Information security for agile companies

Over the course of the past 10 years, information security has become a top priority for every company. This is particularly due to the continual increase in companies offering online services that store and manage confidential information. Information security standards, such as ISO 27001, provide a framework of policies and procedures to help organizations handle such information securely.

Two key questions emerge during the implementation of ISO 27001

1. What challenges can you face implementing security standards when you are a rapidly growing company focused on Agile software development?

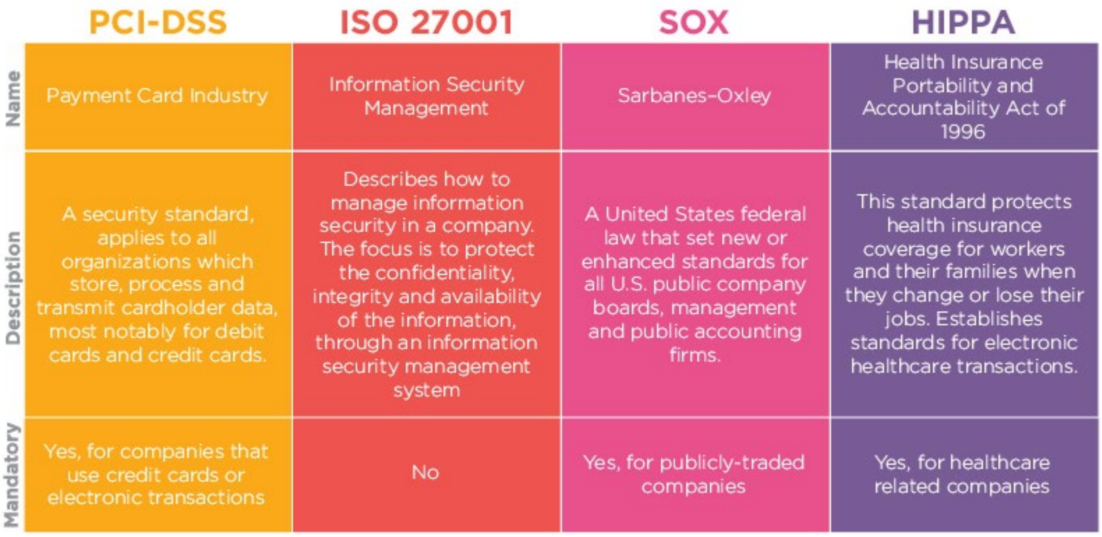
2. How can you align your treatment of information risk with Agile methodologies?

In this whitepaper we outline Belatrix's experience implementing the standard ISO 27001 for information security, and in doing so, answer these two key questions.

Why ISO 27001?

While there are several security standards available for companies, Belatrix chose the ISO 27001 standard because it helps to manage the security of all company assets such as: financial information, intellectual property, employee personal information, and also information entrusted to Belatrix by third parties (i.e. clients). It also creates the base with which to align processes with many other security standards, and covers in a more general way the security requirements to ensure that the information managed in the company is secure.

The most important information security standards



	PCI-DSS	ISO 27001	SOX	HIPPA
Name	Payment Card Industry	Information Security Management	Sarbanes-Oxley	Health Insurance Portability and Accountability Act of 1996
Description	A security standard, applies to all organizations which store, process and transmit cardholder data, most notably for debit cards and credit cards.	Describes how to manage information security in a company. The focus is to protect the confidentiality, integrity and availability of the information, through an information security management system	A United States federal law that set new or enhanced standards for all U.S. public company boards, management and public accounting firms.	This standard protects health insurance coverage for workers and their families when they change or lose their jobs. Establishes standards for electronic healthcare transactions.
Mandatory	Yes, for companies that use credit cards or electronic transactions	No	Yes, for publicly-traded companies	Yes, for healthcare related companies

What is a risk and how to identify them?

A risk is an event or series of events related to information security, that have a possibility of compromising business operations, and represents a threat to company information.

But, how do we know what is, and what is not, a risk?

To answer this, the standard defines three important aspects that, if an asset were affected by, then it must be considered as a risk. The aspects are:

- **Confidentiality:** Ensures information can only be accessed by individuals with authorization.

