

# WHITE PAPER

Implementing ISO 31000 with  
Active Risk Manager

---

## STARTING WITH ISO 31000 – A BUSINESS SCENARIO

# Implementing ISO 31000 with Active Risk Manager

You are working in a growing organization, risk and its management has become increasingly important to your organization's performance. The current risk management process is outdated and leaving the organization exposed. You have been given the task of reviewing and implementing changes to improve the process.

Your copy of ISO 31000 is on your desk and you think you can use it as a basis for your revised risk management process. Good start – but how can you turn the theory into reality?

### THE WHAT, WHY AND HOW

Like any standard, ISO 31000 is strong on the 'What'. It tells you what the components of the system are called and which components you may need in your process. There is less about the 'Why'. This detail will be needed to support the business case. You will need to prove that the investment being made is returning good value for the business. Within the ISO standard, some of the connections are clear, others are merely hinted at, some are not mentioned at all.

When it comes to the 'How', as could be expected, standards documents have less to say - it is not their purpose. Turn to the front cover of ISO 31000 and it says 'Principles and Guidelines', that is not 'How'.

We have put this paper together to flesh out the concepts introduced in ISO 31000 with more detail from our own risk management project experience. This is will help you implement ISO 31000 effectively in your own business.

### WHERE SHOULD YOU FOCUS?

When advising people on risk management processes, our experience from numerous risk management projects suggests that there are three major elements to think about:

- The risk management principles, policy, framework and process documentation
- The risk culture of the organization
- The risk recording and sharing system

These are all touched upon within the documentation of the ISO 31000 standard.

### A GUIDED TOUR THROUGH ISO 31000

Below you will find a guide to how the ISO 31000 document relates to each of the three major elements of risk management. It would be useful to have a copy of the ISO 31000 document as you read the next section.

- **The risk management principles, policy, framework and process documentation** (ISO 31000: Page 2 Clauses 2.3, 2.4 and Page 3 Clause 2.8). This relates to the suite of documents that tell people what a risk is for your organization. It encapsulates the organization's method for capturing risks, exploiting opportunities, establishing the appetite for risk held within the business and it lists the principles against which the organization operates. Turn back to page vii in ISO 31000 and you have the structure for that documentation set.
- **The risk culture.** How does the organization engage with risk and its management? How can a culture of managed risk taking within the boundaries set by management be fostered and maintained? How can this culture be developed from where it is to support the more mature process you are trying to introduce?

Establishing and driving the cultural change needed is often the most neglected part of risk management. So many see it as a side show, but the truth is the risk culture needs to be centre stage. Without the right risk culture the policy, process and performance in risk management will flounder. ISO 31000: Page 3 Clauses 2.10 and 2.11 External and Internal Context; these are the clues. Clause 4.2 on Page 9, alignment between culture and policy is seen as important. Clause 4.3.3 on Page 11, it is easy to see true accountability depends on the

right risk culture and this too is recognized within the standard. Look at the principles (Page 7 Section 3 Principle H) – risk management takes human and cultural factors into account. Getting the culture right and keeping that culture alive is key to a successful risk management process.

- **The risk recording and sharing system** (ISO 31000: Page 14 Section 5.2 Communication and consultation. Page 20 Monitoring and Review). How are the communication and reporting goals going to be achieved with a sub standard data recording and sharing system? How about meeting the principles that provide the business case for the risk management system, can you afford to fall short in this area? What do the ISO 31000 principles suggest? Page 7 Section 3 Principles. F) Best available information. E) Risk management is systematic, structured and timely. J) Risk management is dynamic.

Go ahead, take a look at the array of Excel risk registers currently in use in your organization. Is Excel really up to the task or is it part of the problem? Being able to adequately capture the risks, share the information appropriately and in time, mine the risk information for subtle changes; this is how risk management will meet the ISO 31000 principles which relate specifically to process:- ISO 31000 Principles: A) Risk management creates value and protects. B) Risk management is an integral part of decision making. D) Risk management explicitly addresses uncertainty I) Risk management is inclusive and transparent. Note principle D) is clear about addressing uncertainty and that means the information cannot be locked away in multiple spreadsheets or in a tool that lacks the ability to share the information at an enterprise level.

