A PRACTICAL GUIDE TO COMPLIANCE PROGRAM REVIEW & FSGO BENCHMARKING
The key to a successful legal compliance and ethics program lies with a program’s fundamental ability to mitigate a company’s potential legal risks. Designing a program itself can prove challenging, though guidance on basic program elements and operating processes have emerged over the years. These best practice approaches often include hallmarks found in various legal guidelines and standards, including:

- U.S. Federal Sentencing Guidelines for Organizations (FSGO)
- Brazilian Presidential Decree 8,420 (2015)
- “Good Practices on Internal Controls, Ethics, and Compliance” from the 2010 Organization for Economic Co-Operation and Development
- The United Nations Global Compact’s 10 Principles
- The World Bank’s “Integrity Compliance Guidelines”
- “Partnering Against Corruption – Principles for Countering Bribery” from the World Economic Forum

The U.S. FSGO hallmarks represent the most commonly used framework for ethics and compliance program effectiveness. These hallmarks are considered universal and have been echoed and expanded in case law and U.S. Department of Justice memoranda:

1. Written standards and procedures
2. Program oversight
3. Due care
4. Training and communications
5. Monitoring and auditing
6. Enforcement and internal investigations
7. Remediation

Measuring program effectiveness is a regulatory expectation specifically listed in many of these legal standards, most notably within the FSGO monitoring hallmark. But that isn’t the only reason regular program review should be part of any effective compliance program.

---

1 U.S.S.G. §8B2.1(b)(5)(B), “The organization shall take reasonable steps— to evaluate periodically the effectiveness of the organization’s compliance and ethics program... .”
WHY IS IT IMPORTANT TO REVIEW A PROGRAM’S EFFECTIVENESS?

Beyond legal expectations, the most important reason to review a program’s effectiveness is simply that things change. You want to prevent program processes from becoming outdated because of regulatory or business process changes, which can make program processes susceptible to breakdown or scrutiny. Ultimately, program effectiveness depends on the program staying current.

The Guidelines and related standards also acknowledge that, while no program is perfect, effective programs are demonstrably committed to continuous improvement.

Assessing program effectiveness can also identify process improvement opportunities and efficiencies, and highlight emerging risks or trends impacting a program. Performing a review assures that the initiatives designed to address each hallmark criteria remain current, relevant and in alignment with regulatory standards and broader business objectives.

Mitigating ethics and compliance risks can have far-reaching effects, often addressing other types of risk (e.g., operational or strategic risk).

TANGENTIAL BENEFITS

A good example of a compliance program process that mitigates multiple types of risks is third party due diligence. Performing third party due diligence affords an organization proper insight into a potential partner’s operating history, business model and performance. This information can include legal or regulatory issues, financial status, management background, etc., enabling the organization performing the diligence to make decisions related to larger operational and strategic goals like market penetration, geographic expansion, capital investments or even divestiture of an asset.

Ongoing evaluation of a compliance program has multiple benefits, not least of which is achieving strategic business objectives across the organization.
HOW DO YOU MEASURE A PROGRAM’S EFFECTIVENESS?

Most, if not all, compliance teams know they should be measuring program effectiveness, but many professionals still struggle with meaningful execution. Best practice and regulatory standards call for risk-based program reviews to specifically account for an organization’s unique risk profile. Working from a risk-based assessment framework can establish the metrics needed to identify program improvement opportunities. Basing your assessment on criteria such as the FSGO hallmarks gives you an roadmap to follow, while providing a transparent, objective, repeatable and defensible program review process.

On the next page you’ll find a sample program review guide. The form is designed to assess each program hallmark using the FSGO framework and a quantitative process maturity rating scale of 1-4. Each identified and evaluated program area is given a rating. An aggregate rating can then be calculated for each hallmark. The ratings allow you to identify opportunities, analyze the root cause of the deficiency, assign ownership for improvement action and track next steps to ensure any vulnerabilities or weaknesses are resolved.

RATING SCALE:

1. **Needs Improvement**: The compliance risks identified within the organization are either not fully mitigated by controls or there are inconsistencies in the processes that make them susceptible to breakdowns and/or scrutiny.

