Scrut Automation

A CFO's Guide to Governance, Risk and Compliance

Scrut Automation

Contents

Introduction

The role of the CFO is constantly shifting and evolving. Today, they are being asked to do more than ever before.

The acronym GRC – Governance, Risk, and Compliance – was devised by the Open Compliance and Ethics Group, or OCEG. It refers to the salient areas of expertise that must be integrated at a C-suite level of businesses to ensure that they operate in a compliant and risk-averse manner.

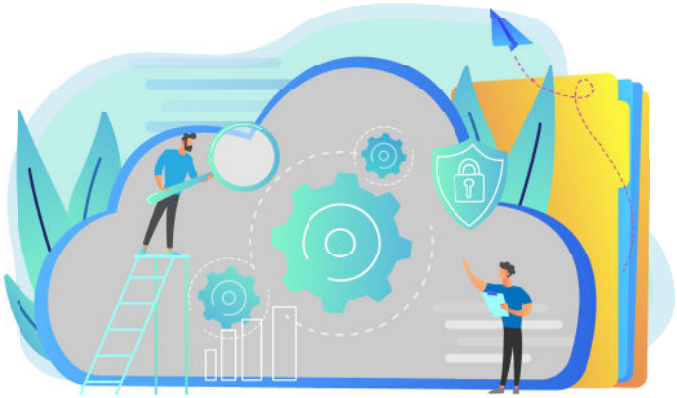
Businesses must have a clear understanding of their GRC obligations to ensure that they are taking the necessary steps to protect their stakeholders, employees, and clients. This knowledge includes fully comprehending the requirements of relevant laws and regulations and developing and implementing internal policies and procedures to mitigate risks.

There are several potential pitfalls for the role of the CFO in governance, risk, and compliance. One is that the CFO may be too focused on financial risks and not give enough attention to other risks, such as operational or compliance risks.

Another potential pitfall is that the CFO may not have enough knowledge or experience in risk management or compliance. Finally, the CFO may be unable to effectively communicate the risks and compliance requirements to the rest of the organization.

To avoid these pitfalls, a CFO must employ an effective GRC program. It can help companies save money, mitigate risk, and utilize resources wisely.

Role of the CFO in Governance



The Chief Financial Officer (CFO) occupies a unique position within an organization. They are responsible for the organization's financial health and have a strategic role to play in setting and achieving its goals.

The CFO is a crucial member of the senior management team and, as such, plays a vital role in shaping the organization's direction. They are often the voice of financial reasons within the organization.

They can objectively analyze opportunities and risks and offer advice grounded in economic data. This ability to provide sound financial advice is essential in helping the organization to make informed decisions and to achieve its goals.

CFO as a Strategic Partner

The role of the CFO has traditionally been focused on financial management and reporting. However, in recent years, the CFO has increasingly been viewed as an organization's strategic partner. They play a significant role in organizational strategy and decision-making.

They can provide valuable insights into an organization's financial health and performance. This information can inform strategic decisions about where to allocate resources and how to grow the business. Additionally, they can help to identify and manage financial risks.

Another way the CFO can be a strategic partner in an organization is by driving growth. They can help an organization achieve its growth potential by providing financial insight and advice, working closely with other senior management team members, and playing a pivotal role in developing and implementing the company's growth strategy.

To be an effective driver of growth, the CFO must deeply understand the organization's financial position and provide accurate and timely financial information. They must also be able to work in conjunction with other C-suite executives to develop and implement a growth strategy.

By taking on a strategic role within the organization, the CFO can help to create value and drive growth. In doing so, the CFO can position him or herself as a thought leader and driver of change.

CFO as a Change Agent

The CFO can be a powerful change agent within an organization. The chief financial officer is responsible for the company's financial health and has a broad view of the business. This responsibility gives them a unique perspective on where the company is headed and where improvements can be made.

1. They can use their influence to champion change within the organization. They can work with other department heads to identify areas where the company can be more efficient and profitable. In addition, they can use their financial expertise to help develop new strategies for growth.

By being a change agent in the organization, the CFO can help make positive modifications that will benefit the company in the long run.

The CFO can also play a key role in helping to manage risk and ensure compliance with financial regulations. By working closely with the CEO and other senior managers, the CFO can help to ensure that the organization is on track to achieve its long-term goals.

2.

By being a change agent in the organization, the CFO can help make positive modifications that will benefit the company in the long run.

3.

