Deloitte.

Implementing risk transformation in financial institutions

Governance and culture

Know the worth of risk.

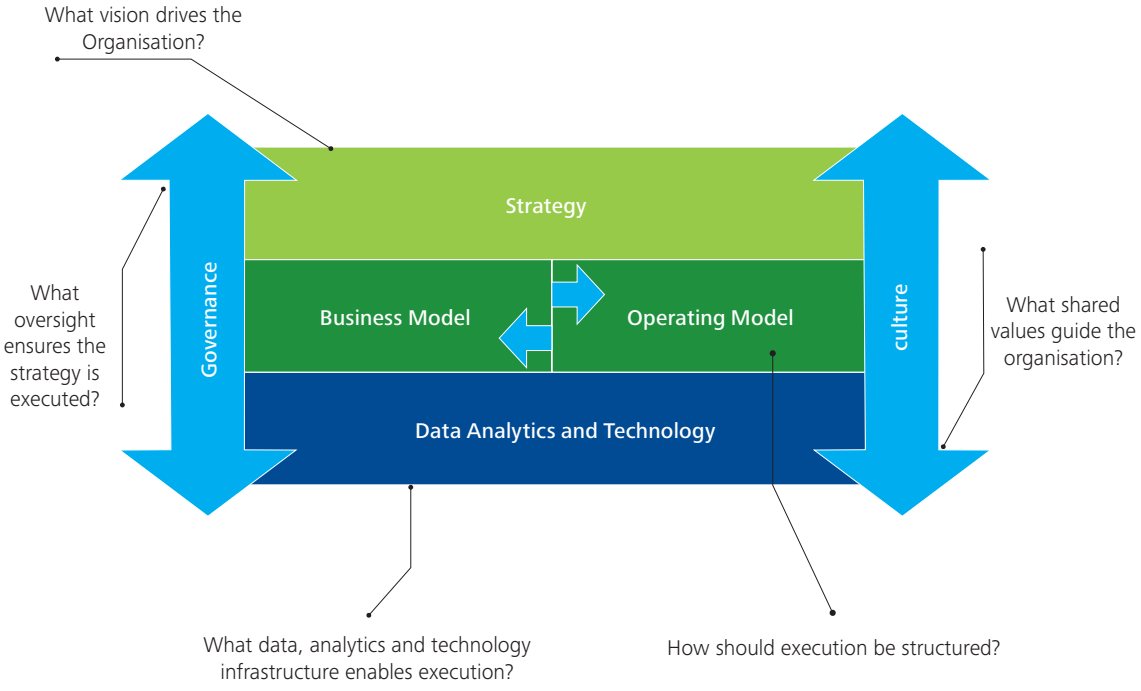
Risk transformation can enable a financial institution to elevate risk management from a functional capability to an enterprise responsibility that permeates the entire organisation. When that happens, every business, function, and individual becomes responsible for, accountable for, and capable of recognising and addressing the risks within their purview. Moreover, risk awareness and appropriate risk-related skills can become an integral component of every individual's responsibilities at every level. In these ways, risk transformation can enhance the organisation's ability to implement business strategies and achieve goals while addressing risks and complying with evolving regulations.

This document is one in a series of four on the cornerstones of risk transformation (see Figure 1):

- Strategy
- Governance and culture
- Business and operating models
- Data, analytics, and technology

As explained in Aligning risk and the pursuit of shareholder value: Risk transformation in financial institutions,[1] when these cornerstone frameworks and capabilities are in place, risk management, risk governance, and regulatory compliance can be implemented in a more aligned and integrated manner.

Figure 1: The cornerstones of risk transformation



[1] *Aligning risk and the pursuit of shareholder value: Risk transformation in financial institutions,* 2013, Deloitte <http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/AERS/us_imo_grc_RiskTransformation_in_Financial_10152013.pdf>

As Figure 1 shows, governance and culture envelope and interconnect with the other three cornerstones. Only with the right risk culture can management effectively implement its business strategies and objectives. (Generally speaking, the "right culture" for a specific organisation is one which enables it to pursue strategic goals within its risk appetite while managing the risks of doing business and fulfilling regulatory compliance obligations.) Governance provides mechanisms that assist management in shaping organisational risk culture. The business and operating model, and a firm foundation of data, analytics, and technology, also play significant enabling roles in risk transformation.