2. **Operational**: Program processes and controls are in place to mitigate risk and are consistently operating.

3. **Best Practice**: The process area has achieved best practice criteria.

4. **Transformational**: The process area has matured beyond best practice criteria and/or is subject to re-engineering due to high impact changes affecting the process.
## Compliance Program Hallmarks Assessment Template

### Standards and Procedures
- A company’s written standards of conduct should be comprehensive, well-written, organized and accessible in order to meet their fundamental goal of preventing misconduct and ensuring compliance.

<table>
<thead>
<tr>
<th>Item</th>
<th>Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>[organizational mission, vision and values]</td>
<td>[in process]</td>
</tr>
<tr>
<td>[comprehensive Code of Conduct; CEO Introduction; audience-appropriate writing level; learning aids used]</td>
<td>[complete]</td>
</tr>
<tr>
<td>[highest risk policies or procedures]</td>
<td></td>
</tr>
<tr>
<td>[policy management process/governance]</td>
<td></td>
</tr>
<tr>
<td>[non-retaliation policy availability and prominence]</td>
<td></td>
</tr>
<tr>
<td>[policy comprehensiveness; ease of access; easy to understand; contain clear guidance]</td>
<td></td>
</tr>
</tbody>
</table>

### Program Oversight
- Overall responsibility for the compliance program should be delegated to high-level personnel with proper resources and authority, including access to the Board. In addition, the company’s governing authority should be knowledgeable about and practice oversight of the compliance program.

<table>
<thead>
<tr>
<th>Item</th>
<th>Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>[program resources/personnel and reporting structure are documented; adequate resources and authority]</td>
<td></td>
</tr>
<tr>
<td>[access to the Board or subcommittee with documentation of interaction]</td>
<td></td>
</tr>
<tr>
<td>[Board training on Code; overall program; and risk areas like COI]</td>
<td></td>
</tr>
<tr>
<td>[ethics and compliance management committees]</td>
<td></td>
</tr>
</tbody>
</table>

### Due Care
- A company needs to take reasonable steps to exclude individuals who have engaged in illegal activity or misconduct from positions of authority. Care should also be taken to prevent conflicts of interest.

<table>
<thead>
<tr>
<th>Item</th>
<th>Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>[conflict of interest training; disclosure process]</td>
<td></td>
</tr>
<tr>
<td>[annual conflict of interest certification]</td>
<td></td>
</tr>
<tr>
<td>[background checks]</td>
<td></td>
</tr>
</tbody>
</table>

### Training & Communications
- Company employees (including senior management) and agents should receive mandatory compliance training. The curriculum plan should be formalized and periodically reviewed and updated.

<table>
<thead>
<tr>
<th>Item</th>
<th>Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>[training plan and cadence; risk topic coverage; periodic curriculum review process]</td>
<td></td>
</tr>
<tr>
<td>[communication plan]</td>
<td></td>
</tr>
<tr>
<td>[new employee onboarding process]</td>
<td></td>
</tr>
<tr>
<td>[Code of Conduct certification]</td>
<td></td>
</tr>
<tr>
<td>[Tone at the Top messaging/actions]</td>
<td></td>
</tr>
</tbody>
</table>

---

**Download the Compliance Program Hallmarks Assessment Template >>**
Your organization’s risk profile should be defined within the context of your program in order to isolate measurement requirements and assert a risk-based methodology. This is best accomplished by a compliance risk assessment or as part of a larger enterprise risk assessment.

This infographic depicts numerous examples of compliance metrics throughout multiple program process areas. Following both the program hallmark criteria and targeting your organization’s highest priority risks will help drive your program review.
The Four Stages of Review

Before you begin your program assessment, document a project plan with these four high-level phases:

1. **Stakeholder Identification**
2. **Document Collection & Interviews**
3. **Evaluation**
4. **Reporting**

Include milestone dates for each phase in order to drive prioritization and accountability among the project team and participants. Following a disciplined plan will ensure that the program review is done in a comprehensive and efficient manner given the scope and resources available.

**Caution: Common Pitfall**

Not thoroughly documenting all the assessment steps with timelines and responsible parties or not leveraging internal resources that may assist or support tasks.

