Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2022, 9(10):72-79

Research Article ISSN: 2394 - 658X

Developing Standards, Policies, and Procedures for Regulatory Compliance

Mohammed Mustafa Khan

ABSTRACT

Organizations must develop robust standards, policies, and procedures in an increasingly regulated global environment to ensure compliance with various regulatory requirements. The paper focuses on creating robust compliance frameworks that protect not just from legal retribution but also improve brand perception and streamline business processes. Compliance 101 examines the elements of effective compliance programs, from developing well-crafted policies to enacting procedures related to those policies and ongoing monitoring and auditing for sustaining a compliant organization. This paper aims to evaluate business case studies, best practices, and phase plans for organizations performed by regulatory compliance.

Keywords: Regulatory compliance, standards, policies, procedures, risk management, compliance framework, monitoring, auditing, legal penalties, and organizational reputation.

INTRODUCTION

Regulatory compliance is very crucial in every organization. It is the aspect of the organization to comply with internal policies and procedures and relevant external laws or regulations. Failure to comply with regulations could cause dire consequences to the organization, such as legal actions, which could include fines and litigations, which, in the end, could tarnish the organization's reputation [1]. The global regulatory landscape is getting more complex, and organizations are under increased pressure to build compliance programs that satisfy legal mandates and contribute to broader organizational priorities. Standards, policies, and procedures are necessary for any effective compliance program. These components work together to systematically control compliance risks so organizations stay to the guiding principles and rules applicable to them [1]. This paper aims to have a 360-degree outlook on the core components such as business rules, validation lists/regulations, and Expression Logic & Signature Tab to develop these within a regulatory compliance perspective.

THE IMPORTANCE OF REGULATORY COMPLIANCE

***Source**: https://media.licdn.com/dms/image/C4D12AQGS2prUoc0jWA/article-cover_image-shrink_720_1280/0/1647972854163?e=2147483647&v=beta&t=ovsv2ruUtzEYtn9THmK-CmKlq7XdSrgOsWZx3UsCvkM*

Avoiding fines and penalties

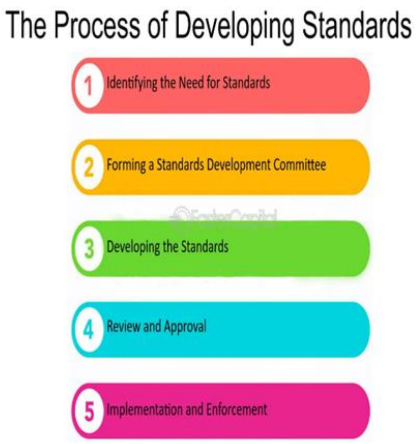
Regulations and laws are fundamental to any organization. Researching and identifying the rules and regulations that apply based on your location and industry is essential. For instance, specific regulations should be adhered to for a company that collects customer data, whether website cookies, credit card information or personally identifiable information [1]. Therefore, to prevent the organization from facing litigations, it is essential to adhere to the set regulations based on the state and the line of work your company operates. Similarly, complying with industry regulations and laws helps organizations create streamlined, scalable internal business processes and procedures [2]. For instance, HIPAA compliance is set to help organizations protect individual employees who handle PHI in their day-to-day operations. Some regulations include data backup, access management, disaster recovery, retention, and incident response policies. Adhering to the policy and streamlining internal processes assists in preventing and reducing data breach risks, improving employee engagement and retention, and enhancing the organization's overall security posture.

Adhering to regulations helps the organization prevent security breaches. Organizations dealing with data collection and storage are at risk of cyber-attacks. Industries such as healthcare and finance hold sensitive information and are more vulnerable to these attacks. Substantial regulatory compliance is crucial to prevent cyber criminals from attacking the organization and keep the data safe [1]. Keeping data safe per regulation adherence increases customer confidence with the company. Massive security breaches can significantly impact a company's reputation [2]. Repairing the trust among customers and stakeholders can be a very daunting task. Hence, regulatory compliance should be taken seriously to demonstrate organizational commitment to maintain the confidence of vendors, clients, and customers.

