



appliedcompliance

A Demonstrable & Sustainable Approach to Compliance Program Effectiveness

Version 1.0
May 2025

Integrity Bridge provides strategic, operational, technology and data analytics support to ethics & compliance, third-party risk management and human rights teams.

For more information on Integrity Bridge's services please visit:

www.integritybridge.com

Integrity Bridge has established Applied Compliance,
a free resource center for compliance professionals, available here:

www.appliedcompliance.com

A. THE MEANING AND DRIVERS OF COMPLIANCE PROGRAM EFFECTIVENESS

Regulatory Expectations of Compliance Program Effectiveness Have Evolved

Historically, the existence of a (paper-based, shelf-situated, dust-attracting) corporate compliance program was considered by some as a proxy for its effectiveness in preventing and detecting criminal conduct. Towards the end of the last decade, advances in technology - particularly data analytics - elevated the expectations of U.S. prosecutors as to compliance program effectiveness, and the required evidence to demonstrate this. More recently, these expectations evolved further, focusing on a plan for the consistent and sustainable measurement of “the success and effectiveness” of a company’s compliance program.¹

For U.S. corporate criminal prosecutions, this assessment of a company’s compliance program (including efforts to measure its effectiveness) is undertaken by prosecutors when determining (a) whether to charge a company for corporate wrongdoing; (b) whether to negotiate a plea or other agreement; (c) the criminal penalty discount to be afforded to a company, in recognition of its remediation efforts and improvements to a compliance program; and (d) the need for a corporate monitor.² While the nature of U.S. criminal corporate enforcement going forward is currently unclear, there are other regulatory drivers for an effective compliance program.³ For example:

- ⚡ Several countries have introduced laws that impose criminal and/or civil penalties on companies and their management for a *failure to prevent* fraud and/or corruption.⁴
- ⚡ The Customs Trade Partnership Against Terrorism (CTPAT) is a voluntary, public-private partnership program led by U.S. Customs and Border Protection (CBP) that enhances supply chain security

¹ U.S. Department of Justice (DOJ) Criminal Division *Evaluation of Corporate Compliance Programs* (ECCP) (2024). The September 2024 version of the ECCP includes this question: “Measurement – How and how often does the company measure the success and effectiveness of its compliance program?” However, the concept of compliance program effectiveness in U.S. corporate criminal enforcement is not new. The *U.S. Sentencing Commission, Guidelines Manual*, § 8B2.1 (USSG) includes the following: “The organization shall take reasonable steps...to evaluate periodically the effectiveness of the organization’s compliance and ethics program”, which was first included in the 2004 version of the Guidelines. The model DOJ Non-Prosecution Agreement (NPA) and Deferred Prosecution Agreement (DPA) require the production of a workplan which shall “identify with reasonable specificity the activities the Company plans to undertake to review and test each element of its compliance program”; the preparation of an annual report which includes “a complete description of the testing conducted to evaluate the effectiveness of the compliance program and the results of that testing” with the third annual report including “a plan for ongoing improvement, testing, and review of the compliance program to ensure the sustainability of the program.”

² *Principles of Federal Prosecution of Business Organizations in the Justice Manual* (JM) JM 9-28.300; USSG §§ 8B2.1, 8C2.5(f), and 8C2.8(11)) as summarized in the DOJ ECCP.

³ Presidential Executive Order February 10, 2025 “*Pausing Foreign Corrupt Practices Act Enforcement to Further American Economic and National Security*”.

⁴ *Bribery Act 2010* (UK), c.23, §7, which creates a strict liability offence for commercial organizations that fail to prevent bribery by associated persons unless “adequate procedures” are in place; *Economic Crime and Corporate Transparency Act 2023* (UK), c.56, §199, which introduces a new corporate offence for failure to prevent fraud, applicable to large organizations with a compliance-based defense; *Law No. 20.393* (Chile), *Ley sobre Responsabilidad Penal de las Personas Jurídicas* (2009), which establishes corporate criminal liability for offences such as bribery and money laundering where companies fail to implement adequate compliance programs; and *Criminal Code of Canada*, R.S.C., 1985, c. C-46, §§22.1–22.2, which imposes liability on organizations that fail to take reasonable steps to prevent criminal offences by their representatives.

against terrorism while offering participants benefits such as reduced customs examinations, expedited processing, and access to dedicated security specialists. Through enforcement of trade laws, CBP requires CTPAT participants to maintain a forced labor compliance program as a condition to CTPAT membership.⁵

- « The Uyghur Forced Labor Prevention Act (UFLPA) provides a clear example of a compliance program that must be demonstrably effective. It creates a rebuttable presumption that goods made in, or with materials from, the Xinjiang Uyghur Autonomous Region (XUAR) are produced with forced labor. CBP may detain such goods at the border unless importers supply detailed supply chain evidence proving no link to the XUAR. In this context, CBP's focus is not on the responsible sourcing program itself, but on supply chain documentation showing no connection to the XUAR region; in other words, raw evidence showing the compliance program working in practice.⁶
- « Australia, Canada, and the United Kingdom each require companies to publicly disclose their efforts to address modern slavery risks. These laws require annual statements detailing governance, risk assessment procedures, mitigation actions, and mechanisms for measuring effectiveness.⁷

Moreover, new and overlapping compliance risks are reinforcing the need for a consistent and integrated approach to program design and assurance. For example, in recent years, we have seen the introduction of data privacy, cyber security and responsible artificial intelligence (AI) laws and associated compliance program guidance. A more holistic, flexible and less U.S./FCPA-orientated approach to the measurement of program effectiveness is required.

Other Stakeholders Are Interested in Compliance Program Effectiveness

Stakeholders interested in the effectiveness of compliance programs now extend well beyond prosecutors and regulators. Ethics and compliance professionals are already familiar with responding to FCPA-driven questionnaires and books and records audits from customers. But the universe of stakeholders has expanded dramatically in recent years, and each have their own unique substantive and evidentiary requirements. For example:

- « **ISO Auditors:** Some companies are submitting themselves to independent assessment against compliance-related audit standards, such as those maintained by the International Standards Organization (ISO).⁸ Auditors require detailed supporting evidence of compliance with these standards.

⁵ CTPAT U.S. Importers Minimum Security Criteria (CBP Publication 1747-0422). Also see CTPAT "Forced Labor Requirements Frequently Asked Questions", last updated June 2023.

⁶ The UFLPA is enforced under Section 307 *Tariff Act* of 1930, codified at 19 U.S.C. § 1307, which prohibits the importation of goods mined, produced, or manufactured wholly or in part by forced labor, including forced or indentured child labor. See also CBP "Uyghur Forced Labor Prevention Act (UFLPA) Enforcement: Frequently Asked Questions".

