In 2013, the Financial Stability Board (FSB) – the single most global authority in the international securities regulator - issued the following guidance that calls on national regulators to costly a new regulatory expectation from boards of directors:
The board of directors must establish the institution-wide RAP (Risk Appetite Framework) and approve the risk appetite statement, which is developed in collaboration with the chief executive officer (CEO), chief risk officer (CFO) and chief financial officer (CFO) |
Likewise, in the UK, the 2014 update of the ‘compel or explain’ UK Corporate Governance Code governing all UK listed public companies states the following principle in section C.2: Risk Management and Internal Control:
The board is responsible for determining the nature and extent of the principal risks it is willing to take in order to achieve its strategic objectives. The board should maintain sound risk management and internal control systems.

The code further elaborates on this principle through specific code provisions that respectively require the board to:
(1) monitor the company’s risk management process (2) ensure that they have carried out a robust assessment of the principal risks facing the company and (3) ‘monitor the company’s risk management and internal control systems and, at least annually, carry out a review of their effectiveness, and report on that review in the annual report’. For the many impacted by these rising expectations, and a multitude of others like it in countries around the world, this global trend can be summarised as follows had to 64 directors are now increasingly expected to oversee management’s risk appetite and tolerance and take steps to ensure that it is aligned with the board’s risk appetite and tolerance.

For various reasons, many public company directors are not intimately familiar with the newest board risk oversight expectations. If prompted, many might as well respond with this all sounds reasonable but what does it really mean in practice for me?.

What is risk appetite and risk tolerance?
The International Organization for Standardization (ISO), the global standards setting body, in Guide 73 defines these two terms as follows:  
Risk Appetite (3.7.1.2): Amount and type of risk that an organisation is willing to pursue or retain |
Risk Tolerance (3.7.1.3): Organisation’s or stakeholder’s readiness to bear the risk after risk treatment in order to achieve its objectives. 

While these definitions are the product of intense global debate and discussion, the definitions require us also to clearly understand what is meant by the terms risk and risk treatment that are part of the two definitions. Thus, Guide 73 defines the two terms as follows: 
Risk (1.1): Effect of uncertainty on objectives 
Risk Treatment (3.8.1.1): Process to modify risk

The term ‘risk treatment’ is further elaborated by noting that the process can involve one or more of the seven following actions:

Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk
Taking or increasing risk in order to pursu an opportunity
Removing the risk source
Changing the likelihood
Changing the consequences
Sharing the risk with another party or parties, including contracts and risk financing
Retaining the risk by informed decision

In our daily lives, many times unknown to us, we are confronted with one or more risks. Assuming rationality, our personal ‘risk management process’ revolves around what we explicitly or implicitly think our objectives are and how we approach the task of identifying, evaluating and responding to the events that we perceive will create uncertainty and stop us from achieving those objectives. This is manifest itself in many ways.

A real-life example for people who have been to the beautiful island of Maui in Hawaii would be to decide whether to take the famous scenic drive on what is locally known as ‘the road to Hana’ on Routes 36 and 360. The Hana Highway is about 64 miles long. A Google search will reveal pictures, stories, cautions and accolades about this famous road. Visitors that rent cars may even be told by their car rental agency that their insurance cover on the car rental does not extend to those that elect to take ‘the road to Hana’ trip. Those that seek advice from locals may be told that it is critical that if you choose to undertake the trip, you do it clockwise not counter clockwise. The image above provides the clue that explains the cautions and the advice.

The VW emissions scandal of 2015 is a graphic illustration of widespread wrongdoings in a public company that may eventually turn out to involve thousands of employees.

The adventurers who take the advice will do the trip in clockwise direction. This allows their car to hug the right side of the road which means if the passengers have the misfortune of meeting another car or, in an even worse case scenario, a truck, the other vehicle will have to pass on the outside edge close to the precipice. The recommended direction of travel would be counter clockwise if the road was in Australia or in the UK where drivers drive on the left side of the road.