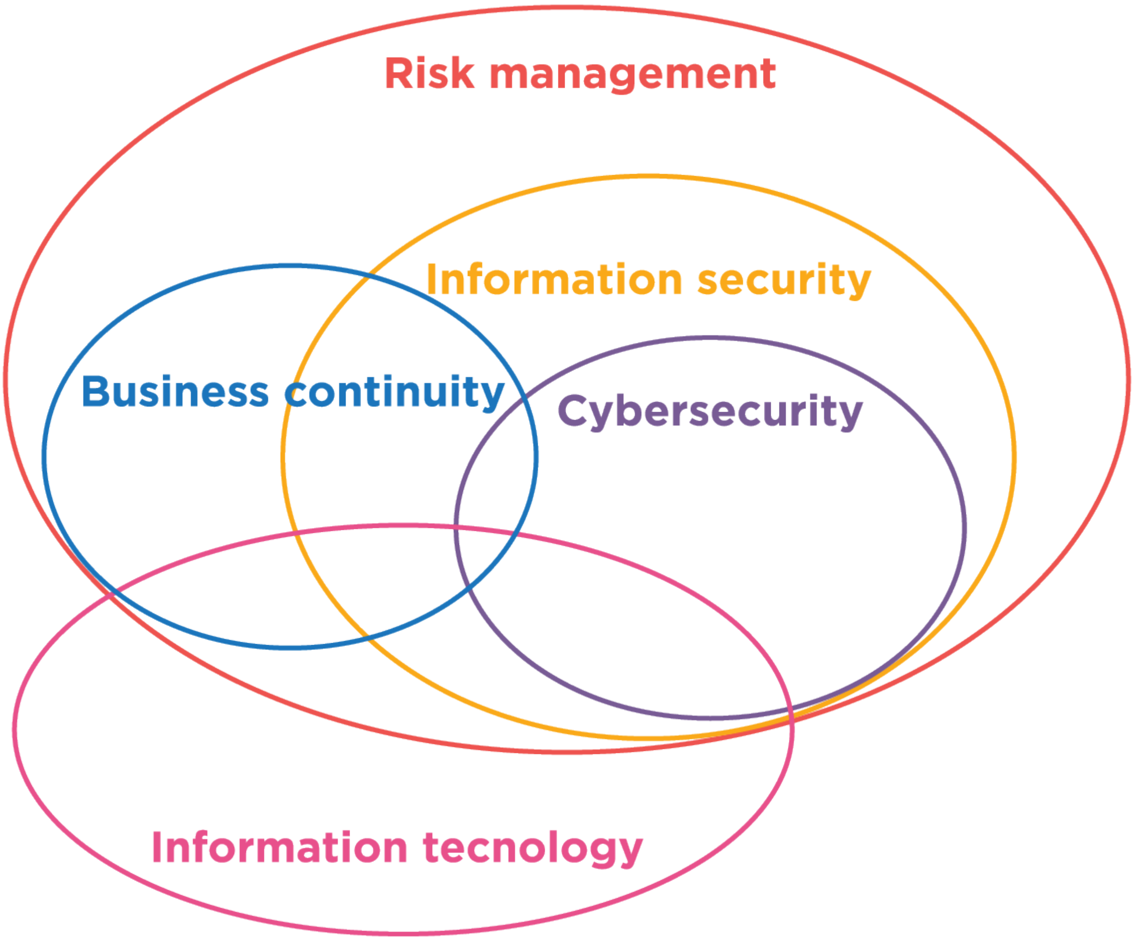
- **Integrity:** Involves maintaining the consistency, accuracy, and trustworthiness of data.

- **Availability:** Ensures that information is available when it’s needed.

ISO 27001 also emphasizes the importance of protecting information assets. This refers to every system, tool, service, document or person that stores confidential information and has value to the organization. Information security risks should be identified for every asset of the company.

Incidents have a major role here too, and they should be prioritized and managed. An incident is defined as an active information security breach. This could be the materialization of a detected risk, or one that hasn’t been detected or managed yet. In either case, if an incident occurs, it affects an asset.

