

Prepared By:

Michael Rasmussen
J.D., OCEG Fellow, CCEP
Business Ethics & Compliance
Lecturer, Author, & Advisor



“The CECE in the 21st century must assure the board and other stakeholders that the company can maintain reliable achievement of objectives while addressing uncertainty and acting with integrity. The role must see that the organization will meet its objectives while being compliant with the boundaries set by laws, regulations, contractual and corporate commitments, and social responsibility obligations.”

www.Corp-Integrity.com
 research@Corp-Integrity.com
 +1.888.365.4560

Compliance Risk Management in the 21st Century

From Finding and Fixing Problems to Compliance Risk Management

Regulations, ethics, and integrity are challenging the organization like never before. Governments are increasing scrutiny of organizations, stakeholders demand transparency, clients want assurance the organization is reputable and upholds their values, and business partners require commitments to compliance and ethics.

The role of the chief ethics and compliance officer (CECO) has changed: it has evolved from various compliance areas to become a strategic pillar of the enterprise. The CECO in the 21st century has more to do than find and fix problems and ensure compliance requirements are met. Today's CECO has to ensure compliance risk is understood and managed, that organizational obligations are more than written policies but part of the fabric of business operations and interactions, and that there is a strong corporate culture that ensures social responsibility as part of the ethical environment. A strong compliance program is based on values, but requires a risk-based approach to understanding and prioritizing limited resources to combat risk.

CECOs are climbing the corporate ladder to a higher status. What was scattered across business functions — with a concentration in legal — is now coming of age

Table of Contents

- From Finding and Fixing Problems to Compliance Risk Management 1
- Regulations and Demand for Integrity Bear Down on the Organization 2
 - U.S. Perspective2
 - European Perspective2
 - Australian Perspective.....3
 - The Era of the Corporate Bounty Hunter3
- Integrity: Does Your Organization Walk Its Talk? 3
 - Compliance and Integrity in Dynamic and Distributed Business.....4
 - Who Defines the Organization's Values and Ethics?4
- Compliance and Ethics in the 21st Century 5
 - The Critical Role of the CECO in a GRC Strategy.....6
 - Building Relationships across the Business.....8
 - CECO: Answering to the Board and Executives on Compliance.....9
- Understanding and Approaching Compliance and Ethics Risk 9
 - Business Process Framework for Managing Compliance Risk in the 21st Century 11
 - Components of a Corresponding Compliance Technology Architecture..... 13
 - SAI Global Delivers a Holistic Approach to Compliance Risk Management in the 21st Century 14
- About this Paper 16
- About Corporate Integrity 16
- About Michael Rasmussen 16

Compliance Risk Management in the 21st Century

as a senior executive role. With the burden of increased scrutiny, oversight, and ethics the CECO is often reporting directly to the board of directors and senior executives.

Yesterday's compliance program will no longer work. The 21st century demands a robust compliance program to manage the breadth and depth of ethics and compliance risk that bears down on the organization today.

Regulations and Demand for Integrity Bear Down on the Organization

Managing an organization's ethics and values is challenging enough. A legion of laws, regulations, contractual obligations, judgments, and fines bear down on the organization and the CECO in the 21st century. There is a difficult path ahead for ethics and compliance management. Compliance is particularly difficult, as business is bombarded with thousands of new regulations each year.

U.S. Perspective

At the U.S. federal level (not including U.S. state or local jurisdictions) there were more than 3,500 new regulations issued last year. This brings the total number of regulations issued since 1995 to nearly 60,000. Another 4,000 new laws and regulations are pending, waiting for approval.¹ The sheer volume is staggering. FCPA is a particular hotbed of compliance in the U.S.:

- The court found Frederic Bourke, Jr. was willfully blind and as an investor he should have done more due diligence and should have known that the energy company he invested in bribed foreign officials.
- The government told Nature's Sunshine's CFO and COO they should have had better controls over financial reporting, even though the SEC never stated they specifically knew of the bribery happening within the corporation.
- The average cost of an FCPA settlement is \$50 million plus the expense for an external monitor to validate a compliance program is in place for the next 10 to 20 years. This does not include investigation expenses.
- The U.S. Department of Justice assessed nearly \$2 billion in fines in 2010. Eight of the top 10 FCPA settlements occurred in 2010. BAE Systems was the third largest fine at \$500 million. Daimler AG had \$185 million in fines and disgorgements. Snamprogetti had \$365 million in fines (the fourth-largest).
- Charles Jumet, former VP of Ports Engineering Consulting Corporation, was sentenced to 87 months in prison.
- Siemens spent \$850 million in fees and expenses to investigate anticorruption. Daimler had a five-year investigation that cost over \$500 million.

European Perspective

Europe has been known for a principles-based (or outcomes-based) approach to compliance — which originates from the United Kingdom's Financial Services Authority. They have turned their focus away from specific requirements toward understanding and interpreting compliance in light of the risk the organization faces, requiring a risk-based approach to compliance. Adding to compliance mandates, the U.K. approved the U.K. Bribery Act (UKBA) legislation in 2010, which went into enforcement in July 2011. This brings broader scope and implications to anticorruption compliance. Both the FCPA and the UKBA are country-specific initiatives in support of the Organization for Economic Cooperation and Development's

¹ www.opsi.gov.uk/acts/acts2010/ukpga_20100023_en_1

Compliance Risk Management in the 21st Century

(OECD) anticorruption initiatives in 34 countries.² The OECD has released Good Practice Guidance for internal controls, ethics, and compliance to combat corruption around the world.³

Australian Perspective

Australia, through the ASNZ 3806 standard, takes a principles-based approach to compliance. The 12 principles provide guidance to organizations designing, developing, implementing and maintaining an effective compliance program, encompassing:

1. Commitment
2. Implementation
3. Monitoring and measuring
4. Continual improvement

In addition, mandates such as those provided by the Australian Securities and Investments Commission (ASIC) and Australian Prudential Regulation Authority (APRA) broaden the scope and compliance requirements for listed organizations or those within the financial services industry.

