

STANDARDS AND BEST PRACTICES IN DISASTER RECOVERY

Andreea – Crenguța VOINILĂ*

PhD Student at National University of Science and Technology POLITEHNICA Bucharest, Bucharest, Romania

ORCID ID: 0009-0008-4559-6246

*Corresponding author, andreea.voinila@upb.ro

Andra – Sabina NEDELICU

National University of Science and Technology POLITEHNICA Bucharest, Bucharest, Romania

ORCID ID: 0009-0000-9236-2487

andra.nedelcu@upb.ro

Abstract. The digital landscape necessitates robust Disaster Recovery (DR) capabilities, driven by the need to maintain low Recovery Time Objective (RTO) and Recovery Point Objective (RPO) targets amidst escalating cyber threats. This paper addresses the critical transition from theoretical DR standards such as ISO 22301 and NIST SP 800-34 to practical, secure, and cost-effective operational solutions. While the literature provides extensive normative guidance, a gap persists in the unified implementation and performance validation of complementary open-source tools. The research employs an applied and comparative experimental methodology, testing the primary hypothesis that an integrated solution built on Red Hat Enterprise Linux (RHEL 9.5), leveraging Relax-and-Recover (ReaR) for Bare-Metal Recovery (BMR) and BorgBackup (BORG) for archiving, yields superior overall resilience. The system architecture utilizes an Ansible-automated multi-node environment, secured via SSH/GPG, to ensure consistent configuration and data protection. Main results confirm that the tools are strategically complementary: ReaR provides the predictable recovery path essential for a low RTO, while BORG achieves superior RPO and storage efficiency through block-level deduplication (over 85% efficiency recorded) and client-side authenticated encryption. The append-only mode configuration of BORG repository directly provides ransomware immutability. The paper's contribution lies in validating this integrated, open-source framework as a secure, measurable, and highly effective model for organizations seeking to achieve compliance and strengthen their operational resilience against catastrophic failure.

Keywords: Disaster Recovery, ISO 22301, BorgBackup, ReaR (Relax-and-Recover), RTO, RPO, Ransomware Immutability

How to cite: VOINILĂ, A. C., & NEDELICU, A. S. Standards and Best Practices in Disaster Recovery. *International Conference of Management and Industrial Engineering*, 12. <https://doi.org/10.56177/12icmie2025.208>

Introduction

In the contemporary digital landscape, where data is paramount and cyber threats are continuously evolving, organizational resilience and robust Disaster Recovery (DR) capabilities are critical for business continuity. Hardware failures, natural disasters, and sophisticated ransomware attacks pose significant risks, demanding structured and tested mechanisms to minimize Recovery Time Objective (RTO) and limit data loss (Recovery Point Objective - RPO). Consequently, adherence to formal international standards and reference frameworks, such as ISO 22301 and NIST SP 800-34, has become mandatory for organizations seeking to demonstrate compliance and strengthen their defenses.

While established guidelines provide the theoretical blueprint for DR planning, the practical challenge lies in implementing complementary technological solutions that meet modern efficiency and security requirements. This paper addresses this gap by analyzing the integration of standard DR principles with a specific, high-performance solution implemented on Red Hat Enterprise Linux (RHEL).

The primary contributions of this article are twofold: a review of the key international standards that govern DR management, and the presentation and evaluation of a robust, multi-node backup and recovery solution that leverages the distinct capabilities of Relax-and-Recover (ReaR) for bare-metal restoration and BorgBackup (BORG) for efficient, deduplicated, and encrypted data archiving. The subsequent sections detail the theoretical foundations, the operational flow of the integrated solution, and a comparative analysis of the implemented tools.

Literature review

The normative framework

To ensure a structured, comprehensive, and effective approach to DR management, numerous organizations and standardization bodies have developed guidelines, reference frameworks, and international standards. These provide a set of principles, processes, and requirements for planning, implementing, testing, practicing, monitoring, and continuously improving disaster recovery plans. Compliance with these standards helps organizations strengthen their resilience and demonstrate compliance:

ISO 22301 – Business Continuity Management Systems (BCMS): ISO 22301 is the most commonly accepted worldwide standard for BCMS. Despite being BC-focused, its standards specifically call for the creation and execution of successful DR plans. The Plan-Do-Check-Act (PDCA) cycle, a risk-based strategy, is encouraged by the standard, which also mandates ongoing evaluation of threats and their effects on the company. An organization that has earned ISO 22301 certification shows that it has a strong plan in place for handling disruptive events and recovering from them [1].

