ISSN: 2754-6705

Journal of Mathematical & Computer Applications

SCIENTIFIC Research and Community

Review Article

Open Access

Risk First Mindset in "Security First vs Compliance First" Debate

Pranith Shetty

Information Security and Risk Lead, Cisco, New Jersey, US

ABSTRACT

The idea of Security first vs compliance first approach has been plaguing the Cybersecurity industry and others, for a while now, Subject matter experts on both sides of the aisle have been debating and trying to make their point heard across the other side, explaining why is it that a certain approach is better than the other!. All of these points are valid and backed with facts and use cases.

However, there is need for a unique problem solving perspective which brings together the positives from both approaches and quashes the negatives associated with each, striking a much needed balance between the two mindsets.

The seamless collaboration between various security teams, quarterbacked by the Risk management team will help the organizations in maturing towards a Risk First mindset as opposed to debating between Compliance first and / or Security First approach. This article here does a deep dive on both the Compliance and Security approaches, listing their positives and negatives, thus stepping into the Risk first approach brings clarity to the whole organization and enables everyone from staff to leadership on a singular vision of maturing the Risk posture.

***Corresponding author**

Pranith Shetty, Information Security and Risk Lead, Cisco, New Jersey, US.

Received: January 03, 2024; **Accepted:** January 15, 2024, **Published:** January 22, 2024

Keywords: Compliance First, Security First, Risk First Mindset, Risk Management, Striking a Balance in Security vs Compliance

Introduction

Organizations in technology, financial services or any other sector are structured in a way that have security teams specializing in different niche domains, we would see a team focused on Offensive Security testing, conducting assessments like penetration testing, architecture reviews, Threat modeling exercises etc., we would also see teams like the Risk management that work on collaborating with all lines of defense within the firm to report on the holistic risk posture of the organization, there would also be teams that work on developing security products to cater to the engineering teams and stakeholders within the business unit.

Rationale for this Study

In spite of having such a varied list of teams with diverse talents there would always be a question of Security first vs Compliance first approach, which of these two benchmarks are important. On one hand Compliance first approach is where we leverage industry standards like ISO 27001, NIST and go through an entire list of controls to measure our current state and then define our target state based on assessment and analysis, on the other hand Security first approach is where we constantly test our systems for threats and work on threat models to address confidentiality, integrity and availability of our systems operations. Risk first attitude is an answer to such confusion, this not only unites all the teams involved but also helps work towards a unified goal for the betterment of the org. The Security team then appears to be working a single unit towards remediation of all risks. Risk management teams play a crucial role of shepherding the entire portfolio of work

Literature Review

Cost of Compliance First Mindset

Volkswagen – In 2015, it was discovered that Volkswagen had installed a software to cheat emission tests, company's compliance first culture pressured employees to meet emission targets at the expense of ethical behavior [1].

Equifax – In 2017 suffered a similar misfortune, where a massive data breach was exposed, company's focus on meeting compliance goals rather than genuinely improving the risk and security posture was one of the driving factors [1].

In this article Karen explains why it's important to have a Risk first mindset as opposed to only compliance [2].

As per Bradley in this article, it's a balancing act between Security and Compliance, not necessarily one of them is better, and that's where the Risk first mindset can drive the strategy bringing in the positives from both approaches [3].

As per Simon, an experienced GRC executive in this post, Striking the balance between Compliance and Security should be the modern strategy that firms should [4].

Some articles do talk about Security first approach to Compliance, or Risk approach to Compliance meaning to consider both approaches but preference to one, this does not appear to strike

a balance rather to create rift or competition between firm's own teams working on each side [5,6].

Positives and Negatives of each Approach

Compliance First Approach

Compliance first mindset prioritizes compliance with laws, regulations and industry standards over other considerations in decision making and operations [1].

