10 Best Practices to Build a Strong Compliance Program

External - v1.0

WHISTLEBLOWER SECURITY a Case IQ company

Contents

CHAPTER 1

The Importance of Corporate Compliance

Having a corporate compliance program is crucial in today's highly regulated business environment. An effective compliance program is an important part of an organization's internal controls process and is an important component to detecting and preventing ethical violations.

Organizations should take a proactive approach when promoting compliance and should recognize the value of having an effective, credible, and well-designed program.

A credible program will demonstrate the organization's commitment to conducting business within the law while informing employees about their legal duties, and what potential repercussions could happen when not complying with the law.

Compliance programs help employees identify boundaries of permissible conduct, as well as inform about situations where seeking legal advice should take place.

Some immediate benefits of a well thought out compliance program include:

- **Help** maintain a good reputation
- **Reduce** litigation costs, and fines
- **Reduce** bad publicity and the disruption to business operations
- **Reduce** stakeholder exposure to criminal, civil or penal liability
- **Improve** the ability to recruit and retain staff
- **Improve** the ability to attract and retain customers and suppliers

Compliance programs should be adapted to an organization's specific industry, business, and risks. Effective compliance programs promote a culture within an organization that encourages ethical conduct, and a company-wide commitment to adhering to the law. They should protect an organization's reputation, brand, relationship with investors, protect assets, and help in the detection and prevention of misconduct, including regulatory violations. When regulators need to get involved in the organization's business, they look at whether an organization has self reported, cooperated, and taken appropriate actions to righting a wrong, and will put forth appropriate action that takes into consideration the existing adequacy of an organization's compliance program.

Three basic questions an organization should consider are:

- Is the organization's compliance program well designed?
- Is the organization's compliance program applied in good faith?
- Does the organization's compliance program work?

Compliance Risks

Compliance programs are going to differ depending on type of organization and industry. There's no 'one program fits all' as organizations have differing needs. Banks and financial institutions have different risks compared to manufacturers. The healthcare sector has different risks compared to the education industry. An effective compliance program should take into account these differing business risks and needs.

Large corporations are going to have many more factors to take into consideration compared to small and medium sized businesses. But one thing that is certain to any sized business is that a check-the-box mentality is just not complex enough to satisfy regulators like the DOJ, SEC, and FCPA. No matter the organization, a compliance program that is thoughtfully laid out, designed carefully, implemented purposefully, and enforced fairly company-wide should help in the effort to detect violations that do occur, and make it more efficient to initiate an appropriate outcome.

The purpose of a company's compliance program is to reduce compliance risk and avoid regulatory enforcement or financial loss resulting from non-compliance to laws. Some common compliance risks that can affect any company, no matter the size, or industry include:

Corruption

Corruption is dishonesty or fraudulent activity conducted by those in power. Some examples of corruption include bribery, embezzlement, bid rigging, lobbying and extortion.

Environmental, Health, and Safety

Also known as EHS compliance, it refers to laws, regulations, and workplace procedures designed to protect the wellbeing of workers. An example would be ensuring compliance with OSHA, including ensuring there are preventative measures in place for fall protection, hazardous substance exposure, and environmental pollution.

Data Protection

Companies need to ensure they are employing formal standards to protect sensitive data from loss, theft, and misuse. An example is under GDPR where companies need to protect personal data and privacy of EU citizens for transactions that occur within EU member states.

Employment

Employment refers to how a company maintains an ethical workplace. This includes how it handles wage-and-hour issues, anti-discrimination, anti-harassment, and more. This is where an ethics reporting hotline can be utilized to report on any inconsistencies in these areas.

BEST PRACTICE 1

Tone From the Top

Tone from the top is the visible willingness of leadership to promote not just an ethical culture company-wide, but a culture that is inclusive, fair, honest, and fee from retaliation.

Tone from the top refers to the ethical atmosphere that is created by leadership. We've all heard the saying "actions speak louder than words". If the climate at the top of an organization is nonchalant and if directors and senior management skirt around important issues and don't obey and enforce the rules they have initiated themselves, then it's unlikely that the rest of company is going to take any ethics or compliance initiatives seriously themselves. A compliance program begins with directors and senior management setting the proper tone for the rest of the organization to follow because employees take their cues from corporate leaders. A strong compliance program should be enforced in good faith and clearly articulated to every single employee.

