Ethics & Compliance Professional as Cardiologist:

How to Avoid and Recover from Corporate Heart Attacks

JUNE 2021

By Jonny Frank and Michele Edwards

Jonny Frank
Partner, StoneTurn
jfrank@stoneturn.com
+1 212 430 3434

Michele Edwards
Partner, StoneTurn
medwards@stoneturn.com
1 312 775 1221

The law regards corporations as persons. By extension, serious ethics and conduct failures equate to corporate heart attacks and E&C professionals to cardiologists. This article considers how E&C, acting as corporate cardiologists, can re-frame the compliance value proposition and help companies prevent, detect and recover from serious ethics and compliance failures.

Cardiologists would starve if their practice depended on patients who have not yet experienced heart disease symptoms. And their patients would be better off, if they heeded Benjamin Franklin's "An ounce of prevention is worth a pound of cure."

E&C professionals face the same, if not worse, dilemma. Cardiologists have the benefit of patients experiencing angina and other recognizable symptoms. But, in the corporate world, the symptoms of an imminent 'heart attack' are not only non-existent, the company often performs better financially because of the misconduct. Without an immediate problem or crisis, companies often hesitate from investing in compliance resources. E&C functions can even lose

resources when organizations mistakenly assume the absence of ethics and compliance failures means it has no problems.

Overcoming Optimism Bias. Compliance professionals (and cardiologists) must overcome "optimism bias," the belief a negative event that happens to others will not happen to us. For example, even after a close relative dies from cardiac arrest, we continue to eat unhealthfully and not exercise, believing, at least subconsciously, "it won't happen to me."

Organizations commonly engage in optimism bias regarding ethics and compliance issues. Consider money laundering and sanctions compliance violations at financial institutions. Peer organizations incur billion-dollar fines and penalties, yet banks routinely fail to beef up their financial crime programs.

Scare Tactics Don't Work. Some E&C practitioners resort to scare tactics—a strategy that rarely works. Business leaders tune out when Compliance bases requests and recommendations on "the law requires." Compliance professionals must develop a different value proposition to gain buy-in just like cardiologists emphasize benefits, not negative consequences, to cajole patients to live healthfully.

Because "for profit" corporations exist for profit, E&C gains buy-in more effectively if it touts business benefits of investing in compliance, rather than the threat of legal consequences. As opposed to protecting senior management from "orange jump suits," E&C professionals are more successful if they can demonstrate a positive ROI from mitigated revenue leakage, lowered expenses, and safeguarded tangible and intangible assets.

What If...? To quickly measure compliance effectiveness, ask what would happen if the government repealed the underpinning laws and regulation. Consider safety laws and regulations. Because companies embrace worker safety as good for business, industrial manufacturers would answer "no," if asked whether repeal of safety laws would affect their safety programs. Similarly, what companies would permit smoking in offices if the government repealed smoke-free regulations?

But what if the government repealed antitrust, bribery laws or money laundering laws? Would your or your client's organization collude with competitors, pay off government officials or work with ethically deficient business partners if it were legal? If so, how does it square with the organization's commitment to a culture of integrity and the effectiveness/maturity of the ethics program?

Diagnose & Respond To Vulnerabilities

A comprehensive exam forms the foundation of cardiological care. Early in the relationship and periodically thereafter, the cardiologist asks about the patient's medical history and lifestyle and conducts procedures to diagnose vulnerabilities and suggest a course of treatment.

Similarly, comprehensive compliance risk assessment lays the foundation of the E&C program. Holistic and ongoing risk assessment can pinpoint the conditions likely to lead to a cardiac event, identify ethics and compliance vulnerabilities, and aid in developing a plan to keep risks within

appetite. Like cardiac exams, risk assessment results are not 100% accurate and do not rule out an E&C failure. However, serious ethics and compliance failures typically arise from one of two reasons: the organization (1) failed to anticipate the risk; or (2) over-relied on ineffective control activities.

