International Journal of Pharmacy and Analytical Research (IJPAR)
IJPAR |Vol.12 | Issue 4 | Oct - Dec -2023
www.ijpar.com
ISSN: 2320-2831
DOI : https://doi.org/10.61096/ijpar.v12.iss4.2023.584-590

Review

Standard Practices In Regulatory Compliance

Chinnam Apparao *, D. Venkata Ramana [1], P. Sai Mounika [1]

Department Of Regulatory Affairs, Holy Mary Institute Of Technology And Science (College Of Pharmacy), Keesara - Bogaram - Ghatkesar Rd, Kondapur, Telangana 501301

*Author for Correspondence: Chinnam Apparao
Email: apparao.chinnam@gmail.com

Published on: 30 Oct 2023

Published by:
DrSriram Publications

Abstract

Regulatory compliance is an organization's adherence to laws, regulations, guidelines and specifications relevant to its business. Violations of regulatory compliance regulations often result in legal punishment, including federal fines. The International Organization for Standardisation (ISO) produces international standards such as ISO/IEC_27002. The International Electrotechnical Commission (IEC) produces international standards in the electrotechnology area. Compliance is about more than prevention. It's also about navigating opportunities. Regulatory compliance is not just about playing defence. It also offers an opportunity to consistently strengthen your organisation through strategic, proactive measures—such as best practices, employee training, internal controls, and benchmarking appropriate for your industry and size.

Keywords: Regulatory Compliance , ISO, IEC, Industry

INTRODUCTION

Regulatory compliance is an organization's adherence to laws, regulations, guidelines and specifications relevant to its business. Violations of regulatory compliance regulations often result in legal punishment, including federal fines.[1]

Examples of regulatory compliance laws and regulations include the Dodd-Frank Act, Payment Card Industry Data Security Standard (PCI DSS) , Health Insurance Portability and Accountability Act (HIPAA), the Federal Information Security Management Act (FISMA) and the Sarbanes-Oxley Act (SOX).

As the number of rules has increased since the turn of the century, regulatory compliance has become more prominent in a variety of organizations. The trend has even led to the creation of corporate, chief and regulatory compliance officer positions to hire employees whose sole focus is to make sure the organization conforms to stringent, complex legal mandates.[1]

Regulatory compliance

In general, compliance means conforming to a rule, such as a specification, policy, standard or law. Regulatory compliance describes the goal that organisations aspire to achieve in their efforts to ensure that they

are aware of and take steps to comply with relevant laws and regulations. Due to the increasing number of regulations and need for operational transparency, organizations are increasingly adopting the use of consolidated and armonized sets of compliance controls. This approach is used to ensure that all necessary governance requirements can be met without the unnecessary duplication of effort and activity from resources.

Standards and regulations

The International Organization for Standardisation (ISO) produces international standards such as ISO/IEC_27002. The International Electrotechnical Commission (IEC) produces international standards in the electrotechnology area. The ISO 19600:2014 standard provides a reminder of how compliance and risk should operate together, as "colleagues" sharing a common framework with some nuances to account for their differences.[2]

Some local or international specialized organizations such as the American Society of Mechanical Engineers (ASME) also develop standards and regulation codes. They thereby provide a wide range of rules and directives to ensure compliance of the products to safety, security or design standards.[3]

There are a number of other regulations which apply in different fields, such as PCI-DSS, GLBA, FISMA, Joint Commission and HIPAA. In some cases other compliance frameworks (such as COBIT) or standards (NIST) inform on how to comply with the regulations.

Fig 1: Regulatory Compliance

USA

Corporate scandals and breakdowns such as the Enron case of reputational risk in 2001 have highlighted the need for stronger compliance and regulations for publicly listed companies. The most significant regulation in this context is the Sarbanes–Oxley Act developed by two U.S. congressmen, Senator Paul Sarbanes and Representative Michael Oxley in 2002 which defined significantly tighter personal responsibility of corporate top management for the accuracy of reported financial statements.

The Office of Foreign Assets Control (OFAC) is an agency of the United States Department of the Treasury under the auspices of the Under Secretary of the Treasury for Terrorism and Financial Intelligence. OFAC administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against targeted foreign states, organizations, and individuals.