Source:*https://res.cloudinary.com/youverifyhq/image/upload/v1690441781/Best_Practices_for_Avoiding_Compliance_Fines_e7fdf60219.png*

DEVELOPING STANDARDS FOR COMPLIANCE

A compliance framework should follow compliance standards that perform a set of checks following broadly accepted best practices to ensure the organizational infrastructure and business services are managed, configured, organized, and monitored correctly [9]. These standards provide information related to issues that affect customers with similar problems and provide mechanisms that can help prevent them from happening again [3]. These standards work as a compliance control that should be tested to determine if they are followed and adhered to.


The Process of Developing Standards
1 Identifying the Need for Standards
2 Forming a Standards Development Committee
FasterCapital
3 Developing the Standards
4 Review and Approval
5 Implementation and Enforcement

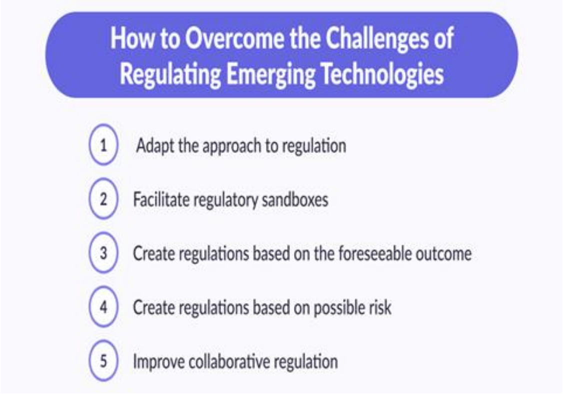
Source: *https://fastercapital.com/i/Standards--Setting-Industry-Standards--The-Role-of-Regulatory-Bodies--The-Process-of-Developing-Standards.webp*

Jurisdictional Regulations

Regulatory requirements and compliance obligations can vary substantially from one jurisdiction to another, creating a challenging landscape for multinational organizations. Jurisdictional regulations include many requirements, including labor laws, environmental standards, tax obligations, and consumer protection measures. For instance, if you run a company in the E.U., you must abide by GDPR, under which data privacy and personal information handling face harsh regulations [3]. In the U.S., however, organizations may fall under different data protection rules, such as those defined in the California Consumer Privacy Act (CCPA) [1]. The nuance in this requirement is that for multinational operators, the challenge becomes coordinating compliance activity across various regulatory environments, wherein you need to ensure individual jurisdiction-specific needs are met [10]. This frequently involves creating regional compliance standards aligned with local legal and cultural differences [10]. There are several repercussions for failure to adhere to regulations regarding your jurisdiction. The business might lose its license or face several legal fights, which could lead to a loss of money.

Emerging Regulations

Technology is changing at a very high speed, which means new trends are being introduced to the market every single day. Therefore, new rules and regulations must be set to capture the new trends and ensure customer safety is guaranteed. For instance, the introduction of blockchain technology and digital currency has brought a new sense of operations in the business world. These technologies were not covered in the previous regulations, meaning new laws must be formulated to accommodate their operations. Similarly, the world has faced the emergence of strict environmental laws due to the rise in concern about global climate to ensure ecological sustainability [3]. Organizations are now forced to focus on how their activities affect the climate and implement mechanisms to reduce or prevent their effects, such as waste management, resource conservation, and carbon emissions [1]. Similarly, the automotive industry has seen changes in regulations governing both their accounting and operations. Some changes include IFRS, Block Exemption Regulation, and Sarbanes Oxley. Due to these changes, organizations must stay updated on the current regulations to avoid any unforeseen effects on their business. To do this, organizations need to keep up to date with regulatory news, engage in industry forums and have a team of legal experts who can interpret the new laws and inform them on handling specific situations [10].



How to Overcome the Challenges of Regulating Emerging Technologies

1 Adapt the approach to regulation

2 Facilitate regulatory sandboxes

3 Create regulations based on the foreseeable outcome

4 Create regulations based on possible risk

5 Improve collaborative regulation

Source:*https://geniusee.com/storage/app/media/blog/blog_254_regulating_emerging_technologies/how_to_overcome_challenges_of_regulating_emerging_technologies.png*

Establishing Organizational Standards

Once the applicable regulations have been identified, the next step is to establish organizational standards that align with these regulations [10]. These standards should provide clear guidance on the organization's expectations for compliance and set the foundation for developing policies and procedures.