Effective risk assessment mitigates both causes. This article assumes the reader's organization completed a risk assessment that (1) identifies known, hidden and emerging schemes and scenarios that give rise to ethics and compliance risks; (2) organizes the risks in risk taxonomy; (3) links risks to a control activities inventory (i.e., policies, processes and controls) that describes the type and frequency of the control activity, identifies the risk, process and control owner(s) and summarizes design and operating effectiveness testing results; (4) develops a risk appetite; (5) assesses inherent and residual risk; and (6) includes a risk response for events and scenarios out of risk appetite. And, like a doctor who must protect against allegations of malpractice, organizations can rely on the compliance risk assessment, and if conducted and documented effectively, it can be used to defend the compliance program in the wake of serious misconduct.

Subject High-Risk Areas To An E&C "Cardiac Stress Test"

At some point, a cardiologist may suggest a cardiac stress test to measure the heart's response to external stress in a controlled clinical environment. Once you've completed an effective risk assessment, E&C professionals similarly can subject high-risk areas to a controlled environment stress test. Below we discuss several ways to undertake this process.

- **Red Team vs. Blue Team and Other Game Exercises** Hold brainstorming sessions and focus groups with members from the first, second and third lines of defense. Debate how the known, hidden or emerging risks could occur and what preventative and detective controls are in place that would mitigate the risks.

  Find creative ways to convene and engage key stakeholders. Leverage and add fun to existing senior management and business unit meetings. For example, assign one team to devise a scheme and another to describe how existing preventive and detective control activities adequately defend the organization.

  To prepare, gather internal and external information such as results of internal investigations, root cause analyses, risk assessments, audit and regulator findings, Re-engineer the findings into schemes and scenarios. To identify emerging and hidden risks, maintain a collection of information on competitors or companies operating in the same industry and geographical area.

- **Deep Dive Review** Have your Internal Audit department or a third party conduct a deep-dive review or audit of a particular area of high risk. If the organization has not yet done so, create a list of risk indicators and estimate the likelihood that the risk is occurring (e.g., red flags an investigation would uncover if the event materialized.)

  Evaluate the design of key control activities to mitigate the risk. Look at the control suite taken as a whole, not individual control

activities. Do the control activities, if operating effectively, reduce the risk to within risk appetite?

Next, test operating effectiveness including the competency and authority of the persons executing the control activities. Apply standard audit procedures (e.g., walk-throughs, sample transaction testing, re-performance) to evaluate design and test operating effectiveness.

- **Mock Regulatory Examination** Consider arranging a mock regulatory examination in an area of high risk. The examiners (typically former regulators) undertake a process that mimics a regulatory examination (e.g., information request, employee interviews, transaction testing and file reviews). Be sure to address findings and implement recommendations from the mock review.
- **Simulated Misconduct** It is common for companies to conduct attack and penetration exercises and simulated phishing attacks to test cybersecurity control activities. Apply the same concept to other high-risk areas to attempt to perpetrate a scheme or scenario identified in the risk assessment or discussed in a Red Team vs. Blue Team Exercise. Banks, for example, use dummy transactions to test AML and trading surveillance programs. Attempt to override the management controls in place.

In all of these scenarios, communicate the results and lessons learned with business leaders and process owners. And be sure to address identified deficiencies and vulnerabilities. Imagine a prosecutor, regulator or plaintiff lawyer's glee if they discovered the company knew and did nothing to address a risk that later manifested into an actual event.

Survive & Recover From Corporate Heart Attacks

Despite receiving the best care, cardiological patients suffer heart attacks, and, even if not in the operating room, cardiologists serve crucially both in the patient's short-term stabilization and long-term recovery. Like the cardiologist-patient relationship, E&C professionals help companies survive and recover from significant ethics and compliance failures. Besides legal benefits (e.g., reduced sanctions, no government-imposed monitor or suspension), effective remediation restores eroded brand value and trust; repairs damaged relationships with regulators, employees, customers and other stakeholders; and reduces talent flight, management distraction and lost productivity.