⁷ *Modern Slavery Act 2015* (UK), c. 30, § 54; *Modern Slavery Act 2018* (Cth) (Australia), Part 2, §§ 13–16; *Fighting Against Forced Labour and Child Labour in Supply Chains Act*, S.C. 2023, c. 9 (Canada), §§ 4–11.

⁸ Key ISO standards relevant to ethics and compliance programs include: *ISO 37301:2021 (Compliance Management Systems – Requirements with Guidance for Use)*, which provides a certifiable standard for establishing, developing, implementing, evaluating, maintaining, and improving an effective compliance management system; *ISO 37001:2016 (Anti-Bribery Management Systems)*, which outlines requirements and guidance for implementing measures to prevent, detect, and respond to bribery; and *ISO 37002:2021 (Whistleblowing Management Systems – Guidelines)*, which offers a framework for receiving, assessing, and managing whistleblower reports while ensuring confidentiality and protection from retaliation.

- « **Sustainability Auditors:** Certain ethics and compliance program elements (e.g., grievance mechanisms) are now routinely evaluated in broader sustainability audits.⁹ The focus of and required supporting evidence for these audits can differ substantially from traditional FCPA books and records or ISO compliance audits. For example, more detailed evidence of consultation with affected rightsholders (e.g., employees of direct/indirect suppliers, members of the local community) may need to be maintained.
- « **Marketing Standards & Indices:** Marketing-oriented certifications - such as Ethisphere's World's Most Ethical Companies designation – and sustainability ratings/indices require the periodic production of specific supporting evidence.¹⁰
- « **Public Reporting Controllers & Auditors:** Compliance-related disclosures in sustainability and modern slavery reports are the subject of SOX-style internal controls and independent assurance.¹¹
- « **Providers of Public Financing:** Public and multilateral funding bodies often require applicants to undergo ethics and compliance due diligence as a condition for receiving grants or financing.¹²
- « **Company Management:** Your own company may require you to report on specific performance measures. Many companies utilize Objectives & Key Results (OKRs) to track business unit and function performance, each with their own unique evidentiary requirements.

But perhaps the most important stakeholder is you, the ethics and compliance officer. You and your team have invested significant time, energy, and political capital in building the compliance program. You want assurance that those efforts are delivering an efficient and cost-effective program that is *working*; one that can disincentivize, prevent, detect, and respond to conduct that breaks the law or your company's values.

⁹ For example, the Initiative for Responsible Mining Assurance (IRMA) *Standard for Responsible Mining* includes specific ethics and compliance-related requirements. These include measures to prevent corruption and bribery (Chapter 1.6), such as prohibitions on facilitation payments, obligations to implement anti-corruption policies, and expectations for training and reporting. IRMA also requires that sites implement operational-level grievance mechanisms that are accessible, transparent, and effective (Chapter 2.10), aligning with the UN Guiding Principles on Business and Human Rights. See: IRMA Standard for Responsible Mining, Version 1.0 (2018), with draft Version 2.0 currently the subject of consultation.

¹⁰ Examples include Ecovadis, Sustainalytics and the Dow Jones Sustainability Index.

¹¹ For example, the *European Commission Directive 2022/2464 amending Directive 2013/34/EU as regards corporate sustainability reporting* known as the *Corporate Reporting Sustainability Diligence Directive* (CSRD) requires companies to implement internal control systems for sustainability disclosures, many of which touch on ethics and compliance (e.g., anti-corruption, due diligence, grievance mechanisms); World Business Council for Sustainable Development, *Internal Controls over Sustainability Reporting (ICSR): Executive Summary* (2023).

¹² World Bank, *Procurement Regulations for IPF Borrowers* (2020), Sections 3.14–3.17 (mandating integrity, fairness, and transparency in procurement and allowing for enhanced due diligence in high-risk contexts); U.S. Office of Management and Budget, *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards*, 2 CFR Part 200 (requiring internal controls and compliance with applicable laws and regulations as a condition of federal grant funding); OECD, *Recommendation on Public Integrity* (2017), para. IV.15 (encouraging public entities to conduct integrity screening of recipients of public funds, including pre-grant due diligence).

What is “Compliance Program Effectiveness”?

The inherently subjective and elusive nature of compliance program effectiveness is perhaps the reason it is the subject of so much debate. A starting point is to consider the desired *outcome* of a compliance program. At the most simplistic level, an effective ethics & compliance program is one that ensures that a company (including its employees and associated third parties) complies with the applicable law (compliance), and the company’s core values (ethics). But this clearly requires some unpacking:

Is the Program Preventing Breaches of the Applicable Law?

- ⌞ **Incentives:** Are employees and third parties incentivized to act or not act (e.g., through compensation) in accordance with the law, company values and policies? Conversely, are they disincentivized (e.g., through discipline) to act inappropriately?
- ⌞ **Culture:** Is there a healthy workplace culture, reinforced by management, that encourages employees and third parties to comply with the applicable law? Is there explicit or implicit pressure to not comply?
- ⌞ **Controls:** Are employees and third parties aware of company requirements to manage the applicable legal risk? Do they understand them, and know how to apply them in their day-to-day work? Are they following those requirements? Even if an employee or third party deliberately, recklessly or innocently acts in breach of those company requirements, does the company have process and system controls that prevent a violation of the applicable law?

Is the Program Detecting Potential Breaches of the Applicable Law?

- ⌞ **Monitoring & Audit:** Is the company able to detect employee non-compliance with company requirements, and/or potential violations of the applicable law?
- ⌞ **Investigations:** Is there a culture within the company of speaking up when potential violations are identified? Conversely, is there a fear of futility (“nothing will be done if I report”) or retaliation? Is the investigation process rigorous enough, and are the investigators sufficiently experienced, to identify misconduct?

Are Identified Program Breaches & Weaknesses Being Addressed?

- **Root Cause:** Is there a practice of identifying underlying root causes for breaches of company requirements identified during monitoring, audits and investigations?
- **Remediation & Continuous Improvement:** Is the remediation for identified root causes appropriate? Has the remediation been completed?

These questions are illustrative, and by no means comprehensive. Some compliance programs may have goals that differ to the above, such as the modern slavery requirements of rightsholder consultation, remediation and public reporting mentioned above. This serves to reinforce the importance of actively considering the desired outcome of a compliance program, and the impact that has on its design and associated testing. We also challenge the concept that making a program more effective means doing “more” – in some instances, a program can be made more effective through simplification or even elimination of program requirements.

How Can Compliance Program Effectiveness Be Measured?

The U.S. DOJ's Justice Manual (expanded upon by the ECCP) provides a helpful starting point for the effectiveness evaluation of any compliance program. The DOJ asks 3 foundational questions:

- ⌞ Is the corporation's compliance program well designed?
- ⌞ Is the program being applied earnestly and in good faith?
- ⌞ Does the corporation's compliance program work in practice?

