

A practical guide to risk management in SMEs

Asociación española de gestión de
riesgos y seguros AGERS



agers

About this guide:

This guide has been produced by Asociación Española de Gerentes de Riesgos y Seguros (**AGERS**)¹, based on the belief that risk management should be straightforward, useful and accessible to all businesses. When used effectively, it is a competitive advantage that creates value for any type of business. Historically, large companies and the most heavily regulated sectors have had standardised mechanisms and tools for proactive risk management; these mechanisms can also be implemented in small and medium-sized enterprises by following a structured approach.



In this context, this guide, led **by Edgar García** (AGERS regional representative for Catalonia), **Alicia Soler** (AGERS coordinator for the Guide) and with the support of a team of risk experts comprising **Gemma Giró, Josep Vaque, Enrique Dick and Rodrigo López**, brings together practical insights from companies of different sizes and sectors with a single aim: **to democratise and make accessible to all companies the key principles of risk management that enable them to anticipate problems, reduce surprises and improve long-term resilience.**



Edgar García Corominas



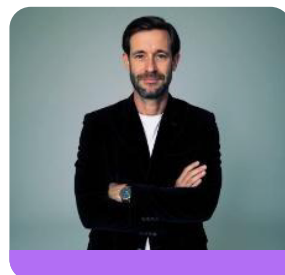
Alicia Soler



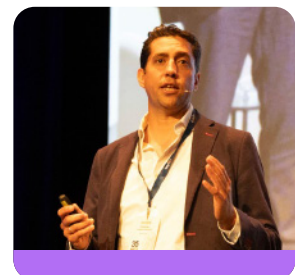
Gemma Giró



Josep Vaque



Enrique Dick



Rodrigo López

In particular, we would like to thank **Víctor García, Eric Álvarez, María Jesús Romero and Laura Piquer** for their work in reviewing, editing and improving the document throughout the editing process.

¹ <https://agers.es/>



Executive summary: What will you find in this guide?

In this practical guide, designed for small and medium-sized enterprises (hereinafter SMEs), you will find the key principles and essence of risk management, tailored to the size and challenges of SMEs, presented in a simple and concise manner across 6 sections:

1

A practical introduction to risk management in SMEs: Find out why anticipating problems can save you thousands of euros and give you peace of mind so you can sleep better.

2

Essential principles – What Every SME Needs to Know: The basics for starting to protect your business without any complications or technical terms. Understand the risks that really matter and how to start managing them.

3

Key risks and how to manage them in practice: Learn how to avoid unpleasant surprises: from defaults to fires. Practical solutions to the most common problems that can bring your business to a standstill.

4

How to implement a risk management system step by step: A clear and straightforward plan to get your business in order in just 90 days. Improve your control, reduce losses and gain an edge over the competition.

5

The insurance programme (transferring risks in a simple way): Protect your business without overspending. We'll explain what insurance you might need (and what you don't need, but might find useful), how to save on premiums, and how to avoid financial surprises.

6

Financing tools and the benefits of risk management: Do you want to secure better terms from your bank or attract investors? Effective risk management can enhance your financial standing and open up new opportunities.

7

The role of the director: you don't just run the business: You also take on legal responsibilities that can have consequences in criminal law. This section explains which legal risks you need to be aware of and how to protect yourself through prevention, compliance and insurance.



You are about to embark on a journey that will transform the way you make decisions in your business! This guide will give you the keys to anticipating problems, cutting unnecessary costs and gaining peace of mind. Get ready to discover **how to protect your business** and turn risk management into a competitive advantage. Buckle up and enjoy the ride!

Edgar García Corominas

Expert in risk management, internal control, compliance and auditing; ERM Catalonia representative at AGERS

1. A practical introduction to risk management in SMEs

Risk management refers to the set of actions a company takes to anticipate and control potential events that could affect its objectives. Put simply, it involves **identifying what could go wrong** in the business and taking steps to prevent it from happening or, if it does happen, to minimise its impact. In SMEs, this discipline is often overlooked due to the pressures of day-to-day operations or the belief that 'that only happens to large companies'. However, SMEs form the backbone of the economy (accounting for 99.8% of the business sector in Spain) and are particularly vulnerable: data shows that approximately 50% of SMEs close down before reaching their fifth anniversary, often because they have failed to anticipate and manage their risks.

Why is risk management crucial for SMEs? Because it enables you both to avoid losses that could prove fatal and to anticipate events that may affect the bottom line of the profit and loss account. An unforeseen event (a fire, a major default, a serious breakdown, a fine) can jeopardise the survival of a small business with a much greater relative impact than it would have on a large corporation. In fact, SMEs tend to suffer more and take longer to recover from adverse situations than large companies. Implementing basic risk management practices is not a cost, but a strategic investment that safeguards a company's results and business continuity. According to a study² by the United Nations Office for Disaster Risk Reduction (UNDRR), every €1 invested in protection yields a saving of €4. Tangible benefits include the prevention of accidents and losses, cost reduction (through fewer disruptions and optimised insurance premiums), greater financial stability, improved access to finance (banks value companies with good risk management and control) and the peace of mind to undertake projects knowing that 'safety nets' are in place.

99,8%

**of Spanish companies
are SMEs**

SMEs make up the vast majority of the business sector in Spain and account for two out of every three jobs in the country.

50%

**of SMEs close down within
their first 5 years**

Half of all SMEs do not survive beyond their fifth anniversary, often due to a lack of risk planning and financial resilience.

57%

**do not have a risk
mitigation plan**

Fewer than 60% of SMEs have a formal disaster risk reduction strategy, leaving many businesses vulnerable.

² <https://www.undrr.org/es/sobre-undrr/financiamiento>

³ https://ine.es/dyngs/INEbase/es/operacion.htm?c=Estadistica_C&cid=1254736161927&idp=1254735576550

⁴ <https://ipyme.org/Publicaciones/Retrato%20de%20la%20PYME/Retrato-PYME-DIRCE-1-enero-2023.pdf>

Failing to manage risks, on the other hand, often leads to common mistakes that put the company at risk. Some SMEs that lack risk management fall into common pitfalls such as: failing to plan (they only react once a problem has already arisen), ignoring warning signs (minor breaches, client complaints, minor accidents... until a serious incident occurs), failing to allocate resources (neither time nor budget for prevention), and a lack of information (not knowing what insurance cover they have or what legal obligations apply to them, for example). Our aim is that, by the end of this guide, every business will be able to avoid these mistakes and implement a practical approach to risk management suited to its size, without the need for significant expenditure.

In this guide, we will focus on the negative side of risk (threats), addressing the growing strain that the current climate places on the day-to-day operations of SMEs: rapid digitalisation, rising cyber risks, political multilateralism and armed conflicts that escalate overnight. The contents of this guide are intended, as a general guideline, for companies with more than 50 employees and an annual turnover of more than €5 million. Nevertheless, the principles outlined and the essence of the guide are applicable to any smaller business. We will use the example of a fictional waste recovery company, EcoReciclaje, S.A., as a central theme, illustrating in each section how the concepts detailed in this guide would be put into practice.



Let's look at a brief introductory example: EcoReciclaje, S.A. is a (fictitious) SME specialising in the recovery and recycling of industrial waste, with 80 employees. In 2022, it suffered two serious incidents: a minor fire in a warehouse (which halted operations for a week) and the unexpected bankruptcy of its largest client (leaving them with a very large unpaid invoice). This made the owners reflect. They used to think that 'risk management was a luxury for large corporations', but they realised that if they had assessed their risks, they would have discovered: (1) the lack of fire mitigation systems, and (2) a 40% reliance on a single client for their sales. Fortunately, the company survived, albeit with considerable losses. As a result, they decided to implement a basic risk management system.

