THE HOW TO GUIDE ON CREATING

A Robust Ethics & Compliance Program

vault.

01

ESTABLISHING, INTEGRATING & MAINTAINING AN EFFECTIVE COMPLIANCE PROGRAM

Every company is unique, and they each need a compliance program to match. Risk profiles vary, and so too do the appropriate mitigation methods. This is true regardless of the size of the business, and even for multinational organizations. Management model, number of employees, industry, geographic footprint, and regulatory landscape are just a few of the many factors in play.

As such, it is important to understand that there is no single, rigid formula to which every organization could or should adhere. However, in this section we hope to offer a framework by which specific policies can be developed, and a set of considerations that might be taken into account.

ECI
BENCHMARK

In 2016, the ECI's Blue Ribbon Panel released the Principles and Practices of High-Quality Ethics & Compliance Programs report. This has since become a benchmark for constructing an effective E&C program. The objective of the original report was to focus on the five critical principles of a high-quality program (HQP), and the recommended techniques for practitioners to use when building out their own.

THE FIVE PRINCIPLES HIGHLIGHTED IN THE REPORT ARE:

STRATEGY
Ethics and compliance is central to business strategy.

RISK MANAGEMENT
Ethics and compliance risks are identified, owned, managed, and mitigated.

CULTURE
Leaders at all levels across the organization build and sustain a culture of integrity.

SPEAKING UP
The organization encourages, protects, and values the reporting of concerns and suspected wrongdoing.

ACCOUNTABILITY
The organization takes action and holds itself accountable when wrongdoing occurs.

These five principles provide the standard framework on which an E&C program should be developed. The word 'program' is crucial here: a good compliance regime will be approached as a program, and not simply as a process or tick-box exercise. This interpretation was endorsed by the US Department of Justice (DOJ) in its 2020 update to its guidelines for Federal prosecutors on the evaluation of the effectiveness of corporate compliance programs. This guidance represents the standard by which all Ethics & Compliance programs should be judged, whether or not they operate in the United States.

One of the key reasons for this is set out by Thomas Fox, who in 2020 noted the much needed alignment between compliance professionals and lawmakers. He wrote: "The 2020 Update is most welcome news for every Chief Compliance Officer (CCO), compliance professional, and corporate compliance program in the US and beyond. The reason is simple: it ends, once and for all, the clarion call for paper compliance programs written by lawyers for lawyers. The DOJ has now articulated what both the business and compliance communities have been learning—that compliance is a business process, and as a process, it can be measured, managed, and most importantly, improved."

The DOJ will measure the effectiveness of corporate compliance programs through three specific lenses. We can also use these lenses as a starting point for the development of any individual program.

THEY ARE:

- Is the corporation's compliance program well-designed?
- Is the program being applied earnestly and in good faith? In other words, is the
- Program adequately resourced and empowered to function effectively?
- Does the corporation's compliance program work in practice?

DESIGN

A well-designed program does not only set out a clear message that misconduct is not tolerated; this, alone, is not enough. In addition, a good program employs policies and procedures (including assignments of responsibility, training, and incentives) to ensure complete integration of E&C principles into the company's operations.

Finally, this must be adhered to by leadership and rank and file employees alike.

GOOD FAITH & EMPOWERMENT

Companies where leadership has a 'do as I say, not as I do' approach end up with cultures of tolerance for rule-breaking. A perception that misconduct will not be taken seriously is perhaps the most important factor in disincentivizing employees from speaking up.

This, in turn, creates more misconduct because of a lack of repercussions for perpetrators and an acceptance that 'this is how things are done here'.

WORKING IN PRACTICE

The design of a good E&C program must be based on relevant metrics (which will, again, be unique to the organization in question) identified through a risk assessment that must be continually assessed and improved.

Here the 'program' aspect of E&C comes to the fore again: good E&C isn't a one-time activity, but instead an ongoing practice.

BUILDING THE PROGRAM

E&C programs should be unique, but in order to assist in their d evelopment there are several key questions that should be asked.

THESE INCLUDE:

- How do you identify risks?
- Do you allocate time and resources appropriate to those specific risks?
- Do you constantly review and revise this risk assessment? Is it a 'living process' rather than a periodic snapshot?

BUILDING THE PROGRAM

- Are your policies and procedures easily accessible by all employees, with appropriate signposting and offline materials if required?
- Are they written in an understandable and accessible way, including in multiple languages if required?
- Can you track which policies are most accessed by employees, and are you using this data to help improve the program?
- Who has responsibility and accountability for policies and processes?
- Are you satisfied that the 'gatekeeper' positions are occupied not by compliance professionals but by subject matter specialists, for example HR, payroll, or internal audit?

vault.

