Step-by-step explanation of ISO 27001/ISO 27005 risk management

Making certification simple.

Table of Contents

Introduction

Businesses are full of risks, and to ensure competitiveness and the achievement of objectives, organizations should do their best to identify, evaluate, and treat all of them – or, at least, the most relevant ones. This is called risk management, which can vary from subconscious decisions to fully aware choices based on complex methodologies and data arrangements, applicable to a wide variety of risk fields, including risks related to information security.

The very nature of risks makes risk management a complex job, but it is often mystified unnecessarily, and many organizations make this process even more difficult by adopting needless or extremely complex activities.

This white paper helps you implement ISO 27001 risk management and ISO 27005 compliance, explaining the basic elements of both risk assessment and risk treatment, with tips on how to implement them in a cost-effective way to benefit your organization while protecting sensitive and critical business information.

ISO 27001 risk assessment & treatment – 6 basic steps

Although risk assessment and treatment is a complex job, it can be summarized in these 6 basic steps:

1. ISO 27001 risk assessment methodology: You need to define rules for how you are going to perform the risk assessment to ensure that the whole organization does it the same way.

2. Risk assessment implementation: Once you know the rules, you can start identifying the potential problems that could arise, and determining which ones are unacceptable and have to be treated – you need to identify, analyze, and evaluate the risks.

3. Risk treatment implementation: This is where you need to get creative and figure out how to decrease the risks with minimal investment. It is possible to achieve the same result with less money – and this paper will show you ways to do just that.

4. ISMS Risk Assessment Report: Unlike the previous steps, this one is quite boring – you need to document everything you've done so far. You aren't only doing this for the auditors; you may want to check out these results for yourself in a year or two.

5. Statement of Applicability: This document summarizes the results of the risk treatment. It is very important, because the certification auditor will use it as the main guideline for the audit.

6. Risk Treatment Plan: This is the step where you have to move from theory to practice, going from a purely theoretical job to showing some concrete results. You'll need to define exactly who is going to implement each control, in what timeframe, within what budget, etc.

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

The following sections will provide more details about how to implement each step, considering the most common approaches used by companies around the world.

For additional information, consider attending this webinar: The basics of risk assessment and treatment according to ISO 27001.

How to write the risk assessment methodology

ISO 27001 requirements are not very difficult – here is what clause 6.1.2 requires, and some commonly adopted approaches:

Requirement	Common approaches
1) Define how to identify the risks that could cause the loss of confidentiality, integrity, and/or availability of your information.	You can identify risks based on assets, threats, and vulnerabilities, based on your processes, based on your departments, using only threats and not vulnerabilities, or any other methodology you like.
2) Define how to identify the risk owners.	You should choose a person who is both interested in resolving a risk and positioned highly enough in the organization to do something about it.
3) Define criteria for assessing consequences and assessing the likelihood of the risk.	You should assess separately the consequences and likelihood for each of your risks, but you are completely free to use whichever scales you like.
4) Define how the risk will be calculated.	This is usually done through addition (e.g., 2 + 5 = 7) or through multiplication (e.g., 2 x 5 = 10). If you use a scale of Low-Medium-High, this would be the same as using a scale of 1-2-3, so you still have numbers for calculation.
5) Define the criteria for accepting risks.	If your method of risk calculation produces values from 2 to 10, then you can decide that an acceptable level of risk is, e.g., 7 – this would mean that only the risks valued at 8, 9, and 10 would need treatment. Alternatively, you can examine each individual risk and decide which should be treated or not based on your own insight and experience, using no pre-defined values.

It is important to note that:

- Anything less than one of the approaches described for each requirement won't be enough, but more importantly – anything more is not needed, which means you should try not to complicate things too much; and
- You need to ensure that the risk assessment results are consistent – that is, you have to define a methodology that will produce comparable results in all the departments of your company.

To see what a Risk Assessment and Treatment Methodology document looks like, see this free demo: Risk Assessment and Risk Treatment Methodology.

Risk assessment: How to match assets, threats and vulnerabilities

The 2022 revision of ISO 27001 allows you to identify risks using any methodology you like; however, the old methodology (defined by the old 2005 revision of ISO 27001), which requires identification of assets, threats, and vulnerabilities, continues to dominate.

Risk identification is the first half of the risk assessment process, and to make your risk assessment easier, you can use a sheet listing assets, threats, and vulnerabilities in columns; you should also include additional information like risk ID, risk owners, impact and likelihood, etc.

