Culture, Risk and Governance

An ISC Executive Briefing Paper

Paper Number 1. March 2019

"The working environment at [organisation] is largely collegial, with high levels of trust in peers, teams and leaders."[i]

This sounds like a positive culture that organisations may strive to achieve, but this quote continues: "However, the Panel observes that this strength has been somewhat exaggerated, leading to some over-collaboration in [organisation] and over-confidence in abilities." In this case it led to a lack of challenge, and poor accountability across the organisation.

Culture is one of the most challenging aspects of a business to manage, in terms of generating the desired culture and cultivating throughout all levels. It is often said the 'tone is set at the top', so how then does the desired culture permeate throughout the organisation down to levels not in routine contact with the top? How is it measured and evaluated? Can a board and the most senior executives be accountable for the culture? These are some common questions being discussed in board rooms around the world, following the release of the report into the recent Royal Commission into misconduct into the banking sector in Australia.

Introduction

This executive briefing paper will discuss some key findings and learnings from a range of recent, and not so recent reviews, and how they apply to managing major hazard risk. These include:

- Prudential Inquiry in to the Commonwealth Bank of Australia, Laker, J. Broadbent, J. Samuel, G. 2018
- Final Report, Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry, Hayne, K. 2019
- The Report of the BP U.S. Refineries Independent Safety Review Panel, Baker, J. 2007

Key areas of focus include organisational culture and how it drives performance and behaviour, including the impact of remuneration structures on culture and behaviour, management of non-financial risk in organisations, including the three lines of defence model and lastly overall corporate governance and the need for those in control to challenge the business.

Organisational Culture

When considering how culture is created and maintained in an organisation, it is important to recognise that the organisational structure can enhance or hinder it.

In the case of the Commonwealth Bank of Australia (CBA), there was a federated structure in place, whereby all business units were managed independently and there was then an executive committee consisting of the business unit leaders and the chief executive. This could have been a very powerful structure that provided effective leadership of the organisation. For example, if the executive committee held a collective sense of accountability for the overall business it could have operated as a way to constructively challenge business decisions. It could have also provided benefits of diverse thinking in problem solving. In reality, the executive committee was operating in a way to minimise group accountability, and without any challenging of business decisions. There was a high level of trust among the executive committee, however this bred complacency, reduced challenge and resulted in a state of "chronic ease".[ii]

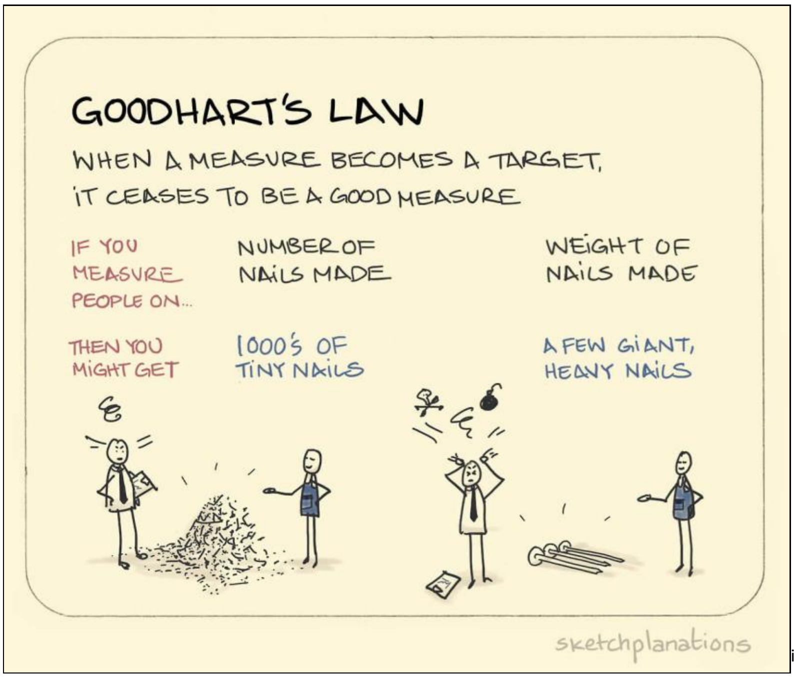
A key part of maintaining a positive culture is to ensure that all levels of employees have responsibility for the tasks, but ultimately the culture will be set based on the observed actions of the CEO and business unit leaders. Where the espoused actions to not match the observed actions, people will conclude the actual culture is more aligned with the observed actions. It is the responsibility of the board to hold the CEO and business unit leaders to account for their behaviours and actions. It is in this way that a board can influence the culture. This also means the board need to behave in a consistent manner to the culture they desire.

It is not enough to rely on holding people to account to drive a culture though. As was stated by Hayne, "…entities should, as often as reasonably possible, take proper steps to:

- assess the entity's culture and its governance;
- identify any problems with that culture and governance;
- deal with those problems; and
- determine whether the changes it has made have been effective."[iii]

There are many different techniques that can be used to asses an organisation's culture, and it is likely that any organisation will employ a range of means to gain a reasonable cross section of their culture.

