INTELLECTUAL PROPERTY MANAGEMENT APPLIED FOR SAVING AND SECURING DATABASES IN A KNOWLEDGE-BASED ORGANIZATION

Radu Costin Moisescu[1], Aurel Mihail Țîțu [2,3,4]

Abstract: *The proposed research makes an important contribution to detailing and analyzing the most important processes and mechanisms for saving and securing databases in information systems within an organization whose purpose is the protection of intellectual property. The problem of analyzing the architectures and technologies that can be applied in the field of saving and securing databases in existing information systems is an extremely relevant aspect analyzed and explained in this research. The research contains and presents in detail the recovery strategies that can be adapted and implemented to secure the data in the database of organizations active in the field of intellectual property in case of a disaster. Business continuity planning sets out risk management processes and procedures that aim to prevent critical service outages and restore full functions for the organization as quickly as possible.*

Keywords: *information system, computer system, data architectures, data, data security management and data networks.*

JEL Classification: *O30, O32, C82.*

1. Introduction

Intellectual property (IP) belongs to any original creation of the human intellect, such as artistic, literary, technical, or scientific creation.

[1] Radu Costin MOISESCU, State Office for Inventions and Trademarks, Bucharest, Romania, radu.moisescu@osim.ro

[2] Aurel Mihail ȚÎȚU, Lucian Blaga University of Sibiu, Romania, mihail.titu@ ulbsibiu.ro

[3] Aurel Mihail ȚÎȚU, The Academy of Romanian Scientists, Bucharest, Romania

[4] Aurel Mihail ȚÎȚU, Romanian Association for Alternative Technologies Sibiu, Romania

Intellectual property rights (IPR) refer to the legal rights granted to the inventor or creator to protect his invention or creation for a certain period of time. These legal rights confer an exclusive right on the inventor / creator or its addressee to make full use of his invention / creation for a certain period of time. IPR is a powerful tool to protect the investment, time, money, effort invested by the inventor / creator of an IP, because it gives the inventor / creator an exclusive right for a certain period of time to use his invention / creation. Thus, IPR contributes by promoting healthy competition and encouraging industrial development and economic growth to the economic development of a country. Business continuity is the ability of an organization to maintain essential functions during and after a disaster. Business continuity planning establishes risk management processes and procedures that aim to prevent mission-critical service outages and restore full function to the organization as quickly and smoothly as possible. According to the international standard ISO 22301: 2019, a business continuity plan (also called a business continuity plan) is defined as "documented procedures that guide organizations to respond, recover, resume and restore a predefined level of operations following business interruption (ISO22301:2019, 2019). ISO 22301: 2019 was revised at the end of 2019 to reflect the ongoing changes in the world of business continuity and to bring more value to users. The text has also been improved to provide increased clarity and consistency. Changes to the standard include:

a) The structure of the standard has been revised to make it easier to read and implement, with greater clarification of what is needed;

b) Language and terminology have been simplified to eliminate duplication and to better reflect today's thinking in the business continuity industry;

c) The high-level structure has been simplified to remain in line with all other standards of the ISO management system.

In this context, continuity planning in organizations engaged in intellectual property is in itself a complex activity, because concepts such as uncertainty and risk are not part of the regular education of most

employees of an organization. The organization of continuity management in intellectual property (IP) organizations, which is the environment for the development, exercise, and maintenance of the continuity plan, must have a clear development framework that is in line with organizational simplicity and limited resources, materials, and human resources, which the institution can invest in continuity management. A model of disaster recovery strategy that can be implemented in an IP organization such State Office for Inventions and Trademarks (OSIM) is represented in the figure 1. This strategy includes the three levels of the implementation of a Disaster Recovery Plan (DRP):

a) Establish, define, design, implement the disaster recovery strategy;

b) Test, validate the plan and train the responsible persons;

c) Execute the DRP and adjust the proper changes.

In IP organization, the processes of online filing, examination, publication and granting protection titles are fully computerized. In this context, the information operation systems and communication technology services (ICT) are essentials to ensure the recovery of the basic activities, and business continuity processes after a possible disaster.

The development of a business continuity plan within IP organizations in accordance with ISO 22301:2019 includes four stages (ISO22301:2019, 2019):

A. Carrying out an impact analysis on the business environment to identify time-sensitive or critical functions and processes and the resources that support them.