Compliance in the USA generally means compliancy with laws and regulations. These laws can have criminal or civil penalties or can be regulations. The definition of what constitutes an effective compliance plan has been elusive. Most authors, however, continue to cite the guidance provided by the United States Sentencing Commission in Chapter 8 of the Federal Sentencing Guidelines.[4]

On October 12, 2006, the U.S. Small Business Administration re-launched Business.gov (new Business.USA.gov) which provides a single point of access to government services and information that help businesses comply with government regulations.

UK

There is considerable regulation in the UK, some of which is from EU legislation. Various areas are policed by different bodies, such as the FCA (Financial Conduct Authority), Environment Agency and Scottish Environment Protection Agency, Information Commissioner's Office, CQC and others. Important compliance issues for all organisations large and small include the Data Protection Act 1998 and, for the public sector, Freedom of Information Act 2000.

The UK Corporate Governance Code (formerly the Combined Code) is issued by the Financial Reporting Council (FRC) and sets out standards of good practice in relation to board leadership and effectiveness, remuneration, accountability and relations with shareholders. All companies with a Premium Listing of equity shares in the UK are required under the Listing Rules to report on how they have applied the Combined Code in their annual report and accounts (The Codes are therefore most similar to the US' Sarbanes-Oxley Act).

Australia

Standards Australia revised the standard titled "AS 3806 - Compliance Programs". While many aspects of the original standard produced in 1998 standard appear in the 2006 version there are additional principles covered. The regulators in Australia continue to endorse and encourage (by regulation) the use of the standard when establishing a compliance framework.

The regulators are the Australian Securities and Investment Commission, AUSTRAC (for AML), ATO (for FATCA and CRS) and the Australian Prudential Regulation Authority (APRA).

Compliance demands in the superannuation industry continue to increase due to the new licensing regime implemented by APRA. The new licensing regime requires trustees of superannuation funds to demonstrate to APRA that they have adequate resources (human, technology and financial), risk management systems and appropriate skills and expertise to manage the superannuation fund. The licensing regime has lifted the bar for superannuation trustees with a significant number of small to medium size superannuation funds exiting the Industry due to the increasing risk and compliance demands.

The 19600 standard on “Compliance Management Systems” reflects largely the existing AS 3806-2006 standard, which it will replace.[5]

Canada

See Keeping the Promise for a Strong Economy Act (Budget Measures), 2002, commonly known as C-SOX or "Bill 198".

Challenges

Data retention is a part of regulatory compliance that is proving to be a challenge in many instances. The security that comes from compliance with industry regulations can seem contrary to maintaining user privacy. Data retention laws and regulations ask data owners and other service providers to retain extensive records of user activity beyond the time necessary for normal business operations. These requirements have been called into question by privacy rights advocates.[6]

Compliance in this area is becoming very difficult. Laws like the CAN-SPAM Act and Fair Credit Reporting Act in the U.S. require that businesses give people the “right to be forgotten.” In other words, they must remove individuals from marketing lists if it is requested, tell them when and why they might share personal information with a third party, or at least ask permission before sharing that data. Now, with new laws coming out that demand longer data retention despite the individual’s desires, it can create some real difficulties.[7]

Although everyone in IT seems to be talking about compliance, few are actually doing much about it. At least part of the problem is that there's a lot of confusion about what the regulations require and what's necessary to be in compliance with them. We've gathered information about some of the most relevant legislation and the current status of industry compliance as well as some expert advice on the fine points.[8]

Legislative and Regulatory Requirements. All people and organisations are required to comply with relevant legislation to which they are subject. This includes prescribed laws, regulations and by-laws. Organisations need to determine their legislative obligations.

Compliance management

Compliance management is the process which ensures that a set of people are following a given set of rules. The rules are referred to as the compliance standard or compliance benchmark, while the process is what manages their compliance. Compliance management can take many forms. It can be a mix of policies, procedures, documentation, internal auditing, third party audits, security controls, and technological enforcement. There are two recognized models for implementing compliance management.

Model 1: The Ten Commandments

This model sets forth the rules and vigorously punishes those who do not comply with the rules. There is often minimal recourse for transgressions. This model is largely inflexible and suffers from significant breakdown when there is room for interpretation. It works well when there is little room for dissent regarding the compliance.

For example, if a manufacturing rule states that all ball bearings will be 1 inch in diameter, plus or minus 0.1% at 65 degrees Fahrenheit, the standard is clear. However it does not work well if, for example, the temperature were neglected, as metals may change size with the temperature.