We refer to these effectiveness measures as Program Design, Empowerment and Execution respectively. Behind each of these three measures, there is an implicit fourth: is there Evidence to support this "measurement" of program effectiveness? If not, you cannot fully answer the three preceding questions.

Despite the increasing range of compliance program drivers and heightened evidentiary expectations, the way program effectiveness is evaluated has not kept pace. For example, program assessments have tended to be:

- ⌞ Periodic, snapshot, exercises whose value quickly fades as the information upon which the assessment is based becomes dated.
- ⌞ Too generic, attempting to tackle entire compliance (e.g., anti-corruption) or even "ethics & compliance" programs.
- ⌞ Too narrow in scope focusing solely on program design, and employee compliance metrics.
- ⌞ Conducted in isolation of other areas of compliance or related businesses processes.
- ⌞ Conducted by outside advisers who do not have sufficient in-house experience of compliance and business processes, systems, data analytics, metadata, and the pressures compliance teams face building and operating a compliance program.

In this article, we advocate taking a more intentional, data-driven and technology-enabled approach to continuous program effectiveness assessment through:

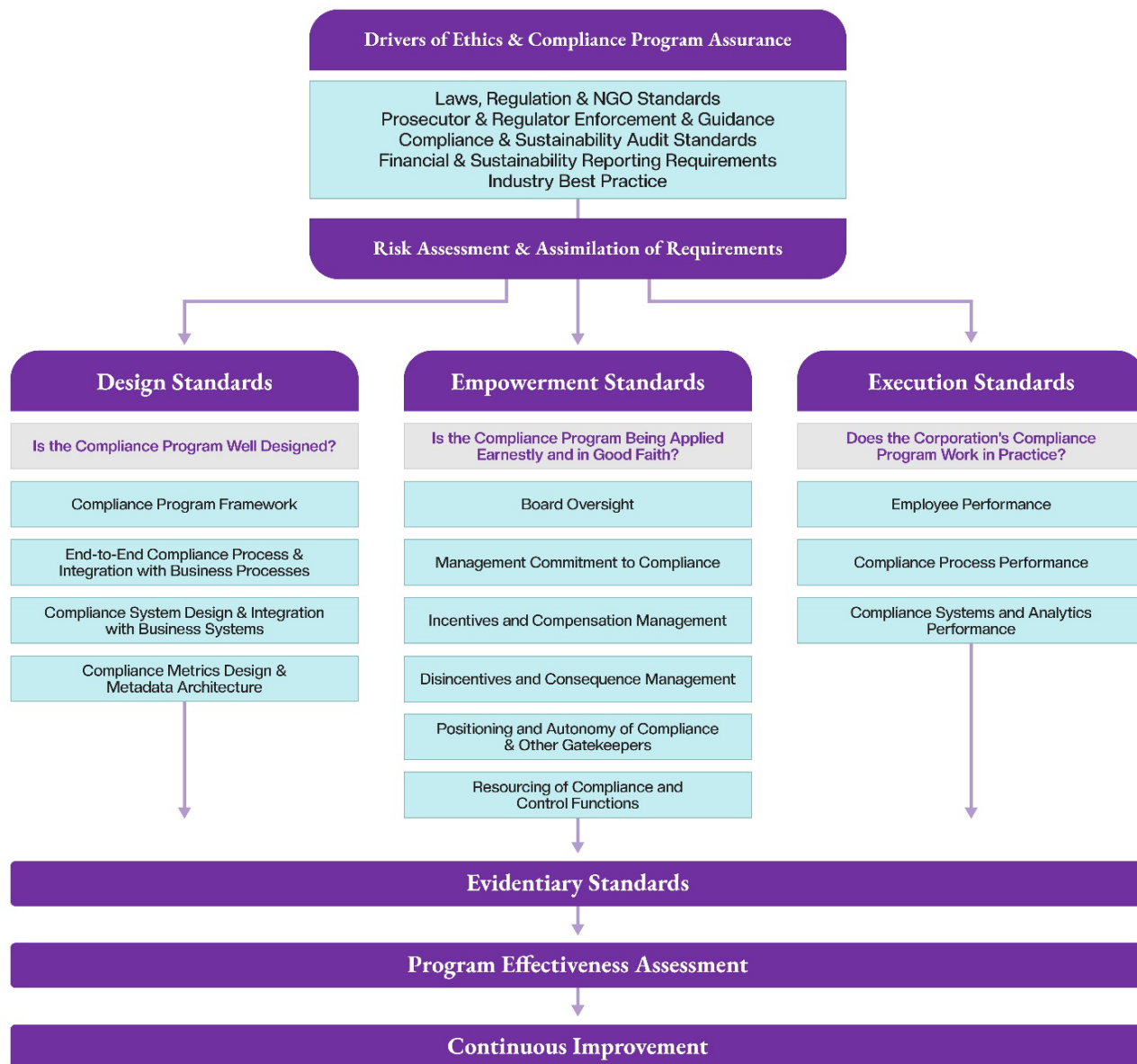
- ⌞ Risk-based prioritization of program testing.
- ⌞ Development of clear performance standards relating to program design, empowerment and execution.
- ⌞ Identification, maintenance and tracking of supporting evidence for each performance standard.
- ⌞ Selection of the right people to undertake each type of testing.



This intentional approach requires conscious investment of time and resources. However, generative artificial intelligence (Gen AI) offers the opportunity to reduce this burden, and extract even more insights into compliance program effectiveness. Throughout this article, we highlight ways in which Gen AI can support your program effectiveness testing.

This article references the related concepts of compliance risk and cultural health assessments, to the extent that they serve as inputs to/beneficiaries of a program effectiveness assessment. Full treatment of these important topics is outside the scope of this article.

Framework for Compliance Program Effectiveness Testing*



* This framework can also be applied to related business processes and systems (e.g., accounts payable, employee expense management and delegations of authority)

B. FRAMEWORK FOR ASSESSING PROGRAM EFFECTIVENESS

Determining Which Compliance “Program” to Test

As indicated above, the traditional approach has been to assess programs at the ethics & compliance or substantive risk level (e.g., anti-corruption, antitrust). Such high-level assessments often fail to consider the design, and execution realities of individual program elements. For example, the practical management of anti-corruption risk associated with charitable donations differs to the management of vendors involved in government permitting processes. Moreover, the charitable donations program should not be solely assessed through an anti-corruption lens; such donations give rise to tax, reputational and other risks.

Adopting our recommended approach to program assurance requires time, focus, and engagement across the organization. It is neither practical nor necessary to apply this level of rigor across the entire ethics & compliance program all at once.

