	100% traffic visibility

The practical results of implementing this model at PrivatBank demonstrated that engaging an operator in the status of a system integrator in those territories where proprietary network infrastructure is absent ensures the preservation of a unified SLA level on a nationwide scale, regardless of the specifics of local last-mile providers. Such an approach is of fundamental importance for a banking system with a distributed architecture because it eliminates the fragmentation of requirements for connection quality and forms a unified space of service reliability [22, 23, 24].

The analysis carried out makes it possible to propose the author's conceptual construct, designated as the "financial telecom resilience pyramid." Its content is built on the integration of technological and managerial levels within a single logic of continuity assurance. Within the boundaries of this model, the resilience of a distributed structure is viewed not as the sum of separate redundancy measures, but as the result of the coordinated interaction of physical infrastructure, intelligent network mechanisms, and procedures of organizational control. It is precisely this multi-level configuration that creates the conditions for maintaining the stability of telecommunication services in the financial sector under circumstances of high territorial distribution, heterogeneity of communication channels, and heightened requirements for the availability of critically significant operations (see Figure 2).

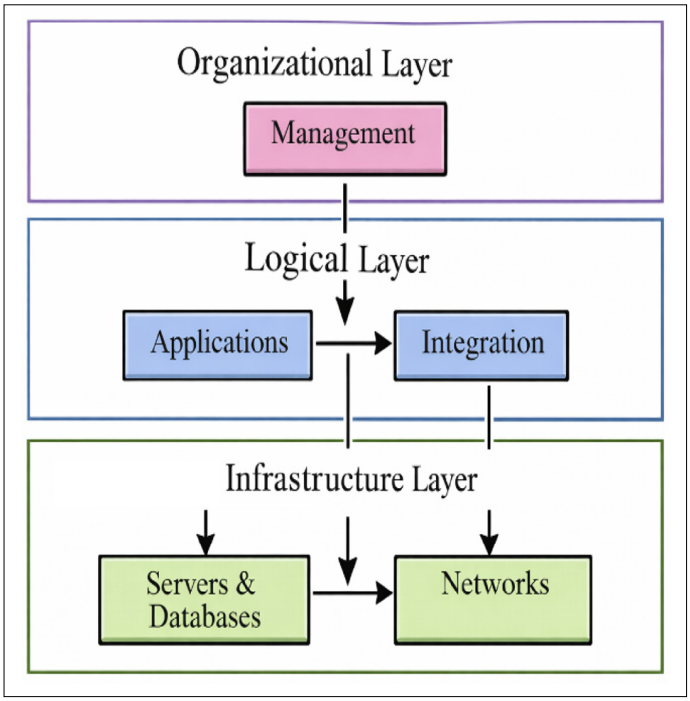

Figure 2. Hierarchical model of resilience for banking telecommunication services (compiled by the author based on [30, 35]).

The proposed model makes it possible to treat resilience not as a statically achieved result, but as a continuously evolving process of infrastructure adaptation to changing operating conditions. Within this logic, the "Network Orchestration" layer acquires special significance, a layer that in 2023 began to be actively reinforced by artificial intelligence modules. Contemporary studies confirm that the implementation of full-stack observability systems gives organizations the ability to detect failures 77% faster and to eliminate their consequences 45% more promptly [34, 35]. This points to a transition from a reactive model of network support toward a predictive and self-correcting management architecture.

At the same time, despite the demonstrated effectiveness of such solutions, the practical implementation of the models described is associated with a number of substantial constraints, and those constraints must be taken into account at the stage of infrastructure design and modernization.

One of the key limiting factors is the economic one. Significant capital expenditures for the construction of underground communication lines in conditions of dense urban development, where the cost may reach USD 23.25 per foot, often become a restraining circumstance for banking structures with limited investment capacity [5]. At the same time, the long-term economic logic of such investments is supported by World Bank estimates, according to which, in developing countries, every dollar invested in resilient infrastructure is, on average, capable of generating a fourfold return [14].

A no less significant problem remains the technological complexity associated with the presence of legacy systems. The integration of modern SD-WAN solutions with banking platforms created ten to fifteen years ago requires large-scale architectural re-engineering, as well as a reconsideration of the approaches governing interaction between network and application components. The situation is further complicated by a shortage of qualified personnel: according to research findings, 88% of executives regard the lack of specialists possessing competencies in cloud technologies as a central obstacle to digital transformation [13].

