ISO/IEC 27001 and the General Data Protection Regulation (GDPR)

How the ISO/IEC 27001 framework supports GDPR compliance

Gemserv

INTRODUCTION

ISO 27001 is a framework for information protection. ISO 27001 focuses on the people, processes and technology of an organisation and ensures that a framework is put in place to prevent breaches and ensure that a proper mechanism is created for reporting, logging incidents and maintaining an organisation's information security environment.

According to GDPR, personal data is critical information that all organisations need to protect. ISO 27001 provides the means to ensure this protection and wider compliance with this regulation.

The ISO 27001 provides a framework for information protection which is a fundamental cornerstone for achieving compliance with the GDPR helping to ensure companies can maintain customer trust and confidence in their ability to handle their personal data appropriately and securely. This paper is intended to help explain how an ISO 27001 framework may assist organisations to establish a solid foundation for GDPR compliance.

THE NEW REGULATION

The GDPR will repeal the current data protection legislation when it comes into force on 25th May 2018.This means the Data Protection Act 1998 (DPA) and the European Union legislation it is derived from - the Data Protection Directive, will no longer apply.

It introduces new regulatory requirements, giving individuals more control over the data that organisations hold about them. Working with the Regulation is a legal compliance exercise as well as a technical and security governance exercise.

Organisations that fail to demonstrate compliance with GDPR, will face significant fines of up to €20 million or 4% of annual global turnover, whichever is higher.

THE ISO/IEC 27001 STANDARD

The origin of this standard, BS 7799, traces back to 1995 when it was first published by the United Kingdom Government Department of Trade and Industry (DTI). Since then, it has seen several iterations and become a well-recognised international industry standard.

The current version has been created by the International Organisation for Standardisation (ISO) in conjunction with the International Electrotechnical Commission (IEC) in 2013. In essence, it is a specification for an Information Security Management System (ISMS), to help organisations of any size, type or nature of business to manage people, processes, and technology.

HOW GDPR AND ISO 27001 INTERACT

INFORMATION SECURITY

The parallels between GDPR and ISO 27001 are most pertinent when it comes to the security of personal identifiable data. To ensure compliance with both GDPR and ISO 27001, companies are required to implement adequate security measures to protect personal data and to ensure ongoing confidentiality, availability and integrity, as it is mentioned in ISO 27001.

ISO 27001 requires organisations to protect Personally Identifiable Information (PII) in line with relevant legislation and regulation. For organisations trading in the UK, this is currently the DPA but will move to GDPR in 2018.

ISO 27001 specifically recommends implementing a data protection policy specifying requirements for data protection supported by specific procedures regarding aspects of data protection e.g. retention and destruction.

The GDPR stipulates that personal data shall be 'processed in a manner that ensures appropriate security'.

Unlike the current data protection legislation however, the GDPR does somewhat unusually provide specific suggestions for what kinds of security actions might be considered "appropriate to the risk," including:

- The pseudonymisation and encryption of personal data;
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

ISO 27001 requires organisations to implement appropriate organisational and technical controls to support compliance with these requirements. The protection of PII and compliance with legislation is already a key control requirement in ISO 27001.

Several ISO 27001 Annex A controls can be used to support GDPR compliance when it comes to protecting personal data.

For example, A.10.1 specifies encryption requirements for the organisation. The use of encryption and/or pseudonymisation can maintain the confidentiality of personal information, whether on the network, in transit or held mobile devices.

A.9 covers the topic of access control, which, if implemented properly, will ensure only individuals with a legitimate right can access information according to their privilege level.

In addition, the IT systems must be sufficiently resilient to external attacks. The ISO framework's control 18.2.3 requires companies to perform vulnerability tests and penetration tests with due care, so that the systems tested are not compromised. The requirement to manage technical vulnerabilities under ISO 27001 requires organisations to patch systems, keep a record of logs, etc.

Both GDPR and ISO 27001 emphasise the importance of implementing measures based on a thorough risk assessment. Further, ISO 27001 and GDPR both require companies to ensure security measures are tested regularly, and that data may be recoverable in the event of a security incident.

As part of the ISO framework, top management is required to demonstrate leadership and commitment to drive the information security management framework by ensuring that the responsibilities and authorities for roles relevant to information security are appropriately assigned.

