5 Key Stages to Effective Risk Management

Risk management is an increasingly important business driver and organizations have become much more concerned about risk. Risk is a driver of strategic decisions; it is a cause of uncertainty in the organization; and it is also simply embedded in the activities of the organization. **An enterprise-wide approach to risk management enables an organization to account for the potential impact of all types of risks on all processes, activities, products and services.**

The underlying premise of enterprise risk management (ERM) is that every organization exists to provide value for its stakeholders. All organizations face uncertainty, and the challenge for management is to determine how much uncertainty to accept as an organization strives to grow stakeholder value. Uncertainty presents both risk and opportunity, with the potential to erode or enhance value. **Enterprise risk management enables management to effectively deal with uncertainty and associated risk and opportunity, enhancing the capacity to build value.**

According to COSO, **ERM can be defined as follows:**

Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

A successful enterprise risk management initiative can affect the likelihood and impact of risks materializing, as well as deliver benefits related to better informed strategic decisions, successful delivery of change and increased operational efficiency. Other benefits include reduced cost of capital, more accurate financial reporting, a competitive advantage, improved perception of the organization, better marketplace presence and, in the case of public service organizations, enhanced political and community support.

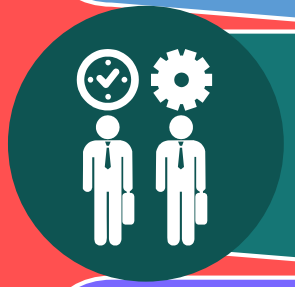
There are several distinct stages involved in the risk management process, yet **a robust risk lifecycle can be summarized in just five stages that serve as the basis for the main risk management regulations,** including COSO and ISO 31000.

Identification

The starting point is to uncover risks and define them in some detail using a structured format.

Assessment

Risks are examined in terms of the likelihood and impact in case of risk occurrence.

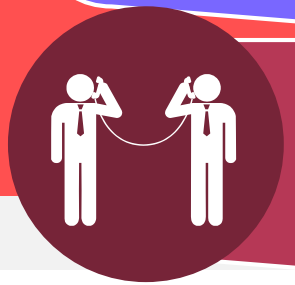


Treatment

An approach for treating each risk must be defined, which in some cases may be to do nothing. This requires an analysis of whether the risk is acceptable as is or whether an action plan is required to prevent, reduce or transfer the risk.

Monitoring

An ongoing review process is essential to proactive risk management, driven by an agreed timeframe for reassessing risks and tracking the status of treatments that have been put in place.



Reporting

Reporting at each of the four sequential stages is a core part of driving decision-making in effective risk management.

01 | Risk identification

Articulate corporate and operational objectives. A fundamental starting point to identifying risks is clarity on what these objectives are. This will allow you to identify events that weigh your ability to achieve your objectives.

List all relevant risks. Usually the best process for drawing up a long list of all potential risks is to engage in a combination of brainstorming workshop sessions and individual interviews. You might like to look for risks in broad areas such as: financial, management, reputational, economic, environmental, technological, fraud, and others.

Identify risk factors. You need to try to establish probable causes for the risk – the factors that might make the risk happen in the first place. There may be just one cause of risk but it is also equally likely that there are many causes.

Specify existing internal control measures. For many risks, you will already have some measures in place to control the likelihood or impact of the risk occurring. To be effective, such internal controls should be demonstrable by policy, procedure or practice. A key question is whether the existing controls are adequate or whether further controls are required to effectively manage the risk.

Assign ownership and responsibility. For effective risk management, it is critical that each risk has an owner who is responsible for dealing with the risk, ensuring that all internal controls are working and that relevant treatment actions are taken. This role also involves regularly monitoring the risk status and adjusting risk ratings accordingly, based on current information and knowledge.