B. Identification, documentation, and implementation to recover critical functions and operations.

C. Organizing a business continuity team and develop a business continuity plan to manage a business outage.

D. Organizing training sessions for the business continuity team, testing and practice to evaluate both strategies and recovery plan.

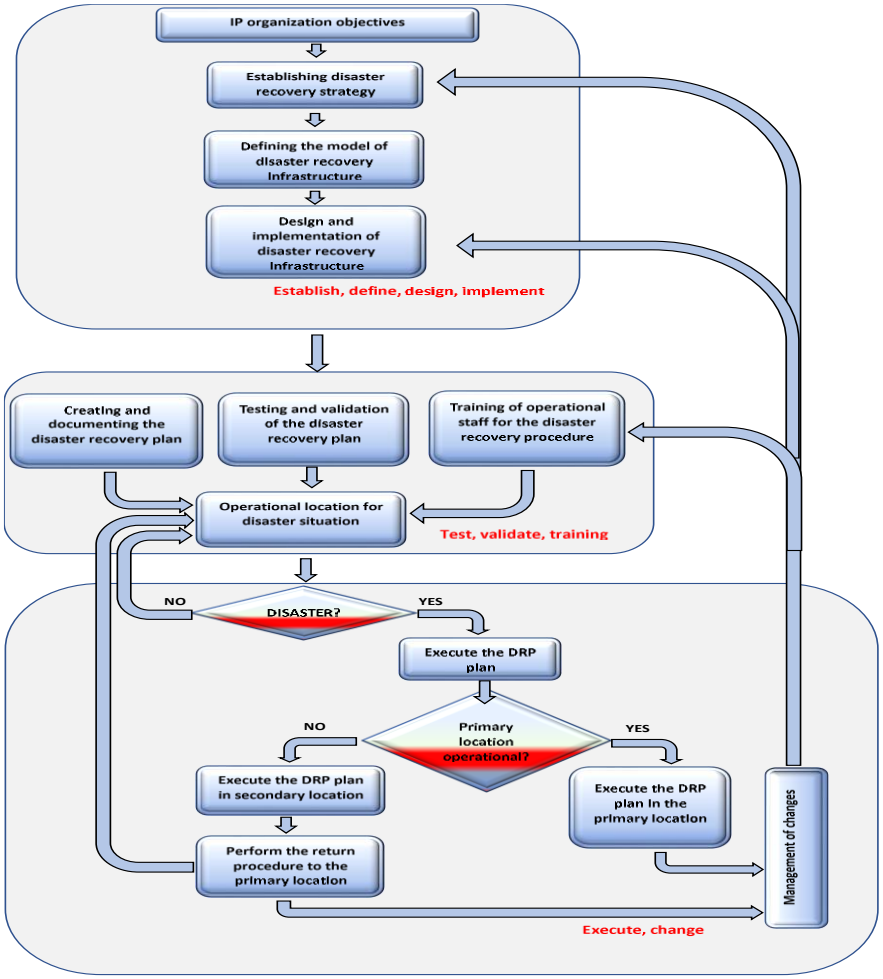

Figure no. 1. Proposal for the implementation of a recovery strategy in OSIM

The Information and Communication Technology Services of an IP organization include both the hardware and software resources but especially the human resources strictly necessary to be able to ensure the continuation of operations after a possible disaster. It is important that the public servants understand the necessity for information security in the digitalization process of public administration. (Banciu, Petre, & Dumitrache, 2019). Therefore, recovery strategies for information

technology should be developed so that the organization's IT infrastructure can be restored in time to ensure the institution's ability to continue its work. In this context, manual solutions should be part of the IT plan so that the organization's operations can continue while the info systems.

Given that more than 90% of the processes carried out in an industrial property organization such as OSIM are computerized, the plan for recovery and continuity of institutional activity must include several steps required to completely restore an IT environment:

a) Organizing the centralized system for saving data and databases belonging to the IP organization;

b) Organizing the necessary IT infrastructures to ensure that the restore process of the data and databases of the IP organization will be completed successfully;

c) Scenarios for the continuation of organizational activities depending on the disaster.

Developing an IT disaster recovery plan in an IP organization begins with building an inventory of hardware (e.g., servers, desktops, laptops, and wireless devices), software applications, and data. The plan should include a strategy to ensure that all information is included and updated.