Similarly, a requirement for a specific Windows service that must be disabled at all times would do well in this model, but not if the caveat existed which stated "unless it severely impacts a critical business process". What constitutes "severe" or a "critical business process" is ambiguous, at best.

Model 2: Quality Management

The Quality Management method allows for judgement calls to be made in many circumstances, even though the regulations may explicitly state that a rule is required to be followed. It is generally understood that not every rule can be followed in every instance and thus, exceptions must be made to allow the business to operate as best it can, while following as many of the rules as possible.

This model has been widely adopted and has been largely successful. This model is especially important because many companies which are required to follow a compliance standard often have multiple standards to follow, some of which may overlap or conflict with one another. When two standards oppose each other for the same company, who has the authority to say which one is to be followed?

This model allows for some flexibility on the part of the company implementing the standards to make those judgement calls without being harshly penalized for something which may not make sense for the company.[9]

Regulatory compliance & reporting

The flow of new rules and regulations across regional, national and international borders continues to intensify. No matter how large, small or diversified your organisation, almost every part of it is touched by a complex web of constantly evolving regulations—and subject to enforcement actions and fines. Not to mention reputational risk. It's no wonder that CEOs everywhere are more focussed on managing risk than ever before. Compliance is about more than prevention. It's also about navigating opportunities. Regulatory compliance is not just about playing defence. It also offers an opportunity to consistently strengthen your organisation through strategic, proactive measures—such as best practices, employee training, internal controls, and benchmarking appropriate for your industry and size.

Measures that can uncover value, even as they help assure compliance.

PwC's independent assurance specialists are ideally positioned to help. Whatever sectors or regions you operate in, and whatever your size or geographic reach, we offer both local, in-depth, on-the-ground knowledge, and global, state-of-the-art regulatory compliance tools.

We can help you assess your risk profile—and, though strategic benchmarking, your competitive position and business performance. And if you're contemplating entering a new market or industry, we can advise you on the very latest regulations that would affect your investment, allowing you to make the right strategic decision.

With the regulatory environment continually changing, compliance remains a moving target. PwC is here to help you stay on track, with a relentless focus on adding value through assuring compliance. We invite you to contact us to learn more about our full complement of audit and assurance services. Depending on the independence and regulatory requirements that may be applicable, such as Sarbanes-Oxley, certain services may not be available to audit clients of PwC member firms.[10]

MetricStream Regulatory Compliance Management Software Solution

MetricStream provides a common framework and an integrated approach to meet cross-industry regulations such as OSHA, EH&S, FCPA, and ISO standards. The MetricStream solution also enables compliance with industry focused regulatory guidelines from FDA, FERC, FAA, HACCP, OMB A-123, AML, Basel II, and Data Retention laws.

MetricStream Regulatory Compliance Solution supports compliance management through document control, compliance training, ongoing auditing, and recording and reporting of exception events and corrective actions.

Role-based dashboards, control diagrams, and scorecards provide visibility into ongoing compliance efforts, and bring high-risk areas into focus. The solution has the ability to track process ownership, assessment plans, remediation status, etc. on graphical charts with real-time information that can be accessed globally. Drill-down capabilities allow users to easily access deeper levels of information with a single click.

The MetricStream solution uniquely combines software and content to deliver solutions for effective and sustainable compliance. The solution provides embedded best practice templates and access to training content from an expert community, and enables integration of business processes with regulatory notifications.[11]

What is Regulatory Compliance and Why is It Important?

Regulatory compliance can take on different definitions according to the industry in which you are applying the policies. Since compliance means incorporating standards that conform to specific requirements, regulatory compliance is the regulations a company must follow to meet specific requirements.

When you apply regulatory compliance to IT, the regulations apply to two different aspects of company operations which include the internal requirements for IT and compliance standards that are set forth by external entities. Both types of regulatory compliance affect IT company operations and can potentially restrict what a company can and cannot do.

Company Concerns with Regulatory Compliance

When it comes to information technology and security, regulatory compliance for IT can impose added costs on company operations depending upon the industry. At the same token, the cost of not complying with regulations both internally and externally can be significantly higher in terms of fines and time invested following up on a security breach.

One of the primary issues with regulatory compliance is information security and the potential for data leaks. Although there may be policies in place, it is necessary to ensure that employees follow the policies as well as the entire staff within a company. This is an ongoing process and one that can lead to a high profile data breach if companies become too lax on policy enforcement. A primary example of this is the Sony breach earlier this year which can undermine a company reputation and end up costing more in fines than it would if you followed the compliance policies.