If senior management encourages employees to engage in misconduct in order to achieve business objectives, the compliance program is pointless. And if the DOJ and SEC become aware that bad behaviour is being enforced, or ignored, this will be taken into consideration when evaluating possible violations. By adhering to ethical standards, and clearly articulating the organization's standards, senior management will be able to encourage middle management to also adhere to those ethical standards, and that in turn will filter down to every employee.

BEST PRACTICE 2

A Code of Conduct Should Reflect the Business

We've often heard that the Code of Conduct is the foundation of an organization's compliance program. And as mentioned earlier, a Code of Conduct is going to differ from industry to industry. The DOJ has repeatedly stated that an effective code is clear, concise, and easily accessible to every employee and those doing business with the organization. This includes having a code in all available languages for employees and vendors across the world. If employees can't access it, or don't understand it, your code is not effective.

The Code of Conduct needs to be up-to-date and reflect the risks associated with the size and type of business. Some of the risks a company should assess Include the nature and extent of transactions with foreign governments, including payments to foreign officials; use of third parties; gifts, travel, and entertainment expenses; charitable and political donations. These standards also need to apply to all employees at every level of the organization, no matter their location.

What should be included in a Code of Conduct?

- A message from the CEO or other top leadership -it starts with a sincere message
- The company's values – what does your company value? Respect? Accountability? Motivation?
- Respect for others – what interactions between colleagues, and customers is appropriate?
- Respect for the community – how does the company interact with the community in a responsible way?
- How to report violations – what are considered violations of the code and how can they be reported?

BEST PRACTICE 3

Risk-Based Reviews

A company can find itself on the wrong side of regulators and the law if a compliance program is not actively enforced. Companies may have good intentions in the beginning by communicating their program throughout the organization. However, actively enforcing it falls short of the mark. The program is forgotten.

Let’s say a in few months an organization acquires a subsidiary in a foreign country yet fails to communicate the compliance program to the new foreign employees. These employees continue to operate in the way they are accustomed to. And now the organization finds itself in violation of the FCPA. It’s a situation that could have been avoided with a bit of due diligence.

As companies change over time through growth, mergers or acquisitions, policies that were put together for the organization five years ago aren’t going to work with the same organization today.

A company needs to periodically evaluate its compliance policy and codes by conducting risk assessments that address the individual circumstances of the company at that time and into the near future.

The compliance program should be tailored to that organization’s unique risk profile.