02 | Risk assessment

Score risks on likelihood of occurrence. In order to establish the risk rating for each risk, you need to first decide the likelihood of the incident occurring, in spite of the existing controls that are in place. Another way of looking at this is the probability of the risk occurring, and sometimes these terms (likelihood and probability) are used interchangeably.

Score risks on impact. The impact of a risk is often considered in terms of its level of severity, and sometimes these terms (impact and severity) are used interchangeably. Establishing a basis for scoring the impact of risks is more complex than likelihood as there is an element of "it will vary by risk category."

Provide an overall risk rating score. The overall risk rating is found by combining the likelihood and impact scores, usually by multiplying them together – the so-called "risk evaluation matrix." It is common to divide the matrix into traffic-lighted zones to provide a visual clue as to risk status, in addition to the rating itself.

Prioritize risks and set risk appetite. It is not possible to get rid of all risks, and a number will offer little scope for treatment. Therefore, it is important to broadly define what the organization's tolerance for each risk will be and specify a priority for each risk based on this tolerance. Setting a priority gives you secondary information on the risk, in addition to its traffic-lighted status, so you can readily identify the most significant or urgent-to-deal-with risks.

03 | Risk treatment

Define the broad approach for each risk. There are four generic approaches you can take to deal with risks (tolerate, transfer, treat and terminate). The relative merits and practicalities of each approach will depend largely on the nature of the risk and, in particular, on the level of priority assigned to it. For all risks besides those you are taking a “tolerate” approach to, you need to articulate a risk mitigation action plan to prevent, reduce or transfer risk.

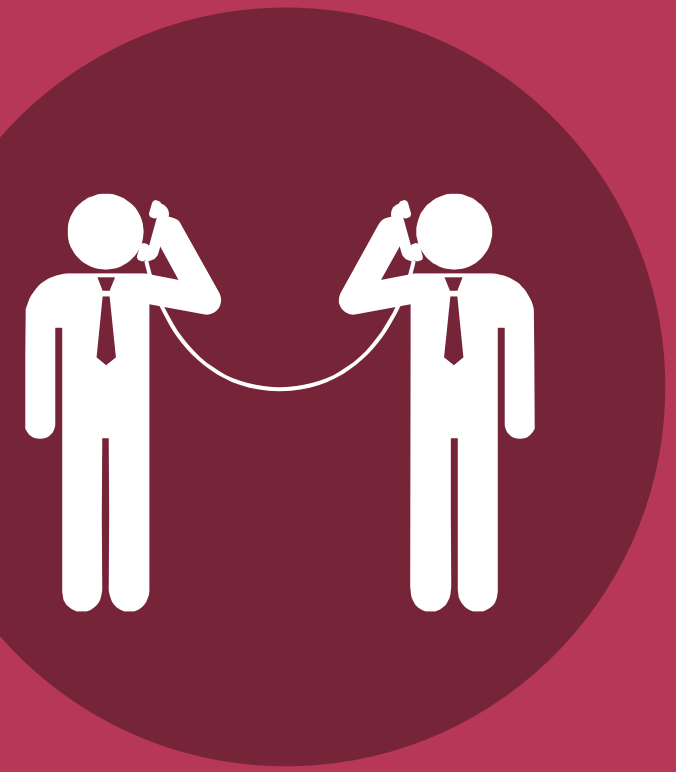
Create risk mitigation actions for priority risks. For all those risks that you want to actively treat you should create a mitigation action plan. With mitigation actions, the objective is not necessarily to eliminate the risk in its entirety. You will need to consider the cost/benefit perspective on treating or not treating a risk.

04 | Risk monitoring

Reassess the risk regularly. A key objective of monitoring risks is so that assurances can still be given that the organization's risks are being managed effectively. The risk assessment should be reviewed regularly by the personnel responsible for the risks, providing an updated score based on:

- Mitigation progress and other recent developments that may affect the risk profile.
- Identification of new risks since the last risk review meeting.