As you can see, risk management serves as the base layer in the information security framework of every company.



Aligning the treatment of information security risks with Agile

After deciding which standard we should adhere to, we came up against with another challenge. This was the fact that we are a company growing rapidly, maturing, and which focuses on the Agile software development methodology. This is why we needed to find a method to ensure that the risk treatment strategy could be aligned with Agile practices.

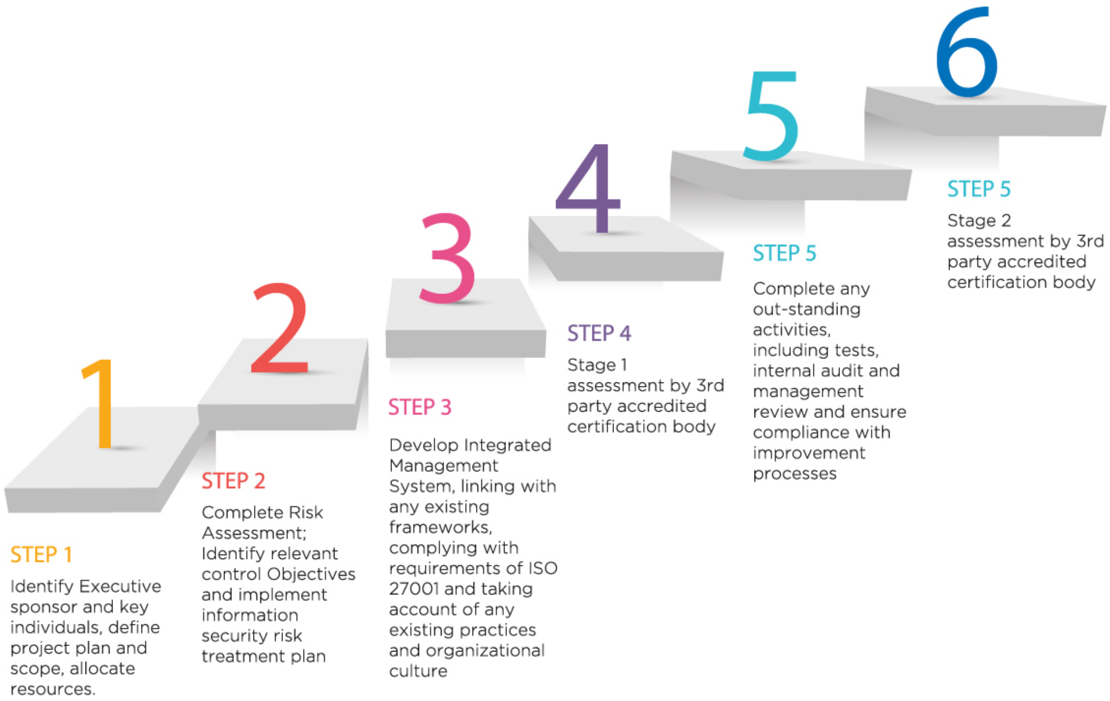
At the beginning of this process we considered using a spreadsheet to manage assets, risks and incidents. However we realized that this spreadsheet would rapidly grow to the point of being unmanageable. Thanks to our experience in Agile, we believed that the use of an issue tracker which was Agile-oriented, would allow us to better manage the Information Security Management System (ISMS). We can define an ISMS as a set of policies and procedures that guides the organization on how to manage confidential information.

At first, it was hard to parameterize and set the issue tracker, but after a couple of months, the use of this tool allowed us to link risks, assets and incidents, and classify and prioritize them. It also enabled us to assign an impact, probability, and exposure to all risks (we also created a Wiki where we can store and explain all the procedures to manage risks and share related information).

Certification process and result

Once we completed the information security programme required to certify ISO 27001 and filled up our ISMS with risks, incidents, assets, and processes, we achieved the audit requirements, and we obtained the ISO 27001 certification. The external auditors highlighted as a "strength" the use of an issue tracker for managing the ISMS (the auditors also commented that many companies choose to buy an expensive tool or use a spreadsheet to do this job, which typically don't have good results).

