Review of ISO 9001:2015 and ISO 27001:2013 Implementation in Financial Institution – Case Study

Ajla Cerimagic Hasibovic*, Anel Tanovic**
* Faculty of Electrical Engineering, University of Sarajevo, Sarajevo, Bosnia and Herzegovina
acerimagic@etf.unsa.ba
** Faculty of Electrical Engineering, University of Sarajevo, Sarajevo, Bosnia and Herzegovina
atanovic@etf.unsa.ba

***Abstract* – In today's technologically-driven world, protecting ICTs (Information and Communication Technologies) is of great importance. Due to the amount of personal data and the obligations of high transaction accuracy, financial institutions such as banks and insurance companies are even more sensitive to data protection. On the business side, ICT is fundamental for day-to-day operations, so investing in ICT is investing in business continuity, operating and resilience. Integration of ISO 27001:2013 and ISO 9001:2015 standards into an organization's Information Security Management System (ISMS) and Quality Management System (QMS), respectively, further enhances the importance of protecting ICT. It is also important for organizations to implement these standards as a useful baseline for further compliances, such as for example GDPR (General Data Protection Regulation). These standards provide a framework for continually improving management systems in critical areas, which is just one more reason for implementation.**

Keywords – Audit, ISO 9001:2015, ISO 27001:2013, Information Security Management Systems

I. INTRODUCTION

The common tool to perform data security risk assessment is ISO 27001, the international standard for an information security management system [1]. It emphasizes a risk-based approach to information security. The standard analyzes information security from the following 12 levels: 1. Security of organizational information; 2. Security of human resources; 3. Asset management; 4. Logical security; 5. Cryptography; 6. Security of operations; 7. Security of communications; 8. Security of development environments; 9. Security in the management of suppliers; 10. Safety from the aspect of occurrence and resolution of incidents; 11. Business continuity; 12. Compliance with legal regulations. It requires organizations to identify, assess, and manage information security risks systematically. This is particularly relevant to ICT, where the evolving threat landscape requires proactive measures to identify and mitigate potential vulnerabilities [2]. ISO 27001 helps organizations ensure compliance with legal and regulatory requirements related to information security. This is crucial for protecting sensitive data stored and processed through ICT systems.

ISO 9001:2015 is the base for Quality Management System (QMS) implementation. Companies implement quality procedures and devise policies aiming to increase customer satisfaction and ensure the consistency of their practices. In the ICT sector, where organizations often rely on complex supply chains, ISO 9001 can help manage quality across the supply chain [3]. Both ISO 27001 and ISO 9001 encourage process-oriented thinking. Integrating the QMS and ISMS ensures that processes related to information security and quality management are aligned, and they simplify and improve business processes.

This paper provides GAP analyzis of an existing organization and potential recommendation for any further ISO 9001:2015 and ISO 27001:2013 implementations. The complete research has been done in Lovcen Bank ad Podgorica, which is 6th bank by size in Montenegro according to the report of Central Bank of Montenegro. During the research, authors had access to all business and IT systems together with a relevant literature. The duration of research was 120 working days. This paper coud be used as base for furher cases in banks and insurance companies.

First chapter of this paper explains standards and motivation for writing this paper. Section II is for ISO9001:2015 GAP analysis. In Section III we provide GAP analysis for ISO 27001:2013. Discussion is presented in Section IV. Section V is for conclusion and future analysis.

II. GAP ANALYSIS FOR ISO 9001:2015

This analysis helped identify areas where existing organization met the standard's criteria and areas where there are gaps that needed to be addressed for compliance.

