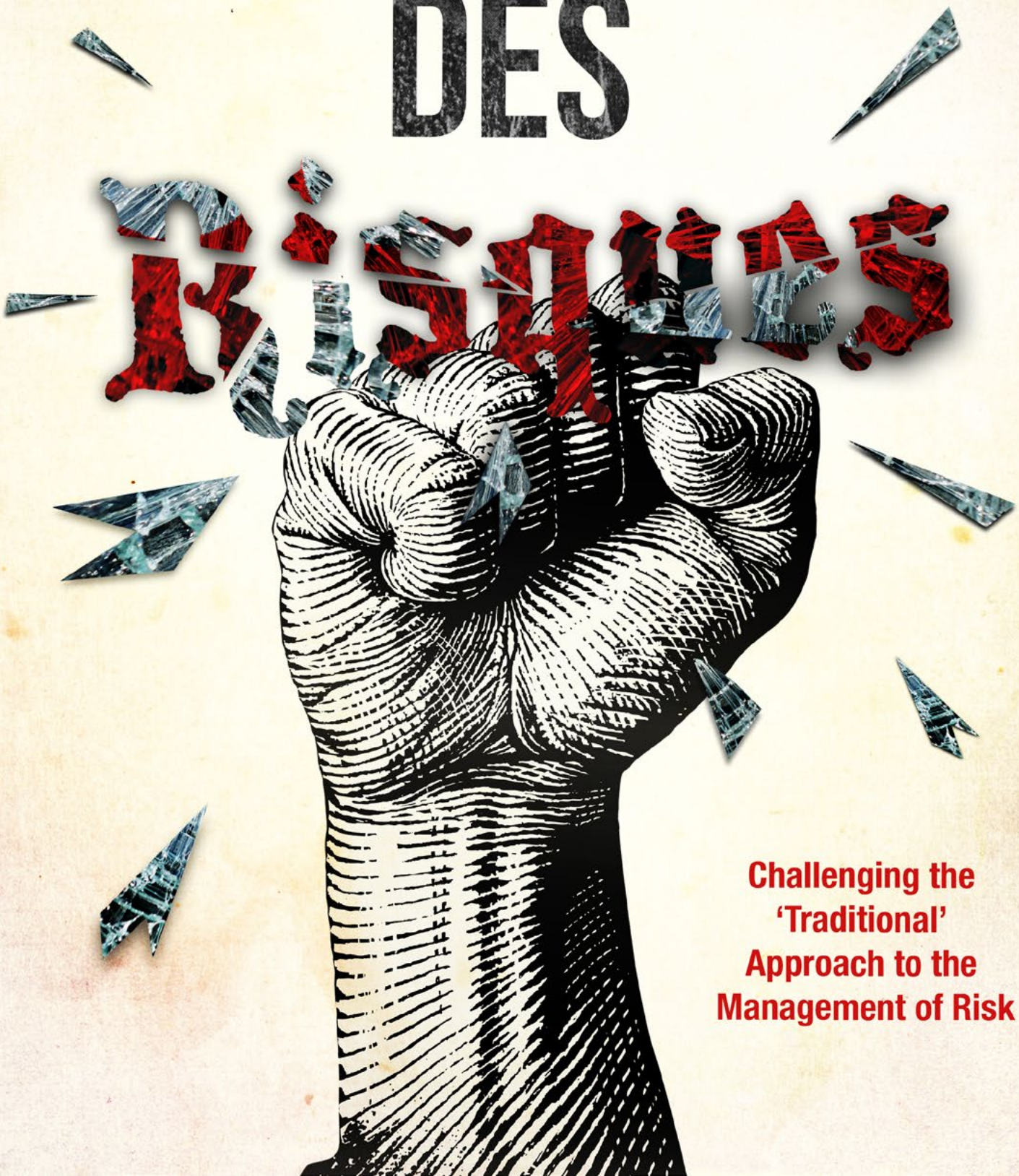
ROD FARRAR

RÉVOLUTION DES RISQUES



Challenging the 'Traditional' Approach to the Management of Risk

CHAPTER 9 – EMBEDDED RISK MANAGEMENT – THE 'HOLY GRAIL' OR AN ACHIEVABLE GOAL?

INTRODUCTION

If I had a dollar (preferably a US Dollar) for every time I hear an organisation state that their goal is to embed risk management as part of their day to day business I would be a very rich man. I would be extremely poor, however, if I was relying on a dollar from every organisation that had achieved it.

You see, there is a fundamental problem; no one has been able to articulate what that actually looks like. That is, until now.

This might surprise you, but a significant amount of embedding of risk management into the day to day business is **already occurring** in every organisation, even those who do not have risk registers.

