


# P&SM: Risk Management



Risk management facilitates the taking of decisions and actions to control risk appropriately by providing a disciplined and objective approach.



CIPS members can record one CPD hour for reading a CIPS Knowledge download that displays a CIPS CPD icon.

### Introduction

The CIPS' practice documents are written as a statement in time. They are a collection of views on good practice within a particular subject area and are intended to provide direction on good practice with some guidance for context and interest. The reader is encouraged to use the CIPS practice documents for their own purposes, such as writing policy statements, guidance or procedures. This particular practice statement has been written primarily for the benefit of full-time purchasing and supply management professionals, but can be used by anyone associated with, or interested in, purchasing and supply management (P&SM).

This document is about risk management.

### Definition

CIPS suggests that risk can be defined as 'the probability of an unwanted outcome happening'. Risk management facilitates the taking of decisions and actions to control risk appropriately by providing a disciplined and objective approach.

### Background

Risk management involves four key activities: risk recognition, risk analysis, risk assessment and risk mitigation.

Risk recognition is the process of identifying all the potential areas throughout the supply chain where risk is present.

Risk analysis is the process of analysing all the potential areas of risk and estimating the probability of each happening.

Risk assessment is the process of assessing the likely impact of a risk on the organisation. Highly predictable risks may have low impact and therefore it is possibly not worth taking any action to control or avoid the risk. On the other hand, low probability risks can have a significant impact and some form of action may be demanded 'just in case'. The cost of controlling or avoiding the risk needs to be taken into account.

Risk mitigation involves drawing up plans and assigning responsibilities in order to control and lessen the risks that have been identified and assessed. Risks should then be allocated to an owner who is responsible for managing them, possibly with the help of other team members.

### Explanation

#### Risk recognition/analysis

Risk recognition/analysis is part of the strategy development process. When a need is identified then a strategy is developed which takes into account all relevant commercial issues (such as specification, supply market, finance, etc.). Risk recognition/analysis methodologies allow all risks to be identified and objectively assessed. The purchaser can then decide on an appropriate sourcing strategy. Once the sourcing strategy is decided, the contract strategy can be formulated; it is at this stage that a decision of whether a risk/reward type contract is appropriate.

CIPS considers that risk recognition/analysis should be part of any significant purchasing and supply management process. For example, its use is vital when determining the overall strategy towards individual plans for categories of expenditure, sourcing and even, if appropriate, tactical procurement. It is a key skill of any P&SM professional and its use is key in controlling (as far as possible) the risks associated with any commercial activity.

The recognition/analysis can be either a simple or very formal process. The latter approach is more appropriate for high-value and high-risk projects such as a new IT solution (and may involve following a set procedure, working cross-functionally with colleagues, brainstorming and risk evaluation). Recognition/analysis can also be informal, using an iterative or intuitive process, for less significant procurements, or it may even be reactive, such as in response to a crisis.

There are no golden rules of best practice in risk recognition/analysis - the key is to be able to identify and analyse all the risks relating to a particular procurement including the impact of that procurement on the business, and to decide what level of effort is appropriate to the circumstances. For more complex situations, the risks can be brainstormed and categorised into groups such as 'technical risks', 'financial risks', etc. Alternatively, a more detailed approach may be adopted. In some public sector areas, particularly for IT or PFI projects, there are quite specific analyses to be undertaken and failure to address all aspects fully can result in rejection of the procurement by a higher authority such as the Treasury.

The second stage is to assign a level of probability to these risks. Some methods express the impact of the risks and the cost of controlling them and so decisions on trade-offs can be made.

### Risk Assessment

It may be that some risks are not very easily controlled or managed. These may fall into the category which needs to be insured, if indeed the insurance market is prepared to insure them. The process of risk assessment is not all encompassing, as there is usually a degree of uncertainty. This uncertainty increases as the probability of the unwanted outcome increases. Uncertainty can be addressed by 'sensitivity analysis'. This involves manipulating the variables or assumptions, i.e. events that can lead to the unwanted occurrence, to see the effects of these. It can illustrate where the outcomes may be different if some assumptions are incorrect.

Another point to consider during risk assessment is 'compensating behaviour', where people who are aware that a particular risk is being controlled or managed, compensate by doing more of the unwanted behaviour, thereby increasing the risk. An example would be insuring laptop computers; where laptop computers are insured against loss or theft, some users take less care over their protection and leave them in their cars overnight, etc.

### Risk Mitigation

The allocation of risk should be dependent on the assessment of the likelihood and consequence of the risk and then the identification of who is best able to control or manage that risk. This is an important aspect of any significant procurement and so something in which P&SM professionals should be involved.

Having allocated the risk, the issue of what is a fair reimbursement mechanism is a related but separate issue. Like all reimbursement it should be fair and reasonable. Forcing vendors to assume risks they cannot control by offering an incentive or a reward is not good practice.

It should be remembered that risks change over time. Risk assessment should be iterative. CIPS recommends that when undertaking whole life costing, purchasing and supply management professionals should identify the relevant risks associated with each stage in the life of the product/service. Thus in some cases, risk might increase dramatically towards the end of the life cycle due to end of life problems such as disposal or obsolescence.

One route to risk mitigation is insurance. CIPS suggests that purchasing and supply management professionals ascertain what insurance arrangements their organisations have in place as some risks may already be covered by insurance. It is also good practice to understand what insurance cover your supplier has in place that is relevant to the requirement. Equally, insurance is not always appropriate if the risk in question is not an insurable risk or if the risks can be managed properly by the parties to the contract. .