The Era of the Corporate Bounty Hunter

Government is cracking down on organizations that lack integrity in their ethics and compliance practices. The current environment is seeing increased actions and judgments for noncompliant behavior such as corruption, insider trading, antitrust abuse, harassment, discrimination, fraud, and privacy violations. Fraud and unethical behavior is not tolerated — government and society have had enough. One aspect of this change is the government focus on initiatives that establish rewards for corporate whistleblowers. This heralds the era of the corporate bounty hunter.

The U.S. government recently introduced its most extensive regulation to uncover corporate wrongdoing in the Dodd-Frank Wall Street Reform and Consumer Protection Act (Pub.L. 111-203, H.R. 4173).⁴ Title IX Subtitle B gives the SEC powers to enforce a “whistleblower bounty program.” This program allocates a 10 percent to 30 percent reward to corporate whistleblowers who provide information leading to a successful government enforcement action with monetary sanctions of more than \$1 million. In an era of increased scrutiny and judgments for anticorruption, insider trading, and other areas, this significant concern keeps executives, the board, legal, and compliance professionals up at night.

This just scratches the surface of the regulatory burden on organizations amidst thousands that span areas of employment, quality, health and safety, environmental, business transactions, privacy, security, and many other areas. Distributed businesses that cross jurisdictions in transactions and relationships have a great deal to answer for when it comes to regulatory oversight. The burden is so great it demands companies use limited resources and a risk-based approach to understand where its greatest ethics and compliance risks are. A risk-based approach complements a values-based approach and enhances corporate culture. While culture and values ultimately drive compliance, an organization must understand where its greatest compliance exposure is and allocate resources accordingly.

² http://www.oecd.org/department/0,3355,en_2649_34855_1_1_1_1_1,00.html.

³ <http://www.oecd.org/dataoecd/5/51/44884389.pdf>

⁴ The Dodd-Frank Act was passed as a response to the recession and represents the most sweeping change to financial regulation in the United States since the Great Depression. It delivers significant change in the US financial regulatory environment and impacts nearly every aspect of the US financial services industry. Based upon the success of a similar program established by the IRS in 2006. In one respect this is nothing new - The False Claims Act dates back to 1863 and permits private individuals not associated with the U.S. government to file claims against federal contractors and receive a bounty on fraudulent claims uncovered. In the last decade the US government has established the role of Recovery Audit Contractors in the healthcare space that receive a bounty on fraudulent or inappropriate Medicare claims that have been made by a healthcare entity.

Compliance Risk Management in the 21st Century

Integrity: Does Your Organization Walk Its Talk?

Compliance risk management in the 21st century boils down to defining and maintaining corporate integrity. Organizations operate in a field of ethical, regulatory, and legal landmines. Any day of the week, business and trade publication headlines reveal failures to heed compliance obligations and ethical practices. Led by WikiLeaks and widespread coverage of corporate exposure and scandal, the organization must understand, manage, and monitor the range of ethical and compliance risks challenging the integrity of the organization.

Most organizations have written ethics and compliance practices to govern business practices, transactions, processes, employees and relationships. However, as the growing number of scandals and legal issues attest, this solution is often just smoke and mirrors, and not an integrated part of the corporate culture and business operations. Corporations in the 21st century must establish and maintain integrity to ethics, values, and compliance practices — and demonstrate they are reality, not fiction.

Integrity in compliance and ethics involves walking the walk — not just talking the talk. Integrity is measured by what a corporation does and does not do when it thinks it can get away with something. All too often corporate reports, filings, and stakeholder communications state one thing when in reality the corporation is doing something else. This inconsistency comes as a result of ignorance, market and management pressure, but far too often is simply an outright willingness to deceive.

Integrity is a mirror revealing the truth about a corporation's ethics and compliance practices. Integrity is violated when corporate policies and procedures are thrown out the window. From an organization's perspective, personal and corporate integrity are two sides of the same coin. For a corporation to have integrity, it must be an ethical environment with employees and business partners willing to follow and enforce corporate culture, policies, and procedures. Employees want to work for a corporation committed to doing the right thing, in sync with their personal values and beliefs, and which has the integrity to live by their communicated practices and commitments.

Compliance and Integrity in Dynamic and Distributed Business

Compliance risk management in the 21st century organization is not easy. Business is global. Organizations across industries have global clients, partners and business operations. The larger the organization is, the more complex its operations are, particularly interactions with external entities around the world.

Adding to the complexity of global business, today's organization is dynamic and constantly changing. The modern organization changes every minute. New employees come into the organization; others change roles, some leave. New business partner relationships are established; others terminated or changed. The business executes on strategy and enters new markets, opens up new facilities around the world, contracts with agents, or introduces new products and services. New laws are introduced that impact the organization, regulations change, and the risk environment (e.g., economic, geopolitical, operational) changes -- impacting how business is conducted.