But that makes no sense I hear you say. How can we have risk management embedded into our day to day workplace if we do not have a risk register? **The answer lies in the humble control.**

THE PREMISE

Very few things are going to happen within your organisation that haven't happened before - in either your organisation or a like organisation

That is not to say that nothing new happens – particularly in highly complex new endeavours. For **most** organisations, however, something that happens that has not occurred before in the organisation or a like organisation is a rarity. When it does, new controls can be introduced in an attempt to prevent the same thing from happening again in the future.

I contend that, for the most part, the **risks** to hospitals, universities, hotels, councils, child care centres, aged care facilities etc. are the same, the only thing that differs is the context (i.e. what controls are in place [beyond those that are legislated], its location, the level of staff experience etc.)

I provide a case study on my courses of a student who worked for a major retail chain in Australia. He was the manager of the importation and distribution of plants and trees on behalf of the company. He relayed to me the controls he had in place and mentioned the $150,000 he had just received in his budget to fund an additional training and awareness campaign for biosecurity. The risk is obvious: *release of a biosecurity threat into the community*. However, when I enquired as to whether the risk was in the risk register, he stated that they didn't have one or, if they did, he had never seen it. The point is, he was managing the risk by ensuring all of the controls were effective, so when he identified what he perceived to be a control gap, management trusted his judgement and provided funding to address the deficiency. **He was managing the risk without a risk register**, that is to say, the management of risk was totally embedded in the day to day operations of the business.

I am not suggesting for a minute that we abandon the risk management process and throw away our risk registers. What I am suggesting is that the manager in this case was managing his risk in a manner that far exceeds what I witness in so many organisations despite not having the risk recorded in a risk register. He was **managing the risk**, not simply **doing risk management**.

So let's test this theory by identifying just 10 common risks that could exist in each of the organisations highlighted above.

Hospital
Legionnaires outbreak in the hospital
Contaminated food served to patients/staff
Wrong medication or wrong dose of medication administered to a patient (particularly schedule 8 drugs)
Theft of pharmaceuticals by a member of staff
Surgical instruments/equipment left in a patient after surgery
Assault of a patient by a member of staff (including sexual assault and use of unreasonable force)
Issue motivated person takes control of part of the hospital or causes harm to staff and patients (e.g. active shooter)
Assault of staff or other patients in the emergency room of the hospital
Wrong surgery undertaken on a patient
Member of staff takes action (e.g. legal action, self-harm) as a result of unresolved/poorly handled bullying and harassment claim

University
Systemic plagiarism uncovered within the university
Member of staff exchanges higher grades for benefits
Fraudulent claims for government subsidies
Issue motivated person takes control of part of the university or causes harm to staff and students (e.g. active shooter)
Explosion in university teaching facility
Students involved in a prank/incident that is contrary to the law or community standards
Member of staff or student takes action (e.g. legal action, self-harm) as a result of unresolved/poorly handled bullying and harassment claim
Theft of funds from University trust account/s
Unauthorised release of, access to, or changes to student data
Uncontrolled release of a toxic substance from a laboratory

Hotel
Legionnaires outbreak in the hotel
Uncontrolled descent of an elevator
Contaminated food served in the restaurant
Theft of items from a guest room by a member of staff
Member of staff takes action (e.g. legal action, self-harm) as a result of unresolved/poorly handled bullying and harassment claim
Item (e.g. window, piece of the building etc.) dislodges from hotel and falls to the ground
Guests unable to escape from the hotel during a fire emergency
Unauthorised release of, access to, or changes to customer confidential data (including financial data)
Bedbug infestation at the hotel
Member of staff assaults a guest (physical, sexual or verbal)

Local Council
Theft of council supplies/equipment
Explosion at bulk fuel storage facility
Loss of council records (electronic and/or hard copy)
Untreated sewage released into the adjacent water source
Member of staff or student takes action (e.g. legal action, self-harm) as a result of unresolved/poorly handled bullying and harassment claim
Legionnaires outbreak in council operated facility
Member of council staff or counsellor accept benefits for approval of works
Unauthorised release of, access to, or changes to resident confidential data
Systemic overcharging or undercharging of resident rates
Disruption to collection of rubbish
Note: *If the council operates an aged care facility and/or a childcare centre, the risks detailed below will also be applicable.*

Childcare Centre
Child kidnapped from childcare centre
Child leaves the childcare centre unaccompanied
Inappropriate behaviour towards a child by a member of staff
Heavy item falls on a child from height (e.g. bookcase, television, tree branch etc.)
Child falls from heights
Fire in the childcare centre during opening hours
Structural failure of outdoor playground equipment
Child left in childcare centre after closing
Child ingests poisonous substance (including medication)
Child exposed to dangerous foreign objects (e.g. broken glass/syringes etc.) in playground

