MITRATECH

The Seven Hallmarks of Effective Compliance Programs

Table of Contents

Introduction

For many compliance professionals, the concept of an effective compliance program is not a new one. The problem lies with trying to decrypt what effective really means, what regulators actually look for and how you can prove your program is effective.

Many people argue that the true goal of compliance is to create and implement processes and procedures that help mitigate the risk of a compliance breach. However, the fact remains that if a breach occurs, your ability to prove that your compliance program follows regulatory guidelines can reduce your culpability score and lead to significant reductions in fines and penalties.

To bring clarity to these ethics and compliance issues, Mitratech recently interviewed former Department of Justice (DOJ) compliance consultant Hui Chen. Read the interview here.

If a breach occurs, your ability to prove that your compliance program follows regulatory guidelines can reduce your culpability score and lead to significant reductions in fines and penalties.

Originally based off a series of blog posts, we've now compiled these seven hallmarks of an effective compliance program into one easy-to-follow guide, complete with information on how technology can help your compliance program.

Through examining these hallmarks, laid out by the Federal Sentencing Guidelines of Organizations, our goal is to help you understand what regulators are looking for and what it takes to make your compliance efforts truly effective.

In this guide, we will explore the following hallmarks:

1. Written policies and procedures
2. Program oversight
3. Ethical due care
4. Training and communications
5. Monitoring and effectiveness
6. Enforcement and internal investigations
7. Remediation

We'll start by taking a look at the first measure of effective compliance – a company's written policies and procedures.

01 Hallmark 1: Written Policies & Procedures

Written policies form the basis of a company's expectations and conduct, while procedures implement these standards. However, simply having policies and procedures is not enough.

With the February 2017 release of their "Evaluation of a Corporate Compliance Program," The DOJ gave insight into their investigation process. The publication highlights commonly asked questions, and the core investigative elements that consider management and review, accessibility and operational integration.

"A company's code of conduct is often the foundation upon which an effective compliance program is built," the publication states. The code helps ensure that policies and procedures are managed effectively, owned by the appropriate departments and individuals and reviewed periodically. These three steps are essential elements in any compliance program.

"A company's code of conduct is often the foundation upon which an effective compliance program is built."

HUI CHEN
Former DOJ Counsel Expert

Organizations that cannot clearly evidence the genesis and history of a policy with periodic reviews are not able to demonstrate the type of rigor regulators look for. By maintaining written policies, organizations have a chance to prove that their company places significant value on the conduct expected of its employees.

Once implemented, many organizations fail to provide a clearly communicated program that is relevant and accessible to their employees. Hui Chen challenges organizations to consider the purpose of their policies and procedures and to question whether they are just completing a tick-box exercise or actually effectively impacting the behavior of their employees.

"I have rarely met anybody who engaged in misconduct that honestly did not know what they were doing was wrong," Chen states. "The problem is not with knowledge. The problem is with behavior. You should be measuring behavior."

An organization's attention to accessibility provides evidence to regulators that they are doing all they can to best educate their employees and ensure that employees have the information they need, relevant to their role, to conduct business in an ethical and compliant fashion.

"I have rarely met anybody who engaged in misconduct that honestly did not know what they were doing was wrong," Chen states. "The problem is not with knowledge. The problem is with behavior. You should be measuring behavior."

HUI CHEN
Former DOJ Counsel Expert

After ensuring that policies and procedures are consistently managed, reviewed, accessible and relevant, organizations should focus on the operational implementation. They should be able to demonstrate that policies are actually working and evidence employee understanding with ongoing measurements.

In her interview, Chen mentioned that organizations should continuously reflect on how their system works. Adapting policies and procedures is a critical component for remediation, which we'll discuss more in depth in the seventh hallmark.

While policies and procedures are only one out of seven hallmarks of an effective compliance program, they are the foundation on which these programs are built. You cannot have a robust and effective compliance program without this base.

02 Hallmark 2: Program Oversight

According to the Federal Sentencing Guidelines for Organizations (FSGO), the seven compliance hallmarks are the minimum amount required to create due diligence and promote an organizational culture that encourages ethical conduct and a commitment to compliance. The promotion of an organizational culture is the reason our second hallmark, program oversight, exists.

Essentially, program oversight means board-level involvement in compliance, with a commitment to a "tone from the top," as many experts say.

The seven compliance hallmarks are the minimum amount required to create due diligence and promote an organizational culture.

When it comes to program oversight, the FSGO suggests that:

1. The organization's governing authority should be knowledgeable about the content and operation of the compliance and ethics program.

2. Specific high-level personnel should have overall responsibility to ensure the compliance program is effective.

3. Specific individuals tasked with day-to-day operations must be given appropriate resources to demonstrate effectiveness to the board.

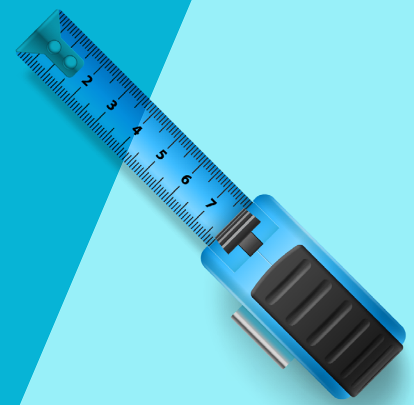
These guidelines raise some interesting points of conversation. Particularly in their description of how to demonstrate the effectiveness of and allocate resources to a compliance program.