INFORMATION CLASSIFICATION

Data is at the heart of every business which is why data classification is so important. Information classification ensures the correct handling and monitoring of sensitive information both in and outside of a business, a critical aspect when it comes to protecting the most valuable data.

Data classification is a natural first step because it provides the ideal way to order and prioritise data based on its sensitivity. Which data does your company place the most value on? Is it your finance records, customer data or maybe the direct marketing list? Classifying data in accordance with its value and sensitivity enables an organisation to easily identify its most sensitive assets and by appropriately protecting it, reduces the risk of falling foul of most compliance mandates.

As previously established, encryption is a technology that most organisations have to ensure that information is protected while in transit or at rest. Identifying and classifying the sensitive

content means that the focus can be centred on encrypting the most valuable assets.

Data Loss Prevention (DLP) tools can also be enhanced by making it easier to intercept information being uploaded into the cloud or sent via email. Creating rules with DLP is often cumbersome, consequently, system overheads can increase and false positives can be created. Classifying a document by adding a “confidential” label into the metadata, tells the DLP that the data should NOT leave the organisation and will block it, avoiding the need to scan the entire content.

A fundamental requirement for organisations wishing to obtain ISO 27001 compliance, is the need to develop an asset inventory which will help you understand which classified information you have in your possession, and who is responsible for it (i.e., who is the owner).

ISO 27001 does not prescribe the levels of classification – it allows you the freedom to set your own rules - this is something you should develop on your own, based on what is common in your industry. The bigger and more complex your organisation is, the more levels of confidentiality there will be. However, ISO 27001 does place responsibility on the information asset owner classifying the information – and this is usually done based on the results of the risk assessment: the higher the value of information (the higher the consequence of breaching the confidentiality), the higher the classification level should be.

A huge number of data leaks are accidental and could have been avoided if only a data classification policy had been in place to raise user awareness and prevent sensitive content from being stored on a USB or uploaded to third party web portals such as Dropbox. Using visual labels also encourages users to be more responsible and aware when handling physical copies of data that have been printed out.

TRAINING AND AWARENESS

ISO 27001 promotes a culture and awareness of security incidents in organisations. Information security is not only about technology it's also about people.

DATA PROCESSOR / SUPPLIER MANAGEMENT

There is a fair amount of overlap among several GDPR articles in this chapter and the ISO framework. GDPR identifies data controllers and data processors, obligating controllers to only engage processors that provide sufficient assurance that controls are in place to manage personal data. This is a similar approach used in ISO 27001 to manage suppliers and third parties, as defined in A.15 Supplier Relationships. By assessing data processors against a code of connection or an approved certification, data controllers can demonstrate compliance. These requirements should be documented and agreed between controllers and processors.

RECORDS OF PROCESSING ACTIVITIES / ASSET MANAGEMENT

Under GDPR, companies are required to create and to maintain an internal record of processing activities which contain a description of the categories of personal data, retention period(s), and a general description of the technical and organisational security measures.

Defining asset owners and assigning them the responsibility to protect the confidentiality, integrity and availability of the information is one of the fundamental concepts in ISO 27001. ISO 27001 control A.8 (Asset management), leads to inclusion of personal data as information security assets and allows organisations to understand what personal data is involved, where to store it, how long for, its origin, and who has access, which are all requirements of GDPR.

Similarly, a Record of Processing Activities (data processing inventory) reflects how the business processes data and starts with listing the processing activities and their purpose. In view of the parallels and objective to identify data, it is clear that organisations which are ISO 27001 compliant can use their existing information asset register as a foundation to create a data inventory mandated by GDPR.

COOPERATION WITH THE SUPERVISORY AUTHORITY

Both ISO 27001 and GDPR requires organisations to maintain contact with supervisory authorities, which, in the case of the UK would be the Information Commissioner's Office (ICO).

