
SIX
ESSENTIAL
ELEMENTS OF
AN EFFECTIVE
COMPLIANCE
PROGRAM

TABLE OF CONTENTS

Introduction

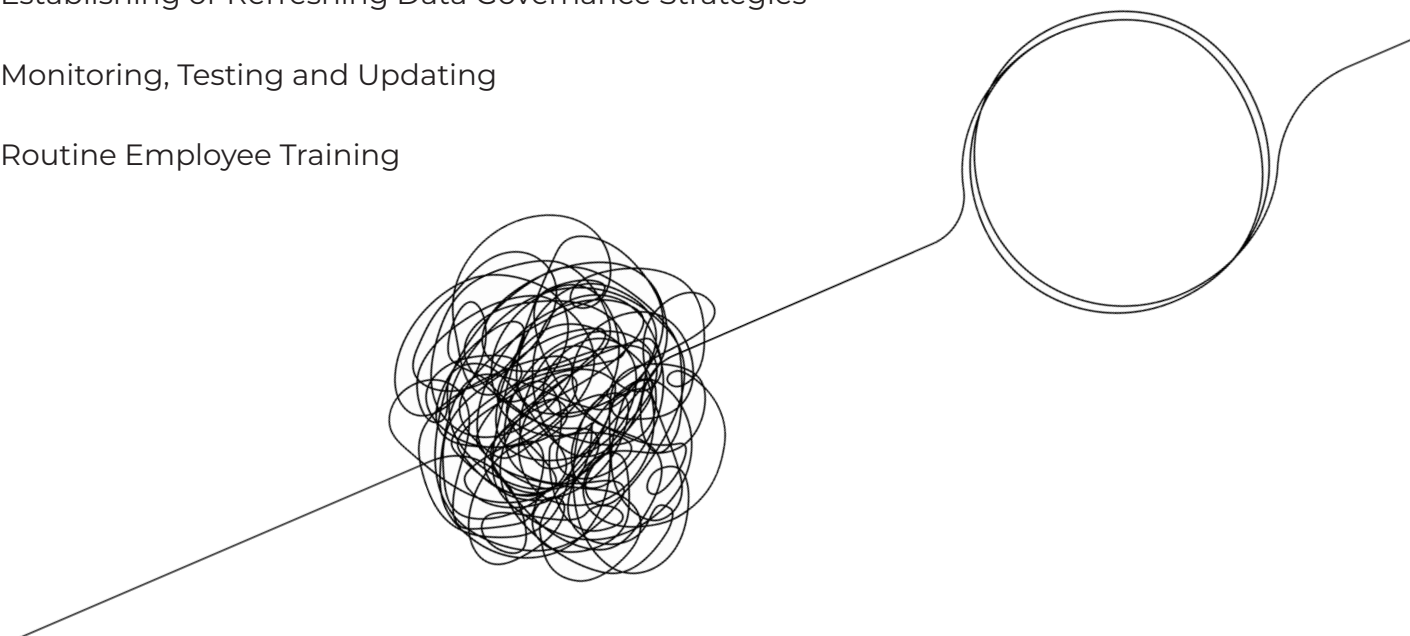
A Corporate Compliance Program aims to protect an organization and the people it serves from compliance risks. The program accomplishes this by ensuring the business complies with relevant laws, regulations and contractual obligations.

You could consider your compliance program to be an internal insurance policy that creates evidence of compliance while instilling a culture of compliance. Establishing a foundation for compliance and accountability regarding legal or contractual requirements is a company's best protection against catastrophic financial setbacks and reputational damage arising from non-compliance.

Keep in mind that compliance programs are not one-size-fits-all programs. You will need to develop a plan that meets your business's specific needs while recognizing that compliance requirements will limit your ability to make decisions based on your risk tolerance and desire to control costs. Rather than recreating the wheel, you can adopt a recognized security framework that aligns closely with your compliance requirements. Your ultimate goal should be to build an effective and comprehensive compliance program that can stand up to scrutiny.