TABLE I. GAP ANALYSIS FOR ISO 9001:2015

Standard requirement (ISO 9001:2015) - QMS	ISO 9001: 2015 clauses	Implemented YES/NO
Understanding organization and it's context	4.1	Yes. Defined through strategic planning
Understanding the needs and expectations of interested parties	4.2	Yes. Defined through strategic planning
Determining the scope of the quality management system	4.3	Yes. Organization has clearly defined the scope for the implementation of the QMS
Quality management system and its processes	4.4	No. There is no process scheme, no management processes scheme, no business process management tool. Recommended
Leadership and Commitment	5.1	Yes. Decission management
General	5.1.1	Yes. Decission management
Customer focus	5.1.2	Yes. Decission management
Policy	5.2	Mandatory to implement in accordance with the requirements of the ISO 9001 standard
Establish the quality policy	5.2.1	Mandatory to implement in accordance with the requirements of the ISO 9001 standard
Communicating the Quality Policy	5.2.2	Mandatory to implement in accordance with the requirements of the ISO 9001 standard
Organizational roles, responsibilities, and authorities	5.3	Company's organization scheme
Actions to address risks and opportunities	6.1	Mandatory to implement in accordance with the requirements of the ISO 9001 standard
Quality objectives and planning to achieve them	6.2	Mandatory to implement in accordance with the requirements of the ISO 9001 standard
Planning of changes	6.3	Change management procedure
Resources	7.1	Human resources policy
General	7.1.1	Human resources policy
People	7.1.2	Human resources policy
Infrastructure	7.1.3	Yes. Existing contract
Monitoring and Measuring Resources	7.1.5	Human resources policy
Competence	7.2	Human resources policy
Awareness	7.3	Human resources policy
Communication	7.4	Ethical codex
Documented information	7.5	No Document Management System. Recommended
General	7.5.1	No Document Management System. Recommended
Creating and updating	7.5.2	No Document Management System. Recommended
Control of Documented Information	7.5.3	No Document Management System. Recommended
Operational planning and control	8.1	Existing policies and procedures
Requirements for products and services	8.2	New product procedure. Project Management
Customer communication	8.2.1	New product procedure. Project Management
Determining the requirements for products and services	8.2.2	Yes. New product procedure. Project Management
Changes to requirements for products and services	8.2.3	New product procedure. Project Management
Design & Development of products & services	8.3	Mandatory to implement in accordance with the requirements of the ISO 9001 standard
General	8.3.1	Mandatory to implement in accordance with the requirements of the ISO 9001 standard
Design & Development planning, inputs, control, outputs	8.3.2, 8.3.3, 8.3.4, 8.3.5	Mandatory to implement in accordance with the requirements of the ISO 9001 standard
Design & Development Changes	8.3.6	Mandatory to implement in accordance with the requirements of the ISO 9001 standard
Control of externally provided processes, products and services	8.4	Supply chain management procedure
General	8.4.1	Supply chain management procedure
Type and Extent of control	8.4.2	Supply chain management procedure
Information for external providers	8.4.3	Supply chain management procedure
Production and service provision	8.5	New product procedure. Project Management
Control of production and service provision	8.5.1	New product procedure. Project Management
Identification and traceability	8.5.2	New product procedure. Project Management
Property belonging to customer or external providers	8.5.3	New product procedure. Project Management
Preservation	8.5.4	New product procedure. Project Management
Post-delivery activities	8.5.5	New product procedure. Project Management
Control of changes	8.5.6	Change management
Release of products and services	8.6	No. Qualitative tests defined in A.14. in ISO 27001:2013
Control of Nonconforming Outputs	8.7	Mandatory to implement in accordance with the requirements of the ISO 9001 standard
Monitoring, measurement, analysis and evaluation	9.1	Mandatory to implement in accordance with the requirements of the ISO 9001 standard
General	9.1.1	Procedure for managing client objections
Evaluation of Compliance	9.1.2	Procedure for managing client objections
Analysis and Evaluation	9.1.3	Mandatory to implement in accordance with the requirements of the ISO 9001 standard
Internal audit	9.2	Mandatory to implement in accordance with the requirements of the ISO 9001 standard
Management review	9.3	Mandatory to implement in accordance with the requirements of the ISO 9001 standard
General	9.3.1	Mandatory to implement in accordance with the requirements of the ISO 9001 standard
Management review inputs	9.3.2	Mandatory to implement in accordance with the requirements of the ISO 9001 standard
Management Review Outputs	9.3.3	Mandatory to implement in accordance with the requirements of the ISO 9001 standard
General	10.1	Mandatory to implement in accordance with the requirements of the ISO 9001 standard
Nonconformity and corrective actions	10.2	Mandatory to implement in accordance with the requirements of the ISO 9001 standard
Continual improvement	10.3	Mandatory to implement in accordance with the requirements of the ISO 9001 standard