Some aspects of risk can be transferred to suppliers, where it is appropriate and agreed. Risk mitigation is a calculated trade off. Too much risk transfer to a supplier will simply lead to cost increases as the supplier seeks to offset the risk. Insufficient transfer of appropriate risk leads to the buyer accepting a disproportionate amount of the risk, which might be better accepted and managed by the supplier.

CIPS' position is that risks are best allocated to the person or party best able to manage them. This may be in terms of expertise, time and/or resource. Where this is a supplier, or a sub-contractor, P&SM professionals should be mindful of the fact that suppliers are likely to build in a suitable contingency amount to charge the buying organisation.

### **Risk from the viewpoint of the supplier**

If the supplier perceives risk to be high they will naturally build in extra safety and extra margin. An effective buyer will try and identify and improve upon areas of concern. Often this can be done in discussion with the supplier and involves little, if any, cost or compromise on behalf of the buyer. There are a number of sophisticated computer programs in the marketplace to aid the process of risk management.

### **The role of the P&SM professional**

CIPS holds that the P&SM professional's role regarding risk management is to:

- Identify and promote the business need for robust risk management in procurement and supply management
- Identify who in their organisation is/should be responsible for this and work with them in analysing and assessing the risks
- Inform himself/herself sufficiently about the supplying organisation(s) and the people involved to make discretionary judgements about the balance of probability of the supplier causing or allowing risks within their own control, to materialise
- Make a value-added input to commercial decision by leading a commercial risk assessment in the development of commercial strategies



- Be fully conversant with a range of contract strategies that can be applied when setting up contracts to achieve best value in meeting organisational objectives

Various purchasing and supply management techniques can make a substantial contribution to this process, for example supplier appraisal or tender evaluation can minimise the risk of using unsuitable suppliers.

Where there is no-one identified as responsible for risk management, the P&SM professional should communicate probable risks to all internal stakeholders. They should seek to challenge assumptions and encourage colleagues to manage risks. Where there is little interest, the P&SM professional should take responsibility for all significant procurement risks and document these accordingly, e.g. assessing a potential supplier's financial standing, taking references etc. For complex projects a cross-functional team should assume responsibility for risk management and the P&SM professional may well lead this team.

With respect to wider business issues (such as risk to reputation) CIPS would advocate that, as a P&SM professional often has an external focus in the organisation, he/she has a responsibility to feed into the organisation anything they detect which may generate a risk to the business. CIPS firmly believes that all P&SM professionals have a responsibility to understand the objectives of their organisation and to ensure that the procurement strategy is in line with the corporate strategy and the wider business objectives.

### Skills required

CIPS believes that in order to undertake risk management, P&SM professionals should have:

- A knowledge of the risk management techniques available and an awareness of ISO 31000, the global risk management standard<sup>1</sup>
- An analytical mindset with an ability to prioritise and to build a risk management framework
- The skills to assess risk effectively and to select and apply appropriate risk management techniques
- Knowledge of the external marketplace and relevant regulation
- The relationship that risk management has with governance and other functions. Supply chain awareness and an awareness of global issues such as culture and communication when building an effective risk management framework

### Conclusion

Organisations are increasingly aware of the importance of managing risk. CIPS believes that P&SM professionals can add value to any risk management process within an organisation, whether or not it is directly related to P&SM.

CIPS believes that an awareness of risk should be regarded as a positive trait in the successful buyer; it should not be seen as an expectation that things will go wrong, but rather an

---

<sup>1</sup> The Institute of Risk Management (IRM) has produced a paper on "A structured approach to ERM (Enterprise Risk Management) and the requirements of ISO 31000 [http://theirm.org/documents/SARM\\_FINAL.pdf](http://theirm.org/documents/SARM_FINAL.pdf) (last accessed 08/10/2012)

alertness to the fact that they might do so, coupled with a readiness to take positive steps to prevent undesirable outcomes.

---

**CIPS Group** Easton House, Easton on the Hill, Stamford, Lincolnshire, PE9 3NZ, United Kingdom  
T +44 (0)1780 756777 F +44 (0)1780 751610 E [info@cips.org](mailto:info@cips.org)

---

**CIPS Africa** Ground Floor, Building B, 48 Sovereign Drive, Route 21 Corporate Park, Irene X30, Centurion, Pretoria, South Africa  
T +27 (0)12 345 6177 F +27 (0)12 345 3309 E [infos@cps.org.za](mailto:infos@cps.org.za)

---

**CIPS Australasia** Level 8, 520 Collins Street, Melbourne, Victoria 3000, Australia  
T 1300 765 142/+61 (0)3 9629 6000 F 1300 765 143/+61 (0)3 9620 5488 E [info@cipsa.com.au](mailto:info@cipsa.com.au)

---

**CIPS Middle East & North Africa** Office 1703, The Fairmont Hotel, Sheikh Zayed Road, PO Box 49042, Dubai, United Arab Emirates  
T +971 (0)4 327 7348 F +971 (0)4 332 5541 E [mena.enquiries@cips.org](mailto:mena.enquiries@cips.org)

©CIPS 2013



*Printed on stock containing  
50% post consumer  
recycled content*

---

[www.cips.org](http://www.cips.org)

CIPS™ is a registered trademark of the  
Chartered Institute of Purchasing & Supply