Using Preliminary Risk Assessment in a Formative Evaluation

James Vesper
Murdoch University, Australia
jvesper@learningplus.com

Thomas Reeves
The University of Georgia (Emeritus)
treeves@uga.edu

Jan Herrington
Murdoch University, Australia
j.herrington@murdoch.edu.au

Abstract
Risk assessment is used to identify potential hazards and prioritize those that may be most likely to have a significant impact. While widely used in the aviation, power, pharmaceutical, and chemical industries, formalized risk assessments are not often used for instructional interventions, particularly e-learning. As part of a formative evaluation for an e-learning course being developed, facilitators and design team members performed a risk assessment on topics related to the technology used in the course, the communication of mentors and participants, sustainability, and evaluation. With this information, the design team and mentors prepared a risk management plan, identifying ways to prevent unwanted events as well as to plan for contingencies in the case of their occurrence. The framework of the plan is described, together with details of its implementation in a formative evaluation of the course.

Introduction
Risk assessment and risk management are used in almost every industry and profession to make data-supported, proactive decisions on how to best use resources to prevent the occurrence of unwanted events, and should they occur, to protect the assets of value in the environment. Despite the usefulness of risk assessment in enabling potentially problematic events to be articulated and then possibly accommodated, such assessments are only rarely performed in planning e-learning environments. Nevertheless, such risks do exist. While technology-based learning environments have inherent (and easily predicted) risks related to data security, data loss and technology failure, more subtle risks related to learning activities and assessment can equally create critical obstacles for students engaged in e-learning. These risks are compounded when used by e-learners in different countries and different cultures.

In this paper, we describe a risk assessment plan developed during the design and creation of an e-learning environment, the *e-Pharmaceutical Cold Chain Management*. The course used principles of authentic learning (Herrington, Reeves & Oliver, 2010) to cognitively mirror the e-learning equivalent of a tried and tested six-day, real-world course on handling time-temperature sensitive pharmaceutical products. The 'real-life' experiential course took 15 select participants on a bus tour that began in Istanbul, Turkey, and follows the path or "cold chain" used for the products from manufacturers, distributors, medical centers, community health centers, and retail pharmacies (Vesper, Kartoğlu, Bishara, & Reeves, 2010). While successful in achieving the intended outcomes, it was expensive and limited in reach with only small numbers of participants able to complete the course each year. In 2009, a project was commenced to create an online course encompassing a virtual bus tour. The design principles for the course, together with early evaluative data has been published (Vesper & Herrington, 2012; Vesper, Reeves, & Herrington, 2011). In this paper, we describe the process of risk assessment within formative evaluation of the online environment.

Risk assessment and risk management
Risk assessment is defined as the "overall process of risk identification, risk analysis, and risk evaluation" (ISO, 2009). In performing a risk assessment, one seeks answers to five basic questions (Kaplan & Garrick, 1981):

1) What can go wrong?
2) How bad can it get?
3) How could it happen?
4) How likely is it to happen?
5) Should we try to do something about this?

With answers to these questions, one can then move into risk management where three other questions are asked (Haimes, 1991):

1) What can be done to control, mitigate or prepare for this unwanted event?
2) What are the best options given the circumstances?
3) What other risks or issues might the selected option(s) create?

These questions are asked in a series of phases using a variety of well-defined methods and tools to document the process and results. Figure 1 shows a model of a typical risk assessment and risk management process.

