ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Creating a Compliance and Ethics Program from Scratch

Compliance and Ethics


ETHICS


ETHICS

CHEAT SHEET

- ***Survey and assess.*** Use the company's organization chart and latest annual report to map out key risks associated with the business and who takes care of the risk. It's important that such an assessment be done on an annual basis to tailor the compliance and ethics program to the growing needs of the company.
- ***Double check.*** The company should, as part of the compliance and ethics program, take due care to ensure that individuals with substantial authority do not engage in illegal activity or unethical conduct. Support these policies by building in a process of due diligence on employees who are promoted to senior positions.
- ***Education is key.*** Compliance and ethics training is only as good as the policies on which it is based. Work with your internal communications team to launch policies, provide snippets of information, and more. In addition, record company policies and update material on an annual basis.
- ***Disciplinary action.*** For employees — and regulators — to believe in a compliance and ethics program, it is essential that the company provide a rational procedure for enforcement. Have one person from the compliance and ethics team be responsible for internal investigations, and encourage a partnership with human resources.

Congratulations! Your company has recognized the need for a dedicated compliance and ethics function and you have been chosen to lead it. You have three months to present a plan of implementation to the company's audit committee. You marshal resources, order a review of company policies, investigate how your foreign intermediary was on-boarded, pay top dollar to several technology providers to provide you with compliance tools, and start off the compliance and ethics function. At the end of the second month, you realize that each action item you undertook has opened up a Pandora's box and that you are at a loss as to what to report to the audit committee.

Back up.

No matter how big or small a company is, for a new ethics and compliance program to succeed, a thoughtful, structured program will reap rewards, not only in the form of appreciation from the board, but also in the form of acceptance from regulatory bodies, clients, and the supply chain.

So let's start at the very beginning.

What is a compliance and ethics program? Modern compliance and ethics programs are policies, procedures, and systems established by companies to attempt to prevent, detect, and respond to violations of law, company policy, and ethical standards by employees and others. The modern form of the compliance and ethics program originated in the United States when several corporate scandals led to rethinking how compliance programs should be implemented. Beginning in the mid-1970s, many government agencies noted a lack of holistic programs that would ensure that a company had adequate policies and procedures to enable compliance with US laws. Ultimately, 1991's US Federal Sentencing Guidelines, through its introduction of incentives for compliance with the laws, led to the framing of the hallmarks of the modern ethics and compliance program. However, it did not spell out what a compliance program should consist of. It is a guideline that tells you, if you

were to follow these rules, whether there is a good chance that any potential penalties would be mitigated in the event of an investigation.

It is not just in the United States. The UK Bribery Act, for example, requires companies to demonstrate appropriate procedures to ensure compliance with the law. Once upon a time, it may have been adequate for companies to provide a tracker with compliance statistics, but no longer. From recent US Foreign Corrupt Practices Act (FCPA) enforcement actions, to the much-debated DOJ Evaluation of Corporate Compliance Programs, there is much to be said for setting up a thoughtful, values-based compliance and ethics program that goes beyond tick-the-box compliance and utilizes the tenets of the modern compliance and ethics program.

Tenets of a compliance and ethics program

The US Sentencing Guidelines provide a formula for calculating an organization's criminal fine based on the seriousness of the offense, and the presence of mitigating and aggravating factors. The mitigating factor that received the most attention was whether an organization had "an effective program to prevent and detect violations of law." The guidelines have evolved since 1991, notably to expand the scope to a compliance and ethics program. A company's compliance and ethics program should contain these key principles:

1. **Written standards:** A company must have compliance standards in the form of a code of conduct and underlying policies.
2. **Tone from the top:** The board of directors must be knowledgeable about the content and operation of the ethics and compliance program, and must exercise reasonable oversight of that program. The management should assign "high-level personnel" in the compliance and ethics department to oversee compliance with such standards and procedures.
3. **Risk assessment:** Any compliance and ethics program must be tailored to the specific risks that a particular company faces owing to its business, strategy, and location of operation, to name a few.
4. **Due care:** The company must take care to ensure that adequate due diligence is conducted on senior employees to ensure unethical conduct is detected, and that only employees of high integrity are recruited, especially to senior roles.
5. **Training and communication:** The company must undertake planned and targeted training for employees focused on identified compliance risk areas.
6. **Monitoring and auditing:** The company should have a benchmarked process for reporting violations and review of the compliance and ethics program.
7. **Enforcement and discipline:** There should be uniform consequences for violations by employees and concurrent policy changes.