2. Essential principles - What Every SME Needs to Know

In this chapter, we will cover the basic concepts that form the foundation of risk management. We will clarify some key definitions, present the main categories of risk, and explain how to organise responsibility for risk management within an SME. These fundamentals will help you create a common language within your company for discussing risks.

Firstly, the objectives.

The purpose of risk management is to safeguard the achievement of the organisation's objectives; therefore, **the first essential step is to clearly identify what those key objectives are**. More often than one might think, companies do not have clearly defined objectives, nor do they share these with key personnel, which makes it difficult to align risk management with what really matters. A first step is to clarify and agree on the goals the company aims to achieve (not only financial, but also in terms of quality, regulatory compliance, business continuity, employee and client safety, innovation, etc.) for the coming year, and for the medium to long term, for example 3 years.

Effective risk management is only possible when the organisation is aligned and is completely clear about what it wants to achieve; everyone in the company must know its objectives and row in the same direction. Once defined and integrated, risk management must be incorporated into day-to-day decision-making, always keeping the objectives defined as priorities as the guiding star.

Main risk categories in SMEs.

There are many ways to classify business risks. A useful approach for SMEs is to consider **five broad categories: strategic/governance, operational, financial, compliance and environmental risks**. (Sometimes a sixth category—reputational and third-party risks—is added, which we will discuss briefly later on). Each category groups together certain types of similar threats. The table below summarises the key risk categories and provides some **typical examples** for each:

Risk category	Typical examples risks in SMEs
Strategic risks	Company ownership and succession/transition plans, the threat of new competitors, changes in market preferences or technology, and excessive reliance on a single client or supplier
Operational risks	Workplace accidents, fires or damage to premises, breakdowns of machinery or IT systems, supply chain disruptions, human error and fraud. This category also includes digital and cybersecurity risks: cyberattacks (phishing, ransomware), data loss or theft, and digital fraud.
Financial risks	Lack of liquidity (cash flow issues), client defaults, rising costs (inflation, higher interest rates), currency fluctuations (in the case of exports).

Risk category	Typical examples risks in SMEs
Compliance risks	Non-compliance with laws or regulations: legal penalties or fines, tax issues, reliance on imports, data protection breaches, and breaches of labour or environmental regulations that may result in penalties and legal liability.
Enviromental risks	Extreme weather events (floods, storms, heat waves) that damage facilities or disrupt operations; accidental environmental pollution (spills, emissions) that results in fines or reputational damage.

Note 1:

Reputational risk is often discussed as a category itself. However, the reputational aspect is a consequence of other risks (for example, a case of fraud or a serious accident), not a risk in itself. Reputation is usually affected as a result of other materialised risks (for example, a serious accident, an ethical scandal or quality issues). That is why it is always worth bearing it in mind: when faced with any risk, ask yourself, 'What would happen if this became public? Would people have less confidence in my company?' Similarly, **third-party** (or value chain) **risks** refer to problems experienced by our suppliers, strategic partners or key clients that have an impact on us. The bankruptcy of a critical supplier, for example, is a risk to our company (it affects supply or an outsourced service); similarly, the loss of our best client is a financial risk. In short, we must consider the company's exposure to risks within its ecosystem, not just internal risks.

Note 2:

Among operational risks, it is worth noting that **cyber threats and digital risks** require a very specific approach, as the speed at which they evolve means that all companies (regardless of size) must protect themselves and implement mitigation measures to prevent these risks from materialising. Investing in cyber risk mitigation can make the difference between a major scare and having to close the business.

Every company should draw up at least a **list of its main risks in each category**, prioritising 5 risks on which the company should focus its mitigation efforts (maximum 10 areas). Risk management involves resources, so it is very important to prioritise the most critical risks and gain a **holistic view** of the threats to which you are most exposed.



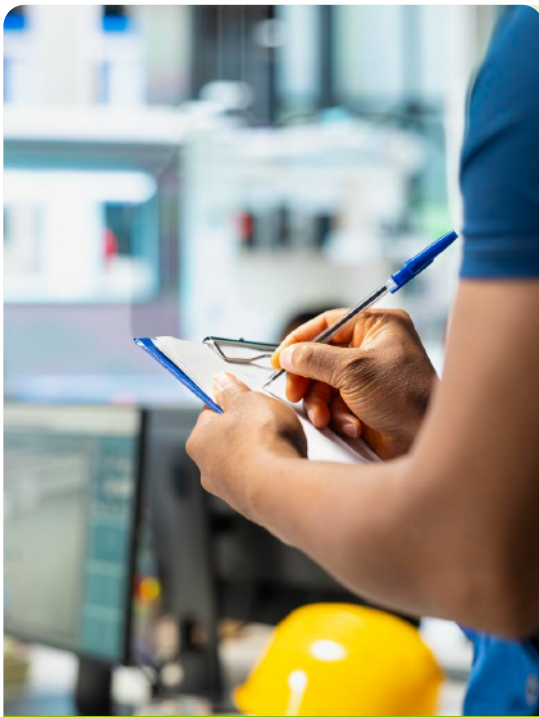
Who should be in charge of risk management in SMEs?

Risk management is the **responsibility of the entire company**, from the business owner down to the lowest-ranking employee. However, it is essential to assign clear responsibilities: otherwise, what belongs to everyone may end up belonging to no one. Given its strategic nature, senior management must be directly involved in key decisions (for example, defining the company's objectives and its risk appetite – that is, how much risk are you willing to take to achieve your objectives? There is no single answer, but it is important that it is a conscious decision). To ensure the process runs smoothly, **it is recommended that an internal manager be appointed to coordinate the implementation and monitoring of risk management**. In small businesses, this could be the owner or managing director themselves; alternatively, the role could be delegated to an existing position (for example, the finance manager for financial and insurance risks, the head of operations for operational risks, etc.). It is essential to have a focal point to drive and oversee the process.



This person (or 'risk coordinator') will be responsible for ensuring the process is implemented and continuously improved. However, specific corrective actions (the work that needs to be done to mitigate the risk) usually fall to the owners of each risk (i.e. those directly responsible for each area, known as the 'front line'). For example, if the risk is a workplace safety issue at the plant, the head of operations, safety and/or production must lead the corrective actions in that area.

Are external resources needed to manage risks? It is not essential to have a dedicated department or to incur significant upfront costs. Many SMEs make use of external support to improve their risk management systems in specialist areas where they need it. For example, a trusted insurance broker can help identify insurable risks and propose suitable cover (not just sell policies), or a consultant, adviser or freelancer can assist with the use of risk assessment methodologies that involve highly technical aspects (occupational safety, cybersecurity, complex legal issues, etc.). This external support is valuable, but it does not replace internal management: business knowledge lies within the company, and risk prevention must be embedded in the day-to-day culture. The most common approach is a combination of in-house staff and external experts, brought in on an ad hoc basis where needed.



Even if you are a small business, it is advisable to review your risk profile on a regular basis. You can incorporate risk discussions into your routine monthly or weekly meetings, taking the opportunity to review past incidents, necessary actions or changes to the most significant risks. This simple habit fosters a culture of prevention and keeps risk management on the management agenda.

Consider bringing in external experts (advisers, consultants) who can provide an outside perspective and a 'challenging' view of this process. If your company is very small, even an informal monthly chat to go over 'what's on our minds this month?' can be useful. The key is to follow this up regularly.

3. Key risks in SMEs and how to manage them in practice

In this section, we will describe some of the risks that most frequently affect SMEs and suggest how to manage them in a concrete manner. Many of these fall into the categories outlined in the previous chapter, but here we will look at them in a more practical way, with basic recommendations for mitigating them.