Software applications specific to the activities of electronic filing of protection applications, examination of these applications, publication and granting of titles, critical information, as well as the hardware necessary for their execution are an important component of this plan. It is recommended to use standardized hardware that will help replicate and reintegrate the hardware into the information system. An important component is ensuring the availability of copies of the software to allow reinstallation on equipment in the secondary location, as well as prioritizing hardware and software restoration. An important step in developing a plan to recover the activity of an IP organization after a possible disaster is the documentation and regulated testing of the plan to ensure that it is up to date and especially functional.

2. Contribution regarding the valuation of the international standard in intellectual property organizations

The elaboration of the continuity plan of the activity in the IP organizations in accordance with ISO 22301:2019 standard, must include the basic operations and processes of the institution:

A. Registration of protection claims;

B. Publication of applications for protection and decisions taken in review processes;

C. Examination of applications for protection;

D. Granting of protection titles in the field of industrial property.

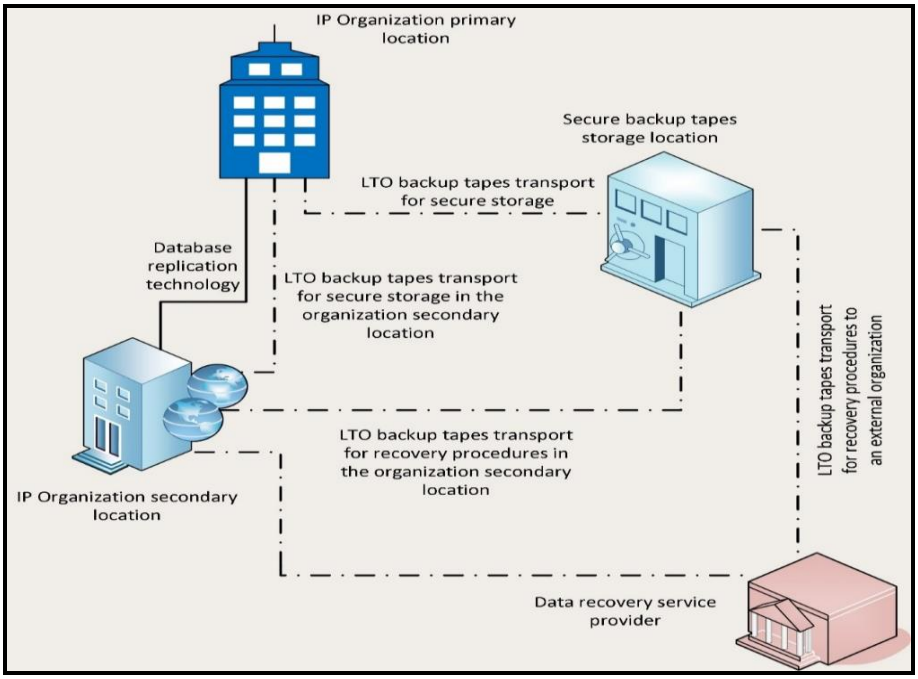

Figure no. 2. The proposed system for ensuring the restoration processes and the business continuity in IP organization after a possible disaster

The minimum framework in which continuity management can be developed at an IP organization, which benefits from legal support in the Code of Internal Managerial Control of Public Entities, mandatory for organizations with intellectual property activity, require:

- a policy on continuity management, promoted by the president of the organization and supported by its directors and the secretary general;
- the declarative and factual personal commitment of the president of the organization towards the actions and processes of continuity management;
- a manager who enjoys credibility and respect to take over the role of continuity manager;
- a budget that can adequately support a reasonable annual program of preparation, testing of technical systems and exercise of the continuity plan and procedures;
- a communication and consultation mechanism, for the promotion in the organization of the discussions on risk and continuity topics;
- introduction of continuity management in the internal audit plan.