Understanding the lay of the land, AKA risk assessment

In short, risk assessment means that different companies have different compliance needs and their programs need to be tailored based on the business they follow. Spend some time understanding how compliance is currently managed in the company. For example, does the company operate in a regulated industry like healthcare or financial services? Use the company's organization chart and latest annual report to map out the key risks associated with the business and who takes care of each risk. Does the company have dedicated compliance experts for various functions? How do these compliance experts stay abreast of the applicable laws and regulations? Do they need any additional resources? Undertake a survey and based the results, make an assessment of the areas

that need additional focus.

You could follow this structured method of risk assessment, with the assistance of your colleagues in the risk management team.

- Assemble a multi-functional team (legal, finance, internal audit, risk management) to kick-off the process.
- Obtain the most recent company risk assessment or risk factors published in SEC filings.
- Obtain the current year's internal audit plan.
- Identify a compliance coordinator for each business unit, subsidiary, and country/geographical area. This will form the overall compliance committee. It is key that compliance not be limited to legal/finance as business is where risks are on the ground — where the people are. Similarly, risks need to be localized for additional buy-in.
- Prepare a questionnaire with risk scoring to be circulated to business and subsidiaries to identify additional risks.
- Review the questionnaires and review risk scores. Discuss risk factors and categorize risks.
- Identify mitigating measures and convey to the compliance coordinators for implementation.
- These risks must be discussed during quarterly compliance review. Emerging risks also need to be identified.
- Prepare a plan on the basis of risk categorization.

The outcome of this activity, which should be done on an annual basis, is that the compliance and ethics team is able to identify the key risks associated with the business, which can help you tailor the compliance and ethics program accordingly.

Enlist board and management support, AKA tone from the top

A compliance and ethics program cannot exist in a silo, to be the sole responsibility of the compliance and ethics team. It must be an organization-wide effort, and must be absorbed by everyone from the chairperson of the board to the employees. For example, the board of directors or any supervisory body must be trained on the company's compliance and ethics program. The US Sentencing Guidelines require that an organization's board be knowledgeable about the content and operation of the ethics and compliance program, and that it exercises reasonable oversight of that program. The 1996 Caremark[1] decision was seminal in ascribing to corporate directors an affirmative duty to establish, and exercise oversight over, some form of internal compliance activity (e.g., an organizational corporate compliance program) that is subsumed under their core duty of care.

1 In Re Caremark International Inc. Derivative Litigation 698 A.2d 959, 1996 Del. Ch. LEXIS 125 (Del. Sept. 25, 1996) {960}.

Boards must assure that the "information and reporting systems exist in the organization that are reasonably designed to provide to senior management and to the board itself timely, accurate information sufficient to allow management and the board, each within its scope, to reach informed judgments concerning both the corporation's compliance with law and its business performance."

This oversight obligation is subsumed under the core duty of care. The standard for breach of this oversight obligation is bad faith (i.e., that the directors knew that they were not discharging their fiduciary obligations). Subsequent decisions have drawn a distinction between an inadequate or flawed effort to effect fiduciary obligations, and a conscious disregard for those duties.

Until recently, there was very little guidance under US law as to what steps the board was expected to take. However, the publication of the DOJ's Effectiveness Questions implies the following questions will be asked of the board and senior management in the event of an investigation:

- What compliance expertise is available on the board of directors? Are there board members who have experience in overseeing or managing the compliance and ethics portfolio?
- Have the board of directors and/or external auditors held executive or private sessions with the compliance and control functions? Have the compliance and relevant control functions had direct reporting lines to anyone on the board of directors?
- What types of information have the board of directors and senior management examined in their exercise of oversight in the area in which the misconduct occurred? What types of relevant audit findings and remediation progress have been reported to management and the board on a regular basis?
- How often does the compliance officer meet with the board of directors? Is management present?
- How have the board and management followed up?