When it comes to regulatory compliance for IT on the external level, companies that follow the regulations set forth by external organizations are more likely to survive a potential investigation than companies that neglect regulatory compliance. Additionally, there are many benefits that come with following regulatory compliance policies which include protection of company reputation.

Issues Associated with Regulatory Compliance

In order to ensure that the proper steps are taken to meet regulatory compliance policies, it is first important to understand where the weaknesses in IT are so you know exactly what practices should be applied. If you skip this step and then try to meet regulations and policies, it is highly likely it will cost more over the long term since the practices were not implemented correctly.

The main issue that surrounds regulatory compliance is that many companies face multiple policies and regulations with regard to IT and data storage. This presents a challenge for most businesses, especially if the IT personnel changes frequently or over a number of years. Some compliance regulations require companies to archive data for a specified period of time. If IT staff changes over a period of time it is easy to lose sight of data storage and retrieval processes.

How to Make Regulatory Compliance Work

The number one priority for making regulatory compliance work is assessment and evaluation. If you do not know where the company weaknesses are in terms of IT then this makes it nearly impossible to put the best practices into action.

Once you know where the best practices should be applied there are many new tools that assist with simplifying the processes for regulatory compliance. These are automation tools that save time and perform the necessary requirements according to schedule. Tools for regulatory compliance are also capable of monitoring IT processes and providing reports to be used for analysis and future modifications.

The other alternative that ensures policies and procedures are carried out according to requirements is to consider using a virtualization solutions provider. A professional solutions provider such as Thrive Networks can help your company design strategies that guarantee your business will remain in compliance both within the company and with the external organizations that audit your processes.[12]

Compliance with laws, rules and regulations

Know and comply with all the laws, rules and regulations applicable to your job.

As a global company, we are subject to numerous laws, rules and regulations. While we do not expect you to be a legal expert, all of our employees are expected to understand and comply with laws, rules and regulations applicable to their jobs and know when to seek advice from your manager or the Prometric legal department. Any violation of laws, rules or regulations applicable to us could jeopardize our integrity. Fraud, dishonesty or criminal conduct will not be tolerated.

As part of your job responsibilities, you should:

- Learn about laws, rules and regulations that affect what you do at the Company,
- Attend periodic training and seek to keep up on any legal developments, and

- Consult with the Prometric legal department if you have any questions about the applicability, existence or interpretation of any law or regulation.

We comply with applicable trade restrictions and boycotts.

Our Company must comply with all applicable trade restrictions and boycotts. Boycotts may restrict our ability to ship products or offer services in a particular country.

We comply with environmental laws and regulations that apply to our Company.

We seek to abide by all applicable environmental standards in the countries in which we operate. Employees have a responsibility to conduct our operations in a manner that complies with laws and regulations, and which minimizes any adverse effect on the environment. We believe that protecting the environment is an important part of being a good corporate citizen. If your job involves contact with regulated materials or involves you in decisions about them, you should understand how those materials can be safely handled to protect you and your fellow employees from harm.

We must recognize the interests of the places in which we do business – currently over 160 countries. In addition to obeying laws and regulations, employees should also respect the local customs of host countries.

If you find yourself in a position that you believe may violate a law, regulation, this Code or another Prometric policy, you should report the violation or what you believe or suspect is a possible violation. You can report your concerns to a manager, your Human Resources department or the Prometric legal department. You can choose to report confidentially and anonymously, as discussed in the section "Questions & How to Report Concerns & Violations" of this Code.

Protect all intellectual property owned by prometric and respect the rights of other companies.

Our brand identity and intellectual property are among our most valuable assets and are essential to maintaining our competitive advantages. These include the Prometric name, logo, inventions, processes, innovations, content and software. It is extremely important that we protect these assets, and honor those of third parties. We are responsible for using basic intellectual property protections (such as copyrights, trademarks, service marks and patents) consistently and appropriately.