Get these three elements right for your organization and get them working together and you have a living risk management process that will meet the organizational principles of ISO 31000. See principles G) Risk management is tailored [to your situation] and K) Risk management facilitates continual improvement of the organization.

#### **SYSTEMS TAKE ON A LIFE OF THEIR OWN**

ISO 31000 certainly provides for all the right process components and by consolidating them under three headings we hope we have started to clarify how these components depend on each other. It should also be clear now that risk management requires a systematic approach to process design.

Such an approach recognizes that each component interacts with the other components. Often, as in the case of a good risk management process, those interactions can be quite complex. Systems also have some strange properties. Components that make up a system interact to provide another set of emergent properties which make the system 'greater than the sum of its parts'.

In systems, failure to maintain adequate quality in any one part can threaten the whole system. In a risk management context, this is often where risk management programmes fall down. People may not understand or respect the system dynamics. As risk management consultants, we often see these kinds of systemic problems emerge. This is why all three risk management elements need constant focus.

#### **HOW CAN ACTIVE RISK HELP?**

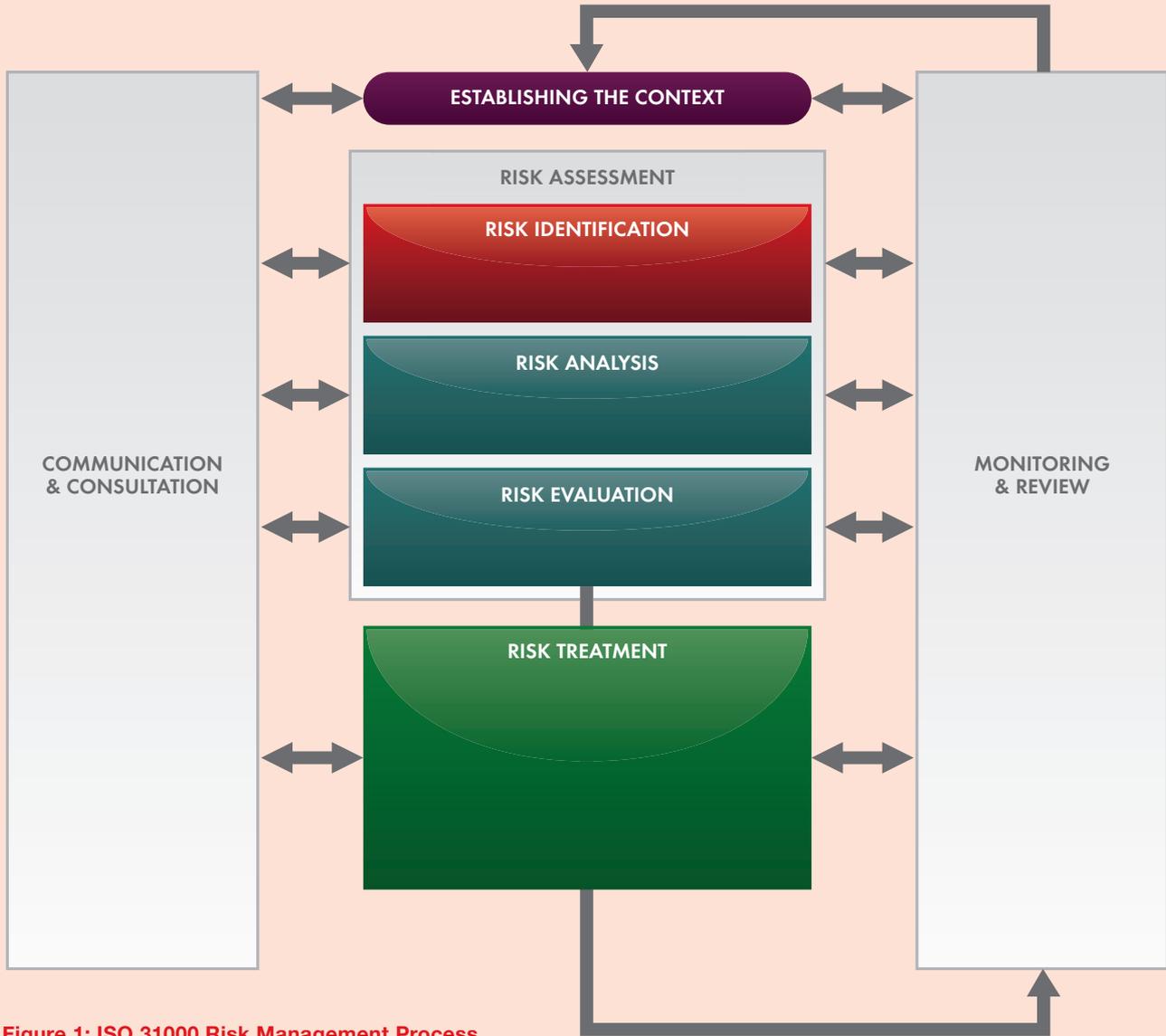
Active Risk Manager (ARM) software is recognized as having "the most extensive range of risk management capabilities currently available". ARM underpins enterprise risk management (ERM) projects in over 170 of the globe's most respected and demanding organizations, projects and supply chains.