Each document in this series focuses on a single cornerstone so that leaders can launch risk transformation initiatives across all four cornerstones or start with a single one. This document examines the importance and workings of governance and culture.

Governance and culture as a cornerstone

In the past several years, virtually all major financial institutions have been working to strengthen their risk governance practices and risk culture. These continuing efforts have sought to address lapses in conduct and enhance controls, while enabling organisations to respond to new regulatory demands and increased scrutiny of risk governance, risk management, and operating cultures (see sidebar).

In addition, significantly increased regulatory capital and liquidity requirements are forcing financial institutions to stress capital efficiency in their strategies and objectives and, in particular, to reconfigure business models to emphasise those that are less capital-intensive. Transforming this cornerstone supports movement from business models based on high capital leverage, to those based on enhanced capital efficiency and lower leverage.

This said, each institution must define its own governance system and culture given its investor value proposition and capital return objectives. This paper is presented in this spirit; it does not aim to define an ideal for governance and culture or to promulgate one approach to risk transformation. It recognises, for example, that different degrees of centralisation and decentralisation will influence governance systems and culture needs. This paper points to ways in which leaders can define and design their governance system, shape the risk culture that their institution requires, and transform the way risk is managed across the organisation.

Scrutiny of governance and culture

The following are a few of the many sources citing the critical role of governance and culture in the management of financial institutions:

- Risk Culture in Financial Organisations by the London School of Economics and Political Science (LSE) (and others) noted that "The most fundamental issue at stake in the risk culture debate is an organisation's self-awareness of its balance between risk-taking and control." This report pointed out that "the presence of a centralised risk management function and apparently strong risk governance did nothing to prevent disaster."[2]
- Business Standards Committee Impact Report issued by Goldman Sachs noted the link between "cultural" behavior and how people are recognised and rewarded. It also stressed the link between client relationships and culture and cited post-crisis changes made in the organisation's "committee governance." Those changes included creating new committees, assigning formal accountability for reputational risk management, and codifying enhancements to committee governance and business standards.[3]
- Reforming Culture and Behavior in the Financial Services Industry, a workshop sponsored by the Federal Reserve Bank of New York in October 2014, examined the roles of size, complexity, and incentives in promoting certain behaviors and how they may affect organisational and industry-wide culture.
- Other sources citing the role of governance and culture include the Walker Report, the Wall Street Reform and Consumer Protection Act (Dodd-Frank), and Basel III requirements.

[2] *Risk Culture in Financial Organisations, 2013, London School of Economics and Plymouth University* < http://www.lse.ac.uk/researchAndExpertise/units/CARR/pdf/Final-Risk-Culture-Report.pdf>

[3] *Business Standards Committee Impact Report, May 2013, Goldman Sachs* <http://www.goldmansachs.com/a/pgs/bsc/files/GS-BSC-Impact-Report-May-2013-II.pdf>

Governing risk

Among other elements, corporate governance includes board and management oversight of activities, with an emphasis on the board's role as overseers and advisors to management and stewards of shareholder interests. Risk governance refers to board and management oversight of risk and risk management and the risk policies, processes, and practices that govern and support sound risk taking.

The Deloitte risk governance framework (Figure 2, explained in detail in a separate Deloitte document[4]), centers on risk (the centermost triangle). Board governance is the overarching activity (the outer blue band). The central relationship between risk and culture is depicted in the "culture" pyramid around risk. Risk governance, a dimension of corporate governance, includes, among other things, risk oversight, risk appetite and risk limits, risk capacity, risk monitoring and reporting, and risk-related roles, responsibilities, and authorities. These elements should inform the ongoing interactions between the board and management and the organisation's risk culture.

Figure 2: Deloitte risk governance framework

Sound risk governance encompasses risk-related committees, policies, processes, and practices, and fulfills their intent in activities such as monitoring risk exposures, challenging risk-related decisions, escalating risk issues to higher levels, and reporting on risk. Sound risk governance goes hand-in-hand with a strong risk culture. By the same token inconsistent, incomplete, or pro forma risk governance goes hand-in-hand with a weak risk culture.

Culture rules

Culture comprises the values, beliefs, and behaviors the organisation expects and elicits in employees and other stakeholders. Risk culture consists of those elements with regard to risk-related decisions, such as credit approvals and trading transactions, and behaviors, particularly those concerning employee conduct with regard to risk and employee interactions with customers. In the Deloitte risk governance framework (Figure 2), culture stands at the center—with risk—in that the two need to be tightly intertwined within a financial institution's modus operandi.