A final cultural element worth exploring is how remuneration structures drive actions and decisions. Typically, we see performance measured against outcome, not taking into account how the outcome was achieved. Additionally, it is possible that poor behaviours are encouraged because the result is rewarded. Care also needs to be taken when establishing metrics that the outcome is measured by. This is because there can be a focus on managing the measure rather than managing the system. The illustration below explains Goodhart's Law, which states "when a measure becomes a target, it ceases to be a good measure", with respect to measuring performance.



[iv]

Management of non-financial risk

The three lines of defence model has been used for some time in the banking sector as well as having been adapted for other industries. It has similarities to how high hazard risk is managed in hazardous industries. The lines are defined as follows:

First line resides within the business, whereby the business "owns" the risk and is responsible for ensuring that critical controls or barriers are in place. They are responsible for managing the business within the organisation's risk appetite.	This is similar to the Roben's concept where by responsibility for managing risk lies with those who create and work with it. This is where the front line process safety people are embedded within the business at facilities. But operational risk management should rest with the operational team, supported by the embedded process safety personnel.
Second line is the independent risk management and compliance function in an organisation. This group is responsible for setting the policies and procedures, promoting a consistent approach across an organisation. It also provides an independent review and challenge to the first line.	This covers the overall risk management processes in an organisation. This function would be similar to the corporate process safety personnel, outside of the operational management of the organisation. A key to this working is for the second line to report independent of the operation, allowing them to be free of undue influence.
Third line covers the independent audit function, both internal and external. Its role is to provide independent assurance that the framework is suitable and operating adequately.	This focuses on the assurance aspect of auditing, providing the independent review and challenge to how the business is operating, ensuring the adequacy and health of controls or barriers.

All of the lines need to be overseen and reviewed by senior management to ensure each one is functioning correctly. It is not sufficient to have only the lines checking on themselves or each other only.

In the case of the CBA, the second line of defence was the business unit chief risk officers, however they reported to the business unit leader, and not to a separate function at the executive committee. This meant they were beholden to their business unit, and not an independent risk management role. Risk related issues were therefore driven down to be solved within the business unit and did not receive attention at executive committee or the board. Any detail that was reported up was so aggregated that it provided no insight into the issues, and tended to focus only on financial risk, leaving non-financial risk not adequately addressed.

There was a risk management program that covered assessment, assurance of controls, managing change, and incorporating learnings from incidents, however it lacked a clear articulation of minimum standards, adequate training and enforcement.[v] This resulted in inconsistent application across different business units. While there were action tracking systems in use, actions were often just extended without explanation, and a review was not conducted on whether the actions produced the desired outcome. There seemed to be more emphasis put on the risk assessment process at the expense of managing the outcomes of the risk assessment.

The CBA inquiry also looked at the concept of compliance risk verses conduct risk. It stated "Compliance obligations are broader than strict legal requirements and incorporate standards of integrity and ethical behaviour. For that reason, compliance risk and conduct risk overlap. Conduct risk is 'the risk of inappropriate, unethical or unlawful behaviour on the part of an organisation's management or employees.' At its simplest, conduct risk management goes beyond what is strictly allowed under law and regulation ('can we do it?') to consider whether an action is appropriate or ethical ('should we do it?'). The 'can we/should we' distinction is a recurring theme in the Inquiry."

Governance

From a governance perspective, the reports discuss the importance of clear accountability. There is a need for boards, their committees and senior executives to challenge the information reported to them. This means that the correct metrics need to be reported, and they need to be given insight into what the data is saying.

When considering the royal commission report, it stated that boards and their committees must:

- challenge management
- take steps to satisfy themselves that they are receiving all the right information to enable them to make complex decisions – where they are not receiving the information they need, they must challenge the organisation until they receive it
- monitor and measure the culture and governance of the organisation
- provide oversight of the organisation, including non-financial risks.

Hayne stated: "When I refer to boards having the *right* information, I am not referring to boards having *more* information. As I noted earlier, it is the quality, not the quantity, of information that must increase. Often, improving the *quality* of information given to boards will require giving directors *less* material and more information."[vi] This can be thought of as metrics *with* insight.

The review of the CBA defined accountability principles that should be maintained in an organisation. These are defined as below and form a solid basis for managing accountability of a federated organisation. A key element here is that not only does accountability need to be clearly defined, it then must be enforced, with people being held to account for their actions and decisions.