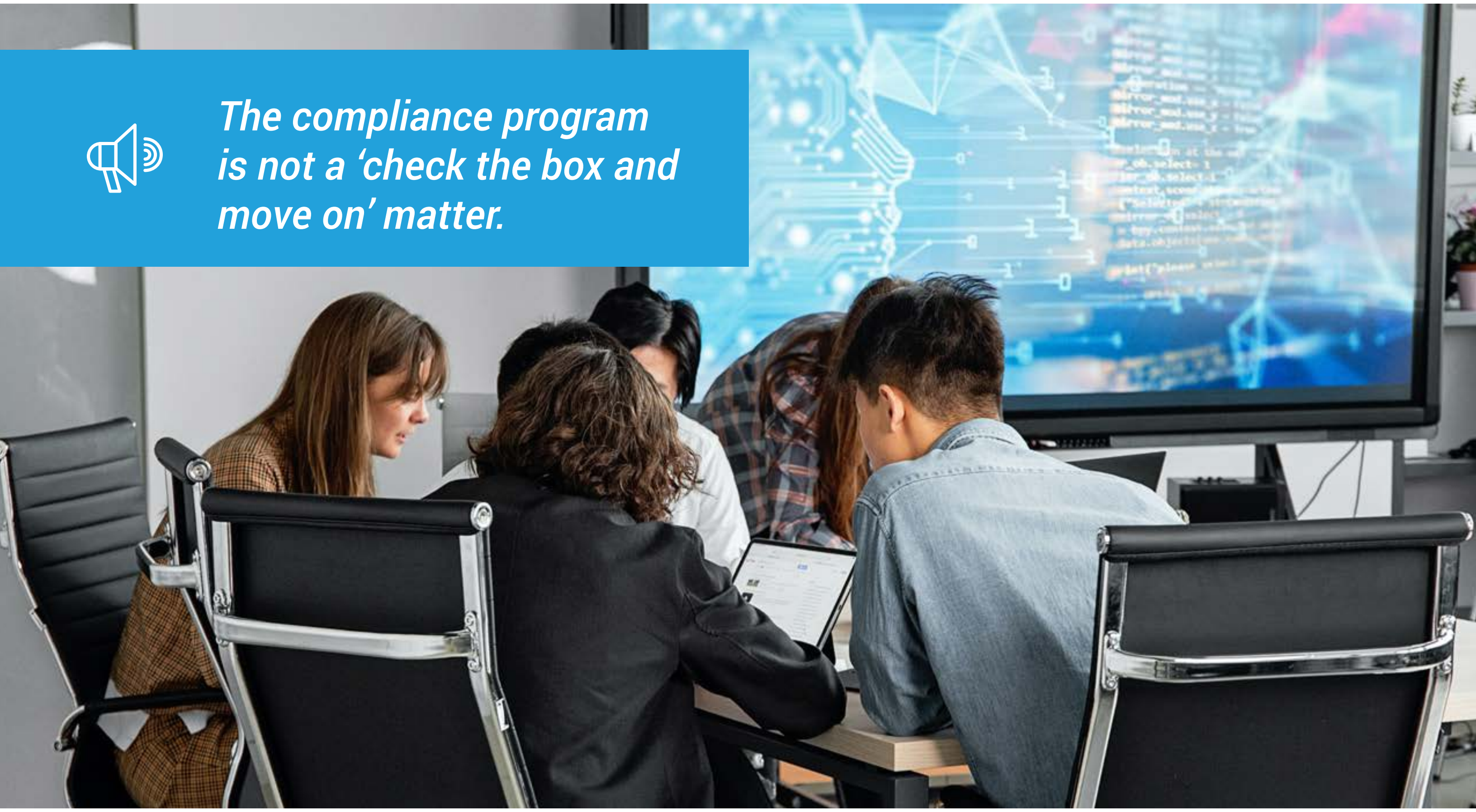
BEST PRACTICE 4

Oversight and Resources

Compliance programs need resources. In larger companies, a board of directors' fiduciary duties include ensuring that company management has an effective corporate compliance program in place. Duties also include applying oversight of that program and taking regular steps to stay informed of the program's content and operation. Additional oversight is conducted by the Chief Compliance Officer and often a compliance committee. All parties involved in maintaining a compliance program need to be fully invested in its success as there will be many adverse consequences of an inadequate compliance program, or an inadequately managed compliance program.

Any breach of duties can result in shareholder litigation and possibly personal liability under some circumstances. A failure in the compliance program can lead to operational, reputational, and other business challenges that can critically harm, or even destroy a company.

Like any other responsibility the board and compliance committee are responsible for, the compliance program is not a 'check the box and move on' matter. The board, the COO and any committees involved need to remain vigilant when it comes to monitoring compliance. It does not need to be addressed at every meeting, but it should remain a priority.



The compliance program is not a 'check the box and move on' matter.

BEST PRACTICE 5

Training

Regulators will evaluate whether or not an organization has taken steps to ensure that policies and programs have been communicated throughout the organization. This includes directors, officers, employees, agents, and business partners. Training means repeated communication, frequent and effective training, and an ability to provide guidance when issues arise.