This approach relies on following the compliance framework, industry standards and regulations like NIST CSF (National Institute of Standards and Technology - Cybersecurity framework), ISO 27001(International Organization of Standards), PCI DSS (Payments Card Industry – Data Security Standard). There are many more but the below listed in the visual are some of the prominent ones that firms adopt and adhere to. Each of these frameworks have a set of control statements diving into areas like access management, encryption, logging and monitoring, need for annual risk assessments, PenTest and the list goes on. It's up to the organization to attest to a certain framework on certification depending on their market access needs and sales targets. Sometimes it might be due to requirements or requests placed by the customer.

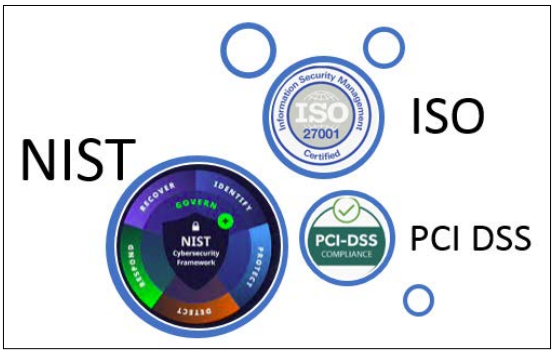

Figure 1: Various Industry Compliance Certifications and Frameworks

Every framework has a set of predefined process steps and controls, Firms follow those steps and provide evidence to the Third party assessors that they are compliant, this follows an annual review cycle [7]. To put things in perspective, NIST CSF for example relies on 5 steps namely as shown below;

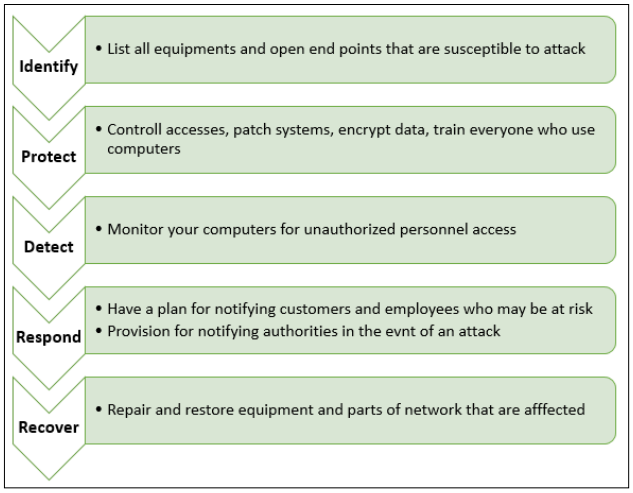

Figure 2: NIST CSF Five Areas

Positives

- Compliance is a mechanism through which you can communicate your security posture for others to understand [3].
- Policies and procedural coverage ensures teams are paying attention and being proactive towards the operating environment.
- Compliance helps with Market access of products, builds faith and trust amongst customers, ensuring competitive edge [4].
- Compliance ensures that firms are following independent industry benchmarks and are compliant to government regulations thus avoiding fines and reputational impact.

Negatives

- Compliance often eds up being a check the box exercise where organization fails to understand the true value [3].
- Stakeholders start thinking once complaint there is no need to be proactive in terms of security since they have fulfilled the obligations.
- Fear of noncompliance and fines forces accountable teams to sweep critical/high issues under the rug to avoid reputational damage [3].
- Compliance first mindset may lead to limited customer focus thereby sidetracking their needs in the urge to be compliance [1].

Security First Approach

Security first approach weaves security into every process, targets implementation of the basic tenets like for example CIA (Confidentiality, Integrity and Availability), Zero trust which means locking down access to data and profiling the systems trying to access on different parameters like time, posture, geographical location [8]. Offensive security techniques like penetration testing, security architecture reviews, threat modeling etc.

