International Journal of Computer Techniques – Volume 10 Issue 2, 2024

Title – Contribution of Risk management teams helping firms with compliance and market access to their products.

Name: Pranith Shetty
Job role: Information Security and Risk Lead
Company: Cisco
Location: New Jersey

Abstract

Every business aims to be profitable through sales of its products and or services, this is possible through entering new markets, selling to new customers, and increasing their sales across their existing customer base continuously. One of the ways, to achieve this business goal is by attesting to industry standards and frameworks, showing evidence of their operating control environment to prove that firms are not susceptible to existing threats and have reasonable future-proof controls against new, evolving threats. This can be achieved through compliance certifications like SOC2, and ISO that have a very detailed set of control statements around security domains like Access Management, Physical Security, Encryption, Data retention, Privacy, Logging and monitoring, and many more. Firms need to attest to each of these controls with evidence to show that they have what it takes to achieve this certification, this enables trust and faith across the existing and new customers. Compliance is also a key pillar in terms of conforming to all possible regulations that apply to the product and service lineup. Risk management serves a more strategic approach of staying risk averse, ensuring risks are within the risk appetite, and constantly communicating to leadership and senior management so that decisions can be taken, and resources and budget can be smartly allocated.
Combining both these pillars of Risk management and compliance helps the firm scale new heights, in terms of market access. For example: Firms following a risk-based approach, successfully certify against industry frameworks as compared to their peers, this paper aims to provide context on both pillars and helps provide an understanding of how Risk and Compliance can tag team together to solve problem statements in favor of market access.

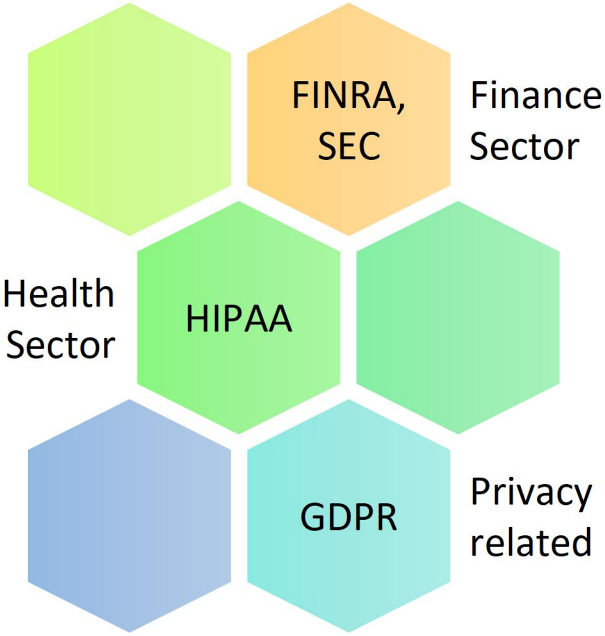
***Keywords** – Risk management, Compliance, Certifications, Market Access, Sales, Risk*

1. Introduction

[1] There are many misconceptions about risk and compliance, often these concepts are used interchangeably by executives and sometimes they are even assumed as the same thing. We might have seen all these functions grouped up together and called GRC (Governance, Risk, and Compliance) in many firms. Businesses believe that achieving compliance would position them better in terms of risk management, and there are a few firms that would think having a better risk management function would get you compliant. It’s important to understand both are important and necessary functions to get you into markets, enable sales, and in turn generate revenue, book profits, etc. There is an overlap between these functions, and when they both work together seamlessly that is how we end up with a mature control operating environment. This would help the firms be more proactive than reactive to information security threats. Risk management is a subjective approach looking more into critical processes, technology, assets, etc. from a strategic lens while Compliance is more an objective and tactical approach targeted to achieve short-term goals of certifications or regulatory compliance, etc.