IMPORTANT:

Every business is different; the idea is for you to identify which of these examples apply to your business and consider what steps you could take. The aim of this document is not to specify the exact risks you need to manage, but to provide you with the tools to adapt them to your specific situation.

Strategic/governance risks

These are factors that could affect long-term objectives or the viability of the business model. For example: the lack of a structured plan for shareholder succession; reliance on a small number of clients (the risk of losing a significant portion of revenue if a key client leaves); new competitors or market changes that could erode your market share; or new technologies or regulations that could render your product or service obsolete.

How should they be managed?

Analyse your business model regularly: diversify as much as possible so as not to 'put all your eggs in one basket' (clients, suppliers, product lines), and keep up to date with trends in your sector to anticipate changes. For example, EcoReciclaje realised it was too dependent on a single client and decided to launch initiatives to expand its commercial portfolio by selling services and by-products, ensuring that no single client accounted for more than 20% of its sales. They also kept a close eye on environmental regulatory changes to adapt before the competition, using a firm specialising in regulatory analysis that provides information on monthly updates for a subscription fee of €90 per month. The idea is to stay one step ahead. If you identify a strategic threat (a cooling market, an emerging technology), you can react in time (seek alternative clients, modernise your offering, review your strategy, etc.) rather than being left paralysed once the change has already happened.

Operational risks:

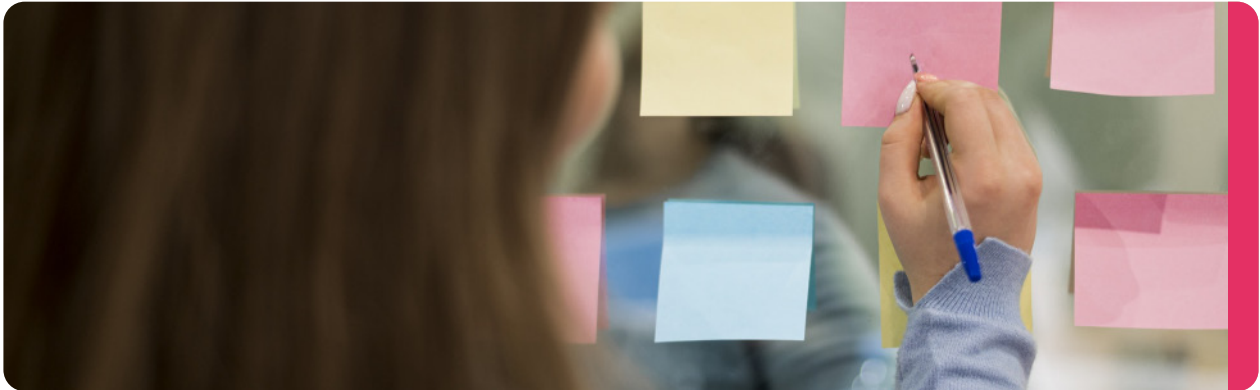
These are day-to-day risks, usually relating to processes, people, premises, systems and suppliers. Common examples include workplace accidents, fires or theft, IT failures (computer system crashes, cyberattacks), problems with suppliers (delays or breaches that halt your production or service), breakdowns of critical machinery, or human error leading to losses.

How should they be managed?

The key here is prevention and preparedness: implementing safety and maintenance measures to prevent accidents and incidents (e.g. training staff in occupational risk prevention, having fire extinguishers and fire suppression systems in place, backing up systems, establishing maintenance plans for machinery, diversifying critical suppliers, etc.). At the same time, it is important to draw up contingency plans: what would you do if one of these serious problems occurred? For example, EcoReciclaje set up backups of its systems on alternative servers through its systems provider, enabling it to continue operating in the event of a serious IT failure. They also created manual, paper-based procedures to enable invoicing and data recording in the event of a total IT failure. Think about and write down how your business would operate without IT systems: could you dispatch products? could you sell or invoice? And for how long? It may seem pointless, but these exercises (known as contingency plan drills) will allow you to assess how well you cope in a crisis situation without it actually happening, where nerves and the need to act quickly can play tricks on you.

A good next step is to identify which processes are truly critical to the survival of the business and to assign them a name and a person in charge. Not everything is equally important: collecting payments, paying wages, looking after key clients, or maintaining a minimum level of operations are usually at the top of the list. A very useful exercise is to ask yourself: 'If we were unable to operate for a week starting tomorrow, which three things absolutely cannot fail?'

From there, set realistic maximum recovery times (for example, ‘invoicing within 48 hours’, ‘minimum production within 72 hours’) and document simple solutions: alternative suppliers, temporary manual labour, one-off subcontracting or the use of external facilities. This simple yet structured exercise forms the basis of any business continuity plan tailored to an SME.



Furthermore, it is essential to prepare people, not only systems. A plan that only exists on paper is of little use in a real crisis. Make sure that key staff know what to do and who to contact in the event of an incident. Define a clear chain of command (who decides to shut down operations, who informs clients, who speaks to suppliers or the insurance company) and ensure this information is accessible outside of IT systems (for example, in printed form or on a mobile phone). Some very useful tools for SMEs include: an up-to-date list of key contacts, simple client communication templates, and a ‘first 24 hours checklist’ to follow in the event of an incident. This reduces the need for improvisation and stress when it matters most.

Finally, consider the business continuity plan a living, evolving document, not a complex project. There is no need to start with lengthy manuals: an SME can have an effective plan in 5-10 pages or even a clear outline. Review it at least once a year or whenever something significant changes (new IT system, move to new premises, new key client). Use minor incidents or ‘near misses’ to improve it. Over time, this approach not only reduces losses during a crisis but also boosts the confidence of clients, banks and employees, demonstrating that the business is prepared to withstand and recover when things do not go as planned.

Another example from EcoReciclaje: after assessing their fire risk, they reorganised their warehouse to reduce combustible materials and installed fire-fighting equipment, as well as taking out business interruption insurance so that, should an incident force them to shut down the plant, the insurance would cover their fixed costs and loss of revenue whilst they recover. In summary, for operational risks, preventive controls (security, backups, maintenance) should be implemented, insurance should be taken out where possible, and alternative plans (alternative suppliers or systems, emergency procedures) should be in place to ensure business continuity.

Financial risks:

These relate to the financial management of the business. A key risk is a lack of liquidity – for example, the business running out of cash to pay wages or bills.

Other common financial risks include: client defaults, internal or external fraud (such as embezzlement or theft), unexpected cost increases (due to inflation or higher raw material prices), exchange rate fluctuations (if you operate in foreign currencies), or excessive debt.

How should they be managed?

Prevention in this context involves sound financial planning: maintaining a liquidity buffer (reserve funds) for unforeseen events, monitoring receipts and payments (for example, ensuring that clients do not accumulate overdue invoices), and seeking to diversify sources of funding (various financing mechanisms or pre-approved credit lines with the bank should the need arise, etc.). To reduce the risk of late payments, check the creditworthiness of new clients (using tools such as Informa), set internal credit limits and clear payment terms (for example, requesting partial payments in advance for large contracts). You can also make use of tools such as trade credit insurance, which covers part of the cost of bad debts and provides you with information on your clients' financial health. As for fraud, implement basic controls: segregation of duties in accounting (prevent a single person from being able to create a supplier, record orders, receive them, record invoices and pay them), regular account reviews, and fraud insurance (if your operation is highly decentralised and you want extra control). In short, keep your finances under control by understanding your projected cash flow, having plans for worst-case scenarios (which expenses would you cut if sales fell? how would you renegotiate a debt if interest rates rose?), and protecting yourself against defaults and other unexpected financial events.