Let's deep dive on one of the techniques (Threat Modeling) mentioned above;

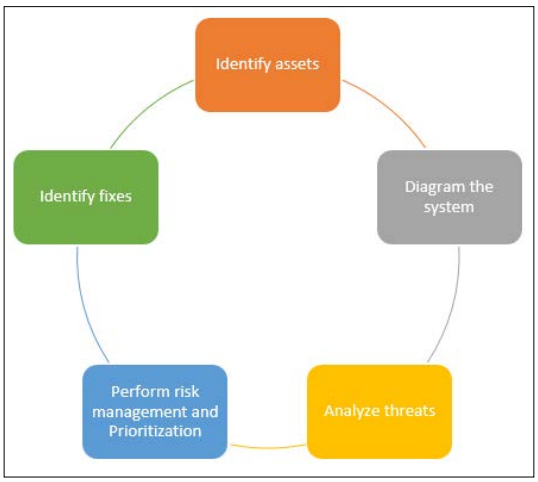

Figure 3: Threat Modeling [9].

- **Identify Assets**
  An asset could be account data, intellectual property, or simply the reliable functioning of a system.
- **Diagram the System**
  DFDs provide a high-level, asset-centric view of systems and the data flows of attacks. An attack tree, or graphic representation of an attack path, illustrates the possible origins and paths of attacks.

- **Analyze Threats**
  Use threat modeling methods to further analyze specific threat types, identify potential threats, map data flows, and quantify risk.
- **Perform Risk Management and Prioritization**
  Many threat modeling tools produce threat scores and data for calculating risk. Stakeholder input is essential to this step.
- **Identify Fixes**
  Once you identify the areas, assets, or threats that matter most to the organization, the next steps may be apparent. Changing firewall, encryption, or multi-factor authentication settings are examples of steps to address a threat.

Positives
- Using this method ensures proactive defense and prepared for threats [4].
- This is a cost efficient approach since internal staff and resources can be utilized and no need to hire external resources like compliance (3rd party independent attestation).
- Continuously evolving threat models ensures resources and systems are constantly evaluated and not just annually like the compliance review cycles.

Negatives
- It is difficult to explain the risk posture and security status to external customers since there is no 3rd party attestation or independent authority that is being used to evaluate.
- Market access is difficult for the same reason as above, thereby impacting sales and revenue.
- Compliance does ensure governance and communication from top to bottom and vice versa since there is a predefined framework in place.

Method
Risk first attitude or mindset relies on firstly defining the Organization context meaning leadership and senior management including top Security SMEs should come together to define some of the basic principles or terms like Risk Appetite - The types and amount of risk, on a broad level, [an organization] is willing to accept in its pursuit of value [10].

Risk Tolerance - The level of risk an entity is willing to assume in order to achieve a potential desired result, this is also defined as the amount of deviation from appetite that an organization is willing to accept [11]. All of these terms once solidified by leadership helps staff down the chain to understand the context set and work towards a better Risk posture of the firm.

The aim here is to get the risks through the Risk management life cycle that is from dentification, Analysis, response to Risk reporting. Risk managers are responsible to ensure a collaborative approach between various teams including Product Security, Compliance and Internal audit teams. This collaborative approach can be defined using RACIs between all the teams involved so that everyone is clear on what the expectation is, right from the beginning. Draw out the roles and responsibilities clearly at a granular level to avoid any confusion. Risk teams should also get themselves involved in the security related assessments as much as they can to get context on the shortcomings of a product, system or service. On the other hand, they should also be involved in the compliance related assessments that would give them context on the possible control gaps, ratings of those findings, remediation or acceptance measures.

As a result of the Risk team's involvement in all of these findings, they would be able to track, monitor these continuously, report on the risk profile to leadership and management ensuring communication and transparency

Discussion and Extended use Cases
By implementing this approach, no one team gets preference, Compliance teams need to be in positions to conduct those assessments to enable the products with market access certifications which would help with sales, involving the risk teams is the only additional criteria here.