**A note on privilege:**

Before initiating your review, have an internal discussion about attorney-client privilege as it applies to both the review work and final report. Invoking attorney-client privilege should be determined by existing organizational legal protocols, legal counsel and applicable laws concerning privilege (which vary by jurisdiction). Risks related to the disclosure of information should not preclude a program review, but rather be addressed up front with authorized legal department personnel or outside counsel.
PHASE 1:
STAKEHOLDER IDENTIFICATION & ENGAGEMENT

When identifying project stakeholders, include your reporting audience (board of directors, CEO, executive team, etc.) as well as those who have a vested interest in the program review results due to their organizational role or program oversight responsibility. Involving other departments, managers and front-line workers who play an active in protecting your company from risk on a daily basis is a good way to spread the compliance culture throughout the entire organization and ensure it aligns with overall business goals and practices.

Common program stakeholders typically include:
- Chief Compliance Officer
- General Counsel
- Chief Audit Officer or internal audit management team
- Chief Human Resources Officer or HR executives
- Chief Information Officer and/or Chief Information Security Officer
- Privacy teams
- Compliance program team members
- Internal investigation leads
- Policy owners

Knowing who you need to speak with and where they are located (logistically as well as organizationally) will help determine how much time you’ll need to accomplish these milestones:

- **Onboard the stakeholders.** Once you’ve identified who needs to be part of this process, inform them about the project and rationale for performing the program review. Developing a project onboarding presentation that explains the project’s purpose and some high-level steps will engender support and also set expectations about project deliverables or outcomes.
- **Schedule interviews and arrange to collect pertinent documents from stakeholders.** Identify and communicate a consistent way to receive and collect documents.
- **Determine the final reporting audience and method.**

---

**Caution: Common Pitfall**

Not considering global or regional stakeholders, despite their important geographic location, reporting or functional relationships, etc.
PHASE 2: DOCUMENTATION COLLECTION & INTERVIEWS

The most resource intensive parts of a program review are the stakeholder interviews and document collection. To manage the interviews, maintain an interview schedule and cross check it against your stakeholder list to be sure you speak to everyone with a role in supporting, managing or influencing the program. Use questionnaires created and reviewed ahead of time to conduct interviews that focus on the individual stakeholder’s role, their particular governance responsibilities, process or document descriptions and any changes or updates to processes or documents.

The document collection process should adhere to company security procedures with regard to the access, transmission and storage of any proprietary, confidential or sensitive information (including but not limited to certain company policies). Follow a designated process for requesting and storing all program documentation and data.

Use a standardized policy inventory template to help identify and track organizational policies relevant to the compliance program. Assess policy effectiveness by including ratings for each document. Review and approval dates should also be tracked either on the inventory template or through a policy management process to ensure regular and consistent reviews for revisions. To help track policy documents, a sample policy inventory template is included on the next page.
### Policy Inventory Template

<table>
<thead>
<tr>
<th>Policy Name</th>
<th>Policy Owner</th>
<th>Effective Date</th>
<th>Review Date</th>
<th>Effectiveness Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Readability</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Accessibility</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Risk Coverage</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Enforcement</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Reporting &amp; Non-Retaliation</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Learning Aids</td>
</tr>
</tbody>
</table>

This document can be used to:
- Inventory policy documents
- Track policy review dates
- Rate policy effectiveness using the criteria and scale below

**Effectiveness Rating Criteria:**
- Readability: Reading level, presentation, tone
- Availability: Access to the policy
- Risk Coverage: Substantive risk mitigation
- Enforcement: Consequence management for non-compliance
- Reporting & Non-Retaliation: Processes in place and communicated
- Learning Aids: Related training materials

**Effectiveness Rating scale:**
1. Needs Improvement
2. Operational
3. Best Practice
4. Transformational

[Download the Policy Inventory Template >>](#)
PHASE 3: EVALUATION

By aggregating the information provided in interviews and documents, an effectiveness rating of 1-4 can be determined for each process or control. When incorporating interviews from stakeholders outside the compliance department, remember to evaluate feedback through the lens of their roles and responsibilities. Their feedback should be weighted and measured as it relates to the organization as a whole (what may be a major risk for them might not dramatically impact the company’s risk profile).