Further, just as a heart attack does not mean the patient received poor cardiological care, ethics and compliance failures do not indicate an ineffective program or poor E&C performance. Fair or not, E&C professionals should expect finger-pointing and questioning from senior management, the Board, regulators and prosecutors. For senior E&C professionals, leading a successful remediation effort can mean the difference between being hero or scapegoat.

After a corporate heart attack, E&C professionals need to both "stabilize the patient" in the short-term and help develop and implement a long-term recovery plan.

Stabilize in the Short-Term

- **How Serious?** Companies often categorize investigations based on the severity of the allegation. E&C professionals can help develop prioritization criteria. We suggest, for ease of consistency, that companies apply the same criteria they use in risk assessments.
- **What Extent?** Companies vary on whether to include the compliance function to investigate. Even if Compliance is on the outside looking in, E&C professionals can identify risk indicators for the investigation team. And they must remain apprised generally of the scope and findings of the investigation in order to establish a parallel remediation plan.
- **How Much?** Similar to assessing impact during the risk assessment process, E&C professionals should consider the range of impact or consequences of the incident (e.g., suspension and other administrative penalties, potential loss of business, damage to reputation and brand value) and determine who may potentially be impacted.
- **Who to Alert?** E&C professionals are critical to proper reporting, particularly in regulated industries that have an expectation of immediate reporting. E&C professionals should work with senior management, the Board of Directors and outside counsel to determine reporting obligations and strategies.

Recover in the Long-Term

Cardiac surgeons, because they spend their time in operating rooms, typically do not have the knowledge, skills and experience to supervise long-term rehabilitation. Likewise, being an excellent investigator does not qualify an attorney or investigator to conduct a root-cause analysis or supervise a large remediation program. E&C professionals are or, should be, trained in remediation.[1]

Just like a patient who has recovered from a heart attack may eventually revert to the very same unhealthy lifestyle habits that potentially led to the event, companies too often take a "lightning doesn't strike twice approach" and reduce compliance resources, fail to update their risk assessment or stop monitoring and periodically auditing the effectiveness of their E&C programs altogether. Or, they simply do not apply sufficient rigor or an independent lens in doing so. After all of the efforts and investment expended to remediate a serious ethics and compliance failure, E&C professionals need to help the company "stay the course."

- **Initiate and Organize—**Speed is critical. It is one thing to demonstrate completed remediation and quite another if the company can assert only that it plans to take, or has just taken, corrective actions. Delayed remediation suffers from investigation and fee fatigue. Organizing separate workstreams (investigation and remediation) helps protect the attorney-client privilege and protects E&C practitioners from the distraction of an investigation.

- **Conduct a Root Cause Analysis–** Comprehensive root cause analysis (RCA) underpins remediation efforts just as ethics and compliance risk assessment forms the foundation of an effective E&C program. Apply an acceptable RCA process and methodology (e.g., Cressey's Fraud Triangle, COSO Internal Control Integrated Framework, "5-Whys"). What incentives and pressures motivated the misconduct? How did the perpetrators—typically people of integrity—rationalize their behavior? What control weaknesses did they exploit? Did the company's risk assessment process identify the risk—why not and, if so, what preventive and detective measures did the company take? What did prior internal audits show? What red flags did the company fail to spot?
- **Read Across the Organization–** Experience teaches how wrongdoers typically engage in a range of misconduct and unethical behavior. Effective remediation considers the potential for other misconduct by the same perpetrator(s) and similar misconduct by others in the organization. The RCA forms the basis for extended inquiries. Read across is very different, for example, if the RCA determines poor operating effectiveness to be the cause of misconduct rather than an issue of design.
- **Develop & Implement Corrective Measures–** The RCA will guide necessary improvements in control activities. As a practical matter, and the DOJ acknowledges: "No compliance program can ever prevent all criminal activity." If prevention is not practical, the company must implement detective control activities. Start with the root-cause analysis of red flags the company failed to spot. These red flags form the basis for key risk indicators to provide an early signal of recurrence.
- **Assess & Monitor–** Periodic testing to assess remediation effectiveness is a fundamental Board and government expectation. To be credible, the review must come from an independent source. Counsel lacks independence because lawyers serve as company advocate. Internal audit can provide independent assurance provided it is not reviewing its own work and is knowledgeable, skilled, and experienced in auditing remediation and compliance programs.