At the same core security teams should be working with accountable stakeholders and build continuously evolving threat models, conduct offensive or Red hat security exercises to identify threats proactively, again the best approach here is to involve the risk teams so that they can track, monitor these risks towards completion or work with Senior leadership and management on Risk acceptances. The continuous monitoring program if implemented by the risk team would enable sending risk reports on a predefined cadence to the Senior Management this would help them understand the holistic risk posture of the firm.

The risk first mindset or approach can be implemented in all firms regardless of the sectors they are in, at present it is part of Technology Security teams setup, but this can easily be adopted across financial and manufacturing firms through governance forums and framework.

Conclusion
Compliance first mindset does have its pros and cons, its not a harmful mindset or approach at all, some firms have benefited from this mindset and still do, if avoiding fines, sales are the bottom line, whereas Security first mindset does have more pros than cons still this approach does run into problems with establishing trust with customers and getting into more markets since there is no independent attestation that has been performed [12].

Risk first attitude or mindset gets all the key players onto the table and helps the firm benefit with contributions from all teams. This helps organizations in the long run and not only secures the product without getting into a false sense of hope, at the same time ensuring there is no impact to market access and sales of the products [13,14].

References
1. Shailesh Rangari (2023) From Compliance-First to Risk-First: Why Companies Need a Culture Shift. InfoQ https://www.infoq.com/articles/risk-first-compliance/#:~:text=A%20compliance%2Dfirst%20mindset%20prioritizes.
2. Karen MacDougalln (2023) Avoiding a Compliance-First Mindset and Choosing a Risk-First Attitude. ISACA https://www.isaca.org/resources/isaca-journal/issues/2023/volume-5/avoiding-a-compliance-first-mindset-and-choosing-a-risk-first-attitude.
3. B Thies (2021) Security vs. Compliance: A Balancing Act. BARR Advisory https://www.barradvisory.com/blog/security-vs-compliance-a-balancing-act/.
4. Simon Turner (2023) Striking the Balance: Compliance-Centric vs. Security-First Strategies in Modern Organisations. www.linkedin.com https://www.linkedin.com/pulse/striking-balance-compliance-centric-vs-security-first-simon-turner/.
5. Jim Kennedy (2018) Taking cybersecurity beyond a compliance-first approach. CSO https://www.csoonline.com/

article/564643/taking-cybersecurity-beyond-a-compliance-first-approach.html.

6. H Team (2021) When Organizations Take a Risk-First Approach to IT Compliance, They're Better at Avoiding Security Incidents. Hyperproof https://hyperproof.io/resource/risk-first-approach-to-compliance/.
7. FTC (2018) Understanding the NIST cybersecurity framework. Federal Trade Commission https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework.
8. The Crucial Role of a Security-First Approach in Continuous Compliance. Scrut Automation https://www.scrut.io/ebooks/the-crucial-role-of-a-security-first-approach-in-continuous-compliance.
9. What Is Threat Modeling?. Cisco https://www.cisco.com/c/en/us/products/security/what-is-threat-modeling.html.
10. NIST (2023) Risk Appetite - Glossary | CSRC. csrc.nist.gov https://csrc.nist.gov/glossary/term/Risk_Appetite.
11. NIST (2023) Risk tolerance - Glossary | CSRC. csrc.nist.gov https://csrc.nist.gov/glossary/term/risk_tolerance.
12. R Haleliuk (2023) The importance of adopting a security-first mindset and why compliance is a bad substitute for security. ventureinsecurity.net https://ventureinsecurity.net/p/the-importance-of-adopting-a-security.
13. Leveraging a Security-First Approach to Compliance. www.techtarget.com https://www.techtarget.com/searchaws/evidentio/Leveraging-a-Security-First-Approach-to-Compliance.
14. Karen Walsh (2019) For Cyber Security, Use 'Security-First' to Approach Compliance | Zeguro Blog. zeguro.com https://zeguro.com/blog/for-cyber-security-use-security-first.