Many organizations mistakenly convince themselves that just by proving policies and procedures exist and training occurs they have an effective compliance program. That just by demonstrating knowledge transfer to employees, they've done enough to tick boxes off the compliance checklist.

Former DOJ Counsel Expert Hui Chen takes a different approach. Chen highlights the importance of understanding the objective of your compliance program and what it needs to accomplish.

"The problem is not with knowledge," Chen states. "The problem is with behavior. You should be measuring [employee] behavior."

However, conducting this type of analysis presents a host of challenges. Many organizations simply lack the tools, technology or resources to measure their compliance program's effectiveness.



This leads us to the guideline on resources — that people tasked with day-to-day compliance operations need enough resources to do their jobs properly. While some organizations argue they allocate resources because they have a compliance program, simply having a program is not enough. Chen argues that to truly create a culture of compliance, leadership needs to put their time, money and action where their mouth is.

"When you pause and think about it, it all comes down to the choices that are made, how time is spent and how resources are allocated," Chen mentions. "These answers are what ultimately convince you of a manager's or company's commitment–not what they say."

The DOJ's 2017 whitepaper, "The Evaluation of Corporate Compliance Programs," provides insight into what proper resource allocation should look like. According to the whitepaper, when determining proper resource allocation, regulators search for answers to several questions. First, regulators want to know how companies decide to allocate personnel and resources for compliance functions. Second, they check whether a company denies resources in response to requests from company compliance and control functions.

"When you pause and think about it, it all comes down to the choices that are made, how time is spent and how resources are allocated," Chen mentions. "These answers are what ultimately convince you of a manager's or company's commitment–not what they say."

HUI CHEN
Former DOJ Counsel Expert

Throughout the whitepaper, regulators acknowledge that, to achieve the guidelines in place, companies need resources.

When it comes to program oversight, the message is clear. Regulators look to board members to create a culture of compliance and ethics. Not only is leadership responsible for ensuring they have a compliance program, but they must also demonstrate its effectiveness and make resources available to empower their compliance team and drive ethical behavior. A company cannot achieve this level of commitment simply by ticking a box.

A company cannot achieve this level of commitment simply by ticking a box.

03 Hallmark 3: Ethical Due Care

As tough as it can be to implement, our third hallmark of an effective compliance program, ethical due care and due diligence, just makes good business sense.

If a compliance offense occurs, a common misunderstanding is to consider the whole program ineffective. However, this is not necessarily the case. There's a reason the Federal Sentencing Guidelines for Organizations are just that – guidelines. Because regulators recognize that one size does not fit all, that people are fallible and that no program is perfect.

Chapter eight of the guidelines mentions that compliance programs should be designed, implemented and enforced so they are generally effective at preventing and detecting criminal conduct.

There's a reason the FSGOs are just that – guidelines. Because regulators recognize that one size does not fit all, that people are fallible and that no program is perfect.

"The failure to prevent or detect the instant offense does not necessarily mean that the program is not generally effective in preventing and detecting criminal conduct," the guidelines state.

In fact, if a violation occurs but an organization can demonstrate they have an effective compliance program, **regulators can reward them with up to a 60% reduction in the potential fine.** Putting in the effort to establish and enforce effective compliance programs can literally pay off. What regulators really need companies to demonstrate is due diligence.

Hallmark three involves looking for evidence that adequate controls are in place, even if they do occasionally fail. (See hallmark seven for information on the remediation of failed controls).

While the FSGO mentions the entire program should enforce due care, they also emphasize a focus on vetting persons of authority within an organization.

“The organization shall use reasonable efforts not to include within the substantial authority personnel of the organization any individual whom the organization knew, or should have known through the exercise of due diligence, has engaged in illegal activities or other conduct inconsistent with an effective compliance and ethics program,” the FSGO states.

Regulators search for appropriate due diligence around controls and processes to prevent personnel from being involved in illegal or unethical activities on behalf of an organization. A few measures organizations can adopt to remain vigilant include conflicts of interest trainings and surveys, appropriate policies and procedures and vigorous HR background checks. The difficulty for many organizations is to identify potential conflicts and violations before they occur. To accomplish this, organizations should implement systems that allow employees to feel safe disclosing any conflicts or information that could result in compliance violations.

Organizations should implement systems that allow employees to feel safe disclosing any conflicts or information that could result in compliance violations.

There have recently been numerous and significant high profile cases involving record breaking penalties where organizations were found to have knowledge of violations, but failed to self-report it to regulators. For example, one of the world's largest mortgage lenders recently paid a $1.2 billion settlement for improper mortgage lending they failed to report. While it's difficult to say exactly how much the company could have saved through self-reporting, the ability to do so and reduce culpability scores by five points could very well have eliminated any potential fines.

While public scandals concerning compliance breaches cast a shadow on any organization, regulators will often remove potential fines and penalties associated with the breach if an organization self-reports. We saw this recently in the new Foreign Corrupt Practices Act (FCPA) policy, which grew out of a positive self-reporting pilot scheme run by the DOJ. The pilot program would remove five points from an organization's culpability score if the organization self-reported an issue. Effectively, this program rewards companies for their due diligence and transparency by potentially removing any penalties or fines.