You should, therefore, work to ensure that regular meetings with the board are scheduled for the compliance and ethics function, including time with the independent directors, if any. In the beginning, share a risk assessment with a mitigation plan and then report on the progress made on implementing the program. Meet the directors once a quarter and schedule an annual training for the board on compliance and ethics aspects.

Check, double-check, AKA due care

While every employer undertakes background checks on new employees, until recently, it was not too common for additional checks to be done as employees moved to senior positions within the company. If it is not the practice to conduct background checks on senior personnel upon promotion, it is prudent to initiate the process. Prior to this, put your house in order. Initiate a background review into the compliance and ethics team. The compliance and ethics team requires professionals whose integrity and ethics cannot be questioned. Additionally, review whether the compliance and ethics team includes sufficiently experienced professionals. Having team members who have some amount of background and experience in the company will always come in handy. Balance this with new hires in specialized areas of focus for the company.

The company should, as a part of the compliance and ethics program, take due care to ensure that individuals with substantial authority have not engaged in illegal activities or other conduct inconsistent with an effective compliance and ethics program. Clearly drafted and disseminated corporate policies can serve as a record of the company’s diligence in selecting employees holding sensitive positions. Support these policies by building in a process of due diligence on employees who are promoted to senior positions. Annual conflict of interest certifications also help detect any situation of conflict. A positive screening may not always lead to the outcome that the employee must be let go — for example, an employee may be identified as a Politically Exposed Person (PEP)[2] and certain steps may have to be taken, including recusing the employee from certain projects to stay within the boundaries of the law. Ensure that employee policies also detail a requirement to self-report criminal offenses.

2 A politically exposed person (PEP) is defined by the Financial Action Task Force (FATF) as an individual who is or has been entrusted with a prominent public function. Due to their position and influence, it is recognized that many PEPs are in positions that potentially can be abused for the

purpose of committing money laundering (ML) offences and related predicate offences, including corruption and bribery, as well as conducting activity related to terrorist financing (TF).

Manage base policies, AKA review the code of conduct

The code of conduct is the underlying policy for any compliance and ethics program. Chances are that if the company is listed or otherwise regulated, it would already have a simple code of conduct in place. **In many companies, the code of conduct is a document that is seen rarely and read even less frequently. Chances are that it was drafted by a lawyer and is excessively legalistic as well. However, this is the one document that is the motherlode for all the steps you will take in your program.** Hence, it is imperative that it conveys the basis for your compliance and ethics program; lays out the regulations applicable to the company, and provides guidance to employees on navigating tricky situations. Remember that, unlike a risk assessment, the code of conduct is available to the employees of the company. It may very well be through the code of conduct that employees are introduced to the compliance and ethics program. Hence, undertaking a review of the code of conduct and ethics should be a priority for the compliance and ethics program.

Spend some time reading the Code and understanding how it appears to the average employee. You can use the code to convey the company's value systems. An introduction from the CEO is often perceived to set the tone. Intersperse the text with FAQs and pointers. Highlight the options available to employees to raise concerns. Have a page devoted to the expectations that the company has from each employee, manager, or officer of the company. Avoid the paper copies and opt for an online portal that employees can click-through. If the workforce consists of employees on the go, consider having a mobile application as well. Remember that if the company is in a regulated sector, there may be some specific regulatory requirements to be incorporated in the code of conduct. The code should convey the company's position on key regulatory matters and indicate what options are available to employees to raise concerns if there are any violations.

Training and communication, AKA showcase your hard work

Much of a good compliance and ethics program consists of educating employees about the things they should and should not do. While we churn out innumerable policies and create the perfect compliance structure, it is essential that employees are trained on the policies that apply the most to them. Some of the key trainings that employees should undergo are on the code of conduct and ethics, anti-bribery policy, discrimination, anti-sexual harassment, etc. Some jurisdictions may also require you to have employees of certain seniority undergo training in certain areas. If your company is in a highly regulated industry, such as healthcare or insurance, it may require specific training as well. So how do you make sure that you are educating the right people? After all, the first question in the training and communications section of the DOJ effectiveness questions is on risk-based training.