We have been helping our customers, not just to implement ERM, but also to embed a risk-and-opportunity aware culture which turns what is often seen as a 'cost of doing business' into a system which can drive improved corporate performance.

At Active Risk we have seen how the right system supported by the right process, in the right environment can yield true value to an organization. Let's start by describing how the concepts in ISO 31000 can be turned into reality in your own company with the features which have been built into ARM based on our ERM project experience.

#### **ARM AND THE ISO 31000 RISK MANAGEMENT PROCESS**

**Figure 1** on the next page shows what ISO 31000 names 'the risk management process' (ISO 31000 Page 14, Figure 3). It is called the risk management process, but it does not address the supplementary parts of management engagement and supporting documentation, those are shown in the diagram on page 2 of the ISO document. As you can see there are three major sections to this diagram and we shall address these one at a time. In the central section, you have the data capture stage. **Establishing the Context** is an important step and it is the policy and procedural documentation that will help you most here. What constitutes a risk for your organization? What is the scope of activity that should be looked at through the risk management process?



**Figure 1: ISO 31000 Risk Management Process**

The next block of steps, encapsulated under the title **Risk Assessment** allows you to identify the risk in line with your procedures and policy as well as assess its potential impact on your organization. **Risk Analysis** in this context is looking at the impact the risk may have in ways the organization can understand, normally money, time, reputation etc. **Risk Evaluation** is about assessing each risk’s importance to your organization so you can prioritize your resource allocation and decide what to do in the last step of this section, the **Risk Treatment Plan**.

**CAPTURING RISK AND OPPORTUNITY DATA WITH ARM**

**Figure 2** (opposite) is the same diagram overlaid with some of the elements of ARM that will enable you to capture this important information.

In ISO 31000 a risk is defined as:

*[The] ‘effect of uncertainty on objectives’*

The ISO definition means a risk can be a threat or an opportunity. ARM allows you to capture both risks,

which could have a negative result, and opportunities. Employees may not have all the information about a risk or opportunity at the outset, so ARM also lets you capture the full range of ‘sources of uncertainty’ such as concerns, assumptions and expectations.

ARM also enables the recording of, not only quantitative information, but also qualitative data. This allows us to gain context around the risk or opportunity. For example, causes, in other words what might lead to the risk occurring, and consequences, which is a way of describing the impact the risk may have in general terms that people can understand. ARM also captures the Risk Owner, as defined in ISO 31000 Clause 2.7.