Due diligence is a tough hallmark to attain. Organizations must first create and maintain a culture of ethics and compliance in the workplace. This culture grows from the implementation of the first two hallmarks – clear

written policies and procedures and program oversight. Afterwards, an organization must follow through with its own ethical values and ensure the right personnel and controls are in place to ensure any unethical and noncompliant behavior is identified, reported and remediated.

This can be a difficult task when you consider the difference between a company's legal and compliance functions in order to achieve proper due care. At times, compliance may have different interests than legal.

"Legal, by definition, may be more interested in protecting the organization," Industry expert Hui Chen states. "Sometimes that protection may be interpreted as 'We don't want to know too much,' whereas compliance always wants to know more. A good compliance function wants to know what happened, how to fix things based on what you learn about what happened and what are the system weaknesses."

"A good compliance function wants to know what happened, how to fix things based on what you learn about what happened and what are the system weaknesses."

HUI CHEN
Former DOJ Counsel Expert

04 Hallmark 4: Training & Communications

While many organizations and compliance departments think they handle this hallmark well, they often fall short of their full potential in this arena. Hallmark four helps us expose exactly where organizations fall short and provides clarity on regulators' expectations in this space.

According to the Federal Sentencing Guidelines for Organizations, organizations should take steps to regularly communicate their standards and procedures in a practical manner. This means organizations should communicate their compliance and ethics programs through effective training and sharing information appropriate to individuals with specific roles and responsibilities.

Organizations often fall short of this goal due to their interpretation of this hallmark and the amount of care and detail they give to it.

Organizations should take steps to regularly communicate their standards and procedures in a practical manner.

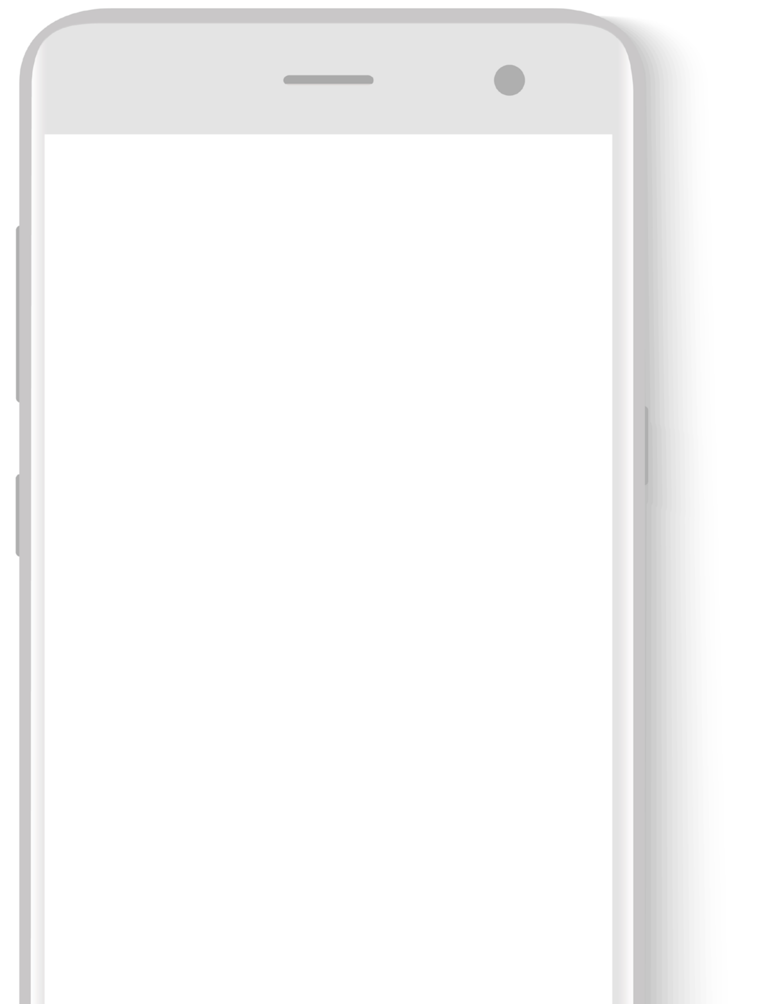
Typically, organizations fail to meet the requirements of this hallmark in four key ways:

1. Lack of periodic review and continuous communication

2. Not ensuring training and communication of policies are relevant to the employee

3. Incorrect or lack of measurement of the effectiveness of training and policies

4. Not considering the risk prioritization of training



Periodic Review and Continuous Communication

Firstly, many organizations roll out all their policies and training programs at once and host the material on a corporate intranet for employees to visit at will. In a sense, simply making this information available to employees removes a sense of ownership and responsibility for compliance and ethics enforcement from leadership. Many organizations think that, because the information is now available, their work is done since their employees have been informed.

However, informing employees is just the first step towards effective training and communication of a compliance program. Companies should regularly review, update and redistribute policies and training materials to ensure their relevance. Even when there is no need to change content, organizations should remind employees of their duties and the behavior expected of them.

Companies should regularly review, update and redistribute policies and training materials to ensure their relevance.

