COSMOS
Navigate the Compliance Universe

CEP Magazine - May 2023



Robert Roach (rroach@guidepostsolutions.com) is a Senior Advisor at Guidepost Solutions LLC in New York, New York, USA.



Jordan E. Segall (jordan.segall@xylem.com) is Legal Counsel for Ethics and Compliance at Xylem Inc. in Philadelphia, Pennsylvania, USA.



Scott Kahn (scott_kahn@comcast.com) is Counsel, Investigations and Compliance at Comcast Cable in Philadelphia, Pennsylvania, USA.

On the cutting edge: Emerging issues and best practices for ensuring effective compliance programs

By Robert Roach, Jordan E. Segall, and Scott Kahn, CCEP

When establishing and implementing a compliance program, most organizations attempt to follow the U.S. Federal Sentencing Guidelines for Organizations (FSG) § 8B2.1 *Effective Compliance and Ethics Program*.[1]

The elements of an FSG compliance program include:

1. High-level company personnel who exercise effective oversight and have direct reporting authority to the governing body or appropriate subgroup (e.g., audit committee);
2. Written policies and procedures;
3. Training and education;
4. Lines of communication;
5. Standards enforced through well-publicized disciplinary guidelines;
6. Internal compliance monitoring;
7. Response to detected offenses (including remediation of harm caused by criminal conduct) and corrective action plans (including assessment and modification of the compliance and ethics program); and
8. Periodic risk assessments.

While the FSG set forth basic elements of an effective compliance program, they make clear that no single compliance program design fits every organization, and an organization's industry, size, structure, and mission all influence program design and operation.

The challenge for compliance professionals trying to implement and monitor an effective FSG compliance program is that nothing happens if you do your job really well and have a little luck. Thus, every compliance

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

officer faces the challenge of how to answer the same existential question: "Is your compliance program effective?"

Compliance professionals can take heart that recently, the U.S. Department of Justice (DOJ) Criminal Division has provided an updated guidance memo that sets forth additional detail regarding its expectations of effective compliance programs. In this article, we synthesize the recent DOJ guidance and provide suggested best practices. Also, new tools—such as Capability Maturity Models (CMM)—are discussed, which can be adapted for measuring compliance program effectiveness.

Evaluation of Corporate Compliance Programs, March 2023 update

In March 2023, DOJ updated its *Evaluation of Corporate Compliance Programs*.[2] This 20-page document provides specificity into the elements required of a corporate compliance program. While not exhaustive, the guidance provides a critical roadmap for compliance professionals to benchmark their programs in the event of a worst-case-scenario review and enforcement action from DOJ. While DOJ is the focus of this article, compliance professionals should note their industry-specific regulators that may have additional requirements for an effective corporate compliance program (e.g., U.S. Department of Health & Human Services, Office of Inspector General; Securities and Exchange Commission; Department of Commerce; Department of State; Department of the Treasury; and local attorneys general).

The 2023 memo poses three guiding questions when evaluating a compliance program:

- Is it well designed? In other words, does it provide maximum effectiveness in preventing and detecting wrongdoing?
- Is it adequately resourced and empowered to function effectively? In other words, is the program implemented, reviewed, and revised as appropriate in an effective manner? This includes resourcing and communications about the compliance program.
- Is it working in practice? In other words, how is misconduct detected and remediated, and how has the program grown since the misconduct?

DOJ provides a good amount of information in its memo on what it wants to see related to design and resourcing/effectiveness. In the area of design, DOJ wants to see processes around risk assessment, policies and procedures, training and communications, confidential reporting and investigations (with incentives and discipline), third-party management, and due diligence around mergers and acquisitions.

In the area of resourcing and effective functioning, DOJ wants to see a culture of compliance from the top and middle of the organization, with the compliance program having the appropriate level of independence and resourcing. The March 2023 memo also focuses on compensation structures and consequence management, with a goal of enhancing individual accountability. DOJ now will be assessing whether the organization internally publicizes disciplinary actions and tracks data related to disciplinary actions to ensure effectiveness. Extensive guidance is also now in place for how compliance must effectively and consistently be built into promotion criteria and clawback actions throughout an organization's human resources (HR) process, disciplinary measures, and financial incentives for employees.[3]

This article focuses on assessing whether a compliance program is actually working in practice.