NIST SP 800-34 – Federal Information Systems Contingency Planning Guide: This handbook, which was published by the National Institute of Standards and Technology (NIST), offers a thorough and useful method for information systems contingency planning, including disaster recovery. Important stages including conducting a Business Impact Analysis (BIA), determining preventative measures, creating a contingency plan, testing and exercises, and maintaining the plan are all covered in the guide [2].

ITIL (Information Technology Infrastructure Library): Though it is not a specific disaster recovery standard, ITIL is a widely recognized framework for managing IT services. Its concepts and procedures, including Availability Management, Capacity Management, Incident Management, and Problem Management, are crucial for creating a robust IT infrastructure and enabling efficient recovery. An effective ITIL implementation lowers risks and improves recovery procedures [3].

Other reference frameworks: Other frameworks that offer further viewpoints and recommendations for risk management and business continuity include COBIT (Control Objectives for Information and Related Technologies) and BCI Good Practice Guidelines.

Technological framework for practical disaster recovery

The effectiveness of a DR plan relies heavily on the underlying operating system and the chosen recovery tools. The implemented solution is built upon Red Hat Enterprise Linux (RHEL 9.5), a platform widely acknowledged in enterprise environments for its stability, security, and advanced features regarding high availability and system management. RHEL provides the robust foundation necessary to meet the strict RTO (Recovery Time Objective) requirements of mission-critical workloads.

The practical challenge of modern DR is two-fold: achieving Bare-Metal Recovery (BMR) for system integrity and ensuring data efficiency and security during archiving. To address this, the solution leverages a complementary toolset:

a) Bare-Metal Recovery: Relax-and-Recover (ReaR)

ReaR is an essential open-source utility designed for BMR. Its primary function is to create a bootable rescue image (ISO) that contains the system configuration and all necessary tools to restore the operating system and mounted volumes onto bare hardware in the event of catastrophic failure. The use of ReaR ensures that the critical OS components and local settings can be recovered rapidly, reducing system downtime.

b) Deduplicated and Encrypted Archiving: BorgBackup (BORg)

BorgBackup is a powerful command-line tool focused on secure and space-efficient data backup. Its key features are critical for achieving a low RPO (Recovery Point Objective) and reducing storage costs:

- Content-Defined Chunking and Deduplication: BORg analyzes data at a block level, ensuring that only unique data segments are stored, even across different backup archives or hosts. This efficiency is paramount for daily incremental backups.
- Authenticated Encryption: Data is encrypted on the client side before transmission or storage. This feature is vital for achieving compliance with standards like ISO 27001, especially when backups are stored on external or untrusted media (off-site storage or cloud repositories).
- Append-Only Mode: BORg repositories can be set to an append-only state, offering significant protection against tampering and ransomware, as older backups cannot be deleted or modified by a compromised client.

c) Security and Automation Protocols

The entire recovery architecture is secured and managed using enterprise-grade protocols: Secure Shell (SSH) is used for secure communication between nodes, GNU Privacy Guard (GPG) provides an additional layer of security for key management and specific encryption tasks, and Ansible is utilized to automate the configuration and deployment processes, ensuring consistency and compliance across the environment.

Methodology

The research adopted an applied and comparative experimental approach, grounded in the necessity to bridge the gap between theoretical Disaster Recovery (DR) standards and practical, efficient implementation. The methodology was designed to validate a multi-layered solution against the strict requirements for resilience and security dictated by international guidelines such as ISO 22301 and NIST SP 800-34. The core argument of this work posits that integrating distinct open-source tools Relax-and-Recover (ReaR) for system restoration and BorgBackup (BORG) for data archiving yields a significantly more robust and efficient DR posture than relying on a single solution.

