The National Law Institute University, Bhopal

Offers Programme

Master
of

Cyber Law and Information Security

Project On

"Implementation of ISO: 27001 with GDPR"

Subject

"Information Security and Compliances"

SUBMITTED TO:	**SUBMITTED BY:**
Mr. Mayank Tiwari	**Isha Gaur (2019MCLIS58)**

Contents

A. ABSTRACT

The European Union's General Data Protection Regulation (GDPR) has made it mandatory under the law for the organizations to adopt suitable policies, processes and procedures for the protection of the personal data they hold. The organizations need to protect the personal data of not only its customers, but its employees as well, while failing to comply with the regulation may attract hefty fines. Hence, it has become important for organizations worldwide, to which the GDPR apply to, to understand the regulation and comply with it operationally.

ISO: 27001 standard is one of the few frameworks that ensure this protection. The international standard facilitates achieving operational and technical requirements needed for the compliance with the regulation. ISO: 27001 mainly focuses on protection of information and information assets in an organization, which includes the personal data to be considered as a critical asset, thereby requiring them to adopt suitable measures to protect it. There are many overlapping areas between the GDPR and ISO: 27001 standard, and compliance with the standard can ensure 75-80% compliance with GDPR[1]. This paper discusses about how compliance with the GDPR can be achieved by ISO: 27001 implementation, by mapping similarities between the two.

KEYWORDS:

General Data Protection Regulation, GDPR, ISO: 27001, Information Security Management System, ISMS

[1] https://www.certificationeurope.com/insights/gdpr-iso-27001-mapping-tool-now-available/ (Accessed on 25/11/2019)

1. INTRODUCTION

The European Union General Data Protection Regulation (hereafter referred to as GDPR) is the latest EU wide data protection law which aims at protecting the personal data of European citizens processed by the organizations all over the world. The term personal data includes any information, regarding an identifiable natural person, like name, address, email address, photo, race, religion, location data, biometric data, etc. Hence, any organization, dealing with the personal data of its employees or customers residing in the European Union are required to comply with the Regulation, failing which might attract hefty fines. The primary requirements of GDPR include[2] establishing accountability and governance, complying with the six data processing principles – lawful and fair processing of data, data collection limitation, purpose specification for the processing of data, data accuracy, data storage limitation and secured processing of data; consideration of privacy rights of the individuals, obtaining valid consent, implementing data protection by design and default, transparency and privacy notices, requirements and obligations for data transfer outside EU, data breach reporting, and appointing a Data Protection Officer (hereafter DPO) with relevant roles and responsibilities.

ISO 27001: 2013 is an international standard provided by the International Organization for Standardization (ISO) which provides a framework to protect the information assets of an organization. ISO: 27001 compliance offer many benefits to the organization, including identifying and managing risks, periodic reviews, global acceptance, market recognition, and gaining trust of the stakeholders[3]. It emphasizes on implementation of Information Security Management System (hereafter ISMS) which aims at incorporating information security within organization's processes providing a holistic approach to implement security. The standard can be tailored to meet the requirements and needs of any organization, considering its individual contexts and processes, as well as the interests of the related parties or stakeholders. It is also the best standard among its family for the implementation of ISMS. It suggests implementing the Plan, Do, Check, Act (PDCA) cycle for effective implementation and continual improvement of the ISMS.

2. OVERVIEW OF ISO 27001: 2013

ISO/IEC 27001: 2013 is an international standard for implementing, maintaining, and continually improving an Information Security Management System within an organization. This standard is applicable to any organization, irrespective of its type, nature, or size. It is compatible with most of the other standards as well, for instance, the quality management standards provided by the ISO 9000 series. This standard consists of 10 clauses, out of which, Clauses 4-10 are mandatory for compliance with the standard. Apart from these, it

[2] https://www.itgovernance.co.uk/data-protection-dpa-and-eu-data-protection-regulation (Accessed on: 25/11/2019)

[3] Individuals or organizations or other interested parties that can be affected by the decision or activity of an organization.

also consists of 114 controls and 35 control objectives defined in Annex A. The requirements described under the mandatory clauses of the standard are[4]:

2.1 Context of the Organization

It is important to understand the context of the organization before implementing ISMS in it. It includes determining the internal and external contexts[5] and the needs and expectations of the interested parties, which may include legal and regulatory requirements and contractual obligations. Also, scope of the implementation of ISMS must be identified and documented and the ISMS must be implemented accordingly.