When evaluating each process area or program control, consider some of the following factors:

- Proper approval levels are in place, as applicable, for actions like expense report approvals, policy approvals, etc.
- Consistent (repeatable) and complete processing—e.g., documented gift and entertainment approvals if required per policy, standardized internal investigation process and protocols, etc.
- Accessible to all employees and third parties such as vendors, suppliers and agents.
- Relevant risk coverage, reflecting current regulatory and business process environments.

Caution: Common Pitfall

Not applying objective analysis or concluding an element is “good enough” due to lack of resources, budget, etc. Making excuses related to budget or headcount, for example, and cutting corners will not give you a true measure of program effectiveness.
If a particular process or control is deficient by one measure or another, the rating should inherently begin moving towards “1 - Needs Improvement.” Risk prioritization, impact and likelihood should also influence the effectiveness ratings.

Aggregating the ratings within each hallmark can produce an average hallmark effectiveness rating (with the least effective rating falling between 1.0 and 2.0). The final aggregate rating of all hallmarks will provide your organization with the overall health of the program as measured against the hallmarks set forth in the Federal Sentencing Guidelines. It’s important to note that one weak area can negatively impact—and weaken—your program’s overall effectiveness.
PHASE 4: REPORTING

Developing a final report or scorecard of the program review can be done using various approaches: custom dashboards, verbal report, executive summary, slide presentation, etc. At the outset of the project, you should have determined your final reporting audience. Knowing your audience should in turn drive the reporting method.

The report should include the individual hallmark rating averages—particularly if certain areas are weaker or stronger than the rest—as well as the overall review rating. The final assessment may give rise to action plans to address improvement opportunities, which should also be outlined in your report. The final assessment should also be used as a recurring metric or benchmark to reflect program effectiveness as improvements or process changes are made.

Caution: Common Pitfall

Not following up on remedial recommendations with recommended actions, assigned ownership and proper tracking and re-evaluation.
It is not only encouraged, but strongly recommended, that the assessment results and resulting action plans for improvements be shared with your Board of Directors, given their oversight responsibilities for an organization’s ethics and compliance program. All identified action plan owners should be notified of the results and provided an explanation of the process improvement opportunity and recommended action, along with a timeline for follow up.

In the spirit of transparency, it’s also best practice to circulate results and identified process improvements to all the people you interviewed. This reinforces the fact that their time and input were important and the assessment results are being evaluated and acted upon.

Finally, have a set schedule and tracking method for following through with action plans and improvement opportunities (this can be accomplished on the larger Assessment Guide found on page 5). Sharing these plans and timelines with the board will help you stay on track and keep all involved parties accountable.

---

2 See §8B2.1(b)(2)(A), “The organization’s governing authority shall be knowledgeable about the content and operation of the compliance and ethics program and shall exercise reasonable oversight with respect to the implementation and effectiveness of the compliance and ethics program.”
FINAL STEPS

Having a completed review and action plan in hand is not, in itself, the final step. Compliance program improvement should be ongoing and this review undertaking is simply another step in that process. Follow up is key.

Using the basic rating criteria and metrics outlined in this guide can help you set program benchmarks and provide a method for tracking ongoing program improvements as you move forward. Let this assessment guide your next actions rather than be something to simply complete.

As a final note, it’s important to remember the techniques discussed here are not absolute and can—and should—be modified to suit your specific needs or culture. This guide is designed to give you practical tips for reviewing your program and isn’t intended to be a formal performance analysis tool. Measurement, analysis and reporting of program KPIs are a separate and equally important exercise!
Convercent’s risk-based global compliance solution enables the design, implementation and measurement of an effective compliance program. Delivering an intuitive user experience with actionable executive reporting, Convercent integrates the management of corporate compliance risks, cases, disclosures, training and policies. With hundreds of customers in more than 130 countries—including Philip Morris International, CH2M Hill and Under Armour—Convercent’s award-winning GRC solution safeguards the financial and reputational health of your company. Backed by Azure Capital, Sapphire Ventures (formerly SAP Ventures), Mantucket Capital and Rho Capital Partners, and based in Denver, Colorado, Convercent will revolutionize your company’s compliance program.

Request a demo today!