The continuity management process must consist of a cyclic set of activities, which at the first iteration results in the preparation of the continuity plan and at subsequent iterations provides data for updating and improving the plan. Basically, due to this cycle of continuous improvement, there is never a final version of the continuity plan; there is only the latest version. Having a purely theoretical strategy, unverified in the real environment, at the time of an incident, an IP organization may face a unique situation, and the way to react to an incident may sometimes be deficient (Lindström, J. & Hägerfors, A., 2009). Thus, there is a major risk that in the event of a major disaster (a flood, fire or earthquake that destroys the building), the organization will lose both the data center and the data that is saved on tape. It is also necessary to make a realistic assessment of the needs of the organization, taking into

account both financial resources, but especially the level of data protection (Singh, 2009). The evaluation will include:

- an analysis on the adoption of a backup and disaster recovery strategy (Infrastructure Audit);
- drafting an effective Disaster Data Backup and Restoration strategy;
- performing tests and verifications of the parameters provided in the process, in real case on various physical or virtual media VMware, Hyper-V, using the existing backup and restoration software;
- implementation of backup, archiving, replication, on-premises or in a secondary location solution (William, 2006). Thus, through a realistic analysis of needs compared to costs and based on a mix of technologies on the market, a plan can be made to minimize risks and ensure the continuity of operations specific to the IP organization after a disaster (Daniel Mellado & Rosado, 2012).

Table no. 1: Scenario I for recovery and business continuity

SCENARIO I		
Replication of data and databases to the secondary location		
The aftermath of the Disaster	**Activity recovery**	**Business continuity**
IP Organization building destroyed	- The information system in the secondary location is functional - Data and databases are replicated	- Online filing, examination, publication and IP tools are functional in the secondary location - The staff of the organization continues its activity at home by connecting remotely to the informational system in the secondary location

SCENARIO I		
Replication of data and databases to the secondary location		
The aftermath of the Disaster	**Activity recovery**	**Business continuity**
IP Organization Datacenter destroyed	- The information system in the secondary location is functional - Data and databases are replicated	- Online filing, examination, publication and IP tools are functional in the secondary location - The staff of the organization continues its activity in the main building connecting remotely to the computer system in the secondary location

The proposed system for ensuring the restoration processes and the continuation of the IP organization's activity after a possible disaster is presented in Figure 2. In most cases, at present, organizations have implemented only one backup system that ensures the saving of data and databases on LTO tapes. In the majority of cases, the backup tapes are stored in the same datacenter or in the same building where the institution's computer system operates (Kepenach, 2007). In order to meet the requirements of the ISO 22301: 2019 standard, we propose two working scenarios regarding the recovery and continuation of the IP organization's operations in case of disaster.

These two scenarios are:

A. Scenario 1 – Data recovery and continuity of activities when the main Data Center of the IT organization of the IP organization is inoperative.

B. Scenario 2 – Data recovery and continuity of activities when the main Data Center of the IT system of the IP organization is inoperative and the replication mechanism between the primary data center and the secondary one is non-functional.

Table no. 2: Scenario II for recovery and business continuity

SCENARIO II		
Transport and storage of backup tapes in the secondary location		
The aftermath of the Disaster	**Activity recovery**	**Business continuity**
IP Organization building destroyed	- The information system in the secondary location is functional. - Applications, data and databases are recoverable by restoring data saved on LTO6 tapes. - Restoration process can be done in the secondary location or at another external provider.	- Applications, data and databases are recoverable by restoring data saved on LTO6 tapes. - The restoration is performed in the secondary location or at another external provider. - The staff of the organization continues its activity at home by connecting remotely to the computer system in the secondary location
IP Organization Datacenter destroyed	- The information system in the secondary location is functional. - Applications, data and databases are recoverable by restoring data saved on LTO6 tapes. - Restoration can be done in the secondary location or at another external provider.	- Applications, data and databases are recoverable by restoring data saved on LTO6 tapes. - The restoration is performed in the secondary location or at another provider of such services. - The staff of the organization continues its activity in the primary building connecting remotely to the information system in the secondary location.

In this context, the organization must define work scenarios that can be analyzed, tested in the first phase and subsequently applied in case of disasters. The 2 working scenarios we propose for analysis, regarding the recovery and continuation of the IP organization's operations in case of disaster, are presented in tables 1 and 2 (Järveläinen, 2012).

In table 1 are presented the stages of recovery of the institution's activity, the scenario in which the data center or even the entire building of the

organization is inoperative. In this context, the activation of the secondary location where both the main elements of the hardware infrastructure and the data, basic applications and databases are replicated becomes the essential objective for the continuation of the organization's activity. In the second table, the continuation of the institution's activity is based on the possibility of restoring data and databases by restoring them from the backup tapes (Zambon, Bolzoni, & Etalle, 2007). This restoration process can be performed in the secondary location or to an external provider of such services.