2.2 Leadership

Top management is required to offer leadership and commitment regarding the ISMS ensuring an appropriate information security policy is established, resources required for the ISMS are made available, information security objectives are identified and established, relevant roles and responsibilities are assigned, and making employees aware of the ISMS and its importance.

2.3 Planning

Planning for the implementation of the ISMS begins with the risk assessment[6] process, which includes identification of risks associated with the information and information assets within the scope, analysis and evaluation of risks based on the predefined risk criteria, and then defining the risk treatment process by applying appropriate control from the list provided in Annex A or any other control, if appropriate.

2.4 Support

Top management need to provide support for the implementation of the ISMS. This includes the resources needed for the implementation, competent employees, awareness among the employees about the information security policy and the ISMS and their responsibilities, as well as carrying out proper communication as required. The organization shall also maintain a record of documented information mandatory under the standard and ensure management and control of these records.

2.5 Operation

The organizations need to implement the plans laid out in the planning phase for achieving the ISMS. It shall carry out effective change management, periodic risk assessments and implement relevant risk treatment plans. Each of these processes need to be documented.

2.6 Performance Evaluation

The organization is required to evaluate the effectiveness of the ISMS at planned intervals. Internal audits and management reviews are to be carried out periodically regarding performance of the ISMS.

2.7 Improvement

The organization shall identify the non-conformities, and take relevant corrective actions to further improve the ISMS. The suitability, adequacy and effectiveness of the ISMS needs to be continually evaluated and improved.

[4] Refer ISO 27001:2013 official document.

[5] Defining the external and internal parameters to be taken into account when managing the risk.

[6] Overall process of risk identification, risk analysis and risk evaluation.

3. MAPPING ISO:27001 AND GDPR

ISO: 27001 is a framework for protection of information assets within an organization. GDPR on the other hand, requires personal data of the data subjects to be protected. During the implementation of ISMS, the personal information of the people are considered as a critical asset to the organization and is provided utmost security against the risks associated with such data. Furthermore, GDPR consists of six data processing principles, out of which, three, including – data accuracy, storage limitation, and integrity and confidentiality of the data are addressed within the ISO: 27001 standard. Also, the standard significantly helps in complying with the seventh additional principle of accountability since each step of the ISMS requires proper documentation. The requirements of the ISMS can further be tailored a little to match the requirements of the GDPR. Apart from these, there are many other similarities between the ISO: 27001 standard and the GDPR which enables the organizations implementing the standard to comply with the Regulation to an extent. Some of these similarities between the two are mapped below[7]:

GDPR	ISO 27001:2013	Remarks
	Clause 4 – Context of the Organization The organization shall identify the scope of the ISMS depending on the external and internal contexts and the requirements of the interested parties, which may include the legal and regulatory requirements, and shall establish, implement, maintain and continually improve the ISMS accordingly. **Control A.18 – Compliance** It includes compliance with legal, statutory, contractual or regulatory obligations including intellectual Property rights, privacy and protection of personally	The ISO: 27001 standard by default requires consideration of legal and regulatory requirements before implementation of the ISMS, which shall include GDPR as well, if applicable. Hence, it is mandatory to comply with GDPR and consider its requirements during the implementation of the standard. GDPR at its very core states about the protection of personal data of EU citizens. In the ISMS implementation, Control A.18 refers to the personal data as personally identifiable information and requires it to be protected, and kept private thereby complying with the core purpose of the Regulation.

[7] https://iapp.org/media/pdf/resource_center/IAPP-OneTrust-Bridging-ISO-GDPR-final.pdf