Risk areas of focus

Anti-bribery: Review the 2012 DOJ-SEC FCPA Guidance.

Antitrust: Review the International Chamber of Commerce Antitrust Toolkit.

Cybersecurity: Check the Securities and Exchange Commission's statement on cybersecurity.

Data protection: Read up on the European General Data Protection Regulation implementation.

Human trafficking: Review the UK Government's guidance on the Modern Slavery Act, 2015.

Third-party management: Review Transparency International's guidance on managing third party risk.

Mergers and acquisitions: Review the DOJ's Effectiveness Questions to assess what needs to be baked into your mergers and acquisitions practice from a compliance and ethics perspective.

Sector specific compliances: Export controls (review the Bureau of Industry and Security's Manual on setting up an export compliance program).

Key policies to implement:

- Code of conduct and ethics;
- Whistleblower policy;
- Anti-bribery policy and,
- Conflicts of interest policy.

Creating a plan

- Identify the key risk areas, based on the company risk assessment.
- Identify all the risk areas where training is presently carried out in the company, including the frequency and the target audience for the trainings. This is important because it is not only the compliance and ethics team conducting training. While it is likely that the compliance and ethics team may conduct training on the code of conduct or on antibribery, training on discrimination and sexual harassment are probably conducted by the human resources team; and training on information security and data privacy by the subject matter experts in these departments. All these areas are key to the compliance and ethics program. Use available resources in the company to bolster the training and communication plan.
- Create a multi-year training and communication plan which should cover risk areas, recipients of training, mode of training, frequency of training, and who maintains the records.
- Publish a copy of the training and communication plan to the compliance committee and prepare a report consisting of training numbers for employee, feedback from employees, and next steps.
- Have the chief compliance officer or an external consultant train the board of directors on key company policies.

Pro-tips on C&E implementation

Be your own best cheerleader

If your company is setting up a new program, you are likely to face resistance or a lack of awareness about what a C&E program is. Be enthusiastic about your portfolio and miss no opportunity to talk about it to your larger team. Utilize your own legal team meetings, quarterly town hall discussions,

and internal conferences to push the need for the program.

Create a governance structure

Set up the system of compliance liaisons in each country and business unit. They will be your eyes and ears on the ground. Have them cascade compliance concerns to your team. Make them the evangelists for the compliance and ethics program within their team. Give them credit for this role in their performance evaluation.

Keep all avenues of communication open

Maintain email, open door, and hotline communication and be curious about all that your company is doing.

Records, records, records

Make sure you have noted and saved all the work you have done in training and communicating your compliance and ethics program.

Keep learning

There are plenty of free and paid resources on compliance and ethics. Invest in the right learning tools. Encourage the compliance and ethics team to take e-learning and live courses. Update internal clients and the compliance committee on regulatory updates and it costs nothing to keep abreast of the latest trends and hot topics.

Creating the training

Compliance and ethics training is only as good as the policies on which it is based. This starts from the time a policy is created. Policies may be created for multiple reasons, to comply with new regulations, to showcase the company's values, or to reduce the company's exposure to risks. However, policies should be comprehensible to the average employee. Have a standard format. Include comprehension aids such as FAQs, quick links, etc. Have policies available on a company portal. While a full-blown review of policies should be on the charts, start off with the areas that you want to train employees on and review the current policies around it. Make sure the policies are in sync with the concepts that you are trying to teach your employees. If there are any inconsistencies, resolve them through dialogue with other teams. Now you are ready with the base material for the training.

Work with your internal communications team if the company has one. A common communication tool is mailers. These can be used to launch policies, provide snippets of information, and more. Targeted live training is arguably the most effective means of training, but the length and content of the session need to be carefully considered. Video based training can be used for larger audiences. Quizzes can help in testing the knowledge of the employee. Try to include redacted versions of actual misconduct that happened in your company and what the company did about it.

Recording the training

Keep records of all the training and communication material disseminated by the compliance and ethics team. Some companies create an intranet portal to upload past communication mailers, links to policies, helpline service, etc. Additionally, ensure that the compliance and ethics team maintains a record of the employees who attended the training session. At an early stage, it may be as basic as a physical copy of the attendance sheet.