Once we have entered the risk, ARM lets us record the impact that risk may have in up to twelve different ‘impact categories’. This is a rich recording environment that allows both qualitative and quantitative assessments of those impacts to be made. ARM will then show the Risk Score which sets the risk in

context with the Risk Evaluation process set out by the organization.

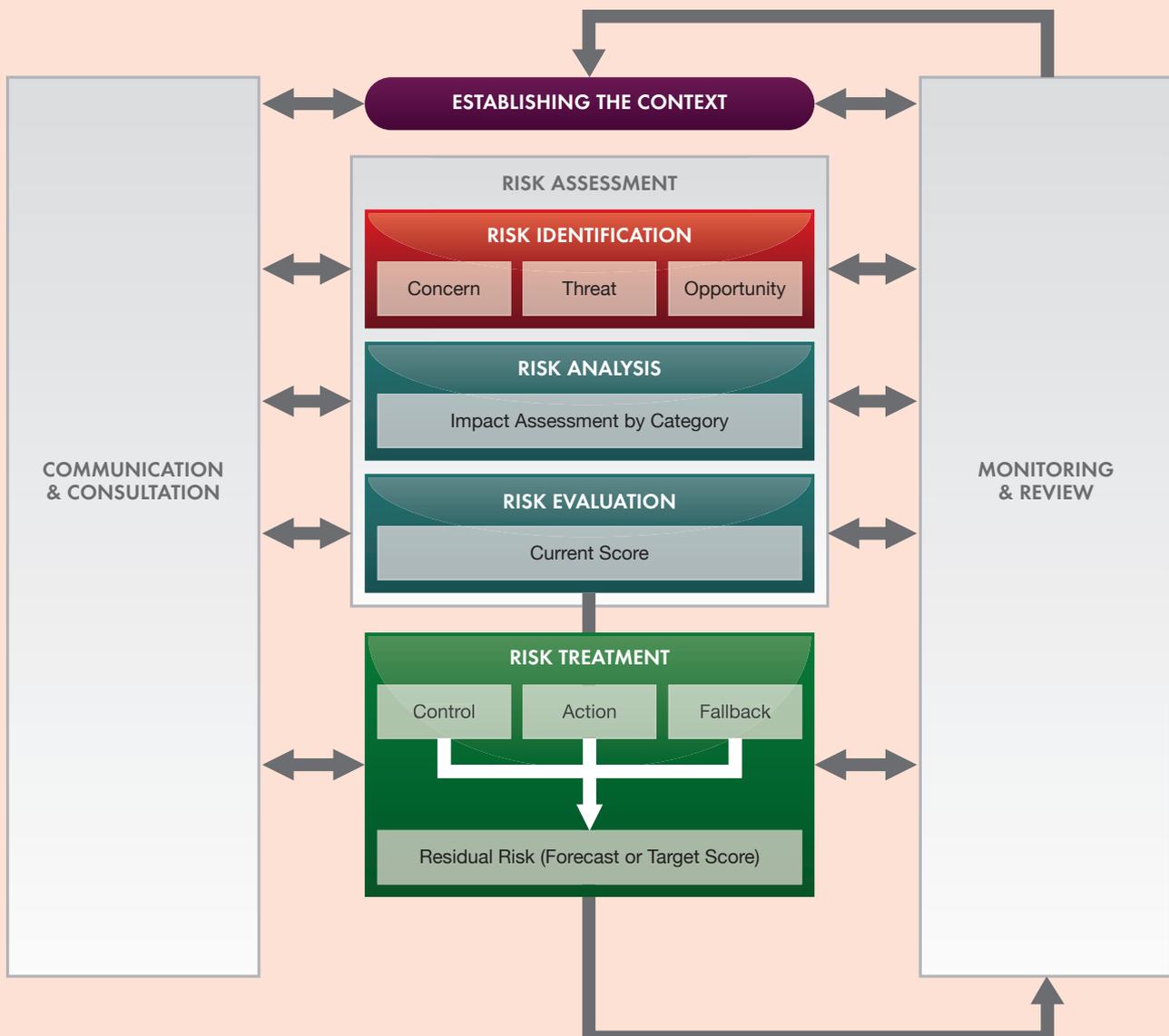
When recording the Risk Treatment that has been decided, ARM allows separate configurations for Controls, Actions and Fallback plans. This is important as each serves a different function. Put in simple terms:

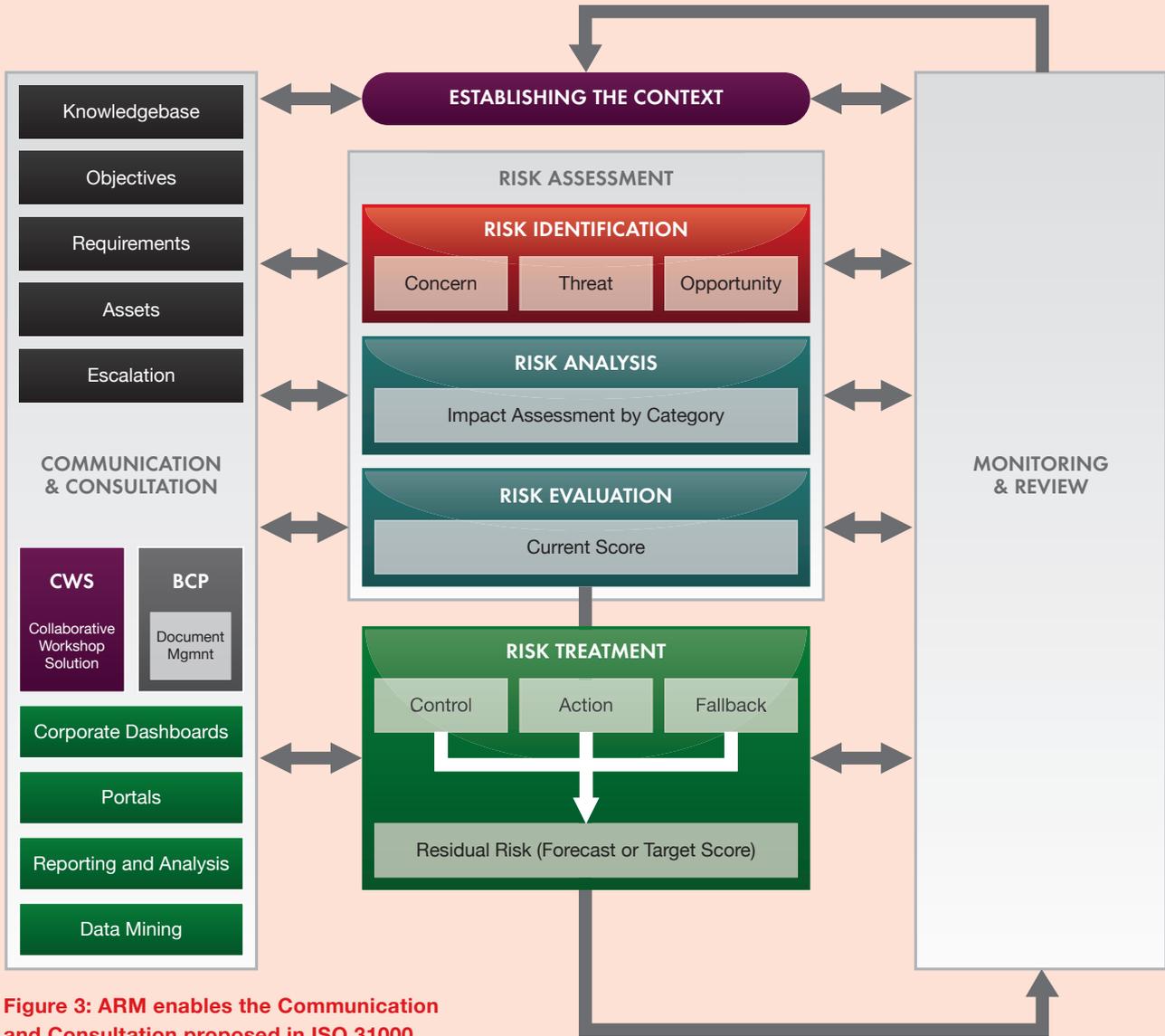
- **Controls** are activities that are in place for an extended period of time to either prevent or detect the occurrence of a risk.
- **Actions** are activities which may be undertaken to change the impact or likelihood of a risk occurring. Actions may lead to new Controls being put in place
- **Fallbacks** are the category most often overlooked by organizations. No matter how well a risk is managed, in some cases a risk may still occur. Fallbacks make up the backup steps which should be instigated if the risk occurs