The distributed and dynamic nature of business makes defining and maintaining corporate integrity a challenge. How does an organization validate that it is current with its legal, regulatory, policies, and other obligations in the face of an ever-changing business environment?

Who Defines the Organization's Values and Ethics?

Values and ethics that establish corporate integrity practices must be defined, communicated, and modeled. The issue is, who defines these values and ethics?

The answer stems from the corporation's overall culture — but that too has to be modeled and defined somewhere in the organization. There are several places that values and ethics can be molded. These are:

Compliance Risk Management in the 21st Century

- **Directors and executive management:** Ultimately the board and management have a key stake in establishing the culture, ethics, and values of the organization. It is at this level that the code of conduct should be defined and enforced. The board is also critical in establishing risk appetite and tolerance levels that impact how an organization defines its culture of risk-taking, which impacts compliance risk and the culture of the organization.
- **Employees:** If executives fail to define, communicate and train about values and ethics, then employees are left to define corporate culture themselves. Even when executives define and communicate values, employees mold, shape, and make the corporate culture a reality and communicate it to the rest of the world.
- **Business partners:** An organization is no longer an entity unto itself — it is impossible to define where the boundaries of an organization start and stop. The extended enterprise of business partners, supply chain, outsourcers, service providers, contractors, consultants, temporary staffing, and clients influence and shape the culture and brand of an organization. Organizations, particularly in an era of corporate social responsibility, need to validate they are doing business with organizations that share the same values. No organization wants to be in the media spotlight for partnering with an unethical business.
- **Clients:** Ultimately an organization exists to provide value. For commercial organizations this is financial value, not just ethical value. To achieve financial value it is necessary to attract clients. Clients obviously want to achieve value in quality products and services from the organization. However, they are also becoming more selective in doing business with organizations that share the same ethical and social values.
- **Governments:** Through regulation, legal liability, and plain old pressure, governments extend great influence on the culture and values of the organization. The economic crisis of 2008-2011 has provided many examples of government's influence and control over entire industries as well as practices within those industries (e.g., salary and bonuses).
- **Nongovernment organizations (NGOs):** Nonprofits, lobbyists, and associations all have sway over organizations and how they define culture, values, and ethics. NGOs wield great political, social, and media influence.

The net result is that organizations will have their values and ethics defined somewhere. Either management will lead, or others will define it for them. Where values and ethics are not centrally defined and communicated as a part of corporate culture, the organization risks going in a direction it never intended. Additionally, an ad hoc approach to defining corporate values leaves the door wide open for corruption.

This requires the organization to define its culture at the top, but also to communicate and model it down to the lowest level employee. No longer can an organization sit back and show unwillingness to influence employee behavior. The job of the CECO is to articulate and communicate the culture as defined by the board of directors and executives, establish it in policies and procedures, and monitor compliance on a continuous basis. In the past this was done in reaction to SEC requirements and Sarbanes Oxley in a post-Enron world. After the first decade of the 21st century, this has changed significantly. Expanded regulations, a flat world, increased criminal and personal liability on executives, extensive decentralization of the enterprise, social media, the era of WikiLeaks, an agitated public, and stressed economic markets all require that the organization do more than talk about integrity.

Compliance and Ethics in the 21st Century

Twenty-first century organizations are expected to do everything possible to manage and maintain corporate integrity. Demands coming from governments, the public, business partners, and clients require the organization to have defined values and ethics practices that are monitored and adapted to the demands of a changing business and regulatory environment.

Compliance Risk Management in the 21st Century

Most organizations at least try to address external legal requirements and compliance obligations. The demands of the 21st century are changing the role of the CEO and moving organizations to actively manage and monitor compliance risk. Both internal and external stakeholder forces and events cause organizations to increase compliance monitoring and reporting, especially with regard to regulatory compliance, where demands grow every day. Boards and executive management desire a deeper understanding of how the organization addresses compliance risk, whether compliance activities are effective and efficient, if they're current enough for a distributed and dynamic business, and whether they enhance compliance activities.

The Critical Role of the CEO in a GRC Strategy

The focus on risk management is on the rise as stakeholder groups, rating organizations (e.g., Standards & Poor's), shareholder advocacy groups, and enterprise partners increase their demands for transparency. So the CEO needs to manage and monitor ethics and compliance risk as part of an overall governance, risk management and compliance (GRC) program. The CEO is critical to a GRC strategy that brings together compliance, ethics, legal, risk, audit, finance, and business operations to collaborate and provide accountability. With responsibility for understanding the compliance, ethics, and cultural obligations and risks faced by the organization, the CEO is a critical player in the strategic design of collaboration and management of GRC.

The requirements of the 21st century compel CEOs to guide the enterprise beyond traditional concepts. The CEO must be a champion of corporate values, culture, and ethics. This requires that the CEO be an integrated part of the organization's GRC capabilities. Today's CEO must have a full understanding of the ethical, regulatory, and cultural risks the company faces, how they relate to each other, and how they fit into broader enterprise risk strategies. The CEO must be able to rely on well-managed cultural, compliance, and ethical risk management and governance processes to provide assurance that ethics and compliance efforts are appropriate to meet requirements and operate as designed.

The CEO in the 21st century must assure the board and other stakeholders that the company can maintain reliable achievement of objectives while addressing uncertainty and acting with integrity.⁵ The role must see that the organization will meet its objectives while being compliant with the boundaries set by laws, regulations, contractual and corporate commitments, and social responsibility obligations.