In this context, the baseline scenario for substantiating a recovery and continuity plan, proposes the implementation of a system for remote replication of data and databases in a secondary location located at least 50 km from the main building of the IP organization.

Replication and management of this data will be done through a dedicated and secure data network exclusively for these operations. One of the systems for remote replication of Informix databases that can be implemented in intellectual property organizations is asynchronous replication (IBMi v.7.1). In this context, this mechanism uses asynchronous data replication to update databases that are in the secondary location after a change has been made to the database in the primary location. Compared to synchronous replication mechanisms when Informix-type databases are replicated as soon as changes are made to the main location, asynchronous ones are preferred because they work even in the presence of temporary system or network errors (Abawajy & Mustafa , 2014).

With asynchronous replication, the delay in updating databases in the primary location may vary depending on the requirements of the applications used in the organization or the configuration set by Informix database administrators. However, the data eventually synchronizes with the same value in all secondary locations. The major advantage of this type of data replication is that if a particular database server is down, the replication process can continue and all transactions in the replication system will be enabled (Dey, 2011).

Additionally, as shown in Figure 2, we propose that the transport, management and safe storage of LTO6 backup tapes be performed by an external provider specializing in such services, in a rented space or owned by the IP organization (Snedaker, 2013).

3. Management processes and mechanisms for saving and securing databases applicable in IP organization

According to ISO 22301: 2019 and ISO 27001:2017 standards, in the database administration processes in IP organizations, the backup and restore of data is of particular importance (ISO 27001:2017, 2017). The mechanisms for saving databases that can be implemented in the IT systems of IP organizations must be adapted to the infrastructure of the IT system, the structure of these databases, as well as the level of training of human resources that manages these systems (Toigo, 2012). In this context, we summarize in the presentation of a mechanism for saving Informix databases that can be deployed in IP organizations using HP Data Protector technology as a backup medium. We propose for analysis a backup solution for data and databases using the HPE Data Protector platform, which can be implemented in an IP organization. In this regard, the organization must implement a centralized backup platform for all IT systems from the physical and virtual card to institutions, as well as advanced integrations with equipment such as Storage Area Network (SAN) with technologies developed by DellEMC (Dell Unity or DellEMC DataDomain).

3.1 The backup mechanism on LTO6 tapes and discs

The mechanism for saving data and databases shown in Figure 3 ensures the transfer of information from both the DMZ area and the LAN area to the two backup image storage units analyzed: one LTO6 dual tape drive library (i.e., Overland Neo 2000e type) and the disk drive unit (Data Domain). These backup streams are represented in Figure 3 by 2 continuous lines.

The green line shows one of the backup data streams that will be made through the backup server to the Overland Neo 2000e LTO6 tape

library. This data stream connects via 16Gbps capacity fiber optic network (FO) network the organization's SAN system where the databases of the LTO6 Overland Neo 2000e tape library will be stored.

