Bowtie risk assessment methodology in practice

Bradley Hocking[1], Chris Sproston[2]

Abstract Risk management is a term that is used widely in organisations managing physical assets, where hazards must be controlled to minimise effects on personnel, environment and performance outcomes. Managing such risks requires a risk assessment methodology that is sophisticated enough to sufficiently evaluate the risk but simple enough so that stakeholders can make sense of it. Furthermore, the risk assessment needs to be considered as part of a system which can also ensure actions are taken as they need to be. Bowtie Risk Assessment (RA) is a methodology that allows risk to be evaluated in terms of multiple scenarios surrounding an unwanted event, and presents a holistic picture of the overall risk which is easy to communicate. The methodology is particularly suitable for risks that are complex either in the way that they can possibly manifest, or in the way that they could impact an organisation. This paper details the experiences of the authors in the development of bowtie RAs; the integration of these bowties into an Integrated Risk Management System (IRMS); and the successful transition of the IRMS into operations.

Keywords Bowtie, Risk, Risk Assessment

1 Introduction

1.1 Risk Management and Asset Management

For organisations managing physical assets, the term 'risk management' is not new. Risk management is well understood as being fundamental within the wider context of asset management and this is reflected in several different concept models, but perhaps most notably the Asset Management System model by Asset Management Council (refer to Figure 1). Perhaps this is because an obvious aspect of managing any substantial asset (such as a processing plant or railway network) is that hazards abound, and these must be controlled to minimise effects on personnel, environment and performance outcomes. Unfortunately, this is highlighted from time to time by the catastrophic effects of major incidents, such as Deepwater Horizon oil well blowout (April 2010), Santiago de Compostela derailment (July 2013), and Grenfell Tower fire (June 2017). In each of these incidents it is easy to focus on the minutiae of the actions leading up to the incident but above all, the common thread is a weakness in the management of risk across all levels of the organisations accountable for the assets involved.

ISO 31000 (ISO, 2018), originally published in 2009 and updated in 2018, serves as a superior guidance document even for those organisations not seeking to achieve compliance to the standard. It provides a high-level overview of risk management and how a system for risk management can be implemented. It suggests that a system for risk management can be characterised by three aspects, namely: principles, framework and process. The most important of these three for the subject of this paper is process and therefore this is described further in this section.

At the centre of the risk management process described in ISO 31000 are the activities of risk assessment and risk treatment, which are supported by four related activities, namely:

- Scope, context, criteria
- Communication and consultation
- Monitoring and review
- Recording and reporting

[1] B. Hocking
Shoal Engineering Pty Ltd, Australia
e-mail: bradley.hocking@shoalgroup.com

[2] C. Sproston
Shoal Engineering Pty Ltd, Australia
e-mail: chris.sproston@shoalgroup.com

Figure 1 Risk management is fundamental to asset management (Asset Management Council, 2014)

Risk assessment is decomposed into three steps referred to as identification, analysis and evaluation. The 'core' risk management processes can therefore be illustrated as something like that shown in Figure 2. In the authors' view, it is always worth noting that of all the elements within the risk management process described in ISO 31000, the most important is risk treatment. It is perhaps stating the obvious, but it is the physical actions taken by people within an organisation that reduces risk, not the presence of polices, manuals or risk registers. That is not to say that these are not important, but their sheer presence should not create the false belief that risk is now being adequately managed.

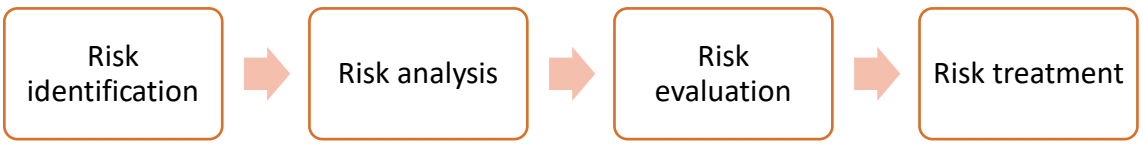

Figure 2 The core risk management process described in ISO 31000

1.2 Typical Risk Management Process

Many organisations have implemented a risk management system to minimise the likelihood and/or severity of unwanted events and in doing so are genuinely less exposed because of it. However, there are cases where underlying weaknesses remain hidden behind a false belief that the very existence of a risk management system will prevent an unwanted event. Where organisations are managing risks that could credibly result in catastrophic consequences (e.g. loss of life), finding and addressing such weaknesses should be paramount. In the author's experience, there are several practices that can contribute to ineffective risk management as shown in Figure 3. These are discussed further below.