You should be aware that:

- Any intellectual property that employees create in the performance of their job responsibilities or that is related to Company business or activities belongs to the Company and should always be adequately protected. Also, where permitted by applicable law, intellectual property created by contractors or agents under a contract with us are also the property of the Company as a work-for-hire. You are expected to promptly disclose any inventions, discoveries and improvements conceived or made during your employment with the Company or that are related to Company businesses or activities,
- You are required to execute applications, assignments or other instruments upon the Company's request for applications for, and the attainment of, patents or to otherwise protect the interests of Prometric,
- You should report any unauthorized use of the Company's copyrights, patents, trademarks, service marks or other intellectual property to your manager or the Prometric legal department,
- You should get written permission to use a third party's copyrights, patents, trademarks, service marks or other intellectual property. If you want or need to use intellectual property that belongs to someone else, we must obtain a license to use the property or purchase the outright ownership of the property,
- You should not make copies of, nor publish any copyright-protected materials until we have obtained written permission from the holder and determined that copying or publishing is legally permitted,
- You should put appropriate copyright notices on all Prometric materials, information, products, services and other documents or products intended for public distribution or circulation. If you do not know what copyright notice is appropriate, please contact the Prometric legal department, and
- You should not copy or distribute software or related documentation without ensuring that the licensing agreement permits copying or distribution.

Contractual authorization

Don't sign a contract or agreement on behalf of Prometric unless you are authorized.

The Company's contractual agreements govern its business relationships. Because the laws governing contracts are numerous and complicated, policies and procedures are in place to ensure that any contract entered into by and on behalf of the Company has the appropriate level of review and approval.

As a result, employees of the Company who enter into contracts or agreements on the Company's behalf must have proper authorization, including legal review where required by policy, prior to the execution of any contract.

Gifts, meals, services and entertainment

Use your best judgment in giving and receiving gifts
We allow employees to offer or receive business gifts, favors and entertainment within specific guidelines. Gifts given or received should never include cash.
Giving gifts - Most countries where we do business forbid employees from making or participating in making any payments designed to cause or improperly influence the decisions of an individual, a company or a governmental official to act in a way that gives the company or the employee an advantage.

CONCLUSION

With the current business landscape, where legislation emerges and changes continuously with increasing requirements to keep business on the right track, it is critical for every organisation to implement adequate and effective structures to embed a culture of compliance. Internal Auditors must take responsibility to become familiar with the legislative universe of their organisations and assist in providing assurance that structures and processes are adequate and effective to mitigate compliance risks .

ACKNOWLEDGEMENT

The Authors are thankful to Sura Labs, Dilshukhnagar, Hyderabad for providing the necessary facilities for the research work.

REFERENCES

1. http://searchcompliance.techtarget.com/definition/regulatory-compliance
2. Tattam, David. "Compliance Risk Management". Protecht Risk Management Insights. Retrieved 27 March 2015.
3. Boiler and Pressure Vessel Inspection According to ASME
4. "Special Reports and Discussions on Chapter Eight". USSC.gov., Archived November 23, 2010, at the Wayback Machine.
5. Tattam, David. "Compliance Risk Management". Protecht Risk Management Insights. Retrieved 27 March 2015.
6. Compliance Challenge: Privacy vs. Security". Dell.com. Retrieved 2012-06-19
7. https://en.wikipedia.org/wiki/Regulatory_compliance
8. http://whatis.techtarget.com/reference/Fast-Guide-to-Reg ulatory Compliance#general%20info
9. https://www.auditshark.com/Education/what-is-compliance-management.aspx
10. http://www.pwc.com/gx/en/services/audit-assurance/regulatory-compliance.html
11. http://www.metricstream.com/solutions/regulatory_compliance.htm
12. http://www.thrivenetworks.com/blog/2011/10/27/what-is-regulatory-compliance-and-why-is-it-important/
13. https://www.prometric.com/en-us/Ethics/pages/legal-and-regulatory-compliance.aspx
14. http://www.astm.org/FULL_TEXT/E2107/HTML/E2107.htm
15. http://www.pitneybowes.com/us/shipping-and-mailing/case-studies/regulatory-compliance-best-practices.html
16. file:///C:/Users/SURA%20LAB/Downloads/nicta_publication_full_7038.pdf
17. https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/ZA_RA_EnsuringRegulatoryCompliance_IntegratingRiskAdvisoryAssurance_2015.pdf
18. https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/ZA_RA_Ensuri RegulatoryCompliance_IntegratingRiskAdvisoryAssurance_2015.pdf
19. http://enablon.com/applications/regulatory-compliance
20. https://technet.microsoft.com/en-us/magazine/2006.09.businessofit.aspx