ISO 27001 is a framework for information protection. According to GDPR, personal data is critical information that all organizations need to protect. Of course, there are some EU GDPR requirements that are not directly covered in ISO 27001, such as supporting the rights of personal data subjects: the right to be informed, the right to have their data deleted, and data portability. But, if the implementation of ISO 27001 identifies personal data as an information security asset, most of the EU GDPR requirements will be covered.

ISO 27001 provides the means to ensure this protection. There are many points where the ISO 27001 standard can help companies achieve compliance with this regulation. Here are just a few of the most relevant ones:

- **Risk Assessment** – Because of the high fines defined in EU GDPR and the major financial impact on organizations, it is only natural that the risk found during risk assessment regarding personal data is too high not to be dealt with. On the other side, one of the new requirements of the EU GDPR is the implementation of Data Protection Impact Assessments, where companies will have to first analyze the risks to their privacy, the same as is required by ISO 27001. Of course, while implementing ISO 27001, personal data must be classified as high criticality, but according to the control A.8.2.1 (Classification of information): "Information should be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification." (Read the article ISO 27001 risk assessment & treatment – 6 basic steps to learn more.)
- **Compliance** – By implementing ISO 27001, because of control A.18.1.1 (Identification of applicable legislation and contractual requirements), it is mandatory to have a list of relevant legislative, statutory, regulatory, and contractual requirements. If the organization needs to be compliant with EU GDPR (see section above), this regulation will have to be part of this list. In any case, even if the organization is not covered by the EU GDPR, control A.18.1.4 (Privacy and protection of personally identifiable information) of ISO 27001 guides organizations through the implementation of a data policy and protection of personally identifiable Information.
- **Breach notification** – Companies will have to notify data authorities within 72 hours after a breach of personal data has been discovered. 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." According to EU GDPR, data subjects ("The Data Subject is a living individual to whom personal data relates.") will also have to be notified, but only if the data poses a "high risk to data subject's rights and freedom." The implementation of incident management, which results in detection and reporting of personal data incidents, will bring an improvement to the organization wishing to conform to GDPR.
- **Asset Management** – ISO 27001 control A.8 (Asset Management) leads to inclusion of personal data as information security assets and allows organizations to understand what personal data is involved and where to store it, how long, what is its origin, and who has access, which are all requirements of EU GDPR.
- **Privacy by Design** – The adoption of Privacy by Design, another EU GDPR requirement, becomes mandatory in the development of products and systems. ISO 27001 control A.14 (System acquisitions, development and maintenance) ensures that "information security is an integral part of information systems across the entire lifecycle."

- **Supplier Relationships** – ISO 27001 control A.15.1 (Information security in supplier relationships) requires the "protection of the organization's assets that are accessible by suppliers." According to GDPR, the organization delegates suppliers' processing and storage of personal data; it shall require compliance with the requirements of the regulation through formal agreements.

Is ISO 27001 enough?

In addition to the adopted technical controls, structured documentation, monitoring, and continuous improvement, the implementation of ISO 27001 promotes a culture and awareness of security incidents in organizations. The employees of these organizations are more aware and have more knowledge to be able to detect and report security incidents. Information security is not only about technology; it's also about people and processes.

The ISO 27001 standard is an excellent framework for compliance with the EU GDPR. If the organization has already implemented the standard, it is at least halfway toward ensuring the protection of personal data and minimizing the risk of a leak, from which the financial impact and visibility could be catastrophic for the organization. The first thing an organization should do is conduct an EU GDPR GAP Analysis to determine what remains to be done to meet the EU GDPR requirements, and then these requirements can be easily added through the Information Security Management System that is already set by ISO 27001.

From the ISO 27000 family, ISO/IEC 27018 should also be consulted (Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors) if the organization stores/processes personal data in the cloud. See the article ISO 27001 vs. ISO 27018 – Standard for protecting privacy in the cloud to learn more.

To summarize, almost any company that is operating internationally will have to comply with this regulation. As ISO 27001 is internationally recognized and implemented all over the world, it may be the best option to facilitate immediate compliance with EU GDPR.

1. Risk assessment methodology

This is the first step on your voyage through risk management. You need to define rules on how you are going to perform the risk management because you want your whole organization to do it the same way – the biggest problem with risk assessment happens if different parts of the organization perform it in a different way. Therefore, you need to define whether you want qualitative or quantitative risk assessment, which scales you will use for qualitative assessment, what will be the acceptable level of risk, etc.

2. Risk assessment implementation

Once you know the rules, you can start finding out which potential problems could happen to you – you need to list all your assets, then threats and vulnerabilities related to those assets, assess the impact and likelihood for each combination of assets/threats/vulnerabilities and finally calculate the level of risk.

In my experience, companies are usually aware of only 30% of their risks. Therefore, you'll probably find this kind of exercise quite revealing – when you are finished you'll start to appreciate the effort you've made.

3. Risk treatment implementation

Of course, not all risks are created equal – you have to focus on the most important ones, so-called 'unacceptable risks'.

There are four options you can choose from to mitigate each unacceptable risk:

1. Apply security controls from Annex A to decrease the risks – see this article ISO 27001 Annex A controls.
2. Transfer the risk to another party – e.g. to an insurance company by buying an insurance policy.
3. Avoid the risk by stopping an activity that is too risky, or by doing it in a completely different fashion.
4. Accept the risk – if, for instance, the cost for mitigating that risk would be higher that the damage itself.

This is where you need to get creative – how to decrease the risks with minimum investment. It would be the easiest if your budget was unlimited, but that is never going to happen. And I must tell you that unfortunately your management is right – it is possible to achieve the same result with less money – you only need to figure out how.