Instead, go narrow and go deep. Focus on a company’s highest compliance-risk activities and assess the specific program elements that manage the risk. Take the example of a global construction company that relies heavily on government-facing vendors to secure local building permits in countries with elevated corruption risk. In this scenario, an obvious candidate for program assurance would be the anti-bribery & corruption third-party due diligence program. At the same time, the company might also consider reviewing the effectiveness of related procurement and finance processes such as vendor qualification, competitive sourcing, and accounts payable.

Then move on to the next compliance program element. Over time, a series of maintained deep-dive reviews can collectively form a reliable basis for assurance across broader risk areas (e.g., anti-corruption). The table below provides a representative map of elements of an anti-corruption program that could be prioritized and tested according to the materiality of the bribery & corruption risk that they manage:

Activity	Compliance Program/System Elements to be Tested	Business Process/System Elements to be Tested
Sales	ABAC Due Diligence on Sales Intermediaries Compliance Due Diligence Platform	Third-Party Screening Customer On-Boarding/CRM System Customer Contract Management Delegation of Authority Inquire to Cash/Accounts Receivable
Procurement	ABAC Due Diligence on High-Risk Vendors Compliance Due Diligence Platform	Third-Party Screening Vendor Qualification/Competitive Sourcing Vendor Risk Management Platform Vendor Contract Management Delegation of Authority/Accounts Payable

Activity	Compliance Program/System Elements to be Tested	Business Process/System Elements to be Tested
External Affairs	ABAC Program Governing Direct Engagement with Government Officials	Charitable Donations Process/Platform Community Projects Process/Platform Commercial Sponsorships Process/Platform Lobbying Disclosure Political Donations
Human Resources	Hiring Current/Former Government Officials	Prospective/Current Employee Screening
Finance	Gifts & Hospitality	Employee Expense Management Process/Platform Corporate Purchasing Cards Process/Platform Petty Cash
M&A/JVs	Pre & Post Acquisition ABAC Due Diligence	M&A/Business Development Process

The remaining focus of this article will be the testing of specific compliance program and business process elements such as those listed above. However, it is worth noting that an *enterprise* level assessment of these program elements may also be merited. For example, an enterprise level design assessment of:

- « **Risk Assessment** would involve a review of the design of company's group level compliance risk assessment process, and its integration with broader enterprise risk management processes.
- « **Policies and Procedures** might include a review of the company's policy on policies, and the configuration of its policy management system and supporting metadata.
- « **Controls** could include an assessment of how compliance controls are managed within the company's broader (SOX) controls process and platform, and how compliance-related approvals align with a company's delegation of authority.
- « **Training & Communications** would involve a review of the company's enterprise training strategy and governance, the configuration of its learning management system and supporting metadata and how compliance training fits within this.
- « **Third-Party Management** would include an assessment of third-party screening processes and platforms, and how they integrate with know your customer, supplier qualification and enhanced compliance due diligence processes.
- « **Audits** would involve a review of the company process for planning, execution and remediation of audits and unique considerations relevant to compliance-related audits.

Mapping Relevant Compliance Program & Evidentiary Requirements

Having selected the program (element), what are the drivers of the relevant testing framework?

The design, empowerment, execution and evidentiary requirements of a compliance program are obviously driven by the relevant legal risk assessment.¹³ While the laws themselves rarely go into the minutiae of compliance program design, the enforcement practices and guidance of prosecutors and regulators form the foundation of program effectiveness measures.¹⁴



While not a substitute for legal advice, or constituting a full program effectiveness assessment, AI-driven gap assessments of a company's existing policies and procedures against applicable regulatory frameworks are now being offered by several companies.

However, regulation, enforcement and government guidance are not the only drivers of program effectiveness; mindful of the stakeholders referenced above, there may also be quasi-legal, audit and other requirements that need to be considered:

- ⚡ Compliance program guidance issued by Non-Governmental Organizations.¹⁵
- ⚡ ISO, sustainability and other audit standards and the evidentiary requirements of auditors.¹⁶
- ⚡ Public reporting standards, and the evidentiary assurance required by financial controllers and auditors.¹⁷
- ⚡ Customer compliance and sustainability questionnaires.
- ⚡ Contractual commitments owed to business partners and lenders relating to compliance performance.
- ⚡ Compliance benchmarks and industry-specific best practices.¹⁸
- ⚡ Company requirements relating to performance measurement, budgeting, planning and project management.

¹³ The U.S. Department of Justice takes a similar risk-based approach when reviewing the effectiveness of compliance programs. In the ECCP they state: “We recognize that each company’s risk profile and solutions to reduce its risks warrant particularized evaluation. Accordingly, we make a reasonable, individualized determination in each case that considers various factors including, but not limited to, the company’s size, industry, geographic footprint, regulatory landscape, and other factors, both internal and external to the company’s operations, that might impact its compliance program.”

¹⁴ Examples include DOJ & SEC, *A Resource Guide to the U.S. Foreign Corrupt Practices Act* (2nd ed., 2020); DOJ, *Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations* (November 2024); European Commission, *Compliance Matters: What companies can do better to respect EU competition rules* (2013); U.S. Department of the Treasury, and Office of Foreign Assets Control, *A Framework for OFAC Compliance Commitments* (2019)

¹⁵ Examples include OECD, *2021 Anti-Bribery Recommendation (Annex II: Good Practice Guidance on Internal Controls, Ethics and Compliance)*; OECD, *Guidelines for Multinational Enterprises on Responsible Business Conduct*; OECD *Due Diligence Guidance for Responsible Business Conduct*, and the *Guidelines on Anti-Corruption and Integrity in State-Owned Enterprises*; World Bank, *Integrity Compliance Guidelines* (2020).

¹⁶ See footnote 8, supra.

¹⁷ e.g., CSRD

¹⁸ Integrity Bridge maintains a list of ethics & compliance benchmark reports which is by clicking [here](#).



Understanding the full design and evidentiary scope of these requirements enables your company to make a more informed decision as to the required time and resources to be invested in the applicable program, and the associated framework for measuring effectiveness.



Generative AI can play a role here supplementing pre-existing legal risk assessments by extracting and summarizing the design, empowerment, execution and evidentiary requirements of these other sources. For example, Gen AI can review existing contracts with customers or lenders to identify common and unique program and evidentiary requirements that need to be factored into your program design and testing.

Document Your Standards for Program Effectiveness

In areas of compliance such as environmental or cyber-security, global audit standards (e.g., ISO, NIST) have been accepted as an assimilation of these various drivers into a proxy for program effectiveness. In contrast, for example, the *ISO 37001 Anti-bribery management systems* standard has gained less traction. Moreover, company's SOX controls frameworks may not extend to all compliance controls, and certainly not broader standards of program effectiveness. In this assurance vacuum, the trigger tendency in ethics & compliance has been to move subconsciously straight from risk assessment to program design, governance in particular.