TRAINING & COMMUNICATIONS

- Are the Ethics & Compliance professionals trained appropriately?
- Does training need to be extended beyond E&C, for example to managers or specific functions?
- Do some personnel need specialized training?
- Is training accessible, for example in multiple languages or in an offline format for employees not online (for example those working on oil rigs or in mining operations)?
- How do you handle transparency and follow-up during and after a misconduct incident? Do you inform employees when a member of staff is terminated for misconduct? Do you close the loop and follow up during investigations, even in the case of anonymous reports? Do employees understand the process of reporting and investigation?

TRAINING & COMMUNICATIONS

An effective and accessible incident reporting and resolution mechanism is the backbone of any compliance program. But paradoxically, whistleblowing (and especially external whistleblowing) is often cast in a negative light, for example as a disgruntled employee with a grudge against their employer. Dr. Margaret Heffernan sums up the figure of the whistleblower as follows:

“While the popular image of the whistleblower is typically an eccentric loner, the truth is more prosaic: whistleblowers are likely to be loyal employees, passionate about high standards, who go outside their organisation as a last resort when nobody takes them seriously. They aren’t defiant troublemakers; they’re disappointed believers”.

The point is, employees are your best first warning system when something isn’t right. This is especially true, as Dr. Heffernan says, of the “believers”.

According to the DOJ, one hallmark of a well-designed compliance program is “the existence of an efficient and trusted mechanism by which employees can anonymously or confidentially report allegations of a breach of the company’s code of conduct, company policies, or suspected or actual misconduct.”

There are two main factors that tend to prevent employees speaking up: lack of confidence that action will be taken; and fear of retaliation. The simple existence of a Code of Conduct is not enough to tackle this. In businesses in which there is a disconnect between conduct and culture, there is unlikely to be the infrastructure required in order to enable the transition to a more positive culture. Drawing more attention to the Code of Conduct is useless if the tools in place to expose and resolve misconduct are ineffective or non-existent.

When designing incident reporting and resolution mechanisms, we should ask the following questions:

- Is the reporting channel designed, established, and operated in a secure manner that ensures the confidentiality of the reporter's identity and that of any party mentioned?
- Have you considered alternatives to traditional hotlines that might be more accessible, such as Vault Platform?
- Is a confirmation of receipt of the report given to the reporting person within an appropriate time frame, including in the case of anonymous reports?
- Does a competent person or department follow up on the reports? Can this person maintain communication with the reporting person and provide feedback, including in the case of anonymous reports?
- Is a careful follow-up investigation carried out on the report by the designated person or department?
- Is a reasonable time limit set for giving feedback or closing the loop on the report from the acknowledgment of receipt?
- Does your case management and resolution system give you real-time data on the status of ongoing investigations and specific categories of incidents?

AND WE CAN ASK SIMILAR QUESTIONS WHEN DESIGNING MECHANISMS FOR SPECIFIC ACTIVITIES:

01 THIRD PARTY & PARTNER ECOSYSTEMS

- Do all or a specific subset of the above questions also apply to partners, suppliers, customers, or the general public?
- How do third parties or partners report misconduct to you, and how do you follow up? Is this process clearly communicated and accessible?

02 MERGERS & ACQUISITIONS

- Is an effective risk assessment process carried out during the due diligence process of M&A?
- How are any risks handled?
- How will the multiple compliance programs be integrated?

03 IS THE PROGRAM FUNCTIONING EFFECTIVELY?

- Is the program adopted top-down and bottom-up - that is, by leadership and rank-and-file employees alike?
- Who has oversight? For example, is it the Board of Directors? What experience or training do they have to ensure adequate capability of oversight?

CONTINUOUS IMPROVEMENT, PERIODIC TESTING & REVIEW

According to the DOJ, another hallmark of an effective compliance program is its capacity to improve and evolve:

“The actual implementation of controls in practice will necessarily reveal areas of risk and potential adjustment. A company’s business changes over time, as do the environments in which it operates, the nature of its customers, the laws that govern its actions, and the applicable industry standards. Accordingly, prosecutors should consider whether the company has engaged in meaningful efforts to review its compliance program and ensure that it is not stale.”

Best-practice compliance programs require practitioners to have access to continuous and real-time transactional data within the organization - even across multiple silos such as HR, ESG/CSR, and E&C. However, getting to this stage is an iterative process, and one that does not happen overnight. Organizations are not sanctioned if they can demonstrate they are moving in the right direction. The key is to ensure that everything is documented; by documenting the basis for your decisions, you can more easily explain that calculus in the event of a regulatory investigation.

