

At the risk of remaining unheard

Identify, map and evaluate the organisation's business processes, the consequences of unmanaged risks, and do it in the language of the executives you want on board.

BY KEVIN DWYER AND MICHELLE LINTON

The Executive General Manager tightened his belt as he prepared to give his keynote speech to the project team that was to be responsible for the rollout of an EDRMS to thousands of staff. His attitude was stern.

"This project is very important to us. We *must* comply with the State Records Act by next year." His countenance brightened as he indicated to the woman beside him. "Which is why we have elected to give oversight of the project to Sally. Sally is one of our best managers, and I know she will do a good job. That is why I hereby transfer the poisoned chalice to you, Sally, in full confidence you won't let us down."

Sadly, over three years, that was about the best contribution the Executive General Manager made to the conversation about the information management needs of the organisation.

Was it his fault that he did not understand that information management is not about compliance but about boosting productivity and reducing risk through on-demand collaboration across the organisation? Our thoughts are no, he should not be expected to be knowledgeable about modern information practices, no matter how much we wish that he was. It is our role as records and information management professionals to reframe what we know about records and information management and Electronic Document and Records Management Systems (EDRMS) into the language of senior executives. Too often, however, we know too little about business processes, which means we also, therefore, know little about how the functionality of the EDRMS and good information management practices can actually increase productivity and, in particular, reduce risk.

When it comes to articulating the reduction in risk, we are doubly challenged. Not only do we have difficulty in getting a good understanding of the business processes, but also

most people – including some senior executives, not just records and information management professionals – have a poor understanding of the concept of risk.

When presenting a business case for a budget to implement an EDRMS, or materially change the organisation's information management practices, it is insufficient to just proclaim that we can reduce risk. We must be able to show, with specific examples, how risk will be reduced from a level which is unacceptable to a level the organisation is comfortable with.

It is somewhat helpful to refer to 'scary stories' of risk events being realised when poor information management practices occur. At Change Factory and Linked Training, we use them quite a lot in our training of superusers and records management teams with good effect. However, to influence an executive team, our arguments must be more concrete and rooted in known business processes.



Story snapshot

- To achieve the uptake of EDRMS, records and information managers must use the language of the senior executive to communicate their message.
- Use specific examples and case studies to demonstrate how risk will be reduced.
- Identify risks which compromise the integrity, availability and confidentiality of information.



To be able to reframe our knowledge of information management practices and the functionality of the EDRMS into risk reduction benefits to an organisation, we must learn risk concepts and how to apply them.

If you have a good understanding of risk terms, you can skip forward. If you do not have a good understanding, then read on.

RISK TERMS

- **Risk sources:** In the physical world this is easy, the sources of risk usually being a type of energy – kinetic, electrical, potential, etc. In the information world, it's not so clear cut, but sources of risk can be reasonably classified in terms of integrity, availability and confidentiality. When identifying risk in information management, we should look at processes which have the potential to create an event that will compromise the integrity, availability or confidentiality of information.
- **Risk event:** Slips, trips, falls, mechanical failures and so on in the physical world. In the information world, this includes (but is not limited to) human behaviour such as misplacing or misfiling or transcribing incorrectly, poorly executed operational processes such as scanning or copying or mailing, natural events such as floods or cyclones, and legal events such as freedom of information or court action.
- **Risk context:** The same as in the physical world, it is the criteria by which we measure the consequence of a risk event happening. In most organisations the risk context includes an assessment of the potential impact on:
 - Reputation
 - Environment
 - Assets (financial and physical)
 - People (customers and employees)
- **Risk analysis:** Determining the likelihood of a risk event occurring and the consequence if it does occur. The likelihood is rated on a scale, from Unlikely (event occurs every ten years or more) to High (event occurs one or more times a year). The consequence is rated on a scale from Insignificant to Major in the contexts already established. We need to think about what the consequences would be if specific information is compromised with regard to integrity, availability or confidentiality.

- **Risk evaluation:** Evaluating whether the risk likelihood and consequence is acceptable to the organisation. This is where most non-risk professionals make a mistake in that they intuitively evaluate the likelihood of risk but not the consequence if the risk event, albeit unlikely, does occur. This can result in a gross underestimation of the actual level of risk the organisation faces.
- **Risk treatment:** The actions taken to reduce the likelihood and/or the consequence of the risk event occurring to a level acceptable to the organisation.
- **Residual risk:** The risk remaining after risk treatment.

RISK ANALYSIS THAT EXECUTIVES WILL LISTEN TO

So now we have completed Risk Management 101, how do we use this knowledge to our advantage in influencing senior executives to spend some money on information management? Or, even better, to get them to enthusiastically sponsor the project we are seeking budget for?