Aged Care Facility
Assault of a resident by a member of staff (including sexual assault and use of unreasonable force)
Assault of a member of staff by a resident or a family member/visitor
Theft of resident's property by a member of staff (including manipulation of will)
Contaminated food served to residents
Wrong medication or wrong dose of medication administered to a resident (particularly schedule 8 drugs)
Residents unable to be evacuated during an emergency event
Theft of pharmaceuticals by a member of staff
Resident struck by a motorised mobility aid within the facility
Residents unable to be evacuated during an emergency event
Gross mistreatment/ malnourishment of residents

What you may notice from the above is that there are risks that are also common across industries, so we need not restrict ourselves to identifying things that have gone wrong within our own industries.

So what does this mean in practice?

For the most part, whether it be required by legislation and/or regulation or whether it be through internal policies and procedures, these risks should already be **managed** through the controls that **currently exist**. Therefore, when an incident occurs, in a significant proportion of cases (if not nearly all), it has been caused due to a **failure of existing controls** and not because of a lack of controls. This is an extremely important concept to understand.

What this also means is that to embed risk management into your organisation you don't need risk registers with hundreds (or thousands) of risks. What you require is a means of capturing all of the controls linked to each risk **and** a program to continually monitor their effectiveness.

As I look at the news over the last few days I see stories such as: patrons injured when grandstand collapses; man killed after part of a carnival ride dislodges and lands on the car travelling behind; Legionnaires outbreak in Sydney; two cases of Salmonella contamination from the same source in three months, and the list goes on. The common thread: all of these incidents were avoidable and should not have happened and, most likely there has been a failure in the **existing** control environment.

Let's look in more depth at one of those examples.

There have been recent cases of Legionnaires outbreaks across New South Wales and yet, there are multiple controls in place through various pieces of legislation and regulation that **should** prevent such an outbreak. These include (but are not limited to) [12]:

- development of a Legionnaire's risk management plan;
- installation of a drift eliminator;
- water in storage areas of hot water systems is kept at a temperature of at least 60°C at all times while the system is in operation;
- cooling tower maintenance program which includes:
    - towers serviced at least monthly;
    - continually treated with biocides, anticorrosion agents and a bio dispersant;
    - recirculating water sampled and analysed at least once a month for HCC; and
    - recirculating water sampled and analysed at least once every three months for Legionella.
- temperature of hot water systems to be tested at least monthly and recorded in the maintenance log book kept in relation to the system;
- corrective management program; and
- notification protocols to Department of Health upon discovery of bacteria above set limits.

And yet, Legionnaires outbreaks are a reasonably regular occurrence despite all of these controls. Why? The answer is simple: in such cases it is usually discovered after the event that the controls were not implemented or maintained effectively (i.e. there were control gaps).

I heard a quote from aviation expert Richard Quest on the Sunrise Program on 20th May 2016 in relation to the crash of the EgyptAir aircraft and the speculation it was caused by an explosive device that, I think, provides an insight into why things that should not happen continue to occur. The program hosts asked the obvious question about whether the plane is inspected and checked at each stop on the journey. Mr Quest stated that it was a requirement to do that but:

[12] Source prensa National Summary of Cooling Tower Legislation, March 2011 and South Australian Public Health (Legionella) Regulations 2013 under the *South Australian Public Health Act 2011*

"Familiarity breeds complacency; complacency breeds negligence and something eventually slips through".[13]

What he was eluding to was that, even with the best control frameworks, control gaps do arise, particularly when there is a human interface.

Avoiding these control gaps is particularly critical for risks where the consequences are **severe.** If we continue with the Legionnaires example, an outbreak at a hospital would have a **severe** consequence (as was the case at the Wesley Hospital in Brisbane in 2013). To that end, the controls associated with the maintenance of the cooling towers and hot water services are **critical** to ensuring such an event doesn't occur. Therefore, the control program needs to be documented in a cohesive manner, evidence needs to be collected and documented, and assurance activities need to be factored (and costed) into the control program to verify that the activities are actually being conducted (even more critical if the function is outsourced).

Subsequent to the outbreak at the Wesley Hospital, Queensland Health directed Queensland's 17 hospital and health services, and requested 103 private and day hospitals and health facilities to test their potable water systems for Legionella.