Reviewing the training

Review company policies and update the training material on an annual basis. This is because laws change very frequently and enforcement actions may necessitate reviews to policies and procedures. Feedback forms and other information about the training already provided can strengthen the review process.

Monitoring and auditing or multiple pairs of “eyes”

Preventing violations involves constant monitoring of activities that have the potential to violate legal obligations. For example, including appropriate system controls, providing options for stakeholders to raise issues, annual audits of the compliance activities for the year, analyzing patterns of whistleblower complaints, and undertaking appropriate policy and process improvements. Here, we review some of these key aspects.

While is it important to have a strong code of conduct, and effective processes underlying it, it is crucial to have a multitude of ways by which employees can raise concerns of violations of the code, in a confidential and anonymous manner. While third-party whistleblower hotlines may be commonly used in any compliance and ethics program, do not discard the facility to raise issues through email, or even a handwritten letter. Some jurisdictions are not comfortable with overseas hotlines. For those, it may be better to provide other options. It is important to review the whistleblower policy so that employees know what they can report and what happens once they do. Institute a process whereby all violations of the code of conduct and ethics are brought up to the compliance and ethics team so that you have complete oversight. Ensure governance by instituting a report to the audit committee of the key matters and any trends. These trends are later fed into the risk assessment cycle along with associated process improvements. If you outsource your whistleblower hotline, ensure that a senior member of your team has ownership over the process and manages the issues raised on a day-to-day basis. Remember that the company whistleblower policy is only as good as the company’s stand on anti-retaliation, and you must work with local human resources teams to ensure that there is no retaliation and employees are comfortable speaking up.

Also, while a compliance officer approves policies, it is important to also check what the underlying controls, payment systems, and certification under the policies say. It is especially important to train your employees who interface with employees at the time of payments. Create a recurring plan to have an internal audit team review the underlying controls and see if anything additional needs to be added.

Enforcement and discipline

For employees to have faith in the compliance and ethics program and for regulators to believe in it, it is essential that the company have a rational procedure for enforcement and discipline. This includes, for instance, having a structured internal investigations process, consistent disciplinary action, and a focus on apt reward of ethical behavior.

How do you demonstrate to employees, and to regulators, that the company is interested and invested in reviewing and correcting lapses? Undoubtedly, by having a robust and empowered internal investigation function. To start off, have one person from the compliance and ethics team be responsible for internal investigations. The compliance and ethics team will be working closely with the human resources function, as they are likely to be dealing with employee concerns on a regular basis. It is worth having them report trends to you for onward reporting to the audit committee. An uptick in the number of wage-related inqueries might lead to a rework of your compensation policies, for instance.