Measuring program effectiveness: What does DOJ want to see?

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

In its 2023 memo, DOJ outlines several parameters on how to assess if a compliance program is working in practice to promote individual accountability. DOJ's focus on individual accountability—and DOJ's desire to see compliance programs designed around individual accountability—is not unique among federal authorities. The U.S. Federal Trade Commission, for example, recently finalized a remarkable order against online alcohol marketplace Drizly and, notably, its CEO, James Cory Rellas. The order, which arises from a consumer data breach, imposes certain information security requirements on Drizly and Rellas individually, *even if Rellas moves to a different company*.[4]

Generally, DOJ wants to see continuous improvement, monitoring, and testing with an emphasis on root cause analysis. The program must also incorporate lessons learned through culture surveys, audits, investigations, and updated risk assessments, policies, and practices. DOJ also has specific guidance related to root cause analysis. It needs to be timely in looking at the numbers of misconduct involved, the control failures for the misconduct, the prior opportunities to correct the misconduct beforehand, and the specific remediation and accountability steps going forward.

The March 2023 DOJ memo also outlines two new sections. The first requires compliance investigators receive appropriate compensation and discipline to be able to promote an ethical culture and adjudicate misconduct throughout an organization.

The second section extensively discusses third-party messaging applications that may contain company information relevant to an investigation. This section covers present-day methods of communication, including use of social media/ephemeral messaging applications and the common practice of employees bringing their own device for use in official company communications. Prosecutors will now ask two things: "What electronic communication channels do the company and its employees use, or allow to be used, to conduct business?" and "What mechanisms has the company put in place to manage and preserve information contained within each of the electronic communication channels?"[5]

To have an effective compliance program, companies will need clear policies that permit the company to maintain, preserve, and retain company messages, data, and information transferred using private phones or messaging applications on the company's record-keeping systems. These policies must also be communicated, followed, and enforced in practice. In a recent speech, DOJ even announced it will go to the lengths of verifying the access to communication channels if a company claims it cannot provide information to DOJ.[6]

Suggested best practices

Compliance professionals should continue to look for additional revisions to DOJ policies. In the meantime, compliance professionals can take several actions to demonstrate their compliance program's effectiveness.

First, a compliance program charter is a good way to show how it functions and works to meet DOJ's requirements.[7] The document can also evolve to show DOJ how the program improves, monitors, and tests itself over time. As part of this charter, the compliance program can show its approach to shared values and organizational integrity.[8]

In addition, compliance professionals can use several internal data points to assess and report on the effectiveness of their compliance program and begin to build a case for declination if needed. Some examples include:

- Investigations metrics such as whistleblower complaint volume, complaint substantiation rate, anonymity rate, complaint volume by issue types, sanctions, and days to implement remediation. As part of these

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

metrics, root cause analysis should be deployed to show how investigations improve the compliance program's evaluation of controls and culture and lead to effective disciplinary actions.

- Metrics related to compensation, clawbacks, and specific linkages between: (a) compliance and an organization's hiring and incentive structure for employees and (b) investigations leading to appropriate disclosure to DOJ.[9]

- Training metrics surrounding the number and types of training modules taken per year, including completion rate and those that failed to complete (with corrective action). This should also incorporate "lessons learned" by internally publicizing instances of misconduct.

- Leader "scorecards" or "heat maps" showing key compliance metrics (e.g., number of substantiated complaints, anonymity rate, number of gift or business entertainment requests) by leader/department. Other data, such as employee climate survey results, can also be incorporated. The scorecards can help to identify organizational pain points and provide targeted training to certain leaders or departments. They can also be used to demonstrate improvement over time.

- Policy metrics surrounding required policy reviews and the number of general visits to the organization's policy database and relevant websites.

- Conflict of interest disclosure metrics surrounding the number and type of disclosures, the organizational level of those disclosing, and the number and type of management plans. This would include those requiring annual disclosure and updates.

- Enterprise risk management and internal audit findings surrounding the organization's risk assessment, evaluations of risks and controls, and plans to mitigate and improve risk and controls.

