

Introducing Risk Management Or

Everything I know about risk management I learned from watching Clint Eastwood movies



"I know what you're thinking, 'Did he fire six shots or only five?' Well to tell you the truth, in all this excitement I've kind of lost track myself. But being this is a .44 Magnum – the most powerful handgun in the world – and would blow your head clean off, you've got to ask yourself one question: 'Do I feel lucky?' Well, do ya punk?"

A fistful of words have been written on risk management. The first words written included much on how essential good risk management is for an organisation to thrive. Later, the emphasis changed to explaining how a big investment in risk management could turn it into a near scientific discipline that would help organisations make the 'right' decision every time. And more recently many more words have been written on how the most lavish investments in risk management (by the financial industry) have completely failed to protect these organisations from disastrous losses.

We thought it was time for a few words more. Why? Risk management can be a simple topic. There are lots of real life reasons why it is a very desirable thing to do and it is possible to get a lot of benefits without having to bet the ranch on paying

for it. But in all the words and front page news stories we may have lost track of the fundamentals. So this white paper is dedicated to setting things straight, with added insight from Clint.

What's it for?

"Walk a straight line through a cow pasture you gotta step in some cow pies."

Anyone and any organisation that sets out to accomplish anything is going to have things go wrong. Risk management at its heart is about avoiding making the mistakes which will stop you getting where you want to go. And there are a lot of potential mistakes to make; things can go wrong in every phase of activity. In fact things will go wrong, without any doubt, so the smart organisation does enough risk management to make sure these problems don't prove fatal. Half of this story is using risk management to try and make sure things work in your organisation the way you want them to. The other half is using risk management to help decision making, choosing between alternatives and going for the option that seems to offer the best upside for the least downside. *"If you want a guarantee, buy a toaster."*

What you need to do right – the Do's

Know your core risks

"You forgot your fortune cookie. It says... you're s(ure) out of luck."

You don't need a fortune cookie to figure out the major things that can badly derail your organisation. It has been said there are only seven basic plots in the movies – Clint against nature, Clint against man, Clint against the culture, Clint against technology, Clint against the supernatural, Clint against himself and Clint against God. Likewise there are only ten basic risks every organisation faces – damage from your staff, damage

from your systems, damage from your customers, damage from your suppliers, damage from your business model, damage from your financiers, damage from the government, damage from nature, damage from your competitors and damage from criminals.

There is devil in the detail. How that damage can occur and how big the damage could be, will vary depending on what the organisation does and how it does it. For instance everyone faces the risk of customers who cause damage by failing to pay what they owe; that risk is bigger for an organisation with a few large customers than it is for one with many small customers. Or the risk of damage from systems failure which is a bigger risk for an internet retailer than it is for a taxi firm - as the damage that would follow would be more costly. What you have in every case, though, are the core risks - the big ticket areas that could do a lot of damage. Understand what these are and you can figure out how to tackle each one.

A word of caution: "A man's got to know his limitations" and the biggest blind spot organisation's have in understanding their core risks is the feeling that it could never happen to them. You might be confident that you won't be damaged by the ten basic risks, but if your justification for this opinion relies on a lot of 'soft' adjectives (we have 'good' staff, 'trustworthy' suppliers, 'loyal' customers, 'reliable' systems etc.) then you aren't doing risk management. Risk management assumes things can and will go wrong no matter what soft adjectives you think might apply. In risk management "It's not real easy to like something you know nothing about".

Set the rules

"I've got a firm policy on gun control. If there's a gun around, I want to be the one controlling it."

You know your core risks, the loaded guns that could really do a lot of damage. Next you need to decide what to do about them. Some organisations write a policy which defines how they want a risk to be managed - they usually say who is responsible for watching that risk and escalating problems, who can make decisions affecting the risk, what limits there are on these decisions and how they should be made (e.g. after obtaining particular evidence or the opinions of particular people).

Unless an organisation is happy to have an anarchic model for managing risk, where anyone can do anything, they are going to need a clear set of rules for staff to follow, whether its called a policy or not. A clear procedure might not always be followed; but if there is one there is a lot better chance of avoiding a damaging situation, or reacting quickly to damage that is occurring, than having no procedure at all. The best policy rules of all are the simple ones. *"I'm warning you, you mess around and I'll put the cuffs on you. You talk dirty, I gag you. If you run, I'll shoot you."*

Know what is really going on

"Please don't wake me unless you're sure we're gonna crash cause I wouldn't want to miss something like that."