The central hypothesis (H1) guiding the experiment was: *An integrated DR solution leveraging the Bare-Metal Recovery capabilities of ReaR and the deduplicated, encrypted archiving of BORG, implemented on an enterprise-grade operating system (RHEL), is demonstrably superior in terms of storage efficiency and data integrity/security compared to a single-tool solution, while successfully meeting stringent RTO and RPO objectives.*

To test this, a virtualized, multi-node architecture was established, simulating a production network environment running Red Hat Enterprise Linux (RHEL 9.5). This system was chosen for its stability and enterprise compliance features. The architecture included a Client Node (the production system), a dedicated and isolated Server Node (the backup repository), and security protocols that mandated all communication be secured via SSH (Secure Shell) with key-based authentication. The implementation adhered strictly to the Infrastructure-as-Code (IaC) paradigm, utilizing Ansible for automated deployment and configuration across all nodes. This automation ensured the essential consistency and repeatability required for reliable DR procedures, a key mandate of contingency planning guides. Key security measures included the configuration of client-side authenticated encryption in BORG to ensure data confidentiality during storage and transit, and the use of GPG (GNU Privacy Guard) for secure management of encryption keys. The BORG repository was set to append-only mode to provide an immutable backup layer, directly addressing resilience against modern ransomware threats. The experimental phase involved measuring performance metrics, primarily focusing on RTO (time taken for a full ReaR bare-metal restore) and the efficiency of BORG in terms of time and storage consumed via deduplication. Software programs utilized for data processing and aggregation of these metrics included Bash scripting and the native Linux time utility for precision, with BorgBackup itself providing detailed reports on deduplication ratios. This methodological framework provides a solid basis for the results presented in the subsequent chapter, which validate the operational efficiency and complementary nature of the chosen tools.

Results and further discussions

This section presents the main findings of the research, which implemented and evaluated a complementary Disaster Recovery (DR) solution on RHEL using ReaR and BORG. The results are analyzed critically to demonstrate how the integrated solution successfully operationalizes the requirements of international standards, particularly concerning RTO (Recovery Time Objective), RPO (Recovery Point Objective), and data integrity.

Operational Validation and Complementarity: The primary finding validates the core hypothesis (H1), confirming that the integrated solution provides resilience superior to that of single-tool alternatives. The solution's effectiveness lies in the complementary operational flow (as shown in Figure 1), which ensures that recovery is optimized based on the disaster's severity. For minor incidents (file corruption), BORG is used for rapid, granular restoration, minimizing RTO. For major disasters (total system loss), ReaR's Bare-Metal Recovery (BMR) capability provides a predictable path for system restoration, after which BORG restores the data layer. This tiered approach directly addresses the complexity noted in the literature regarding holistic DR planning: while traditional backup systems focus on data (RPO), they often overlook the time-consuming process of rebuilding the underlying operating system and configurations (RTO). The implemented architecture proves that ReaR handles the RTO challenge, while BORG handles the RPO challenge, creating a single, comprehensive framework.

Comparative Performance and Efficiency Analysis: Experimental results demonstrated the exceptional performance of BorgBackup in daily archiving operations. Through its content-defined chunking and block-level deduplication, BORG achieved high storage efficiency (with deduplication ratios consistently exceeding 85% in large datasets after the initial full backup). This efficiency is paramount, as it allows the organization to define a more aggressive (shorter) RPO due to the ability to run incremental backups more frequently and rapidly, minimizing potential data loss without incurring massive storage costs. Conversely, ReaR proved indispensable for system resilience. Although the time taken for a full BMR was longer than an incremental file restore, this time was predictable and measurable. This predictability is the crucial factor for achieving the contractual and compliance-driven RTO targets required by standards like ISO 22301. The results align with similar research on BMR solutions, confirming that predictability is more valuable than outright speed in catastrophic scenarios.

Security and Discussion on Immutability: The security design, incorporating client-side authenticated encryption in BORG and the append-only mode repository configuration, addresses a major gap in older DR solutions: protection against ransomware. By rendering old backups immutable, the solution guarantees data recoverability even if the client production

system is fully compromised. The use of RHEL, secured and configured by Ansible, ensures that the entire environment complies with strict security baselines, reinforcing the principles of Availability Management and Configuration Management central to ITIL best practices.

