Avoiding a Compliance-First Mindset and Choosing a Risk-First Attitude

Compliance is a subset of risk. Failure to comply with standards or laws can involve legal or financial risk, yet it is difficult to identify emerging risk with a compliance-first mindset. For example, as one article notes:

> *When the unsinkable* Titanic *sank in 1912, it was fully compliant with all marine regulations. In fact, it exceeded the number of lifeboats mandated by the British Board of Trade at the time. But when catastrophe struck, the ship was not equipped with enough lifeboats to save all passengers on board. The problem? Management, too focused on meeting compliance, undermined real-world risks. Cybersecurity compliance too is a lot like that. There's a compliance document where every checkmark becomes as valuable as the next checkmark. Security teams develop a kind of checkmark mentality because the end goal is not to be secure but to be compliant.*[1]

Many compliance standards cannot keep pace with new risk scenarios, and many do not rank controls based on risk. In addition, compliance audits are generally based on one point in time, yes or no questions are often the norm, and guidelines may fail to address the purpose of controls.[2] Enterprises that may truly be compliant at the time of audit may lack resilient security controls and still be vulnerable to breach (e.g., Target, Equifax).[3] A compliance-first mindset focuses on implementing regulatory controls and enterprise rules leading to a belief in safety (e.g., the *Titanic*). It may also result in unnecessary expenditures and time spent checking off boxes to meet audit requirements.[4] On the other hand, taking a risk-first approach means an enterprise focuses on policies, processes and controls that protect it while also considering its culture and maturity (**figure 1**).

Toward a Risk-First Attitude

What does it mean to have a risk-first attitude? First, it is important to understand the tone from the top. Cybersecurity management is about reducing risk to an acceptable level. Therefore, a security program must have management buy-in and policies that support management's defined risk tolerance. In practice, the quantification of risk is not well understood because the technical definition of risk may not be management's definition of risk. The US National Institute of Standards and Technology (NIST) defines risk as "The level of the potential impact on an organization['s] operations (including mission, functions, image, or reputation)…assets, or individuals of a threat or a given likelihood of that threat occurring."[5]

Cybersecurity professionals should understand this definition, as it identifies impact categories for organizational operations and the likelihood of an adverse event happening. This can be used to begin the conversation with leaders about how cyberrisk affects the bottom line. Then the risk can be quantified using tools such as Factor Analysis of Information Risk (FAIR), which enables the quantification of risk in financial terms.[6]

Risk assessment is the first step in any risk-aware cybersecurity program. A mature enterprise should

FIGURE 1

A Compliance-First Mindset vs. a Risk-First Attitude

Compliance-First Mindset	Risk-First Attitude
Security controls are not ranked based on risk.	Security controls are ranked on specific risk.
Audits are a point in time.	Compliance standards are part of a continuous risk management program.
Audit controls generally serve to meet regulations (perceived safety).	The compliance program focuses on security controls functioning effectively (risk-aware protection).

KAREN MACDOUGALL | CRISC, CCSP, CEH, CISSP, PCIP, SECURITY+

Has an academic background in finance, computer science and information security. During her 25-year career, she has worked at start-ups, major corporations and in government. Her interests include applying risk concepts to cybersecurity programs and monitoring emerging threats.

also have a continuously monitored risk management program. Policies, procedures and processes should reflect the enterprise's risk appetite. Staff, contractors and third parties that are expected to adhere to administrative controls should also be trained to effectively implement the organization's policies, procedures and processes. The risk management program, in turn, should accommodate changes in risk, technology and emerging threats.

Continuous improvement is important to ensure that risk management strategies and processes address new and emerging threats.

Using Frameworks as Strategic Approaches to ERM

A framework provides a guide to follow when building something according to certain standards. Enterprises can choose from a multitude of risk management frameworks. As is applicable in making any organizational decision, factors influencing the choice of the framework include enterprise culture and the maturity of processes. Senior management buy-in influences the success of the implementation of any framework chosen. As such, the successful implementation of a risk-first attitude depends on the given framework's suitability and implementation in the enterprise.

One important development in the field of enterprise risk management (ERM) is the framework developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). It was first developed in 2004 when internal audit was still a main driver for risk management. It was later updated in 2017 to focus more on strategy and performance.[7]

The five main COSO ERM components are:[8]

1. Governance involves the tone from the top.
2. Strategies to develop a risk-aware culture include policies, procedures and training.
3. Performance involves the quantification of identified risk factors because one cannot manage what cannot be measured.
4. Review and revision are related to risk management monitoring and improvement.
5. Information communication and reporting include continuous monitoring and measurement.