Compliance risks

These relate to breaches of laws, regulations or contractual obligations. These can include legal sanctions or fines (for instance, regarding tax, employment, environmental, or data protection matters), lawsuits from clients or employees, or even criminal liability for the director in severe cases.

How should they be managed?

The first step is to identify the regulations that apply to your business – tax, employment, health and safety, environmental, sector-specific, etc. – and ensure you comply with them.

It may be useful to seek the help of a legal adviser or an accountancy firm to keep up to date with regulatory changes and check that you are in compliance (for example, is your occupational health and safety policy up to date? Do you comply with the General Data Protection Regulation (GDPR) when processing client and employee data?). Invest in basic training for yourself and your employees on critical compliance requirements (for example, health and safety if you run a workshop). A simple calendar or log sheet of legal requirements (taxes, licence renewals, machinery inspections, audits, etc.) will help you avoid non-compliance due to oversight.

The best defence in tax matters is day-to-day prevention. Keep a close eye on your tax obligations using a clear tax calendar (quarterly VAT, withholding tax, corporate income tax, etc.), without waiting until the last minute to file each return. Remember that the tax authorities impose automatic surcharges for late tax filings (for example, a single day's delay in a VAT quarter results in a 5% surcharge on the tax due). Work closely with a trusted accountancy firm or tax adviser: they will help you keep up to date with regulatory changes and periodically review your accounts to correct errors before the tax authorities do. This approach avoids penalties and prevent extreme scenarios: it is essential to steer clear of any practice that could be considered deliberate fraud; bear in mind that defrauding the tax authorities of over €120,000 in a single financial year (per tax) constitutes a tax offence under the Criminal Code, carrying potential prison sentences – an unacceptable risk for any director.

Finally, consider taking out general liability or specific insurance policies (e.g. directors' and officers' insurance, where applicable) to provide financial protection in the event of certain legal claims. At EcoReciclaje, for example, they identified that they needed to improve training in health and safety and update certain environmental permits to avoid penalties; they also decided to review all their supplier and client contracts with their solicitor, to avoid any hidden surprises regarding issues such as data protection or the business continuity of their main business partners. The key is to be proactive when it comes to compliance: it is better to invest a little in legal prevention than to face a costly fine or lawsuit due to ignoring regulations. Legal non-compliance, in its most severe aspects, can carry criminal liability (subject to the Criminal Code), for which liability lies with the company's most senior officer (the director). Consider carrying out an assessment of compliance with the requirements of the Criminal Code for Spanish companies (for example, having a whistleblowing channel in place for companies with more than 50 employees⁵).



⁵ <https://www.boe.es/buscar/act.php?id=BOE-A-2023-4513>

Environmental risks:

These include environmental damage caused by the company (e.g. a waste spill, polluting emissions), which usually results in fines and clean-up costs, as well as risks arising from natural or climatic events that affect the company. Examples: floods or storms that disrupt operations, heatwaves that force a shutdown or reduce productivity, etc.

How should they be managed?

If your business has an environmental impact, ensure that you strictly comply with environmental regulations and that you have the necessary permits and insurance (for example, in industrial sectors in Spain, environmental liability insurance covering the costs of accidental pollution is mandatory). Take preventive measures: for example, EcoReciclaje has implemented protocols to store waste safely and prevent spills, and has reviewed its drainage systems to minimise damage in the event of heavy rain. It also included extreme weather events in its business continuity plan, setting out what to do in the event of flooding or other natural disasters.

Many environmental risks can be transferred through insurance (for example, in Spain, the Consorcio de Seguros⁶ automatically covers certain catastrophic events such as floods and earthquakes if the company has valid property insurance). Of course, it also contributes to reputational risk: poor environmental practices could ruin the company's image. That is why the general recommendation is to go beyond legal requirements when it comes to environmental and safety issues: not only do you avoid penalties, but you also protect your reputation and the trust of clients and investors.

As you can see, many common risks can be mitigated through relatively simple measures. Below is a table setting out some examples of common risks faced by SMEs, along with basic controls or actions that could be implemented to manage them:

Workplace accidents (employee wounds and injuries)

Implement safety measures and training: signpost hazardous areas, provide personal protective equipment, deliver regular training on risk prevention, and monitor compliance with safety regulations

Fire on the premises

Implement preventive measures: fire safety systems (fire extinguishers, alarms, sprinklers), safe storage of flammable materials, an evacuation plan and regular drills. In addition, take out property damage and business interruption insurance to mitigate the financial impact should a serious fire occur

IT failure or cyberattack

Perform frequent backups of critical data (ideally automated on a daily basis), ensure that cybersecurity solutions (antivirus software, firewalls) are kept up to date, and have an IT contingency plan in place (backup servers, alternative manual procedures) to maintain operations in the event of a system failure.

⁶ <https://www.consorseguros.es/>

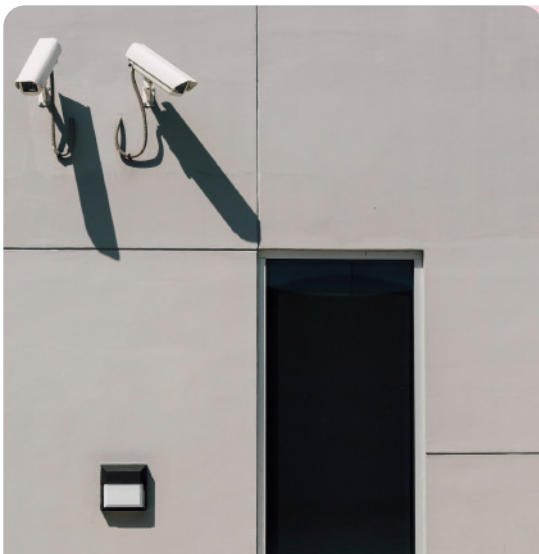
Default by a major client

Check clients' creditworthiness before offering them credit; establish payment terms (either upfront or in instalments) for large contracts; set an internal credit limit per client. For large sums, consider taking out credit insurance to cover a percentage of the debt in the event of default.

Key supplier failure

Identify your critical suppliers and arrange for alternative suppliers or contingency plans (additional safety stock) in case any of them fail. Risk of reliance on staff – this affects 62% of SMEs, which are unable to find qualified staff, according to an OECD report. Include penalty clauses or guarantees in contracts with key suppliers, and regularly assess their reliability. These measures reduce dependency and enable the business to continue operating if a supplier fails to meet its commitments.

Please note that these are general examples. Each company will need to tailor its control mechanisms to its specific risks. The important thing is to understand that, **for every risk identified, you must decide** on a course of action: whether to mitigate it (reduce its likelihood or impact through control measures), avoid it (if it is unacceptable, perhaps by abandoning a particular high-risk activity), transfer it (through insurance, contracts or other means, such as credit insurance, damage insurance, etc.) or, if it is a minor risk, consciously accept it and simply monitor it.



Often, the strategy will be a combination of all of them: for example, when faced with the risk of theft, you can mitigate the risk (by installing an alarm or strengthening locks) and also transfer part of the impact (through insurance that covers theft), perhaps accepting minor losses as part of the cost of doing business. Risk management should not be an extra luxury on top of day-to-day operations, but rather another factor that we must integrate into the way we operate. Questions such as 'What if our major client fails to pay our next stage payment, or our supplier does not deliver the order?' must be incorporated into the company's existing routines. Avoid holding meetings dedicated solely to risk; instead, incorporate risk management into daily, weekly or monthly meetings, planning sessions, metrics review sessions and sales monitoring.

In the next section, we will look at a step-by-step method for implementing a risk management system in your SME, integrating all of the above in a structured and easy-to-follow way.