To highlight this issue, we look to the DOJ's whitepaper on the "Evaluation of Corporate Compliance Programs." This paper provides clarity on the types of questions enforcement officers ask when evaluating effectiveness.

Per the whitepaper, the DOJ not only reviews periodically-released subject matter training, but also looks for what senior management does to let employees know the company's position on any occurrences of misconduct.

For example, the DOJ wants to know what communications went out after an employee is terminated for failure to comply with the company's policies, procedures and controls. Employees need to clearly understand the consequences of inadequate and unacceptable behavior.

Relevant Training and Communication of Policies to Employees

Another common issue organizations fail to address is the need to disseminate information appropriate to an individual's respective roles and responsibilities. Training and communication should be targeted and relevant. Failure to provide this targeted training leads to failure at being effective.

The next question the DOJ asks is whether training is offered in a form and language appropriate for the intended audience. They search for evidence that policies and trainings are communicated in the native language of a recipient, and that they are appropriate to a recipient's location, geography, function, role and responsibility area.

Training and communication should be targeted and relevant. Failure to provide this targeted training leads to failure at being effective.

Measuring the Effectiveness of Training and Policies

The objective of ensuring communication is relevant to the employee is to increase the effectiveness of training. The measurement of effectiveness is an area of great debate, and one that former enforcement consultant to the DOJ, Hui Chen, feels passionately about.

“Often, when companies talk about a robust tone, they are just using the wrong metrics and measuring the wrong things,” Hui Chen states. “People often ask me what they should measure in training and my response is for them to tell me what the purpose or goal of their training is. What exactly do you want your training to accomplish? I think it goes back to the ‘why’ questions. Why are you doing this training? If your training is successful what would be the result? I don’t think people are asking the ‘why’ question enough.”

“I think it goes back to the ‘why’ questions. Why are you doing this training?

HUI CHEN
Former DOJ Counsel Expert

Risk Prioritization of Training

The 'why' question leads us to the final shortfall for many organizations in this hallmark — risk based training.

"If you don't even know what the risks are, how are you supposed to address them?" questions Chen. When asked what she looks for from risk based training, Chen replies, "Are you allocating your resources— whether it's time, money or control systems—in a way that's proportionate to the potential damages it could cause?"

The "Evaluation of Corporate Compliance Programs" also supports this view. The DOJ wants to know what analysis a company undertakes to determine who should receive training and on what subjects.

Once again, as with many of the hallmarks, regulators ask organizations to go past the tick box exercise of simply delivering compliance training. In order to be truly effective, training and communications needs to be reinforced, relevant, measured and risk based.

In order to be truly effective, training and communications needs to be reinforced, relevant, measured and risk based.

05 Hallmark 5: Monitoring & Effectiveness

As the name of our fifth hallmark suggests, monitoring and effectiveness are critical parts of the seven hallmarks of an effective compliance program. According to the Federal Sentencing Guidelines for Organizations, this hallmark breaks down into three areas:

1. Monitoring and auditing the organization's compliance program
2. Periodically evaluating a program to establish its effectiveness
3. Ensuring the proper mechanisms are in place to report on this hallmark or to seek guidance on minimizing or resolving potential conflicts

Monitor and Audit a Compliance Program

According to Hui Chen, many companies count training completion rates as a measure of a training program's success and the effectiveness of their compliance program.

Chen, however, disagrees with using completion rates as a measure of success. Using completion rates as a metric is on par with grading students based on class attendance only, without ever checking their homework.

"Now, if you're a company that rewards people with a promotion simply because they show up at their job every day, then go ahead — that would be consistent with your values," Chen states. "But I don't know of any company that awards promotions purely because somebody showed up for work. They need to demonstrate that they do good work, so why is the same not true when you're measuring training?"

While many organizations think that measuring and monitoring simply that employees receive training on a program is enough to prove compliance, this is not always the case. For an organization to effectively manage their compliance program, they must prove that employees have not only received certain training, but that they actually understand the content of that training and can follow their instructions. They need to continuously measure their employees' understanding of what they've been told.

In other words, it's not about teaching employees a subject, it's about ensuring they know what to do. In order to efficiently run an effective compliance program, companies should keep in mind they don't need to turn their employees into subject matter experts in specific areas of compliance. Rather, they need to teach their employees how to follow the rules that keep them compliant.

"For example, why would you want to turn your employees into anti-trust experts or have them be knowledgeable about anti-UK bribery acts?" Chen asks. "What you actually want is for them not to take a bribe, not to give a bribe and to raise their hand if they see something that needs to be reported."

In this case, Chen states, you don't need employees to understand the differences between different types of bribes or what specific statute various bribes violate, you just need them to recognize what a bribe looks like and not take one.

"The problem is not with knowledge," Chen states.

"The problem is with behavior.

You should be measuring behavior."

Evaluate the Effectiveness of Your Compliance Program

Remember that compliance is never a one-time event. There is never just a single point in an organization's history where their commitment to compliance will be put to the test. Compliance is an ongoing commitment. While many organizations are guilty of "compliance cramming" at the end of the year to prove their compliance via annual certifications to auditors at audit time, to maintain an effective compliance program, organizations should regularly conduct reviews. They need to regularly question, evaluate and prove their compliance program's effectiveness.