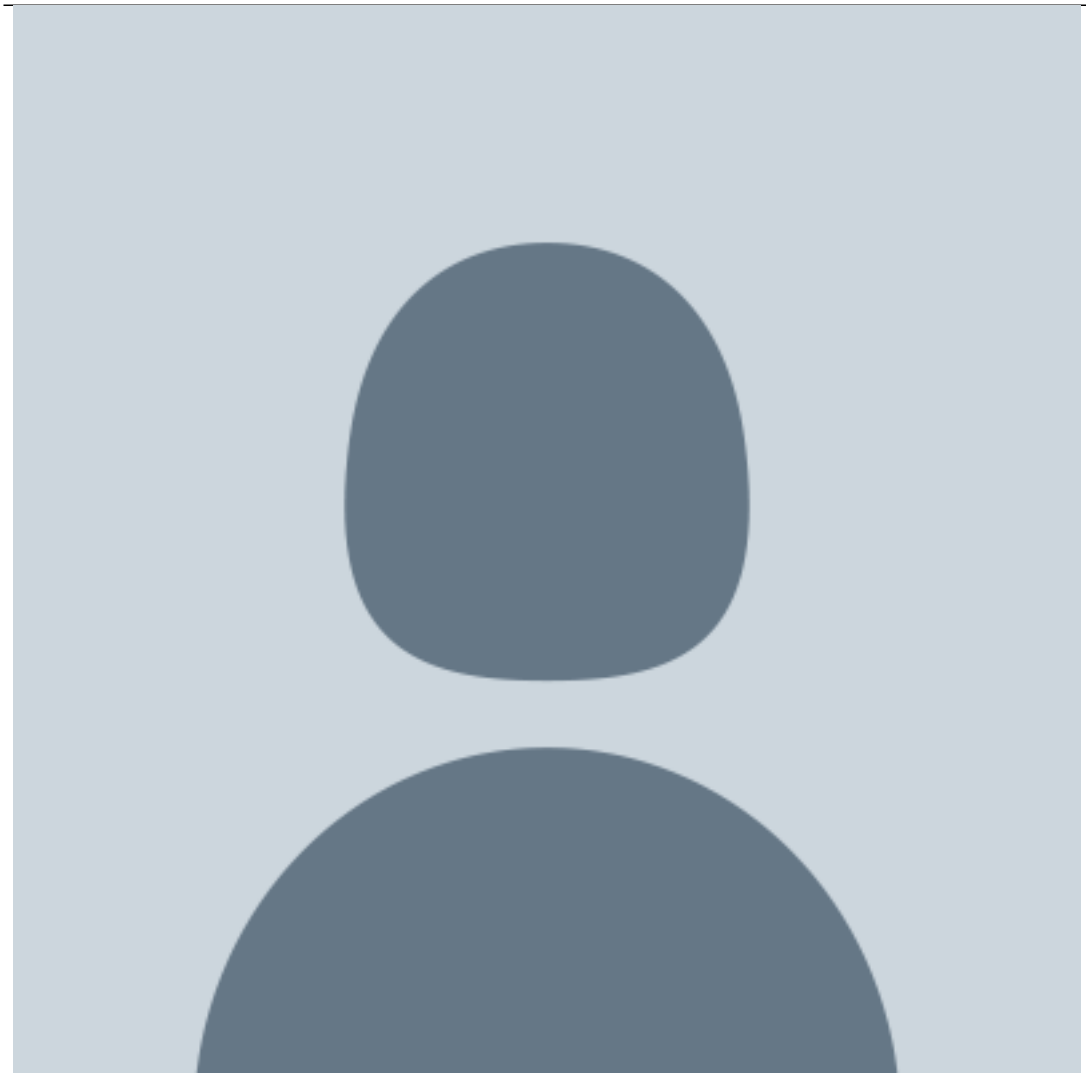
The DOJ's Effectiveness Questions also stress on the aspect of appropriate and consistently applied disciplinary actions. Of course, the Effectiveness Questions are in the context of an enforcement action. However, the questions that they ask range from the number of times such incidents occurred and what disciplinary action was undertaken, to whether the company held a manager accountable for what his team member did and what were the disciplinary actions undertaken. Hence, it is important to review the disciplinary action matrix that your HR team applies and ensure that you have visibility over the disciplinary actions taken in the context of code of conduct violations.

Additionally, it is worth reviewing incentive structures in place. Highly skewed incentive structures can cause ethical issues. On the other hand, having an incentive for acting in an ethical manner may also be a concern — you want to reward those who go above and beyond and assist the company in the compliance and ethics sphere. Rewarding those who sign up to be a compliance liaison or including ethical behavior in the performance evaluation are efforts that can be considered.

Summary

No matter what is said, it is impossible to create a compliance and ethics program from scratch in 90 days or even a year, or to apply for an ISO 37001 certification for your anticorruption compliance program. What can be done, however, is to understand what your company's program lacks, and then commence work on fixing and improving the highest risk items. Remember, no matter if you're working on an anticorruption compliance program or an anti-money laundering compliance program, the tenets explained here are good. Indeed, the learnings from one program can often be used for the next, and your job will be made a bit easier. Keep in mind that while there is a tool for everything these days, your expertise and knowledge of the business cannot be outsourced to an entity. Identify where technology can really help you, as in the case of repetitive tasks, and identify where it is only an enabler.

Nirupama Pillai



Corporate Counsel at the Office of Integrity & Compliance

Infosys Limited

Infosys Limited is a global provider of technology services and consulting. Pillai works on designing and implementing a compliance and ethics program for the Infosys group. Prior to Infosys, she worked in private practice at Trilegal, a law firm in Bangalore, India, on their Corporate and TMT team.