- Metrics from culture surveys with data analysis surrounding compliance program elements, including speaking up, retaliation, and ethical culture.

- Metrics around compliance by third parties and relevant actions taken to mitigate those risks, including corrective action (particularly relating to financial compensation), training, and policy enhancements.

- Any program-specific metrics required by external regulators as part of prior audits, settlement agreements, or enforcement actions.

In addition, compliance professionals can use several external data items that assess and report on the effectiveness of their compliance program. Some of these items are listed below:

- An organization's internal audit program is a critical partner in providing an external view of the functioning of the compliance program. These audits should be viewed as a value add to show testing to improve the compliance program.

- Similarly, audits from external accrediting and government agencies provide strong data points to test for improvement and effectiveness.

- Peer reviews and surveys can also serve as a strong benchmark to monitor whether compliance programs need to be updated and modified to meet the latest standards of effectiveness. These can be done with partner entities or associations, such as the Society of Corporate Compliance and Ethics.

Of important note, creating a written record to measure a compliance program's effectiveness by its nature enhances potential liability in showing gaps within the organization. There are potential steps that can be taken

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

to try to protect this information through the attorney–client privilege and the reporting lines of the compliance program. While not the subject of this article, there are pros and cons to housing the compliance function within an organization's legal department. Compliance professionals should carefully evaluate these with their legal counsel.

CMMs

The concept of a CMM was developed at Carnegie Mellon University in the 1980s for the U.S. Department of Defense to help measure the capability of potential vendors in the software industry to fulfill government contracts. The most recent version of Carnegie Mellon University's CMM was developed in 2006 by its Software Engineering Institute. The term "maturity" refers to the degree to which an organization's processes have been formalized, implemented, and integrated into an organization's operations.[10]

CMMs have been developed for many fields and areas. In this article, we have used CMM principles to establish a "Compliance Maturity Model" that we hope to provide:

- A useful means for assessing your compliance program against recognized standards.
- A method for identifying "next steps" required to advance your compliance program.
- A process for measuring progress against internal and external benchmarks.
- A tool that can be used to measure progress in specific compliance areas and projects or your overall compliance program.

Compliance CMM maturity levels

A Compliance CMM focuses on integrating your compliance program into your organizational business processes by analyzing the "maturity" of your program. Maturity levels range from ad hoc practices to formally defined steps, up to active optimization of processes. As an organization moves up the maturity model, ownership spreads across the organization and becomes embedded within the culture of the organization.

CMMs can vary in the number of maturity levels they use—usually three to five. They also use somewhat different descriptive labels. We have developed a Compliance CMM with five levels and with the most frequently used labels for each maturity level. These levels, from least to most developed, are:

1. **Ad hoc:** Procedures are usually informal, incomplete, and inconsistently applied.
2. **Fragmented:** Some compliance controls are in place, but they are not consistent across the organization. Often limited to certain areas or managed in "silos" (e.g., finance, Foreign Corrupt Practices Act).
3. **Defined:** Compliance controls and procedures are documented and standardized across the organization.
4. **Mature:** Compliance procedures are integral to business processes, and periodic reviews are conducted to assess program effectiveness.
5. **Optimized:** Regular review and feedback are used to ensure continuous improvement toward optimization of compliance processes; elements are often automated, which are more effective at preventing compliance failures and ultimately less costly than manual controls focusing on detection.

Using these CMM maturity levels, we developed a set of Compliance CMM templates, which follow each of FSG element of an effective compliance program. In turn, these templates can be used to assess the maturity and

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

effectiveness of your compliance program. To obtain a complete set of templates, see footnote.[11]