Statistics for ISO9001:2015 implementation in this company:

- Sucessfully implemented controls (100%): count: 34, success rate: 58,87%
- Partially implemented controls (50%), count: 5
- Unimplemented controls (0%): count 23, success rate: 41,13%.

Total ISO9001:2015 realization rate is 58,87%.

III. GAP ANALYSIS FOR ISO 27001:2013

The table below lists the requirements of the ISO 27001:2013 standard with proof of whether the implementation was successfully implemented in the business environment of the observed company.

TABLE II. GAP ANALYSIS FOR ISO 27001:2013

Standard requirement (ISO27001:2013) - ISMS	**ISO 27001: 2013 clauses**	**Implemented YES/NO**
Has company defined internal and external context for the ISMS system	4.1	Yes. Defined through strategic planning
Has company defined the understanding and expectations of all interested parties for the implementation of the ISMS system	4.2	Yes. Defined through strategic planning
Has company clearly defined the scope for the implementation and application of the ISMS system	4.3	Yes. Company has clearly definde scope for the implementation and application of the ISMS system
Are there clearly defined roles, responsibilities and authorities in teh company from the aspect of implementing the ISMS system	5.3	Organizational chart for IT and Information Security
Has company defined all possible threats to strategic information assets	6.1.2	Procedure for risk management in the information system Procedure for operational risks
Is there a defined and documented best practice for the realization of real Threat Management Systems?	6.1.2	Procedure for risk management in the information system Procedure for operational risks
Has company defined all possible vulnerabilities on strategic information assets	6.1.2	Mandatory to implement in accordance with the requirements of the ISO 27001 standard
Is there a defined and documented best practice for the realization of real Vulnerability Management Systems	6.1.2	Mandatory to implement in accordance with the requirements of the ISO 27001 standard
Has company performed an evaluation of threats to strategic information assets	6.1.2	Mandatory to implement in accordance with the requirements of the ISO 27001 standard
Has company performed a vulnerability evaluation of strategic information assets	6.1.2	Mandatory to implement in accordance with the requirements of the ISO 27001 standard
Has comapny determined risk factors as well as levels for successful resolution of all risks	6.1.2	Mandatory to implement in accordance with the requirements of the ISO 27001 standard
Are the Risk Owners determined?	6.1.2	Mandatory to implement in accordance with the requirements of the ISO 27001 standard
Is there a defined Risk Treatment Plan for risks with indicated: risk management activities, risk owners, level of risk management, time period required for risk management	6.1.3	There is a Register for risk management Report on Risk Assessment
Are the Information Security Objectives defined with indicated activities and metrics for measuring them	6.2	Mandatory to implement in accordance with the requirements of the ISO 27001 standard
Has company defined a procedure for managing documents	7.5.1, 7.5.2, 7.5.3	Document management procedure
Has company defined a procedure for managing data records	7.5.1, 7.5.2, 7.5.3	Document management procedure
Is there a defined metric with clearly displayed KPIs for all points of the standard: A.5 – A.18	9.1	Mandatory to implement in accordance with the requirements of the ISO 27001 standard