AS TOM FOX SAYS:

> *“No compliance professional, compliance program or even company under Foreign Corrupt Practices Act (FCPA) investigation or scrutiny has ever been punished for making an incorrect decision where a succinct and documented business justification was in place.”*

CULTURE

The role of compliance in speak-up culture is increasingly understood not only by Ethics and Compliance professionals but also by lawmakers, as reflected in the DOJ’s 2020 update. All parties now acknowledge that the function plays a key role in helping organizations navigate the waters of bias, diversity, and equality.

Over the last 18 months we’ve seen an increased focus on the intersection between the functions of Compliance, Legal, and HR, particularly regarding the direction of a company’s culture and whether the company and its employees act with integrity.

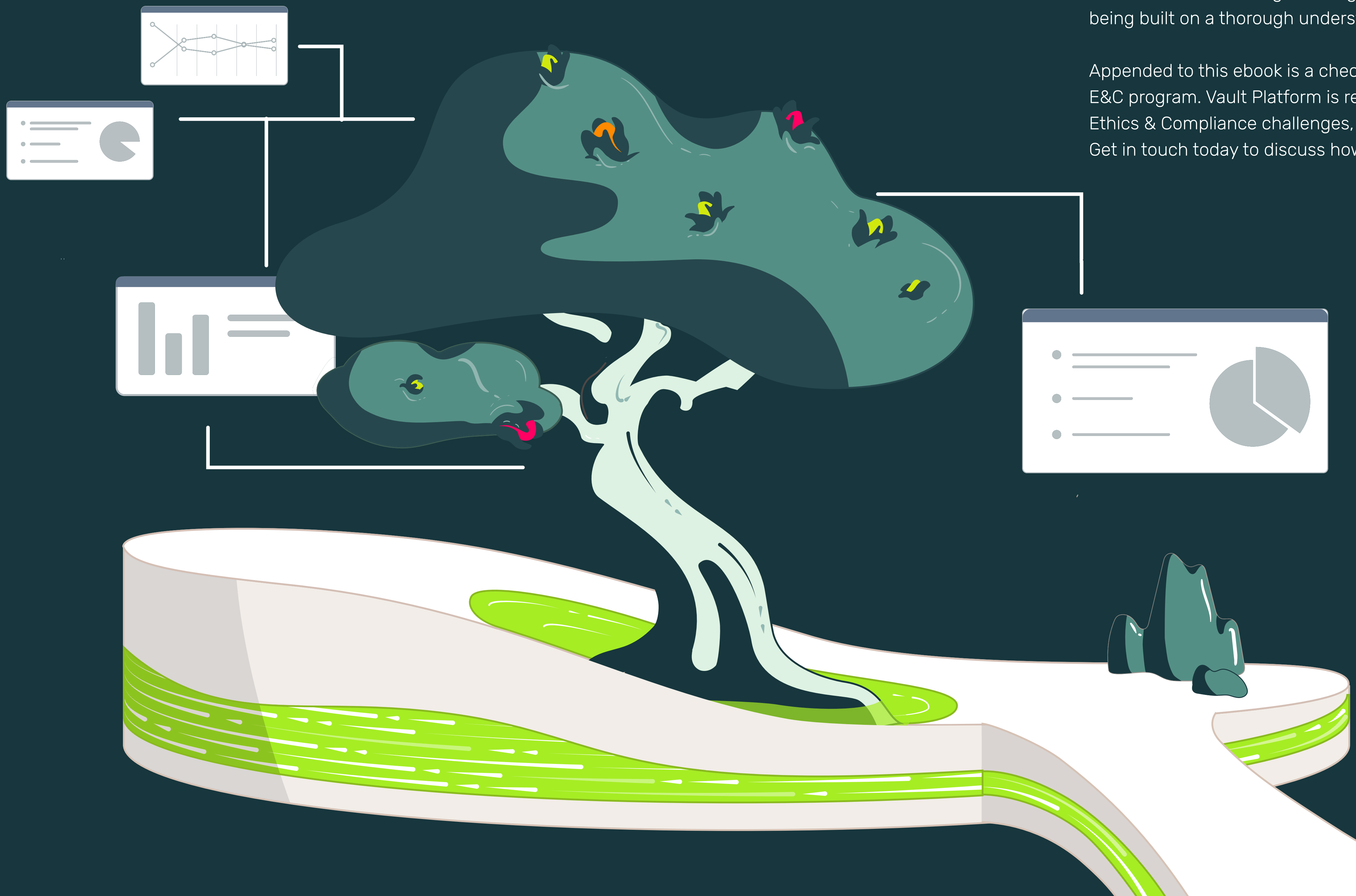
In an article for Harvard Business Review, Rob Chesnut, who was most recently Chief Ethics Officer at Airbnb, warns that it’s the end of the line for ‘canned codes of ethics’, and for companies that treat their code as just another legal box to check. Doing the bare minimum required for legal compliance is no longer enough as companies are pushed by employees, governments, and customers to step up and adopt a multi-stakeholder approach that serves social purposes as well as investor demands.