Setting Performance Standards
01
Importance of setting performance standards
02
Establishing performance standards
03
Best practices for setting performance standards

Key considerations include:

Alignment with Regulatory Requirements: Organizational standards must follow specific regulations that are meant to be relevant to the business. This could include data protection, financial reporting and environmental sustainability — to name a few areas associated with the industry in which an organization operates.

Incorporation of Best Practices: Organizational standards should meet regulatory requirements and include industry-best practices. This optimization will be the perfect combination of legislative compliance and ethical conduct that is ideally suited to meet program sponsorship requirements [3].

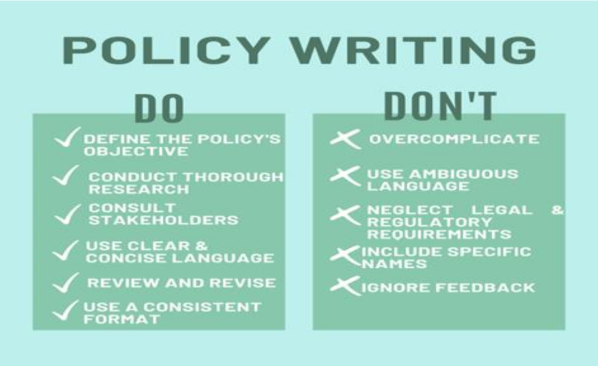
Flexibility & Scalability: The regulatory environment changes over time, and organizational standards must be adopted. Organizational controls should be flexible enough to work with processes in place while being scalable so they can grow more significantly [4]. Making this happen may mean regularly reviewing and updating standards based on new laws and regulations, emerging risks, or organizational changes.

CREATING COMPLIANCE POLICIES

Policies are the specific guidelines that define how the organization will implement its standards and achieve compliance [2]. It includes details of how employees should act during specific scenarios and states the behaviour expected throughout the organization.

Defining Clear and Concise Policies

The best compliance policies should be clear, concise, and to the point. The policies should offer employees the necessary resources to comply with regulations and business policies without making them overly convoluted or obtuse.



POLICY WRITING

DO
- ✓ DEFINE THE POLICY'S OBJECTIVE
- ✓ CONDUCT THOROUGH RESEARCH
- ✓ CONSULT STAKEHOLDERS
- ✓ USE CLEAR & CONCISE LANGUAGE
- ✓ REVIEW AND REVISE
- ✓ USE A CONSISTENT FORMAT

DON'T
- ✗ OVERCOMPLICATE
- ✗ USE AMBIGUOUS LANGUAGE
- ✗ NEGLECT LEGAL & REGULATORY REQUIREMENTS
- ✗ INCLUDE SPECIFIC NAMES
- ✗ IGNORE FEEDBACK

Source: *https://www.sweetprocess.com/wp-content/uploads/2023/10/how-to-write-a-policy-27.png*

Key considerations include:

Clarity and simplicity: Policies should be clear, straightforward, and written in a language all employees can understand. The policy is more readable by all staff whether or not they have the required minimum level of skills with both preparation and law enforcement typically using as simple an approach to wording policies [1].

Specificity: Policies should be specific to provide clear directions on what employees are expected to do. A data protection policy, for instance, will describe exactly what actions employees need to take to defend critical information (like encrypting it and using secure passwords) [4].

Consistency: Policies must be consistent with organization standards and support regulatory requirements. Conflicting policies or an absence of clear policy guidance can create confusion and increase the risk of non-compliance.

Sharing and Enforcing Policies

Once policies have been developed, they must be effectively communicated and implemented across the organization. This requires everyone to know the policies and their role in compliance.

Key considerations include:

Training and Education: It is essential to provide ongoing compliance policy training so employees know what to do [9]. This can consist of organizing workshops and seminars or even online training sessions to educate employees about the policies of their organizations as well as how those regulations are met [4].