In addition to periodic strategic risk reviews of the success of the process, there is a range of operational information you can use when conducting reviews. For example, the log of incidents will provide an indication of how effective the risk treatment process and internal controls have been.



05 | Risk reporting

Consolidate the information and check risk progress. Reporting on the risk management framework is a process that applies at all stages in the risk lifecycle, though it is fair to say that it is most critical at the monitoring stage. The reporting framework is therefore something that should be defined at an early point in the risk management framework, by focusing on report content, format and frequency of production.

Risk profile, critical risks, mitigation actions progress, risk status, risk trend and heat maps are some of the types of risk reports that you might want to put in place for each stage in the risk lifecycle.

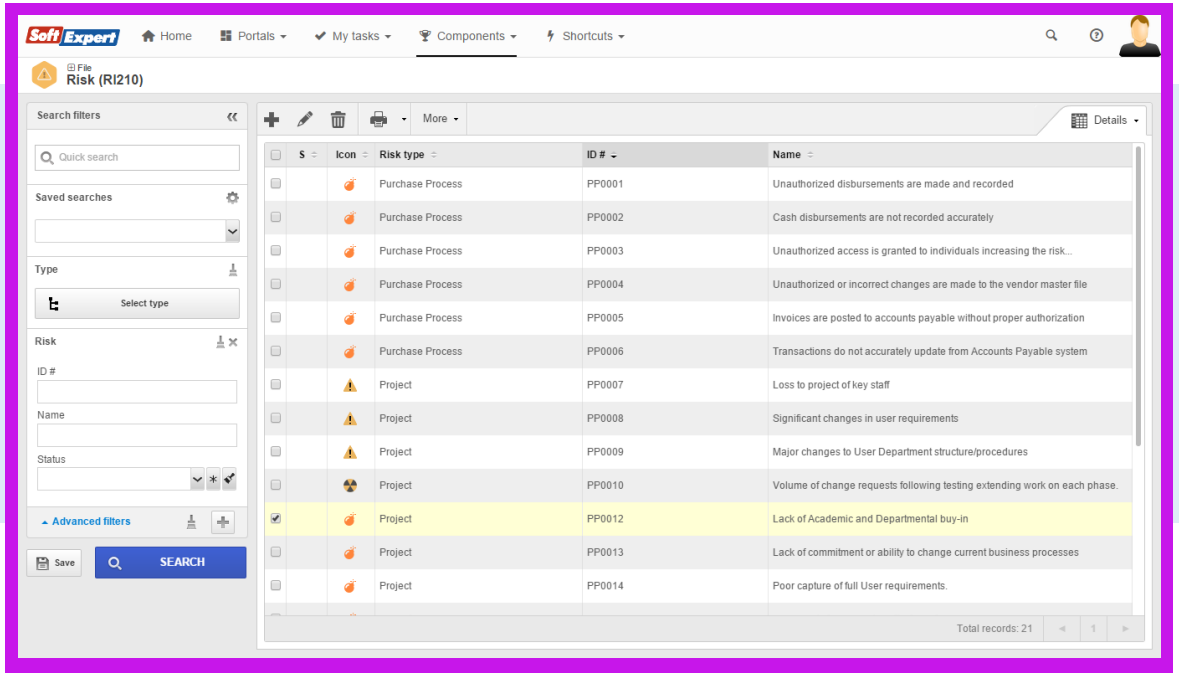
Now that you already know the **main steps for an effective risk management process**, find out more about the most complete and innovative solution on the market for enterprise risk management excellence.