	identifiable information and cryptographic controls.	
Article 32 – Security of Processing Data controller or processor shall implement adequate security measures following a risk based approach, which may include (but not limited to) – pseudonymization[8] encryption of personal data, protection of the confidentiality, integrity and availability of the data, achieving resilient processing systems, timely recovery in case of an incident, and periodic checks for the effectiveness of the security measures. The data controller or processor shall also protect unauthorized processing of personal data by any natural person under their authority. **Article 5(1)(f) – preserving the integrity and confidentiality** Appropriate technical and organizational security measures shall be taken for the protection of the personal data.	**Clause 6.1.2 – Information Security Risk Assessment** This clause requires the organization to perform information security risk assessment identifying the risks associated with the assets, the risk owners, analyse and evaluate them based on risk levels and the risk evaluation criteria. **Clause 6.2 – Information Security Objectives and Planning to achieve them** It requires organizations to establish and document information security objectives taking into account the results of risk assessment and risk treatment. **Clause 8 – Operation** It requires organizations to implement the actions determined in Clause 6.1, including risk assessment and risk treatment and implement plans to achieve the objectives established in Clause 6.2.	Implementation of ISO: 27001 involves following a risk based approach, including risk assessment, which further includes identification of risk associated with the information assets, protecting them from loss of confidentiality, integrity and availability, risk analysis and evaluation based on the risk criteria, followed by the risk treatment. These requirements helps organizations to comply with Article 32 of GDPR which also requires a risk based approach to protect the CIA[9] of the personal data. Furthermore, Control A.10 of ISO: 27001 suggests inclusion of cryptographic controls during the implementation of the standard, as also suggested by the GDPR.

[8] **Pseudonymization** is a data management and de-identification procedure by which personally identifiable information fields within a data record are replaced by one or more artificial identifiers, or pseudonyms.

[9] Confidentiality, Integrity and Availability also commonly referred to as the CIA triad.

	Clause 10 – Improvement It requires organizations to adopt continual improvement of the ISMS by periodically analysing and evaluating the effectiveness of the ISMS, identifying the non-conformities and correcting them. **Control A.10 – Cryptography** Policies shall be made to ensure effective use of cryptographic controls and key management.	
Article 33 – Notification of a personal data breach to the supervisory authority The controller shall, in case of a personal data breach, notify the same to the competent supervisory authority without undue delay and not later than 72 hours after becoming aware of it. The only exception stated is when the breach is unlikely to cause risk to the rights and freedoms of the concerned natural persons. The notification shall include the nature of the breach, the categories and approximate number of the data subject and personal data records concerned, name and contact details of the data protection officer, the consequences of the breach, and the measures taken or proposed to address and mitigate the breach and its impact.	**Control A.16 – Information Security Incident Management** Security incidents shall be responded quickly and effectively, documented, timely reported, and further investigated for future improvement.	Control A.16 deals with the information security incident management which is similar to the GDPR requirements of Article 33 and Article 34 to an extent. These processes can be tailored to comply with the Regulation to report the incidents to the competent supervisory authority within 72 hours of the identification of the breach, and the data subjects if applicable, including the relevant mandatory information as required.

Article 34 – Communication of a personal data breach to the data subjects The controller shall, in case of a personal data breach which is likely to pose high risk to the rights and freedoms of natural persons, notify the same to the concerned data subjects without undue delay. The notification shall include the nature of the breach, name and contact details of the data protection officer, the consequences of the breach, and the measures taken or proposed to address and mitigate the breach and its impact.		
Article 28 – Processor Data controllers shall impose legal and contractual obligations to protect the personal data that is to be processed by the data processors. The processor is required to, as per the contract, implement adequate organizational and technical safeguards to protect the personal data and its confidentiality. The contract shall be valid and must include the duration, nature and purpose of processing, the type of personal data, the categories of the data	**Clause 8 – Operation** It requires organizations to plan, implement, control, and oversee the information security and outsourced processes. **Clause 9 – Performance Evaluation** This clause requires the organization to monitor, measure, analyse and evaluate the effectiveness of the ISMS, carry out periodic internal audits and management reviews considering the changes in internal and external issues.	The requirement of protection of data, when transferred to a data processor or an external party can be met by including the outsourced processes and external context and issues in the ISMS process. Also, Control A.15 suggests incorporating security into the supplier agreements, and drafting an information security policy for supplier relationships as contractual obligations. Control A.18

subjects, and terms of deletion or returning of personal data to the controller.	**Control A.15 – Supplier Relationships** It aims to safeguard organizations from the risks associated with the assets which are accessible to the suppliers. Information security policy for supplier relationships and security within the supplier agreements shall address these risks. Control A.18 – Compliance It includes compliance with legal, statutory, contractual or regulatory obligations including intellectual property rights, privacy and protection of personally identifiable information, and cryptographic controls.	further requires organizations to comply with these contractual obligations.
Article 30 – Records of processing activities The controller or processor needs to maintain documented records of the processing activities under its responsibility, including the name and contact details of the controller and its DPO, the purpose and categories of processing, the categories of personal data and data subjects, transfer of data to any third country with suitable safeguards, time limits for the erasure of data, and the technical and organizational safeguards	**Clause 7.5 – Documented Information** The organizations need to retain documented information regarding the ISMS with appropriate description, reviews and control. **Clause 8 – Operation** It requires organizations to retain documented information regarding	The requirements of the ISO: 27001 can be extended further to include relevant information about the information and information assets in the documentation as required under GDPR. Transfer of data to the external parties can be governed by the policies, agreements and contracts including transfer of data to any third country, which will help in fulfilling the