One of the ways Chen recommends companies achieve this goal is to measure a company's compliance culture, as well as their tone from the top. In the anti-corruption community, Chen mentions, there's a belief that you can't measure culture. However, the Corruption Perception Index is often cited as a type of perception measurement.

"It's interesting that people say they don't know how to measure culture, yet they're actively using this metric without thinking about the specifics," Chen states. "If you can measure a whole country's perception, why can't you measure a company's perception?"

According to Chen, you can generally measure a company's commitment to compliance through the choices they make, the way they spend their time and how they allocate resources.

"There are a number of ways to measure tone from the top," Chen states.

"When you just measure the number of times someone says something pro-compliance, that measurement doesn't present the full picture. Are you also measuring how often the same people send messages that may be contrary to compliance and comparing the two numbers?"

You can generally measure a company's commitment to compliance through the choices they make, the way they spend their time and how they allocate resources.

Ensure Proper Mechanisms are in Place

While monitoring and evaluating a compliance program's effectiveness are two important steps in adhering to the fifth hallmark, those two items alone can't be fully effective without a third component. This third component provides employees with a well-known and understood system for reporting that allows for anonymity, confidentiality and for employees to seek guidance regarding potential or actual criminal conduct without fear of retaliation.

One of the main areas regulators look for when it comes to proving effectiveness is employee whistleblowing. These employee led reports prove an organization truly has a culture of compliance in place where employees can feel safe reporting violations.

"What I look for is a form of measurement to back the adjectives people tend to use," Chen states. "For example, if a company states they have a robust compliance tone at the top, yet a survey indicates a significant number of employees believe they will be retaliated against if they raise an issue, then the measurement doesn't back up the claim."

One way an organization can measure their compliance culture and the effectiveness of their reporting mechanisms is to look at the data on the number of violations reported. This data can prove a trend in the right direction towards greater transparency and cultural compliance.

Implementing and providing technology as a reporting tool can be a great way to allow for easier and more anonymous employee reporting.

“I do think that technology offers the ability to make certain processes easier,” Chen states. “If you want people to behave a certain way, it helps to make that behavior an easier choice to make.”

According to the DOJ’s whitepaper on the Evaluation of Corporate Compliance Programs, DOJ regulators thoroughly review a company’s internal reporting mechanisms when it evaluates compliance programs. For example, regulators will evaluate how a company collects, analyzes and uses information from these mechanisms, as well as how the company assesses the seriousness of the allegations it receives. Lastly, they measure whether the compliance function within an organization has full access to reporting and investigative information.

Implementing and providing technology as a reporting tool can be a great way to allow for easier and more anonymous employee reporting.

In order to go beyond merely ticking off boxes on a how-to-be-compliant checklist, organizations need to monitor and evaluate how to make their compliance programs truly effective. They also need to put the proper mechanisms in place so employees can report misconduct without fear of retribution.

Without this vital hallmark in place, even the best written policies and procedures, program oversight, ethical due care and training and communications will fall short of creating a truly effective culture of compliance.

06 Hallmark 6: Enforcement & Internal Investigations

"Legal, by definition, may be more interested in protecting the organization," Former Department of Justice (DOJ) enforcement consultant Hui Chen states. "Sometimes that protection may be interpreted as 'we don't want to know too much.' Whereas compliance always wants to know more. A good compliance function wants to know what happened, how to fix things based on what you learn about what happened and what are the system weaknesses."

Compliance **always** wants to know more.

Our sixth hallmark of an effective compliance program focuses on promoting ethics within an organization, on providing processes for reporting unethical or noncompliant activities and on responding to them effectively. This is the realm of internal compliance enforcement and investigations.

According to the Federal Sentencing Guidelines for Organizations, an organization should enforce their compliance and ethics programs by providing appropriate incentives to act ethically according to their programs' standards and appropriate disciplinary measures for engaging in criminal conduct. They should also provide disciplinary measures for failing to take the steps necessary to prevent or detect this conduct in advance.

As Chen suggests in our recent interview with her, one of the most important aspects for a regulator reviewing compliance issues is to first look at the organization's internal policies for handling any issues or violations. To do this, the compliance function of an organization needs to proactively protect their company by knowing exactly what's happening, how to fix issues and learn from them and how to correct any weaknesses in the system.

Thus, the goal of legal and compliance are actually aligned, but compliance officers have the benefit of protecting an organization before an incident occurs or before an issue can get out of hand.

One way organizations can better their internal compliance enforcement is through the types of incentives they offer to their employees. It's important to use the right types of incentives, because the wrong types, which are far too common these days, can lead to negative consequences.

It's important to use the right types of incentives, because the wrong types, which are far too common these days, can lead to negative consequences.

Take, for instance, the recent banking fiasco in the U.S. where employees were put under extreme pressure to meet targets, so they opened unauthorized credit cards to boost their sales records.

According to an article on the slippery slope of sales incentives in the Harvard Business Review, as soon as this first unethical act happens, an outright fraudulent act is not far off. The employee's justification for these acts can quickly move from "unethical but technically legal" to "well it's not harming anyone" to "no one will notice" pretty quickly. When these types of oversights and behaviors are tolerated by an organization, they quickly grow more severe and can spread through the organization like an infectious disease.