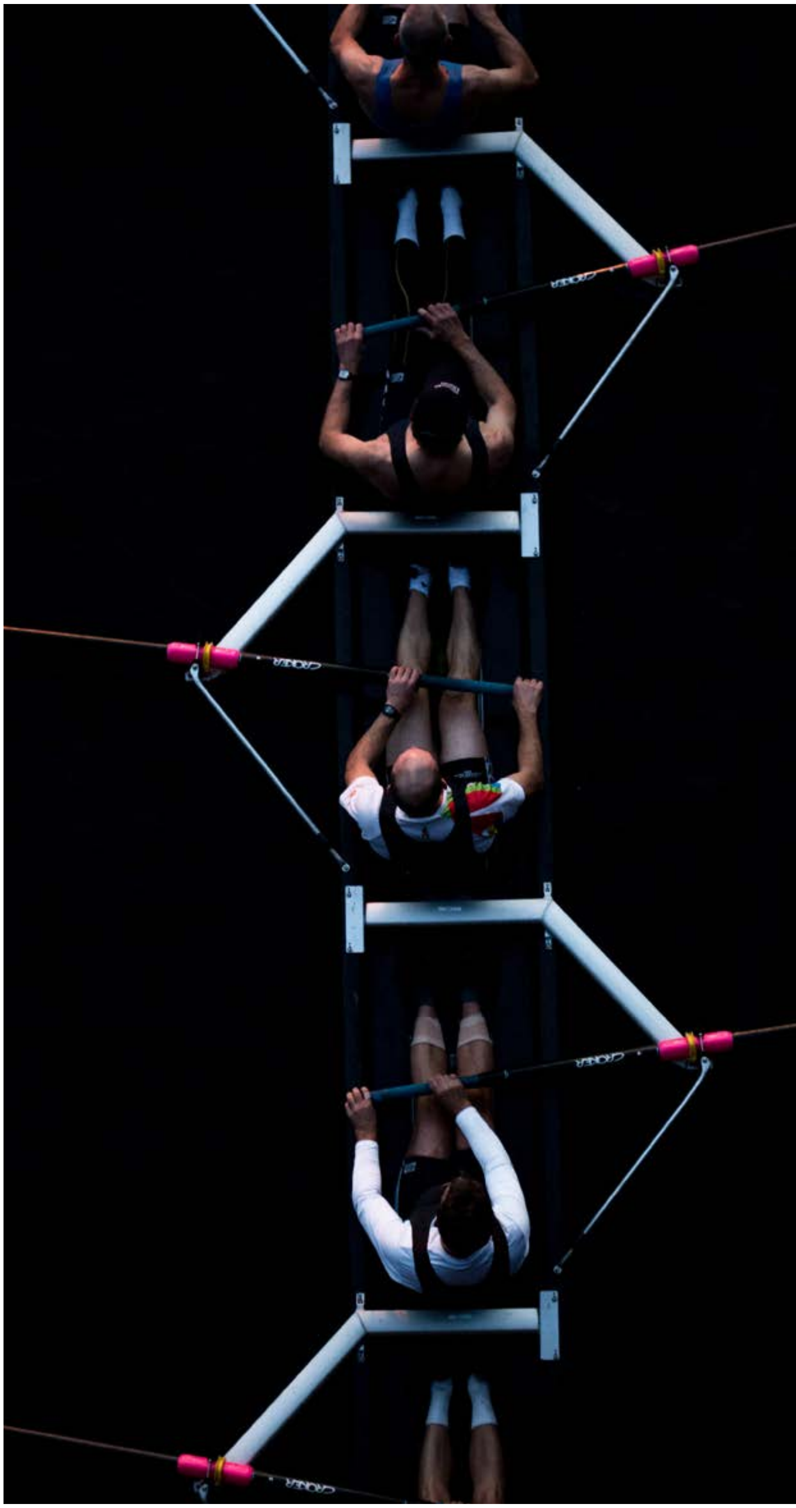
The purpose of compliance training is to:

- Ensure all staff is aware of their compliance responsibilities
- Reduce risk caused by non-compliance
- Remove legal liability from the organisation in the event of malpractice
- Protect the organisation's reputation
- Create a better workplace culture

Training should cover internal company regulations and external laws. Priority training should be given to any risk areas that may make the company more vulnerable. Ensure training is covered in these areas first so that control measures can be put into place sooner.