We recommend listing items column by column, not row by row – this means you should list all of your assets first, and only then start finding a couple of threats for each asset, and finally find a couple of vulnerabilities for each threat.

To learn which types of assets you should take into account, read this article: Asset management according to ISO 27001: How to handle an asset register / asset inventory, and click here to see a catalog of threats and vulnerabilities appropriate for smaller and mid-sized companies.

Here are some examples of what this matching of the three components could look like:

Asset: paper document

- Threat: fire; vulnerability: document is not stored in a fire-proof cabinet (risk related to the loss of availability of the information)
- Threat: fire; vulnerability: there is no backup of the document (potential loss of availability)

- Threat: unauthorized access; vulnerability: document is not locked in a cabinet (potential loss of confidentiality)

Asset: digital document

- Threat: disk failure; vulnerability: there is no backup of the document (potential loss of availability)
- Threat: virus; vulnerability: anti-virus program is not properly updated (potential loss of confidentiality, integrity, and availability)
- Threat: unauthorized access; vulnerability: access control scheme is not properly defined (potential loss of confidentiality, integrity, and availability)
- Threat: unauthorized access; vulnerability: access was given to too many people (potential loss of confidentiality, integrity, and availability)

Asset: system administrator

- Threat: unavailability of this person; vulnerability: there is no replacement for this position (potential loss of availability)
- Threat: frequent errors; vulnerability: lack of training (potential loss of integrity and availability)
- Etc.

Some people prefer using tools for this kind of work, and we agree this could be a good move for larger companies; but, for smaller ones, using a tool would only take too much time – see an explanation here: Toolkits vs. Conformio – Which is more applicable for my company?

Regarding how many risks a company should identify, you should focus only on the most important threats and vulnerabilities, while including all the assets, and a good start would be that per each asset, you should identify on average five threats, and for each threat, an average of two vulnerabilities. This way, you would end up with 500 risks for a smaller company with 50 assets, which is quite manageable.

How to assess consequences and likelihood in risk analysis

The second half of the risk assessment is to calculate how big the risk is – this is achieved through assessing the consequences (also called the impact) that would occur if the risk were to materialize, and assessing how likely the risk is to happen; with this information, you can easily calculate the level of risk.

There are basically two main approaches for assessing likelihood and consequences: qualitative and quantitative.

In qualitative risk assessment, the focus is on interested parties' perceptions about the probability of a risk occurring, and the impact on relevant organizational aspects (e.g., financial, reputational, etc.). This perception is represented in scales such as "low – medium – high" or "1 – 2 – 3," which are used to define the final value of the risk.

On the other hand, quantitative risk assessment focuses on factual and measurable data, and highly mathematical and computational bases, to calculate probability and impact values, normally expressing risk values in monetary terms.

If your company needs quick and easy risk assessment, you can go with qualitative assessment (and this is what 99% of companies do). However, if you need to make a really big investment that is critical for security, perhaps it makes sense to invest time and money into quantitative risk assessment. One way to justify the required investment for security is by identifying the costs of an incident, as well as the potential returns this investment could bring to the organization. (Take a look at this Free Return on Security Investment Calculator.)

Qualitative risk assessment also includes two ways to analyze the risks: simple risk assessment and detailed risk assessment.

In simple risk assessment, you assess the consequences and the likelihood directly – once you identify the risks, you simply have to use scales to assess separately the consequences and the likelihood of each risk. For example, you can use the scale of 0 to 4, where 0 would be very low, 1 low, 2 medium, and so on, or the scale 1 to 10, or Low-Medium-High, or any other scale. The larger the scale, the more precise the results you will have, but also the more time you will spend performing the assessment.

So, for example, in simple risk assessment you might have something like this:

- Asset: laptop
- Threat: theft
- Vulnerability: employees do not know how to protect their mobile devices
- Consequences: 3 (on a scale from 0 to 4)
- Likelihood: 4 (on a scale from 0 to 4)

In detailed risk assessment, instead of assessing two elements (consequences and likelihood), you assess three elements: asset value, threat, and vulnerability. So, here's an example of this detailed risk assessment:

- Asset: laptop
- Threat: theft
- Vulnerability: employees do not know how to protect their mobile devices
- Asset value: 3 (on a scale from 0 to 4)
- Threat value: 2 (on a scale from 0 to 2)
- Vulnerability value: 2 (on a scale from 0 to 2)

Again, calculating risk is actually very simple – this is usually done through addition (e.g., 2 + 5 = 7) or through multiplication (e.g., 2 x 5 = 10). If you use a Low-Medium-High scale, then this is the same as using 0-1-2, so you still have numbers for calculation.