Compliance CMM Templates

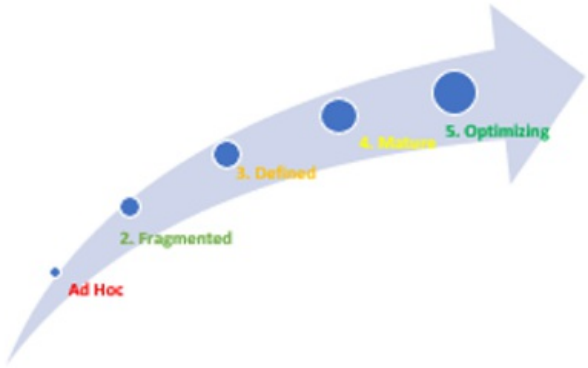
1. Structure and Accountability

In CMM Template 1 (Figure 1), we set forth the qualities of the first element of an FSG compliance program—structure and accountability—which define each of the five CMM maturity levels. The analysis at each level focuses on evidence of compliance leadership, distributed responsibility, and adequate resources; enterprise-wide coordination and oversight; and demonstrated enterprise commitment. Generally, in developing and implementing your compliance program over time, you should strive to attain a maturity level of "defined" to meet the basic FSG standards for each of the elements of an effective compliance program. Lower levels of maturity reflect characteristics of programs that are in the process of being developed. In some circumstances, lower levels may meet the requirements for compliance programs at "small organizations," which the FSG permit to have a greater level of informality. Higher levels of maturity represent the qualities normally found in more mature programs that strive to optimize the levels of compliance program effectiveness.

Figure 1: CMM Template 1 — Structure and accountability

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

1. Ad Hoc	2. Fragmented	3. Defined	4. Mature	5. Optimized
There is no formal compliance structure.	Senior management and board encourage compliance but are not consistent in providing necessary support.	A compliance structure has been established, with accountability assigned to key risk area officers.	. .	Network of identified compliance officers/partr representing every signif operation is in place, and they meet regularly to coordinate compliance activities.
There is no independent oversight.	A senior compliance committee may exist, but compliance activities are reactive and in silos.	The senior compliance committee meets at least quarterly, receives regular reports from the chief compliance officer, and actively plans for compliance contingencies.	Reporting by risk area officers to the chief compliance officer is timely and consistent.	Leadership (including the senior compliance committee) considers compliance a strategic priority. Compliance risk scenarios have been identified, assessed, and mapped to compliance controls, which are upda at least annually.
Accountability is not defined.	Individuals may be aware of compliance responsibility but are not formally appointed.	A chief compliance officer or other individual with day-to-day responsibility for compliance is appointed.	The chief compliance officer has independent and direct access to the board or audit committee and makes regular reports on compliance activities to the board/audit committee.	The board/audit committ and executive managem show a demonstrated commitment to complian throughout the organizati
Compliance risks are not understood.	Compliance risks are understood but not formally documented.	A process is in place for identifying compliance risks and developing mitigation plans by assigned risk area officers.	Compliance risk assessments and mitigation plans are completed by risk area officers on a regular, timely, and consistent basis	Compliance, risk management, and intern audit have implemented integrated work plans. Integrated functions are supported by automated processes.



Scoring: To score your compliance programs' Structure and Accountability maturity level, review the program descriptions for each maturity level in the template above. Typically compliance program's characteristics will fall i several different maturity levels. Score your ov program, add up each individual score, and divide by 5 for your average overall score.

2. Policies

In CMM Template 2 (Figure 2), we set forth the qualities of the second element of an FSG compliance program—policies—and define each of the five CMM maturity levels. The analysis at each level of maturity focuses on evidence of distributed and assigned policy responsibilities; policy development and publication; ease of policy accessibility and quality of communication; and policy tracking, review, and maintenance. Score your compliance policies' maturity level in the same way as Template 1.

Figure 2: CMM Template 2 — Policies

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

1. Ad Hoc	2. Fragmented	3. Defined	4. Mature	5. Optimized
Some compliance policies exist.	Compliance policies exist but are not consistently documented.	Policies for all significant compliance areas are documented in a consistent format. They are widely available and easily found on the organization's website. Policies identify executive and day-to-day responsible officers for questions.	Policies are reviewed regularly to ensure compliance with regulatory changes.	Legislation is proactively monitored to ensure that and amended policies ar implemented in a timely fashion. Legislation servi are utilized.
Employees may be informed about policies, but communication is sporadic and inconsistent.	Employees are provided guidance on the organization's policies; however, communications are sporadic or undocumented.	The organization has formal processes in place to communicate information and guidance on compliance policies.	Compliance policies and the consequences of noncompliance are communicated regularly, at least annually.	Changes and improveme are made to messaging communication techniqu response to periodic assessments. New and amended policies are communicated shortly af changes are approved.
Processes for policy approval and subsequent review are informal, sporadic, and inconsistent.	Consistent procedures for approval of policies and subsequent review exist but are not formally documented nor consistently followed.	There is a formal policy approval process. Monitoring for process compliance does not occur or is sporadic and undocumented.	Monitoring of compliance with the policy review process is formal and documented.	The policy management monitoring process may automated.