As a key player at the center of the strategic team of the enterprise, the CEO must address wide-ranging stakeholder demands and concerns, such as:

- The desire to move compliance from corporate cop to champion of values, ethics, and culture within the organization.
- Key external stakeholder (investors, regulators, NGOs, local communities) demands for transparency and evidence of effective compliance and ethics.

OCEG's definition of GRC...

GRC is a capability and a culture that enables an organization to reliably achieve objectives while addressing uncertainty and acting with integrity.

GRC requires the organization to engage in the following activities:

- Prioritize stakeholder expectations
- Set and evaluate achievement of objectives
- Ensure that objectives are achieved with integrity and excellence
- Manage the desirable and undesirable effect of uncertainty on objectives
- Operate within voluntary and mandatory boundaries of conduct
- Communicate with internal and external stakeholders about system performance
- Provide assurance that the system is effective, efficient and agile

⁵ What OCEG calls Principled Performance

Compliance Risk Management in the 21st Century

OCEG GRC Capability Model...

The OCEG GRC Capability Model™ describes key elements of effective GRC and specifically a compliance architecture that integrates the principles of corporate governance, risk management, compliance, ethics and internal control. It provides a comprehensive guide for anyone implementing and managing a GRC system or some aspect of that system. The OCEG GRC Capability Model™ has eight components:

1. **Culture & Context:** Understand the current culture and the internal and external business contexts in which the organization operates, so the GRC system can address current realities — and identify opportunities to affect the context to be more congruent with desired organizational outcomes.
2. **Organize & Oversee:** Organize and oversee the GRC system so that it is integrated with, and when appropriate, modifies the existing operating model of the business, and assign to management specific responsibility, decision-making authority, and accountability to achieve system goals.
3. **Assess & Align:** Assess risks and optimize the organizational risk profile with a portfolio of initiatives, tactics, and activities.
4. **Prevent & Promote:** Promote and motivate desirable conduct and prevent undesirable events and activities, using a mix of controls and incentives.
5. **Detect & Discern:** Detect actual and potential undesirable conduct, events, GRC system weaknesses, and stakeholder concerns using a broad network of information gathering and analysis techniques.
6. **Respond & Resolve:** Respond to and recover from noncompliance and unethical conduct events, or GRC system failures, so that the organization resolves each immediate issue, and prevent or resolve similar issues more effectively and efficiently in the future.
7. **Monitor & Measure:** Monitor, measure and modify the GRC system on a periodic and ongoing basis to ensure it contributes to business objectives while being effective, efficient and responsive to the changing environment.
8. **Inform & Integrate:** Capture, document and manage GRC information so that it efficiently and accurately flows up, down and across the extended enterprise, and to external stakeholders.

- The board and C-suite need clear and reliable information about ethics, culture, and regulatory risks to drive strategic decisions and future outcomes.
- Compliance executives need to allocate limited resources to minimize exposure to significant compliance and ethical risks.
- Line executives need policy communications, training, surveys, and compliance risk assessments that do not disrupt operations, as well as coordinated compliance calendars, and content.
- An overarching need for improved efficiencies and reduced risk throughout the extended enterprise that align business relationships with the organization's values and code of conduct, while meeting compliance obligations.
- Management of decentralized organizations where compliance owners and managers are located around the world.
- Establishment of clear lines of accountability to gain greater control and responsibility for compliance risk.
- Validation that the organization's culture and practices align with other commitments to corporate social responsibility and sustainability.



OCEG's GRC Capability Model

Compliance Risk Management in the 21st Century

All the while, the CECO must embrace a strategic view that satisfies the demands of all of these competing forces while keeping an eye on the prize — meeting organizational objectives and delivering strategic value. This requires the CECO to build collaborative relationships with other GRC roles across the business.

Building Relationships across the Business

The CECO is faced with the challenge of encouraging other executives to work together to revamp existing siloed, and haphazard risk management, compliance and governance systems, and turn them into an integrated process that provides greater transparency, reliability and value. A well-defined and implemented GRC approach is essential for 21st century compliance management. Without it, governance and strategic planning is weakened while integrity and compliance is threatened by misallocation of resources. Additionally, this GRC approach must include the elements necessary for objective, independent and measurable evaluation of GRC systems. There must be capable, well-informed ethics and compliance personnel in place to provide assurance to management and the board that all of this is effectively and efficiently working as designed. To develop and maintain a strong GRC management process, the CECO must have the support of, and share information with, a number of key members of the executive team.

It is critical that the CECO play a key role to develop and drive GRC strategy by understanding the compliance and ethical risks the organization faces and the opportunities to control cost, improve resource utilization and create sustainable scalability and alignment with company goals and objectives. CECOs should be prepared to champion corporate compliance and ethics goals, for example:

- **Articulate** to the board why having a clear and conformed view of compliance and ethics effectiveness is critical to the organization's culture, performance, as well as meeting the board's fiduciary responsibilities
- **Demonstrate** how centralized oversight and supporting technologies for policy communication and training drive predictable behaviors and performance results.
- **Communicate** the benefits of including compliance and ethics within business change initiatives and partner/supplier relationships.
- **Influence** key functional executives to support compliance and ethics' role in the organization's achievement of business objectives.
- **Collaborate** with key executives to develop GRC processes for measurable evaluation of effectiveness and efficiency, and to support business agility.
- **Assist** the CEO in evaluating opportunities and preventing adverse effects from identified regulatory compliance and ethical risks.
- **Help** management appreciate how an integrated GRC model can improve processes while reducing or eliminating redundant efforts that can be leveraged across assessment, training, awareness, investigations and policy management.
- **Incorporate** compliance risk management and assurance across extended business relationships (e.g., supply chain, vendors, and contractors).