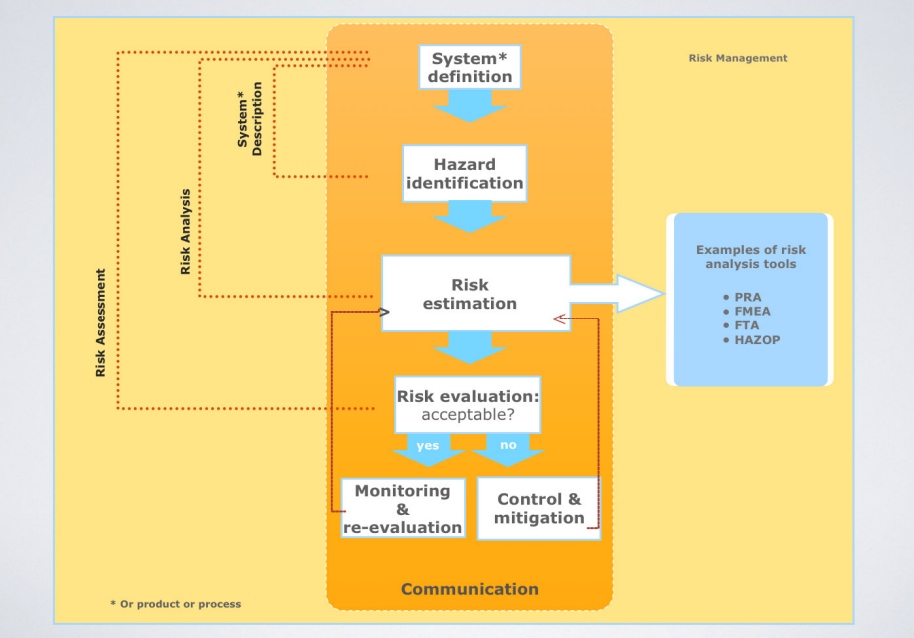

Figure 1. The typical process for risk assessment and risk management (Vesper, 2006).

Risk assessment can be performed using a variety of tools (such as those illustrated in the right column of Figure 1). Some tools are very basic and may be informal, for example, simply asking "what if…" questions. Other tools, like *fault tree analysis* (FTA) and *failure mode effects analysis* (FMEA) are highly structured and well-defined (Stamatis, 2003; Vesely, Goldberg, Roberts, & Haasl, 1981). Certain tools are optimized to help identify hazards – hazard analysis or hierarchical holographic modeling – while others like *hazard analysis* and *critical control points* go through the entire risk assessment and risk management process (Vesper, 2006).

There is limited literature on risk assessment in relation to evaluation. Lynch and Roecker (2007) recommended that risk assessment be used as part of an evaluation, presenting a simple form to collect data to be used in the assessment. Similarly, Benson and Brack (2010), in their planning guide for online learning and assessment, noted that an important administrative function in planning online assessment was the completion of a risk assessment of: 1) student support factors (such as access and equity issues), 2) technical issues (such as access to hardware and software, bandwidth, etc.), 3) authentication (such as cheating, collusion, plagiarism, etc.), and 4) consideration of the instructor's administrative skills (such as ability to use software, manage online grading, copyright, etc.). However, no model or framework of risk assessment appeared to exist that provided guidelines for the assessment of a complex online authentic learning environment involving a community of learners. In the next section, we describe the design and development of such a framework.

Project background
For the past several years, a project has been underway at the World Health Organization (WHO) to create a unique e-learning program aimed at developing the expertise of those handling time-temperature sensitive pharmaceutical products like vaccines. The e-learning course is modeled after a course that is offered annually in Turkey by WHO (WHO, 2008). This e-learning solution, known as *e-Pharmaceutical Cold Chain Management*, is being developed focusing on the development of expertise within an authentic learning environment (Herrington, Reeves & Oliver, 2010). In addition to evaluation at all stages of development (Reeves & Hedberg, 2003), the project is being researched using a design-based research approach (Reeves, 2006) by the primary author of this paper.

Formative evaluations have been conducted to help ensure that various elements of the proposed learning solution contribute to its success. The first formative evaluation was performed by graphic and instructional designers (Vesper, et al., 2011) as they reviewed early sketches of screens and activities. The second formal evaluation was conducted in February 2013 by design team members and the intended course mentors (facilitators) using a working version of the program. This evaluation had the goals of:

- Optimizing the e-learning solution before the course is released for pilot;
- Conducting a sequential walkthrough of entire working version of the e-learning course;
- Identifying potential issues with learning materials (e.g., activities, instructions, resources);
- Achieving consensus on expectations for learning activities (e.g., acceptable/non-acceptable results);
- Beginning to develop a reference guide for current and future facilitators; and
- Identifying significant risks and ways to control and mitigate them.

The risk assessment activity conducted was specifically aimed to meet the last evaluation goal, but it was also important that it addressed the requirements the other listed goals. The process of assessing risks in such a context is examined in the developing framework, described in more detail below.

Risk assessment of complex authentic environments

Getting started
Before starting a risk assessment, what is being assessed needs to be clearly defined. This can be done by a written description, flowchart, or diagram (ICH, 2005). Risk assessments are best performed by a team of people with different areas of knowledge and experience. Team members need to be identified before starting the assessment, and led by a knowledgeable and skilled facilitator. One other important but often overlooked element is clearly defining the "risk question" – the question that the risk assessment is meant to answer (Vesper, 2006). This is consistent with one of Reeves and Hedberg's (2003) key reasons for doing a formative evaluation – answering questions that can be used to make decisions about development. Examples of risk questions include:

1. What are the IT/technology risks associated with this e-learning project?
2. What are the risks related to the community of learners due to inappropriate communication?
3. What are all the risks that could arise when using this e-learning program?