4. How to implement a risk management system step by step

Roadmap: Implementation within 90 days

1	2	3	4	5	6
Week 1 - 2	Week 3	Week 4 - 5	Week 6 - 8	Week 9 - 12	Month 3 onwards
Identification	Register/map	Analysis and assessment	Management plan	Implementation	Ongoing review
Define your company's key objectives and ask: <i>'What might prevent us from achieving them?'</i> Bring together 2-3 key people. Brainstorm. Review past incidents.	Organise each risk into a simple table - Description - Category - Likelihood (High/Medium/Low) - Impact (High/Medium/Low) - Existing controls	Assess each risk: How likely? How serious? Prioritise the 3-5 most critical ones for your business objectives.	For each risk, decide: Reduce? Transfer (insurance)? Accept? Assign a person in charge, a date and resources. Maximum 10 actions.	Let's get started! Put the plan into action. Start with the quick wins. Weekly progress update.	Include in regular meetings (5 mins). Define 2-3 early warning indicators. Conduct a full review every quarter or six months.
Initial list of risks	Risk register	Top 5 prioritised risks	A concrete action plan	Operational measures	Continuous improvement cycle
You don't need to get everything perfect right from the start. Start with the essentials, achieve some early wins, and improve with every cycle.					
Understand Weeks 1 - 5		Implement Weeks 6 - 12		Uphold from month 3 onwards	

Based on international standards (COSO, ISO 31000) and tailored to the needs of SMEs.

Now that you know the basics, let's look at how to implement risk management in your business in a practical way. We propose a simple six-step process, inspired by international standards (the ones used by large companies, namely the COSO framework), but adapted to the reality of an SME. The idea is to start with something basic and improve it over time. You'll be surprised at how much you can achieve in just a few months with very specific actions.

Step 1

Risk and opportunity identification. Start by defining your company's key objectives (as we saw in section 2) and then ask: 'What factors could prevent us from achieving these objectives?' Gather your trusted team and brainstorm potential risks. Review past incidents, client complaints, audits or any previous warning signs. Use lists of examples (such as the categories in chapter 3) to ensure you don't overlook any important areas. The outcome of this step should be an initial list of risks that exist within your business and that concern you. Do not worry about quantifying them in detail; first, make sure you do not miss any important ones.

⁷ <https://www.coso.org/erm-framework>

Step 2

Risk register or 'risk map'. Take the list from step 1 and organise the information for each risk into a simple template, often referred to as a risk register or risk matrix. You can use a table in Excel or Word. For each risk identified, note down at least: a brief description of the risk as it applies to your specific situation, the category to which it belongs (strategic, operational, financial, compliance or environmental), an estimate of the likelihood of it occurring (use qualitative criteria for now, such as high, medium or low, which can be refined later), an estimate of its impact or damage if it occurs (for example: critical, moderate or minor, using the same criteria as defined for probability) and the existing controls (if you already have anything in place to help manage it, such as 'we have fire extinguishers and insurance' for the risk of fire). This register will serve as a basis for the next steps and give you an overview of your 'risk map'.

Step 3

Risk analysis and assessment. Now that you have your register, it is time to analyse each risk in more detail. Essentially, you need to assess how likely it is to occur and how serious it would be if it did. You can use a simple likelihood vs. impact matrix to rank the risks (for example, those with high likelihood and high impact will be the most critical). You do not need complex calculations; simply prioritise them into three levels (high, medium, low) or use subjective scores from 1 to 5. Involve those who are familiar with each area in this analysis (the production manager will be best placed to comment on operational risks, the finance manager on liquidity risks, and so on). Prioritise the risks at the end of this step: identify your priorities (the 5-10 most critical risks that require immediate attention), those that are important but not urgent, and those that are minor and can be accepted for now. Remember: not all risks are equally likely, nor would they all cause the same damage; focus on those that could genuinely 'sink' or seriously hamper your business. Bring together key people from across the company to align perspectives and gauge sensitivities. Make it clear that this is a company-wide exercise, not a criticism of any department. It is normal for operational departments to face more risks; therefore, there will be more priorities and actions. Approach it as a strategic exercise: the most important areas receive greater focus and more resources to mitigate risks.

Step 4

Risk management plan. For each priority risk (the critical risks identified in step 3), decide which strategy you will adopt: there are four main options (avoid, mitigate, transfer or accept). Typically, you will want to mitigate most of them (reducing the risk through control measures) and transfer those you can (for example, through insurance or contracts with third parties), avoiding only those that are unacceptable and accepting those that are very minor. Be very specific here: for each major risk, outline the specific actions to be taken, who will carry them out, and the required deadline. This will define your action plan. For example, if the risk is 'warehouse fire', your actions might be 'Install automatic sprinklers by the end of the month (person in charge: Juan, Head of maintenance) and obtain quotes for fire insurance with business interruption cover (person in charge: María, Administration Department, by the end of this quarter).' Document these actions in your plan so that you can monitor them together. Also prioritise what to do first – usually, start with the solutions for the highest-level risks. You may find that some actions mitigate several risks at once (for example, a good data protection and backup system helps you mitigate operational and cyber risks). Make sure you allocate resources (time, and some budget if necessary) to implement these improvements. Do not prioritise more than 10-15 actions, to ensure you stay focused. Use clear timeframes to manage the plan: actions to be implemented in the coming month, the coming quarter, the coming six months or over the course of the year (do not plan more than 12 months ahead).

Step 5

Implementation of the measures and initial monitoring. Let's get started! Start implementing the action plan. Execute the improvements, take out the necessary insurance, train staff, etc. It is important that the company's management supports and monitors these tasks, so that they are not forgotten. You could hold brief weekly or fortnightly meetings whilst implementing the measures, to check on progress (e.g. 'Have we installed the alarms yet? How are the credit insurance negotiations going?'). This step may take weeks or a few months, depending on how many issues you need to address, but many basic control measures can be put in place within days (for example, making a backup today, or buying fire extinguishers this week). Don't try to get everything perfect straight away: start with the most critical issues and build on that. There will probably be risks that require longer-term solutions; identify the actions that can be implemented quickly (quick wins) and those that will take longer, and secure some early wins that demonstrate the benefits of risk management (for example, fixing dangerous wiring today prevents a fire tomorrow).

Step 6

Ongoing monitoring and review. Risk management does not end once you have implemented the initial measures (although congratulations – your business is already safer than before!); it's an ongoing process. You should establish a mechanism to monitor risks and periodically review your risk map, incorporating this into existing meetings (e.g. committees, monthly follow-up meetings). Including these reviews in existing meetings (daily, weekly, monthly) will allow you to incorporate risk management into routine tasks, thereby achieving the cultural change you are aiming for. As previously discussed, define some key indicators or early warning signs for your main risks and review them at appropriate intervals. For example, EcoReciclaje decided to monitor: (i) the frequency rate of workplace accidents (for its staff safety risk), (ii) the moisture content of stored scrap metal (as an indicator of the risk of spontaneous combustion, linked to the risk of fire), and (iii) the amount of debtor balances outstanding for more than 60 days (for default risk). Each company will choose its own. In addition, schedule at least one comprehensive review of your risk register each year (in large companies with complex operations, this is done 2 or 3 times a year). During the review, update the list: Are there any new risks (due to changes in the business or the environment)? Has any risk ceased to be relevant? How are the actions you set out to take progressing? Update the likelihood/impact assessments if anything has changed since the measures were implemented. For example, a risk that you previously assessed as high might now be medium because you have already implemented controls (that's a success!). Also document any incidents or near-misses that have occurred and the lessons learnt, and inform all staff of any significant changes or new protocols you have defined. In short, embed risk management into the company culture: make it a habit to stay alert and anticipate problems, rather than just reacting once they have already happened.



