Richard P. Kusserow

Understanding the Difference between Compliance and Risk Management

Richard P. Kusserow is the president and chief executive officer (CEO) of Strategic Management. He can be reached at 703/683-9600, ext. 411 or by email at rkusserow@strategicm.com.

In the Eleventh Annual 2020 *Healthcare Compliance Benchmark Survey Report*, four out of 10 respondents reported their compliance office had assumed responsibility for risk management. This should raise some concerns, as distinguishing risk management from compliance is often an area of confusion for many. Compliance is not the same thing as risk management, and care should be taken not to bundle them in a single function.

Without question, the two are closely related. Both are needed to protect their organization's security and integrity in many ways and need to support one another. It is important, however, to recognize their differences, as well as their similarities, in order to ensure they are coordinated to the benefit of the organization.

Risk management identifies, assesses, and analyzes risks and seeks ways to mitigate them whereas compliance focuses on meeting established rules, regulations, and standards to prevent their organization from regulatory and legal violations that could give rise to serious liabilities. Only when leadership teams and risk managers fully understand how compliance and risk management differ, and how to appropriately bring the two together, can it make a positive impact at their organization. To do that, it is important to examine the two functions and their capabilities.

Compliance[1]

Health care compliance can be defined as an ongoing process of meeting or exceeding the legal, ethical, and professional standards applicable to a health care organization or provider. A key phrase often used to describe compliance is that its mission is preventing, detecting, and correcting wrongdoing associated with failure to meet regulatory requirements or internal standards. This means there is a sound risk management role for compliance, as they should be involved in identifying and mitigating *regulatory risks* to the organization, where the cost of noncompliance can result in serious regulatory actions, including fines, penalties, and damage to reputation. Compliance with governance rules and regulations, however, rarely translates into evaluating the financial, operational, and clinical risks of new business propositions, partnerships, and lines of business.

Compliance usually stops with verification that a rule has been followed to avoid risks. A large part of that is verifying the laws, regulations, rules, standards, policies, and the code to ensure the organization is obeying them and avoiding the risk of noncompliance. Inasmuch as a failure in compliance can result in expensive fines and penalties, as well as damage to reputation, it is an area that cannot be ignored by risk management when new plans are being formulated. While compliance is more narrowly focused on regulatory risk, this specialization is essential for ensuring compliance is able to devote the time, attention, and resources necessary to advance the mission of the compliance program.

Risk Management[2]

Risk management is the process of identifying, assessing, and controlling threats to an organization's capital, earnings, and reputation. This refers to the practice of identifying potential risks in advance that could include financial uncertainty, legal liabilities, strategic management errors, accidents, clinical incidents, and natural disasters. By implementing a Risk Management Plan and considering the various potential risks or events before they occur, an organization can save money, improve operations, and protect their future. This is because a robust plan will help a company establish procedures to avoid potential threats, minimize their impact should they occur, and cope with the results.

This ability to understand and control risk gives organizations greater confidence about their business decisions. Furthermore, strong corporate governance principles that focus specifically on this can help a company reach its goals.[3] In health care, this is potentially more important than in any other industry in that strategies not only focus on preventing and mitigating financial losses but extend to matters related to patient safety. Risk management in this industry can mean the difference between life and death that makes the stakes significantly higher.

Another key point of difference is risk management focuses more on forecasting the impact risks will have on the organization. When it is reactive, it is usually the result of some event occurring and then looking to prevent future occurrence. It involves analyzing innovation processes, new ways of doing business, possible new relationships or lines of business, etc. This predictive approach involves focusing strategically in order to measure the cost of risks, and in some cases deciding on whether they are worth taking.

Looking ahead to new and innovative methods, means, and processes to minimize risks is in direct contrast to compliance, which focuses on following established rules in conducting business. Whereas compliance tends to be more narrowly focused on individual departments, risk management tends to focus on a larger picture involving and integrating multiple operations, technology systems, and processes to determine the risks to

the organization and how they should be handled. When new initiatives are being considered, it falls to a risk management team to collect, process, assess, and analyze information about the risks that may be involved (strategic, operational, regulatory, clinical, and ethical risks). This includes those areas where there may be an impact, such as legally, financially, business wise, and reputational. Of course, included in this mix are issues related to compliance. For hospitals and other institutional providers, risk management often deals with clinical issues and is involved with injuries, sentinel events, and potential malpractice issues, etc.

Conclusion

Compliance and risk management are different in mission and operation but are inter-related and can be complementary to one another. Whereas risk management involves identifying all areas of risks to the organization and taking steps to control, avoid, mitigate, or eliminate unacceptable risks, compliance focuses on identifying and mitigating regulatory risks. Compliance usually stops with verification that a rule has been followed to avoid risks, whereas risk management must be anticipatory, flexible, and proactive. It focuses on identifying risks as well as monitoring and managing changes.

To appreciate the difference in roles, all one has to consider is that risk management requires different competencies than those of compliance such as evaluation of (a) financial risks of a new line of business; (b) operational risks with an acquisition or merger, or establishing a new line of business; (c) IT risks for new systems and software; and (d) clinical risks of a new medical procedure, device, or process; etc. There is no question that there may be compliance issues associated with these ventures, but risk managers must be able to go far beyond focusing on compliance matters to evaluate all areas of these risks.

- Four out of 10 compliance officers report being responsible for risk management.
- Not recognizing the difference is a big mistake.
- Compliance is prescriptive in nature, and risk management is predictive.
- Compliance has an oversight role, but risk management is an operational one.

Endnotes

1. *Defining Healthcare Compliance*. compliance.com/blog/defining-healthcare-compliance.
2. Risk Management Handbook Volume I Chapter 10, *CMS Risk Management Terms, Definitions, and Acronyms. www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH_VI_10_Terms_Defs_Acronyms.pdf*.
3. searchcompliance.techtarget.com/definition/risk-management.

Reprinted from Journal of Health Care Compliance, Volume 22, Number 3, May–June 2020, pages 49–50, 68–69, with permission from CCH and Wolters Kluwer.
For permission to reprint, e-mail permissions@cch.com.