Is there a defined methodology for measuring metrics	9.1	
Are there first measured results of the metrics and critical deviations from the desired ones	9.1	Mandatory to implement in accordance with the requirements of the ISO 27001 standard
Is there a defined internal audit procedure with associated forms: order, program, checklists, etc.	9.2	Mandatory to implement in accordance with the requirements of the ISO 27001 standard
Are there any results of an internal audit with a clear internal audit report?	9.2	Mandatory to implement in accordance with the requirements of the ISO 27001 standard
Is there a defined procedure for managing non-conformities together with the associated forms	10.1	Mandatory to implement in accordance with the requirements of the ISO 27001 standard
Is there a defined procedure for the management of corrective measures together with the associated forms	10.1	Mandatory to implement in accordance with the requirements of the ISO 27001 standard
Is there a plan for continuous improvement of the ISMS system after the completion of metric measurements, internal audit and management review	10.2	Mandatory to implement in accordance with the requirements of the ISO 27001 standard
Has the Information Security Policy been defined and officially published?	A.5.1.1	Information security policy
Is the review procedure defined by the administration?	A.5.1.2, 9.3	Mandatory to implement in accordance with the requirements of the ISO 27001 standard
Was the review carried out by the management?	A.5.1.2, 9.3	Mandatory to implement in accordance with the requirements of the ISO 27001 standard
Are security roles defined in the management of the ISMS system with clear obligations to the regulatory authorities in company's country	A.6.1.1, A.6.1.2, A.6.1.3, A.6.1.4	Organizational chart, Workplaces systematization
Is there a defined project management procedure from the aspect of the ISMS system	A.6.1.5	Mandatory to implement in accordance with the requirements of the ISO 27001 standard
Is the Mobile Device Management Policy defined and published?	A.6.2.1	Mandatory to implement in accordance with the requirements of the ISO 27001 standard
Is the Remote Work Policy defined and published?	A.6.2.2	The procedure of remote access to the information system
Are the recruitment criteria defined in the Employment Regulations from the point of view of the ISMS system?	A.7.1.1, A.7.1.2	Code of Business Conduct - Code of Ethics Rulebook on disciplinary procedure Statements on getting to know each other during the employment relationship Disciplinary procedure
Have all employees sign a statement that they are familiar with the Information Security Policy	A.7.2.1	Code of Business Conduct - Code of Ethics Rulebook on disciplinary procedure Statements on getting to know each other during the employment relationship Disciplinary procedure
Is there a defined education management procedure with clearly defined roles and responsibilities for the implementation of education	A.7.2.2	Code of Business Conduct - Code of Ethics Rulebook on disciplinary procedure Statements on getting to know each other during the employment relationship Disciplinary procedure
Are all minor security incidents and serious security incidents listed with all necessary corrective measures in the existing Rulebook on disciplinary responsibility?	A.7.2.3	Code of Business Conduct - Code of Ethics Rulebook on disciplinary procedure Statements on getting to know each other during the employment relationship Disciplinary procedure