If you are intimately involved in all the day to day activity of your organisation then congratulations: And don't read further. Most are not, and in an organisation of any size or complexity it is not possible for the few people at the top to have that level of

involvement. Here is where risk management needs to be a factor in defining the reports and analysis that go to inform the senior management team.

Without the right information management are steering blind, and often the information they get is dominated by data on business activity levels and the good news stories that staff are always happy to escalate to their bosses. Missing from this picture is information on the way the threat level of risks might be changing (which might dictate a change of plan) or potentially where those risks are already damaging the organisation. If management can get this picture of current state threats and damage then they have the information they need to make an informed decision on whether they want to do anything different about it. Without that picture there's a good chance that a risk which does great damage will come as a surprise that no one in management saw coming.



Know what you are getting into

"Ever notice how you come across somebody once in a while you shouldn't have (m)ucked with? That's me."

One of the great things about the opportunity of doing new things is that you can usually say 'no thanks' if you don't think you'll like it. In risk management terms you can avoid damaging your organisation if you avoid doing new things that are likely to cause issues. A new product or system, a critical new hire, a new supplier or outsourcing - without the right due diligence you stand a chance of making a costly mistake that was entirely avoidable. Doing anything new is going to come with some risk, but with good risk management you can check beforehand that it is not going to be far more damaging than the potential upside. Sometimes you are forced to act, perhaps by launching a new product to meet a competitor's aggressive challenge even before you are sure that staff and systems can actually support it - but if you know the risks you are taking on you can watch them like a hawk and be ready to respond if the worst does happen.

Invest in failsafe controls

Clint - "We're not just gonna let you walk outta here."

Robber - "Who's we, sucker?"

Clint - "Smith, Wesson, and me."

A lot of organisations spend a lot of time and money putting in place systems and equipment to make their business run efficiently. This is one of the major sources of competitive advantage and cost control. Unfortunately few of these organisations spend any time with these new tools building in failsafe controls that will limit some of the worst damage risks can cause. Result, you have a system which you might rely on for the next 20 years and you haven't used it to block off any of

the major mistakes or abuse that it could contribute to. Basic examples include enforcing segregation of duties which would prevent a dishonest employee from falsifying a transaction and stealing money. More sophisticated examples might be building in automated checks on the quality of data being entered or exception reports which quickly flag items or transactions which look unusual.

Incentivise people to do the right thing, deter them from doing the wrong thing

“Any sonofabitch takes a shot at me, I’m not only gonna kill him, I’m gonna kill his wife, all his friends. Burn his damn house down. Nobody better shoot.”

If you want people to follow a procedure, to behave in the way you’ve asked them to in order to control risks, human nature dictates that you need a mix of incentives and threats. This works a lot better than relying on people to do the right thing because they are ‘decent’ rather than because they have an incentive. *“If we cut down my percentage, liable to interfere with my aim”.*

Putting your expectations in their job description and objectives is a good starting point. Linking performance of those expectations to bonuses and non-performance to disciplinary action is even better. The greatest risks demand the strongest deterrent and biggest incentive. *“All you have to do to have an equal share of this money is crank this turret around and blow a hole in that door.”*

Manage a crisis

“When things look bad and it looks like you’re not gonna make it, then you got to get mean. I mean plumb, mad-dog mean! Cause if you lose your head and you give up, then you neither live nor win.”

Bad things will happen. The best risk management in the world won’t foresee everything or stop it all from occurring. When serious issues do inevitably strike the way the organisation manages the crisis will be the difference in how well it emerges from it. Crisis management is something every organisation should plan for, understand the response and who will lead it, which third parties they are going to need to turn to, and what options are available for some of the more likely scenarios.

Running simulations, drills in which a crisis has occurred and managers are asked to respond in realistic but not optimal conditions (e.g. some key managers are on holiday, now who takes over?) is a way to prepare for these situations. Loss of a key building and sudden loss of a key source of cash funding are two of the most dangerous and common scenarios. There are many others – too many to prepare for individually - which is why practice is so important as it gets management used to dealing quickly with major problems. A well practiced management team can react to a crisis without chaos or hesitation and has a much better chance of surviving the experience.

React to warning signs

“Oh you’re welcome. About as welcome as a turd in a swimming pool.”