We recommend an intermediary step, assimilating these legal, enforcement, audit, reporting and other drivers - filtered through a company-specific risk assessment - into a tailored series of documented program design, empowerment, execution and evidentiary standards. In this regard, the design and format of SOX controls, ISO and other audit standards can help ethics and compliance professionals to curate their own program effectiveness standards that reflect their organization's unique risk profile and operational reality.

For example, if your company's antitrust risk is high, you may have decided to develop standards relating to employee participation in industry associations. Program design standards would likely include several relating to training, perhaps taken from US, EU and other guidance as well as industry best practice:

- ⌞ Training addressing unique antitrust issues arising from participating in industry associations has been prepared.
- ⌞ The training is tailored to the company's market sector(s) and the associations it participates in.
- ⌞ Outside antitrust counsel, Legal and External Affairs were consulted on the draft training materials, and the employees to be trained.
- ⌞ The format of the training is appropriate for the subject matter and audience.
- ⌞ The employee roles to be automatically assigned industry association antitrust training have been determined.
- ⌞ Records of completed antitrust training are maintained.¹⁹

Empowerment standards might focus on management support for and participation in the training. Execution standards would include not only training completion metrics, but also employee feedback on the quality of training and the impact of the training on employee conduct during association meetings.

¹⁹ DOJ ECCP; U.S. DOJ, *Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations* (November 2024); European Commission, *Compliance Matters: What companies can do better to respect EU competition rules* (2013)

Since training is a type of control, one might observe that this is simply a form of control effectiveness assessment. That would be correct; however, the same type of effectiveness assessment can be applied to program design, empowerment and execution standards beyond controls.

Evaluate All Dimensions of Program Effectiveness

How are these program effectiveness standards to be structured?

There is a tendency for companies to overly focus on program governance, tone from the top communications and employee compliance metrics as proxies for program design, empowerment and execution effectiveness respectively. We submit that the concept of compliance program effectiveness is broader. The table below shows the full scope of compliance program effectiveness, utilizing the DOJ's design, empowerment and execution questions as a guiding framework. The same approach can also be utilized to assess the effectiveness of related business processes, systems and analytics.

Design	Empowerment	Execution
Is the corporation's (compliance) program well-designed?	Is the (compliance) program being applied earnestly and in good faith?	Does the corporation's (compliance) program work in practice?
Compliance program framework design	Board oversight	Employee performance
End-to-end compliance process & integration with relevant business processes	Management commitment to compliance	Compliance process performance
Compliance system design and integration with relevant business systems	Incentives and compensation management	Compliance systems & analytics performance
Compliance metrics design, and supporting meta-data architecture	Disincentives and consequence management	
	Positioning and autonomy of the compliance function and other gatekeepers	
	Resourcing of compliance and control functions	

We consider these elements, and the associated evidence, in more detail in Section D.

Assign The Right People to Undertake Testing

The traditionally narrower focus of program design audits may be a function of who has undertaken them. Outside advisors without prior in-house experience may not have a working understanding of how, in practice, compliance programs work in parallel with each other, or how they are embedded in functional processes and systems. Resulting assessments are reliant on surface-level documentation, tend to be generic in nature and do not offer granular, operational-level recommendations for improvement.

Similarly, simply relying on self-assessments by the relevant “subject matter expert” owner of a specific program raises questions about objectivity and may overlook opportunities and challenges where the program under review intersects with other compliance programs (e.g., corruption -> sanctions and antitrust).

True program effectiveness testing requires a broader team, with the appropriate blend of skills and experience, who can:

- Advise on regulatory and other drivers of program standards.
- Independently review self-assessments prepared by program owners.
- Assess the effectiveness of integration between different areas of compliance, with business processes and supporting systems.

When designing your performance standards, it will often become clear as to who is best placed to test performance against each standard.

C. THE INTENTIONAL DEVELOPMENT & MAINTENANCE OF SUPPORTING EVIDENCE

The utilization of program effectiveness standards allows you to identify upfront the evidence required to test whether your program meets each standard. Such evidence falls into several categories:

- ⚡ Self-assessment by the person responsible for meeting the standard.
- ⚡ Documentary evidence.
- ⚡ Metrics, supported by metadata.

Maintain a Living Narrative Against Your Program Effectiveness Standards

As part of their due diligence program, companies willingly send out detailed questionnaires to third parties asking them to describe their corporate compliance programs. In their diligence platforms, they will maintain and periodically seek updates to hundreds of these program narratives. And yet, curiously, such narratives are rarely maintained about *their own* compliance program.

Moreover, supporting documentary evidence of a program can only tell half the story. For example, compliance policies and training materials are rightly focused on the positive obligations and prohibitions that employees must follow. They rarely include a narrative as to how these materials were put together, who was consulted or how they are being administered in practice, nor should they. But this does not preclude the need for a contemporaneous narrative to accompany the policy or training material.

At the heart of program effectiveness assurance is the self-assessment narrative; an explanation of how your company is performing against program design, empowerment and execution standards. The person best placed to provide that program narrative is likely the program or process owner responsible for meeting the standard.

Continuing with the industry association antitrust training example, let's focus on the narrative for the following design standard:

The employee roles to be assigned industry association antitrust training have been determined

The responsible person might document the following:

Industry association training is assigned to (a) all employees in external affairs; (b) all employees serving on an industry association board or committee; (c) all employees who are sponsors of company participation in the association. Compliance obtains details of new employees falling into these categories from external affairs, which is responsible for the company's membership of industry associations. We are exploring opportunities to expedite the training assignment process in our Learning Management System, by automating the extraction of employee data from external affairs.

The act of preparing the self-assessment enables the responsible person to identify existing gaps, and area of planned improvement. The narrative does not need to be extensive, but it helps others to review how the responsible person is meeting the standard. For example, the chief compliance officer might provide feedback to the antitrust program owner that members of management above a certain grade should also

receive the training, given the likelihood that they may participate in industry association events from time to time.

Retain Documentary Evidence with Rigor & Consistency

Program narrative is important but is not sufficient by itself. Assurance is also dependent on the consistent retention of supporting evidence, the nature of which is heavily dependent on the program element being assessed and the type of program assessment (design, empowerment or execution) being undertaken. Such evidence could include:

- ❧ Current and archived versions of program documentation (even drafts with stakeholder comments and responses if evidence of prior consultation is needed).
- ❧ Communications via email, company intranet and other broadcast communication tools.
- ❧ Training materials and records.
- ❧ Agendas, minutes of meetings and associated presentation materials.
- ❧ Approvals, signoffs and attestations.
- ❧ Survey results.
- ❧ Photos.