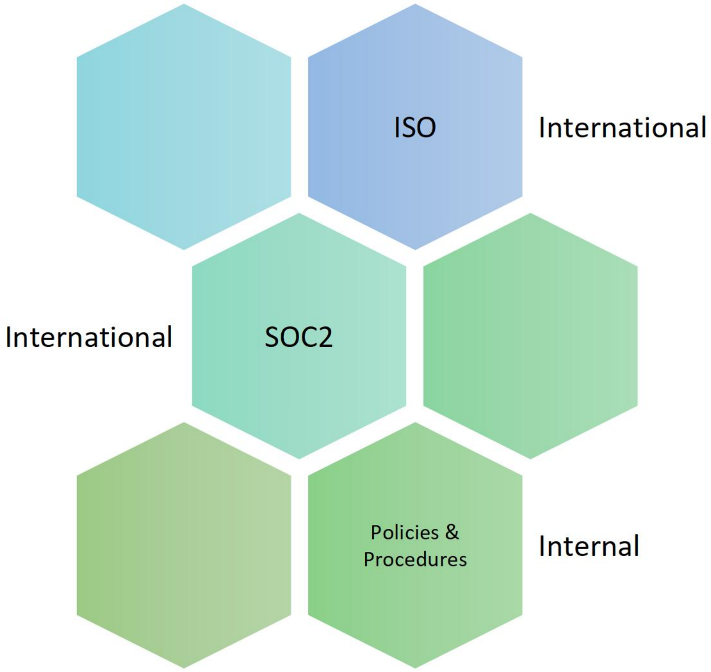
2. Compliance vs Risk management

Compliance:
By definition, it means being compliant or adhering to a set of standards, framework, or regulations for a variety of reasons, either it’s to comply with local, state, federal, or national regulations, Or it could be an international standard or framework that helps with the commercial sales of products/services.
[1] Compliance can be categorized into two buckets namely Regulatory compliance and Commercial compliance.
Regulatory compliance refers to products that are compliant with regulatory frameworks like FedRamp [2], and laws such as GDPR [3], and if in the financial services segment, they would have to conform to procedures laid out by regulatory bodies such as FINRA [4], SEC [5]. Organizations in the health sector especially hospitals must conform to HIPAA [6] to ensure patient data are handled with utmost due diligence in terms of security controls. Compliance with these regulatory bodies and regulations is not optional but mandatory. These must be adhered to, by businesses, non-compliance might result in sanctions on operations, monetary fines, etc. These frameworks or procedures are kept with public interest in mind and aim to ensure equality & justice to all the citizens, and residents within the scope of this regulation. These laws ensure businesses don’t lose sight of their ethics and moral values in the light of competition and profits.
Fig 1: Regulations



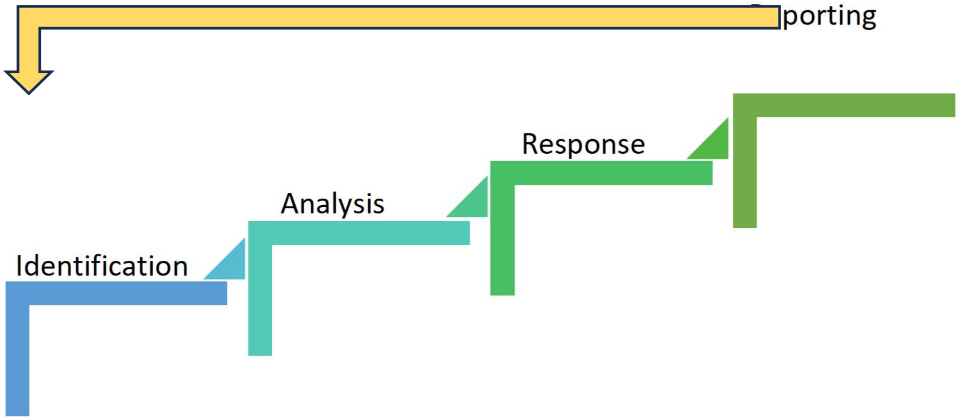
Commercial compliance - means firstly adhering to internal policies and procedures, in addition to the external ones, it also extends to complying with 3rd party, industry frameworks like SOC2 [7], ISO [8], etc. If a product company complies with these frameworks, customers can rely on these certifications and have faith in these products. These certifications help contribute to the sales of products and services. The industry-wide certifications have a comprehensive set of controls that need evidence to comply, thus customers. Compliance with internal policies and procedures, helps businesses to have a matured security posture and stay clear of threats and attacks to a certain extent.

