Safety Science xxx (2017) xxx–xxx

Contents lists available at ScienceDirect

Safety Science

journal homepage: www.elsevier.com/locate/ssci

Risk registers: Structuring data collection to develop risk intelligence

M.C. Leva [a,*], N. Balfe [a], B. McAleer [b], M. Rocke [b]

[a] Centre for Innovative Human Systems, Trinity College Dublin, Ireland
[b] ESB Generation, Lower Fitzwilliam Street, Dublin 1, Ireland

ARTICLE INFO

Article history:
Received 18 November 2016
Received in revised form 21 April 2017
Accepted 16 May 2017
Available online xxxx

Keywords:
Risk register
Risk management
Risk assessment
Process safety

ABSTRACT

This paper presents the results of the development and implementation of a company-wide risk register, based on a clear set of data structures. A case study from an electricity generation company is presented and the process followed is described. The results of the case study indicated areas where the concept of risk registers could be extended to make better use of existing data and to support continuous improvement of risk management. Six key areas are discussed (1) aggregation of risks across the business, (2) supporting controls over mitigation measures, (3) improved estimation of event likelihood, (4) integrating with critical asset registers, (5) improving risk communication, and (6) linking with day-to-day operational practice. The paper concludes with a framework for placing risk registers at the heart of Process Safety.

1. Introduction

In order to maintain safe operations, organisations must continuously review and monitor their risks. This means that the results of safety studies and/or the evidence of issues collected from operational experience must be translated into a format that can be analysed, reviewed and acted upon, and new data about the level of risk continuously collected to keep the safety information up to date (Monferini et al., 2013). This helps to create an 'informed culture', defined by Reason (1997) as a culture in which both management and operators are informed of and knowledgeable about the factors that influence safety as a whole. When the available information is shared between all applicable levels of the organisation, a Common Operational Picture (COP) can be created as the basis for safe and reliable system operation (Kontogiannis et al., this issue). One method of creating this shared understanding, or COP, is through the development and implementation of a risk register.

A risk database, or risk register, is a central tool for organisations to use to monitor and reduce risks, both those identified during initial safety assessments and those emerging during operations (Whipple and Pitblado, 2010). The risk register should contain all analysed risks and should prioritise the areas that require managerial attention and typically contains information describing each risk, an assessment of the likelihood and consequences, a ranking according to a risk matrix, the risk owner, and information on the mitigations to be put in place (Filippin and Dreher, 2004). When populated with information on each risk, including risk ranking, the risk register can analysed to present the risk profile for different aspects of the organisation (Filippin and Dreher, 2004). When reviewed and updated over time, it can also be analysed to present trends within the risk profile and focus management attention on the highest risk activities or facilities (Whipple and Pitblado, 2010).

Risk registers are used in a variety of industries, e.g. medicine (Brown, 2004) and construction (Dunović et al., 2013), as well as high hazard industries such as oil and gas (Hasle et al., 2009) and electricity generation (Leonard, 1995). They are typically used either to support safe operations or to support safe and efficient project management (e.g. De Zoysa and Russell, 2003). Cooke-Davies (2002) found that the adequacy with which a visible risk register was maintained was one of the key success factors for project management. Patterson and Neailey (2002) highlight the importance of the risk register and suggest that the benefit of a risk register is as a method to enable all stakeholders to "consciously evaluate and manage the risks as part of a decision making process" (pp. 365). They also note the importance of the risk register in documenting the process of reducing risk and introducing mitigations. However, Kutsch and Hall (2010) warn of the danger of risk registers becoming 'tick-box' exercises when the owners and contributors do not have a real ability to influence the risks – the danger of irrelevance. Despite the clear importance of risk registers in the risk management process, there is very little guidance on their development and implementation (Dunović et al., 2013). Research conducted by the Design Information Group at Bristol

* Corresponding author.
E-mail address: chiaraleva@gmail.com (M.C. Leva).

http://dx.doi.org/10.1016/j.ssci.2017.05.009
0925-7535/

University found that 67% of their questionnaire respondents working in Engineering Design project, documented their risks on either a paper or computer-based risk register (Crossland et al., 1998). However these were generally individual solutions, usually specific to the organisation and sometimes even specific to a location and hosted locally suggesting the format of a individual risk register than a company wide shared solution (Patterson and Neailey, 2002).