Government Monitors

A government-imposed monitor is like a cardiologist forcing a live-in caregiver or stay in a rehabilitation center. The best way to avoid a monitor is to conduct timely and effective remediation.

E&C professionals can help their organizations maximize the benefits and minimize the intrusion of a corporate monitor by taking a significant role in negotiating settlement terms, selecting, preparing and liaising with the monitor.

- **Settlement Terms–** Government agencies vary on the monitor selection process and scope of duties. E&C practitioners must be familiar with these approaches, particularly if the agency's process is not set in stone.

Terms to suggest to counsel include: (1) organization's role in the selection process; (2) monitor's reliance on company work product and resources; (3) monitor's mandate; (4) monitor's recommendations; (5) certification; (5) form and frequency of reporting; (6) opportunity to review report drafts; and (7) tri- and bi-lateral meetings among government, organization and monitor.

- **Monitor Selection–** Depending on the agency, the company will nominate a single or a slate of candidates to serve as monitor. [2] E&C participation in the process is critical to ensure the monitor and team have the proper knowledge, skills and experience to evaluate and recommend practical enhancements to the E&C program. Besides track record, inquire into the (1) the criteria the monitor will apply to issue the certification or determination ordered in the settlement document; (2) the workplan including milestones, timelines and deliverables; (3) team structure and professional background of key advisers; (4) willingness to rely on company work product and resources; (5) knowledge transfer from monitor to client; and (6) commitment to allow the company to review and correct factual errors in monitor reports before they are published to the government, Board and senior management.
- **Monitor Preparation–** Anticipate the monitor's needs and concerns, ranging from the logistical (e.g., office space, computer access) to the substantive (e.g., evidence to support company meets monitor criteria). Most companies will require a project management office (PMO) to process monitor document and interview requests. But the PMO should be more than a deli clerk. Staff it with company officials who can serve as tour guide as the monitor learns the company and are sufficiently well-respected to arrange meetings with senior leaders.
- **Monitor Liason–** Appoint in-house personnel to liaise with the monitor team. If the monitor creates workstreams, designate a single point of contact (SPOC) at the company to respond to questions and proactively inform the monitor about company developments and accomplishments. SPOCS can help assemble, package and explain artifacts and evidence based on pre-agreed protocols and turnaround times. Prepare business unit and function leaders for monitor interviews and field reviews. Consider mock reviews but take caution not to "coach" employees on how to answer monitor questions.

E&C professionals have the opportunity to please their parents after disappointing them by not attending medical school. Like cardiologists, E&C professionals serve patients, albeit corporate ones. And, like an effective doctor, they must have good bedside manner, help patients prevent and detect sickness; and be there when serious illness occurs to solve the immediate crisis, return the patient to to good health and avoid recurrence.

About the Authors

Jonny Frank, a Partner with StoneTurn, brings more than 40 years of public, private and education sector experience in forensic investigations, compliance and risk management. He joined StoneTurn in 2011 from PricewaterhouseCoopers (PwC), where he was a partner, and founded and led the firm's global Fraud Risk & Controls practice.

Michele Edwards, a Partner with StoneTurn, has more than 20 years of combined experience in fraud and compliance risk management, compliance and monitoring and auditing. She specializes in assessing, implementing and remediating antifraud and compliance programs, including as part of corporate compliance monitorships. She also has extensive experience conducting fraud risk assessments, fraud and compliance training, fraud detection and forensic investigations.

[1] See, J. Frank, 10 Tips to Meet Government Expectations of Remediation Programs (Compliance Week 2020) (available at https://stoneturn.com/insight/10-tips-to-meet-government-expectations-of-remediation-programs); J. Frank, Remediation (Wiley 2015)(available at https://stoneturn.com/insight/remediation).

[2] See J. Frank, SEC Imposed Monitors (Practicing Law Institute 2021) (available at https://stoneturn.com/insight/sec-imposed-monitors-2021)