

RegTech as a whole business enabler?

Whilst the Malta Financial Services Authority in Malta advocates that “RegTech solutions improve regulatory processes with the aim of helping authorised entities to comply with greater certainty and more efficiently to regulatory and supervisory requirements. .”, at Aspida we see utilising RegTech as wider to provide substantially more benefits to businesses.

RegTech has to be an enabler for businesses and proactively deal with the demands of risk management, complexity, cost and compliance in an environment that isn't getting any easier. The period during Covid-19 is a good example of why technology is going to be essential in this area, and without it businesses strategies may be at risk.

There has been plenty of discussion on the future of RegTech and the benefit to firms. Many businesses are struggling to determine how to use technology to their best advantage to manage their regulatory obligations and to improve efficiency in compliance. In itself, the marriage of regulation and technology is not new, but it is becoming more and more crucial as levels of regulation rise and focus on data and reporting increases.

Financial institutions have shelled out more than \$300 billion in fines since the financial crisis according to Bloomberg. The cost of compliance spending is steadily increasing with up to 15% of firms' staff working on governance, risk management and compliance according to the Financial Times. RegTech has the potential to significantly reduce this figure by filling compliance gaps, reducing costs and detecting enterprise risks before the regulators.

RegTech puts a particular emphasis on regulatory monitoring, reporting and compliance but we at Aspida believe that importantly to be practical it needs to assist in managing risks, identifying control issues and providing valuable business insight. This in turn can produce positive outcomes for those businesses clients. Think about how businesses can demonstrate better protection for customers, whilst providing improved and faster services.

Identifying risks and mitigating them to ensure business survival and meeting regulatory obligations is fundamentally important and now more so than ever with the difficulties in operating in the unusual environment during Covid-19. You, your clients and the regulator are largely interested in the

same aspects, namely business resilience, meeting financial resource requirements, minimising operational risks, avoiding fraud and other financial crimes. These are aspects that are very difficult to manage through the use of spreadsheets or other similar tools.

This is where technology can play an important part and finally bridge the gap between risk management and compliance management. Governance, Risk and Compliance (“GRC”) platforms (commonly known as Integrated Risk Management / Enterprise-wide Risks Management systems) should be the answer, but often have some significant shortcomings.

They are not normally specific enough regarding the regulatory environment within which businesses operate, can become very difficult to manage and therefore costly. They often fail to provide useful feedback to assist in the identification of issues that could lead to identifying whether risks are not as expected by the business.

Historically GRC systems have been useful to assist in the creation of risk registers and determining whether the associated controls are effective along with giving some key risk indicators to give as “early warning” of possible changing risks. Assuming that someone has populated the system with the relevant Laws, Rules and Regulations then this will be also be helpful in determining areas of compliance. Even if the GRC system is effective in these areas, more often than not the risk management element of the system is not linked with the compliance management element limiting the system capability and providing the business with only limited valuable information. As a result, most compliance monitoring is responsive to issues rather than looking forward to proactively identify potential risks and issues.

Development in these systems has been needed to make them useful for businesses and to overcome many of their problems. In this regard, Aspida is leading on the development



to provide a practical solution for all businesses.

One key aspect is linking typical processes, controls with the compliance frameworks to provide immediate benefits to the organisation. Any risk assessment can directly influence the compliance-monitoring programme. Any controls that are identified as deficient where there is a high inherent risk which would typically leave a high residual risk should be areas of immediate focus, however controls that are working effectively and there is a lower inherent risk and therefore lower residual risk should be tested less frequently, or perhaps not at all. By linking the controls with the compliance framework immediately means that the system has helped the business identify the important areas to test under the compliance-monitoring programme.