Not every threat or problem can be predicted, and you have to

expect unpleasant surprises. The best way we know of dealing with these surprises is to get to them early, as early as possible. How to do that? It starts with how your organisation reacts to small issues - probably by not spending too much time on them, which is usually the right thing to do. Except that most big issues that cause an expensive problem start out as small issues which were ignored until too late. This is why the organisations that manage risk really well spend at least a little time on every issue, whatever the size. A service issue, a complaint, an error, a failure in procedure, even just noise from the business that not everything is working well, should all be looked at for long enough to get an idea whether it has the potential to develop into a much larger problem. If the answer is yes, you can start running to prevent that from happening.

Learn from mistakes, fast

“Everybody’s got a right to be a sucker once.”

If you don’t learn the lessons from something that has gone wrong, and put a fix in place to stop it happening again then you have a long journey ahead of you to make risk management a strength of your organisation. The principle in the words of Clint - *“You improvise. You adapt. You overcome.”*



What you need to avoid – the Don’ts

Just tackle risks in your comfort zone

Clint – *“When I get to liking someone, they ain’t around long.”*
Loan Watie – *“I notice when you get to disliking someone they ain’t around for long neither.”*

A great strength in many small organisations is the proximity of the top team to the whole enterprise – this means few risks or issues in the business go unnoticed. The downside for these organisations is that the top team is not large enough to carry a full range of subject matter experts. This can lead to the entirely normal consequence of management focusing on those parts of the business where they are most at home and technically able. As a result risks arising elsewhere do not receive the same focus and effort, even though they may be the most pressing risks the organisation faces. Organisations should always make a conscious effort to look at the risks in those parts of their operation that they have not focused on, and overcome their dislike for doing so.

Identify the wrong root cause

Clint – *“Anybody can tell I didn’t do that to him.”*
Chief – *“How?”*
Clint – *“Cause he looks too damn good, that’s how.”*

Where you have a risk, or an issue increasing a risk, that you want to do something about, then it is critical that any action you take is the right action. One of the major mistakes that organisations make when acting on risk is to tackle a symptom rather than the root cause. There is no substitute in these situations for experience and technical expertise; for instance a technology performance issue will need technology expertise to diagnose and solve. Taking the experience route makes it more likely that the right solution will be found, and that it will not produce unintended consequences that might be as bad as the original problem. Remember, *“Nothing wrong with shooting as long as the right people get shot.”*

Over-engineer your risk management solution

“Half the things we do are window dressing. Take running alongside that limousine. It would take an anti-tank missile to put a dent in that damn thing, but there we are... out for show.”

Simple approaches usually work best. Any feedback from those working within an organisation that they do not understand how risk management is meant to work almost always means that the approach adopted is too complex. The simple principles in this paper do not often need to be embellished. Sometimes embellishment is largely cosmetic, for instance colourful risk reports which take a large investment of time to produce. But on other occasions the embellishment can be more significant, and dangerous; for instance in complicated matrix management responsibilities where actual ownership of risk gets lost. A commitment to effective risk management means a commitment to applying simple principles and, wherever possible, simple but effective solutions. *“Take these three items, some WD-40, a vice grip, and a roll of duct tape. Any man worth his salt can fix almost any problem with this stuff.”*

The tricky part

Translating risk management theory into practical actions, actions which both work in practice and improve the organisations where they are being applied, does take skill. This skill is not in the knowledge of those techniques; rather it is in the application of these techniques to the individual organisation. Too much complexity leads to non-use, while a one-size-fits-all approach can damage the best parts of the



business culture that helped the organisation to be successful in the first place. In other cases risk management may need to drive culture change if the organisation has a history of expensive mistakes.

Tailoring the solution to each organisation is where Kingston Smith Consulting LLP, the business protection consultancy, can make a difference. Our team blends individuals with deep risk expertise and those who have experience operating on the board's of large and small businesses alike. This combination results in an approach that utilises knowledge of the best risk management techniques available, but applies them through the filter of commercial common sense to determine what is appropriate and valuable to the client in each case.

Pictures © The Malpaso Company and Matten Productions

Kingston Smith Consulting LLP

Devonshire House, 60 Goswell Road, London EC1M 7AD, UK Telephone +44 (0)20 7566 4000 Fax +44 (0)20 7566 4010
info@kscllp.co.uk www.kscllp.co.uk

A list of partners is available for inspection at the above address.

Registered in England and Wales as a Limited Liability Partnership: No OC341786 Registered office: Devonshire House, 60 Goswell Road, London EC1M 7AD