Fig 2: Commercial standards / frameworks



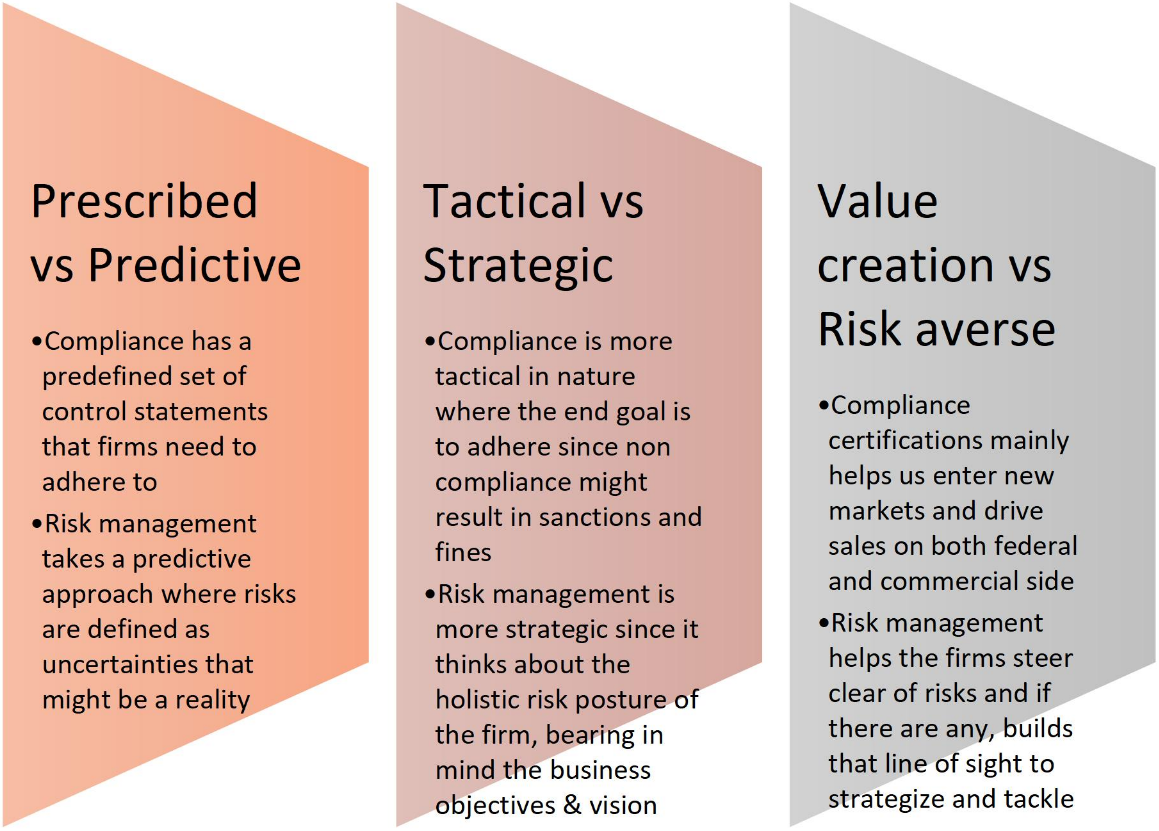
Risk Management:
As per NIST, [9] The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system.
The risk management framework consists of four basic steps, assuming the risk teams are familiar with the organization's context around Risk appetite [10] and Risk tolerance [11].
Risk identification step where risks are identified through various sources.
The analysis mainly qualitative and quantitative would help analyze and score the risks in terms of rating (Critical, High, and Medium).
Risk response is the step where accountable executives will determine the next step meaning if the risk needs to be mitigated and to what extent (usually within the risk appetite).
Risk reporting is a continuous monitoring step where risks are monitored and tracked for statuses by the risk teams and management is kept up to date through reporting.
This mechanism is iterative and sort of cyclic whereas we can see from the below visual Reporting feeds into identification meaning through residual risk posture or check-ins with teams, there is a possibility of identifying risks as one of the sources, which then kickstarts the whole lifecycle again.

Fig 3: Risk Management Framework



Compliance and Risk Management:
The following visual [1] helps understand some of the basic differences between Compliance and Risk management, both are important functions in the business and are essential, they complement each other well. The next section will help understand in detail, how firms can achieve synchrony between these two functions to act as holistic enablers.

Fig 4: Compliance vs Risk management standpoint



Prescribed vs Predictive

- Compliance has a predefined set of control statements that firms need to adhere to
- Risk management takes a predictive approach where risks are defined as uncertainties that might be a reality

Tactical vs Strategic

- Compliance is more tactical in nature where the end goal is to adhere since non compliance might result in sanctions and fines
- Risk management is more strategic since it thinks about the holistic risk posture of the firm, bearing in mind the business objectives & vision