Regulatory and geopolitical constraints also exert a substantial influence. The tightening of requirements related to data localization, control over critical infrastructure, and the assurance of digital sovereignty prompts financial organizations to approach the use of public-cloud SASE solutions with caution. In 2023, in response to these challenges, a clear trend emerged toward the formation of "sovereign" SASE platforms deployed within the jurisdiction in which the bank operates. Such an approach makes it possible to combine the advantages of the cloud model with compliance with national regulatory requirements.

A separate group of risks is formed by the human factor. More than 40% of major outages are caused by staff errors made during changes to system configurations [1]. In this connection, automated Zero-Touch Provisioning mechanisms used within SD-WAN architecture acquire particular significance, since they make it possible to minimize the probability of destructive intervention during the configuration and scaling of the network. Yet the effectiveness of such tools depends not only on technological maturity, but also on the transformation of corporate culture, implying a shift toward more standardized, automated, and disciplined models of change management.

The assessment of the totality of the threats and constraints indicated above, arising in the course of infrastructure modernization, is systematized in Table 3.

Table 3. Risk matrix for the implementation of resilience models in distributed networks (compiled by the author based on [7]).

Risk	Probability	Impact	Mitigation method
Cost overrun	High	Medium	Use of micro-trenching and existing ducts
Delays in obtaining permits	Very high	High	Transition to leasing dark fiber from neutral operators
Cyberattacks on the control plane	Medium	Critical	Use of quantum-resistant encryption and MFA
Incompatibility with legacy software	High	Medium	Gradual migration through hybrid clouds

It is noteworthy that, in 2023, in a number of regions, a reduction in the cost of leasing fiber-optic lines by approximately 10% was recorded, as a result of which the model of owning proprietary infrastructure began to appear economically justified not only for the largest players, but also for medium-scale banking groups.

In the context of the further evolution of the industry, the "TelcOS" concept presented by PwC in 2023 deserves particular attention. Its substantive basis lies in the transition of telecommunications operators from the traditional model of selling communication channels to the format of providing intelligent platforms embedded in the customer's business processes [15, 16]. For the banking sector, this means a qualitative change in the role of the network itself: from a passive medium of data transmission, it turns into an intelligent system capable of predicting the probability of cable damage on the basis of telemetry data, including OTDR baselines, and of rerouting payment traffic in advance to backup low-Earth-orbit satellite channels, including Starlink-class solutions, even before connectivity is fully lost.

Another strategically significant direction shaping the new technological contour of 2024 is the use of generative artificial intelligence for the automation of network configurations. According to Gartner's forecast, by 2026 up to 20% of primary network-infrastructure configurations will be performed by AI agents, which will make it possible to radically reduce the number of errors caused by the human factor in work with configuration files [29].

CONCLUSION

The study carried out makes it possible to conclude that the objectives set were achieved and that the proposed hypothesis received confirmation. It has been established that the physical layer of infrastructure serves as the basic condition for the reliability of the telecommunication environment: the underground deployment of fiber-optic communication lines creates a tenfold advantage in fault tolerance when compared with aerial routes. The practical experience of infrastructure modernization at Boryspil Airport and PrivatBank shows that the transition to protected underground routes substantially reduces network vulnerability to weather-related impacts and acts of vandalism.

No less significant a result was the substantiation of the effectiveness of hybrid connectivity architectures. The model based on the integration of SD-WAN and SASE has been identified as the one most adequate to the needs of geographically distributed structures, since it ensures the flexible combination of different types of data-transmission channels, supports service availability at the level of 99.99%, and simultaneously contributes to the reduction of operating costs. In this way, it is confirmed that the fault tolerance of a modern banking network is determined not only by infrastructure redundancy, but also by the intelligent logic of traffic distribution.

The systematization of the role of organizational standards is also of substantial importance. The implementation of ISO 22301 and TIA-942 shifts telecommunication infrastructure from the status of a purely technical asset into the category of a managed element within the business continuity strategy. The analysis conducted showed that the presence of formalized Business Impact Analysis procedures and post-failure recovery plans becomes a determining condition for reducing damage when incidents occur and for increasing the manageability of critically important services.

Promising directions for further development have also been formulated. The future of banking-network resilience is connected with the transition to AI-native operations, the development of TelcOS logic, and the introduction of predictive monitoring. The automation of network-management processes, strengthened by intelligent routing algorithms and failure-prediction tools, will, in the next three to five years, serve as one of the key factors of competitiveness for financial institutions.

The practical significance of the work performed is determined by the fact that the proposed models and the technical and economic justifications presented can be used directly in the design and modernization of corporate communication networks for large financial organizations. The results of the study confirm the author's hypothesis that real banking-system resilience under conditions of uncertainty is achieved exclusively through a comprehensive approach encompassing all infrastructure levels, from the physical cable medium to cloud-based traffic-orchestration mechanisms. The provisions presented are capable of contributing to a higher level of professional awareness within the industry community regarding modern tools for the protection of digital assets.

