Building an efficient and effective risk framework

February 2020

Concept

The risk-based approach is not a new concept, and it allows businesses to develop a proportionate risk framework based on the size, nature and complexity of business activities. Businesses can build a scalable business model, while maintaining suitable oversight and control of their key risks in a commercial manner.

Autonomy in determining what is appropriate brings the benefit of avoiding unnecessarily over-engineered processes, and allows businesses to measure risks in a fashion which is specific their business.

Each business is exposed to many different risks, and responsibility for the risk framework environment starts with the Board, who are responsible for the effective and ongoing organisation and control of the business.

Risk Appetite Statement

Directors agree a risk policy and risk appetite statement, which chimes with their strategy and business plan, ensuring this is communicated with all relevant employees. This helps everyone to understand the risks that the business is willing to take.

Measuring Risk – Inherent vs. Residual

Inherent risk are those the business is naturally exposed to, without taking into account any controls. Residual risk is the remaining level of risk once appropriate policies, procedures and controls have been implemented to avoid, transfer or mitigate inherent risks. They can also be referred to as gross and net risks respectively.

Agreeing and regularly reviewing inherent and residual (or gross and net) probability and impact metrics enables risks to be measured in a meaningful manner, based on the perceived likelihood and extent of damage that they present to the business. Some businesses may be able to tolerate large financial losses, or survive a reputational impact with good crisis communications, but a loss of regulatory licence could be catastrophic.

In addition, agreeing client risk assessment metrics allows proportionate client due diligence to be completed at the start of a business relationship, with ongoing monitoring and periodic reviews tailored to an appropriate frequency, supported by trigger event controls to capture key changes between scheduled reviews.

Risk Registers

Identifying, recording and categorising risks on risk registers, reflecting the inherent risk that they present to the business also allows for the identification of any confluence of risk factors, which may increase an overall risk. For example, data and cyber security risk is likely to feature in a number of separately identified risks, as opposed to credit risk which may only apply to a few.

Mitigating Measures

Mitigating policies, procedures and controls are developed to treat the inherent risks by reducing the exposure to the business and preventing the risk from materialising, wherever possible, or at least limiting the damage. The frequency that policies and procedures are reviewed can depend on the residual risk that they are mitigating; if there is a fundamental change such as an update to a law or regulation, or if adverse findings and trends are identified during the compliance monitoring programme of testing.

Recording these mitigating controls on the risk registers allows businesses to measure the resultant residual risk. This risk is measured by applying mitigating policies, procedures and controls, considering the strength of the controls employed and therefore the residual risk. Boards can consider whether the risks are presenting an acceptable level of exposure, or whether further action is required.

First Line of Defence

Front-line staff must receive suitable training on relevant policies, procedures and controls, ensuring they understand their key role as the first line of defence, specifically discouraging hierarchical behaviour or silos, and helping them in discharging their responsibilities and imbedding the risk framework firmly into a business.

Validating the Control Environment

The compliance monitoring programme forms part of a business's second line of defence. It consists of a calendar of reviews, with scheduling determined by the residual risk rating, and testing plans, which prescribe sample testing of the control environment, such as compliance with policies and procedures, reviewing breaches or complaints registers, or ensuring that overnight sanctions screening is effective. It is a key method for the Board to have (and demonstrate it has) oversight of the effectiveness of the control environment.

Results can be graded, for example by using a red, amber, green (RAG) rating system and adverse results should be discussed and agreed with individuals and team heads, in order to determine whether there was perhaps a gap in a procedure or a deliberate failure to comply. It is important that the outcome of the discussion is a true reflection of what has happened, and not used as an opportunity for an employee to gloss over any failings.

Equally important is ensuring that the compliance monitoring programme operates in a blame-free culture, where personnel are not afraid of reprimand or punishment (unless misconduct has occurred), and they welcome the opportunity to enhance policies or procedures, or address training needs identified.

Communicating Results

Progress of the compliance monitoring programme and testing results are reported to the Board, and by utilising a RAG rating, Directors can use their oversight time effectively, by focussing their attention on their key risks, red or amber results or trends highlighted.

Updating the Control Environment

Boards subsequently consider the effectiveness of their control environment. This may include: agreeing updates to policies or procedures where they have been deemed inadequate or inefficient, implementing training where knowledge gaps or upskilling is identified, updating compliance monitoring programme review frequencies to increase oversight of a specific matter, or dealing with staff misconduct, where policies and procedures have been deliberately breached.

For more information please contact:

Sandra Lawrence

Compliance Manager, Trust and Corporate Services // Guernsey

t:+44 (0) 1481 734808 // *e:*sandra.lawrence@collascrill.com