Risk culture, a subset of the broader organisational culture, both determines and results from the decisions and behaviors that are rewarded, encouraged, accepted, and tolerated within the organisation. Just as a person's character can be

[4] Framing the future of corporate governance: Deloitte governance framework, Deloitte 2013 <http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Content/Articles/AERS/US_AERS_Governance_%20Framework_102412%20Final.pdf>

defined by what he or she does "when no one is watching," so it is that risk culture can be seen as the risk-related decisions and behaviors that occur "when no one is watching." If what happens when no one is watching is not aligned with the organisation's governance principles, then culture and governance may be misaligned. Management must therefore continually ask, "How do we ensure that the organisation's risk culture and risk governance requirements are always aligned?"

People in an organisation will do what the culture—in all of the messages it transmits—indicates they should do. Their conduct, including the risks they take, the things they say to clients, and the ways they report transactions, will be motivated by incentives and by perceptions of management's goals. Given that culture usually determines conduct, failures in risk culture are frequently characterised as conduct failures, with the term conduct risk now being widely used.

Leaders have sought to review and strengthen their risk cultures because culture determines conduct. The Deloitte risk culture framework can assist these efforts (Figure 3).

Figure 3: Deloitte risk culture framework

Deloitte Risk Culture Framework

Risk competence
The collective risk management competence of the organisation.

Motivation
The reasons why people manage risk the way that they do.

Relationships
How people in the organisation interact with others.

Organisation
How the organisational environment is structured and what is valued.

As Figure 3 indicates, risk culture can be assessed along 16 attributes, related to four determinants: organisation, relationships, motivation, and risk competence. Once the risk culture is understood, elements of it that require strengthening can be identified.

It is often said that "culture eats strategy for breakfast." Thus, to implement a strategy, leaders must consciously foster a culture that will support achievement of the strategy. By the same token, leaders must be wary of—and avoid—strategies that cannot be implemented given the prevailing culture and an inability to change it.

The need for cultural and strategic congruence holds true at the enterprise level and within business units, where specific "subcultures" exist. For example, within the same financial institution the culture, strategy, and risk appetite of an online retail bank will likely differ from that of an investment bank, while those of a corporate finance advisory group will differ from those of a currency trading unit. Geographically diverse operations or markets may also require specific cultural adjustments; home-country organisational culture will rarely transfer to foreign locations without conscious effort and, usually, some level of local adjustment.

What constitutes a sound risk culture will vary among and within institutions. Some organisations will select strategies, goals, customer segments, and product lines that are inherently more risky or less risky. This is as it should be, given the range of customer needs and paths to creating value. However, leaders must consciously choose productive strategies within the risk appetite and then establish an enabling culture.

It's a tall order, particularly for a diversified global financial institution, as revealed in the Deloitte 2013 Bank Survey, which focused strongly on the subject of risk culture.

Deloitte 2013 Bank Survey: Key findings

The Deloitte 2013 Bank Survey[5] shifted from a focus on deleveraging and shoring up balance sheets (the focus of the 2012 survey) to standards, values, and risk culture in financial institutions.

The following were among the key findings arising from this global survey of 41 senior bankers:

- Among respondents, 65 percent see significant cultural problems in the industry, but only 33 percent believe their own banks have such problems.
- Respondents saw the top six causes of cultural problems in the industry as compensation structures, inadequate board oversight, (excessive) compensation levels, lax capital rules, management's inadequate understanding of risk, and misaligned performance metrics.
- Respondents viewed the most effective levers for improving culture at their banks as performance metrics, compensation structures, speaking up, compensation levels, conduct regulation, and board oversight.
- Less than half of the respondents believed that senior management at their bank is effective at punishing wrongdoing.
- Over 90 percent stated that senior leaders are responsible for setting and changing the risk culture.

That last point clearly illustrates that risk culture is a leadership issue.

Changing risk culture

The system of values, beliefs, and behaviors that combine to form the risk culture is shaped by leaders' decisions and actions, reinforced by business and organisational systems, and sustained by employee conduct. As noted, required changes vary from organisation to organisation, and across businesses and locations, particularly foreign locations. Therefore, management must understand the business issues and the cultural requirements at the needed level of detail.