This paper attempts to address the gap in guidance on construction of risk registers by describing the results of a case study in which a risk register was established in an electricity generation company across multiple locations and the preliminary results were used for Management Review decisions. The single central risk register is aimed at collating risks from across the business, including various power stations across different geographical locations. The objectives of the project were:

- To develop a risk register data structure supporting consistent hazard identification and risk rating across different sites;
- To develop equivalent severity and frequency scales for different loss types and for application across different business units, such as operations, maintenance, finance, HR, etc.;
- To use the risk register to highlight key business risks to senior management;
- To use the risk register to gather information about mitigation measures in place and their effectiveness;
- To embed the risk register within a risk management process and share good practices across the company.

1.1. Description of the case study

The analysis presented in this paper is based on the development and implementation of a company wide risk register in an electricity-generating organisation in the Republic of Ireland. As part of an on-going process of Process Safety improvement, the organisation identified a need to advance the identification, analysis and management of risks across the business, and to hold these risks in a format that facilitated comparison and tracking. A project team was therefore assembled, with representatives from different stations and specialisms, to create a risk register capable of meeting the business' needs. The researchers were embedded in this team, and helped to facilitate the process. This paper discusses the process followed in the development and implementation of the risk register solution, evaluates the strengths and weaknesses of the solution, and finally applies the lessons learned to propose a framework for safety and risk management with a risk register as the central point.

2. Developing a risk register

2.1. Key components

Risk registers may take a variety of formats, but some there are some key components that are necessary to enable the management of risk in this format. First is the description of the risk, and a unique identification number to facilitate tracking. A concise description is necessary to allow users and reviewers to understand what is being documented. A more comprehensive description may also be provided, particularly for complex risks or those that have a long history. Each risk must have an indication of its priority, in the form of a risk ranking. Risk rankings are typically calculated from the product of the severity and likelihood of the risk. The calculation may be more or less sophisticated, depending on the data available. Finally, the actions required to improve or manage a risk should be documented, along with the overall risk owner who is responsible for ensuring progress of the risk against the planned timescales (dates). The risk owner may not be responsible for the individual actions required, as these may be spread across a diverse workforce, but they are responsible for ensuring overall progress. Complex or detailed actions may be held in a separate document, but a summary should always be available in the risk register. Table 1 summarises the core components of a risk register.

Additional components may be incorporated into a risk register, including documentation of existing controls in order to assist with monitoring their continued application and effectiveness, the risk status (e.g. open, closed, increasing, decreasing, etc.) to assist with tracking the overall risk profile, the type of risk and associated losses (e.g. safety, financial, reputational, legal, etc.), and the target risk level.

To facilitate risk evaluation, a risk register should be supported with a risk matrix and associated severity and likelihood scales. Different processes and parts of the organisation may already be using matrices and scales, and in order to apply a company-wide risk register, these may need to be aligned for consistency.

2.2. Problem definition

Risk management during operations relies on the on-going identification, evaluation, and monitoring of risks with the potential to affect safety or performance. The partner organisation in this case study, had an existing process which relied on the plant managers from each station across the business reporting their 'Top 10' risks to a central risk manager who collated and analysed the full set for presentation to senior management. A number of issues were identified with this process, particularly:

- It was labour intensive;
- Not transparent to the stations reporting risks;
- Did not facilitate learning across the organisation;
- Not consistent in the reporting and rating of risks;
- Not comprehensive in the types of risks covered;
- Only updated quarterly;
- No ability to data-mine or trend the data.

In order to better manage process safety, the company required a single risk register to be developed that supported the identification and management of operational risks encompassing all business units into a single dynamic source. The risk register should also include a process for communication and review of the top business risks and control measures by senior management at a defined frequency. Finally, feedback and value to the end users (stations) inputting their risks should also be taken into account. Possible value for end users includes:

- possibility to share best practices or solutions with other stations/users having similar problems

Table 1
Risk register core components.

Element	Description
Risk ID	A unique identification number for each risk
Risk Description	A concise description or title for the risk
Risk ranking	A quantification of the risk, based on severity and likelihood
Owner	The person responsible for managing the risk and ensuring actions against it are completed
Actions	A list of actions for each risk
Dates	The date of entry and modification should be held for each risk to assist with reviews. Action target and completion dates should also be included

Please cite this article in press as: Leva, M.C., et al. Risk registers: Structuring data collection to develop risk intelligence. Safety Sci. (2017), http://dx.doi.org/10.1016/j.ssci.2017.05.009