With these six simple steps, you will have implemented a basic risk management cycle in your SME. You can start small (for example, in the first cycle, focus on just 5 critical risks) and gradually expand the scope each year. The key is to move from improvisation to planned anticipation.

5. The insurance scheme for SMEs (transferring risks in a simple way)

One of the most powerful (and often underestimated) tools for managing risk is to transfer it through insurance. Taking out insurance means transferring the financial impact of certain adverse events to an insurance company, in exchange for paying a premium. Put simply: insurance transforms a potential major —but uncertain— loss (such as a fire causing millions in losses) into a fixed, certain and manageable cost (the annual insurance premium). In this way, the SME ‘buys peace of mind’: if a claim is made, the insurer will cover most of the financial losses, enabling the business to survive and recover.



Not all risks are insurable. Insurers typically cover accidental, uncertain events that can be objectively quantified in monetary terms. For example, events such as property damage (fires, floods, theft), civil liability for causing harm to third parties, workplace accidents, cyberattacks, and even client default (through credit insurance) are insurable. However, there are risks that cannot be transferred to an insurance policy, particularly those of a more strategic or deliberate nature: for example, pure business risks (loss of market share, a failed product launch) or penalties for intentional breaches of the law (as no one will insure against fines if you deliberately breach regulations). Nor is loss of reputation or brand value usually insured directly, although some policies include limited services to mitigate damage to reputation.

General rule: If the risk depends on business decisions or market trends, it is difficult to insure against it; if it is a sudden, external or accidental event that causes specific losses, there will probably be some form of insurance cover for it.

The market offers many types of business insurance, but for a typical SME (in Spain), these are the most relevant to consider:

-
- **Third-party liability insurance:** It covers compensation for damage or loss caused to third parties by the company in the course of its business operations. It includes legal costs in the event of claims. It is essential for mitigating legal risks. It acts as a financial 'buffer' against claims from clients, suppliers or the general public (e.g. a client is injured on your premises, a defective product causes damage, or a professional error results in a loss for a client).

Within this policy, it is worth paying particular attention to two key areas of cover which often have significant limitations. Firstly, employers' liability, which covers injuries sustained by employees in the event of a workplace accident where the company is liable. It is common to find insufficient sub-limits in this cover, so it is advisable to review and update them to bring them into line with standard compensation levels.

Furthermore, product liability insurance is essential for companies that manufacture or sell goods, as it provides protection against damage caused by defective products. Surprisingly, some companies do not have this cover, or their cover is insufficient, which can seriously jeopardise their profit and loss account and the trust of their clients.

Note: In certain sectors, holding third-party liability insurance is required by law, but even where it is not, it is highly recommended.

- **Business multi-risk insurance:** It is a comprehensive policy that combines a range of useful cover options for SMEs. It typically covers physical damage to your assets (fire, explosion, flooding, theft, machinery breakdown, etc.) and may also include business interruption cover, i.e. compensation for loss of profits and fixed costs whilst the business is shut down due to a covered incident.

It is worth noting that loss of profits is not always automatically included, as this is a significant form of cover that must be specifically requested and confirmed depending on the business activity. Furthermore, accurately determining the sum insured is critical: it must be based on the insured gross profit (fixed costs + expected profit), and not on the gross profit shown in the profit and loss account, as this can lead to situations of underinsurance. The involvement of a professional insurance broker at this stage is essential to avoid any misunderstandings or surprises in the event of a claim.

This insurance is essential for mitigating operational risks (destruction of premises, machinery, stock) and ensuring business continuity. For example, if a disaster forces you to close temporarily, business interruption cover helps ensure you can continue to pay wages, rent and other fixed costs until operations resume. For most industrial or commercial SMEs, business multi-risk insurance is an essential 'basic package'.

- **Trade credit insurance:** It covers the risk of client default. The insurer reimburses a percentage (usually 70%–90%) of invoices that remain unpaid due to your clients' insolvency or late payment. In addition, these policies usually offer information and debt recovery services (the insurer analyses and monitors your clients' creditworthiness and can handle the collection of unpaid debts). It is a useful tool for B2B SMEs with credit sales, as it mitigates the financial risk of liquidity shortages caused by defaulting clients. In Spain, there are various companies offering credit insurance that is widely used by exporting SMEs and also for the domestic market.

- **Accident insurance and other compulsory insurance:** If you have employees, find out which types of insurance are compulsory under collective agreements or by law. For example, many collective agreements require accident insurance for employees, guaranteeing compensation in the event of death or disability resulting from a workplace accident. Vehicle insurance is also compulsory if the company owns motor vehicles (at least third-party motor insurance is required by law), as well as, in sectors with potential for pollution, environmental liability insurance to cover decontamination costs.

It is also important to remember that paying premiums on time and in full is essential to ensure not only the validity of the cover taken out, but also access to protection from the Consorcio de Compensación de Seguros in the event of extraordinary risks (such as adverse weather events). Given the increase in such events in recent years, this aspect is becoming increasingly important to ensure effective protection for the business. Compliance with these requirements is not only a legal obligation but also a key measure to protect the company against significant risks, which must be transferred to the insurance market.

- **Cyber risk insurance (or cybersecurity):** It is designed to protect the company against the risks arising from technological incidents and cyberattacks, which are becoming increasingly common in the digital environment. It covers both first-party losses (costs of system recovery, data restoration, forensic analysis, business interruption and crisis management) and third-party liabilities (claims arising from personal data breaches, legal costs and, in certain cases, administrative penalties). It acts as a 'financial buffer' against events such as ransomware attacks, identity theft, data breaches or prolonged downtime of critical systems. This insurance does not replace IT security measures, but it is particularly recommended for SMEs that rely on digital systems, handle sensitive data or conduct online operations, as it helps to limit the financial, operational and reputational impact of a serious incident and contributes to maintaining business continuity.
- **Other types of insurance to consider:** Based on the nature of your business, you might consider surety insurance (if you need to guarantee contracts or defer tax payments without tying up your cash), or directors' and officers' (D&O) insurance (if you have investors or wish to protect your personal assets against claims arising from business decisions).

In addition, it is worth considering goods in transit insurance, particularly for companies managing logistics or shipments, as it provides cover against damage or loss during transport. Fidelity insurance is also important, as it covers financial losses arising from internal misconduct – a less visible risk but one that, depending on the type of business, could have a significant potential impact.





Practical tips for managing your insurance:

- **Prioritise according to need:** It is not about taking out ‘every type of insurance under the sun’, but rather about prioritising cover for the risks that could bring your business to a standstill. Generally speaking, make sure you meet the legal requirements first, then protect yourself against catastrophic events (such as fire and third-party liability), and finally consider cover for risks that are more likely to affect your business (for example, cyberattacks if you handle a lot of digital data, credit insurance if you rely on deferred payments, etc.).
- **Avoid underinsurance:** A common mistake made in an attempt to save on premiums is to insure assets for less than their actual value. Be careful: if, for example, you insure your stock for half its value, in the event of a claim the insurer may only pay out half the amount of the loss under the proportional rule. Review your insured values annually (buildings, machinery, stock, turnover for loss of profits) and adjust them to reflect reality. This will help you avoid unpleasant surprises when making a claim. The same applies to excesses: keep an eye on the balance between the premium (what you pay annually), cover (what you will receive if a claim is made) and the excess (the initial amount you cover yourself).
- **Compare cover, not just price:** Look for a good, trustworthy insurance broker or agent. A professional will help you identify your key risks and the cover you need, clearly explaining the small print (limits, excesses, exclusions, etc.). Don’t choose solely on the basis of the cheapest premium: make sure the policy covers what you actually need. It’s even useful to map out your insurance policies: what risks each policy covers, to spot any gaps or overlaps. For example, if you already have a good business multi-risk insurance policy covering damage and loss of profits, you may not need to take out separate basic fire insurance; but make sure your policy includes everything you need (sometimes you have to add extra modules, such as cover for earthquakes or cyber risks). A suitable adviser will guide you through this puzzle.

