Templar Executives
Cyber Security Resilience For Business

The Power of Effective Information Governance

The value of an organisation is often assessed in terms of its assets – defined as 'an item, thing or entity that has potential or actual value to an organisation'[1]. According to the Institute of Asset Management, this involves "the balancing of costs, opportunities and risks against the desired performance of assets to achieve an organisation's objectives".

As well as physical and financial assets, information also has a value for any enterprise. This may be intellectual property, as well as corporate strategies and plans. There are also categories of information which are subject to legislation, such as personal data which is required to be protected under the UK General Data Protection Regulation (GDPR) and Data Protection Act of 2018.

In order to ensure that all information assets are properly protected, organisations must have an effective information governance structure in place. GDPR places a requirement on organisations to have a nominated Data Protection Officer (DPO), but this is a specific defined function relating to the management and handling of personal data. There are other measures that enterprises must also have in place in order to provide the Board and key stakeholders with adequate assurance that all information assets are properly protected – as well as being exploited to maximum effect.

The first step is to understand what information an organisation holds, for what purpose, and where that information is stored. Much of it will be in electronic format, but there will also be information in hard copy as well as other media such as video and voice.

Of course, not all information will be critical to a business or its objectives. The menu for the staff canteen is, technically speaking, an information asset but it is not of itself critical to a business achieving its objectives. Information Assets should therefore be considered in the context of Board priorities and potential business risk. They should also be logged on an Information Asset Register.

As companies become more susceptible to information disruption, particularly through Cyber incidents, so shareholders and the public are becoming more alert to Cyber and information risk. Consequently, an emerging role is that of the Senior Information Risk Owner (SIRO). This function has long been mandated in UK government bodies and is increasingly being taken up by businesses.

[1] ISO 55000, 2014 (3.2.1)

©2024 Templar Executives. All Rights Reserved.

The SIRO is a delegated board-level Executive or Senior Manager on the Board who is responsible for information risks and the organisation's response to risk. The role of the SIRO is to take ownership of the organisation's information risk policy and act as an advocate for information risk on the Board.

Significantly, there is a growing recognition that information and Cyber security is not just the province of the IT team but that it is a fundamental business issue. For this reason, the SIRO may as readily be the CFO or the COO as a technical or IT lead.

In terms of governance and implementation, the SIRO is supported by Information Asset Owners (IAOs). Each information asset, or category of assets, should have a designated owner relevant to the information concerned. For example, the IAO for staff and HR records would be Head of HR; the corporate contracts register would have the Head of Procurement as IAO. Individual projects within an organisation may have IAOs nominated so that the information in their charge is properly understood and managed. Nominees should be logged on the Information Asset Register against their asset, and be given IAO training so they know what they have to do.

The value of this approach is **threefold**.

- First, it provides a clear chain of accountabilities for managing and monitoring information risk. Each IAO understands the information in their own area, who should get to see it – and who should not. IAOs also provide a means for implementing the relevant controls, in accordance with the Information Risk Appetite established by the Board.
- Secondly, as well as cascading effective information behaviours down and across an organisation, the IAOs provide a structure for reporting any emerging risks upwards, so that the SIRO has a real time view and, where necessary, can alert the Board.
- Thirdly, effective information governance provides a means by which controlled changes can be made, particularly should it be necessary to step outside the established Information Risk Appetite. For example, an organisation may wish to engage in a new partnership or venture which means that information may need to be shared more broadly than was previously felt appropriate. Transparency over these changes not only enables a greater degree of assurance, but also provides a level of traceability should an issue later arise.

Information governance is not just about protecting data but also ensuring the effective exploitation of that data, in a way that is properly assured. Any smart investor knows the importance of sweating other assets; the same is true of information. However, we are also entering a new realm of data vulnerability, not least as more and more organisations seek to take up the opportunities afforded by innovations such as Artificial Intelligence.

However, effective information governance of itself need not be complex. The simple steps described above should enable any organisation to protect – and to sweat - their information assets, safely and effectively, as part of wider asset management and risk reduction.

12th April 2024

©2024 Templar Executives. All Rights Reserved.