By allowing users to record a rich set of information around risks, opportunities and the organization's response plans, ARM provides an excellent resource of information to support the two other major sections outlined in ISO 31000 – namely 'Communication and Consultation' and 'Monitoring and Review'.

Earlier we highlighted the need to make the business case for risk management and show value from your investment. One of the ways value can be shown in the risk management process is to use the Treatment Plan to present how the level of risk will be reduced (ISO 31000 Clause 2.23). ARM allows you to record the current risk level and the level of any residual risk (ISO 31000 Clause 2.27).

**Figure 2: ARM data capture and the ISO 31000 Risk Management Process**





**Figure 3: ARM enables the Communication and Consultation proposed in ISO 31000**

**COMMUNICATION AND CONSULTATION**

This left hand side of the model (Figure 3) is about engaging with the organization as a community and it relates very much to the inclusive principles of ISO 31000. ARM is designed to be used enterprise-wide and even with project partners and suppliers. Conversely there is often a need to limit access to information of a sensitive nature. ARM allows for sophisticated access rights to be maintained for each user.

With traditional and spreadsheet-based risk recording systems, having your data captured, but locked within a hard to access and use tool, means employees often see the effort involved in capturing data but can't see benefits which result. This is a quick route to user rejection of the system and will not embed a risk and opportunity aware culture into the organization. Using ARM will unlock the information and knowledge captured.

Using the powerful data mining features within ARM – we call this Filtering – together with ARM's Microsoft Reporting Services interface with our standard reports and custom reports developed specifically for your organization – will turn the raw data into usable information and insight. Information and knowledge is what people value and use to make decisions, so the ability to develop high quality reports to suit the different needs of groups within the organization is an essential element of making the risk process work.

Not everyone in the organization needs to be so close to the risk process day-to-day or has the time to fully learn how to use the capabilities in ARM. However they may need to gain the value from the information ARM holds. Audit committee members, board members and non-executive directors, particularly with their increased responsibility for corporate governance, want to get the distilled information to better inform their decision making. These groups need to benefit

from the real time, rich content held within ARM. Our portal capabilities allow information to be drawn from ARM reports, graphs and executive dashboards. These can all be integrated alongside other management information through the portal capabilities which are part of the ARM solution.