applied for the protection of such data.	operational planning and control, information security risk assessment and risk treatment. **Control A.8 – Asset Management** An inventory of the information assets shall be created and maintained, detailing about the asset owners, and their acceptable usage. Information shall be classified as per value, sensitivity, criticality and legal requirements, and shall be documented, labelled and handled accordingly. Unauthorized disclosure, modification, removal or destruction of information stored on media shall be prevented by proper management, physical transfer and disposal of media devices. **Control A.13.2 – Information Transfer** Security of information transferred within or outside the organization shall be maintained by use of proper information transfer policies, procedures and controls. Business information transferred between the organization and external parties shall be secured by proper agreements. Non-disclosure agreements shall be framed, documented, and regularly reviewed.	requirements of the Regulation.

Article 25 – Data protection by design and by default Appropriate technical and organizational safeguards, for instance pseudonymization, implementing data protection principles such as data minimization and integrating appropriate safeguards into the processing of personal data shall be implemented, considering the nature, purpose, context and scope of the processing. The controller shall also ensure the processing of personal data only necessary for specific purposes are processed. This includes the amount of data collected, the extent of processing, its accessibility and the period of storage.	**Clause 4 – Context of the Organization** The organization shall identify the scope of the ISMS depending on the external and internal contexts, the requirements of the interested parties, which may include the legal and regulatory requirements, and shall establish, implement, maintain and continually improve the ISMS accordingly. **Clause 6 – Planning** Organizations shall conduct periodic risk assessments, identifying the risks, analysing, evaluating it and then treating it accordingly as per the risk acceptance criteria. **Control A.9 – Access Control** For the purpose of limiting access to the information to authorized users only and preventing unauthorized access of the information Access control policies shall be drafted as well as implemented technically throughout the organization. **Control A.10 – Cryptography** Policies shall be made to ensure effective use of cryptographic controls and key management.	Article 25 of GDPR focuses on incorporating security and data protection principles such as collection limitation, data minimization, etc. into the design of the processing of the data by the organizations by implementing appropriate safeguards. This can be achieved by considering both the internal and external contexts of the organization for the implementation of ISMS, considering risks associated with each information asset, and applying controls like cryptography, access controls, etc. as prescribed by ISO: 27001.

Article 39 – Tasks of the Data Protection Officer The Data Protection Officer need to communicate and help the data controller or processor and its employees about the obligations under the Regulation, including their responsibilities, raising awareness and training and examine compliance with the Regulation.	**Clause 5.1 – Leadership and Commitment** Top management of the organizations need to ensure information security policies and objectives are established, are integrated into the organization's processes, shall communicate the importance of an ISMS to its employees, ensuring that intended outcomes are achieved and further promoting continual improvement	ISO: 27001 requires top management to establish information security policies and communicate and direct its employees to implement and periodically review and improve the ISMS. This role can be assigned to the respective DPO with some additional duties required under the Regulation for achieving compliance with GDPR.

4. ADVANTAGES OF THIS MAPPING

1. **Testing and Audits:** Being GDPR - compliant means that an organization needs to carry out regular testing and audits to prove that its security regime is working effectively. An ISO 27001 - compliant ISMS needs to be regularly assessed according to the internal audit guidelines provided by the standard.

2. **Controls and Security framework:** The GDPR stipulates that organizations should select appropriate technical and organizational controls to mitigate the identified risks. The majority of the GDPR data protection arrangements and controls are also recommended by ISO 27001.

3. **Accountability:** ISO 27001 requires companies' security regime to be supported by top leadership and incorporated into the organization´s culture and strategy. It also requires the appointment of a senior individual who takes accountability for the ISMS. The GDPR mandates clear accountability for data protection across the organization.