For program elements supported by compliance or other platforms, the collation of this information can be built into the process. For example, for due diligence of high-risk third parties, approval workflows could make the uploading of meeting minutes with senior leadership mandatory.

For other records there may need to be an intentional decision as to where they are maintained. Compliance tech providers (training, diligence, investigations) tend to be focused on the execution of their process rather than serving as the complete system of record for all supporting evidence of program effectiveness. In this situation, being clear as to where and how other supporting evidence is being filed and retained is critical. That all-important evidence needed in response to a future investigation or audit will not be found if it's in the wrong place and has an unclear filename. Your colleagues in other functions with experience on managing SOX controls assurance or responses to ISO audits may be able to guide you here on best practices.

Identify The Most Useful Metrics

While the focus tends to be on metrics relating to employee compliance, metrics can serve as a proxy for the effectiveness of all aspects of design, empowerment and execution. This is addressed further in Section D

Here we focus on some generic considerations relating to metrics:

- ❧ Basic metrics, such as training completion rates or the volume of calls to a whistleblower hotline, have long been a staple of compliance dashboards. But their utility as proxies for program effectiveness is limited. A high training completion rate, for instance, says little about what

employees actually understood or how they apply that knowledge in real-life scenarios.²⁰ Greater insights on program effectiveness can be obtained by combining different metric sets; using data on one program element (e.g., training completion) to understand the impact on another (e.g., compliance controls performance, speak up culture). These “cross-over” analytics are dependent on different data sets utilizing the same common metadata “keys” (e.g., employee identification number, business unit description, country name).²¹

- ⌞ The challenge with more sophisticated metrics is twofold: first, the underlying data is often spread across multiple platforms; second, many technology providers focus on standardized analytics that serve a broad client base, leaving companies with limited ability to extract custom insights. Advanced program effectiveness metrics may require the development of in-house data analytics capabilities (now made easier using Gen AI).²²
- ⌞ Moreover, program effectiveness metrics should not be evaluated in isolation. They must be assessed alongside broader cultural health metrics - such as employee engagement and comfort with raising concerns - which speak to the likelihood of an employee engaging in inappropriate conduct, and such conduct being reported.
- ⌞ Ethics & compliance metrics have traditionally been lagging indicators, capturing a record of activity after the event. More recently, real-time monitoring has supported the development of coincident indicators that may prevent high-risk transactions from being completed. The aspiration – clearly – is to develop leading indicators, metrics that can accurately predict *future* adverse outcomes, enabling targeted preventative action.



Generative AI has the potential to assimilate structured data (such as metrics) and unstructured information to provide even richer insights as to potential weaknesses in program effectiveness or cultural health.

- ⌞ In the same way that policies and training materials are reviewed for effectiveness, metrics should be subjected to similar scrutiny. Is the metric truly providing meaningful insight? If not, should it be retained? Is the metric in a form that can be easily accessed and understood by stakeholders? Is it being utilized by compliance and management? In other words, is it at least triggering a conversation between the right stakeholders, and remediation where appropriate? If not, why not?

²⁰ See Chen, Hui & Soltes, Eugene, *Why Compliance Programs Fail—and How to Fix Them*, *Harvard Business Review* (March–April 2018). Chen and Soltes highlight that compliance metrics frequently measure inputs rather than meaningful outcomes or behavioral changes, limiting their value in assessing real-world effectiveness; Also see Soltes, Eugene F. “*Evaluating the Effectiveness of Corporate Compliance Programs: Establishing a Model for Prosecutors, Courts, and Firms.*” *NYU Journal of Law & Business* 14, no. 3 (Summer 2018): 965–1011.

²¹ See Moosmayer, Klaus, *Ethics & Integrated Assurance: The Challenge of Building Trust*, *Risk & Compliance Magazine* (April 2024). Moosmayer recommends that compliance and audit functions adopt a joint taxonomy for root cause analysis and remediation activities, enabling consistent classification and reporting to improve transparency and cross-functional assurance.

²² For practical considerations relating to the development of ethics & compliance data analytics programs, please see the Applied Compliance section on data analytics, which contains several articles and podcasts on this topic: www.appliedcompliance.com

Extract All Useful Metadata

Metrics are inherently depending on supporting metadata. Some compliance platforms - such as training, due diligence, and investigations - produce structured data. This can be utilized within or exported from the relevant system and used in cultural health and compliance program effectiveness metrics.

Other compliance activity, particularly that administered outside of workflow platforms, generate unstructured information. In these cases, compliance teams should seek to identify and extract “micro-data” points that can be tracked and compared over time. For example, common measures of program execution effectiveness and cultural health relate to the level of employee engagement with the program. The program owner may already have metadata associated with employee completion of training and survey feedback on the quality of training. The owner might also have data relating to employee engagement with program governance from the company’s policy management system. But there are other potentially valuable data “nuggets” out there, residing in *unstructured* information such as:

- ⏪ Program communications: When was the communication sent and who was it sent to?
- ⏪ Number of program-related questions raised by employees: these questions might be posed via the company’s speak up helpline, but they can also be posed directly of the compliance team or via policy chatbots. Can these questions also be tracked in an easy way?



In the past, the manual effort required to convert such information into structured data may have precluded its extraction and use. However, tools are available that can intelligently read uploaded documents and do that metadata extraction for you. These data points, while small in isolation, can “roll up” and provide an even richer insight into the level of employee engagement with the program.

D. TESTING COMPLIANCE PROGRAM EFFECTIVENESS IN PRACTICE

In this section we demonstrate how this program effectiveness testing can work in practice. For program design, empowerment and execution standards, we consider in detail the relevant supporting evidence of effectiveness.

Design: Is The Compliance Program Well Designed?

Compliance Program Framework Design

There are multiple U.S. and international sources of guidance on the effective design of general corporate and risk-specific compliance programs. For the selected compliance program element, these can be distilled into a series of generic and company-specific design standards or “hallmarks”, and grouped as follows:

- ⌞ Risk assessment
- ⌞ Policies and procedures
- ⌞ Controls
- ⌞ Training & communications
- ⌞ Third party risk management
- ⌞ Monitoring and audit
- ⌞ Investigations and consequence management

It is perhaps program design standards where the self-assessment narrative is most important. Such narrative serves to complement the program governance materials and other supporting documentation. For example, policies and training materials typically do not address:

- ⌞ The applicable risk analysis and/or legal/regulatory obligations.
- ⌞ Who was consulted during development and how their feedback was addressed.
- ⌞ How the intended audience was determined, and its impact on the format and content of material.

