

10 BEST PRACTICES TO BUILD A STRONG COMPLIANCE PROGRAM



About WhistleBlower Security



Making Good Companies Better

WhistleBlower Security Inc. was incorporated in 2005 for the parent company, The Walker Group. The Walker Group began in 1968 in the chemical manufacturing sector, where it quickly became an industry leader in product innovation with a focus on environmental sensitivity. Fostering innovation while maintaining a strict policy of environmental responsibility positioned the Walker Group to develop their own in-house code of ethics and conduct, which eventually grew recognition amongst their stakeholders.

With a success history of internal reporting database development as well as a effective corporate ethics policy, it became evident that the Walker Group was well positioned to offer their WhistleBlower Secured™ model to organizations who are seeking to take their operations to the next level.

WhistleBlower Security Inc. is a Canadian based global provider of customized ethics reporting services dedicated to safeguarding businesses against risk, and committed to promoting a culture of integrity, collaboration and transparency for our employees and clients. WhistleBlower's 24/7/365 hotline, reporting and analytic solutions are combined with advanced security and data management to equip organizations with the tangible tools that will deter and prevent ongoing fraud. For more information, visit whistleblowersecurity.com.

Content

- 5 Corporate Compliance is Crucial**
- 6 Effective Compliance Programs**
- 7 Tone From the Top**
- 8 A Code of Conduct Should Reflect the Business**
- 9 Risk-Based Reviews**
- 10 Oversight and Resources**
- 11 Training**
- 12 Confidential Reporting**
- 13 Investigation**
- 14 Discipline and Incentives**
- 15 Third-Party Relationships**
- 16 Continuous Improvement**
- 17 Summary**

Something to Think About

In appropriate circumstances, DOJ and SEC may decline to pursue charges against a company based on the company's effective compliance program, or may otherwise seek to reward a company for its program, even when that program did not prevent the particular underlying FCPA violation that gave rise to the investigation.

FCPA Guidance

This statement alone should provide enough incentive for an organization to develop a strong compliance and ethics program... but please read on for more incentives.

Corporate Compliance is Crucial

Having a corporate compliance program is crucial in today's highly regulated business environment. An effective compliance program is an important ingredient of an organization's internal controls, and is an important component to detecting and preventing FCPA violations. Compliance programs should be adapted to an organization's specific industry, business, and risks.

Corporate [joint, organized, collective]
Compliance [obedience, adherence, conformity]

Effective compliance programs promote a culture within an organization that encourages ethical conduct, and a company-wide commitment to adhere to the law. Effective compliance programs should protect an organization's reputation, brand, relationship with investors, protect assets, and help in the detection and prevention of misconduct, including FCPA violations.

When the DOJ and SEC come calling, they look at whether an organization has self-reported, cooperated, and taken appropriate actions to right a wrong.

As well, considerations on the adequacy of an organization's compliance program are also taken into account in the decision on what, if any, actions should be taken. There's no mathematical formula. But three basic questions are asked:

- 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?

As an organization, you should get three out of three, and it's because you have the following best practices in place.



Effective Compliance Programs

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 than manufacturers. Healthcare entities have different risks compared to the education industry. An effective compliance program should take into account these differing business needs.

The DOJ and SEC recognize that organizations need to consider different factors when it comes to putting together a compliance program. Large, mega corporations are going to have many more factors to take into consideration compared to small and medium sized businesses. But one thing that does ring true to any organization, any size, is that a check-the-box mentality is just not complex enough to satisfy the DOJ and SEC. No matter what the organization, a compliance program that is thoughtfully laid out, designed carefully, implemented purposefully, and enforced fairly organization-wide should help the organization detect and protect violations that do occur, and help them make fixes appropriately.

“There’s no such thing as a company that doesn’t have any wrongdoing. That company does not exist.”



Tone From The Top

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 themselves, how can proper business conduct possibly filter on down the funnel?

A compliance program begins with directors and senior management setting the proper tone for the rest of the organization to follow. Just like children from their parents, 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 come knocking and see 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.