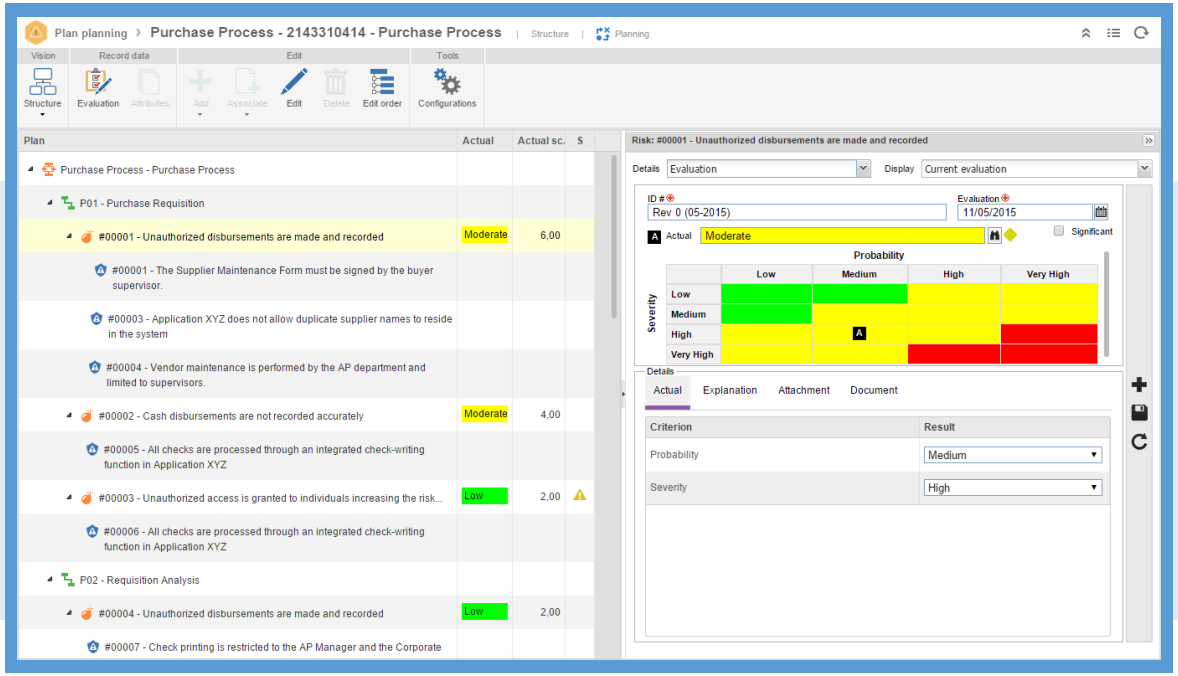
SoftExpert ERM

Reduce risks. Seize opportunities.

SoftExpert ERM software enables organizations to identify, analyze, evaluate, monitor, and manage their enterprise risks using an integrated approach. It brings together all risk management-related data in a single comprehensive environment, including a reusable library of risks and their corresponding controls and assessments, events such as losses and non-conformities, key risk indicators, issues and treatment plans.