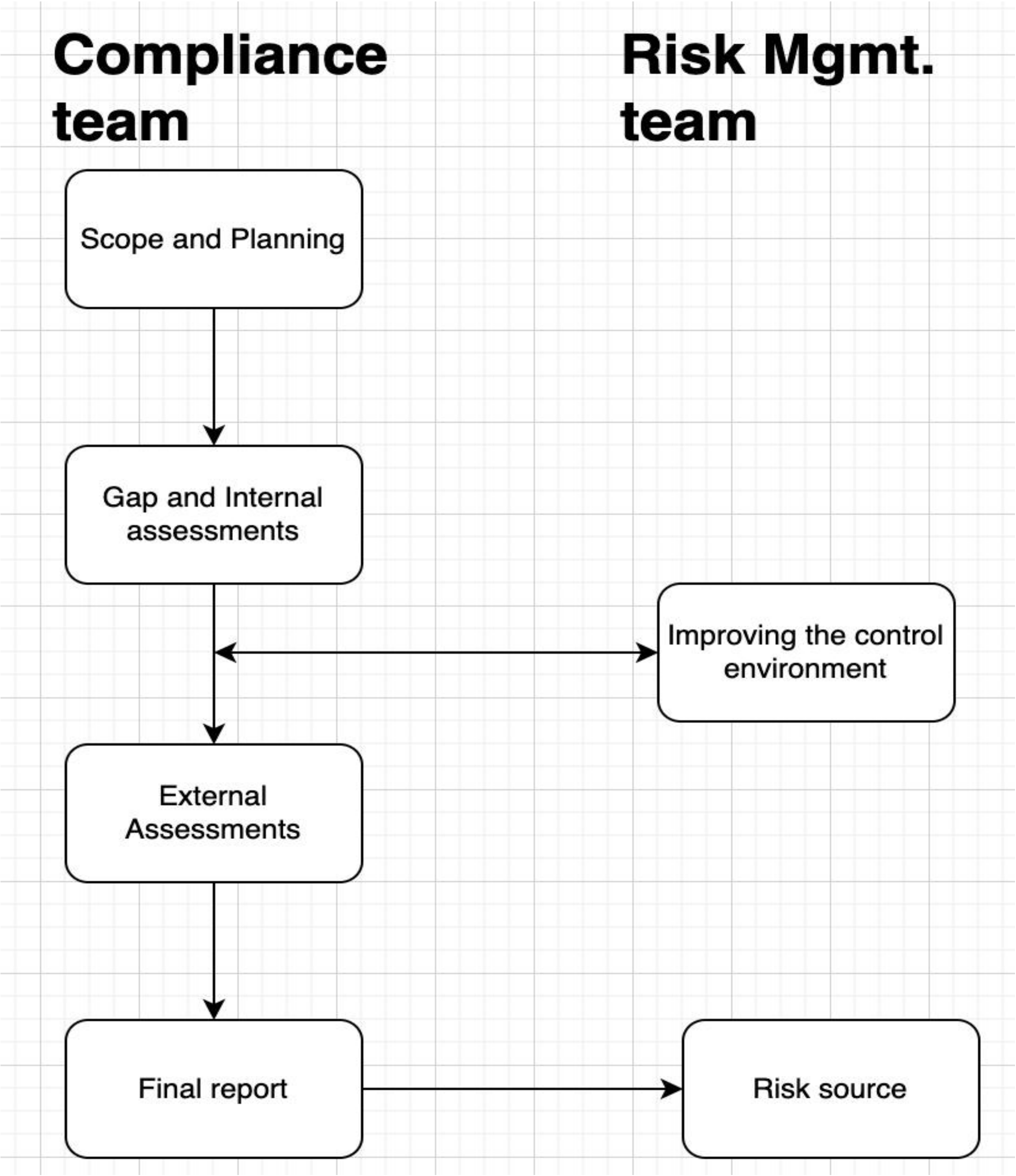
Value creation vs Risk averse

- Compliance certifications mainly helps us enter new markets and drive sales on both federal and commercial side
- Risk management helps the firms steer clear of risks and if there are any, builds that line of sight to strategize and tackle

3. Method, Results, and Discussion

Compliance teams assess the current state environment based on the industry frameworks if it's a commercial compliance-related assessment, similarly for regulatory-related, the assessment teams would measure the current state against the applicable or targeted regulations.
Quick overview - Risk management teams can pitch in and help the compliance teams in between the Internal assessments (meaning conducted by internal teams) and external assessments; performed by 3rd party independent auditors as recommended, Risk teams can work with product and accountable teams to improve the operating environment in terms of controls and try to remediate the gaps, thus helping the stakeholder teams help achieve the certifications. This would get the firm SOC2 or ISO or any other Certification, playing a part in market access and sales.