And yet prosecutors, regulators, and auditors place significant weight on this kind of supporting program evidence. A review of U.S. government guidance reveals over 40 criteria relating to how compliance training should be designed, delivered, and monitored - yet the evidence maintained is often limited to the training material and metrics relating to training completion.²³

²³ *United States Sentencing Guidelines Manual* § 8B2.1; U.S. DOJ, *ECCP* (2024); U.S. DOJ, *Attachment C*; U.S. DOJ and SEC, *A Resource Guide to the U.S. Foreign Corrupt Practices Act* (2nd ed., 2020); U.S. DOJ, *Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations* (2024); U.S. Department of the Treasury, Office of Foreign Assets Control, *A Framework for OFAC Compliance Commitments* (2019); U.S. Department of Health & Human Services, Office of Inspector General, *General Compliance Program Guidance* (2023).

The absence of such a narrative, prepared at the time of developing the policy or training material, makes it difficult to defend the adequacy of the program element in future investigations or audits. And creating narratives after the fact is challenging and risky – critical context can be missed or misremembered and could potentially put the company at risk.

A common refrain is that the creation of such a self-assessment narrative might itself be the source of legal risk, particularly if it is not privileged and prosecutors, regulators and litigants have access to it. We submit that the benefits of maintaining such a narrative exceed the risks arising from discoverability. If truly necessary, privileged could be asserted on the basis that the narrative was prepared for the purposes of seeking legal advice from in-house compliance or outside counsel. But doing so could, ironically, undermine the value of the assessment. Firstly, to preserve legal privilege, access to the narrative would need to be more tightly controlled. Second, conducting the assessment through a legal filter could result in its sanitization undermining its helpfulness as an honest assessment of what is and is not working. This is not to say that a conversation about how such narratives should be prepared should not be had.

Other supporting evidence relating to program design include current and archived:

- ⌞ governance (policies, procedures, controls)
- ⌞ training materials and communications
- ⌞ supporting process materials (e.g., questionnaires, forms, workflows and process maps)

and evidence relating to stakeholder consultation on the above materials.

End-to-End Compliance Process

Assessing the design of a compliance program element according to category (e.g., policies and procedures, training & communications) provides helpful structure, but it does not represent the full picture of design effectiveness.

A supplementary approach is to review how these elements interact with each other in the relevant end-to-end compliance process, and how they interact with related business processes. For example, a review of the design of a company's sales intermediary ABAC due diligence and monitoring process might involve the review of the:

- ⌞ Trigger(s) for ABAC due diligence of sales intermediaries within the customer/sales agent onboarding process (evidence: copies of relevant sales/KYC policies and procedures).
- ⌞ Information required from sales intermediaries and the internal sponsor (archived and current versions of due diligence questionnaires).
- ⌞ Frameworks for assigning a risk rating to a sales intermediary, and the diligence required for each risk level; (due diligence procedure).
- ⌞ Required documentation of due diligence, and how that is communicated to stakeholders (diligence reports or summaries).
- ⌞ Approval of sales intermediaries with differing levels of risk (minutes of meetings, evidence of management approval) and how that aligns with commercial approvals in accordance with a company's financial and contractual delegations of authority.



- ⌞ Completion of required remediation.
- ⌞ Scope and design of reputational monitoring, transaction testing and books & records audits.
- ⌞ Conduct of refresh due diligence.

As noted above, a review of a sales intermediary ABAC due diligence program might be supplemented with the parallel review of related business processes such as inquire to cash.

Compliance System Design

A compliance program design review should extend to the configuration of the supporting compliance system, and its integration with relevant business systems. Continuing the sales intermediary ABAC due diligence example, this would involve a review of the due diligence platform for:

- ⌞ Integration with other compliance systems (e.g., third-party screening).
- ⌞ Questionnaire and workflow approval functionality (evidence: process maps).
- ⌞ The accessibility of metadata to support metrics (metadata maps).
- ⌞ The sufficiency of metrics and dashboard visualizations offered by the system provider, and those developed in-house.
- ⌞ The design of system controls preventing the utilization of a sales intermediary which has not been approved; where refresh due diligence or remediation has not been completed timely; or where a red flag has arisen.

This might also be supplemented with a review of the company's CRM and ERP systems as to the management of sales intermediaries, to test if the customer onboarding and inquire to cash processes are working in practice.

Empowerment: Is The Program Applied Earnestly and In Good Faith?

"In other words, is the program adequately resourced and empowered to function effectively?"²⁴

The DOJ ECCP covers this in detail, and we do not intend to fully restate the relevant standards here. Instead, we focus on the supporting *evidence* that can demonstrate the relevant program was set up for success.

Board Oversight

At the enterprise level, evidence of board oversight – and the chief compliance officer's relationship with the board – can be found in board agendas, meeting minutes and the terms of reference of committee(s) that the CCO reports into. Retention of such formal records is typically the responsibility of the company secretary and generally poses minimal concerns in terms of access. If possible, committee minutes should record the fact (if not the substance) of any executive sessions held with the CCO. Similarly, recording basic details (e.g., dates, topics) of any ad hoc engagement with board members can be helpful.

²⁴ DOJ ECCP

Evidence of board oversight of individual programs or program elements is equally valuable and may require some intentionality as to how and where such evidence is maintained. For example, if a quarterly presentation to the audit & finance committee includes a deep dive on the company's antitrust compliance program, there would be a merit in storing a copy of those materials alongside all your other antitrust program materials (while respective privilege considerations, if any). Moreover, aspects of a company's compliance program may be addressed in other board committee meetings. For example, the management of anti-corruption risk associated with engagement with indigenous communities might be addressed in the board's sustainability committee.

Senior and Middle Management to Compliance

At a minimum this would include communications from leadership on their commitment to compliance, and support for the relevant program. However, ethical leadership in action is much more compelling evidence of tone from the top or middle. For example, has leadership decided to change their go-to-market strategy to manage compliance and other risks? Do they actively participate in meetings reviewing compliance-sensitive third parties or activities? Do they proactively invite ethics & compliance managers to be a member of their business unit or regional leadership team? During meetings do they demonstrably refer to the company's values and Code for guidance? While capturing such evidence (e.g., strategy presentations, meeting minutes, anecdotal stories) might be more challenging than the logging of tone-from-the-top communications, its demonstrative value of management commitment in practice is significant.

Compensation and Consequence Management

How company leadership designs employee incentives, rewards individual employees for "performance" and disciplines employees for misconduct represents one specific and important proxy for management commitment to compliance. Incentivizing employees to work according to a company's values, even if that means not meeting sales or other performance targets, is one of the most important preventative measures in a compliance program. As is robust and consistent enforcement of discipline for misconduct.