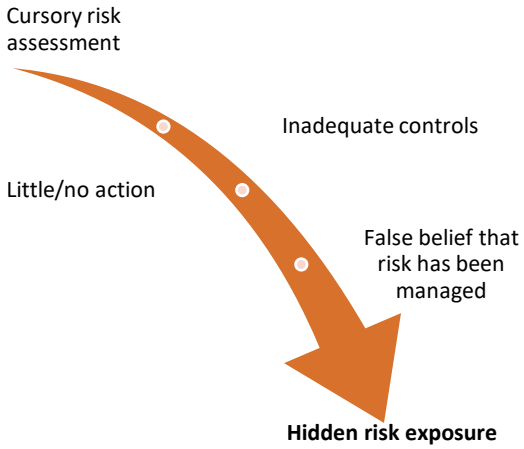

Figure 3 Practices contributing to ineffective risk management

An unintended outcome in some organisations is a culture whereby the purpose of risk management is to follow the process above all else. This focus on 'ticking the box' can be identified by the practices described in this section. In the worst case, risk identification is poorly thought through, risk analysis is non-existent, and the risk evaluation step is done with the aim of obtaining a number on a risk matrix. Such a casual approach to assessing risk then leads to inadequate controls being identified, either because the assessment is too low (or indeed, too high) or because the lack of risk definition/analysis means that it's too difficult to conceive of the actions that will truly control the risk. Not surprisingly, a lack of trust at this stage then leads to lack of commitment in actually taking the necessary actions to implement controls. The next situation to arise is a false belief that the risk has been managed, owing to the fact that all steps of the risk management process have been followed. It's possible to tick all the boxes but not materially reduce the risk and this leads to hidden risk exposure.

It is worth stating that all of the above indicators do not solely represent the actions of individuals but of the organisation – it is how the organisation sets up its risk management framework (of which the process is a part), how its people are trained and how the system is monitored that achieves better outcomes. In the next section, an enhanced risk management process is presented that can overcome some of the issues highlighted here.

1.3 Enhanced Risk Management

Fortunately, alternative approaches are available that can greatly enhance the effectiveness of risk management within an organisation. Firstly, this involves the application of a more rigorous risk assessment methodology referred to as the 'bowtie' technique. Secondly it relies on the data from the bowtie risk assessment being captured in a relational database – there are several software providers that can meet this requirement. Thirdly, the bowtie risk assessment data is coupled with the organisations maintenance and operations data to allow real-time appreciation of the whole-of-business risk position. Finally, the risk management framework must be adapted to the new ways of working that embed the new approach and provide more effective governance.

2 Developing Bowtie risk assessments

2.1 Overview

The origins of the bowtie methodology are not well documented but appear to be a combination of fault tree analysis, event tree analysis and root cause analysis. It provides a visual representation of a risk assessment (which looks like a bowtie – see Figure 4). The methodology gained traction (primarily in the oil and gas industry) after the catastrophic Piper Alpha incident in 1988 which resulted in the death of 167 people (Ross, 2008). Bowtie risk assessments are a better way of understanding a system upon which to conduct a risk assessment.

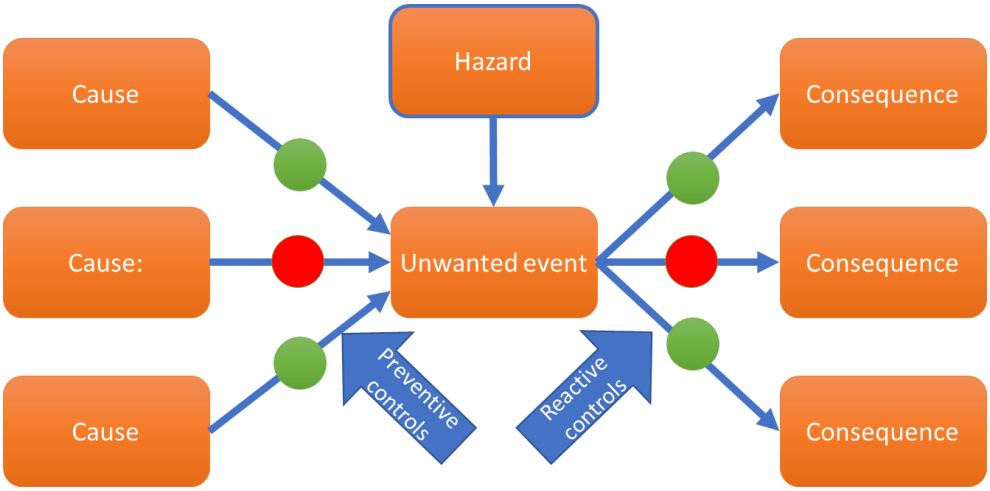

Figure 4 Example bowtie risk assessment diagram

2.2 Elements of a bowtie

A bowtie risk assessment is made up of distinct elements (refer to Figure 4) that can be clearly defined to achieve a consistent approach to risk assessment. Whilst this paper does not seek to be the authority on all aspects of conducting bowtie risk assessments, it is helpful if the reader has a basic awareness of these elements as they are an important aspect in creating an enhanced risk management system.

Hazard

Describes the situation that must be kept under control.in an asset management context this is typically an energy source (e.g. stored pressure, kinetic energy, electrical energy). Each bowtie diagram is focussed on one hazard only.