To accomplish these goals it is essential that the CECO develop and maintain collaborative relationships with the:

- Board of directors
- Chief executive officer (CEO)
- Chief operational officer (COO)

Compliance Risk Management in the 21st Century

- Chief people officer/Human Resources (CPO/HR)
- Chief finance officer (CFO)
- Chief information officer (CIO)
- Chief risk officer (CRO)
- Chief audit executive (CAE)
- General counsel/Chief legal officer (GC/CLO)

Collaboration is required to break down organizational barriers to compliance management and develop a risk-driven GRC strategy that is effective, efficient, and agile enough to meet the demands of a changing business and regulatory environment. Executives already understand they are critical players as the eyes and ears of the organization as it works to achieve objectives. By leading them to understand the value of an integrated GRC approach, the CECO in the 21st century can be a central force to establish and maintain integrity as it drives towards business objectives and performance.

CECO: Answering to the Board and Executives on Compliance

Historically, compliance was a distributed function with lack of consistent processes and approach between distributed functions. Corporate compliance (typically not responsible for all of compliance) was often found in legal. Going forward, though, pressures will increase for one role to have oversight and be accountable for compliance risk management. That will likely be the CECO.

The traditional role of compliance management is moving out of legal and other areas, taking on broader responsibility for ethics, compliance, integrity, culture, and social responsibility across the organization, and having a direct reporting relationship to the CEO and/or board of directors. This is most frequent in highly regulated industries. Some organizations are differentiating between operational compliance and legal compliance by having legal monitor and interpret laws that impact the organization. Regulators and government agencies are in some cases requiring, or at least encouraging, the role of compliance to report outside of legal so it has greater ability to raise issues and see them resolved.

What is becoming critical is the CECO's ability to report to the board of directors. Since 1996 in the U.S., the board has had responsibility to see that a compliance and ethics program is in place.⁶ This was most recently made clear in the United States Sentencing Commission Organizational Guidelines that require that the board be knowledgeable about the content and operation of the compliance and ethics program, and exercise reasonable oversight with respect to the implementation and effectiveness of the compliance and ethics program — with specific ability for the CECO role to have direct access to the board or an appropriate subgroup of the board.⁷

Understanding and Approaching Compliance and Ethics Risk

Historically the compliance function did not understand and model processes for risk management. Compliance documented and met requirements, and found and resolved issues. There was limited modeling of compliance issues and risk to determine business impact and prioritization of resources. Most often compliance was reactive, putting out

⁶ In the 1996 Delaware Chancery Court decision in *In re Caremark International Inc. Derivative Litigation* (698 A.2d 959 (Del. Ch. 1996)), the court defined the fiduciary duty of corporate directors to embrace the adoption and maintenance of corporate compliance programs that are designed to detect corporate wrongdoing and notify management and the board. In November 6, 2006 the Delaware Supreme Court in *Stone v. Ritter* (2006 Del. LEXIS 597, *30-31 (Del. November 6, 2006)), affirmed the Caremark standard for director duty and elaborated on the directors' responsibilities for compliance conduct found to be in violation of law that causes losses to a corporation.

⁷ The United States Sentencing Commission (www.ussc.gov) established organizational sentencing practices. In chapter 8, the USSC defines seven key criteria for establishing an effective compliance and ethics program. This guidance has been adopted by many US regulators and is core to compliance enforcement actions and judgments.

Compliance Risk Management in the 21st Century

fires instead of actively interpreting and predicting compliance and ethics risk issues, and developing treatment plans to mitigate or avoid damage to the organization.

The CECO in the 21st century must take a risk-based approach to compliance processes. This requires the organization to take in information from the external business and regulatory environment, understand the current and future context of a dynamic and distributed business, and model risk and business impact today and into the future. In some industries CECOs are best served to use risk models that support decision tree and scenario analysis to model risk in their environments, but can also benefit from heat maps, MARCI charts (mitigate, assure, redeploy, and cumulative impact), and even quantitative approaches such as loss distributions in Monte Carlo simulations to portray loss and impact (if there is enough data to make these meaningful).

Regardless of the complexity of the analysis, the principles of compliance risk management are the same:

- **Understand your risk:** An organization needs to have a risk-based approach to managing compliance and ethics. This includes a periodic assessment (e.g., annual) of the exposure to the organization for unethical conduct. However, the risk assessment process should also be dynamic, done each time there is a significant business change that could lead to exposure and incidents (e.g., mergers and acquisitions, new strategies and entry into new markets).
- **Approach compliance based on proportionality of risk:** How an organization implements compliance procedures and controls must be based on the proportionality of the risk it faces. If a certain area of the world or a business partner receives a high risk score for ethics or corruption, the organization must respond with stronger compliance procedures and controls. Proportionality of risk also applies to the size of the business — smaller organizations are not expected to have the same measures as large enterprises.
- **Monitor the risk and regulatory environment:** Content and information on changes to risk and regulatory environments is critical. New laws, changed regulations, court rulings, and standards of practice all change what is required of the organization. The compliance function needs to have a defined process and be accountable to monitor risk of changes in the regulatory environment.
- **Tone at the top:** The compliance risk management program needs to be fully supported by the board of directors and executives. Communication with top-level management must be bidirectional. Leadership must communicate what is both acceptable and unacceptable risk, and support the compliance and ethics program. Executives and the board must be informed about the effectiveness and operations of the compliance and risk management strategy to fulfill their fiduciary obligations.
- **Know who you do business with:** Organizations need to know their business relationships. This requires that an established risk-monitoring framework is in place that catalogs the organization's third-party relationships, markets, and geographies. Due diligence efforts must be in place to make sure the organization is contracting with ethical entities. If there is a high degree of risk of corruption, compliance, or ethical issues in a relationship, additional preventive and detective controls must be put in place. This goes beyond business partners: this means knowing employees, and conducting background checks where needed in order to understand if they are susceptible to corruption and unethical conduct.
- **Keep information current:** Due diligence and risk assessment efforts must be kept current. These are not point-in-time efforts, but must be done on a regular basis or when the business becomes aware of conditions that point to increased risk to ethics and compliance issues.
- **Compliance oversight:** The organization must have someone responsible for oversight of compliance risk processes and activities. This includes the authority to report compliance and ethical risk to independent monitoring bodies such as the audit committees of the board.