"**Accountability for the CEO**
(a) The CEO has delegated authority from the Board and is accountable for the overall management of the Group.
(b) The CEO in turn delegates authority to the Group Executives for the effective execution of operational activities.
(c) The CEO retains accountability for any delegation of the Board's authority, and is responsible for the Group Executives executing on their individual and collective accountabilities.
Individual Accountability of Group Executives
(a) Business unit Group Executives are ultimately accountable (with the CEO) for the products and services that their respective business units offer to customers.
(b) Business unit Group Executives are accountable for risk management outcomes, compliance obligations and adverse customer outcomes on an end-to-end basis. This requires that they have appropriate oversight of, and are satisfied with, the overall soundness of governance arrangements, policies and processes, people, systems, and tools and controls in meeting the institution's risk expectations/appetite and delivering an appropriate outcome. Where this is not the case, they should consider the risks involved in continuing the relevant business activity or offering the relevant product or service.
(c) Accountability of business unit Group Executives is not diminished by the location where particular functions are performed within the group (e.g. delegated activities) nor by the extent of Line 2 or Line 3 involvement or challenge.
(d) Group Executives must consistently exhibit leadership behaviours that create an environment that encourages staff to raise issues of concern.
(e) Group Executives must escalate issues of concern to the CEO/Board and ensure follow-up of material issues and effective resolution of root causes.
(f) Group Executives are responsible for cascading the above principles to lower level staff (modified with regard to their more specific roles).
Collective Accountability for Group Executives
All Group Executives are collectively responsible for identifying, escalating to the CEO/Board and mobilising resources within the Group to address systematic issues of concern."[vii]

Alignment with Process Safety

The observations and learnings reviewed here are clearly applicable to the bank and financial services industry but can also be applied to the management of major hazard facilities. This is because there are generic cultural, risk management and governance learnings. Consider for example the recommendations from The Report of the BP U.S. Refineries Independent Safety Review Panel[viii]. In this report ten recommendations were made. At least seven of these recommendations have direct parallels with the learnings and recommendations noted in the banking reports reviewed. The remaining three recommendations by Baker do also appear as minor themes in the banking reports. The key seven recommendations are:

Baker Report recommendation	**Summary**	**Parallel to banking reviews**
Process Safety Leadership	Board of directors and executive management must provide effective leadership in process safety.	The board and executive should demonstrate leadership including an environment of challenge.
Process Safety Culture	Involve relevant stakeholders to develop a positive, open and trusting culture.	Develop a culture of challenge at board and executive level. Monitor the culture.
Clearly defined expectations and accountabilities for process safety	Define expectations and strengthen accountability for process safety performance at all levels of executive management.	Define clear accountability and enforce it across the organisation.
Support for line management	Provide more effective and better coordinated process safety support for the line organisation.	Ensure that line management are aware of their accountability and provided the resources to meet these accountabilities.
Leading and lagging performance indicators for process safety	Develop, implement, maintain and periodically update an integrated set of leading and lagging performance indicators.	Implement leading and lagging indicators to provide data and insight to boards.
Process safety auditing	Establish and implement an effective system to audit process safety performance.	Utilise the auditing function of the third line of defence effectively and ensure that findings are reported to the board.
Board monitoring	Monitor ongoing process safety performance and actions associated with improving process safety.	The board should monitor and challenge the performance of the business to ensure it is operating in the best interests of stakeholders.

Conclusion

Governance and leadership in process safety is vital to prevent major incidents occurring. The principles required to exercise governance and leadership are similar, regardless of the industry sector. As can be seen here, there are several learnings from the banking and financial services sector that can have direct application in a major hazard environment. The concept of due diligence can be applied in safety to provide the framework for exercise the necessary governance.

More information

The IChemE Safety Centre offers a one day program called *Process Safety Leadership and Culture* which discusses the concepts of due diligence and how they can be applied to the process safety leadership in an organisation. If you would like further information please contact the IChemE Safety Centre at safetycentre@icheme.org

The Australian Institute of Company Directors also produced a good summary of the Royal Commission report and this can be accessed at https://aicd.companydirectors.com.au/membership/membership-update/royal-commission-final-report-executive-summary

---

[i] Laker, J. Broadbent, J. Samuel, G. Prudential Inquiry in to Commonwealth Bank of Australia, 2018. pp.89
[ii] Laker, J. Broadbent, J. Samuel, G. Prudential Inquiry in to Commonwealth Bank of Australia, 2018. pp.16
[iii] Hayne, K. Final Report, Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry, Vol 1, 2019. pp36
[iv] Source: https://www.sketchplanations.com/post/167369765942/goodharts-law-when-a-measure-becomes-a-target accessed 27 March 2019
[v] Laker, J. Broadbent, J. Samuel, G. Prudential Inquiry in to Commonwealth Bank of Australia, 2018. pp.27
[vi] Hayne, K. Final Report, Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry, Vol 1, 2019. Pp400
[vii] Laker, J. Broadbent, J. Samuel, G. Prudential Inquiry in to Commonwealth Bank of Australia, 2018. pp.64
[viii] Baker, J. The Report of the BP U.S. Refineries Independent Safety Review Panel, 2007