Within the context of this example, ‘risk appetite’ would involve determining whether the passenger(s) renting the car would even want to undertake the trip in the first place once they clearly understand the corresponding risks that they will be assuming in pursuance of seeing some breathtaking scenery and safe passage with no damage/harm to vehicle or its occupants. Some visitors to Maui may even have unwittingly found themselves on this route. They may not have had an ‘appetite’ or ‘tolerance’ for it had they known and understood the risks. Road signs and maps in the area provide a range of warnings. Some of the warning signs are more graphic than others. An early warning of what is ahead on the road to Hana is shown in the sign pictured below.

The HANA HIGHWAY
With 620 curves and 59 bridges, this stretch of road is a popular tourist attraction in Maui.

The board of directors must establish the institution-wide RAP (Risk Appetite Framework) and approve the risk appetite statement, which is developed in collaboration with the chief executive officer (CEO), chief risk officer (CFO) and chief financial officer (CFO) | Board Governance

Risk appetite and tolerance can be seen in action in this analogy by the speed that people travel the route, the distance of their car from the edge of the road, the type of vehicle they are in, their responses if they have the misfortune of meeting a vehicle in the other direction on a section of the road with a single lane, and other events. Risk tolerance, as defined by ISO, also links to whether the drivers are alone or with others, have dependents. Their finances, resources and ability to absorb the effect of an accident, perhaps without insurance and other similar variables.

Overseeing risk appetite and tolerance in public companies

The 2008 global crisis provided numerous examples of how boards failed to set and oversee their company’s risk appetite and tolerance. In this regard, the public companies that were at the early stage during the financial meltdown were those that, had they an ‘appetite’ to invest in subordinated debt/mortgage-backed assets with material exposure to the US housing market. These companies also had to decide how much effort and resources they were willing to expend to identify and understand the risks to those investments meeting or exceeding their target returns. They also had to decide what risk treatments (such as etc AF - if any), they were willing to put in place to mitigate some or all of the risks. If they did decide to pursue some of the risks to achieve target returns they had to decide how much resource and effort to invest in evaluating the safety and soundness of AIS to be able to honour their contractual commitments if the risk(s) AIS agreed to absorb actually materialised.

On the legal front, all boards must make conscious (or sometimes unconscious) decisions on the organisation’s risk appetite with regard to many issues, such as complying with laws, regulations and contracts, issuing materially misstated financial reports, etc. 

Boards with very low legal risk appetites and tolerance must take all the necessary steps to satisfy themselves that employees at all levels in their organisations, including those in the C-Suite, not only share their risk appetite and tolerance thresholds but also comply them. The VW emissions scandal of 2015 is a graphic illustration of widespread wrongdoings in a public company that may eventually turn out to involve thousands of employees and accrue losses. Companies have been convicted of breaching anti-money laundering laws and bribing foreign officials and have been fined and ordered to pay hundreds of millions to add to the list of examples where risk appetite and tolerance oversight by the boards fail. If anything, these are prime examples of the board’s risk appetite/tolerance.
Another example of risk appetite and tolerance in action can be found in the area of customer service. The boards of directors in many companies routinely make decisions on how many angry and dissatisfied customers they are willing to accept and tolerate. Most readers will have already interacted with companies who have made a conscious decision that 10 or more minutes of wait time responding to customer calls is within their company’s risk appetite and tolerance.

Similarly, in the environmental and sustainability area many companies and their boards must decide what their appetite and tolerance is to polluting the environment through their operations.

As regulators globally start to comprehend that holding a board accountable to oversee management’s risk appetite and tolerance is both a key to better corporate governance and a daunting and a complex task, guidance, such as the types issued by the FSB in 2013 on Principles for Effective Risk Appetite Frameworks and in 2014 on Board Oversight of Risk Culture will increasingly become a gold standard. Provided below are samples of the roles envisioned by the FSB for the boards and the CEOs to ensure their companies have in place an effective Risk Appetite Framework (RAF).