The Compliance function therefore has a powerful platform within the organization, reaching every employee and, if leveraged in the right way, becoming a powerful strategic driver.

THE ROAD TO ETHICS & COMPLIANCE

This ebook is intended to provide a foundation for the establishment of a comprehensive Ethics & Compliance program. Any such program must by nature be an evolving, 'living' project, both reactive and proactive in its nature. It must be agile enough to respond to new challenges, while being built on a thorough understanding of the modern E&C landscape.

Appended to this ebook is a checklist to aid in the development of your E&C program. Vault Platform is ready to provide turnkey solutions to Ethics & Compliance challenges, regardless of the size of the business. Get in touch today to discuss how we can help.



vault.

CHECKLIST

Does your Ethics & Compliance Program meet the Five Principles and Practices of High-Quality Ethics & Compliance Programs set out by the ECI Blue Ribbon Panel Report?

1. STRATEGY

Are Ethics & Compliance acknowledged as being central to business strategy? □

2. RISK MANAGEMENT

Are Ethics & Compliance risks identified, owned, and managed? □

3. CULTURE

Do leaders at all levels across the organization agree and understand how to build and sustain a culture of integrity? □

4. SPEAKING UP

Does the organization encourage, protect, and value the reporting of concerns and suspected wrongdoing? □

5. ACCOUNTABILITY

Does the organization take action and hold itself accountable when wrongdoing occurs? □

Does the program go beyond a 'box ticking' exercise?

1.Is the ethics and compliance program well designed? □

2.Is the program adequately resourced and empowered to function effectively? □

3.Does the compliance program work in practice? Is this measurable? □

Risk Mitigation

1.How do you identify the risks?

Risk Mitigation (continued)

2. Do you allocate time and resources appropriately to those specific risks? □

3. Do you constantly review and revise this risk assessment? Is it a 'living process' rather than a periodic snapshot? □

Policies & Procedures

1. Are your policies and procedures easily accessible by all employees, with appropriate signposting and offline materials if required? □

2. Are they written in an understandable and accessible way, including in multiple languages if required? □

3. Can you track which policies are most accessed by employees, and are you using this data to help improve the program? □

4. Who has responsibility and accountability for policies and processes? Are you satisfied that the 'gatekeeper' positions are occupied not by compliance professionals but by subject matter specialists, for example HR, payroll, or internal audit?

Training & Communications

1. Are the Ethics & Compliance professionals trained appropriately? □

2. Does training need to be extended beyond E&C, for example to managers or specific functions? □

3. Do some personnel need specialized training? □

4. Is training accessible, for example in multiple languages or in an offline format for employees not online (for example those working on oil rigs or in mining operations)? □

Training & Communications (continued)

5. How do you handle transparency and follow-up during and after a misconduct incident? Do you inform employees when a member of staff is terminated for misconduct? Do you close the loop and follow up during investigations, even in the case of anonymous reports? Do employees understand the process of reporting and investigation?

Incident Reporting & Resolution

1. Is the reporting channel designed, established and operated in a secure manner that ensures the confidentiality of the reporter's identity and that of any party mentioned? □

2. Have you considered alternatives or technology to traditional hotlines that might be more accessible? □

3. Is a confirmation of receipt of the report given to the reporting person within an appropriate time frame (even anonymous reporters)? □

4. Does a competent person or department follow up on the reports? Can this person maintain communication with the reporting person and provide feedback (even anonymous reporters)? □

5. Is a careful follow-up investigation carried out on the report by the designated person or department? □

6. Is a reasonable time limit set for giving feedback or closing the loop on the report from the acknowledgment of receipt? □

7. Does your case management and resolution system give you real-time data on the status of ongoing investigations and specific categories of incidents? □

Third Party & Partner Ecosystems

1. Do all or a specific subset of the above questions also apply to partners, suppliers, customers, or the general public? □

2. How do third parties or partners report misconduct to you and how do you follow up? Is this process clearly communicated and accessible?

Mergers & Acquisitions

1. Is an effective risk assessment process carried out during the due diligence process of M&A? □

2. How were any risks handled?

3. How will the multiple compliance programs be integrated?

Is the program functioning effectively?

1. Is the program adopted top down and bottom up (by leadership and rank-and-file employees)? □

2. Who has oversight? The Board of Directors? What experience or training do they have to ensure adequate capability of oversight?

vault.

VISIT VAULTPLATFORM.COM