The CFO can also play a key role in helping to manage risk and ensure compliance with financial regulations. By working closely with the CEO and other senior managers, the CFO can help to ensure that the organization is on track to achieve its long-term goals.

CFO and Cyber Risk Management

Risk appetite is the amount of risk that an organization is willing to take on in pursuit of its objectives.

Risk tolerance is the amount of risk an organization is willing to tolerate in its current state.

A recent study by PwC found that nearly 78% of CFOs say their businesses are "revising or enhancing their ability to manage cyber risk."

The increase in concern is likely due to the increasing frequency and sophistication of cyber attacks. CFOs are responsible for the financial health of their organizations, so it is not surprising that they are worried about the potential for a cyber attack to disrupt operations and cause economic losses.

Given that cyber risk management is now a critical function of the CFO and one that is constantly shifting as technology progresses, the CFO must have a deep understanding of the organization's cyber risks and be able to develop strategies to mitigate them.

Risk appetite and risk tolerance are two important concepts to understand when determining how best to reduce risk.

CFO and Cyber Risk Appetite

A company's cyber risk appetite is the amount of risk it is willing to take on to achieve its business goals. The CFO and cyber risk appetite are connected because the CFO is the one who ultimately decides how much of the company's money and resources will be dedicated to cybersecurity.

An organization's goals and objectives often determine its risk appetite. For example, a company trying to expand may be willing to take on more risks to achieve its goals. Regulatory requirements often drive cyber risk appetite, but CFOs need to be able to strike the right balance between compliance and risk.

CFOs must carefully consider their company's cyber risk appetite when investing in cybersecurity. If a CFO is too reckless, they could risk the company's financial health. On the other hand, if a CFO is too

conservative, they could miss out on opportunities to grow the business. They also need to ensure that the company is taking on an appropriate amount of risk and have the resources to manage it effectively.

CFOs must assess cyber threats to make informed decisions about acceptable risk levels. They also need to be able to communicate these decisions to other members of the organization, such as the Board of Directors and other stakeholders.

When it comes to cyber risk appetite, there is no one-size-fits-all approach. The right level of risk appetite will vary from organization to organization. The CFO needs to understand the company's cyber risks and how they can be managed.

Cyber threats can lead to financial losses and damage a company's reputation, but they can also lead to new opportunities and growth.

CFO and Cyber Risk Tolerance

As the internet of things continues to grow, so does the risk of cyberattacks. A recent study by IBM found that the global average cost of cyber attacks for the companies included in their study was $4.35 million, the highest number they've recorded.

With these numbers in mind, it's no surprise that many organizations are looking to their CFOs to help weigh the risks and benefits of investing in cybersecurity. If a CFO is not well-versed in the nuances of cybersecurity, they may not be able to make an informed decision.

CFOs need to be aware of their company's cyber risk tolerance to manage it effectively. Cyber risk tolerance is the level of risk a company is willing to accept to achieve its business goals. CFOs must understand their company's cyber risk tolerance because it will help them decide where to allocate resources and respond to incidents.

There are a few factors that CFOs should consider when determining their company's cyber risk tolerance:

A cyber risk-tolerant CFO can take on more cyber threats and manage them effectively, which can help improve the organization's overall security. Cyber risk tolerance also allows CFOs to understand and manage the financial impact of cyber risks.

CFO and Compliance

The CFO's role in compliance is to ensure that the company is adhering to all applicable laws and regulations. They are responsible for developing and implementing policies and procedures to ensure compliance with these laws and regulations.

The CFO also works with the CEO and other members of senior management to ensure that the company is taking all necessary steps to comply with applicable laws and regulations.

In addition, the CFO is responsible for ensuring that the organization has adequate internal controls to prevent and detect law violations. These controls include steps to ensure data privacy and incorporate third-party risk management.

CFO and Data Privacy

The CFO has a vital role to play in data privacy and security. They are responsible for safeguarding the organization's financial information and data, including its customer data. They must ensure that the organization's data privacy practices are up to date and compliant with all data privacy laws in locations where the company does business, both locally, nationally, and internationally.

There is a patchwork of data privacy laws around the world. In Europe, the General Data Protection Regulation (GDPR) sets a high standard for protecting personal data. The GDPR applies to any company that processes the data of individuals in the European Union, regardless of where the company is located.

Other international data privacy laws include the Singapore Personal Data Protection Act (PDPA) and the Australian Privacy Principles (APPs), among many others.

DID YOU KNOW ?

According to the United Nations Conference on Trade and Development, 70% of the world's countries, 134 out of 197, have enacted data privacy laws.