Other compliance topics to include in training are:

- Anti-harassment and discrimination
- Workplace violence
- Workplace safety, workplace hazards
- Diversity, Inclusion
- Conflicts of interest
- Bribery
- Reporting violations



BEST PRACTICE 6

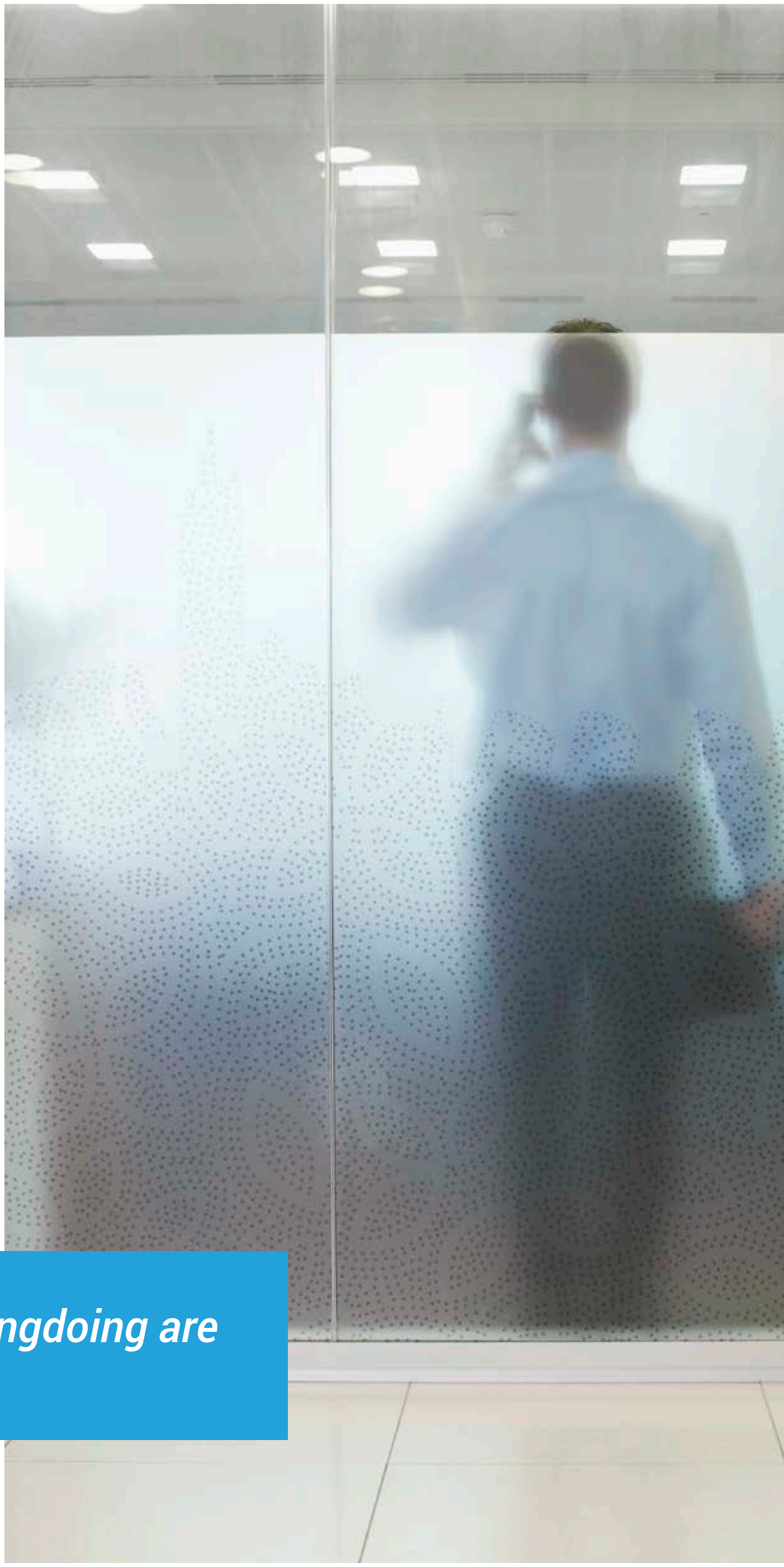
Confidential Reporting

The ability for all stakeholders to confidentially report any violation of the company's compliance program, or any policies, is crucial for the company to remain compliant with laws and regulations. Being able to understand any irregularities or violations early will provide the company with an opportunity to make things right sooner.

Allegations of wrongdoing are going to be made. What's important for the organization is that it implements a mechanism for individuals to come forward and anonymously communicate any suspicions they have of wrongdoing and illegal acts that can harm the organization.