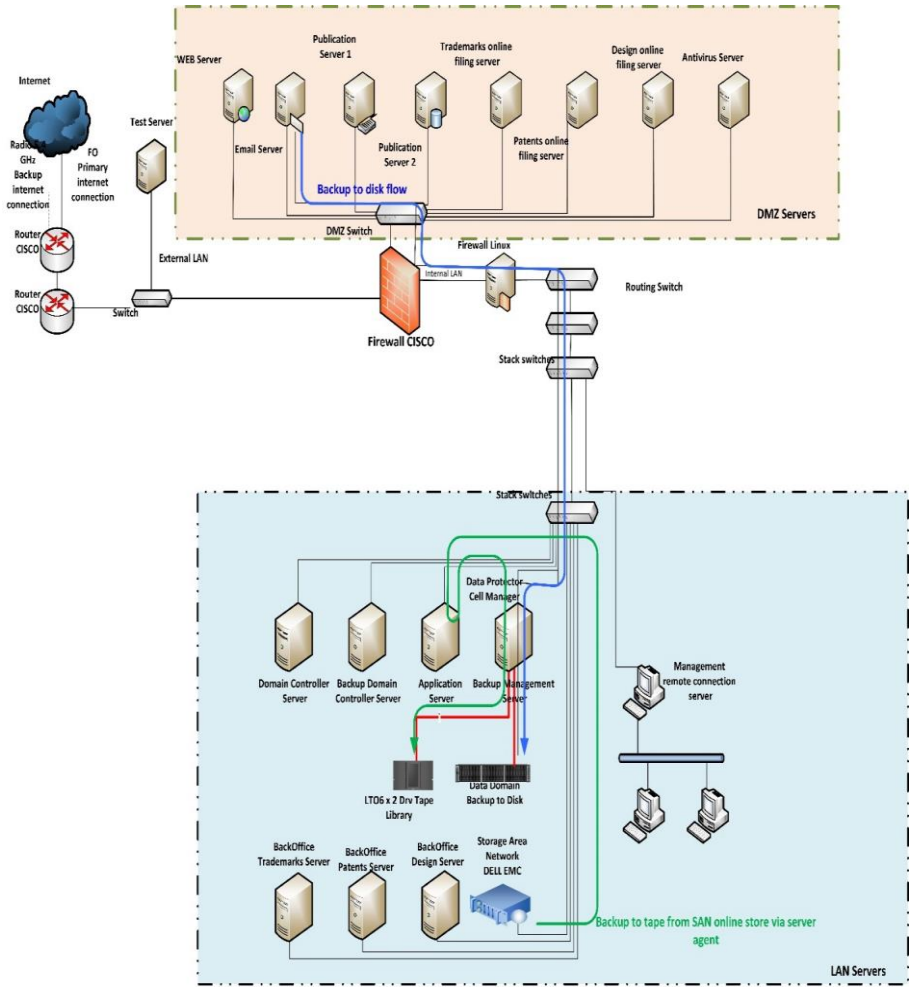

Figure no. 3. Mechanism for saving data and databases through SAN

The blue line shows the second backup data stream to be made through the backup server to the Data Domain disk drive unit. In this drive are

configured disk spaces, licensed, for use in the application, within the TB limit useful before the compression and deduplication processes, on the Data Domain drive which will be configured as a Data Domain Boost destination. The management of the backup sessions is performed by HPE Data Protector application responsible for installation and integration of agents for operating systems and organization-specific applications. Also, the management of LTO6 tape backup media is performed also at the application level, in both cases: those in the library and those that will be removed during the off-line transport and storage procedures in a location outside the library (Banciu, Rădoi, & Belloiu, Information Security Awareness in Romanian Public Administration: An Exploratory Case Study, 2020). Several types of agents, depending on the integration mode, will be installed by Data Protector on client systems. Agents are modular and only the modules needed for integration are installed (Zheng & Wang, 2010).

Figure 3 details a scheme of backup flows that are proposed to be implemented in the IP organization to save data and databases in the 2 different areas: the demilitarized zone (DMZ) where databases are developed for online deposits, online applications for patents, trademarks and industrial designs and the local area network (LAN) where the requests for protection titles are processed, examined, published and granted (Microfocus). The Cell Manager server has all application agents installed by default in order to be able to push them through clients.

The Disk Agent component is installed on any regular client system, through which the client is registered in the Cell Manager and appears in the client list in the backup management server. The Media Agent component is installed only on systems with SAN connectivity or that for architectural reasons must send data directly to storage targets (Singh, 2009).

The Media Agent server is configured with paths for backup clients that have SAN-attached disks and paths to the MSL LTO6 library (Hersyah, A Literature Review on Business Continuity Based on ISO 22301, 2018).

For Hyper-V systems, the Media Agent will be installed on each host server and will be used for LAN backup of the virtual machines on that host. For virtual machine application servers, the specific Informix application agent will be additionally installed.

3.2 Management of backup sessions

The presented LTO6 tape backup system is an integral part of a continuity plan model that can be implemented in an IP organization such as OSIM. The backup system can be configured to provide a weekly, monthly and annual backup of a copy of the data and databases on tape in order to be transported and stored in a secondary backup location at a distance of min. 50km from headquarters.

This backup model is of the "full" type, meaning that the entire database is saved. As previously mentioned, the data stream represented in Figure 3 by the blue line shows one of the backup data streams that will be made through the backup server to the Data Domain disk backup system. This data stream connects through the 16Gbps fiber optic network (FO) network the organization's SAN system where the databases will be stored by the Data Domain disk backup system (Elerath & Pecht, 2007) . To achieve a higher access speed (up to 100 times faster than classic disks) the backup to disks system is equipment with SSD (Solid State Disks) and SAS (Serial Attached SCSI – SCSI Stands for Small Computer System Interface) technology disks (Bhattacharya, 2002).