Unwanted event

Describes the point at which control of the hazard is lost, noting that nothing bad has happened yet, but it could do. To use a popular analogy, the ‘lion is out of the cage’. Each bowtie diagram is centred around a single unwanted event.

Causes

Each cause represents a change to a specific situation that means the unwanted event could now be realised, although the unwanted event will only happen if the other barriers (assuming there are some) fail to function as expected. There can be multiple (many) causes for a single unwanted event.

Consequences

Each cause represents a (negative) thing that may happen as a result of the unwanted event occurring. It does not try to assign a level of consequence (e.g. fatality) but just describe the logical progression of the unwanted event to reach an end state (e.g. train collides with stationary train at platform).

Barriers

Barriers function to either prevent the unwanted event (on the left-hand side of the bowtie diagram) or recover from it (on the right-hand side). Barriers can be passive or active. Passive barriers perform their function by simply being there (e.g. a bund wall or fireproofing). Active barriers can only perform their function as a three-step process of detect-decide-act.

Decay mechanisms

Issues that can impact the effectiveness of barriers over time, and hence cause it to decay. These are not depicted in Figure 4 but are assigned to one or more barriers and should be unique to that barrier. In other words, generic decay mechanisms such as ‘lack of training’ should be avoided.

2.3 Benefits

There are many benefits of using a bowtie methodology for risk assessment and analysis. The most noteworthy in the authors' opinions are:

- **Precise definition** of the situation under consideration through a more sophisticated development of interconnected risk scenarios and the likelihood and consequences of them. The bowtie results in a richer understanding of risk compared with a number from a risk matrix.
- **Visual representation** of the factors affecting likelihood and consequence. This can bring the risk assessment 'to life' in an organisation as it can be quickly interpreted and understood but all people involved from engineers, to operators, to management.
- **Identification of the controls** (or barriers) that can act on the system of interest to prevent or react to the unwanted event. This is critical for identifying what barriers are applicable to what causes, and therefore what causes may require a greater focus of risk treatment.

3 Operationalising Bowtie risk assessments

3.1 Overview

The success or otherwise of any risk management system is the extent to which it takes hold within the operations of an organisation such that risk treatments are implemented and monitored in a way that truly reduces the risk. There are four critical factors that lead to the success of embedding a bowtie methodology within an organisation which are discussed in the following sections.

3.2 Prioritising risks to be assessed

It is important to specify an obvious point: not all risks can be controlled. Bowtie risk assessments should focus on high risk scenario sets that can have significant impacts on the organisation. A common mistake that the authors have witnessed is an organisation undertaking too many risk assessments, to a point where any individual assessment becomes irrelevant or lost. This focus will be different for different organisations, but setting a minimum threshold for a 'significant hazard' that requires a bowtie is important (e.g. any hazard that could result in loss of life or any hazard that could result in a financial loss >$100 million).

3.3 Linking risk assessments with operations and maintenance

As discussed, risks are only controlled if effective treatment is implemented within an organisation. These controls are only relevant if they are integrated within the operations and maintenance of the organisation, as it is these functions that will be interacting with the controls and ensuring their validity. To this end, it is of paramount importance that controls are linked to the assets in the maintenance management system and other relevant operations/maintenance databases. This link can provide the ability for an organisation to truly understand the validity of individual controls and (more importantly) the validity of a set of controls to ensure that the 'holes in the swiss cheese' (Reason, 2000) never align.

3.4 Embedding review of controls

Once embedded in operations and maintenance databases, there must be an effective review process for controls. This could involve inclusion of monitoring in operations systems (such as operator rounds or control panel visibility) and/or their inclusion in the maintenance systems to ensure that the control has not failed (e.g. condition monitoring, functional testing, hard time maintenance, etc.).

3.5 Governance

Like all tasks in an organisation, effective risk assessments, controls and monitoring form part of a priority list. The best (and arguably only) way to ensure that a risk management system remains effective is to obtain the buy-in of top-management and embed risk review as part of the governance of the organisation.

4 Conclusion

Although risk management is well document and well understood, underlying weaknesses remain hidden for many organisations through a lack of sophistication in their risk assessments and therefore inadequacy in their risk treatments. The bowtie methodology provides a visual representation of a risk assessment and is a better way of understanding risk to a system. This risk can then be effectively controlled through links with operations and maintenance and support from top-management. Practical operationalisation of bowties can lead to a greater control of risk for the organisation.

References

Asset Management Council, 2014. *Framework for Asset Management, Second Edition*. [Online] Available at: http://www.amcouncil.com.au/knowledge/publications/ambok-publications.html

Internal Standards Organisation, 2018. *Risk Management – Guidelines*

Ross P, 2008. *The night the sea caught fire: Remembering Piper Alpha*.

Reason, J. T., 2000. Human Error: Models and Management. *British Medical Journal*