INCIDENT MANAGEMENT

Article 33 of the GDPR, requires organisations to *Notify the ICO of a personal data breach* without undue delay and not later than 72 hours after having become aware of a personal data breach. The implementation of ISO 27001 control A.16.1 (Management of information security incidents and improvements) will ensure "a consistent and effective approach to the management of information security incidents, including communication on security events." Incident management is one of the key processes to ensure the effectiveness of any business operation. Security incident management is a critical control by ISO 27001 standards (clause A.13), and has an equal, if not higher, level of importance in other standards and frameworks. Incident management forms an integral part of an organisation's security policies and procedures relating to backup, continuity, disaster recovery (DR), risk management, and configuration management. To achieve this state of maturity, the following security incident management processes must be included in the overall response system:

- Clearly defined roles and responsibilities for the incident response team.
- **RACI chart** that identifies the person who is **R**esponsible, **A**ccountable, **C**onsulted or **I**nformed for defined activities before and after an incident.
- Training programme for all activities defined within the security incident management practice.
- Checklists and templates for operational maintenance.
- **Clearly define links/touch points/dependencies** of the security incident management policy and procedures with other information security management system controls response.
- **Evidence collection procedures** to ensure it is 'good', forensically and legally sound, as part of first security incident management response.
- **Learning** from the incident and updating vulnerability/risk repository.
- **Metrics and relevant reporting** to management.

Adherence to the ISO framework will ensure that organisations are in a position to rapidly detect and effectively manage a personal data breach.

RISK ASSESSMENTS / PRIVACY IMPACT ASSESSMENTS

One of the new requirements of the EU GDPR is the implementation of Data Protection Impact Assessments, where companies will have to first analyse the risks to their privacy.

The adoption of Privacy by Design, another GDPR requirement, becomes mandatory in the development of products and systems. ISO 27001 helps ensure that "information security is an integral part of information systems across the entire lifecycle."

Where a new technology is being deployed that may affect individuals' rights and freedoms a privacy impact assessment becomes necessary, The assessment should also contain a description of the measures envisaged to address the risks.

Risk assessment (and treatment) is the most important step at the beginning of an ISO 27001 implementation project – it sets the foundations for information security in your company.

CONCLUSION

There are some key GDPR requirements that are not directly covered in ISO 27001, such as key concepts of consent, fair processing, data minimisation, storage limitation, the requirement to appoint a Data Protection Officer and supporting the rights of individuals relating to access, rectification, erasure and transfer of data.

However, it is clear ISO 27001 provides a framework that provides a solid foundation for GDPR compliance.

The formation of an information security management system enables organisations processing personal data to demonstrate that risks to personal data are being continuously reviewed, updated and improved. An established ISMS is the perfect framework to manage risks to all assets, inclusive of personal data, and can provide assurance that the organisation takes ISO 27001 and GDPR compliance seriously. In some cases, controls can be precisely mapped to GDPR articles, where both share identical content. In other instances, the controls pave the way and little further work is required to achieve GDPR compliance. Even where the GDPR diverts from the controls found in the ISO framework, the core objectives do not differ radically.

A key objective for ISO 27001 (control A.18.1.1) is to ensure companies are compliant with “legal, statutory, regulatory or contractual obligations” relating to information security. ISO 27001 framework essentially requires companies to achieve compliance with GDPR.

The Regulation should be seen as an opportunity to protect personal data in a meaningful way - and possibly, it is to be seen as a wider opportunity to get a grip on security. In the broad perspective, this may be achieved by taking inspiration from security standard ISO 27001.

The GDPR is a very large and complex regulatory framework. Whilst the Regulation does not state that companies are required to comply with ISO 27001, many of the methods and measures outlined in the GDPR are drawn directly from the ISO standard. It would certainly support the ‘Accountability’ Principle and in the absence of a ‘privacy seal’ help demonstrate to Customers and the Regulators GDPR compliance using ISO 27001 and ISO 27002.

The GDPR can be a daunting process for organisations considering the legal complexities and the financial ramifications of a loss of data, but those that were considering ISO 27001, or already have it in place, stand to benefit from a proactive stance to information security. Almost any company that is operating internationally will have to comply with this regulation. As ISO 27001 is internationally and implemented all over the world, it may be the best option to facilitate immediate compliance with GDPR.

For more information on ISO/IEC 27001 and the GDPR, or if you would like to contact us for any other queries please do so on:

T: +44 (0)20 7090 1091
E: bd@gemserv.com
W: www.gemserv.com

@gemservinfosec

London Office:
8 Fenchurch Place
London
EC3M 4AJ

Company Reg. No: 4419878

Gemserv

INVESTORS IN PEOPLE | Gold Until 2020

ISO/IEC 27001 Information Security Management

GlobalGROUP ISO 14001 UKAS 0039

GlobalGROUP ISO 50001 UKAS 0039

ISO 9001 UKAS 001

CYBER ESSENTIALS PLUS