Communication Channels: Your communication channel should have a reliable source to disseminate solutions and inform them about policies. It includes transmitting policies and notices via digital communication such as email, intranet portals, or other similar avenues.

Enforcement and Accountability: Policies should be consistently enforced throughout an organization, with repercussions for those who do not comply from the senior to junior levels [5]. It can mean enforcing discipline for employees who do not follow the policies or creating a method to report and investigate compliance issues.

ESTABLISHING COMPLIANCE PROCEDURES

Procedures are instructions that tell employees how to apply an organization's policies. They elaborate on the steps to perform specific processes and enforce compliance in routine workflows.

Clearly Defining a Sequence of Steps:

Good compliance processes are highly detailed and sophisticated; they provide clear instructions on how employees should perform their roles compliantly.

Key considerations include:

Step-by-step: The procedures should list the steps for doing specific tasks like processing transactions, handling customer data, and reporting incidents [5]. This means all employees should understand what they are doing, which will help minimize mistakes.

Roles and Responsibilities: Procedures should clearly define the roles and responsibilities of employees involved in the compliance process. This will ensure there is accountability in terms of who should be doing what and making sure that it gets done.

Document procedures: This should be done using an easy-to-find and refer-to method for employees. This could include developing manuals, checklists, and flowcharts to make it easier for employees to follow compliance procedures.

Performing and Monitoring the Action

After establishing and implementing the procedures, monitoring and ensuring every organization member adheres to them strictly is very important.

Monitoring and Reporting Mechanisms
01
Monitoring and reporting mechanisms play a crucial role in ensuring adherence to settlement terms
02
03
04
Collaboration and cooperation between the parties involved is essential for effective monitoring and reporting mechanisms
05
06

***Source**: https://fastercapital.com/i/Legal-compliance--Promoting-Adherence-to-Follow-Settlement-Terms--Monitoring-and-Reporting-Mechanisms.webp*

Key considerations include:

Training and Support: to ensure procedures are followed, it is essential to train employees using different training techniques, such as ongoing helpdesks and team training, to ensure every member is up to date with each procedure [2]. **Monitoring and auditing:** The organization should monitor every employee's movement and ensure every procedure and regulatory compliance is followed. This may include conducting internal audits and implementing real-time monitoring tools to help gauge compliance.

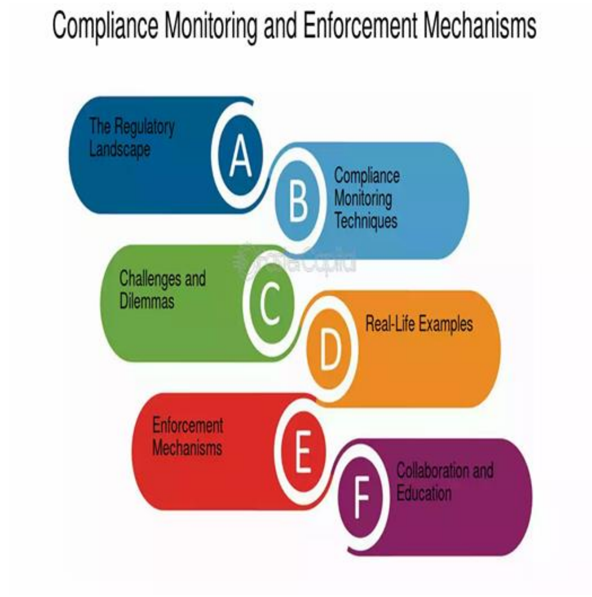
Continuous Improvement: Compliance procedures should be reviewed and updated continuously to remain current with regulations, organizational practices, and emerging risk areas [5]. Some of this includes seeking employee input, conducting risk assessments, and adapting procedures.

PERPETUAL MONITORING AND POST-AUDIT

After monitoring and auditing, the organization can identify areas that need regulations and procedures. This way, they can prevent compliance issues before they become a significant problem [9]. This will ensure the organization stays on its toes with regulatory requirements and help the business grow and move forward.