The following image details the certification process step by step:



STEP 1
Identify Executive sponsor and key individuals, define project plan and scope, allocate resources.

STEP 2
Complete Risk Assessment; Identify relevant control Objectives and implement information security risk treatment plan

STEP 3
Develop Integrated Management System, linking with any existing frameworks, complying with requirements of ISO 27001 and taking account of any existing practices and organizational culture

STEP 4
Stage 1 assessment by 3rd party accredited certification body

STEP 5
Complete any out-standing activities, including tests, internal audit and management review and ensure compliance with improvement processes

STEP 5
Stage 2 assessment by 3rd party accredited certification body

After 3 years of maturing the security process, we took one step further, and made changes to improve our risk management strategy. We created an "Information Security Committee", where members from different parts of the company are tasked with managing the risks related to the area of their responsibility. This improvement brought major enhancements including:

- More people involved in working on the ISMS, as area responsibilities and designated collaborators.

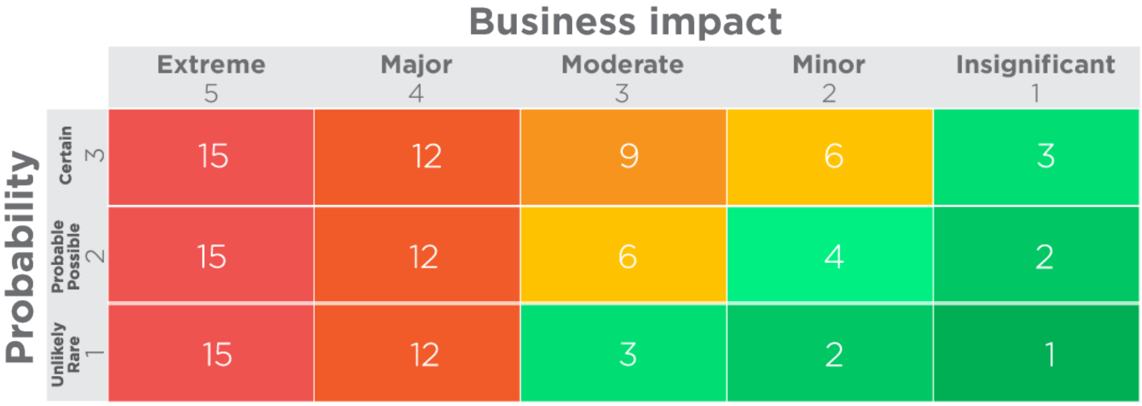
- Enabled us to manage the system better and gain visibility into which risks we should attend to first, the amount of assets that we are protecting, and incidents that were being avoided.

Risks prioritization: Which should you attend to first and why?

The issue tracker tool allows us to define a strategy where we are able to measure risk exposure, based on how information risk affects the running of the company. This tells us how urgently we should attend to risks.

We've developed a risk matrix with two axes: business impact and probability. For assessing the business impact we developed a ranking of 1 (insignificant) to 5 (extreme). For assessing probability, the ranking is from 1 (unlikely/rare) to 3 (certain). Multiplying these two values together, determines the risk exposure. Risks with an exposure of 15 must be treated immediately. We set a value (i.e. 3) where every value below it, it's not mandatory to handle them.

Note: If a risk is assessed as having a business impact of 4 or 5, it's treated as having the maximum probability to ensure it's solved as soon as possible.



Probability	Business impact Extreme 5	Major 4	Moderate 3	Minor 2	Insignificant 1
Certain 3	15	12	9	6	3
Probable Possible 2	15	12	6	4	2
Unlikely Rare 1	15	12	3	2	1

Conclusion

The implementation of these kind of standards are important for every company. They settle new rules, processes and ways of working. In this case it's to protect one of the most valuable assets of every company, information. This is not a task you do just once - rather it is a process that should be continuously improving, ensuring awareness of new risks, and managing them properly. Creating a process where you continuously ensure that information is more secure and more reliable on each iteration.