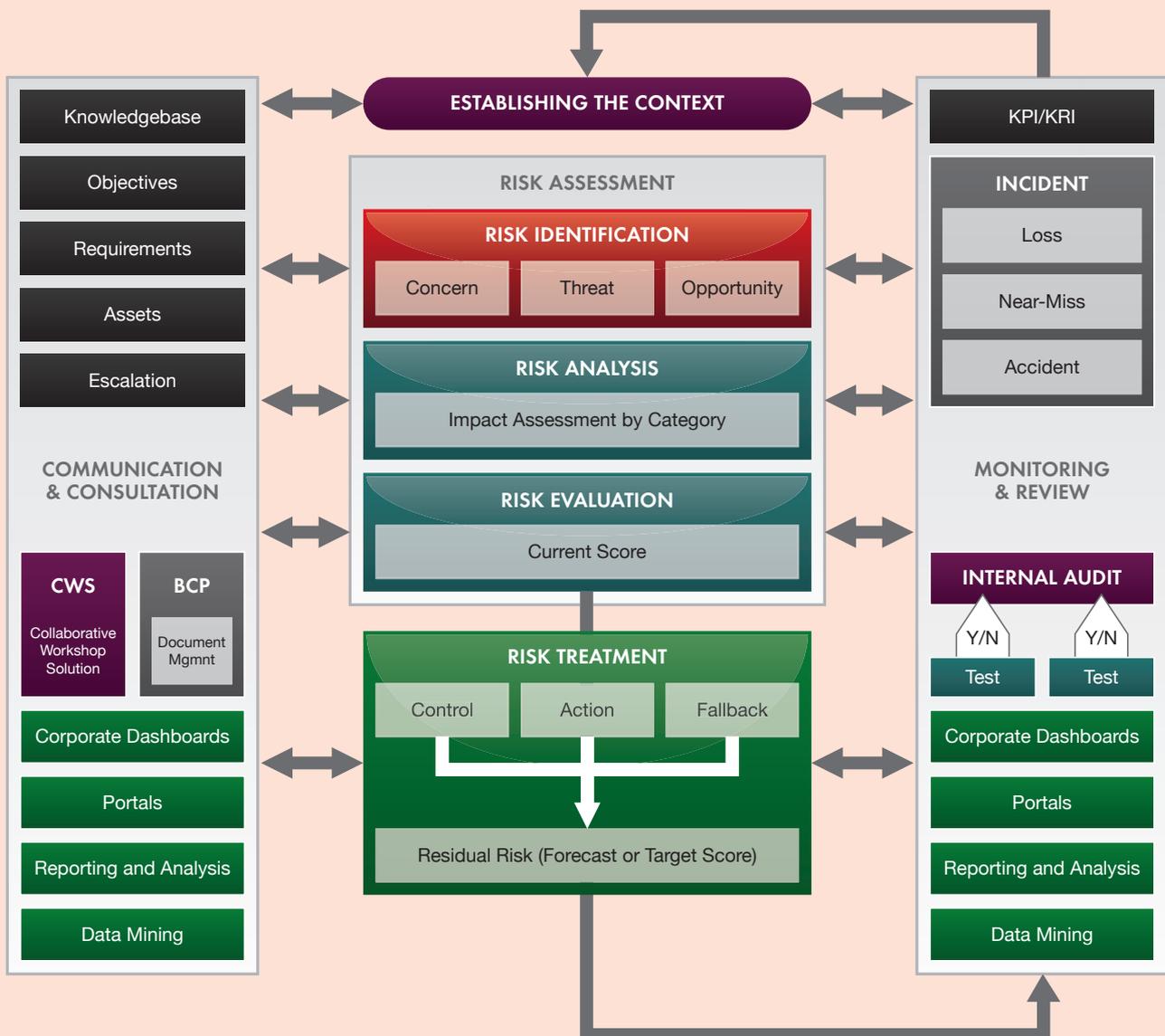
In the spirit of ISO 31000 all types of organizational risks should be managed within a single system, Specific risk-related needs within the business, such as business continuity planning (BCP) are already recognized in the ARM solution and special reports are available out of the box to help organizations get started in such areas.

Engaging with all levels within the organization is vital to communicate corporate risk policies and to consult with people in the field who often understand the risks and opportunities best. However all this information needs to be collected in a common way so that it can be evaluated at the corporate level. To make this happen

Active Risk has developed CWS, the Collaborative Workshop Solution, which integrates with ARM. CWS supports risk and opportunity capture via risk workshops which can be held at remote locations with no connection to the corporate system. Data is then uploaded to the central ARM database later to keep the data integrity and to deliver a complete picture for management.

