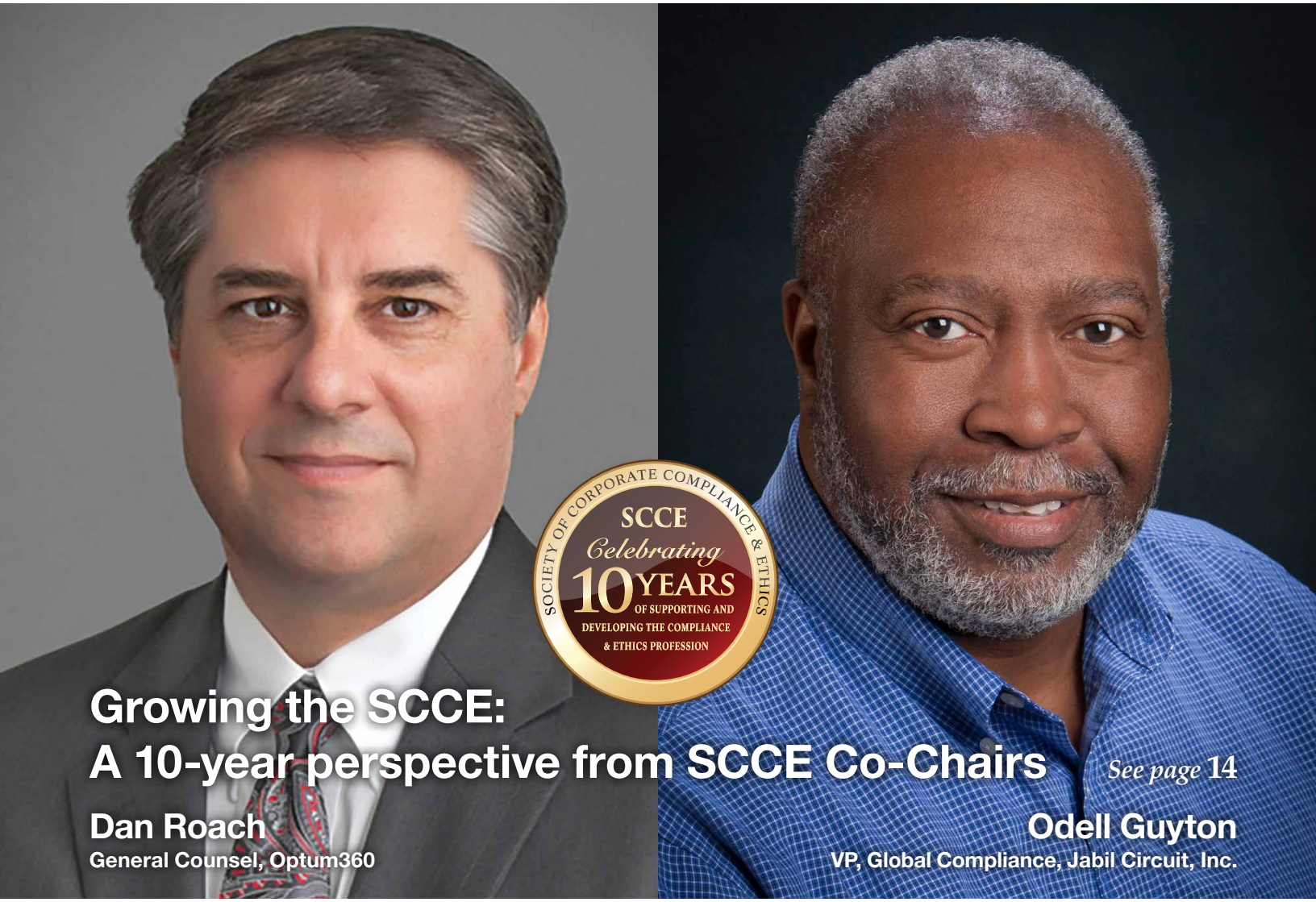
Compliance & Ethics Professional

May 2014

A PUBLICATION OF THE SOCIETY OF CORPORATE COMPLIANCE AND ETHICS

www.corporatecompliance.org



Growing the SCCE: A 10-year perspective from SCCE Co-Chairs

See page 14

Dan Roach
General Counsel, Optum360

Odell Guyton
VP, Global Compliance, Jabil Circuit, Inc.

by Carol Stern, FLMI, AIRC, ACS; and C.J. Rathbun, FLMI, CCEP, HIA, AIRC

ERM + FSGO = CRM: A powerful combination to help keep your CEO out of jail

» A well-established enterprise risk management (ERM) program can build a solid framework for compliance with the Federal Sentencing Guidelines for Organizations (FSGO).

» The chief compliance and ethics officer (CECO) and the chief Risk officer (CRO) should work together to create a compliance risk management (CRM) program that builds a combined ERM and FSGO framework.

» An organization's periodic risk assessment process must include an assessment of the risk of criminal conduct for FSGO.