Compliance Risk Management in the 21st Century

- **Manage change in the business:** The organization must monitor the business for changes that can impact its compliance and ethics program or introduce greater risk to corporate integrity. The organization needs to document changes required for business practices as a result of observations and investigations, and must implement changes through a deliberate program of change management. These changes must be monitored by compliance to actively prevent corruption.

Business Process Framework for Managing Compliance Risk in the 21st Century

Organization exposure to compliance risk is rising at the same time the cost of compliance soars. An ad hoc or reactive approach to compliance brings complexity, forcing business to be less agile. Organizations in the past have addressed compliance as singular issues or obligations, which often resulted in multiple initiatives working in isolation. Isolated compliance initiatives tend to rely on manual processes burdened with costly assessments managed through spreadsheets, documents, and email, which is costly and unreliable. This makes it difficult to adapt to new regulatory requirements while increasing pressure and anxiety for management, employees and business relationships.

Without a business process view to manage compliance risk, organizations will continue to be burdened with the data overload and complexity of compliance data. Organizations need complete visibility into a portfolio of compliance processes spread across a distributed and complex business. Organizations need information and not just data.

Success in compliance risk management begins with a strategy — how to effectively manage compliance across the organization. Ultimately, the organization needs to identify and prioritize major risks resulting from regulatory mandates, and maintain oversight and control over business processes to mitigate these risks. In compliance business process architecture, accountability and compliance is effectively managed and the business has a system of record to understand and manage the diverse complexity of compliance issues. Compliance needs to be an active and living part of the organization and culture to prevent and detect issues across the business. It is a continuous and ongoing process to be monitored, maintained and nurtured. This challenge is taking on a new paradigm that focuses on establishing compliance processes that move from a reactive fire-fighting mode to one that actively manages, monitors, mitigates, prevents, and detects compliance-related risks.

Using the OCEG GRC Capability Model as a basis and integrating compliance risk management requirements from experience as well as guidance from USSC Organizational Sentencing Guidelines, U.K. Bribery Act, and Australia's 3806:2006, there are common core processes that compliance can establish to manage compliance risk. A business process framework to manage compliance risk in the 21st century enables an organization to manage and monitor compliance risk through:

- **Compliance program management:** This is the core process that everything else revolves around. It integrates all the other functions to provide a single cohesive program for managing and scheduling compliance reporting, assessments, controls, investigations, policies, regulatory change, and specific projects and tasks. An effective program delivers a 360-degree view of compliance risk management activities.
- **Compliance risk identification and assessment:** Risk assessments are foundational to compliance initiatives. In addition to a periodic risk assessment, the organization must have regular compliance risk assessment and monitoring activities to ensure policies and controls that maintain integrity are in place and working. The compliance risk identification and assessment process drives every aspect of a successful program as it identifies and models compliance risk that all the other processes build upon.
- **Regulatory and risk intelligence:** To keep current on compliance risk requires that the organization have a process to continuously monitor changes to the regulatory and risk environments impacting the business, and to monitor the business for change. This involves identifying subject matter experts for each compliance risk area that are accountable for monitoring internal changes and external change from regulators, courts, legislatures, and other sources to identify new and developing compliance risks that will impact the business.