4. **Risk Assessments:** ISO 27001 compliance means conducting regular risk assessments to identify threats and vulnerabilities that can affect organizations' information assets, and to take steps to protect that data. The GDPR specifically requires a risk assessment to ensure that an organization has identified risks that can impact personal data.

5. **Assurance:** The GDPR recommends the use of certification schemes such as ISO 27001 as a way of providing the necessary assurance that the organization is effectively managing its information security risks.

6. **Certification:** The GDPR requires organizations to take the necessary steps to ensure the security controls work as designed. Achieving accredited certification to ISO 27001 delivers an independent, expert assessment of whether organizations have implemented adequate measures to protect their data.

5. DIFFERENCE BETWEEN ISO 27001 AND GDPR

Certification with ISO 27001 can simplify the process of achieving GDPR compliance. However, there are several differences between these standards. The GDPR is a global standard that provides a strategic vision of how organizations need to ensure data privacy. ISO 27001 is a set of best practices with a narrow focus on information security; it provides practical advice on how to protect information and reduce cyber threats. Unlike the GDPR, it does not directly cover the following issues associated with data privacy, which are outlined in Chapter 3 of the GDPR (Data Subject Rights):

1. Consent,
2. Data portability,
3. The right to be forgotten,
4. The right to restriction of processing,
5. Right to object,
6. International transfers of personal data.

As we can see, the GDPR focuses on data privacy and the protection of personal information, it requires organizations to put more effort into obtaining explicit consent for data collection and ensuring that all data is processed lawfully. However, it lacks technical details on how to maintain an appropriate level of data security or mitigate internal and external threats. In this regard, ISO 27001 comes in handy, It provides practical guidance on how to develop clear, comprehensive policies to minimize security risks that might lead to security incidents.

6. CONCLUSION

ISO 27001: 2013 provides a comprehensive framework to comply with the requirements a many of these requirements are covered under the standard. Both the ISO standard and the GDPR commit to protect the sensitive and confidential data stored and processed within an organization. However, some of the GDPR requirements are not included in the standard directly and need to be tailored to achieve compliance with the Regulation. The IT Governance forum of UK[10] suggests implementation and compliance to ISO: 27001 standard to aid compliance with the GDPR. Additionally, a certified ISMS is not only beneficial for meeting the GDPR compliance, but also facilitates compliance with other cyber security laws such as the EU Directive on security of Network and Information Systems (The NIS Directive). Further, additional requirements of GDPR, which are not addressed under ISO: 27001 shall be met separately, or with compliance with other standards such as BS

[10] https://www.itgovernance.co.uk/gdpr-and-iso-27001 (Accessed on 26/11/2019)

10012:2018 (Specification for a Personal Information Management System)[11], ISO 27018 if the organization operates on cloud[12], etc. Hence, while complying with ISO: 27001 shall not assure complete compliance with GDPR, it can be used as a framework to start the process and fulfilling about more than half of the requirements of the Regulation.

7. REFERENCES

[1] https://www.yash.com/blog/differences-between-gdpr-and-other-data-protection/

[2] Achieve GDPR Compliance with ISO 27001, Available at www.itgovernance.co.uk

[3] https://plan.io/blog/gdpr-requirements-needed-for-compliance/

[4] https://www.certificationeurope.com/insights/gdpr-iso-27001-mapping-tool-now-available/

[5] https://iapp.org/resources/article/iapp-onetrust-research-bridging-iso-27001-to-gdpr/

[6] https://www.itgovernance.co.uk/gdpr-and-iso-27001

[7] https://www.itgovernance.co.uk/data-protection-dpa-and-eu-data-protection-regulation

[8] https://www.itgovernance.co.uk/blog/how-iso-27001-can-help-you-achieve-gdpr-compliance

[9] https://www.certificationeurope.com/app/uploads/2018/05/GDPR-ISO-27001-Mapping-Guide.pdf

[10] https://koolitus.ee/images/sisu_pildid/ISO_GDPR_link.pdf

[11] https://iapp.org/media/pdf/resource_center/IAPP-OneTrust-Bridging-ISO-GDPR-final.pdf

[12] http://www.british-assessment.co.uk/app/uploads/2017/07/GDPR-ISO-27001-Mapping-Table-2.pdf

[13] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[11] https://www.itgovernance.co.uk/gdpr-and-iso-27001 (Accessed on 26/11/2019)

[12] https://www.yash.com/blog/differences-between-gdpr-and-other-data-protection/ (Accessed on 27/11/2019)