Establishing Monitoring Mechanisms

The organization should employ real-time monitoring tools to help them identify compliance issues and solve them before they occur [7]. The tools are designed to alert members of the organizations in case a problem is about to happen, or there is a need to improve regulation.


Compliance Monitoring and Enforcement Mechanisms
The Regulatory Landscape
A
B
Compliance Monitoring Techniques
Challenges and Dilemmas
C
D
Real-Life Examples
Enforcement Mechanisms
E
F
Collaboration and Education

Key considerations include:

Automated Monitoring Tools: Automated monitoring tools can help organizations track compliance in real-time, alerting them to issues as they occur. This might consist of monitoring transactions, data access, or other relevant activity for compliance purposes using software [9].

Incident Reporting Systems: Creating incident reporting systems helps employees report possible compliance violations rapidly without fear of retaliation [5]. This, in turn, allows organizations to recognize the issues and address them on time.

Regular Reviews: Ongoing reviews of compliance operations and their results help the organization see when something might need improvement. This could mean regular conformity performance tests and assessing how efficiently the control process functions.

Conducting Audits

Source: *https://www.latestquality.com/wp-content/uploads/2018/02/conducting-internal-audits.jpg*

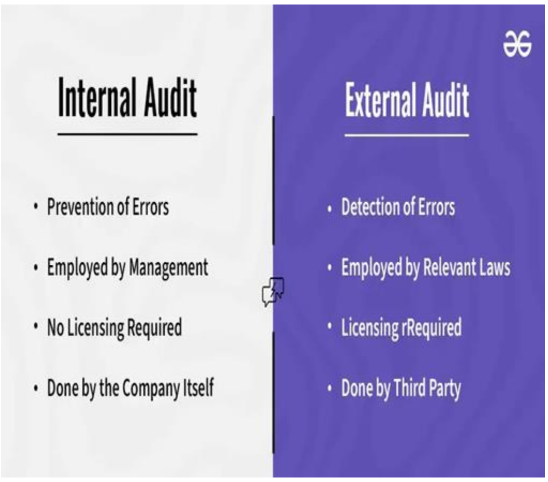
Audits are systematic reviews related to both legal compliance and organizational regulations. They help uncover flaws in the pipes of your compliance program and provide significant intel into areas that need work [9]. There are two basic kinds of audits: internal and external.

Internal Audits

These audits are performed by the organization's compliance or internal auditors. These audits evaluate the organization's policies, procedures, and records against regulatory requirements and organizational standards [8]. These are generally conducted during routine intervals to discover potential outcomes of non-compliance in advance to prevent them from becoming ad-hoc pitfalls. Internal audits provide several advantages to the organization [1]. Since the people within your organization facilitate the process, they can focus on what matters to you and the risks that matter most. In addition to this, they make continuous measurement and rapid response possible. Internal audits promote an environment of continual betterment by introducing workers to compliance practices and making them more accountable for their responsibilities in ensuring regulatory conformance [6].

External Audits

These are audits undertaken by third-party independent bodies such as a regulatory body, external auditors, or specialized compliance firms. These audits measure the organization's compliance with regulatory standards and internal policies [6]. In many industries, especially in the heavily regulated finance, healthcare, and manufacturing sectors, external audits are mandated by law or regulation [2]. The significant advantage of external audits is that they are independent. Exhibiting impartiality in terms of top brass, external auditors help to detect the areas missed during internal audits. Additionally, external audits can enhance the organization's credibility with regulators, investors, and other stakeholders by demonstrating a commitment to transparency and regulatory compliance. However, taking an external audit also comes with challenges [6]. They can be more disruptive to day-to-day operations as they bring in third parties and are costly, especially if you uncover major compliance issues that must be addressed [2]. Nonetheless, external audits are essential to a comprehensive compliance program, providing additional assurance that the organization meets its regulatory obligations [8].