Step 1:

Look for processes where a compromise in the integrity, availability or confidentiality of information would have an unacceptable consequence for the organisation. It may help to think of processes in a segmented way such as:

- **Strategic information processes** such as organisational development, planning, audit, strategy development.
- **Operational processes** such as service provision, policy advice.
- **Support information processes** such as payroll, recruitment, performance management, accounts payable, accounts receivable, procurement.



Step 2:

Map the process and analyse the likelihood and consequence of information risk events occurring at each step in the current process.

BRIGHT IDEA 3

Get people excited about recordkeeping

FREE online training demo

Visit Online Training at www.LinkedinTraining.com.au

HOW? Professional Training Delivery.

Challenges of distance, multiple locations, and tight budgets are solved.

We provide eLearning, Help Sheets, Training manuals, Workflow Analysis, Training Delivery, L & D Plans.

To make your training a success, call 02 8824 4677 or email info@linkedtraining.com.au



Linked Training
the experts

About the authors



MICHELLE LINTON,
Managing Director, Linked Training
Michelle is a Learning & Development professional with 24 years' experience in the planning, design and delivery of training programs. Michelle has developed and delivered innovative,

outcome focused EDRMS training for over 30 government and private organisations since 2005. Michelle's pragmatic approach to learning strategies leading to application adoption has been enthusiastically welcomed by the industry, and she is a regular speaker at RIM events and contributor to industry magazines. Linked Training is the training partner in the REX project which was awarded the J.Eddis Linton Award for Excellence – Most outstanding group in 2010.

- She can be contacted at Michelle@LinkedTraining.com.au



KEVIN DWYER,
Director, Change Factory
Kevin is a Change Management professional with more than 30 years' experience in the planning, design and delivery of change management programs. Since 2001, and the establishment of Change Factory, he has been involved in many Change Management projects ranging from re-engineering of customs processes to reduce risk to creating and revising performance management systems to improve customer service outcomes at five-star resorts. His first EDRMS project was as the Change Management partner for the REX project which was awarded the J.Eddis Linton Award for Excellence – Most outstanding group in 2010.

- He can be contacted at Kevin.Dwyer@changeactory.com.au

**Step 3:**

Evaluate where a particular function of the EDRMS and/or better information management practices can form an effective part of a risk treatment plan to reduce the risk likelihood and/or consequence to a level acceptable to the business.

From this analysis, we can begin to tell a cogent story about the risks which would be ameliorated if we had better recordkeeping processes and used the functionality of an EDRMS better.

An example might be the launch of a new product requiring extensive briefing of a government department, vendors, an advertising agency and an engineering firm. The processes involved here are complex, involving many levels of authorisation and sharing of information. In a poorly functioning information management world, confidential documents will be sent as email attachments; security on who can see what within the organisation's shared drives will be lax; knowledge of which version of specifications is the latest and operational tactics will be poor; and no audit trail will exist – to mention but a few of the shortcomings.

Completing an in-depth analysis of the processes involved at each step will reveal multiple opportunities and a high likelihood

for the new product launch to be leaked to competitors and the media, for specifications to be in error or for operational tactics across departments involved in the launch to be misunderstood; and these are only a few risk events. The consequences will depend on the need for secrecy, accuracy and speed, but in most cases of this type any event will at least damage the timing and most likely the effectiveness of the launch.

A fully functioning EDRMS with good information management practices will reduce the likelihood in many process steps to zero for most risk events. Take that analysis as a case study to the executive management team and you will have their interest and are likely to get some debate about alternative controls and/or a request for more information if you do not get the go ahead then and there. If, instead, you only take a mantra that good information management practices and sensible use of EDRMS functionality reduces risk *without* a case study, they may show interest at the intellectual level, but are much less likely to be engaged in the nuts and bolts of the real benefits.

Good information management practices, coupled with proper use of EDRMS functionality, reduce risk (and increase productivity) by allowing collaboration at the point of need. We have to learn the language of business and its executives and gain the understanding of the key strategic, operational and support information processes or we risk remaining unheard in our quest for improved information management. **IQ**

Show your Senior Managers how to beat risk



You know a well-configured EDRMS can reduce risk in your organisation, providing clear audit trails and a single, unambiguous version of 'the truth'. But do your senior managers?

Show them by mapping the functionality of your EDRMS to your business processes to reduce risk. To find out how, contact us today.

✉ contactus@changeactory.com.au

🌐 www.changeactory.com.au/edrms

☎ (03) 9329 6250