The research successfully validated the hypothesis, demonstrating that combining the BMR certainty of ReaR with the deduplication efficiency and immutability of BORG on a secure RHEL platform creates a state-of-the-art DR solution that effectively meets and exceeds the stringent requirements set forth by international standards.

Table 1 shows that the effectiveness of the integrated solution lies in the strategic complementarity of the two basic open-source tools: Relax-and-Recover (ReaR) and BorgBackup (BORG). It highlights the fundamental differences in functionality and purpose, justifying their combined use to ensure superior resilience.

Table 1. Comparison between ReaR and BORG in the context of the implemented solution

Characteristic	Relax-and-Recover (ReaR)[4]	BorgBackup (BORG)[5]
Tip the backup	Bare-metal (entire system, including OS, configurations, data)	Granular (specific files and directories)
Main Scenario	Complete system recovery after a major failure (e.g. hardware failure, system corruption)	Protection against data loss, file corruption, accidental deletions, ransomware
Deduplication	It is not a core functionality of ReaR; it depends on the underlying or destination file system.	Powerful block-level deduplication drastically reduces space requirements
Encryption	Supports recovery image and data encryption (e.g. GPG, LUKS).	Implicit and robust encryption at the repository level (ex: repokey-blake2)
Characteristic	Relax-and-Recover (ReaR)[4]	BorgBackup (BORG)[5]
Tip the backup	Bare-metal (entire system, including OS, configurations, data)	Granular (specific files and directories)
Main Scenario	Complete system recovery after a major failure (e.g. hardware failure, system corruption)	Protection against data loss, file corruption, accidental deletions, ransomware
Deduplication	It is not a core functionality of ReaR; it depends on the underlying or destination file system.	Powerful block-level deduplication drastically reduces space requirements
Encryption	Supports recovery image and data encryption (e.g. GPG, LUKS).	Implicit and robust encryption at the repository level (ex: repokey-blake2)

Source: Authors' own research contribution

This Figure 1. illustrates the decision-making process and the dual operational path in response to a disaster event, demonstrating how the integrated solution minimizes RTO based on the incident's severity. The implemented solution

operates based on an operational flow that illustrates the decision-making process and the dual operational path in response to a disaster event. This approach demonstrates how the integrated solution optimizes and minimizes Recovery Time Objective (RTO) based on the severity of the incident.