So, using the above examples, here is how to calculate the risk using addition:

- Simple risk assessment: Consequences (3) + Likelihood (4) = Risk (7)
- Detailed risk assessment: Asset value (3) + Threat value (2) + Vulnerability value (2) = Risk (7)

In the detailed risk assessment, you'll notice that I used the scale 0 to 4 for assessing the asset value, and smaller scales of 0 to 2 for assessing threats and vulnerabilities. This is because the weight of the consequence should be the same as the weight of the likelihood – because threats and vulnerabilities jointly "represent" the likelihood, their maximum added value is 4, the same as for the consequence value.

After you've calculated the risks, you have to evaluate whether they are acceptable or not, and then move on to the next step: the risk treatment.

Implementing information security risk treatment

The purpose of risk treatment is to control the risks identified during the risk assessment; in most cases, this would mean to decrease the risk by reducing the likelihood of an incident (e.g., by using non-flammable building materials), and/or to reduce the impact on assets (e.g., by using automatic fire-suppression systems). During the risk treatment the organization should focus on those risks that are not acceptable; otherwise, it would be difficult to define priorities and to finance the mitigation of all the identified risks.

Usually, risk treatment options are to:

1. **Decrease the risk** – this option is the most common, and it includes implementation of safeguards (controls) – like fire-suppression systems, etc. For that purpose, the controls from ISO 27001 Annex A are used (and any other controls that a company thinks are appropriate). See here how the controls are organized: Understanding the ISO 27001 controls from Annex A.
2. **Avoid the risk** – stop performing certain tasks or processes if they incur such risks that are simply too big to mitigate with any other options – e.g., you can decide to ban the usage of laptops outside of the company premises if the risk of unauthorized access to those laptops is too high (because, e.g., such hacks could halt the complete IT infrastructure you are using).
3. **Share the risk** – this means you transfer the risk to another party – e.g., you buy an insurance policy for your building against fire, thereby transferring part of your financial risk to an insurance company. Unfortunately, this option does not have any influence on the incident itself, so the best strategy is to use this option together with options 1) and/or 2).
4. **Retain the risk** – this is the least desirable option, and it means your organization accepts the risk without doing anything about it. This option should be used only if the mitigation cost would be higher than the damage an incident would incur.

When you decide on the option of decreasing the risk, you have to implement controls, and there are three basic types of controls from which you can select:

1. **Definition of new rules:** rules are documented through plans, policies, procedures, instructions, etc., although you don’t have to document some less-complex processes.
2. **Implementation of new technology:** for example, backup systems, disaster recovery locations for alternative data centers, etc.
3. **Change of the organizational structure:** in some cases, you will need to introduce a new job function, or change the responsibilities of an existing position.

To increase the chances of selecting the most effective treatment options and controls, you should consider involving specialists in the related areas (e.g., IT personnel for IT-related controls; human resource specialists if treatment involves trainings, etc.).

Of course, the final decision about any new treatment option will require input from the appropriate management level (e.g., CISO, project team, department head in charge, top executive, etc.). If you have doubts regarding who can decide what, consult with your project sponsor.

Once the treatment is chosen, you have to assess the residual risk for every unacceptable risk identified earlier during risk assessment. So, for instance, if you had identified a consequence of level 4 and likelihood of level 5 during your risk assessment (which would mean risk of 9 by the method of addition), your residual risk may be 5 if you assessed that the consequence would lower to 3 and likelihood to 2 due to, e.g., safeguards you planned to implement.

To see a general view of the Risk Assessment and Risk Treatment, see this free Diagram of ISO 27001 Risk Assessment and Treatment process.

Once risk treatment is finished, you can summarize the risk assessment and treatment in a Risk Assessment and Treatment Report, to give a detailed overview of the process and fulfill the standard's requirements for retaining information about the risk assessment and treatment process (clauses 6.1.2 and 6.1.3). To see what a Risk Assessment and Treatment Report looks like, see this free demo: Risk Assessment and Treatment Report.