Compliance Risk Management in the 21st Century

- **Policy definition, communication, and maintenance:** Organizations must have documented and up-to-date policies and procedures that both address the compliance and ethical risks and are in accordance with the culture, values, and obligations of the organization. Compliance requirements and processes must be clearly documented within policies and procedures. The policy definition, communication, and maintenance process provides proof that the program is sound and controls are adequate.
- **Compliance risk reporting and accountability:** Compliance is a distributed and federated function in most enterprises. While the board has ultimate accountability, responsibility for compliance risk management falls to the CEO, and is delegated across a variety of business processes and functions. To effectively provide assurance to the board and executives, an effective GRC approach requires that a process of compliance risk governance, accountability, and reporting be in place. This requires collaboration with other roles such as internal audit, and establishes lines of communication throughout the business.
- **Due diligence efforts:** An established process to document due diligence efforts shows that employees and business partners are properly screened, and assures the business that it is not engaging with individuals or organizations that have a bent toward unethical behavior. It also assures the organization that individuals have the right background, resources, and experience to do the job they are engaged for.
- **Training and communication:** Written policies are not enough — individuals need to know what is expected of them day-to-day and their business operations. Organizations are increasingly using online training in addition to discussion-led training to raise compliance and ethics awareness. There is also a trend toward using interactive technologies and learning simulations. The training and communication process is key to communicating the corporate culture, obligations, and expectations across the organization and to business partners.
- **Ongoing compliance assessment:** The organization needs ongoing assessment of compliance policies and controls. This involves surveys, self-assessments, and automated assessments for regular compliance risk and control monitoring. Successful organizations conduct assessments not just on a periodic basis but whenever significant business change might impact compliance.
- **Enforcement of the control environment:** While policies and procedures may define how the organization behaves, enforcement ultimately depends on controls. The organization should implement preventive and detective controls that support compliance obligations and policies. The organization needs to ensure these controls are in place and operating as designed. When there are issues, the organization must address these with corrective controls.
- **Record and report issues:** Clearly defined processes must be in place for individuals to report concerns, weaknesses and wrongdoing. Reporting is often done anonymously via call centers or Weblines. Clearly defined processes must be communicated and maintained for management to document reports made directly to them as well so that one database can be maintained and audited.
- **Conduct investigations:** Even in the best organization things go wrong. Investigative processes (e.g., hotline analysis, surveys, management reports, exit interviews) must be in place to quickly identify potential incidents of wrongdoing and quickly and effectively investigate and resolve issues. This includes reporting and working with outside law enforcement and authorities.
- **Implement communication and reporting processes:** The organization must have channels of communication where employees can ask questions on policies and procedures to avoid misunderstanding as well as issues of noncompliance. Possible systems include help lines, interactive intranets with FAQs and 'ask a question', and forms processing where approvals are requested.
- **Third-party relationships:** Central to an integrity and compliance program is the ability to identify and manage the risk of third-parties. Technology enables the ongoing due diligence effort to monitor and score vendor and

Compliance Risk Management in the 21st Century

third-party risk, communicate a supplier code of conduct and other policies to vendors and track attestations, and deliver surveys and assessments.

Throughout all of these processes, compliance risk management needs to have a clearly defined lessons-learned process to make sure the organization is not a repeat offender. Organizations with a history of noncompliant conduct will find that they are not treated favorably by courts and regulators.

Components of a Corresponding Compliance Technology Architecture

Compliance must be an active and living part of the organization and culture to prevent and detect issues that negatively affect corporate integrity. It is a continuous and ongoing process that must be monitored, maintained, and nurtured, and requires implementation of a compliance technology architecture.

Until recently, corporate compliance departments had very little use of budget for technology. Compliance processes were manual and document-centric — which led to laborious and costly processes to gather information and report on compliance. Further, compliance departments overly relied on word processing documents and spreadsheets for assessments; all lacked an audit trail. This is a legal land mine for compliance. The organization is without a defensible position to show that a specific event took place at a specific date and time, and there is no record to show that data may or may not have been compromised or changed to paint a rosier picture and get the organization or individual out of trouble. It is a requirement that 21st century compliance utilize available business technology to track compliance activity, record changes, and provide a complete audit trail.

Compliance technology architecture to support compliance risk management in the 21st century includes the capability to perform:

- **Compliance risk management:** Technology to manage compliance risk surveys, assessments, and related risk information, and to report, analyze and model risk related to compliance and ethical issues.
- **Regulatory change management:** Technology to document and manage regulatory changes and their impact on the business.
- **Learning and training management:** Technology to communicate and document training programs (e.g., e-learning courses) related to compliance. This includes delivery of training, testing, attendee participation and understanding assurance, and maintenance of training records.
- **Policy and procedure management:** Technology that maintains policy lifecycle management across development, maintenance, communication and attestation, and has a robust audit trail and content management capability to make sure policies are kept current and communicated.
- **Investigations management:** Technology enables the organization to manage and monitor issues and incidents, to collaborate and document investigation processes. This includes the ability to record the range of issues reported by hotline or other mechanisms, actions taken, and the results of the investigation.
- **Issue reporting and hotlines:** Technology that provides a system for individuals to report issues and noncompliance so it can be investigated, and a system to document reports made directly to all levels of management.
- **Survey and assessment:** Technology that delivers a consistent experience across the organization for conducting surveys and assessments for compliance.
- **Benchmarking, metrics and dashboarding:** Technology that produces reports to management, executives, and the board that compliance is designed properly and operating properly. This assures executives and the board that their fiduciary obligations for compliance are being met.

Compliance Risk Management in the 21st Century

- **Due diligence management:** Technology that facilitates due diligence efforts to validate that the organization is hiring the right people and partnering with ethical business partners that share the same commitment to compliance with legal and corporate values.
- **Forms automation and processing:** Technology that processes and automates forms that manage interactions such as gifts, entertainment, and facilitated payments through online forms and workflow for approval or disapproval.
- **Compliance program/project management:** Technology that brings compliance risk management together in a cohesive system to manage compliance activities, metrics, and reports. All compliance management personnel and employees should be able to access the system and see the contextually relevant tasks and items that pertain to their job.

SAI Global Delivers a Holistic Approach to Compliance Risk Management in the 21st Century

An organization can choose one of two primary models to manage compliance and ethics. One approach is a build-your-own, ad hoc and ultimately labor-intensive process that produces significant manual processes and piles of documents. A more economical approach focuses on software designed to manage the complex and diverse needs of compliance and ethics to establish and maintain corporate integrity.