While the pressure to make a profit in any business is high, companies should no longer incentivize their employees to compromise ethics and compliance codes for the sake of boosting their sales numbers. The cost of negative incentives can result in tens of millions of dollars worth of fines. As the old compliance adage goes, the cost of noncompliance is roughly three times the cost of compliance. And sometimes the damage to brand reputation from a breach is irreversible.

Across the pond, the UK experienced the backlash from negative employee incentives in the form of the payment protection insurance (PPI) scandal. The PPI scandal involved certain banks who aggressively sold unnecessary insurance to customers once they realized how profitable those sales could be.

"We've always known that people were being mis-sold PPI, but we were still amazed to discover the scale of it. It appears that salespeople are chasing their commissions, their bosses are chasing profits – where's the sense of responsibility to the customer?" personal finance campaigner Doug Taylor mentions in an interview with The Guardian about the scandal.

If incentives, when misused, so often lead to compliance breaches, how do companies offer incentives that actually improve their internal compliance? That encourage their employees to make ethical decisions rather than break ethical codes?

A recent Health Care Compliance Association roundtable offers some insights into positive incentives for ethical behavior. The roundtable encourages companies to think of ways to honor and reward people for modeling integrity, and to consider making compliance and ethics certifications a condition for promotion to senior management positions.

"It appears that salespeople are chasing their commissions, their bosses are chasing profits – where's the sense of responsibility to the customer?"

DOUG TAYLOR
Interview with the Guardian

The roundtable also suggests that companies provide incentives for reporting that helps identify specific problems and system errors that improve overall compliance. Companies should be mindful not to make these reports a type of bounty-hunt for people, but rather make them about operations and systems.

This is where a technology solution that provides a vehicle to capture reporting, resolve a reported event and gain ongoing metrics to better perform risk assessments can play a pivotal role.

According to the DOJ whitepaper on "The Evaluation of Corporate Compliance Programs," regulators ask certain questions when they conduct investigations into a compliance breach. The first item they review is the effectiveness of a company's reporting mechanism. They want to know how the company collects, analyzes and uses information from its reporting mechanisms.

Imagine if the DOJ came knocking and you had only a short amount of time to collect all that information, enterprise-wide, manually? Talk about a nightmare.

Imagine if the DOJ came knocking and you had only a short amount of time to collect all that information, enterprise-wide, manually? **Talk about a nightmare.**

This is where building in a culture of compliance company-wide, paired with the right technology solutions, can provide the peace of mind a company needs to know their compliance will almost always pass a regulator's test.

As Chen mentions, a culture of compliance involves a tone of enforcement and incentivizing from the top that starts from the bottom up. In other words, senior leadership should get to know their employees, understand their goals, needs, ethical and moral codes, and develop a compliance program that reflects both the values of regulatory restrictions and the values of their employees. When compliance and ethics pervade an entire organization from the ground up, creating a culture of compliance, the likelihood of ethical breaches becomes much smaller.

While the ultimate goal of internal investigations and enforcement is to avoid any need for the DOJ to ever look into the effectiveness of your compliance function, if they do come knocking and you have these systems in place, they can really help save your breeches from breaches.

07 Hallmark 7: Remediation

The Federal Sentencing Guidelines for Organizations (FSGO) offer a three point reduction in culpability scores for an organization that can demonstrate an effective compliance program. This lowered score can reduce potential fines up to 60 percent. On an enterprise-scale, that could translate to significant cost savings.

Not only can effective compliance reduce a fine, it has the potential to completely eliminate a fine.

Not only can effective compliance reduce a fine, it has the potential to completely eliminate a fine if a company willingly self-reports and demonstrates they have robust procedures in place to capture, prohibit and remediate compliance breaches.

Despite the best of intentions, no compliance program is ever truly perfect. That's where the seventh hallmark of an effective compliance program - remediation - comes into play.

According to DOJ expert Hui Chen in our recent interview, “Remediation can mean what actions the company took to discipline the employees engaged in the misconduct, whether the company compensated the victims impacted by the misconduct and whether the company enhanced their compliance program as a result of the misconduct.”

Once the other six hallmarks are in place, this seventh hallmark should essentially create a feedback loop to continuously review and improve the implementation of the other hallmarks. While it would be amazing if we could just follow the steps once and have the perfect compliance program forever, the reality is the hallmarks serve as more of a cyclical roadmap than as a race from a starting line to the finish.

The FSGO states that “After criminal conduct has been detected, the organization shall take reasonable steps to respond appropriately to the criminal conduct and to prevent further similar criminal conduct, including making any necessary modifications to the organization’s compliance and ethics program.”

In other words, this hallmark of effective compliance is all about learning from your mistakes, responding appropriately and continuously improving your programs.

> “It appears that salespeople are chasing their commissions, their bosses are chasing profits – where’s the sense of responsibility to the customer?”
>
> **DOUG TAYLOR**
> Interview with the Guardian, 2011

Learn from Your Mistakes

"Every time something goes wrong, you can learn from it, even in situations that aren't that significant," Chen states.

The first step to learning from your mistakes as an organization is to periodically assess the risk of the criminal conduct faced by your company and your employees. After all, hindsight is 20/20, and if we never look back and review, we can never learn from our mistakes.

According to the FSGO, these reviews should lead you to take the steps necessary to design, implement and modify each of the seven hallmarks so you can identify and reduce the risks of criminal conduct within your organization.