This intake program should be efficient, reliable and properly funded if it is run internally. Most organizations will contract with an external third-party that provides an anonymous hotline and case management system allowing individuals to provide important information on alleged wrongdoing.

Being able to show regulators that the company has made every effort to ensure violations don't occur, and if they do, rectify them immediately, will lessen the damage to reputation, financial wellbeing, shareholder litigation and personal liability.



> ***Allegations of wrongdoing are going to be made.***

BEST PRACTICE 7

Investigation

Should any allegations of wrongdoing be reported, it's important that the organization's response to these reported allegations be swift and properly documented. Larger organizations will have more complex violations requiring more resources and investigation. The ability for intake, triage and investigation of these reported instances is proper protocol and shows regulators the company is doing its due diligence.

Organizations should establish an effective process with sufficient resources for responding to, investigating, and documenting allegations of violations. Reporters should be given the opportunity to report their concerns with anonymity if they choose. And having the ability to engage in an anonymous dialogue with the reporter and document all the steps taken, and communication points between all parties, demonstrates the company has strong internal controls in place.

If you conduct an internal investigation, be sure to:

- **Take all complaints seriously**
- **Avoid retaliation**
- **Develop an investigation plan**
- **Assemble your investigation team**
- **Conduct witness interviews**
- **Document everything!**

BEST
PRACTICE 8

Discipline and Incentives

With reporting and investigation of alleged misconduct, comes discipline and incentives to those who do the reporting and those who participate in the misconduct, respectively. And it's just as important that discipline be documented inside the reporting system. Regulators will ask the question "what steps has the organization taken to discipline those who have breached the compliance program, and does the discipline correspond accordingly with the violation?" This can include dismissal.

When discipline is not enforced to those who have initiated illegal conduct, or if discipline is not consistently handed out, it tells the story of a company not serious about maintaining compliance. And chances are employees aren't going to speak up when they do see something.

It's equally important to recognize those who do something right, including when someone blows the whistle on wrongdoing. When an organization recognizes someone for coming forward to report on misconduct, and rewards them, the organization proves that it wants to maintain an ethical culture, and continue to develop the culture of compliance it has built. This shows employees that the organization is serious about its ethical culture and maintaining good standards of conduct.

BEST
PRACTICE 9

Third-Party Relationships

Many larger organizations engage in relationships with foreign countries and officials, and the vast majority of FCPA enforcement actions involve payments of bribes made, not by employees or officers, but by the third-parties. Compliance programs don't stop at the four walls of the organization. They extend out to all business stakeholders – vendors, agents, consultants and foreign officials – and should ensure that all parties involved in the business have been introduced to the importance of non-compliance.

Enforcement actions of the DOJ and SEC demonstrate that third-parties can commonly be used to conceal the payment of bribes to foreign officials. As such, regulators will assess the effectiveness of an organization's compliance program as it extends out to third-parties, therefore, this type of risk based due diligence is important.

Types of third-party risks are:

- **Operational** – if a third-party experiences a cyber attack that shuts down their service, your organization may experience an interruption
- **Reputational** – if a third-party experiences a data breach, your organization may also see a decrease in customer trust
- **Compliance** – third-parties should be held to the same standard of compliance as your company
- **Finance** – loss of revenue if a third-party is unable to meet the fiscal performance requirements

Compliance programs don't stop at the four walls of the organization.