Are the employee's obligations after the termination of the employment contract clearly stated?	A.7.3.1	Code of Business Conduct - Code of Ethics Rulebook on disciplinary procedure Statements on getting to know each other during the employment relationship Disciplinary procedure
Has a list been made of all strategic information assets in the company including: servers, routers, switches, computers, network equipment, databases, operating systems, printers, scanners, IP cameras and other security equipment	A.8.1.1	List of IT assets
For the completed list of strategic information assets, has it been determined who are the owners of these assets and have the owners signed the takeover of all assets?	A.8.1.2	List of IT assets
Is there a defined procedure for acceptable use of the property along with acceptable forms	A.8.1.3	List of IT assets
Is there a defined property recovery procedure along with acceptable forms	A.8.1.4	List of IT assets
Has the data been classified? The information needs to be sorted into several basic categories.	A.8.2.1	No Data Classification System – recommended No Data Loss Prevention System – recommended
Whether all classified information has been successfully tagged	A.8.2.2	Data classification procedure
Is there a defined procedure for property management together with the associated forms	A.8.2.3	Data classification procedure
Is there a defined procedure for managing portable media?	A.8.3.1	Procedures criteria and method of deleting data from the medium
Is there a defined procedure for disposing of media together with the associated forms	A.8.3.2	Mandatory to implement in accordance with the requirements of the ISO 27001 standard
Is there a defined procedure for the physical transfer of media together with the associated forms	A.8.3.3	Mandatory to implement in accordance with the requirements of the ISO 27001 standard
Is the policy for access control defined?	A.9.1.1	Information system access procedure
Has a documented best practice been introduced for introducing a Firewall into the intranet and extranet network of the company	A.9.1.2	Yes
Has a procedure for user registration and deregistration and management of their access been introduced?	A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6	Information system access procedure
Has a procedure been introduced to control access to information as well as manage user access together with the associated forms	A.9.4.1, A.9.4.2, A.9.4.3, A.9.4.4, A.9.4.5	Information system access procedure
Is there a documented best practice for performing code analysis in all application solutions	A.9.4.5	Code is outsourced
Has a password management policy been defined?	A.9.4.3	Password Management Policy
Is there a documented best practice for conducting penetration tests on all information systems	A.9.4.2	Mandatory to implement in accordance with the requirements of the ISO 27001 standard
Has the Policy for the use of cryptographic controls been defined?	A.10.1.1	Procedure for the use of cryptographic controls. Procedure needs to become policy
Has the Policy for the use of cryptographic keys been defined?	A.10.1.2	Procedure for the use of cryptographic controls. Procedure needs to become policy
Is there a document with clearly shown separation zones in the company	A.11.1.1 A.11.1.5	Mandatory to implement in accordance with the requirements of the ISO 27001 standard
Are there defined Disaster Recovery Plans for protection against earthquakes, floods and other natural disasters	A.11.1.3 A.11.1.4	Mandatory to implement in accordance with the requirements of the ISO 27001 standard
Is there a documented best practice for performing quantitative and qualitative work as a place of delivery and loading	A.11.1.6	Mandatory to implement in accordance with the requirements of the ISO 27001 standard
Are there documented best practices for maintaining UPS systems and air conditioning systems in data centers?	A.11.2.2	Procedures, criteria and method of deleting data from the medium
Is there a documented best practice for cabling security specifically for UPS cables	A.11.2.3	Yes
Is there a defined procedure for taking equipment outside the company	A.11.2.4	Mandatory to implement in accordance with the requirements of the ISO 27001 standard
Is there a documented best practice for safe disposal of equipment and for monitoring equipment outside the company	A.11.2.5	Mandatory to implement in accordance with the requirements of the ISO 27001 standard
Is there a defined clean desk and blank screen policy?	A.11.2.9	Mandatory to implement in accordance with the requirements of the ISO 27001 standard
Is there a defined change management procedure with clearly defined and included Committees for dealing with changes and types of changes	A.12.1.2	Change management procedure
Is there a defined capacity management procedure with clearly indicated capacity plans and their planning?	A.12.1.3	Mandatory to implement in accordance with the requirements of the ISO 27001 standard
Is there a defined procedure for separating development and test environments	A.12.1.4	Procedure for separating production and test environments
Is there a defined policy for managing antivirus solutions	A.12.2.1	Antivirus procedure
Is there a documented best practice that shows antivirus solutions and their use in company	A.12.2.1	Antivirus procedure
Is there a defined Backup Management Policy	A.12.3.1	Backup procedure
Is there a defined log management policy with administrator and operator log management practices	A.12.4.2 A.12.4.3	Event management procedure
Is there a unique form in the company where it is recorded	A.12.4.4	Domain controller
Is there a defined policy with clear descriptions of which operating systems are allowed in the company	A.12.5.1	Mandatory to implement in accordance with the requirements of the ISO 27001 standard
Is there a unique form in Company where it is recorded which operating systems are installed on servers and PCs	A.12.5.1	Mandatory to implement in accordance with the requirements of the ISO 27001 standard
Is there a documented best practice related to restrictions on software installations on all strategic information assets	A.12.6.2	Mandatory to implement in accordance with the requirements of the ISO 27001 standard
Is there a defined procedure for the audit (revision) of information systems and does it follow the recommendations of CobiT or ITIL and other similar methodologies	A.12.7.1	Internal audit procedure
Is there a defined procedure for the implementation and monitoring of network segregation and domains in the network of the company	A.13.1.1 A.13.1.2 A.13.1.3	Mandatory to implement in accordance with the requirements of the ISO 27001 standard
Is there a defined policy for the transfer of information	A.13.2.1	Excluded. Impossible to implement in this company