Evolving business issues will continue to demand cultural change in financial institutions. Those issues include aggressive growth targets pursued in an environment of increasing costs, intensified competition, and more voluminous and complex regulatory demands. Potential cultural requirements include the need to increase risk awareness and ownership and to diversify workforces, while engaging employees and focusing more sharply on customer needs.

In addition, the following guidelines can assist management in fostering cultural change:

- **Start from a baseline:** Risk culture can be measured using indices of the attributes shown in Figure 3 and of other attributes that may pertain to the organisation, such as collective focus, shared beliefs, inclusion, and commitment. In addition, perceptions of governance and compliance, willingness to challenge decisions and to escalate and act on emerging risks, and ability to accommodate and address geo-cultural differences can be assessed. A baseline assessment measures key attributes and identifies levers of change.
- **Work across the enterprise**: It's easy to think of risk culture as monolithic or to imagine a single organisational risk culture. However, because risk culture will—and often should—vary with the nature of a business and its strategy, location, and regulatory environment, management must be attuned to these factors. Then leaders must design, implement, and maintain the type of risk culture suited to the organisation as a whole and to its specific business units' objectives and risk appetites.
- **Establish a common purpose:** People need clarity regarding approaches to risk, compliance roles and responsibilities, and customer needs—all in the context of creating shareholder value. Establishing a common purpose goes well beyond issuing a corporate mission

Case in point #1: Strengthening risk governance at a commercial bank

A large banking organisation needed to understand the impact of regulatory requirements on its risk management function. The goal was to develop a governance model for its U.S. based business that would enable it to comply with regulatory requirements and supervisory expectations.

To achieve these aims the team focused on:

- Studying each business function to assess its operations and its relationship to the governance model
- Developing tools for each business function to use in designing target states and operating models to strengthen its U.S. governance model
- Establishing a formal risk appetite and risk limits aligned to the company's strategy and goals
- Clarifying and defining key operating model components, such as decision rights, organisational design, people and culture, and infrastructure
- Creating a clear plan for implementation and transition, including input on change management and leadership communications

Key results included:

- Strengthening of regional and functional risk governance structures
- Alignment of the governance model with the risk management system, as well as enhanced accountability
- Enhancement of compliance efforts related to immediate and longer term regulatory demands

statement. It extends to instilling and sustaining a common purpose in employee on-boarding and training, performance evaluations and compensation systems, and management's conduct and decisions.

- **Maintain a consistent tone:** Risk culture begins at the top, with consistently communicated and reinforced values, beliefs, and conduct among the leadership team. To establish tone at the top, the board and management must be clear among themselves regarding strategy, business and operating models, acceptable risks, and approaches to risk governance and compliance. They must promulgate this tone throughout the organisation at every level. Breakdowns often occur with "tone in the middle" when leaders send faint signals or mixed messages down the ranks. If tone breaks down in the middle, a weak risk culture will frequently prevail, particularly among front-line personnel.
- **Monitor the culture going forward:** Absent strong leadership and sustained effort, the risk culture of the business units, functions, and institution will, over time, inevitably weaken. As a result, middle managers and employees may individually interpret what is in the customer's or organisation's interests or feel they are "on their own" when it comes to risk. Strong leadership and sustained effort are exerted through consistent, conscious use of cultural levers and periodic monitoring of risk culture metrics and performance indicators against baseline and updated values.

Single-point solutions to cultural problems invariably fail. As a collective concept, culture must be steadily nurtured through, for example, consistent communication, training, performance management, controls, and compliance. Risk culture calls for clarity at the leadership level, at the business unit and functional levels, and in individual roles and responsibilities. It is management's role and responsibility to provide that clarity. Simply stated, process follows culture.

Case in point #2: Assessing a subsidiary's risk culture and initiating change
A subsidiary of a global U.S. bank needed to respond to prior regulatory orders and provide an improvement plan for the local regulatory body, which intended to assess the effectiveness of the subsidiary's risk and compliance culture.