"The remediation, root cause analysis and continuous improvement all serve one purpose – to ensure that you don't keep making the same mistakes and to prevent any recurrence of issues," Chen states.

"Every time something goes wrong, you can learn from it, even in situations that aren't that significant."

HUI CHEN
Former DOJ Counel Expert

Respond Appropriately

When it comes to responding appropriately to a compliance issue, Chen mentions that she's seen several companies make mistakes after they get in trouble with the DOJ. Instead of responding appropriately, these companies often respond by throwing money at their problems.

"As a result, they spend a disproportionate amount of money on compliance in a way that's really not necessary for their organization," Chen states. "In those cases, you wonder if these companies are just doing it to show us for now, because this is clearly not going to be sustainable in some organizations. Organizations cannot support an over-bloated type of program of any kind."

Regulators won't be fooled by simply throwing money at a problem. A company needs to prove that their solutions are considered carefully and applicable to their specific issues.

This is where it's important to consider an effective compliance program as part of your overall business strategy. You need to learn to proactively protect your organization from risks and respond appropriately so you can ultimately save your business money and resources, and allocate employee time in a cost effective manner.

This is where technology solutions can play pivotal roles in helping to determine your course of action around compliance. By collecting data, and using the insights from this data to drive your decision making process, you can determine exactly where you should allocate your resources to create and maintain the most cost-conscious and effective compliance program you can.

By collecting data, and using the insights from this data to drive your decision making process, you can determine exactly where you should allocate your resources to create and maintain the most cost-conscious and effective compliance program you can.

Continuously Improve

So how do you continuously improve your compliance function? The questions asked in the DOJ whitepaper on the Evaluation of Corporate Compliance Programs provide some insights on where to get started. First, according to the whitepaper, regulators want to know how often a company updates their risk assessments and reviews their policies, procedures and practices.

"Every time something goes wrong, you should sit down and figure out why it went wrong," Chen states. *"What in the system allowed it to go wrong?"*

According to Chen, people often ask her about rogue employees, and if sometimes rogue employees just happen.

"My answer is yes, of course," Chen responds. *"However, the compelling questions they should be asking are why did the employee go rogue in your organization at this time in this place in this way? How was he or she enabled in going rogue?"*

In other words, the DOJ wants to know what is it about your system or your process that could enable rogue behavior? Usually, the answers to these questions reveal the path forward towards correcting the issues and improving the effectiveness of your compliance program.

Identifying the causes behind why people act out of policy can provide a lot of insight into how you can correct these issues.

The second question regulators ask is whether your policies and procedures make sense for the particular business segments and subsidiaries they're used for.

What is it about your system or your process that could enable rogue behavior?

Summary

It's just good business to be effective, ethical and robust. Not only is the cost of noncompliance often three times the cost of staying compliant, ethics and compliance scandals can damage your company in several ways. Maintaining an effective compliance program not only positively impacts your brand reputation and public image, it can even impact your bottom line.

Not only is the cost of noncompliance often three times the cost of staying compliant, ethics and compliance scandals can damage your company in several ways.

Many people argue that the true goal of compliance is to create and implement processes and procedures that help mitigate the risk of a compliance breach. However, the fact remains that if a breach occurs, your ability to prove that your compliance program follows regulatory guidelines can reduce your culpability score and lead to significant reductions in fines and penalties.

Remember that staying compliant is never finished – rather it's an ongoing process. Be sure to regularly review the Seven Hallmarks of an Effective Compliance Program to proactively protect your company from breaches and penalties today.

Remember that staying compliant is never finished – rather it's an ongoing process.

How Technology Helps Build an Effective Compliance Program

The Federal Sentencing Guidelines for Organizations pioneered the seven hallmarks to define what an effective compliance program should look like. Regulators from across industries embrace these hallmarks as a foundation and agree they play a pivotal role in defining compliance. Regulators also agree that the backbone of an effective compliance program - the thread that links the hallmarks together - is an effective policy management strategy.

While calling it policy management makes a complex field seem simple, true policy management isn't just about policies and procedures. Sure, policies and procedures must exist, but successful policies are born from an effective compliance program that touches all aspects of an organization.

Regulators also agree that the backbone of an effective compliance program - the thread that links the hallmarks together - is an effective policy management strategy.

An effective policy management program threads through all seven of the hallmarks: written policies and procedures, program oversight, ethical due care, training and communications, monitoring and effectiveness, enforcement and internal investigations and remediation.

Policy management must encompass oversight from the top, while simultaneously responding to the needs of employees by taking a bottom-up approach. A true policy management program must monitor its own effectiveness by pinpointing exactly what went wrong, where and how.

Without this information, it's practically impossible to review and change your policies and remediate behavior. If leadership doesn't have insight into employee attestation, understanding based on exams or agreement to adhere to policies, enforcing rules and conducting internal investigations is much more difficult. Not to mention, having solid policies and procedures in place is critical to effectively communicate the requirements of your compliance program to the various stakeholders in your organization.

Many people try to manage these moving parts on their own, arguing that they don't need a software solution to do this for them. However, if you look at the level of granular details regulators ask for, self-created systems simply aren't effective. And you can no longer get away without taking any action.