Are there defined internal agreements in the company related to the transfer of information - examples of Operation Level Agreement agreements	A.13.2.2	Mandatory to implement in accordance with the requirements of the ISO 27001 standard
Is there a Rulebook with clearly defined activities on maintaining the e-mail service	A.13.2.3	Mandatory to implement in accordance with the requirements of the ISO 27001 standard
Are there defined Non-Disclosure Agreements with third parties and suppliers	A.13.2.4	Mandatory to implement in accordance with the requirements of the ISO 27001 standard
Is there a documented best practice for the protection of all application transactions in the internal network of the company	A.14.1.3	Excluded. Impossible to implement in this company
Is there a defined Safe Development Policy?	A.14.2.1	Excluded. Impossible to implement in this company
Is there a defined Policy for separating the pre-production from the Production environment	A.14.2.5 A.14.2.6	Instructions for refreshing the test and development environment
Is there a defined procedure with associated forms for monitoring the externalized development of application solutions	A.14.2.7	Mandatory to implement in accordance with the requirements of the ISO 27001 standard
Is there a defined procedure for testing system security as well as selecting test data for each system test	A.14.2.8 A.14.2.9	Mandatory to implement in accordance with the requirements of the ISO 27001 standard. It is mandatory to have a defined procedure for testing system security as well as selecting test data for each system test.
Is there a defined list of criteria for qualitative tests by suppliers for strategic information assets: servers, routers, switches, PCs, printers, scanners, IP cameras, security systems, databases, operating systems, etc.	A.14.3.1	Mandatory to implement in accordance with the requirements of the ISO 27001 standard
Is there a defined Information Security Policy for supplier management?	A.15.1.1	Mandatory to implement in accordance with the requirements of the ISO 27001 standard. It is mandatory to have a defined Information Security Policy for supplier management
Are there documented security parameters that are an integral part of every contract with suppliers	A.15.1.2	Mandatory to implement in accordance with the requirements of the ISO 27001 standard
Does company have a documented chain of suppliers in terms of monitoring the work of suppliers and subcontractors	A.15.1.3	Mandatory to implement in accordance with the requirements of the ISO 27001 standard
Are there generally defined tests for selecting suppliers from the aspect of ISMS systems and information security in general	A.15.2.1	Mandatory to implement in accordance with the requirements of the ISO 27001 standard
Is there a defined procedure with associated forms for monitoring all changes that occur at the supplier	A.15.2.2	Mandatory to implement in accordance with the requirements of the ISO 27001 standard
Is there a defined procedure for the management of security incidents together with the associated forms and included: goals, activities, responsibilities, metrics, etc.	A.16.1.1 A16.1.2, A16.1.3, A.16.1.4 A.16.1.5 A16.1.6, A.16.1.7	Procedure for monitoring the situation and incidents in the IS with respect to the given recommendations
Is there a defined procedure or rule for separating security problems from security incidents and by what filter is this separation done	A.16.1.1 A16.1.2, A16.1.3, A.16.1.4 A.16.1.5 A16.1.6, A.16.1.6 A.16.1.7	Procedure for monitoring the situation and incidents in the IS with respect to the given recommendations
Is there a defined procedure for managing business continuity together with the associated forms	A.17.1.1	Business Continuity Plan, Business Impact Analysis
Is there a defined procedure for managing the availability of all IT services together with the associated forms	A.17.1.2 A17.1.3	Business Continuity Plan, Business Impact Analysis
Is there a prepared and documented best practice for implementing redundancy for the internal systems	A.17.2.1	Business Continuity Plan, Business Impact Analysis
Is there a prepared and documented best practice for implementing geo redundancy?	A.17.2.1	Business Continuity Plan, Business Impact Analysis
Is there a defined procedure for identifying legal and legal regulations from the aspect of information security	A.18.1.1 A.18.1.2 A.18.1.5	Law on Protection of Personal Data of Montenegro Government regulation on information security of Montenegro Law on Banks of Montenegro Decision on minimum standards for operational risk management
Is there a defined procedure for testing technical compliance with the basic requirements of the ISMS system	A.18.2.3	Mandatory to implement in accordance with the requirements of the ISO 27001 standard. It is mandatory to have a defined procedure for testing technical compliance with the basic requirements of the ISMS system