Any compliance testing, or other data, such as incidents or complaints should be used to identify control deficiencies and provide immediate feedback to the business on the appropriateness of the assessments of the risks. GRC systems should be able to determine whether the residual risk assessment is appropriate and provide input to the business to determine whether controls and/or risks need to be adjusted accordingly. In this scenario, the testing is genuinely providing corroboration of the risks and controls for the business and allowing attention to be focused on key areas. GRC systems need to trigger re-testing of areas that failed first time, trigger testing from other data (such as incidents or complaints) and provide automatic notifications to ensure that regulatory reporting is undertaken as required.

The risks and the testing of a compliance-monitoring programme need to flex to take into account the changing environment. This linking of risk management and compliance management naturally enables this to happen. It is impossible to identify all risks and many people did not foresee the potential issues surrounding Covid-19. Aon's 2019 global risk management survey identified pandemics as 60th in the list of risks. The World Economic Forums 2020 Global Risks Report did not have infectious diseases in the top 10 most likely risks. No doubt this risk will be included in most businesses risk registers going forward, however it is often the ability to react swiftly to risks, identify the controls and compliance aspects that is important. GRC systems need to provide that immediate benefit.

If we stick with Covid-19, businesses have had to think about many relevant risks and have tested the resilience of their businesses. Initially it commenced with business continuity and how do we continue to operate during this time. A lot of businesses implemented work from home plans (whether they were part of their normal plans or not). This itself leads to further risks around information security, data protection, operational risks associated with errors, cyber or fraud. Then there is the importance of financial resilience and health and safety, the latter being especially important as the business starts to work under the new arrangements of social distancing. It is essential that businesses can evaluate each risk and determine the appropriateness of the controls, whilst continuing to meet legal and regulatory obligations. This is a challenge, but made all the easier by a well-designed and forward thinking GRC platform that links these aspects. By tracking certain Key Risk Indicators ("KRIs")

and getting early warning information then it is possible to avoid or mitigate breaches for operational incidents. Having a system that allows you to monitor those risks "live" through KRIs, which are linked directly to any relevant regulations, is hugely beneficial. During Covid-19, liquidity risk is a key risk with a potentially large impact to the business. The basic regulatory requirement (Financial Resources Requirement) may be to maintain a minimum of 25% of liquid assets of annual expenditure. Setting appropriate KRIs (monitoring the Financial Resources Requirement, debtors and cash collection), creating thresholds and tracking the trend on a regular basis would give an early warning to the business if the liquidity looks like it could become a problem. Monitoring this "live" in a GRC platform enables the business to plan, take action and if necessary forewarn the regulator, rather than wait for the actual breach.

It is also important for businesses to get some external factors to determine whether their level of risk and controls are in-line with peers or at least a level that they can understand why they are prepared to accept more or less risk or have looser or tighter controls. By combining anonymous data within a GRC, system it is possible to give key information to determine with the business is an outlier. Again this is helpful during Covid-19, but how often have businesses been told that they are an outlier compared to their peers by the regulator but have no information to determine that prior to an onsite visit by the regulator.

Where GRC platforms need develop further is providing appropriate feedback to the business to enable swift changes to their operating environment. By evaluating the data it may be possible to determine a competitive edge, for example where the business is able to demonstrate a better controls environment than their competitors allowing the take-on of different type of client.

Aspida have developed a GRC system that covers these aspects more effectively, and yet is also able to deliver another key element which is to reduce the cost of compliance.

Just maintaining a programme to meet the current rules and regulations and adjusting to relevant risks and controls environment is almost a full-time job for a compliance officer. Our system does that, but we are well aware of areas that we want to develop further. When we look to the future, it is about how we can incorporate machine learning in the risk assessment and testing. The system should be able to test certain areas if fed data and then do a peer comparison automatically. We should even get to the stage that the GRC platform is able to determine the risk assessment based on the external factors influencing the inherent risk and the internal factors determining the residual risk.

Exciting times, but a demonstration that a properly developed GRC platform can truly become an enabler for the whole business.

**Adriana Cassar is the Executive Director,
Aspida Malta**