- **Incorporate insurance into your business continuity plan:** Remember that insurance is no substitute for preventive measures; it is your last line of defence if, despite everything, the worst should happen. That is why you should incorporate your insurance policies into your emergency plans. For example, if you have a fire response plan, include steps in it to notify your insurer immediately and to document the damage thoroughly, in order to speed up the claims process. Make sure you are fully aware of what each policy covers and does not cover, and what to do in the event of a claim (assistance hotlines, reporting deadlines, required documentation, etc.). Having the right insurance (and your own emergency fund, if possible) can make the difference between reopening after a few weeks or being forced to close down permanently following a disaster.



Let's look at a practical example: EcoReciclaje, S.A., after drawing up its risk map, identified where insurance was crucial. They realised that a major fire could result in losses running into millions, so they took out industrial multi-risk insurance with extensive cover for fire, explosions and other damage, adjusting the sum insured for their premises to the replacement value. They added loss of profits cover for 6 months, so that if the plant were to become inoperative due to an incident, the insurance would cover their fixed costs and lost revenue during that period. As they handle hazardous waste, they also took out environmental liability insurance (mandatory for their licence) for €1 million, to cover clean-up costs in the event of accidental contamination. With regard to defaults, they took out credit insurance covering 80% of the debt owed by their main clients in the event of insolvency. And their broker recommended that they increase the cover under their general liability insurance to €600,000, given the risk of damage to third parties (for example, a fire affecting neighbouring premises). With this insurance programme, EcoReciclaje transferred several of its most critical risks: if a major fire or flood occurs, it will receive compensation to rebuild its damaged assets and to offset the loss of income; if an environmental incident occurs, it will have financial backing to respond; if a major client fails to pay, it will recover most of the invoice; and if it faces third-party claims, the insurance will provide support with legal defence and compensation.



A good insurance portfolio not only protects your company's finances, but also enables you to demonstrate to a bank or investor that your assets and operations are properly insured, thereby gaining access to potentially more favourable credit terms (lower interest rates and fewer guarantees required). In short, with a small investment, you can make insurance your strategic ally for the continuity of your business, but remember, taking out insurance is just another risk management tool. Taking out an insurance policy does not transfer all the risk to the insurer. The risk remains and needs to be managed.

6. Financing tools and the benefits of risk management

Risk management not only protects you from problems: it also improves your access to finance. According to a report by CEPYME, the lack of credit is one of the biggest obstacles for SMEs in Spain; therefore, managing your risks builds greater confidence among banks and investors and will help you secure credit on better terms.



Every business needs financial resources to grow, invest or simply weather difficult times. In Spain, traditional bank financing (loans, credit facilities, leasing, etc.) remains the main source of funding for SMEs. However, it is not always easy to secure on favourable terms. In this context, effective risk management can act as an 'intangible guarantee' that strengthens your position with banks and investors.

Better access to bank credit:

When a bank assesses whether to grant you a loan or credit line, it evaluates the risk that you might default on repayment. In addition to your financial statements and collateral, banks are increasingly looking at the strength of your business management and governance. If you can demonstrate that you have identified and managed your key risks, you will project an image of a more organised, credible, professional and stable company. For example, presenting your business continuity plan to the bank (outlining how you would respond to various crises) or demonstrating that you have key insurance policies in place (third-party liability, business multi-risk, etc.) will lead them to view you as a lower-risk client. This can result in loans being approved more readily, lower interest rates, or fewer guarantees being required. In fact, banks sometimes require certain types of insurance as a condition for lending (e.g., fire insurance on a warehouse used as collateral, or life insurance for long-term loans). If you've already got these aspects covered, the credit process will be smoother and more favourable.

Financial stability and the cost of capital: Effective risk management tends to reduce the volatility of your results (fewer unexpected losses, fewer ups and downs).

⁸ https://cepy.me/storage/2024/09/INFORME-DE-FINANCIACION-BANCARIA-A-PYMES_NOVIEMBRE.pdf

This improves your financial indicators (margins, solvency, etc.) and, consequently, your credit profile with banks and investors. It may even mean that the bank requires less personal guarantee or hard collateral, as it perceives the business to be well managed and less likely to face negative surprises. In short, the figures tell a story, and if your figures demonstrate order and resilience thanks to risk management (for example, fewer unexpected costs due to accidents, continuity ensured by insurance cover, etc.), you will have greater negotiating power when seeking finance.

Investors and alternative financing (investment appeal):

When a bank assesses whether to grant you a loan or credit line, it evaluates the risk that you might default on repayment. If, instead of bank credit, you are seeking capital (partners, private investors, venture capital, crowdfunding), risk management also works in your favour. An experienced investor will analyse the risks of your business before investing, and will view it very positively if you have identified and mitigated them. Presenting a business plan that outlines the main risks and how you intend to manage them instils confidence and conveys professionalism. Conversely, statements such as ‘nothing can go wrong in my company’, or failing to acknowledge potential problems, will put investors off. Even in later rounds, during due diligence, they will review aspects such as the insurance portfolio and its cover, the level of legal compliance, dependence on key clients or suppliers, existing litigation, tax credits generated in previous financial years, third-party audits, or the claims history, to identify hidden risks. If you have already addressed these areas (for example, you have solid contracts with suppliers, adequate insurance, contingency plans), it will be easier for them to invest in your company. Compliance with ESG standards is increasingly becoming a distinct asset, and may act as a barrier to investment if funds are subject to bank loans or European growth funds. In short, an SME that manages its risks well is much more ‘investable’ and attractive to external capital.

Other funding sources: In addition to banks and private investors, Spain offers public credit facilities (such as loans guaranteed by the ICO (Spanish Official Credit Institute)⁹, ENISA equity loans for innovative projects, grants and funding from European funds) and crowdfunding platforms (such as crowdlending and equity crowdfunding). In all cases, having a robust risk management strategy gives you an advantage. For example, ENISA¹⁰ does not require personal guarantees, but it does assess the project’s viability and the management team’s creditworthiness; submitting a plan that demonstrates you have considered risks and contingencies will improve your chances. Similarly, when applying for a competitive grant, it usually helps if your proposal demonstrates that you have considered how to tackle any potential challenges the project may face. And in crowdlending, the retail investors lending money to your SME will evaluate the information you share: if they see transparency and a risk management plan, they will be more confident about funding you.

Support from chambers of commerce, business incubators and business associations: Contact your local chamber of commerce for guidance on how to strengthen your business and ensure its growth. The challenges your company faces are common to many other businesses; others have undoubtedly been through the same situation, and you can learn from their experiences, thereby avoiding the risk of repeating the mistakes they may have made. Seek support from business accelerators, incubators, chambers of commerce, sectoral or regional associations, or any other organised group of experts, such as the Instituto de Gobernanza Empresarial (IGE)¹¹ or AGERS, to obtain guidance on how to structure your company’s governance and risk management in an organised and efficient manner.

