INTERNATIONAL SEVEN JOURNAL
OF MULTIDISCIPLINARY
ISSN: 2764-9547

Risk management in utility systems: audits, compliance, and business continuity from a bcp and international audit perspective

https://doi.org/10.56238/isevmjv2n6-024

Receipt of originals: 11/19/2023 **Acceptance for publication:** 12/19/2023

Leandro Mendes Machado

ABSTRACT

Utility systems are critical to the functioning of modern society, making their risk management essential to ensure safety, regulatory compliance, and service continuity. This article explores how audits, compliance, and business continuity planning (BCP) interrelate within utility environments, drawing on practical experience in implementing BCP and responding to international audits. Through an analysis of common challenges, best practices, and academic literature, the paper highlights the need for integrated governance, effective documentation, scenario-based testing, and strategic alignment with international standards such as ISO 22301 and ISO 31000. It emphasizes that resilience in utility systems depends not only on regulatory compliance but on organizational maturity and the institutionalization of continuity as a core value.

Keywords: Risk Management. Utilities. Compliance. Business Continuity. ISO 22301. Audits. Critical Infrastructure. Resilience. Governance. BCP.

1 INTRODUCTION

Utility systems—comprising electricity, water, gas, and telecommunications infrastructure—are fundamental components of critical national infrastructure. Their uninterrupted operation is vital for societal stability, economic continuity, and public health. Given their centrality, these systems are exposed to a broad spectrum of risks, including natural hazards, technological failures, cyber threats, supply chain interruptions, and regulatory non-compliance. Effective risk management in this context requires a triad approach: robust audit practices, comprehensive compliance systems, and well-structured business continuity planning (BCP). Drawing on firsthand experience in managing BCP and undergoing international audits, this article examines how these elements integrate and where challenges and opportunities emerge.

Audits serve both assurance and improvement functions. Internal and external audits—particularly those aligned with international standards such as ISO 22301 for Business Continuity Management Systems (BCMS), ISO 31000 for risk management, and ISO/IEC 27001 for information security—play a central role in identifying gaps, validating readiness, and ensuring accountability. These audits require clear documentation of risk assessments, business impact analyses (BIA), continuity strategies, roles and responsibilities, and test results. A common audit finding in utility organizations is a disconnect between documented plans and operational practices, particularly when plans are outdated, untested, or unknown to key personnel. Zografopoulos et al. (2021) emphasize that critical infrastructures increasingly face threats stemming from cyber-physical vulnerabilities, necessitating a risk assessment framework that includes both digital and physical dimensions of utility systems.

Compliance extends beyond legal adherence to encompass alignment with best practices and evolving regulatory landscapes. Utility operators are often subject to overlapping national, regional, and international regulatory frameworks. These may impose obligations related to environmental impact, safety, emissions, reliability metrics, and contingency planning. While compliance can be perceived as a burden, it is most effective when embedded into governance and strategic planning processes. As MacGillivray and Pollard (2008) argue, mature utilities incorporate process benchmarking and compliance monitoring as tools to evaluate and enhance internal risk management capabilities.

Business Continuity Planning (BCP) provides the operational backbone for resilience. It enables utilities to identify critical processes, assess risks, and develop strategies for maintaining or rapidly restoring operations during and after disruptions. This includes not only technological redundancy and backup systems but also staff training, communications protocols, and recovery time objectives. The ISO 22301 standard provides a globally recognized framework for implementing BCMS, reinforcing the importance of continuous improvement, stakeholder engagement, and scenario-based planning. According to recent studies (Dehghani & Shafieezadeh, 2022), integrating stochastic and robust optimization models into continuity planning can significantly enhance preparedness for cascading and compound disruptions.

Drawing from direct experience, several challenges consistently emerge during BCP implementation and international audit engagements. First, documentation inconsistencies frequently hinder audit readiness. Plans may not reflect current organizational structures, technologies, or operational realities. Second, testing is often superficial; realistic simulations or full-scale drills are rare, especially those that integrate cross-functional teams or third-party providers. Third, third-party and supply chain risks are frequently underestimated, despite their criticality in continuity scenarios. Many service-level agreements lack clear continuity clauses, and supplier readiness is seldom verified. Fourth, the convergence of IT and operational technology (OT) environments introduces new vulnerabilities, yet few organizations incorporate cyber scenarios into their BCP drills. Finally, organizational culture can present a barrier: when continuity is perceived as a compliance obligation rather than a strategic priority, engagement and investment tend to be minimal.