As can be seen in these examples, risk questions can define the scope of the risk assessment from very narrow (Risk question 2) to very wide (Risk question 3). Often, the risk question drives the selection of the method the risk assessment team selects. A preliminary risk assessment that asks, "What if..." could be used with Risk questions 1 and 2; hierarchical holographic modeling (HHM) and risk ranking and filtering are appropriate for identifying and assessing risks in a large, complex system (Haimes, Kaplan, & Lambert, 2002) such as those that would be examined in answering Risk question 3.

Identifying hazards
Two important definitions to distinguish between are *hazard* – the source of harm – and *risk* – the combination of the **likelihood** of the expression of the hazard and the occurrence of the unwanted event and the **impact** should that hazard be expressed (ICH, 2005). In beginning a risk assessment, one first needs to identify the hazards. There are different ways to identify hazards. A frequently-used method is to simply brainstorm what

could go wrong. Other tools, like *hierarchical holographic modeling* (Haimes, et al., 2002) can be used to first create "success scenarios" from which risk scenarios and specific risks can be identified.

In this formative evaluation, the evaluation team first brainstormed ideas that could have an impact on a successful e-learning Pharmaceutical Cold Chain Management Course (e-PCCMC). From this list, topics were identified that would all be needed to achieve the goal (i.e., a successful e-PCCMC). The team then identified actions, events, or situations – the hazards – that could prevent or interfere with the success. The list was then condensed based on those hazards that were considered most relevant, and then discussed further using a preliminary risk assessment tool.

Determining the risks
A preliminary risk assessment (PRA) can be used early on in a project when minimal information is available, or as a screening tool to identify risks that need to be examined more critically using other tools, such as *fault tree analysis* or *failure mode effects analysis* (Vesper, 2006).

For the purposes of this evaluation, it was felt that the PRA would provide an appropriate level of detail. For each of the hazards, specific questions were asked to help determine the risk. These included:

1. *What are the potential negative impacts to the learners and the desired course outcomes?* Answers to this question provides examples of the consequences, or harm should the hazard be expressed.
2. *What could cause this unwanted event to occur?* Here, one wants to identify how the hazard could be expressed.

With this information summarized on a matrix (see Figure 2), the team estimated the likelihood that the hazard would be expressed resulting in the harm, using a scale of low-medium-high (1-2-3) (Column 5). In a similar way, the impact was estimated, again using a scale of low-medium-high (1-2-3) (Column 6). Multiplying these two numbers results in a risk score – the higher the number the more risk being present (Column 7).

The last step of risk assessment is risk evaluation: deciding on the risks that need to be reduced (Column 8). Generally, these are the high or medium risks that are "treated" through control and mitigation.

Reducing the risks through "treatment"
Risk treatment (ISO, 2009) involves two key concepts: control and mitigation. Control is aimed at *preventing* the unwanted event from occurring in the first place; the focus is on reducing the likelihood by targeting the root and contributing causes. Mitigation assumes the unwanted event will occur but aims at *protecting* the "thing of value" (CSA, 2002). For example, one cannot totally prevent a server crash at a hosting site, but one can take protective measures should that happen. Whenever possible, multiple risk treatment approaches should be taken that have a "layering" of the control and mitigation actions. These are tied to the different causes or mechanisms that were identified. These layers result in a more robust solution should the hazard be expressed.

For each of the risks that were identified, the team identified a risk treatment plan. In some cases, it was providing information, for example, recommending browsers that were tested (and what browsers are not recommended). One identified risk – government does not allow access to a video website – actually occurred at the start of the pilot course. A participant could not access the VIMEO or back-up sites, so the treatment plan – sending a pre-made DVD to him via DHL courier service was executed.

Preliminary Risk Analysis Worksheet

Item analyzed: e-PCCMOW Course (Feb 18 version)

Risk analysis project: Formative evaluation

Risk Question: What are the risks of a TECHNOLOGY RELATED issue with the e-PCCMOW course?