Statistics for ISO27001:2013 implementation in this company:

- Sucessfully implemented controls (100%): count: 52, success rate: 54,08%
- Partially implemented controls (50%), count: 2
- Unimplemented controls (0%): count 44, success rate: 45,91%.

The total ISO27001:2013 realization rate is 54,08%.

IV. DISCUSSION

As the conclusion of both GAP analasysis for ISO9001:2015 and ISO27001:2023, realization rate was provided. It remains to be seen which of the five levels of criticality Company is in in terms of the implementation of these two standards. There are a total of five levels of criticality: critical, poor, satisfactory with mandatory implementation elements, satisfactory and excellent. The criticality level is found by finding the arithmetic sum of the measured values for the ISO 9001:2015 and ISO 27001:2013 standards, they are as follows:

TABLE III. REALIZATION RATE AND ACTIVITIES

Level of criticality	**Realization rate**	**Activities**
Critical	0%-20%	Critical level of implementation of quality and information security within the Company. An urgent reaction of the Company's management is required.
Poor	21%-40%	There are basic elements of quality and information security implementation within the Company. A delayed reaction of the management is required.
Satisfactory with mandatory implementation elements	41%-60%	Satisfactory degree of implementation of quality and information security. No reaction from the company's management is required. The introduction of new documents and technical systems

		should be done periodically and with an established project plan.
Satisfactory	61%-80%	A very satisfactory degree of implementation of quality and information security. The introduction of new documents and technical systems should be done in accordance with the company's business needs.
Excellent	81%-100%	Excellent level of implementation of quality and information security. It is not necessary to introduce new documents or new technical systems.

Overall realization rate of ISO27001:2013 is 54,08% and ISO9001:2015 is 58,87%. The average for both standards is 56,48%. That means that level of qaulity implementation and information security is at the middle level of implementation, no immediate intervention of the company's management is required, but it is necessary to make a project time plan for both the implementation of documentation and the implementation of technical systems. The recommendation is to first complete staffing, then prepare policies and procedures, and only then implement the proposed technical systems.

V. Conclusion and Future Research

Some very important technical issues in the field of information security were not considered in the audit discussed in this paper, as they are not included in the version of the ISO 27001:2013 standard. Based on this practical methodological approach, it is therefore very important to include the following security controls in subsequent revisions of the ISO 27001:2013 standard. The use of the following policies and procedures is imperative based on experience in the banking sector and this is a concrete conclusion from this paper:

- Existence of a policy or procedure to prevent the outflow of data and information (Data Loss Prevention System)
- Continuous monitoring of vulnerabilities in technical systems (Vulnerability Management System)
- Monitoring of administrator rights (Privilege Access Management System)
- The existence of a Security Operations Center for 24/7 monitoring of potential security incidents that may occur (Security Operating Center)
- Existence of a policy or procedure that ensures the protection of data stored in the cloud
- Existence of a technical system for continuous 24/7 monitoring of security logs (Security Information and Event Management System)

With implementing and maintaining ISO9001:2015 and ISO27001:2013 standards, organizations can demonstrate their commitment to good information security practices, high-quality management systems, and the overall well-being of their stakeholders. This paper provided detailed step-by-step guide how to preform GAP analysis for financial institution, which can be used for any future research, and practical application. For observed company we demonstrated a satisfactory degree of implementation of quality and information security. No reaction from the company's management is required. The introduction of new documents and technical systems should be done periodically and with an established project plan.

Since the ISO 27001:2013 standard and the General Data Protection Regulation (GDPR) are both crucial frameworks that organizations often consider in their efforts to manage information security and data protection effectively, future research could connect and compare those two for financial institutions. Further research could explore how organizations can effectively tailor their approach to standard's implementation based on their specific needs.

In future research, it is necessary to use the strict recommendations for improving information security, which are listed in this paper. It is also necessary to use the recommendations of other standards or frameworks in the field of information security, specifically: COBIT, ITIL, ISO 22301, ISO 27014, ISO 27033, ISO 27701.

References

[1] Djordje Krivokapić, Andrea Nikolić and Ivona Živković, "Capacities of Western Balkan Economies (and Their Public Sectors) to Respond to Ransomware Attacks," in *MIPRO*, Opatija, 2023.

[2] Saqib Saeed, Sarah A. Suayyid, Manal S. Al-Ghamdi, Hayfa Al-Muhaisen, Abdullah M. Almuhaideb, "A Systematic Literature Review on Cyber Threat Intelligence," *Sensors - MDPI journal,* vol. 23, 2023.

[3] Ana Pereira, Rui Henriques, João Barata, "An ArchiMate-Based Approach to ISO 9001:2015 Quality Management: Shifting to IT-Enabled Documented Information," in *IEEE 23rd Conference on Business Informatics (CBI)*, 2021.

[4] A. Melicharova, "Standard ISO 9001:2015, most important changes and their impact on supplier complaints management," in *Engeneering for rural development*, Jelgava, 2018.

[5] Tahani Alsahafi, Waleed Halboob*, Jalal Almuhtadi, "Compliance with Saudi NCA-ECC based on ISO/IEC 27001," *Technical Gazette 29,* vol. 6, pp. 2090-2097, 2022.

[6] Z. Hamdi, "A Comparative Review of ISMS Implementation Based on ISO 27000 Series in Organizations of Different Business Sectors," *Journal of Physics: Conference Series,* 2019.

[7] Vasiliki Diamantopoulou, Aggeliki Tsohou, Maria Karyda, "From ISO/IEC27001:2013 and ISO/IEC27002:2013 to GDPR compliance controls," *Information and Computer Security,* 2020.

[8] Kristian Beckers, Stephan Faßbender, Maritta Heisel, Jan-Christoph Kuster, Holger Schmidt, "Supporting the Development and Documentation of ISO 27001 Information Security Management Systems Through Security Requirements Engineering Approaches?," in *Engineering Secure Software and Systems - 4th International Symposium, ESSoS 2012*, Eindhoven, 2012.

[9] L. Fonseca, "From quality gurus and TQM to ISO 9001:2015: A review of several quality paths," *International Journal for Quality Research,* pp. 167-180, 2016.

[10] K. Świtała, "Medical Data in the Digital Era - Legal Challenges Related to Providing Information Security, Applying GDPR and Respecting the Professional Secrecy," in *MIPRO*, Opatija, x2023.

[11] N. Mike, E. Krén, T. Kecskeméti, "Information Security among SMEs in Hungary - An Overview," in *MIPRO*, Opatija, 2023.