Listed below are six foundational elements to consider for your compliance program:

- ☐ Executive Sponsorship and Commitment to Compliance
- ☐ Conducting Risk Assessments and Business Impact Analysis
- ☐ Appointing a Chief Compliance Officer (CCO)
- ☐ Establishing or Refreshing Data Governance Strategies
- ☐ Monitoring, Testing and Updating
- ☐ Routine Employee Training



Executive Sponsorship and Commitment to Compliance

A good compliance strategy begins with sponsorship and compliance at the highest levels of your organization (owners/stakeholders/boards and senior management). A compliance program with sponsorship from an executive sends a strong message. It indicates an endorsement from a top-level executive who will oversee the program and help it progress. It's critical that executive leadership or the board of directors approve policies that align with your compliance requirements because your policies will be the cornerstone that guides behavior. This is vital because, otherwise, a company could simply conduct a business impact analysis (BIA), run regular risk assessments and look excellent on paper, but let severe vulnerabilities slip through the door unchecked.

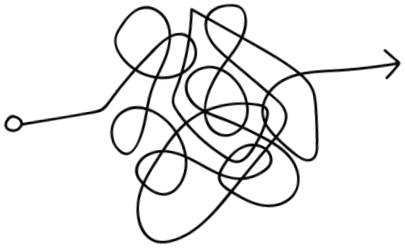
Here's how you can secure an executive sponsorship for a compliance program:

Identify a suitable executive
Create a list of criteria — similar to a job description — that defines what a compliance executive would do. Use that list to measure the suitability of available candidates.

Prepare a business case
Prepare a business case based on all your compliance requirements — laws, regulations, contracts and insurance policies. Emphasize how the compliance program will benefit the business and the executive. Quantify the financial costs of non-compliance. Think of this as your sales pitch. It should offer value to the sponsor as well as to the company.

Schedule a meeting
Scheduling a meeting with a top executive can be challenging because they run on tight schedules. The key to arranging a meeting is to be professional and assertive. If your desired candidate has an executive assistant, establish contact with that person first to explain what you are trying to accomplish and seek their input on how best to approach the request.

Request executive sponsorship
Present the business case in such a way that all intended information is clearly communicated to the executive. Ensure the presentation appeals to the interests of the executive and the business. Keep it short and aim to deliver the overview in 30 minutes or less. Set aside time for questions and feedback at the end. If your first choice declines the proposal, ask them to recommend another.



Conducting Risk Assessments and Business Impact Analysis

Regular risk assessments help detect, estimate and prioritize risks to an organization's employees, assets and operations. A BIA helps quantify the impact of a disruption (due to an accident, disaster, data breach, ransomware attack, etc.) on critical business operations. These must be repeated because, like your health, compliance can be good one day and bad the next.

While a risk assessment identifies vulnerabilities and threats, a BIA helps you prioritize your recovery and prepare to quickly get back on track after an incident. However, both can help to avoid severe damage from a security or compliance shortcoming.

Regarding BIA for compliance, you can start with a list of challenging questions such as:

What steps do you need to take today to become compliant?

A few things to check:

- [ ] Regulations and other obligations that apply to your organization
- [ ] Tracking the reporting deadlines set by regulators
- [ ] Notification requirements for those affected by a breach or compliance violation
- [ ] Ensuring your policies are on par with compliance prerequisites
- [ ] If regular compliance assessments are or can be conducted
- [ ] Communication of responsibilities to all employees
- [ ] Quality of record-keeping

How long will it take to plug compliance gaps?

Once compliance gaps are identified, they must be filled as soon as possible. Always remember that the cost of non-compliance is much more than the cost of a compliance program or service and that regulations and contractual obligations take away your ability to make arbitrary decisions.

Do you have in-house expertise?

To deal with the issue of compliance gaps, the best thing to do is identify talent within the company. If in-house expertise is sufficient, then determine if that is the best use of their time or if it makes sense to augment your internal team's efforts with those of a third party. Some regulations require a third-party independent assessment.

Does it make sense to partner to accomplish goals?

It can be difficult to develop a compliance program on your own that can keep up with changing laws, emerging risks and new regulations. Partnering with an experienced service provider can help you develop a compliance program that also delivers your business goals. Choose a partner who can give you a clear action plan that states where your compliance function currently is, where it needs to be and how to get there.

Appointing a Chief Compliance Officer (CCO)

Appointing a CCO is not an easy job. However, having a dedicated CCO is vital to avoid non-compliance issues in the long run. A CCO:

- Drafts policies and procedures needed for the business's compliance.
- Communicates the policies, procedures and relevant updates across the entire organization.
- Monitors the business's compliance and investigates instances of non-compliance.