The results[14] were astonishing given the **regulated** nature of the controls:[16]

Samples Taken	Positive for L.pneumophila (the bacterium that can cause what is commonly known as Legionnaires disease	Positive for other Legionella	Positive for Legionella in complex care areas.[13]	Number of response Category[14]
6014	309	236	105	28

What is even more astounding is that the Wesley Hospital, which suffered the outbreak that led to the testing program being implemented, **tested positive again in early 2016.**

The lesson here is, if the legislation, regulation, policy, procedures and processes that make up the control environment were strictly followed, Legionnaires would be extremely unlikely. But that is not the case. There are obviously gaps in the control environment that lead to this being a somewhat regular occurrence. To close these gaps and more effectively manage our risks we need to manage our existing control environment more robustly.

Therefore, managing your controls effectively is one of the major contributing factors (as well as the correct description of risks) in moving organisations from doing risk management to managing risk

A control is something that is **currently** in place to reduce risk within an organisation. They have often been introduced/implemented into an organisation (or into organisations by legislators and regulators) as a result of a previous incident. But as I raised earlier, in many cases where an incident/event has occurred, it is not as a result of a lack of controls – but because of a **failure** of **existing** controls. This can be extremely damaging to an organisation when the controls that failed led to a catastrophic incident.

As I raised in my previous E-book, Risk is not a four *letter* word, my proposition is that regardless of the likelihood, internal controls linked to the risks within the organisation that have the highest consequence **must** be the focus of the internal audit program.

---

13 Sunrise Program, 7 Network 20th May

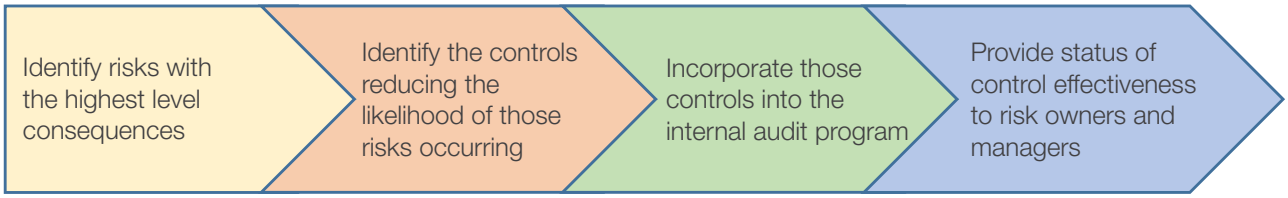
14 https://data.qld.gov.au/dataset/legionella-testing-in-queensland-hospitals-2013

15 Complex care areas include solid organ transplant units, haematology/oncology units, infectious diseases wards (housing patients with suppressed immune systems), medical wards (patients with suppressed immune systems and chronic lung conditions), Ear Nose and Throat wards (especially those with head and neck surgery) and Intensive Care Units. https://data.qld.gov.au/dataset/legionella-testing-in-queensland-hospitals-2013

16 Legionella is detected in a complex care area, clinical management of patient guidelines will also be activated. Plumbing and showerheads in the services areas accommodating complex care patients are to be disinfected. A risk management plan should also be reviewed or developed. https://data.qld.gov.au/dataset/legionella-testing-in-queensland-hospitals-2013

What is the purpose of an internal audit program? The internal audit program provides assurance that the controls currently in place are effective in order to reduce the likelihood that events will occur. Surely it follows then that the controls linked to the events with the highest level of consequence need to be the primary focus. Why? Because there is a **direct correlation** between the effectiveness of the control environment and the Likelihood that the risk will be realised, so if these controls are not the focus then the chances of the risk eventuating becomes greater and nobody within the organisation may be aware that the event could be imminent!!!!

So the process of embedding risk management into your organisation involves:



If your organisation is already doing this and all of the controls are **effective** you have embedded the management of this risk into your daily routine. If you do that for all of your higher consequence risks you will reduce the number of adverse incidents – which is, of course, one of the key outcomes of effective risk management.

THE SUPPORTING RISK REGISTER

In order to be able to adequately support this approach to the management of risk, there is a requirement for a different approach to capturing risks in a risk register. To that end, I have developed a risk register that prioritises the controls and measures their effectiveness as shown below:

Risk #	Risk Description	Risk Cause/s	Controls (aligned to Causes)	Control Owner	Control Effectiveness	Criticality of Control in relation to management of this risk	What is the impact should this risk eventuate?	Controls aimed at reducing Risk Impacts (if any)

There are other columns relating to the analysis of the risk and the risk wtreatment – this is just the information I capture in relation to the identification of the risk. The full template can be accessed here.

I have also included an example using two of the risks for a childcare centre here.

KEY TAKEAWAY

The key takeaway for this chapter is that you are already embedding the management of risk into your organisation, you are just not necessarily aware of it.