	Step #1	*Step #2*	*Step #3*	*Step #4a*	*Step #4b*	*Step #4c*	*Step #5*
Risk ID #	**Unwanted Event/ Hazard**	**Consequences / Harm**	**Contributing Causes**	**Likelihood of Occurrence**	**Severity of Consequence**	**Risk Score**	**Possible Additional Controls/Actions**
	What could happen?	*What is the potential negative impacts to patient, product, regulatory status, other things of value?*	*What could cause this unwanted event to happen?*	*What is the likelihood that the event & the harm will occur? (rating scale)*	*What is the impact of this consequence? (rating scale)*	*(calculated)*	*What might be done to reduce the likelihood and/or severity?*
1	Incompatibility of browser with website	> Limited access to sections of course > No access to parts of pages	> Set-up of browser > Internal browser thing > Coding issue	1	3	**3**	1) Recommendations of browsers NOT to use 2) Determine cause of problem if possible 3) Tell what browers are supported
2	Bandwidth issue (user side)	> User can't get timely access to videos, docs	> Local provider bandwidth issue	2	3	**6**	1) Send out DVD of videos and docs
3	Government (of participant) blocks server sites (e.g., VIMEO)	> User can't get any access to videos, documents, or course	> Local political issues	2	3	**6**	1) Send out DVD (via express shipment e.g., DHL) 2) Have mirrored alternative sites for videos, etc 3) Make videos available as downloads (e.g. DROPBOX or Yousendit) 4) Inform participants of the possibilty; have them communicate to mentors if there is a problem
4	DVDs/downloads get distributed to others	> Information (e.g., imbedded poor practices) gets distributed and used out-of-correct-context	> Information not controlled (e.g., via streaming)	1	3	**3**	1) Have mirrrored sites available for videos whenever possible 2) Put notice on DVD 3) Have participant agree not to transfer to others
5	Server problems or outages – at host sites (host server, VIMEO	> Non-availability of site and resources when needed by participant	> Crashes – unplanned outages > Planned outages (e.g., for maintenance)	1	2	**2**	1) Find out about site's contingency plans 2) Communicate planned outages with participants in advance 3) Mirror materials on other hosting sites

Figure 2. A section of a risk assessment performed using a Preliminary Risk Assessment (PRA) worksheet.

Monitoring and review

After the listed risks are addressed through control and mitigation, there is still the need to periodically review the assessment that was done to see if control and mitigation actions were effective and if the likelihood and impact were correctly estimated. Additionally, monitoring is an ongoing effort to determine if there is anything that changes that could affect the assessment. Another aspect of monitoring is to identify any other risks that were not previously identified.

A formal review of the risk assessment and risk management plan will be performed when the pilot course is completed. In terms of monitoring, the design team realized two weeks into the course that there was going to be a seasonal time change (from "standard time" to "daylight savings time") occurring at two different points during the course. To mitigate the impact, a notice was sent to all participants alerting them to the change. This event will be included in the next listing of risks.

Discussion

Risk assessments are based on the best information available at the time, acknowledging that there is uncertainty. The goal, however, is to reduce that uncertainty by collecting data directly or by making valid inferences. As uncertainty goes down, so does risk (Hubbard, 2009). Another important caveat in interpreting the risk assessment is that the risk score generated during the risk assessment isn't an absolute number; rather, it is a score that allows the prioritization of the risks. Having a risk score of 6 does not mean that the specified risk is twice as more likely to occur or twice as bad as a risk having a score of 3, for example. Rather, it means that given the data that was considered, the risk with the score of 6 should have a higher priority for control and mitigation. As also argued by Slovic (1999) and others, 'the probabilities and consequences of adverse events [cannot] be objectively quantified by risk assessment … instead that risk is inherently subjective' (p. 690). Nevertheless, the process itself is a key value of risk assessment, namely having knowledgeable people talk about risks in a thoughtful, thorough way.

After a risk is "treated" there will be residual risk that remains (ISO, 2009). Ideally, this residual risk will be significantly less than the initial risk estimate. At other times, the residual risk might be considerable due to new problems that intended solution creates. For example, in this risk assessment, one IT/technology hazard identified was "blockage of a website by a government", an event that occurs in some countries through

censorship of offensive material available on the site (BBC, 2013). For this e-learning course, blocks on certain websites would prevent course participants in that country from accessing course materials, videos, and activities. In discussing this, the mentors and design team initially considered downloading videos direct to the user through an ftp site or file transfer service like YOUSENDIT. This, however, could result in a lack of control of the videos; while nothing was proprietary or secret, sections of the video, if taken out of their intended use-context (i.e., purposely showing an incorrect practice) could be misinterpreted. The solution that the team proposed was to have videos available for streaming on several alternative sites, making it unlikely that all such sites could be blocked by any countryAlso, DVD copies were prepared and available to send to the participant..