3. Training and Communication

In CMM Template 3 (Figure 3), we set forth the qualities of the third element of an FSG compliance program, training and communication, and define each of the five CMM maturity levels. The analysis at each level of maturity focuses on evidence of planning and content, distributed and assigned responsibilities, delivery mechanisms (in-person, online, and automated), audience (needs identification), audit trail, tracking and metrics, and assessment and certification. Score your training and communication maturity level the same way as the previous templates.

Figure 3: CMM Template 3 — Training and communication

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

1. Ad Hoc	2. Fragmented	3. Defined	4. Mature	5. Optimized
Formal compliance training is not provided; however, compliance information may be communicated by informal means.	The organization provides formal compliance training, but it is sporadic or in silos.	Formal compliance training is provided throughout the organization in a scheduled and timely fashion. Training metrics may not be collected and reported to executives or the board in a regular or consistent fashion.	An enterprise-wide compliance training program exists and is monitored by management and responsible officers. The organization identifies persons needing training in key compliance areas and monitors their participation. Training metrics are collected and reported to executives and the board at least annually.	A program of compulsory compliance training is implemented. Automatio used in program delivery monitoring. Competency assessments and certification programs ar implemented in key compliance areas. Monitoring and metrics a used to continuously imp training.
There is no formal compliance communication program.	Occasional communication about compliance may occur, but it is sporadic and informal.	Compliance communications such as newsletters, email blasts, posters, and other methods are used. There is no formal documented compliance communication plan.	The organization has developed a formal compliance communication plan that is documented and updated at least annually.	Compliance monitoring a metrics are used to continuously improve the compliance communicati plan.

Additional Compliance CMM templates can be used to assess the maturity level of the other FSG elements of an effective compliance program. As noted above, they provide a useful means for evaluating your compliance program against recognized standards.

These templates can also serve as a pathway for identifying "next steps" required to advance your compliance program and the nature and extent of any additional resources needed to achieve improvement. Moreover, the compliance model makes clear that one size does not fit all, so it gives you a methodology for improving your compliance program effectiveness in a way that most makes sense for your unique organizational resources and circumstances.

Specific compliance areas and projects

It should be noted that, in addition to measuring your overall compliance program effectiveness, Compliance CMM can also be used to measure progress in specific compliance areas and projects, such as compliance complaint processes, specific compliance subject matters (e.g., privacy, export controls, employment), compliance program qualities/results (e.g., compliance culture), and individual departments or compliance function (e.g., human subjects research).

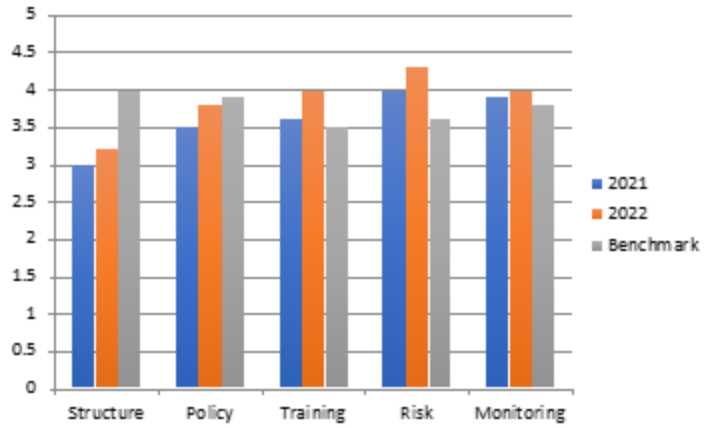
Reporting to executives and governing board/committees

Compliance CMMs can be useful tools for reporting on compliance program effectiveness to your organization's senior executives and board compliance committee. For example, you can provide snapshots of your program by FSG program element (e.g., training and communication, policies). Various Compliance CMM levels can also present target levels or goals or benchmark specific compliance program improvements over the prior year.