4. ISMS Risk Assessment Report

Unlike previous steps, this one is quite boring – you need to document everything you've done so far. Not only for the auditors, but you may want to check yourself these results in a year or two.

5. Statement of Applicability

This document actually shows the security profile of your company – based on the results of the risk treatment you need to list all the controls you have implemented, why you have implemented them and how. This document is also very important because the certification auditor will use it as the main guideline for the audit.

For details about this document, see article The importance of Statement of Applicability for ISO 27001.

6. Risk Treatment Plan

This is the step where you have to move from theory to practice. Let's be frank – all up to now this whole risk management job was purely theoretical, but now it's time to show some concrete results.

This is the purpose of Risk Treatment Plan – to define exactly who is going to implement each control, in which timeframe, with which budget, etc. I would prefer to call this document 'Implementation Plan' or 'Action Plan', but let's stick to the terminology used in ISO 27001.

Once you've written this document, it is crucial to get your management approval because it will take considerable time and effort (and money) to implement all the controls that you have planned here. And without their commitment you won't get any of these.

And this is it – you've started your journey from not knowing how to setup your information security all the way to having a very clear picture of what you need to implement. The point is – ISO 27001 forces you to make this journey in a systematic way.

P.S. ISO 27005 – how can it help you?

ISO/IEC 27005 is a standard dedicated solely to information security risk management – it is very helpful if you want to get a deeper insight into information security risk assessment and treatment – that is, if you want to work as a consultant or perhaps as an information security / risk manager on a permanent basis. However, if you're just looking to do risk assessment once a year, that standard is probably not necessary for you.

Annex A of ISO 27001 is probably the most famous annex of all the ISO standards – this is because it provides an essential tool for managing security: a list of security controls (or safeguards) that are to be used to improve security of information.

It would be a violation of intellectual property rights if I listed all the controls here, but let me just explain how the controls are structured, and the purpose of each of the 14 sections from Annex A:

- **A.5 Information security policies** – controls on how the policies are written and reviewed

- **A.6 Organization of information security** – controls on how the responsibilities are assigned; also includes the controls for mobile devices and teleworking
- **A.7 Human resources security** – controls prior to employment, during, and after the employment
- **A.8 Asset management** – controls related to inventory of assets and acceptable use, also for information classification and media handling
- **A.9 Access control** – controls for Access control policy, user access management, system and application access control, and user responsibilities
- **A.10 Cryptography** – controls related to encryption and key management
- **A.11 Physical and environmental security** – controls defining secure areas, entry controls, protection against threats, equipment security, secure disposal, clear desk and clear screen policy, etc.
- **A.12 Operational security** – lots of controls related to management of IT production: change management, capacity management, malware, backup, logging, monitoring, installation, vulnerabilities, etc.
- **A.13 Communications security** – controls related to network security, segregation, network services, transfer of information, messaging, etc.
- **A.14 System acquisition, development and maintenance** – controls defining security requirements and security in development and support processes
- **A.15 Supplier relationships** – controls on what to include in agreements, and how to monitor the suppliers
- **A.16 Information security incident management** – controls for reporting events and weaknesses, defining responsibilities, response procedures, and collection of evidence
- **A.17 Information security aspects of business continuity management** – controls requiring the planning of business continuity, procedures, verification and reviewing, and IT redundancy
- **A.18 Compliance** – controls requiring the identification of applicable laws and regulations, intellectual property protection, personal data protection, and reviews of information security

One of the biggest myths about ISO 27001 is that it is focused on IT – as you can see from the above sections, this is not quite true: while IT is certainly important, IT alone cannot protect information. Physical security, legal protection, human resources management, organizational issues – all of them together are required to secure the information.

The best way to understand Annex A is to think of it as a catalogue of security controls you can select from – out of the 114 controls that are listed in Annex A, you can choose the ones that are applicable to your company.

Relationship to the main part of ISO 27001

So, not all of these 114 controls are mandatory – a company can choose for itself which controls it finds applicable and then it must implement them (in most cases, at least 90% of the controls are applicable); the rest are declared to be non-applicable. For example, control*A.14.2.7 Outsourced development* can be marked as non-applicable if a company does not outsource the development of software. The main criterion for selecting the controls is through risk management, which is defined in clauses 6 and 8 of the main part of ISO 27001. Learn more here: ISO 27001 risk assessment & treatment – 6 basic steps.

Further, clause 5 of the main part of ISO 27001 requires you to define responsibilities for managing those controls, and clause 9 requires you to measure if the controls have fulfilled their purpose. Finally, clause 10 requires you to fix anything that is wrong with those controls, and to make sure that you achieve information security objectives with those controls.

Relationship to ISO 27002

The truth is that Annex A of ISO 27001 does not give too much detail about each control. There is usually one sentence for each control, which gives you an idea on what you need to achieve, but not how to do it. This is the purpose of ISO 27002 – it has exactly the same structure as ISO 27001 Annex A: each control from Annex A exists in ISO 27002, together with a more detailed explanation on how to implement it. But don't fall into the trap of using only ISO 27002 for managing your information security – it does not give you any clues as to how to select which controls to implement, how to measure them, how to assign responsibilities, etc. Learn more here: ISO 27001 vs. ISO 27002.

Usability of Annex A

There are a couple of things I like about Annex A – it gives you a perfect overview of which controls you can apply so that you don't forget some that would be important, and it gives you the flexibility to choose only the ones you find applicable to your business so that you don't have to waste resources on the ones that are not relevant to you.

It is true that the Annex A doesn't give you too much detail on implementation, but this is where ISO 27002 comes in; it is also true that some companies might abuse the flexibility of ISO 27001 and aim only for the minimum controls in order to pass the certification, but this is a topic for a different blog post.