Another benefit that was seen in the risk assessment conducted for the e-PCCM course was using the experiences and different perspectives of all the team members: those with a background in e-learning shared situations they had learned from; those with international/multi-cultural experience thought of risks that the other team members had never thought of. Together, the team was able to synergistically build on their collective knowledge and arrive at place that a single person would not have been able to do on their own.

Conclusion

Formative evaluation is an essential part of designing, developing, and implementing a learning solution, providing 'the greatest payoff of any function of evaluation' (Reeves & Hedberg, 2003, p. 60), whether it be a traditional leader-led course or an innovative e-learning solution. Identifying potential risks in advance and coming up with ways to prevent them from occurring, or discussing ways to work through problems should they occur, results in an implementation that can have fewer problems and a higher probability of success.

References

BBC. (2013). Egypt ministry appeals against order to block YouTube. Retrieved 22 Feb 2012, 2013, from http://www.bbc.co.uk/news/technology-21497463

Benson, R., & Brack, C. (2010). Online learning and assessment in higher education. Oxford, UK: Chandos Publishing.

CSA. (2002) Risk management: Guideline for decision-makers – CAN/CSA-Q850-97. Ontario: Canadian Standards Assoc.

Haimes, Y. Y. (1991). Total risk management. Risk Analysis, 11(2), 169-351.

Haimes, Y. Y., Kaplan, S. L., & Lambert, J. H. (2002). Risk filtering, ranking, and management framework using hierarchical holographic modeling. Risk Analysis, 22(2), 383-397.

Herrington, J., Reeves, T.C., & Oliver, R. (2010). A guide to authentic e-learning. London and New York: Routledge.

Hubbard, D. W. (2009). The failure of risk management: Why it's broken and how to fix it. Hoboken, NJ: John Wiley & Sons, Inc.

ICH. (2005). Quality risk management – Q9 (Vol. Q9, pp. 23): International Conference on Harmonization.

ISO. (2009). ISO 31000:2009 Risk management — principles and guidelines. Geneva: International Standards Organization.

Kaplan, S. L., & Garrick, B. J. (1981). On the quantitative defintion of risk. Risk Analysis, 1(1), 11-27.

Lynch, M. M., & Roecker, J. (2007). Project managing e-learning: A handbook for successful design, delivery, and management. New York: Routledge.

Reeves, T. C. (2006). Design resesarch from a technology perspective. In J. van den Akker, K. Gravemeijer, S. McKenney & N. Nienke (Eds.), Educational Design Research. London: Routledge.

Reeves, T. C., & Hedberg, J. C. (2003). Interactive Learning Sytems Evaluation. Englewood Cliffs, NJ: Educational Technology Publications.

Slovic, P. (1999). Trust, emotion, sex, politics, and science: Surveying the risk-assessment battlefield. Risk Analysis, 19(4), 689-701.

Stamatis, D. H. (2003). Failure mode and effect analysis: FMEA from theory to execution (Second ed.). Milwauke, WI: ASQ Quality Press.

Vesely, W. E., Goldberg, F. F., Roberts, N. H., & Haasl, D. F. (1981). Fault tree handbook. Washington, D.C.: U.S. Nuclear Regulatory Commission.

Vesper, J. L. (2006). Risk assessment and risk management in the pharmaceutical industry – clear and simple. Bethesda, MD: PDA/DHI.

Vesper, J. L., & Herrington, J. (2012). Considering communities of learners when creating an e-learning course. Paper presented at the EdMedia 2012, Denver, CO.

Vesper, J. L., Kartoğlu, Ü., Bishara, R., & Reeves, T. C. (2010). A case study in experiential learning: pharmaceutical cold chain management on wheels. Journal of Continuing Education in the Heath Professions, 30(4), 1-8.

Vesper, J. L., Reeves, T. C., & Herrington, J. (2011). The application of expert review as a formative evaluation strategy within an educational design research study. Paper presented at the E-Learn 2011, Honolulu, HI.

WHO. (2008). Nothing stands still: Pharmaceutical cold chain management on wheels. Geneva: World Health Organization.