Here are a few ways to go about appointing a CCO:

Appoint an apt candidate from within

Selecting a candidate from within your business is a good option because the person already knows your business. Be sure to give the CCO time and resources to build and manage the compliance program, instead of adding a title and expecting them to continue to handle compliance in addition to their other responsibilities. However, if there is a knowledge gap, provide training or look to a third party to bridge this gap.

Hire an outsider

Selecting a skilled outsider will reduce the burden of training. However, candidates with the right knowledge and skill set are in demand, hard to find, expensive and will need time to become familiar with your organization.

Outsource to a trusted partner

Outsourcing can help you quickly find a candidate with sufficient knowledge and in a more cost-effective manner. A skilled compliance expert will have the experience and knowledge that could take you years to develop internally after a ransomware attack.

Establishing or Refreshing Data Governance Strategies

An effective data governance strategy ensures that data is managed well, thus making data management compliant with internal/external rules and regulations.

» **Assess the current state of data governance and draft a roadmap**

Identify the positives and negatives of the existing data governance strategy and eventually aim to reduce the drawbacks to achieve your compliance goals.

» **Draft policies that can take your business down the path of compliance for years to come**

There should be no loopholes within a newly drafted policy. It must be comprehensive and in adherence with the highest standards of compliance. For this reason, consider refreshing the policy quarterly or annually to ensure new use cases and requirements are addressed.

» **Document compliance processes**

Ensure that all compliance-related procedures and activities are documented and retained so you are ready for audits, investigations and lawsuits. Regulators demand documentation. You should be able to provide recent documentation to prove that your compliance program is fully implemented, and historical documentation to show that the efforts have been in place for a long time.

» **Bring together the right personnel to form a governance department**

While forming a governance department, it is essential to bring together individuals with commitment and knowledge about safe data handling. Although there is no specific method to form a governance department, it would be ideal to include the following:

Steering committee —
This is comprised of senior management, often C-level executives. The steering committee drafts the overall governance strategy and holds the governance department accountable for timelines and outcomes.

Data owner —
A data owner ensures that data from a particular domain is governed throughout the organization. Data owners provide input to the steering committee regarding their data domain.

Data steward —
A data steward is responsible for the day-to-day management of data. They are subject experts who can comprehend/communicate vital information and report to data owners.

Monitoring, Testing and Updating

The regular monitoring, testing and updating of systems and processes ensure they don't inadvertently become non-compliant.

It ensures the control environment is effective and includes:

- **Vulnerability and non-compliance scanning/alerts**
  You must deploy solutions that can conduct regular automated scans to detect vulnerabilities and non-compliance. Once the solution finds an irregularity, it should immediately alert key staff.

- **Patch management**
  Poor patch management provides a freeway for cybercriminals to exploit vulnerabilities. For this reason, it is best to use tools that automate patch management.

- **Policy management**
  Efficient policy management is essential for risk management and compliance. Robust policy management systems can take that load off your shoulders.

- **Acceptable use policy**
  There must be a set of rules to restrict the use of company networks, websites or systems. This helps minimize illegal activities and cyberthreats.

Routine Employee Training

A culture of integrity is essential to encourage good, ethical and compliant behavior. Don't assume your workforce members will automatically do what is documented in your policies. Regular training can help employees remember and stay compliant with data governance policies that help your organization comply with high-stakes regulations related to your line of business.

Here are a few tips to make training more effective:

- **Training sessions must be interactive**
  Ensure that the training sessions are interactive and, if possible, in video format. You can provide textual content as a complementary piece. The session must always allow employees to have their doubts cleared.

- **Break the content into modules**
  You must break the training content into smaller modules because it has a better chance of being retained than a lengthy piece of content. It also lets you send training materials at regular intervals. Consider limiting training sessions to 30 minutes each and aim to make each video topic within a session 5 minutes or less. To improve engagement, consider providing a printable course completion certificate or other small incentives.

- **Self-paced learning is the best**
  Give your employees the freedom to learn at their own pace. However, this does not mean you give them infinite time. Assign deadlines based on topic complexity.

- **Include relevant material**
  Educational content must stay evergreen. Update it regularly to keep pace with the rapidly changing cyber landscape.

- **Conduct quizzes and simulated drills**
  To test your employees' level of knowledge and awareness, conduct quizzes and simulated drills after every session.

- **Document your training activities**
  Retain sign-in sheets and reports from automated training systems to validate that you are meeting your compliance requirements for awareness and training.

Learn more on how to execute a plan that meets your compliance and business goals.

Schedule a consultation today to create a compliance strategy built for success.