This risk and compliance culture assessment, simultaneously conducted in multiple languages, entailed:

- Evaluating the subsidiary's organisational values, incentive programs, and performance management approaches and comparing them with those of the parent organisation
- Identifying similarities and differences among local and expatriate staff members regarding their responses to the communications and actions of senior leaders
- Clarifying the relationship between the organisation's global policies and local rules to illuminate the effects on local staff and interactions with clients
- Assisting the subsidiary's leadership team in developing a prioritised set of actions to initiate and instill culture change
- Assessing the intended tone at the top and how consistently it was transmitted through the ranks

Key results of this assessment—the first for this bank in this country—included:

- More consistent communications from senior leaders and clearer expectations among staff regarding the importance of sound risk management practices
- Changes to certain global policies and programs to better suit the country culture and local operating environment
- A program of culture change geared to establishing a risk and compliance culture consistent with local regulations and local and global organisational objectives and policies—formulated and owned by the local leadership team

Key steps in risk culture change

Key, often iterative, steps in risk culture change include the following:

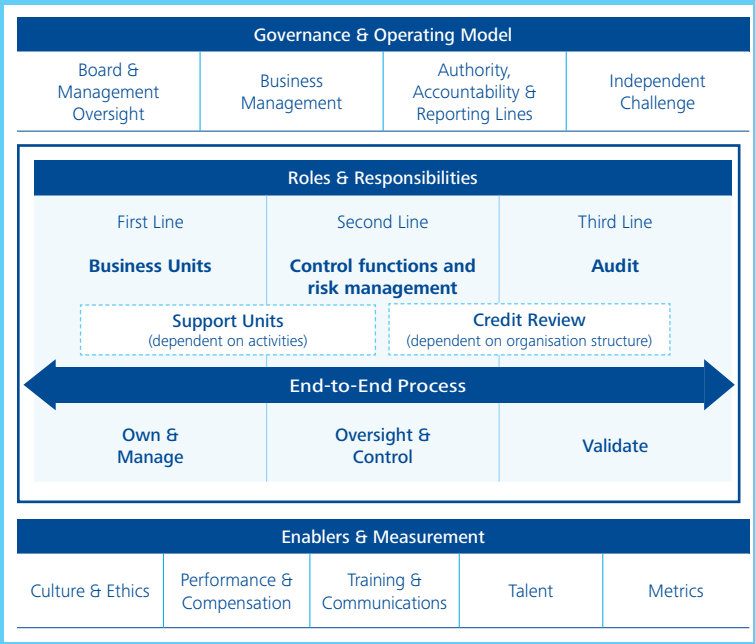
- **Identify the business issues and confirm the common purpose:** Leaders should first articulate the business strategy that the risk culture should enable, then determine which elements of the risk culture advance or hinder the strategy. This enables definition of the desired future state attributes.
- **Define the current state and identify cultural gaps:** Applying a risk culture diagnostic to the organisational or business unit culture generates a more precise assessment of the risk culture (than culture or engagement surveys) and of gaps between the current and desired state. This process should engage key stakeholders in determining which strengths to leverage and which gaps to address.
- **Plan which levers to address and how to address them:** Three broad, related levers can be employed to drive risk culture change: leadership, infrastructure, and processes. Leadership levers are the actions leaders need to start, stop, continue, or modify in order to drive change. Infrastructure levers include the systems, such as compensation and performance management and risk governance systems, which will reinforce the desired risk culture. Processes are the core business processes and associated behaviors that will drive results, and which must mesh with the culture.
- **Implement the plan and sustain the change:** Risk culture change demands ongoing awareness and continual reinforcement. Periodic measurement against the baseline risk culture diagnostic will reveal areas of progress and overall status, while performance measures will indicate the extent to which the business strategy is yielding intended results.

A variety of methods and tools can accelerate risk culture change. These include protocols for change, planning methodologies, and diagnostic tools ranging from surveys to dashboards that enable management to visualise relationships between the drivers and the attributes of the desired risk culture.

Implications for the three lines of defense

Risk transformation strengthens the three lines of defense model—the business units, control functions, and audit function—a generally accepted industry framework (see Figure 4). Transforming governance and risk culture strengthens the three lines of defense by driving risk management and governance practices into the daily activities of each line.

Figure 4: A depiction of the three lines of defense model of risk governance



Source: Deloitte's point of view on the Three Lines of Defense - What's Next?

Each line of defense plays a management mandated role in the risk culture. Those working in each line must understand and interpret their mandate and its risk implications, and conduct themselves accordingly.