An example of a culture that implements the COSO ERM well is the US Internal Revenue Service (IRS) outlining structure, roles, responsibilities and processes.[9] Its ERM program is considered one of the most mature in the US government because it focuses on addressing threats before they impact the agency,[10] employees have channels to report risk and employees can be certified as risk advocates.[11]

The NIST Internal Report (IR) 8286, *Integrating Cybersecurity and Enterprise Risk Management,* examines two vital but different controls that support ERM: internal controls such as COSO, and security controls. It outlines how lower-level risk reporting can be integrated into organizational processes and decision-making, and it defines an approach using a risk register, which forms the basis for a risk profile to highlight the major risk to be addressed, which then flows into the ERM cycle.[12] The benefits of combining cybersecurity risk with enterprise risk include:

- The board can exercise due care and avoid legal or financial penalties by addressing high-risk vulnerabilities.
- Senior management can achieve the organization's mission through a broadened ERM approach that reduces operational risk.
- Cybersecurity events' impact to financial statements and enterprise objectives can be understood.

LOOKING FOR MORE?

- Explore the *Risk Scenarios Tool Kit*. *www.isaca.org/risk-scenarios*
- Learn more about, discuss and collaborate on risk management in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

For ERM to work successfully, cybersecurity risk needs to be considered during the ERM process. In addition, continuous improvement is important to ensure that risk management strategies and processes address new and emerging threats.

To implement NIST (IR) 8286, a risk management framework is needed to determine risk response strategies, and a risk profile should be developed to inform and communicate leadership decisions.

Conclusion

Moving from a focus on compliance to developing a risk-first attitude results in improved security with a better understanding of and ability to mitigate potential threats; better decision-making by addressing likely cybersecurity threats; and senior management's support and investment in security controls that reduce risk.

Moving from a focus on compliance to developing a risk-first attitude results in improved security with a better understanding of and ability to mitigate potential threats.

Endnotes

1 Sjouwerman, S.; "Five Reasons Why Compliance Alone Is Not Efficient at Reducing Cyber Risks," *Corporate Compliance Insights*, 8 June 2022, *https://www.corporatecomplianceinsights.com/compliance-not-enough-cybersecurity-risk/*

2 *Ibid*.

3 Moldes, C.; "Compliant But Not Secure: Why PCI-Certified Companies Are Being Breached," *Cybersecurity and Information Systems Information Analysis Center*, 9 May 2018, *https://csiac.org/articles/compliant-but-not-secure-why-pci-certified-companies-are-being-breached/*

4 Hyperproof Team, "When Organizations Take a Risk-First Approach to IT Compliance, They're Better at Avoiding Security Incidents," *Hyperproof*, 24 March 2022, *https://hyperproof.io/resource/risk-first-approach-to-compliance/*

5 Ferraiolo, H.; R. Chandramouli; N. Ghadiali; J. Mohler; S. Shorter; National Institute of Standards and Technology (NIST) Special Publication (SP) 800-79-2 *Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)*, USA, 30 July 2015, *https://csrc.nist.gov/publications/detail/sp/800-79/2/final*

6 FAIR Institute, "What Is FAIR? From a Compliance-Based to a Risk-Based Approach to Cyber Risk Quantification and Operational Risk," *https://www.fairinstitute.org/what-is-fair*

7 Claypole, A.; "The COSO ERM Framework Explained," Ideagen, 3 May 2021, *https://www.ideagen.com/thought-leadership/blog/the-coso-erm-framework-explained*

8 *Ibid*.

9 Internal Revenue Service (IRS), "Part 1. Organization, Finance, and Management, Chapter 4. Resource Guide for Managers, Section 60," Enterprise Risk Management (ERM) Program, USA, 24 February 2021, *https://www.irs.gov/irm/part1/irm_01-004-060*

10 Dunkin, R.; "Seven Steps to Create a Risk-Aware Culture," *Treasury and Risk*, 21 September 2020, *https://www.treasuryandrisk.com/2020/09/21/7-steps-to-create-a-risk-aware-culture*

11 Ogrysko, N.; "IRS Launches Designated Channel for Employees to Raise Agency Risks," Federal News Network, 12 November 2019, *https://federalnewsnetwork.com/management/2019/11/irs-launches-designated-channel-for-employees-to-raise-agency-risks/*

12 Stine, K.; S. Quinn; G. Witte; R. Gardner; National Institute of Standards and Technology (NIST) Internal Report (IR) 8286 *Integrating Cybersecurity and Enterprise Risk Management*, USA, 13 October 2020, *https://csrc.nist.gov/publications/detail/nistir/8286/final*