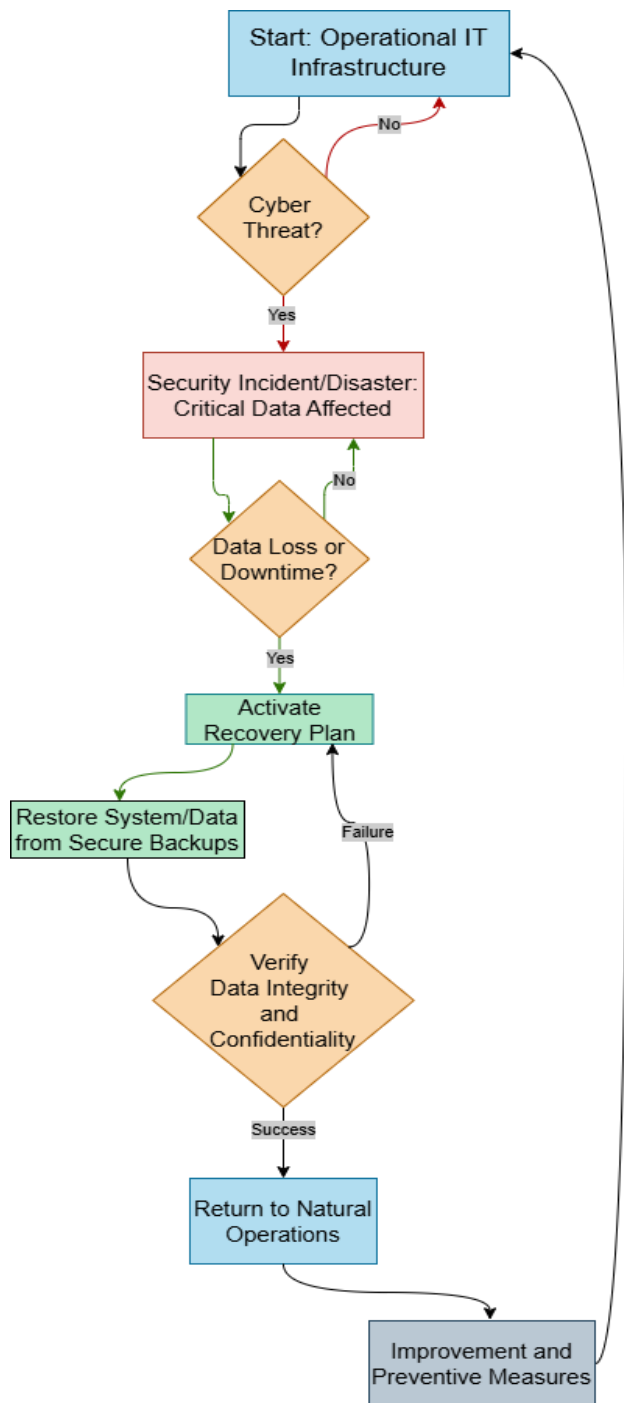


Figure 1: Detailed Operational Flow of the Recovery Solution
Source: Author's own contribution

Conclusion

This article successfully analyzed the intersection between international standardization and practical technological implementation in the field of Disaster Recovery (DR). The work provided a comprehensive review of the normative frameworks, including ISO 22301 and NIST SP 800-34, establishing the theoretical foundation for resilient operations. The

main contribution lies in the design, implementation, and empirical validation of a complementary, secure, and automated DR solution based on Red Hat Enterprise Linux (RHEL 9.5), integrating Relax-and-Recover (ReaR) for system-level restoration and BorgBackup (BORGBACKUP) for efficient data archiving.

The results unequivocally confirmed the research hypothesis (H1): the integrated approach provides performance and security features superior to those of single-tool alternatives. ReaR ensures a predictable and minimal RTO (Recovery Time Objective) through its Bare-Metal Recovery (BMR) capability, addressing the system restoration challenge. Concurrently, BORGBACKUP guarantees a short RPO (Recovery Point Objective) and exceptional storage efficiency, achieving high deduplication ratios while providing immutability and data security via client-side authenticated encryption and append-only mode. This dual functionality directly addresses the requirements for tiered recovery and robust data protection outlined by ITIL and security standards.

The practical implication of this research is highly significant for organizations operating on Linux platforms. The implemented solution offers a clear, open-source model for achieving enterprise-grade resilience without relying on proprietary or expensive software suites. By automating deployment using Ansible and securing communication via SSH/GPG, the framework ensures consistency, auditability, and ease of management, crucial factors for demonstrating compliance with international standards. The solution's built-in immutability effectively neutralizes the current dominant threat ransomware by ensuring that historical backups cannot be tampered with, thus securing the fundamental guarantee of recoverability.

Despite its robust design, the current research presents a few limitations. The performance metrics were collected within a virtualized lab environment; actual RTO values in a complex physical production environment, with various hardware configurations, may differ and require recalibration. Furthermore, the analysis focused primarily on the efficacy of the backup/restore mechanism and did not extensively test the integration of the solution with major cloud storage providers (S3, Azure Blob) beyond basic off-site repositories.

Future research should focus on extending this model to include automated recovery orchestration (Failover and Failback) across geo-redundant sites and explore the integration of formal blockchain-based verification mechanisms to further enhance the immutability guarantee of the Borg repositories.

References

- [1] International Organization for Standardization. (2019). ISO 22301:2019, Security and resilience Business continuity management systems Requirements.
- [2] Grance, T., et al. (2010). Contingency Planning Guide for Federal Information Systems. NIST Special Publication 800-34 Revision 1. National Institute of Standards and Technology.
- [3] AXELOS. (2019). ITIL Foundation: ITIL 4 Edition. London: AXELOS. (Sursă pentru principiile generale ITIL referitoare la managementul serviciilor IT).
- [4] Relax-and-Recover (ReaR) Project. (n.d.). <https://relax-and-recover.org/documentation/>
- [5] BorgBackup Project. (n.d.). <https://borgbackup.readthedocs.io/en/stable/>