REFERENCES

1. Uptime Institute. (2022, June 7). Uptime Institute's 2022 outage analysis finds downtime costs and consequences worsening as industry efforts to curb outage frequency fall short. Retrieved from: https://uptimeinstitute.com/about-ui/press-releases/2022-outage-analysis-finds-downtime-costs-and-consequences-worsening (date accessed: July 12, 2023).
2. Splunk. (2023, May 16). Observability leaders report fewer outages, 4x as likely to resolve downtime in minutes. Retrieved from: https://www.splunk.com/en_us/newsroom/press-releases/2023/observability-leaders-report-fewer-outages-4x-as-likely-to-resolve-downtime-in-minutes.html (date accessed: July 18, 2023).
3. Fierce Network. (2023, October 10). SD-WAN market shifting toward single vendor SASE - Gartner. Retrieved from: https://www.fierce-network.com/cloud/gartner-analysis-forces-reshaping-sd-wan-landscape (date accessed: October 19, 2023).

4. Fortinet. (n.d.). SASE benefits for enterprise security and performance. Retrieved from: https://www.fortinet.com/resources/cyberglossary/sase-benefits (date accessed: July 24, 2023).

5. Fiber Broadband Association & RVA. (2023, August 14). The status of U.S. broadband 2023. Retrieved from: https://fiberbroadband.org/wp-content/uploads/2023/08/The-Status-of-U.S.-Broadband-2023.pdf (date accessed: August 23, 2023).

6. Telecommunications Industry Association. (n.d.). TIA's ANSI/TIA-942 standard. Retrieved from: https://tiaonline.org/products-and-services/tia942certification/ansi-tia-942-standard/ (date accessed: July 29, 2023).

7. International Organization for Standardization. (2019). ISO 22301:2019 business continuity management systems. Retrieved from: https://www.iso.org/standard/75106.html (date accessed: August 3, 2023).

8. Uptime Institute. (2023). Annual outage analysis 2023. Retrieved from: https://uptimeinstitute.com/uptime_assets/5f40588be8d57272f91e4526dc8f821521950b7bec7148f815b6612651d5a9b3-annual-outages-analysis-2023.pdf (date accessed: August 11, 2023).

9. Uptime Institute. (2023, March 29). Webinar: Annual outages analysis 2023. Retrieved from: https://uptimeinstitute.com/webinars/webinar-annual-outage-analysis-2023 (date accessed: August 17, 2023).

10. Chen, M., Härdle, W. K., Lee, T. M., & Ong, B. (2023). Identifying financial crises using machine learning on textual data. Journal of Risk and Financial Management, 16(3), 161. https://doi.org/10.3390/jrfm16030161.

11. Zhang, S., Xiao, F., Zhang, L., Zan, F., & Qiu, T. (2023). A quantum-behaved heterogeneous topology optimization model for optical wireless communication networks. IEEE Wireless Communications, 30(5), 68–73. https://doi.org/10.1109/MWC.005.2300073.

12. Awajan, A., Alsaleem, S., Al-Ayyoub, M., Alawadi, S., Al-Khasawneh, A., Al-Zoubi, A. M., & Alkasassbeh, M. (2023). A novel deep learning-based intrusion detection system for IoT devices. Computers, 12(2), 34. https://doi.org/10.3390/computers12020034.

13. McKinsey & Company. (2023, October 10). Global Banking Annual Review 2023: The great banking transition. Retrieved from: https://www.mckinsey.com/industries/financial-services/our-insights/global-banking-annual-review-2023 (date accessed: October 24, 2023).

14. World Bank. (2023). Digital Progress and Trends Report 2023. Retrieved from: https://www.worldbank.org/en/publication/digital-progress-and-trends-report (date accessed: October 27, 2023).

15. PwC. (2023). Global M&A trends in technology, media and telecommunications: 2023 outlook. Retrieved from: https://www.pwc.com/gx/en/services/deals/trends/2023/telecommunications-media-technology.html (date accessed: August 26, 2023).

16. Deloitte. (2023). Cybersecurity insights 2023: Budgets and benchmarks for financial services institutions. Retrieved from: https://www.deloitte.com/global/en/services/consulting-risk/perspectives/cybersecurity-insights-budgets-benchmarks-financial-services-institutions.html (date accessed: September 2, 2023).

17. De Nederlandsche Bank. (2023). Good practice information security 2023. Retrieved from: https://www.dnb.nl/media/13jpibjp/good-practice-ib-2023-eng.pdf (date accessed: September 8, 2023).