Note, however, that the mandate and its interpretation can vary across the three lines, with the following conditions a common result:

- **Business units:** Due to their frontline positions, business units face intense pressures and often conflicting goals. They must operate within their risk appetite to achieve strong returns while preventing losses and preserving customer relationships. In the process, unrewarded risks, for instance, compliance, legal, and reputational risk—as well as excessively high (or low) risk positions—may be unnecessarily or unwittingly incurred.

The business case for transformation

The business case for transforming governance and culture primarily comes down to performance: achieving business goals while avoiding problems. Given that exposing capital to risk to generate return is a financial institution's core business, the role of risk governance and risk culture in performance cannot be overstated. Needless losses and regulatory compliance violations represent unrewarded risks, which consume capital, management attention, and other resources better employed in value creation.

Regulators, customers, investors, vendors, and the media take major losses and violations seriously. Although some stakeholders may not think of these problems as rooted in governance and culture, they suspect that "something's wrong at the top" and conclude that risks are not being well-managed or their interests are not being well-served. Severe damage to reputation and brand value may result.

Governance and culture determine success not only in product and market initiatives, but also in mergers and acquisitions (M&A). Lax governance and incompatible risk cultures have scuttled many a merger, as has failure to meld two cultures or to develop a new, enabling one. Such considerations, along with regulatory requirements and post-M&A implementation costs, strengthen the business case for risk transformation in any M&A situation. Establishing effective risk governance and a sound risk culture should yield sound returns on senior leaders' investment. Changes in risk governance focus on structures, risk policies, processes, and practices, while risk culture is essentially a board and management leadership issue. While governance and culture require leaders' time, attention, and efforts, as well as specific expertise and facilitation skills, those investments typically carry high returns given the potential positive impact.
Among those returns are reduced risk, improved control, and greater consistency in employee conduct and stakeholder experience.

Finally, and not insignificantly, sound governance and culture bolster the three lines of defense risk governance model, in which financial institutions have already made substantial investments.

- **Control functions:** Control functions and risk management also face pressures and demands, but generally with a clearer mandate. They provide business units with tools and capabilities they need to detect, identify, track, report, mitigate, and manage risks. They are also integral to the risk culture. For example, the CRO should work closely with the chief human resources officer and management to embed a strong risk culture into the organisation, in the context of broader organisational culture efforts.
- **Internal audit:** The audit function may have the clearest mandate: to periodically assess the adequacy of risk management, control, and compliance systems and to assist the board in understanding the risks the organisation faces. Audit should not act as a management quality assurance or quality control function or "police" the other two lines of defense, but should act as a periodic overseer, advisor, and backstop, in the context of providing assurance.

Proper attention to the other three cornerstones is critical to aligning the lines of defense. A clearly understood strategy provides a strong sense of direction and common purpose for all three lines of defense. Practical, integrated business and operating models define the role of each line in implementing the strategy. High quality data, analytics, and technology can provide the risk-related information each line needs to do its job.

Conclusion

As a cornerstone of risk transformation, governance and risk culture can be relatively straightforward to define in risk policies, codes of conduct, and ethical guidelines, but challenging to implement and maintain.

Risk governance establishes roles, rules, and parameters and instills rigor in decisions and activities. Risk culture focuses on social, motivational, and real time pressures, which can be resistant to change through governance alone; however, governance does much to inform and shape risk culture. From a leadership standpoint, conscious alignment between risk governance and risk culture is an imperative for risk transformation.

It is believed that financial institutions that do the best job of managing risk will secure a competitive advantage vis-à-vis their peers. Therefore, in the current business, economic, and regulatory environment, risk transformation should stand as a high priority. Governance and culture represent a key cornerstone and an excellent starting point for a risk transformation initiative.

Key contacts

Peter Matruglio
Partner
Australia
Deloitte
+61 2 9322 5756
pmatruglio@deloitte.com.au

Kevin Nixon
Partner
Australia
Deloitte
+61 2 9322 7913
knixon@deloitte.com.au

Tim Oldham
Partner
Australia
Deloitte
+612 9322 5694
toldham@deloitte.com.au

Grant MacKinnon
Director
Australia
Deloitte
+61 404 804 744
gmackinnon@deloitte.com.au

Scott Baret
Partner
United States
Deloitte & Touche LLP
+1 212 436 5456
sbaret@deloitte.com

MCBD_Hyd_04/15_51615