Best practices to address these challenges include embedding BCP into enterprise governance structures, with board-level oversight and dedicated risk or continuity committees. Risk assessments and BIAs should be regularly updated and scenario-based, incorporating low-probability, high-impact events such as climate extremes or cyberattacks. Continuity plans should be actively maintained, with roles and responsibilities clearly assigned and understood across all levels of the organization. Regular, meaningful testing—ideally integrated with internal and external audits—can uncover weaknesses that static documentation cannot. Moreover, performance metrics such as Recovery Time Objectives (RTOs), Mean Time to Recovery (MTTR), and

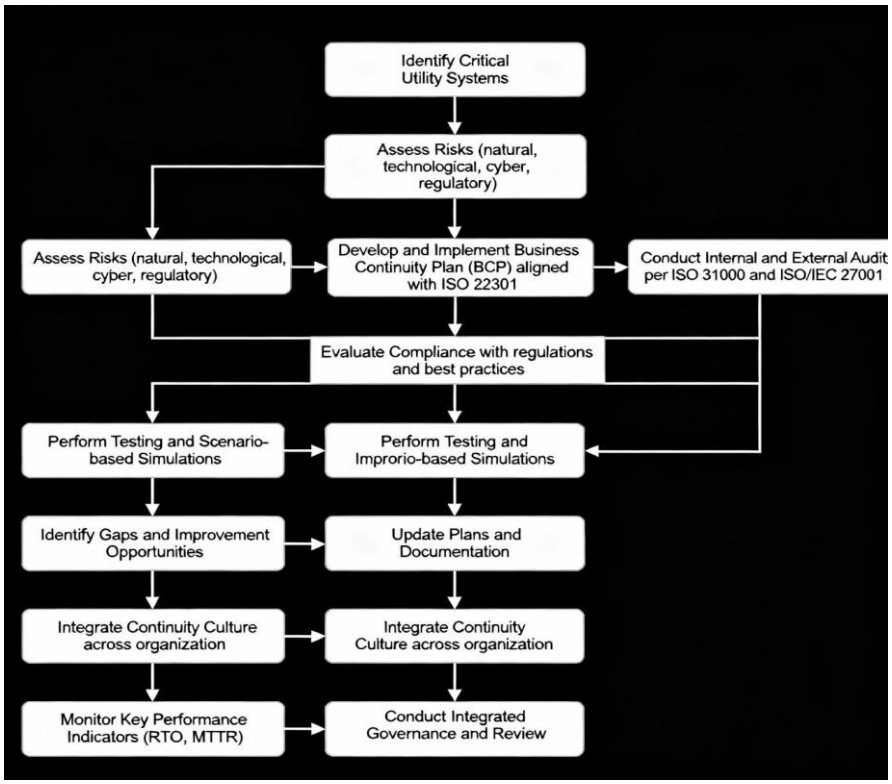
availability percentages should be tracked to evaluate resilience and inform decision-making.

Recent academic contributions further support these strategies. For example, Santos et al. (2023) highlight the importance of applying business continuity management systems to energy-critical entities, particularly in integrating social, economic, and environmental sustainability dimensions. Their study illustrates how utilities that proactively apply international standards and build feedback mechanisms into their continuity planning processes tend to exhibit higher resilience and operational stability. Likewise, research by Knippenberg et al. (2024) shows how integrating community risk perceptions and stakeholder expectations into continuity planning can improve utility decision-making and social license to operate, especially in contexts such as wildfire-prone areas.

The flowchart illustrates the comprehensive risk management process in utility systems, focusing on audits, compliance, and business continuity planning (BCP). It begins with the identification of critical utility systems and proceeds through a thorough risk assessment encompassing natural, technological, cyber, and regulatory risks. The process includes the development and implementation of a BCP aligned with international standards like ISO 22301, followed by internal and external audits in accordance with ISO 31000 and ISO/IEC 27001. Compliance evaluation ensures adherence to regulations and best practices. Scenario-based testing and simulations help identify gaps and areas for improvement, leading to updates in plans and documentation. The flowchart also emphasizes the integration of a continuity culture within the organization, monitoring key performance indicators such as recovery time objectives (RTO) and mean time to recovery (MTTR), and the importance of integrated governance and continuous review to maintain resilience and regulatory adherence in utility operations.

Figure 1

Risk Management Process in Utility Systems: Integration of Audits, Compliance, and Business Continuity Planning (BCP)



Source: Created by author.

In conclusion, effective risk management in utility systems requires more than just regulatory compliance—it demands a culture of resilience, supported by continuous learning, integrated governance, and strategic alignment with international standards. The interplay between audits, compliance, and BCP is not merely procedural but transformational when approached with commitment and rigor. Organizations that prioritize continuity not just to meet audit requirements but as a strategic enabler of trust, reliability, and long-term value are better equipped to navigate the complex and evolving risk landscape facing modern utilities

REFERENCES

Dehghani, N. L., & Shafieezadeh, A. (2022). Multi-stage Resilience Management of Smart Power Distribution Systems: A Stochastic Robust Optimization Model. arXiv preprint arXiv:2205.10459.

Knippenberg, E., et al. (2024). Risk Tolerance, Aversion, and Economics of Energy Utilities in Community Resilience to Wildfires. ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part A: Civil Engineering.

MacGillivray, B. H., & Pollard, S. J. T. (2008). What can water utilities do to improve risk management within their business functions? An improved tool and application of process benchmarking. Environment International, 34(8), 1120–1128.

Santos, D., Mendes, F., & Rosa, M. (2023). Strengthening the Sustainability of Energy Critical Entities Through a Business Continuity Management System. Sustainability, 15(6), 2766.

Zografopoulos, I., Ospina, J., Liu, X., & Konstantinou, C. (2021). Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies. arXiv preprint arXiv:2101.10198.