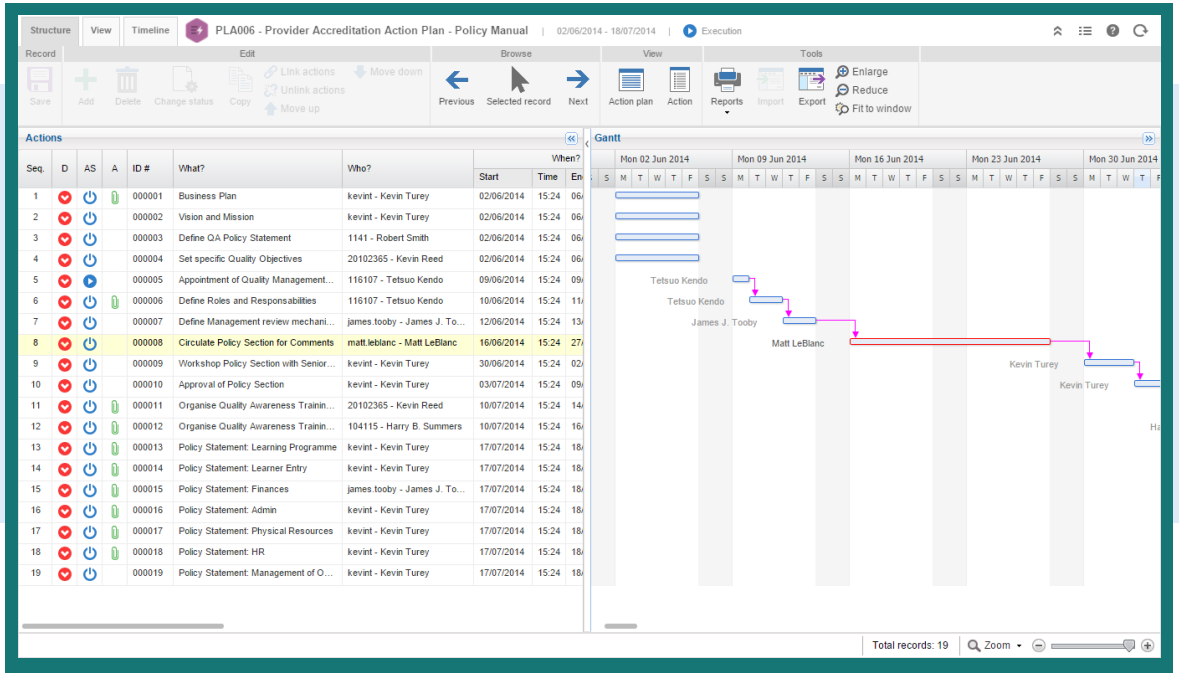
Risk identification

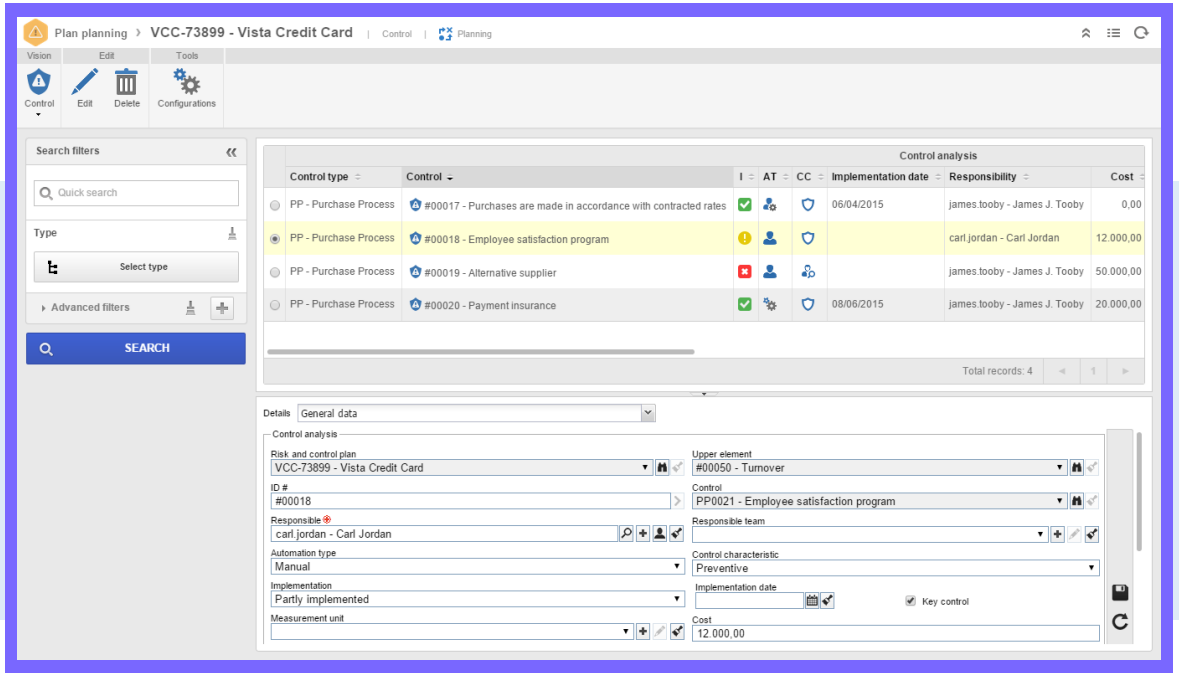




Risk assessment

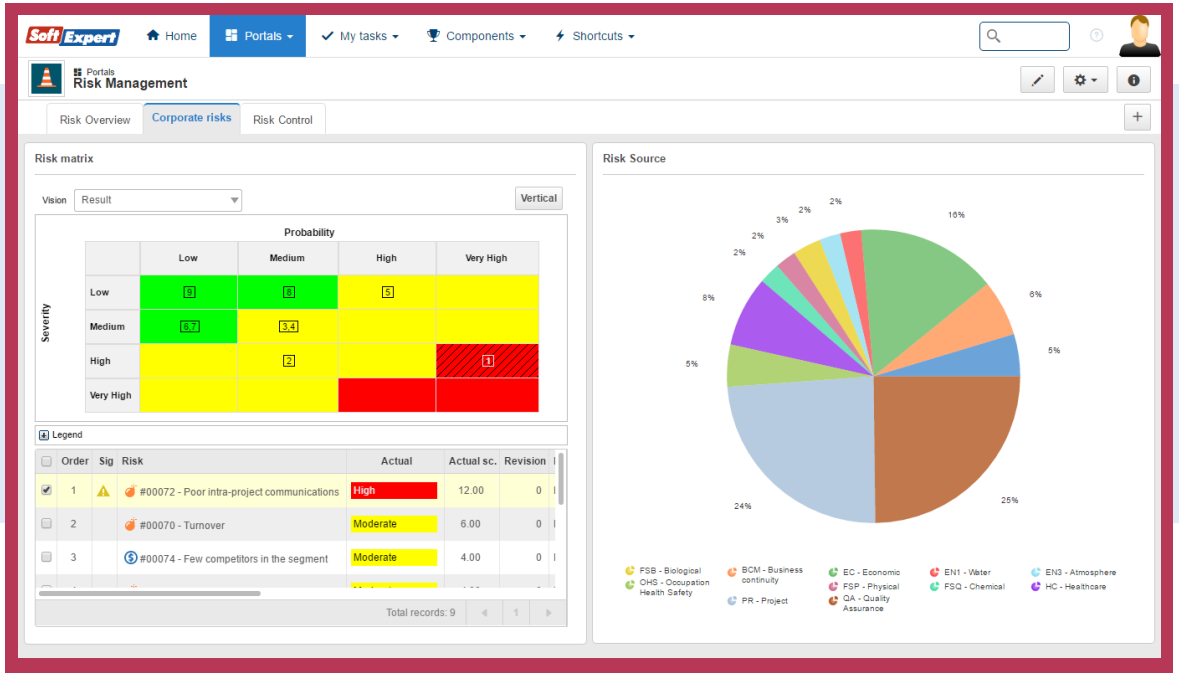
Risk treatment





Risk monitoring

Risk reporting



About SoftExpert

SoftExpert is a market leader in software and services for enterprise-wide business process improvement and compliance management, providing the most comprehensive application suite to empower organizations to increase business performance at all levels and to maximize industry-mandated compliance and corporate governance programs.

Founded in 1995 and currently with more than 2,000 customers and 300,000 users worldwide, SoftExpert solutions are used by leading corporations in all kinds of industries, including manufacturing, automotive, life sciences, food and beverage, mining and metals, oil and gas, high-tech and IT, energy and utilities, government and public sector, financial services, transportation and logistics, healthcare, and many others.

SoftExpert, along with its extensive network of international partners, provides hosting, implementation, post-sales support and validation services for all solutions to ensure that customers get the maximum value from their investments.

Take your business to the next level

www.softexpert.com | sales@softexpert.com