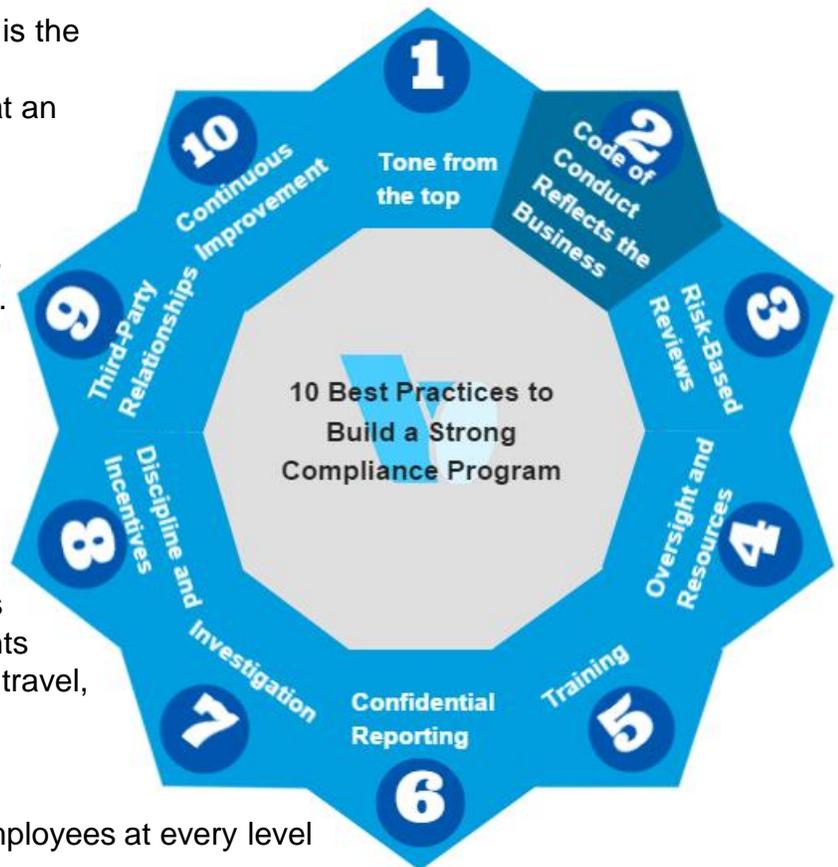


A Code of Conduct Should Reflect The Business

We've often heard that the Code of Conduct is the foundation of an organization's compliance program. 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 local languages for employees and vendors across the world. If they 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.



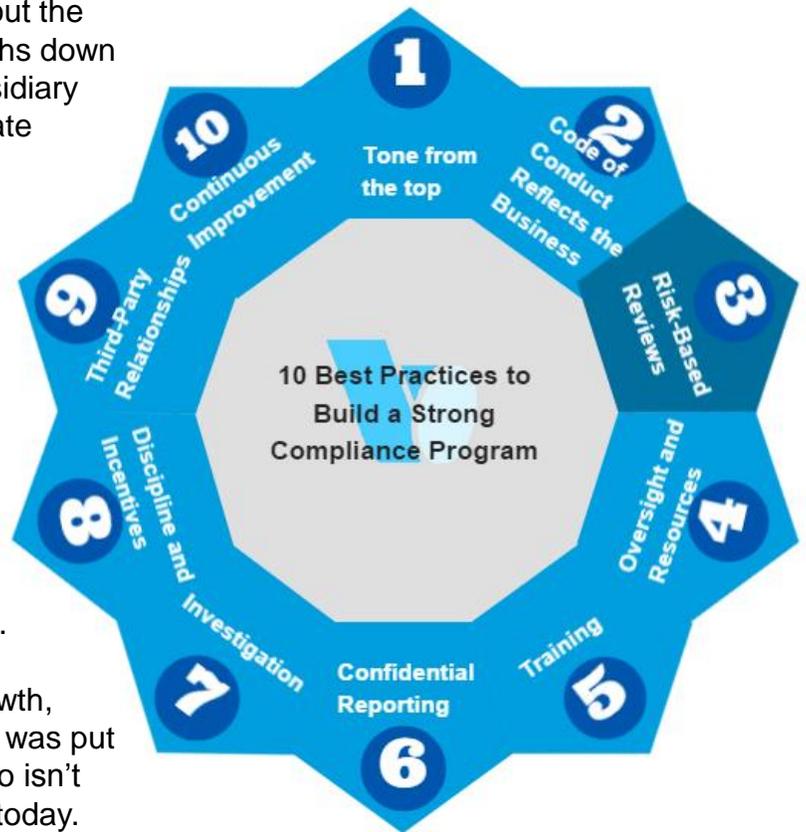
Risk-Based Reviews

Here's a sure fire way to get yourself in trouble with the FCPA:

You've got a compliance program that would score an A if it was so marked. It's been communicated throughout the organization and then left. But a few months down the road, the organization acquires a subsidiary in a foreign country yet fails to communicate the compliance program with the new foreign employees. These employees continue to operate in the way they are accustomed. And now the organization finds itself in violation of the FCPA.

It's a situation that could have been stopped with a bit of due diligence. An organization is a living, breathing organism. As such, compliance programs should also be treated in the same way, changing with the organization.

Companies change over time through growth, mergers and acquisitions. That policy that was put together for the organization five years ago isn't going to work with the same organization today. A company needs to periodically evaluate its compliance policy and codes on the basis of a risk assessment addressing the individual circumstances of the company at that time and into the near future, tailoring it to that organization's unique risk profile.



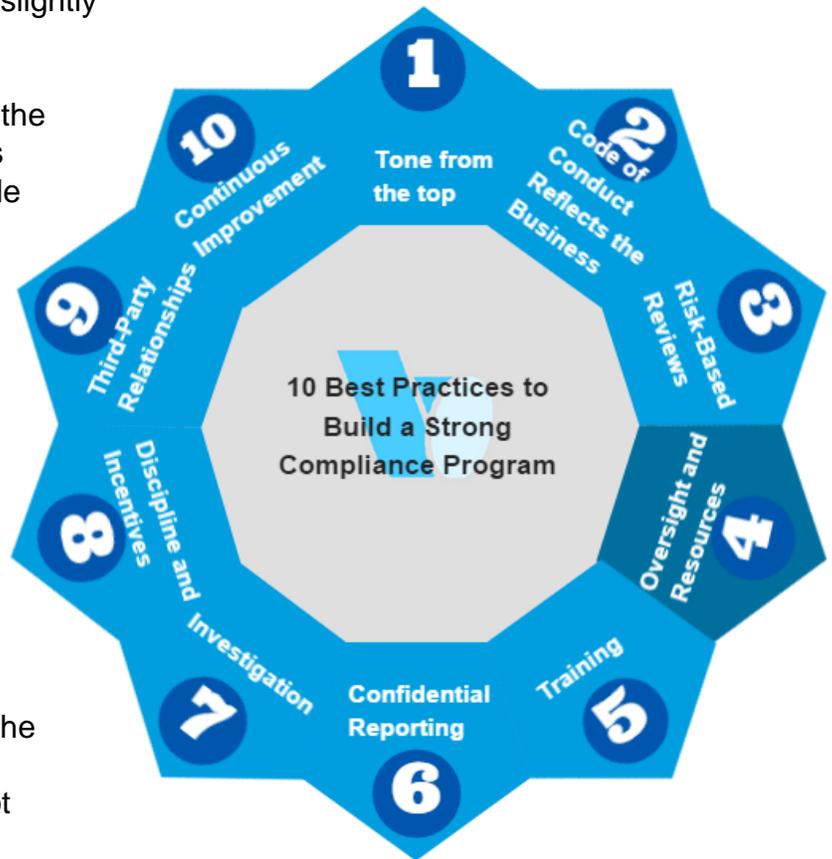
Oversight and Resources

Not that long ago an organization’s chief compliance officer was a function who kept track of policies and procedures and annual training. In some organizations, things are a little different now. The CCO’s role is slightly elevated now, on par with general counsel.

But one thing hasn’t changed. The CCO is the organization’s champion of the firm’s ethics and compliance program, inside and outside the organization. There is an expectation that the person responsible for compliance is of significant stature and seniority, that they will be taken seriously and have direct access to the board of directors.

Compliance programs need resources. An under-resourced program is likely to get the snub from the government. It’s likely to be perceived as having lack of commitment from senior management. As well, it sends a message across the organization that the CCO and the Program are just not priorities and the obligations they are trying to portray are not important.