⁹ <https://www.ico.es/>

¹⁰ <https://www.enisa.es/>

¹¹ <https://igobernanzaempresarial.com/>



In conclusion, financing is the fuel for SME growth, but securing it on favourable terms requires demonstrating financial strength. Integrating risk management into your financial strategy means presenting a more reliable business to third parties: healthy balance sheets, realistic forecasts, adequate insurance and contingencies under control. This not only increases the likelihood of securing credit or investment, but is often a source of savings (lower interest rates, lower insurance premiums due to a good track record) and new opportunities. Ultimately, lenders want to ensure that their money is protected; if you are already taking steps to protect your business, it will be easier for them to trust you. As the saying goes: 'Nothing ventured, nothing gained', but SMEs that manage their risks effectively will be able to take calculated risks and secure the resources they need to succeed.

7. The director's responsibilities

As a director, you must pay particular attention to the legal risks facing your business. Certain breaches of regulations (labour, tax, environmental, data protection laws, etc.) can result not only in financial penalties for the company, but also in direct criminal consequences for you as a director, in the most serious cases. For example, a serious workplace accident caused by a lack of safety measures, a significant tax evasion offence, or a polluting spill with serious consequences for the environment may result in criminal liability under the Criminal Code, which holds the company director ultimately responsible in such situations. In short: managing legal risks properly is not optional; it is essential to protect both your business and your personal assets.



How can you manage and prevent these legal risks? Firstly, identify and comply with all the regulations applicable to your business. Make sure you are aware of your obligations regarding tax, employment, health and safety, the environment, data protection and any specific sector-related regulations, and regularly check that your company is up to date in every area. Seek support from trusted legal advisers or accountancy firms to stay informed of legislative changes and ensure you do not overlook anything. Ask yourself, for example, whether your occupational health and safety measures are up to date or whether you comply with the General Data Protection Regulation (GDPR) when handling client information.

It also fosters a culture of compliance within the company: invest in training for yourself and your employees on key obligations (e.g. health and safety training if you have staff, or basic tax regulations if you handle your own accounts). A simple calendar of legal obligations (tax filings, licence renewals, regular equipment inspections, etc.) will help you avoid non-compliance through simple oversight. Likewise, establish clear internal procedures and communication channels so that any employee can report irregularities without fear. In fact, Spanish law requires companies with more than 50 employees to have an internal whistleblowing channel for reporting potential breaches. Implementing a compliance system that is proportionate to your size – including a code of ethics, internal protocols, regular checks and confidential reporting channels – is one of the best ways to prevent legal risks and demonstrate due diligence. Remember: being proactive about legal compliance is always more cost-effective than having to deal with fines, lawsuits or reputational damage later on for having ignored the regulations.



Finally, protect your business and your own assets with adequate insurance. Third-party liability insurance is essential to cover potential compensation claims and legal costs should third parties claim damages arising from the company's activities. This insurance acts as a financial 'buffer' against claims from clients, employees or suppliers, preventing a legal setback from seriously compromising the business's finances. You should also consider taking out specific D&O (Directors & Officers) insurance for directors and senior managers: this policy covers the costs of legal defence and potential compensation in the event of claims linked to your management decisions. D&O insurance can protect your personal assets if, for example, you are sued by a partner or a creditor due to a business decision.



In conclusion, legal risk management must be integrated into your SME's strategy. Compliance with the law is not merely bureaucracy; it is about ensuring business continuity and protecting yourself as a director. With a preventive approach – strict regulatory compliance, training, early warning systems (whistleblowing) and adequate insurance cover – you can reduce the likelihood of facing penalties or criminal liability, ensuring your business operates within the law, and strengthening its reputation and long-term resilience.

iCongratulations! You have reached the end of this journey. Throughout this guide, you have seen that risk management is neither a theoretical exercise nor exclusive to large corporations, but a practical tool within reach of any SME. By applying a structured, proportionate and action-oriented approach, it is possible to anticipate problems, reduce losses and strengthen business continuity. The key is not to get it perfect, but to get started, prioritise and improve continuously. Turning risk into a managed variable is, now more than ever, a competitive advantage and a critical factor for business survival.



Whether you're looking for more information on risk management, more in-depth content, or more specific advice for your business, you can contact AGERS via **info@agers.es** or **formacion@agers.es**

YOUR ROADMAP

From scratch to risk management in 90 days

You already manage risks every day when you make decisions. This roadmap helps you do so in a more structured way.

	What to do	EcoReciclaje, S.A.
1	WEEK 1 — Define your direction Bring together 2–3 key people (1 hour). Question: What are our 3 objectives for this year? What might prevent us from achieving them? >> A list on a whiteboard or a simple document will suffice.	Objectives: increase sales by 15%, renew environmental licence, reduce accidents. Threats: reliance on a single client (40% of sales), warehouse with no fire protection
2	WEEKS 2–3 — Identify and prioritise List 5–7 risks. For each one: How likely is it to happen? How serious is it for our objectives? (high/medium/low). Prioritise the 3–5 that pose the greatest threat to what you want to achieve. >> What controls do we already have in place? Often, you are already doing more than you realise.	Top 3: (1) Fire in the warehouse — would shut down the plant, (2) Default by a major client — puts cash flow at risk, (3) Environmental penalty — would result in the loss of the licence.
3	MONTH 1–2 — Focus on the critical issues For each priority risk, decide: Do we mitigate it? Do we transfer it (insurance)? Do we accept it? Assign a person in charge and a deadline. Maximum 10 actions. >> Start with quick wins: a backup today, a fire extinguisher this week.	They installed sprinklers and business multi-risk insurance covering loss of profits. They diversified their commercial portfolio (target: no single client >20%). They updated environmental permits.
4	MONTH 2–3 — Make it part of your routine Add 5 minutes on risks to your regular meetings: Any incidents? Any new risks? How are the actions progressing? It is not an extra meeting: it is part of the business discussion. >> Choose 2–3 early warning indicators (e.g. receivables >60 days, accidents/month).	Indicators: (1) accidents/month, (2) moisture in stored scrap, (3) outstanding receivables >60 days. Fortnightly review at management meeting.
5	MONTH 3 ONWARDS — Review and expand Quarterly review: update risks, assess what worked, incorporate lessons learnt. Expand gradually (more risks, more areas). Each cycle will be faster. >> The key is not to get it perfect, but to keep going.	After 6 months: they added cyber risk and credit insurance. The bank improved their terms upon seeing their documented risk plan.

Fundamental principle: Risk management starts with your business objectives.
 The question is always: what could prevent us from achieving what we set out to do?

This is what it looks like in your day-to-day life

It is not a separate discipline. It is a way of making better decisions.

Every important decision	Every week	Every month	Every year
- What could go wrong? - Are we prepared? - Is it worth the risk?	- Review incidents - Status of actions - Warning signs	- Key indicators - New risks - Progress of the plan	- Full review - Update priorities - Lessons learnt

The shift in mindset

WITHOUT risk management	WITH risk management
'A fire? We will see if it happens.' 'Our best client pays whenever they feel like it.' 'Insurance is just an expense.' 'The IT guy takes care of cybersecurity.' 'If there is a crisis, we will improvise.'	'We have fire extinguishers, insurance and an evacuation plan.' 'No single client accounts for more than 20% of sales.' 'Insurance is an investment in business continuity.' 'Everyone knows what to do in the event of a cyberattack.' 'If there's a crisis, we will activate the plan.'

Where to start?

This week, get your team together for an hour and ask: What are the 5 things we are most worried about?
You will have already taken the first step.



A practical guide to risk management for SMEs

ISBN: 978-84-09-86256-6

Copyright: DEP639126263225142567

Legal Notice – Copyright

© 2026 AGERS España

The contents of this work (text, images, graphics, design elements, etc.) are protected by copyright and intellectual property laws. The reproduction or dissemination of its contents requires the prior written consent of AGERS and may only take place provided the source and the relevant date are cited.

agers