Fig 5: Compliance and Risk team partnership



Detail – Before any certification or regulatory audit is conducted by the independent auditor teams, Internal compliance teams "scope and plan" the entire engagement with the help of senior management and stakeholder teams, Compliance teams usually scope out the stakeholder teams. Once scoping is completed, teams are sampled for assessments, and a series of interviews are conducted by the internal teams to assess the current state and compare it against the control statements defined by the frameworks or regulations. This exercise gives everyone an idea on the preparedness of the organization. The control statements are spread across security domains like Access Management, Logging and monitoring, encryption, privacy, etc. These assessments are usually called "Gap and Internal assessments".

Once the assessments are completed and gaps are identified, accountable teams are asked to work on treatment plans to mitigate the risks identified and bring them within the risk appetite, preferably before the External assessments. Risk management teams can be an enabler in this phase before the external assessments, can work with accountable teams, and advise them on the best way forward strategically and not tactically. This approach can benefit the firm in the long run and not just the assessment. Risk practitioners being subject matter experts with connections to various security teams can guide the teams on what the holistic risk posture is and should be.

External assessment is performed by independent auditors to ensure no bias and some regulations and processes mandate this approach. Reports with possible findings and/or recommendations are submitted to the organization.

The risk management team again should use this report as an identification source, and document these in the risk register, this would help in future assessments and projects involving the accountable teams. Risk teams can keep it as part of the security agenda for the teams involved ensuring these are not forgotten. Please see Fig 3 for the framework and Fig 5 for details.

RACIs between Compliance, Risk, and Accountable teams mainly engineering, and product are always a good idea, because this approach delineates the responsibilities involved, and helps in the plan of actions and milestones. The various action items are clear to everyone involved including staff and leadership.

4. Conclusion

Compliance and Risk teams can be viewed as two sides of the same coin, both teams aim at improving the risk posture of the firm. The approach taken by both sides vary slightly, where compliance takes a more tactical approach with control statements and checklist as key, while Risk management takes a more subjective and strategic approach trying to understand the critical assets and processes and then working with relevant stakeholders on mitigating the risks, improving the risk posture etc. Both these functions should be viewed as enablers by the firm leadership, Senior management should ensure staff and leaders managing these teams work seamlessly and not in contention against each other. As we have seen in the earlier sections, Risk teams can "give" their time and effort in helping the compliance and product teams before the external certifications or assessments, similarly, Risk teams can "intake" the findings from the assessments, as part of their continuous monitoring function and bring into the fold via the Risk register. This partnership will eventually help the firms firstly in strategically maturing the risk posture and secondly, it will help firms tactically obtain compliance with regulations and industry frameworks enabling more market access, thus driving sales.

5. References

[1] Learning Center, "Compliance vs Risk Management: What You Need to Know," *SecurityScorecard*. Aug, 2021. [Online]. Available: https://securityscorecard.com/blog/compliance-vs-risk-management/

[2] "How to Become FedRAMP Authorized | FedRAMP.gov," *www.fedramp.gov*. [Online]. Available: https://www.fedramp.gov

[3] GDPR.EU, "General Data Protection Regulation (GDPR) Compliance Guidelines," *GDPR.eu*, 2023. [Online]. Available: https://gdpr.eu

[4] "Cybersecurity Checklist | FINRA.org," *www.finra.org*. [Online]. Available: https://www.finra.org/compliance-tools/cybersecurity-checklist

[5] "SEC.gov | HOME," *Sec.gov*, Feb. 05, 2017. [Online]. Available: https://www.sec.gov

[6] U.S. Department of Health & Human Services, "Health Information Privacy," *HHS.gov*, Jan. 04, 2019. [Online]. Available: https://www.hhs.gov/hipaa/index.html

[7] "SOC for Service Organizations: Information for Users and User Entities," *AICPA*. [Online]. Available: https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/users

[8] ISO, "ISO/IEC 27001 standard – information security management systems," *ISO*, Oct. 2022. [Online]. Available: https://www.iso.org/standard/27001

[9] NIST, "risk management - Glossary | CSRC," *csrc.nist.gov*. [Online]. Available: https://csrc.nist.gov/glossary/term/risk_management

[10] NIST, "Risk Appetite - Glossary | CSRC," *csrc.nist.gov*. [Online]. Available: https://csrc.nist.gov/glossary/term/Risk_Appetite

[11] NIST, "risk tolerance - Glossary | CSRC," *csrc.nist.gov*. [Online]. Available: https://csrc.nist.gov/glossary/term/risk_tolerance