The importance of the Statement of Applicability

The Statement of Applicability (ISO 27001 Clause 6.1.3 d) is the main link between the risk assessment & treatment and the implementation of your information security. In it, you will need to:

- Identify the controls that are necessary for reasons other than any identified risks (e.g., because of legal or contractual requirements, because of other processes, etc.).
- Justify the inclusion and exclusion of controls from Annex A, as well as the inclusion of controls from other sources.
- Record a summarized form of applicable controls (93 from Annex A, plus any additional ones), to present it to management and to keep it up to date.
- Document whether each applicable control is already implemented or not. Good practice (and most auditors will be looking for this) is also to describe how each applicable control is

implemented – e.g., either by making a reference to a document (policy/procedure/working instruction, etc.), or by briefly describing the procedure in use or equipment that is used.

The comprehensive view provided by the Statement of Applicability (what needs to be done in information security, why it has to be done, and how it is done) has at least these benefits:

- It forces organizations to plan their security in a systematic way, optimizing decisions regarding expenses (e.g., buy new equipment? Or change the procedure? Or hire a new employee?).
- A well-written Statement of Applicability can decrease the number of other documents – for instance, if you want to document a certain control, but the description of the procedure for that control would be rather short, you can describe it in the Statement of Applicability and avoid writing another document.
- It provides auditors with guidance to understand the organization's security approach and to check whether you have implemented your controls in the way that was planned. It is the central document for conducting their on-site audit.

To see what a Statement of Applicability looks like, see this free demo: Statement of Applicability.

The Risk Treatment Plan

To start thinking about the Risk Treatment Plan, it would be easier to think of it as an "Action Plan" in which you need to specify which security controls you need to implement, who is responsible for them, what the deadlines will be, and which resources (i.e., financial and human) are required.

As an output of the risk treatment process, the Risk Treatment Plan must be written after the Statement of Applicability, because this document defines the controls that need to be implemented, given a comprehensive picture of information security, considering not only the result of risk treatment, but also legal, regulatory, and contractual requirements, other business needs, etc.

To conclude – the Risk Treatment Plan is the point where theory stops, and real life begins according to ISO 27001. A good risk assessment and risk treatment process, as well as a comprehensive Statement of Applicability, will produce a very usable action plan for your information security implementation; skip some of these steps, and the Risk Treatment Plan will only confuse you.

To see what a Risk Treatment Plan looks like, see this free demo: Risk Treatment Plan.

How does information security risk management really help?

No organization is free of risks, and the increase in international and local regulatory requirements (e.g., EU GDPR and California's CCPA), and internal issues like the need for highly efficient, reliable operations, play vital roles in motivating firms to determine wisely which risks to accept, and which are unacceptable.

By adopting a security risk management approach, companies can benefit from:

- A strategic approach to risk management: this involves creating and allocating resources in the right place, in the right way, and at the right time over time, considering not only the company's needs, but also those of its customers and other interested parties.
- Clear roles: top management, technical staff, final users, experts – all people involved with information security must have defined functions (e.g., make decisions, identify risks, follow procedures, etc.). This is one of the most cost-effective ways to decrease information security risks, because each person will know what is expected from them.
- Actions appropriate to the perceived threats: the same risk scenario may lead to different approaches by different companies, depending upon their needs and expectations, so just copying another's approach is unwise. Companies have to consider and define their own limits, so their actions toward risks will be aligned with their objectives.

For a comprehensive view of ISO 27001, see this ISO 27001 Foundations Course.

Conclusion

Risk is about the "effect of uncertainty on objectives," so if you manage uncertainty in any way, then you can effectively decrease risk to your business.

In terms of the ISO 27001 standard, this means that information can be protected effectively and used to help a business achieve its goals. By systematically identifying, analyzing, evaluating, and treating a comprehensive list of relevant risks, undesired situations can be prevented, and negative impacts minimized.

In short, by defining and performing risk management, you effectively find out about potential problems before they actually happen. In other words, ISO 27001 risk management reminds you: Better safe than sorry.

Check out ISO 27001 compliance software

To see how to use the ISO 27001 risk register with catalogs of assets, threats, and vulnerabilities, and get automated suggestions on how they are related, sign up for a free trial of Conformio, the leading ISO 27001 compliance software.

Advisera Expert Solutions Ltd
for electronic business and business consulting

Our offices:
Zavizanska 12, 10000 Zagreb, Croatia
Via Maggio 1 C, Lugano, CH-6900, Switzerland
275 Seventh Ave, 7th Floor, New York, 10001, U.S.

Email: support@advisera.com