Compliance programs need to be positioned appropriately company-wide, otherwise compliance is the last thing on employee’s minds, especially those working in foreign countries.



Training

The ethics and compliance program isn't supposed to be a secret.

Training and communication is what puts things into action and starts the ball rolling. It raises awareness and instills knowledge. The DOJ and the SEC, should they come knocking, will evaluate whether or not an organization has taken steps to ensure that policies and programs have been communicated throughout the organization, from the bottom to the top. 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.

It also means more than just a computer based program pushed out to all employees. Some employees, executives and business intermediaries may come into contact with foreign officials, and training via a computer program may not be sufficient. Will they know what's required of them?

There are individuals in organizations who are doing battle on the front lines and are more likely to come into contact with bribery and corruption from foreign officials. These employees need more comprehensive and frequent communication on the compliance program in order to prepare them to protect the organization from exposure under the FCPA.



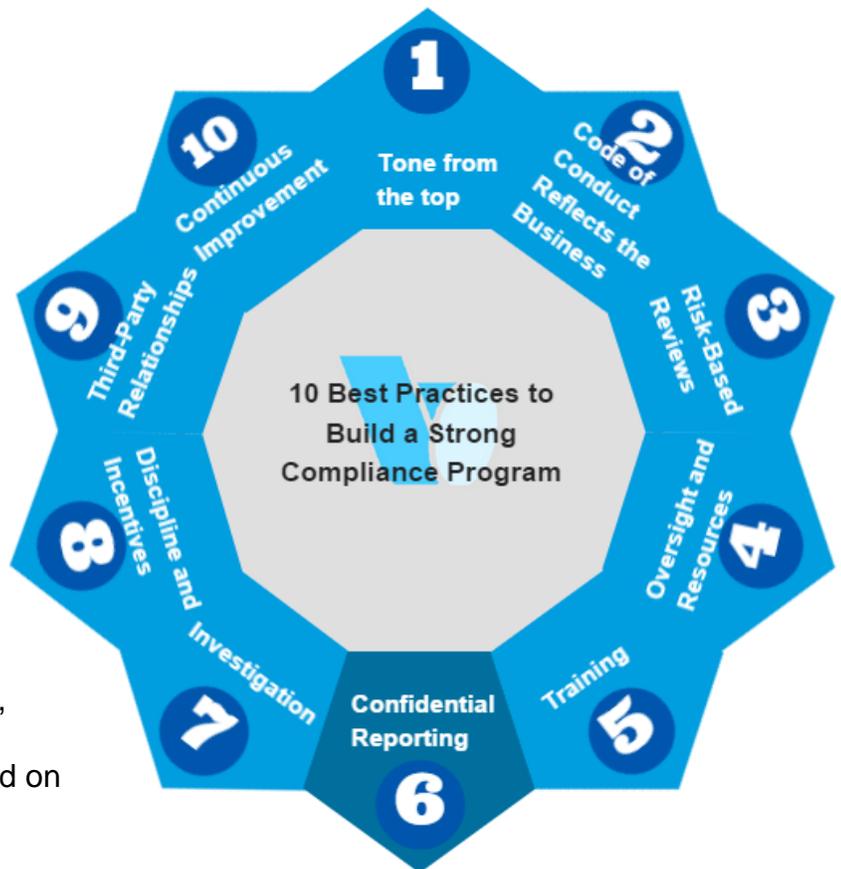
Confidential Reporting

A company should have an effective system for confidential internal reporting of compliance violations.

Allegations of wrongdoing are going to be made. A well thought out compliance program is going to, no doubt, raise red flags that require looking into. 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's 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.

Whichever way an organization decides to go, Internally driven or externally provided, government entities will award appraisal based on its existence and overall efficiency.



Investigation

It's important, also, that the organization's response to reported allegations is also properly documented. The bigger the organization, the more likely there will be instances of wrongdoing that need to be reported. The ability for intake, triage (if you will) and investigation of these reported instances is proper protocol.

Organizations should establish an effective process with sufficient resources for responding to, investigating, and documenting allegations of violations. The larger and sophisticated the organization, the bigger the expectation to have more resources devoted to compliance, compared to a smaller company.