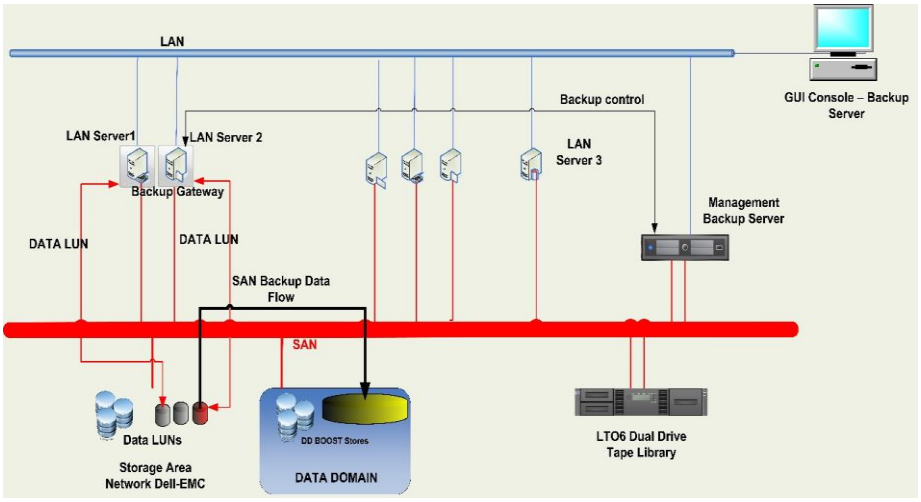

Figure no. 4. Backup mechanism of data and databases in the Storage Area Network and LTO6 dual tape drive library

The data backup solution that is proposed to be implemented through the IP organization continuity plan will be used to save the existing virtual environment, as well as specific file system information and integrations with the Informix type database (Figure 4).

In this way, for any additional backup sessions that will be integrated later, it is necessary to extend also the backup licensing system. Backup operations will be scheduled to run automatically, but it is highly recommended to be periodically checked by a backup administrator for proper and error-free execution and also for applying any remedial action if necessary. In order to ensure the continuation of the basic activities of the institutions in case of disasters, the backup policy that can be implemented within the IP organization also considers the possibility of rapid recovery through recent data restoration processes and medium-term archiving (one year) of operational data. In order to be able to restore or use historical data in case of error discoveries or various investigations, the proposed backup system will perform a daily backup of data changes and databases (Monday to Friday) also called incremental backup, by comparing their changes with the previous day.

Conclusions

This document makes, in its own vision, an analysis of the need to use, implement, and enhance the ISO 22301: 2019 standard in an IP organization. In the current epidemiological context, the concepts of "Business Continuity (BC)" or "Business Continuity Plan (BCP)" are becoming a reality and are not a recent invention. Planning the continuity of an organization's operations is part of the normal practice of any business that enjoys efficient management. Acts of terrorism, outbreaks of severe acute respiratory syndrome (SARS) or various natural disasters have highlighted the importance of a strategy for the continuity of the activities of any organization. Through such a plan, organizations prepare for a number of possible actions and risks that may adversely affect their work.

In the modern era, the information environment of an IP organization can be protected from the impact of disasters by using data duplication technologies, replicating them in different physical locations or by saving them on various encrypted media. Thus, the informational environment of an IP organization can be completely separated from the physical environment, which has the advantage of substantially increasing the availability of services offered to the public in the situation of a disaster. It is therefore necessary for IP organizations to prepare the DRP plan which should include:

- Analysis of the need to recover IP organization operations in disaster situations;
- Analysis of the impact on the organization's operations in disaster situations;
- Analysis of the needs of the organization;
- Preparation and testing of operational scenarios for disaster situations;
- Implementation of the analyzed solutions, testing and permanent updating of the operational scenarios;
- Permanent preparation and training of the human resource involved in the management of disaster situations of the IP organization.