BEST
PRACTICE 10

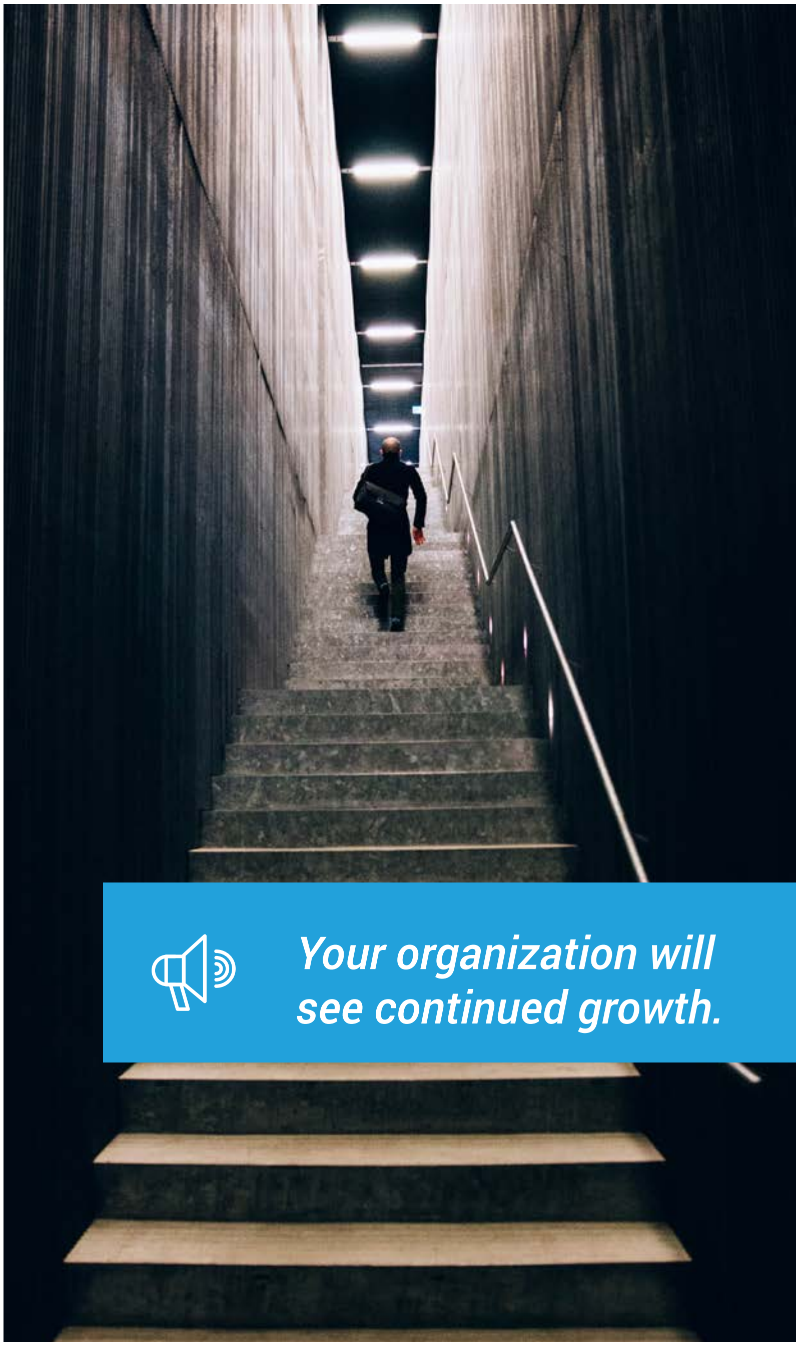
Continuous Improvement

We all know how important it is to constantly review and improve on policies and programs. Your compliance program that was created for the organization ten years ago, probably won't be sufficient enough for the organization today. You've no doubt grown in number of employees, expanded business relationships outside of the country, and governmental regulations that you need to abide by have also seen growth and change.

Your organization will see continued growth. As such, your compliance program needs to reflect the ever changing current and future corruption risks that you'll be faced with. The DOJ and SEC will evaluate compliance programs to ensure they don't fall behind in current compliance risks. They will give credit to those organizations that make the effort to create meaningful, relevant and sustainable compliance programs.

Continuous improvement involves:

- Conduct regular reviews of the goals of the strategic plan
- For each compliance goal, use the KISS method (keep it simple sir) to ensure that the goal is being addressed
- The CCO or other compliance stakeholders should put accountabilities in place and ensure each task is being achieved
- Schedule the next review of the plan and correct any issues that came up



Your organization will see continued growth.

CHAPTER 4

Summary

It's not your perspective that matters when it comes to what's important to the organization from a compliance point of view. What matters is regulators and the government's point of view. Internal perspective might form the opinion that everything is running smoothly, however, what is important to understand is what would an outsider think about our compliance program and how it's been communicated throughout the organization?

If you've covered all the factors of an effective compliance program, then your organization will be in a better position for regulatory readiness. And in some cases, courts have recognized a credible and effective compliance program as a mitigating factor when assessing remedies in the event of a breach.

info@whistleblowersecurity.com

1-888-921-6875