The board of directors should:

A Approve the financial institution’s RAF, developed in collaboration with the CEO, CRO and CFO, and ensure it remains consistent with the institution’s short- and long-term strategy, business and capital plans, risk capacity as well as compensation programmes

B Hold the CEO and other senior management accountable for the integrity of the RAF, including the timely identification, management and escalation of breaches in risk limits and of material risk exposures

C Ensure that annual business plans are in line with the approved risk appetite and incentives/disincentives are included in the compensation programmes to facilitate adherence to risk appetite

D Include an assessment of risk appetite in their strategic discussions, including decisions regarding mergers, acquisitions and growth in business lines or products

E Regularly review and monitor the actual risk profile and risk limits against the agreed levels (e.g. by business line, legal entity, product, risk category), including qualitative measures of conduct risk

F Discuss and monitor to ensure appropriate action is taken regarding ‘breaches’ in risk limits

G Question senior management regarding activities outside the board-approved risk appetite statement, if any

H Obtain an independent assessment (through internal assessors, third parties or both) of the design and effectiveness of the RAF and its alignment with supervisory expectations

I Satisfy itself that there are mechanisms in place to ensure senior management can act in a timely manner to effectively manage, and where necessary mitigate, material adverse risk exposures, in particular those that are close to or exceed the approved risk appetite statement or risk limits

J Discuss with supervisors decisions regarding the establishment and ongoing monitoring of risk appetite as well as material changes in the current risk appetite levels, or regulatory expectations regarding risk appetite

K Ensure adequate resources and expertise are dedicated to risk management as well as internal audit in order to provide independent assurances to the board and senior management that they are operating within the approved RAF, including the use of third parties to supplement existing resources where appropriate

L Ensure risk management is supported by adequate and robust IT and MIS to enable identification, measurement, assessment and reporting of risk in a timely and accurate manner

There is growing consensus that better board-level risk oversight is key to preventing the next wave of corporate governance breakdowns

The CEO should:

A Establish an appropriate risk appetite for the financial institution (in collaboration with the CRO and CFO), which is consistent with the institution’s short- and long-term strategy, business and capital plans, risk capacity, as well as compensation programmes, and aligns with supervisory expectations

B Be accountable, together with the CRO, CFO and business lines for the integrity of the RAF, including the timely identification and escalation of breaches in risk limits and of material risk exposures

C Ensure, in conjunction with the CRO and CFO, that the risk appetite is appropriately translated into risk limits for business lines and legal entities and that business lines and legal entities incorporate risk appetite into their strategic and financial planning, decision-making processes and compensation decisions

D Ensure that the institution-wide risk appetite statement is implemented by senior management through consistent risk appetite statements or specific risk limits for business lines and legal entities

E Provide leadership in communicating risk appetite to internal and external stakeholders so as to help embed appropriate risk taking into the financial institution’s risk culture

F Set the proper tone and example by empowering and supporting the CRO and CFO in their responsibilities, and effectively incorporating risk appetite into their decision-making processes

G Ensure business lines and legal entities have appropriate processes in place to effectively identify, measure, monitor and report on the risk profile relative to established risk limits on a continual basis

H Dedicate sufficient resources and expertise to risk management, internal audit and IT infrastructure to help provide effective oversight of adherence to the RAF

I Act in a timely manner to ensure effective management, and where necessary mitigation, of material risk exposures, in particular those that are close to or exceed the approved risk appetite statement and/or risk limits

J Establish a policy for notifying the board and the supervisor of serious breaches of risk limits and unexpected material risk exposures

Demystifying what needs to be done

The harsh reality is that few companies and their boards are well-equipped today to meet the FSB’s aspiration that boards effectively oversee management’s risk appetite and tolerance. A full discussion of the obstacles and major changes required to make this aspiration a reality is beyond the scope of this article. You are encouraged to read the longer and more detailed articles written by the authors in earlier issues of Ethical Boardroom and in Conference Board Director Notes.

Are boards up to the task?

There is growing consensus that a key element necessary to prevent the next wave of corporate governance breakdowns is better board-level oversight of management’s risk appetite and tolerance. Achieving this will require concerted, sustained, and major effort and, most importantly, tolerance for massive change from boards, regulators, CEOs, chief risk officers, internal audit and risk professions and their professional associations, and more. The changes necessary are quantum in size and radical in nature. Whether boards and the companies they oversee are up to the task remains to be seen. Only time will tell.


Gupta, Leech, The Next Frontier for Boards: Oversight of Risk Culture, Conference Board Director Notes, June 2015

Ethical Boardroom | Winter 2016