» An organization must establish a risk appetite statement under its ERM program for all kinds of operational risk including, but not limited to, the risk of criminal conduct.

» Both ERM and FSGO require that senior management promote an organizational culture that enables ethical conduct and commitment to compliance with the law.

A well-implemented enterprise risk management (ERM) program can foster a more effective level of identifying and managing risks, and can be equally as effective in building a solid compliance framework as defined under the Federal Sentencing Guidelines for Organizations (FSGO). For purposes of combining risk management and effective compliance, more accurate terminology would be "compliance risk management (CRM)," which combines ERM and FSGO requirements and builds a holistic, efficient control framework in the organization.

Stern

Rathbun

Both ERM and FSGO programs are principles-based frameworks, allowing organizations to be flexible in creating a structure that best fits the scale and complexity of their organization, and avoids a "one size-fits-all" standard for compliance. A perfunctory check-the-box approach to either ERM or FSGO will fail to produce the results necessary to promote the culture of risk, compliance, and ethics required by both programs. To create a culture that is both financially strong and committed to the highest requirements of integrity and ethics, the chief ethics and compliance officer (CECO) and the chief risk officer (CRO) must join together to create an environment where they both have the independence, access, and authority to effectively discharge their corporate responsibilities in a combined ERM and FSGO (CRM) framework.

A CRM framework requires a risk culture and a culture of ethics and compliance, where risk management and controls are an ongoing activity, operating at all levels within the organization. This includes ongoing risk assessments for all risks, and appropriate

mitigation steps to design, implement, and modify the program (e.g., controls, policies, and procedures) based on risks found. The periodic risk assessment process must include the risk of criminal conduct for FSGO. This is also the basic framework for any well-designed compliance and ethics program, because an effective program to prevent and detect violations of law must include an organizational culture that encourages and enables ethical conduct and effective risk management.

Effective governance

The CRM framework requires effective governance with a structure that clearly defines and articulates roles, responsibilities, and accountabilities. The culture must support accountability in risk-based decision making, where high-level personnel must:

- be knowledgeable about the program;
- exercise oversight to help ensure its effectiveness;
- ensure that specific individuals have day-to-day responsibilities for each portion of the framework; and,
- report to the organization's governing authority (in most companies, the board of directors).

The CRM framework requires effective governance with a structure that clearly defines and articulates roles, responsibilities, and accountabilities.

That governance includes regular, transparent reports on the effectiveness of the overall program, and assessment of and reporting on whether adequate resources are devoted to the program.

The CRM requires that the organization implement a risk identification and prioritization process that is appropriate and functioning properly at all operational levels. This risk culture should also include a process for continuous improvement, based on its own as well as observed experience, as a function of the drive toward greater effectiveness of the program. The organization must then have an effective monitoring and auditing infrastructure to help detect any material risks, including the risk of criminal conduct.

Monitoring

The monitoring process will include the development of data-driven key risk indicators (KRI). These are quantitative flags whose tolerance range is set by the senior staff of the organization. The flags will indicate when the risk in that specific area needs reporting to the governance team for possible action. Every area of the organization is required to develop, monitor, and report KRIs to the Risk Governance team or Risk Committee to serve as early warnings of escalated risk. Some KRIs for the FSGO risk of criminal activity might include data and trends related to:

- issues employees seek guidance on,
- types of misconduct reported,
- employee satisfaction survey results by business unit or staff function,
- internal and external audit findings,
- complaints and regulatory investigations, and
- exit interviews issues.

Risk assessment and reporting

In addition, a system of risk-incident reporting will complete the monitoring program for

potential high-risk events. Risk incidents are reportable events as defined by the organization that will typically fall within financial and non-financial thresholds established by the Risk Governance team. Examples of FSGO risk incidents that would require immediate reporting would be: (1) any violation of a federal law by an employee or an agent of the organization; (2) theft of funds; (3) document destruction in violation of organization policy; or, (4) any breach of the code of business conduct and ethics.

The CRM program must include regular risk assessments to identify, assess, monitor, prioritize, and report material risks. The detection and prevention of criminal conduct required by the FSGO is only a subset of the risks that an ERM program monitors, and if executed properly, the ERM program enables full FSGO compliance by the organization. The holistic approach to ERM and FSGO of a CRM program should include categories of financial and non-financial risk which will vary based on the organization and the type of business. Some examples of non-financial risks that should be reviewed regularly are:

- **Criminal activity risk** such as external or internal opportunistic or systemic fraud,
- **Legal risk** such as litigation as a result of not managing enterprise risk,
- **Reputation or brand risk** such as bad press reports,
- **Privacy risk** such as breach of customer information, and
- **IT risk** such as system processing failure.