Organizations generate large amounts of data, and data files change throughout the workday. Data can be lost, corrupted, compromised or stolen through hardware failure, human error, hacking and malware. Loss or corruption of data due to a disaster could lead to significant disruptions to the operations of an IP organization. Thus, the backup and restore of data are essential elements of the business continuity plan and the disaster recovery plan. But, no business continuity plan for an IP organization is complete or not working properly for the first time. In this context, developing the right attitude towards continuity at all levels is one of the important points of creating and implementing a BCP (Business Continuity Plan). Any plan must be reviewed, tested, and updated regularly, so there is an opportunity that the processes which did

not work on the first test can be corrected. The development of a data backup strategy begins with identifying the data to be saved, selecting, and implementing hardware and software backup procedures, scheduling, and performing backup sessions, and periodically validating this restored data in test environments. It is also important to correctly and completely identify the data in the organization along with other records and information stored on paper. The continuity plan must include regularly scheduled backup copies. Making backup copies of vital records can be done by scanning paper records in digital formats and allowing them to be copied with other digital data. In this regard, an analysis of the impact on the IP organization's operations must assess the potential for lost data and define the "recovery point objective", with data recovery times being confirmed and compared with the organization's information systems recovery time objectives.

References

Elerath, J. G., & Pecht, M. (2007). Enhanced reliability modeling of raid storage systems. *37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*.

Zambon, E., Bolzoni, D., & Etalle, S. (2007). *A Model Supporting Business Continuity Auditing and Planning in Information Systems*. Internet Monitoring and Protection 2007. ICIMP 2007. Second International Conference.

Abawajy, J., & Mustafa , D. (2014). *Data Replication Approach with Consistency Guarantee for Data Grid. IEEE Transactions on Computers, Volume: 63, Issue: 12*.

Banciu, D., Petre, I., & Dumitrache, M. (2019). *Electronic system for assessing and analysing digital competences in the context of Knowledge Society*,.

Banciu, D., Rădoi, M., & Belloiu, S. (2020). Information Security Awareness in Romanian Public Administration: An Exploratory Case Study.

Banciu, D., Rădoi, M., & Belloiu, S. (2020). Information Security Awareness in Romanian Public Administration: An Exploratory Case Study. *Studies in Informatics and Control, 29(1) 121-129, March 2020*.

Bhattacharya, S. (2002). *Coordinating backup/recovery and data consistency between database and file systems*. ACM 2002.

Daniel Mellado, D., & Rosado, D. G. (2012). An overview of current information systems security challenges and innovations. *ECCWS2014-Proceedings of the 13th European Conference on Cyber warefare*.

Dey, M. (2011). *Business Continuity Planning (BCP) methodology — Essential for every business*. 2011 IEEE GCC Conference and Exhibition (GCC).

Hersyah, M. H. (2018). *A Literature Review on Business Continuity Based on ISO 22301*. International Conference on Information Technology Systems and Innovation (ICITSI).

IBMi v.7.1. (n.d.). *Planul de recuperare din dezastru*. https://www.ibm.com/docs/ro/i/7.1?topic=recovery-disaster-plan.

ISO 27001:2017. (2017). *ISO/IEC 27001 International Information Security Standard published*. International Organization for Standardization.

ISO22301:2019, I. (2019). *Societal security — Business continuity management systems — Requirements*. ISO/TC 292.

Järveläinen, J. (2012). *Information security and business continuity management in interorganizational IT relationships*. Business, Computer Science.

Kepenach, R. J. (2007). Business Continuity Plan Design. *Second International Conference on Internet Monitoring and Protection (ICIMP 2007)*.

Lindström, J. & Hägerfors, A. (2009). *A model for explaining strategic IT- and information security to senior management*. International Journal of Public Information.

Microfocus. (n.d.). Data Sheet – Data Protector Information Management and Gouvernance. *www.microfocus.com*, p. 2020.

Singh, S. K. (2009). *Database management system concept Enterprises*. Pearson Education.

Snedaker, S. (2013). *Business Continuity and Disaster Recovery Planning for IT Professionals*. Syngress Media,U.S.

Toigo, J. (2012). *Disaster Recovery Planning*. Pearson Education (US).

William, C. R. (2006). *Business Continuity Planning for Disasters is Just Good Planning*. MILCOM 2006 – 2006 IEEE Military Communications conference.

Zheng, Z., & Wang, Y. (2010). *The Advanced Data Recovery Technology Based on the Log Recovery*. International Conference on Internet Technology and Applications.