Let past scandals and their outcomes be a lesson for today's business practices. Using these past instances to update internal controls and compliance programs, making them stronger, shows government entities that appropriate time and resources have been allocated to ensure the overall efficiency of an organization's compliance program.

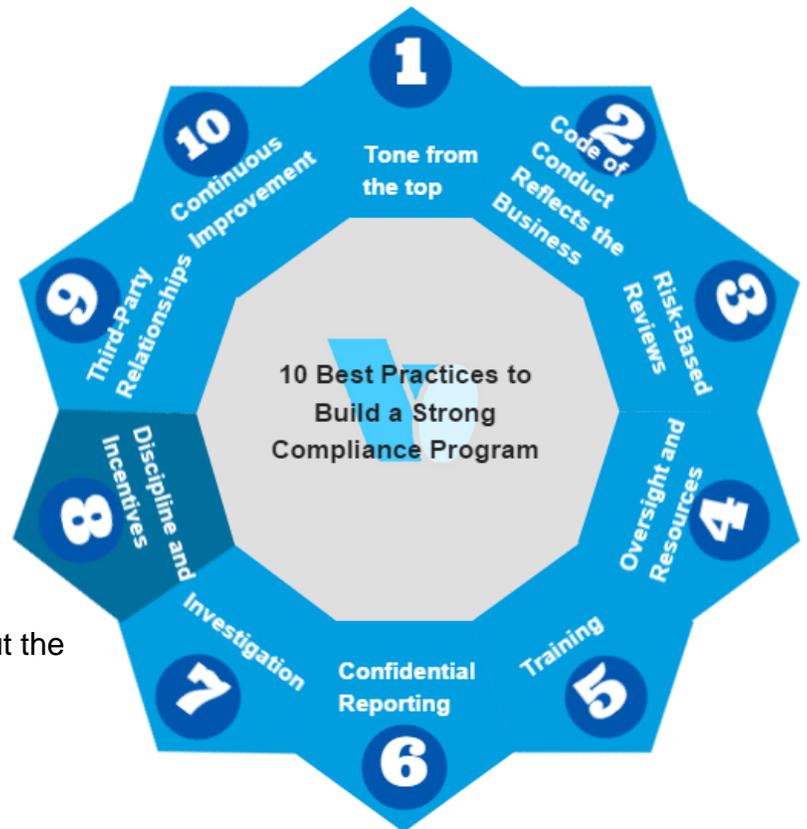


Discipline and Incentives

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 includes dismissal.

On the other hand, too, is the importance to recognize those who do something right. When an organization recognizes someone for coming forward to report on misconduct, and rewards them, the organization can also use this as a means to continue the culture of compliance and communication of compliance throughout the organization.



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, risk based due diligence is important.



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, like every breath you take, is going to expand and contract. 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 into the depths of yesteryear where they become stale and stagnant. They will give credit to those organizations that make the effort to create meaningful, relevant and sustainable compliance programs.

After all, A is for Effort!



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 the government's point of view.

From inside the four walls of your organization, you might perceive that everything is running smoothly - i's are dotted, t's are crossed – and you trained all employees on the compliance program three years ago. However, what's important to understand is “what would an outsider think about our compliance program and how it's been disseminated throughout the organization?”

Put aside all of your, and your organization's, perceptions on how you think your compliance program should be put together. Instead, try to think like an outsider, the regulators, and what their perception of your program would be. If you've covered all the factors of an effective compliance program, then when regulators come knocking at your door, your organization will be in a better position for regulatory readiness.

BUILD AN ETHICAL WORKPLACE

-  Comprehensive services provide everything you need to implement your ethics reporting program
-  Oversight into your operations, wherever they are in the world
-  Limit exposure to risk | protect your organization and your employees
-  Certification to ensure your team is educated, protected and secure
-  Education to provide tools to support your employees
-  Assessment and Consulting to enable you to define your needs for reporting, education and training
-  Enhance relationships and encourage transparency within your organization

WhistleBlower Security supports your efforts to create a more transparent, accountable and ethical work environment.

Learn about the customized service platform we can provide for your business and how to become WhistleBlower Secured™

GET IN TOUCH WITH US!

Call
1-888-921-6875

Email
info@whistleblowersecurity.com