A risk assessment is performed to identify any risks that the organization is exposed to, calculate or understand the probability of the occurrence of a risk incident, and project the impact or effect it will have on the organization if/when it occurs. Those risks may be prioritized into high, medium, and low for their probability of occurrence and may also be ranked independently for their resulting impact. That is, typically a numerical value is assigned and the risk assessed may be translated into terms of numbers and percentages. However, there may be risks that are difficult to "put a number to," in which case a more qualitative approach, focusing on the quality or character of the risk and its impacts, may have to be used. All organizational risks, including the risk of criminal conduct, should be assessed, analyzed, and prioritized using these methods.

Risk appetite

A formal risk appetite statement documents the overall risk-taking principles that an entity follows given its business strategy, financial soundness objectives, and capital resources. Risk appetite defines how an organization weighs strategic decisions and communicates its strategy to key stakeholders. A risk appetite statement can enhance management's ability to make informed and effective business decisions while keeping risk exposures within acceptable boundaries. The organization must establish tolerance levels for the probability and impact of each financial and non-financial risk that is typical for the organization. The risk of criminal conduct under FSGO usually falls into the operational risk category—the risk of direct or indirect loss resulting from inadequate or failed internal processes, people, and systems which are under the organization's control, or from external events beyond the organization's control. A risk appetite statement must be established for all kinds of operational risk, including, but certainly not limited to, the risk of criminal conduct.

A high-level risk assessment (HLRA) is often the easiest way to get an overall risk snapshot for the entire enterprise. Many companies use the HLRA as the way to

decide which areas need a more targeted risk assessment. Acceptable results from an HLRA can fall into any of these four types of decisions on managing risks:

- **Risk avoidance**—Take action to avoid the risk, such as instituting process changes or additional controls;
- **Risk mitigation**—Define actions to take when the risk occurs, such as implement additional controls;
- **Risk transfer**—Have someone else share the risk (e.g. insurance or reinsurance; and
- **Risk acceptance**—Identify the risk as acceptable or within the risk appetite of the organization and let it happen.

As part of the regular HLRA, the risk of criminal activity should be assessed for the FSGO requirement (at least annually).

CRM requires that effective risk reporting and communication provide key constituents with transparency into the risk management processes and thereby facilitate active decision making on risk taking and risk management. FSGO requires that the organization's highest governing authority be knowledgeable about the company's risk strategy and risk appetite, as well as have a high-level grasp of the content and operation of the compliance and ethics program. This knowledge can only be developed through transparent reporting by the CECO, no less frequently than annually, and probably more frequently for larger and more complex companies. The best practice for the combined ERM and FSGO program—the CRM—is where the CECO and the CRO report regularly to the board of directors.

The CRM promotes a risk culture that encourages transparent, risk-based decision making and one where risks based in compliance and other non-financial activities are considered equally as important as standard financial risks. This all-inclusive risk decision-making process will, of necessity, eliminate the silo-driven structure that many organizations have today, where operational risk decisions are often made separately from financial risks decisions.

A step-by-step approach to implementing a CRM program includes:

- **Gap analysis**—Perform a gap analysis as a first step. Use what is already in place and identify what needs to be changed to fully address the two framework requirements.
- **Culture and structure review**—Ensure that the framework fits your organization's culture and management structure, so your CECO and your CRO are empowered to establish a collaborative relationship and effectively merge the two programs.
- **Governance configuration**—Form a Risk Committee comprised of senior management, which owns the program. The committee leads the organization in establishing transparent risk-based decision making, risk prioritization, and the new governance structure. The organization must put the board of directors in charge of corporate risk strategy and policy setting, including receipt and adoption of the new, transparent risk reports.
- **Risk assessment**—Perform a risk assessment to document risk decisions in preparation for risk ranking, evaluation and decision-making. The Risk Committee should draft the risk appetite statement for the board's adoption, establish risk tolerances and triggers, and implement a well-designed risk incident reporting protocol.
- **Risk monitoring and reporting**—KRIs should be established for every area of the organization. Regular KRI reports, along with risk incident reporting, should be provided to the Risk Committee and ultimately to the board of directors.

- **Strategic planning**—CRM must be imbedded into the business plan, the capital management strategy, and the financial tactics of the organization, so risk mitigation is allotted sufficient resources, including budget, IT resources, and staff.

Conclusion

Because both ERM and FSGO require senior management to promote an organizational culture that encourages ethical conduct and commitment to compliance with the law, the merger of these two sets of requirements as a holistic CRM offers the company an efficient way to strategically make risk decisions and align capital across all aspects of the organization. That same program will meet all the enterprise and organizational risk requirements of law. In fact, a well-designed CRM program manages the FSGO-specific criminal conduct risk as one of many which safeguards your organization and helps keep your CEO out of jail. ✳

Carol S. Stern *(Carol.Stern@firstconsulting.com) is a Senior Consultant at First Consulting & Administration, Inc. in Chevy Chase, MD.*
C.J. Rathbun *(Cj.rathbun@firstconsulting.com) is a Senior Consultant at First Consulting & Administration, Inc. in Kansas City, MO.*