CWS can also sit at the centre of your risk review process and be used for management team planning sessions. As part of our range of services, Active Risk provides training, not only in how to use CWS, but also in the techniques for running a productive risk workshop or risk review.

**Figure 4: ARM enables the Monitoring and Review proposed in ISO 31000**



Often, you need to look at the business from a particular view point to see risks that will have strategic importance. Asset-rich organizations or businesses who must supply to tough customer requirements may want to look at their organizations from these perspectives. ARM provides customizable views to support Asset, Requirement or Objective-based perspectives right across the risk register.

Escalation is also an important part of risk management to ensure key risks are identified and brought to the attention of management. ARM provides escalation which can be customized to reflect the organizational hierarchy. This will enable key risks to be escalated, actioned at the right levels and for patterns and trends of risks to be identified which could impact strategy.

#### MONITORING AND REVIEW

The ability to monitor and review is vital to transforming the risk management process into a dynamic, continuous improvement system in line with the ISO principles. An organization needs a system which will give the ability to monitor the risks, to check progress is being made in managing these risks, and the ability to assess the performance of the risk management system itself.

Looking at the last section of our diagram (**Figure 4**) on the previous page, you can see how ARM's capabilities enable this aspect of the ISO process. ARM provides data mining (Filtering), which allows risks with some common relationship to be drawn together, and extensive reporting capabilities. This, and a range of other features, means ARM will provide a living, dynamic risk system which goes way beyond static, periodic paper-based or disconnected spreadsheet methods.

For any organization implementing a Control Environment, the effectiveness of those Controls needs to be monitored by a process of Internal Audit. ARM supports the Internal Audit practice of establishing an 'Evaluation' audit process and the ongoing application of testing to ensure that the effectiveness of the Controls remains sound. ARM underpins the whole process, allowing the Evaluations to be developed, the tests applied and the history of the testing process to be examined. In addition to feeding into the normal Audit Report, the ARM reporting capability can be used to summarise Control Environment performance for risks.

The reporting and audit capabilities provided by ARM will support the growing demands on the organization for increased transparency and the need to show evidence-based decision making. Rating agencies, such as Standard and Poors, are looking for a demonstrable

enterprise risk management approach when deciding the credit rating to assign to a business. The information from ARM will also underpin this credit rating process.

Delivering up-to-date risk information into management and employee portals can be a real help to embed a risk and opportunity aware culture. Quick and available, easy and informative; portal 'reports' range from summarized dashboards or detailed drill-downs. It's about risk management being tailored to the organization and the different needs of employees and job roles. This is an important part of the ISO 31000 principles.

To support continuous improvement, and to see where the value is being derived from the risk management process, an organization needs to track any incidents which occur and show their relationship to identified risks. Equally important an organization needs to monitor the results of near miss incidents. ARM allows incidents to be tracked and linked back to the risks that preceded them. By analyzing this information through ARM, the organization can quantify the real benefit of addressing risks and opportunities as required by ISO 31000 in its principles and guide future efforts with more focus and direction.

#### ISO 31000, BALANCED SCORECARDS AND ARM

Some organizations with a high risk maturity or where the ISO 31000 process is being introduced alongside Balanced Scorecards want to consolidate their monitoring through Key Performance or Key Risk Indicators. Carefully selected measures and Balanced Scorecard approaches are becoming common place among larger organizations. Again, ARM allows risks to be assigned and tracked against an organization's Scorecard parameters.

#### IN SUMMARY – IMPLEMENTING ISO 31000 WITH ACTIVE RISK MANAGER

ISO 31000 represents the encapsulation of many good principles and steps for an effective risk management process, but it is not within its scope to outline a practical implementation strategy.

Active Risk Manager software has been recognized as having the most extensive range of enterprise risk management capabilities currently available. ARM, together with the real-world experience of our industry practitioners and services team, will provide both the system and implementation capabilities needed to make the ISO 31000 theory a practical reality.