Internal Audit	External Audit
• Prevention of Errors	• Detection of Errors
• Employed by Management	• Employed by Relevant Laws
• No Licensing Required	• Licensing rRequired
• Done by the Company Itself	• Done by Third Party

Source: *https://media.geeksforgeeks.org/wp-content/uploads/20240408172802/Difference-between-Internal-Audit-and-External-Audit-copy.webp*

CONCLUSION

There is no doubt that organizations need to have a robust compliance program in place as we now operate under one of the most challenging regulatory environments. It starts by defining clear benchmarks that resonate with the industry-specific, geographic, and upcoming regulations [7]. These standards set the stage for creating specific policies and procedures that inform how an organization achieves compliance. Ongoing monitoring and auditing are the keys to ensuring that such policies are consistently implemented to not jeopardize organizational compliance with federal laws. Real-time monitoring systems, from automatic equipment to incident reporting methods, allow control and timely intervention of compliance matters [7]. Periodic evaluations of compliance operations also help to confirm that the company's program is effective and current. Similarly, internal audits offer a proactive, ongoing assessment of the organization's compliance practices, while external audits provide independent and objective scrutiny of that organization's conformance with regulatory standards.

REFERENCES

[1]. S. Hina and P. D. D. Dominic, "Information security policies' compliance: a perspective for higher education institutions," Journal of Computer Information Systems, vol. 60, no. 3, pp. 201–211, Mar. 2018, doi: https://doi.org/10.1080/08874417.2018.1432996.

[2]. "Regulatory Policy and the Social Sciences," Google Books, 2021. https://books.google.co.ke/books?hl=en&lr=&id=wt_rDwAAQBAJ&oi=fnd&pg=PR7&dq=Developing+Standards (accessed Aug. 24, 2024).

[3]. C. Holley, T. Mutongwizo, S. Pucci, J. Castilla Rho, and D. Sinclair, "Groundwater Regulation, Compliance and Enforcement: Insights on Regulators, Regulated Actors and Frameworks in New South Wales, Australia," SSRN Electronic Journal, 2020, doi: https://doi.org/10.2139/ssrn.3524730.

[4]. R. Zulfikar, N. Lukviarman, D. Suhardjanto, T. Ismail, K. Dwi Astuti, and M. Meutia, "Corporate Governance Compliance in Banking Industry: The Role of the Board," Journal of Open Innovation: Technology, Market, and Complexity, vol. 6, no. 4, p. 137, Dec. 2020, doi: https://doi.org/10.3390/joitmc6040137.

[5]. F. Salguero-Caparrós, M. C. Pardo-Ferreira, M. Martínez-Rojas, and J. C. Rubio-Romero, "Management of Legal Compliance in Occupational Health and safety. a Literature Review," Safety Science, vol. 121, no. 1, pp. 111–118, Jan. 2020.

[6]. V. R. Martinez, "Complex Compliance Investigations," Columbia Law Review, vol. 120, no. 2, pp. 249–308, 2020, Available: https://www.jstor.org/stable/26902675

[7]. J. Armour, J. Gordon, and G. Min, "Taking Compliance Seriously," Yale Journal on Regulation, vol. 37, p. 1, 2020, Available: https://heinonline.org/HOL/LandingPage?handle=hein.journals/yjor37&div=4&id=&page=

[8]. S. Prakash, S. Venkatasubbu, and B. K. Konidena, "Streamlining Regulatory Reporting in U.S. Banking: A Deep Dive into AI/ML Solutions," Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online), vol. 1, no. 1, pp. 148–166, Oct. 2022, doi: https://doi.org/10.60087/jklst.vol1.n1.p166.

[9]. R. F. Ali, P. D. D. Dominic, S. E. A. Ali, M. Rehman, and A. Sohail, "Information Security Behavior and Information Security Policy Compliance: A Systematic Literature Review for Identifying the Transformation Process from Non-compliance to Compliance," Applied Sciences, vol. 11, no. 8, p. 3383, Apr. 2021, doi: https://doi.org/10.3390/app11083383.

[10]. Angraini, R. A. Alias, and Okfalisa, "Information Security Policy Compliance: Systematic Literature Review," Procedia Computer Science, vol. 161, pp. 1216–1224, 2019, doi: https://doi.org/10.1016/j.procs.2019.11.235.