SAI Global is a solution provider in the GRC market that Corporate Integrity has researched and evaluated. Through one of the most complete end-to-end offerings for compliance, SAI Global eases the compliance risk management burden by delivering operational effectiveness, human and financial efficiency, and agility to compliance processes. SAI Global GRC solutions help organizations manage the business processes associated with compliance risk management in the 21st century. By automating and integrating all the components of GRC with compliance learning and communication, SAI Global is the only business partner that provides one auditable view of compliance and risk management across regulatory content, training, policies, controls, procedures, third-party due diligence, investigations, hotlines, risks, assessments, and reporting.

SAI Global enables the compliance risk management program through:

- **Compliance risk identification, assessment and regulatory change management:** SAI Global's GRC platform supports the overall coordination of legal, regulatory, contractual and corporate policy obligations and responsibilities with associated tasks and records. Key stakeholders receive automated alerts when obligations change and can quickly identify gaps in compliance and corresponding risks. Automating a compliance obligations register permits oversight of all individuals, policies, risk profiles, and associated tasks.
- **Training and communication:** SAI Global's offering begins with foundational code-of-conduct benchmarking, writing, design, surveying, communication, certification, and education and progresses through an online catalog of hundreds of titles covering multiple risk areas in a variety of media experiences, learning formats, and lengths in up to 45 languages. Mobile deployment and offline versions are also part of their offering.
- **Policy definition, communication and maintenance:** SAI Global provides a centrally-hosted asset library to allow worldwide access to important documents. Policies can be assigned, versions catalogued, and certifications managed through custom questionnaires, or as part of training. Completions can be noted in individual learning and communication records and exceptions can cause a case to be triggered in their case management software. Different deployment options are offered depending on client requirements.
- **Investigations management, issue reporting and hotlines:** SAI Global's system allows full management of investigations, issues, incidents, events, or cases. Integration with their hotline (or any Web submission hotline) and learning and communication platform permits a full view into other controls necessary for a broad view of

Compliance Risk Management in the 21st Century

compliance management — how much training, when, on what topics, etc. Board-quality, customizable charts and graphs are all available.

- **Ongoing compliance assessment including surveys:** SAI Global offers choices to manage this in both their learning and GRC platforms — providing a consistent and centralized approach to gathering compliance information through assessments and surveys.
- **Benchmarking, metrics, and dashboarding:** Reports are available as standard and custom; clients choose from multiple managed services options depending on budget, internal resources and needs.
- **Due diligence efforts and third-party compliance management:** SAI Global's third-party due diligence solution, built to address bribery and corruption risk, provides a centralized platform for automating the collection and analysis of data relevant to FCPA and UKBA. The platform automates procedures to collect data, profile and screen business partners based on specified risk criteria, and automatically trigger mitigation and issue management. External data matching is included as part of the business process. Other elements of its complete third-party compliance management program (training, policy certification, etc.) can be managed using the same third-party database.
- **Enforcement of the control environment:** SAI Global specifically addresses controls needed for high-risk policies like gifts, hospitality and entertainment, and conflicts of interest. Individuals can self-register, ask questions about a policy, request approval to proceed on a certain course of action, or simply provide information about actions they are taking. A central database of requests, approvals and denials provide both an audit trail and reporting system, and configurations to define escalation policies, conditional logic, and workflow allow spot-on reporting.
- **Compliance program/project management:** Calendaring, email notifications and other management tools enable multiple components of a 21st century program to be linked with dashboarding, reports, and workflow.

SAI Global's broad portfolio of products and services enable legal, risk, audit, compliance and ethics professionals to focus on actively contributing to business results using governance, risk and compliance technology and tools productively and effectively.

Compliance Risk Management in the 21st Century

About this Paper . . .

This white paper is brought to you by SAI Global.

SAI Global provides organizations with a wide range of governance, risk and compliance (GRC) products, solutions and services that help build organizational integrity and answer these key questions:

- Does the organization make its code of ethics, policies, and procedures clear to its employees and business partners?
- Does the organization meet its legal and regulatory compliance obligations?
- Does the organization take risk within its risk appetite and tolerance thresholds?
- Is the organization properly managed and does it have sound governance?

Contact SAI Global Compliance for more information. In the US: info.americas@saiglobal.com; in EMEA: info.emea@saiglobal.com; in AsiaPac info.asiapac@saiglobal.com

About Corporate Integrity . . .

Corporate Integrity, LLC is a GRC strategy advisory firm providing leadership in education, research, analysis, and advisory services by monitoring the challenges and trends in business for corporate governance, risk management, and compliance (GRC).

Through ongoing research, interactions, and analytics, Corporate Integrity is the authority in understanding how organizations can foster a culture that “walks the talk,” where integrity is central to GRC practices. Corporate Integrity educates organizations — and GRC professionals within those organizations — on achieving sustainability, consistency, efficiency, and transparency in their corporate GRC practices to maintain a position of integrity aligned with corporate values and business performance.



About Michael Rasmussen . . .

J.D., CCEP, OCEG Fellow: Business Ethics & Compliance Lecturer, Author, & Advisor



Michael Rasmussen is an internationally recognized pundit on the topics of business ethics, corporate culture, policy management, and compliance. With more than 18 years of experience, Michael helps organizations understand their culture and improve related governance, risk, and compliance (GRC) strategies, processes, and technologies that deliver business agility, efficiency, and effectiveness. He is a sought-after keynote speaker, author, and advisor on compliance and risk management strategies. He is noted for being one of the earliest advocates for a collaborative and integrated approach to GRC.