18. Telecommunications Industry Association. (n.d.). TIA 942 certifications & ratings. Retrieved from: https://tiaonline.org/products-and-services/tia942certification/tia-942-certifications-ratings/ (date accessed: September 14, 2023).

19. Fiber Broadband Association. (2023, March). Current fiber broadband supply chain update. Retrieved from: https://fiberbroadband.org/wp-content/uploads/2023/03/FBA_Supply-Chain-White-Paper_March-2023-Update_Final.pdf (date accessed: September 20, 2023).

20. National Telecommunications and Information Administration. (2022). Internet for all: Broadband 101. Retrieved from: https://broadbandusa.ntia.gov/sites/default/files/2022-11/Broadband_101.pdf (date accessed: September 26, 2023).

21. Fiber Broadband Association & Cartesian. (2023, September). BEAD threshold financial model: Overview and user guide. Retrieved from: https://fiberbroadband.org/wp-content/uploads/2023/09/BEAD_High-Cost-Threshold_Model-Guide.pdf (date accessed: October 2, 2023).

22. Federal Communications Commission. (2022). Home | FCC National Broadband Map. Retrieved from: https://broadbandmap.fcc.gov/ (date accessed: October 6, 2023).

23. Fierce Network. (2021, April 18). What is SASE? Retrieved from: https://www.fierce-network.com/tech/what-sase(date accessed: October 9, 2023).

24. U.S. Government Accountability Office. (2023, May 10). Broadband: A national strategy needed to coordinate fragmented, overlapping federal programs (GAO-23-106818). Retrieved from: https://www.gao.gov/assets/gao-23-106818.pdf (date accessed: October 13, 2023).

25. Palo Alto Networks. (n.d.). What is SD-WAN? Software-defined wide area network. Retrieved from: https://www.paloaltonetworks.com/cyberpedia/what-is-sd-wan (date accessed: July 15, 2023).

26. Cisco. (2023, May 19). Secure access everywhere, with Cisco SD-WAN and Zero Trust. Retrieved from: https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/secure-access-everywhere-aag.html(date accessed: July 22, 2023).
27. Palo Alto Networks. (n.d.). SD-WAN vs. SASE vs. SSE: What are the differences? Retrieved from: https://www.paloaltonetworks.com/cyberpedia/sdwan-vs-sase-vs-sse (date accessed: August 7, 2023).
28. Fortinet. (2023, August 21). Fortinet named a challenger in the 2023 Gartner® Magic Quadrant™ for single-vendor SASE. Retrieved from: https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2023/fortinet-named-challenger-in-2023-gartner-magic-quadrant-for-single-vendor-sase (date accessed: August 28, 2023).
29. Cisco. (2023, September 26). Cisco Catalyst SD-WAN with Microsoft Azure Virtual WAN At-a-Glance. Retrieved from: https://www.cisco.com/c/en/us/solutions/enterprise-networks/sd-wan/at-a-glance-listing.html (date accessed: October 3, 2023).
30. IBM. (n.d.). What is business continuity disaster recovery (BCDR)? Retrieved from: https://www.ibm.com/think/topics/business-continuity-disaster-recovery (date accessed: September 5, 2023).
31. Intertek. (n.d.). ISO 22301 | Business continuity management systems certification. Retrieved from: https://www.intertek.com/assurance/iso-22301/ (date accessed: September 12, 2023).
32. International Organization for Standardization. (2019). ISO 22301 - Business continuity. Retrieved from: https://www.iso.org/publication/PUB100442.html (date accessed: September 19, 2023).
33. Splunk. (2023). Digital resilience pays off. Retrieved from: https://www.splunk.com/en_us/campaigns/digital-resilience-pays-off.html (date accessed: October 11, 2023).
34. Telecommunications Industry Association. (2023). ANSI/TIA-942 the global data center standard. Retrieved from: https://tiaonline.org/wp-content/uploads/dlm_uploads/2021/01/TIA-942-Standard_OnePager-230615.pdf (date accessed: October 18, 2023).
35. Said, I. (2023). Improving the performance of loan risk prediction based on machine learning via applying deep neural networks. European Journal of Electrical Engineering and Computer Science, 7(1), 31–37. https://doi.org/10.24018/ejece.2023.7.1.475.

Citation: Suvorov Serhii, "Models for Ensuring the Continuity and Resilience of Telecommunication Services for Banking and Financial Organizations with a Geographically Distributed Structure", Universal Library of Business and Economics, 2023; 33-40. DOI: https://doi.org/10.70315/uloap.ulbec.2023.004.

Copyright: © 2023 The Author(s). This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.