In the United States, there is no all-encompassing federal data privacy law. Still, several laws provide data privacy protections, including the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, and the Health Insurance Portability and Accountability Act.

Various states in the US have personal data privacy laws, such as the California Consumer Privacy Act (CCPA).

Each of these laws has different requirements and obligations, but they all have a shared goal of protecting individuals' personal data. Businesses need to be aware of these laws and ensure that they are compliant when handling the personal data of individuals from these jurisdictions. Failing to comply with these laws can result in significant penalties, including fines, damages, and even criminal charges.

The CFO should work closely with the company's IT department to ensure adequate security measures are in place to protect its data. The CFO should also know the company's compliance with data privacy and security laws and regulations.

Data privacy and security are more critical in today's digital world. Customers trust businesses with their personal information, and the company must ensure that this trust is not misplaced. The CFO has a vital role to play in maintaining this trust.

CFO and Third-Party Risk Management

The CFO's role in Third-Party Risk Management has come under increased scrutiny in recent years. As organizations have become more reliant on third-party providers, the potential for financial losses due to fraud, errors, or other malicious or negligent acts has risen.

The CFO ensures the organization has adequate controls to protect against these risks. This responsibility includes assessing the risks posed by specific third-party providers and developing mitigation strategies. The CFO must also ensure that these strategies are adequately documented and communicated to key stakeholders.

A comprehensive plan for third-party risk management for CFOs should include discussing the main elements of an effective risk management program and the CFO's role in overseeing the program.

There are three primary elements of defence against third-party risk: due diligence, ongoing monitoring, and termination.

Defence Against Third-Party Risk:

Due Diligence

Reviewing the partner's financial statements, business licenses, references, and data security policies

Ongoing Monitoring

Periodic checks with vendor on adherence to contract and establishing KPIs

Termination

Ending business relationship in case of non adherence of standards

Due Diligence is the process of investigating a potential vendor before entering into a business relationship. This investigation can include reviewing the partner's financial statements, business licenses, references, and data security policies.

The CFO should consider the following factors:

- The nature of the relationship: What is the scope of the work being outsourced? What is the level of interaction between your organization and the third party?
- The third party's track record: Does the third party have a history of successful projects? Are there any red flags in their past performance?
- The third party's financial stability: Can the third party sustain its operations over the long term?
- The third party's compliance with laws and regulations: Have they ever been out of compliance, and if so, why? Have they ever been the victim of a cyber-attack or data breach?

Ongoing Monitoring is the process of periodically checking in with the vendor to ensure that they are still meeting the standards agreed upon in the original contract and establishing KPIs that will give the CFOs a benchmark for evaluating their compliance.

Termination is the process of ending the business relationship if the vendor is no longer meeting the standards agreed upon or if the business relationship is no longer beneficial to the company.

CFOs need to have a clear understanding of third-party risk management. They need to be able to identify and assess risks and put in place controls to mitigate them.

Furthermore, CFOs need to continually monitor these controls' effectiveness, ensure that they are updated in line with changes in the business environment and terminate any excessively problematic relationships.

Conclusion

The **CFO's role in governance, risk, and compliance** is crucial to the success of any organization. By understanding the risks involved and implementing adequate controls, the CFO can ensure that the organization complies with relevant regulations.

CFOs must have the most accurate information available to make the best possible decisions for their company. They need to be able to access that information quickly and easily.

One such tool is Scrut Risk Management. It can provide CFOs with the information they need to make informed decisions about risk management and allow them to identify risks early and take steps to mitigate them.

Scrut uses an analytics-driven approach to assess and monitor a company's risks. It is specifically designed for small and mid-market businesses that might not have the resources of a larger enterprise.

A combination of data analytics, real-time risk monitoring (including key risk indicators), and regulatory insight provides information about an organization's risk profile. This information helps customers to identify their organizations' most pressing risks and enables them to respond quickly to emerging exposures.

A growing company must balance the need to make quick, well-informed decisions with ensuring they have an accurate and up-to-date view of the risk and regulatory environment. Having timely, accurate, and forecasted insight into regulatory changes, as well as a better view of the overall risk environment, helps them anticipate and respond to changes in the regulatory environment in a timely and effective manner. With that information at their fingertips, the CFO can protect the organization from potential losses and help it to achieve its goals.

Contact us today to learn more about how **Scrut Risk Management** can give the data and tools they need to master governance, risk, and compliance for their company.