White Paper: Risk Management 101

It's not what you know, it's what you don't!

Introduction

We support hundreds of organisations here at Ethical IT, from 4 person start up charities to 1,000+ desk national social change organisations. Sometimes, things go wrong. Unexpected events from political struggles to natural disasters to, yes, IT system failures, can happen to anyone. How prepared that organisation it to deal with these events often aligns to how successful they are in general, and how well run they are overall.

Risk Management is a big part of that ethos. It sounds daunting and time consuming but it needn't be – recently we went through ISO27001 Certification and found a robust mechanism to capture, monitor and control our risks, which we wanted to share with you.

If I could predict the future…

…you'd probably be wealthy, it's true. The nature of risk is uncertainty, which cannot be stopped, but what you *can* control is what sort of response you are prepared for, covering most of the basis where issues may crop up that disrupt your operations.

These will of course change over time, so the real challenge is embedding Risk Management into your ethos and working routines, to avoid unknown unknowns having as bigger impact as they might.

The five-step approach below can act as a checklist to building your Risk Register; it is based on the principals of:

1. **Identify** – brainstorm, record
2. **Analyze** – score, compare
3. **Action** – plan, mitigate
4. **Monitor** – watch, listen
5. **Control** – review, update

1. Identify

This first step is arguably the hardest to do well. You will need to assemble a team that spans as many levels of the organisation as possible, each with an intimate knowledge of how things are done, what the market is doing, what the law books say, how the accounts are looking, what competitors are up to even.

Use a neutral facilitator if you can, consider allowing anonymous submissions too – we want to

encourage as much information out of the team as possible.

Risk Id	Risks	Current Risk: Likelihood	Current Risk: Impact	Current Risk: Severity	Status	Owner
Category 1: Project selection and Project finance						
	Financial attraction of project to investors	4	4	16	Open	
	Availability of finance	3	4	12	Open	
	Level of demand for project	3	3	9	Open	
	Land acquisition (site availability)	3	3	9	Open	
	High finance costs	2	2	4	Open	

Break down the risks into sections:

- Internal: Facilities, Processes, Systems, Access, Staff
- External: Legislation, Audits, Compliance such as Health & Safety, Security Breaches
- Knowledge management: Skills gap through turnover, documentation, intellectual property
- Financial: cashflow, 3rd Party Supplier costs / stability, governance
- Strategic: Political climate, long term objective changes, reputational damages

The end goal is to form our Risk Register, each risk being given a unique ID and an owner responsible. Don't reinvent the wheel – there are loads of templates you can use such as this:
https://www.stakeholdermap.com/risk/risk-register.html#risk

2. Analyze

Next, we need to your risks against one another and score them, to allow you to focus the most effort on the biggest risks.

Impact \ Likelihood	1	2	3
1	Low	Low	Medium
2	Low	Medium	High
3	Medium	High	High

Each risk should be rated for:

- Impact: how catastrophic would it be
- Likelihood: how probable is it

A common technique is to score each out of 3 and use a simple table to give a Red, Amber, Green (RAG) status on your Risk Register.

Page 8 of this document from the Risk Management Institute can help define these measures:
https://www.theirm.org/media/886059/ARMS_2002_IRM.pdf

3. Action

Red and Amber risks should now be allocated a Risk Response. This can be anything from a complex set of documents such as a Disaster Recovery Plan, to a simple instruction or action.

Broadly speaking, a Risk Response can fall into one of four categories:

Accept: the risk is too small to warrant a plan and is accepted

Mitigate: steps can be taken to reduce the impact and/or likelihood of the risk

Transfer: liability for this risk is moved elsewhere, such as paying a 3rd party for a service to cover this (in itself a possible risk!)

Avoid: plans are put in place to render the risk not applicable to you

In almost every case, training and knowledge / communication is going to be a key output, ensuring all and sundry are versed on the risks and their responses.

4. Monitor

The Risk Register is a living document. Left alone it will become useless and leave you exposed to serious risks and lack of awareness.

The Board of Directors should sign off the Risk Register and it should be reviewed at the highest level on a regular basis.

Department Heads should own their risks and play an active part in reviewing the Risk Register on a regular basis.

Staff should know the key risks and their responses; it should be part of induction and regular training.

The point is, everyone should know where the Risk Register lives, what is in it, and how to report potential risks – of known and unknown varieties – upwards for review.

External reporting is also advised; 3rd Party Vendors should input to this document on a regular basis, and Trustees kept informed as part of routine communications.

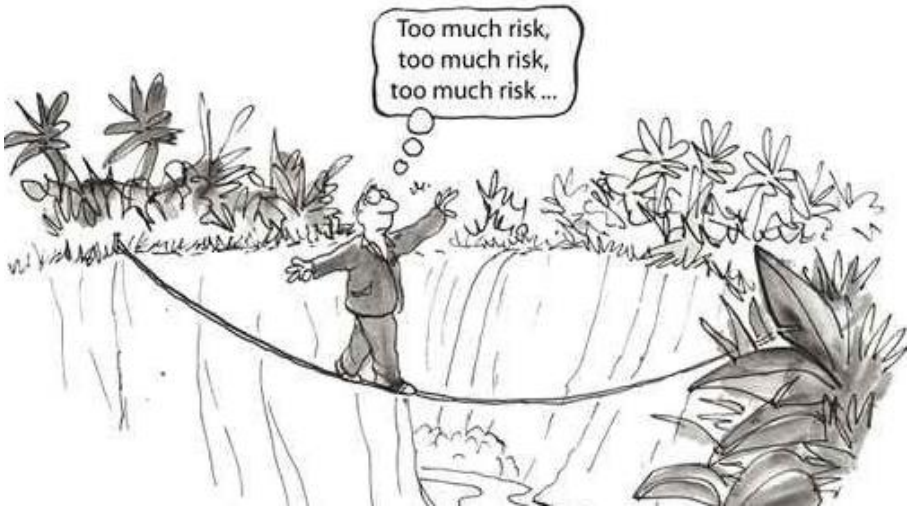
5. **Control**

True Risk Management only happens when your process is embedded, reviewed, updated, and tested.

For example, when was the last time you *really* tested your backups work? Or simulated your office becoming inaccessible? What if someone in your company got a virus by opening a spam email and it infected your whole shared drive – could you recover? Being able to answer these questions shows you take risk seriously, it will educate your team and will be a godsend if you are unlucky enough to experience a real incident.

The Risk Management function should be named and sit within a team who has the responsibility of scheduling reviews, tests and scrutinizing the Register with the full support of the leadership. Internal Audit can be very revealing and relatively cost effective when done by new recruits!

Above all else, the Chief Executive signs off on the Risk Register, but it is *owned by everyone*



Further Reading

Risk Management Institute Guide: https://www.theirm.org/media/886059/ARMS_2002_IRM.pdf

Risk Register Templates http://www.hse.gov.uk/risk/casestudies/

10 Golden Rules of Risk: https://www.projectsmart.co.uk/10-golden-rules-of-project-risk-management.php

Examples of Positive Risks: http://business.simplicable.com/business/new/9-examples-of-positive-risk

Aviva guide to Charity Risk - https://broker.aviva.co.uk/document-library/files/ch/charities_and_not_for_profit_risk_management_guide_2011_3.pdf