To proactively protect your organization, your employees and ultimately yourself from compliance breaches, you must act now to create an effective program.

Why should you use technology to help you accomplish this goal? Aside from mitigating risk, which, let's face it, is pretty much the reason you have a compliance program to begin with, what are the benefits of shelling out for a software solution? How can the right technology help increase the effectiveness of your compliance program?

The right policy management software, such as the PolicyHub solution, provides three major benefits to your overall compliance program. It helps to ***enforce, automate*** and ***evidence*** your program.

Enforce

Enforcement is not only a key pillar of an effective compliance program, it's also a pivotal spoke on the best practice wheel for a policy lifecycle. A policy management solution helps you enforce your tone from the top compliance as well as your adherence to the other hallmarks.

Enforcement is not only a key pillar of an effective compliance program, it's also a pivotal spoke on the best practice wheel for a policy lifecycle.

The right software provides program oversight into the granular details of how employees understand policies, where knowledge gaps may lie and who exactly is struggling to understand and adhere to a specific policy. With these insights, enforcement becomes easier because leadership has the information they need to enforce a program effectively and efficiently - without wasting anyone's valuable time.

PolicyHub, for instance, allows you to follow up with any struggling employees, review your current strategy, provide remedial training and clarification as necessary and enforce ethical behavior as needed.

According to a case study with international reinsurance company Transatlantic Re, they use PolicyHub not only as a communication channel, but because of the essential compliance information it provides to senior management and auditors.

"Transatlantic Re can demonstrate a clear record of which staff have received, read and understood each policy, when they agreed to them and those who have not," the case study states.

In other words, knowing whether or not an employee read and understood a policy is no longer a question, which makes enforcing compliance an easier problem to solve.

Automate

Imagine if you had to use a document management system to create and edit policies, try to track files to ensure your version is the most recent and accurate, try to track who received what policy through email and manually track that information in a spreadsheet. Now imagine you had to send written tests to everyone and grade them by hand. Maybe you don't have to imagine this, maybe it's your life right now.

In this scenario, you have no way of knowing if anyone actually reads a policy, much less if they agree to follow it. Running a report with this 'system' would also be a total nightmare, if it were possible at all.

Now imagine if you could automate all those processes. If you could just set a few workflows, edit a policy and turn it on. If it could automatically go to the right people at the right time in the right language. If it could automatically require people to attest that they read a policy and agree to adhere to it. Imagine if you could automatically trigger a test to assess the employee's knowledge of that policy and alert you if an employee failed this test. If you could also automatically send periodic surveys to ensure employees continue to comply to these policies. And if you could set reminders to review your policies in a few years, as regulations change.

These are the exact benefits offered by an effective policy management software solution. A solution like PolicyHub streamlines and automates key compliance business processes so your talented team can focus their attention on more important tasks. With everything automated, including your reports to regulators, you can rest easy, knowing your software has your back.

According to a Mitratech client who is part of the world's largest provider of food and beverage services for travelers, PolicyHub provides the automation and consistency their international company needs. For a large organization, trying to manage training and communicating policies and procedures by hand to employees is simply out of the question.

For this client, PolicyHub established a structured and repeatable process for them to create, update, review and capture deviations for all policies and procedures throughout the company. They can now automatically distribute the right policies to the right employees at the right point of the globe at the right time in the right language.

PolicyHub established a structured and repeatable process for them to create, update, review and capture deviations for all policies and procedures throughout the company.

Evidence

In today's regulatory environment, the simple truth is you have to create an audit trail you can easily report on. You have to effectively deliver written policies and procedures, train and communicate those policies to your employees and prove yourself to regulators. And you have to do all this in a way that makes good business sense.

With ad hoc systems, running reports for regulators can take several days, if you can find the information you need to run reports at all. Without a single source of truth for your policy management information, trying to gather everything into one place during a regulatory time crunch can cause chaos across your organization.

With an automated policy management system in place, these reports no longer take days, they take minutes. With a few clicks, you have all the insights into your data you would need to drive informed decisions, report to leadership and most importantly, prove your compliance to regulators. And all the information's in one easy-to-find place.

"PolicyHub gives us a truly flexible and effective solution," Vincent Eng, AVP Assistant General Counsel at TransRe states. "Firstly for communicating policies and ensuring response, but more importantly it delivers the compliance reporting and assurance we need to satisfy internal audit, external regulators and the board of directors."

For more about Mitratech's PolicyHub solution, visit www.mitratech.com/policyhub/

About Mitratech

Mitratech is a proven global technology partner for corporate legal professionals who seek out and maximize opportunities to raise productivity, control expense and mitigate risk by deepening organizational alignment, increasing visibility and spurring collaboration across the enterprise.

With Mitratech's proven portfolio of end-to-end solutions, operational best practices permeate the enterprise, standardizing processes and accelerating time-to-value. By unlocking every opportunity to drive progress and improve outcomes, we're helping legal teams rise to the challenge of serving the evolving needs of the modern, dynamic enterprise.

For more info, visit: **www.mitratech.com**

MITRATECH

CONTACT US

info@mitratech.com

www.mitratech.com

Mitratech US

+1 (512) 382.7322

Mitratech EMEA

+44 (0) 1628.600.900

Mitratech AUS

+61 (0)3.9521.7077