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

Compliance CMM metrics can also effectively illustrate year-over-year comparisons of compliance program changes and improvements (Figure 4).

Figure 4: Compliance program performance — Year-over-year comparison



Conclusion

Undoubtedly, compliance officers will continue to be faced with the question: "Is your compliance program effective?" We can take heart that government guidance, data analysis, and modern tools can help answer this question.

Takeaways

- Documenting and testing program effectiveness through culture surveys, periodic risk assessments, audits, external benchmarking, investigations, and root cause analyses can help meet expectations regarding effectiveness.
- The U.S. Department of Justice makes clear that individual accountability is key to an effective compliance program. Accountability must now take the form of "carrots and sticks" with compensation calculations incorporating compliance metrics, clawing back ill-gotten gains, and disciplinary measures.
- A written compliance program charter is a good way to show how a program functions and evolves while representing organizational commitment to compliance and a program's empowerment.
- A wide variety of program metrics can help illustrate how a compliance program works in practice, including statistics on whistleblower complaints, disclosure programs, and policy and training. Leader scorecards are also a good way to show specific organizational areas to target for demonstrated improvement over time.
- Compliance professionals can use other modern tools, such as Compliance Capability Maturity Models, to help assess and improve overall compliance program performance.

1 U.S. Sent'g Guidelines Manual § 8B2.1 (U.S. Sent'g Comm'n 2018).
2 U.S. Department of Justice, Criminal Division, *Evaluation of Corporate Compliance Programs*, updated March 2023, https://www.justice.gov/criminal-fraud/page/file/937501/download.
3 Matt Kelly, "More on Clawbacks, Message Apps," Radical Compliance (blog), March 3, 2023, https://www.radicalcompliance.com/2023/03/03/more-on-clawbacks-message-apps/.

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

4 Combined consent, Drizly, LLC v. James Cory Rellas, Docket No. C-4780 (Federal Trade Commission, Jan. 9, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/2023185-drizly-combined-consent.pdf.
5 DOJ, *Evaluation of Corporate Compliance Programs*, updated March 2023, 17.
6 Kelly, "More on Clawbacks, Message Apps,"
7 "Temple University Ethics and Compliance Office Charter," Temple University, January 24, 2023, https://www.temple.edu/sites/www/files/uploads/ECO%20Charter%20-%20Final%20%28January%2024%2C%202023%29.pdf.
8 For more information, *see* Lynne S. Paine, "Managing for Organizational Integrity," *Harvard Business Review*, March-April 1994, https://www.hbs.edu/faculty/Pages/item.aspx?num=5758; Gary R. Weaver and Linda K. Trevino, "Compliance and Values Oriented Ethics Programs: Influences on Employees' Attitudes and Behavior," *Business Ethics Quarterly,* April 1999, https://pennstate.pure.elsevier.com/en/publications/compliance-and-values-oriented-ethics-programs-influences-on-empl; and Tom Tyler, John Dienhart, and Terry Thomas, "The Ethical Commitment to Compliance: Building Value-Based Cultures," *California Management Review* 50, no. 2, January 2008, https://journals.sagepub.com/doi/abs/10.2307/41166434.
9 There has been debate whether disclosure to DOJ needs to be immediate or after reasonable analysis and remediation of misconduct. The March 2023 DOJ Memo seems to indicate that it is the latter in stating it will be a "strong indicator that the compliance program was working effectively" if a company's compliance program identifies potentially unlawful conduct; "allows for timely remediation" of the conduct, and then subsequently engages in self-reporting to the prosecutor."
10 SCAMPI Upgrade Team, *Standard CMMI Appraisal Method for Process Improvement (SCAMPI) A, Version 1.2: Method Definition Document*, Carnegie Mellon University Software Engineering Institute, August 2006, https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=7771.
11 For a complete set of Compliance Maturity Model templates, email the authors at rroach@guidepostsolutions.com.

This publication is only available to members. To view all documents, please log in or become a member.

Become a Member Login

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.