Having auditable standards and evidence relating to a company's enterprise level performance appraisal and disciplinary process is important. However, a similar assessment can and should be undertaken at a narrower, tactical, program element level. For example, if you are reviewing the design and execution of your company's sales intermediary due diligence program, this should involve an assessment of explicit and implicit incentives for the sales team to act in compliance with or violation of the program or applicable laws. Is there a special incentive program for sales teams that include unreasonably high revenue targets? Do the contracts with customers impose performance standards that would incentivize sales or supply chain teams to cut corners? Similarly, are there performance or disciplinary consequences for employees who fail to follow the due diligence process? Are those consequences consistently applied? Assessing *and documenting* incentives and consequences at a program element level is an important part of your assurance process.

Positioning and Autonomy of the Compliance Function and Other Gatekeepers

There is much official and industry commentary on the importance of the positioning and independence of the chief compliance officer. *Evidence* of this should be diligently maintained and can include (a) grade and compensation; (b) extent and nature of contact with the board (including participation in executive sessions); (c) participation in management committees (e.g., compliance, sustainability, disclosure) and leadership team meetings; and (d) early involvement in M&A and other strategic initiatives.

However, other evidence is relevant when considering the positioning and autonomy of the broader compliance team in the tactical execution of individual program elements. For example, in relation to third-party screening and due diligence, does a compliance manager have the authority to reject a new or block an existing third party found to have material compliance concerns? How many third parties have they blocked? Is that authority undermined in practice by business leaders “going over the top” and escalating to senior executives who can over-rule the compliance manager or even the chief compliance officer? During investigations, is there evidence of management seeking to interfere with the conduct or influence the outcome of the investigation?

There is much focus on the completion of cultural health and/or program effectiveness surveys by employees. But junior members of the compliance team and other stakeholder functions are exposed to somewhat unique pressures that may require a tailored approach in terms of being heard. This could be through mentoring or a dedicated survey; the key is that compliance professionals feel comfortable speaking up about any challenges to their authority and independence, and that those concerns are being addressed.

Resourcing of Compliance and Control Functions

The cut and thrust of the annual planning and budget setting season can be a testing time for chief compliance officers and their teams. From a documentary perspective, your finance function is focused on the numbers. Maintaining that budget information is important, including how your budget compares with other functions. But a spreadsheet or system-generated report only tells half the story and may even be counter-productive if that is your only maintained evidence of compliance resourcing discussions, and it shows year-over-year *decreases*. If the compliance budget was supported by an accompanying management presentation, it is important to retain that together with a contemporaneous record of the discussion with management.

Execution: Does the Corporation’s Compliance Program Work in Practice?

It might be tempting to conclude that the absence of specific compliance concerns over time means that the relevant program is working. Without additional program assurance, that would be a dangerous assumption to make. For example:

- ⌞ How can you be sure that there haven’t been any compliance concerns? Are employees comfortable about speaking up if they see such a concern? Are your preventative controls working? Is your monitoring configured correctly? Have relevant investigations been conducted appropriately?
- ⌞ Are you sure there are no bottlenecks in your compliance process causing frustrated employees to cut corners with compliance and related business processes?
- ⌞ Even if there haven’t been any concerns to date, has there been a recent change in employee pressures, incentives or broader ethical culture such that a compliance concern might be imminent?

A perfectly working program is also an elusive, and perhaps unrealistic goal. Instead, focus on gathering more proxies for execution effectiveness to provide you a richer picture of what is working, and what is not. These measures can be grouped into three categories: employee performance, compliance & business process performance and systems & analytics performance.

Employee Performance

Monitoring employee activity in relation to the compliance program is the obvious starting point. There is a temptation to jump straight to employee *compliance* metrics but there are several valuable precursor measures that can offer a richer picture:

- ⌞ **Awareness of Program Requirements:** this can be tested through surveys, audit interviews and/or ad hoc employee engagement by the compliance team. This measure serves as a particularly useful measure of the program's training and communications -> is the message getting through?
- ⌞ **Comprehension:** Do employees know how to behave in a compliance-sensitive situation? Do they understand when specific program obligations (e.g., a pre-approval) apply? This can provide meaningful insights into the quality and accessibility of your policies, training and communications. Is the message *understood*? Testing comprehension is one of the most challenge effectiveness measures. For example, is asking employees to complete a quiz straight after training, an assessment of short-term memory or a real measure of employee understanding? A more effective approach might be to pose those questions several months later, and in context. Your cyber-security teams might already send mock phishing requests to employees to see how they react "in the wild" and provide just-in-time feedback for those who "click on the link". Are similar types of activity possible for the program your testing?
- ⌞ **Engagement:** is the program generating curiosity or any other type of employee engagement? Are they consulting the relevant section of the code or policy? Are they asking questions? Are they completing the assigned training in a timely manner?
- ⌞ **Compliance:** finally, are employees meeting the relevant compliance requirements? That may include a combination of disclosure, consultation or requirement to obtain approval. These control performance metrics are very valuable, but they are also the most challenging to calculate. For example, how can you be sure that 100% of government-facing vendors were the subject of due diligence before use? Is your monitoring robust enough to confirm that? Also, are employees following associated business processes? Your focus might be on the gifts & hospitality program but are employees accurately documenting those gifts in your company's employee expense tool?

These measures collectively provide insight into employee performance with the compliance program under review. Many of these measures of employee engagement and compliance can also feed into broader assessments of cultural health.

Compliance & Business Process Performance

Poor execution of compliance and related business processes can have a significantly detrimental effect on program effectiveness. Delays in conducting due diligence may prompt employees to circumvent that process in the future. A failure to communicate outcomes of an investigation to a reporter, or inconsistent administration of discipline, may adversely affect the local speak up culture. A failure to complete required remediation following a compliance audit might increase risk further.

The optimal way to address this is to communicate compliance performance expectations upfront to the team and other gatekeepers. For example, processes, checklists or templates can serve to enhance the quality, timeliness and consistency of diligence, monitoring and investigations. They also enable compliance



teams to conduct peer reviews of their respective work or for outside advisors to conduct a consistency review against a defined standard.

To provide additional assurance, the development of process performance metrics is critical. For example, what is the average length of diligence and investigations? What % of audit, investigation or third-party remediation is complete? How many purchase requisitions have been rejected for non-compliance?

Employee perceptions of the compliance program are also an important input and can be obtained via risk assessments, audits and surveys. Compliance teams at some companies utilize net promoter scores to track employee sentiment towards a compliance process.

Systems & Analytics Performance

Finally, tracking the performance of relevant systems and analytics is important. For example:

- ⌞ are your system and data integrations working properly?
- ⌞ are you tracking the quality and completeness of compliance, ERP or other system master data?
- ⌞ is your third-party screening or fraud testing yielding too many false positives? Does the sensitivity or risk weighting need to be adjusted?
- ⌞ are you spot checking generative AI for bias or hallucinations?

Ideally the tracking and reporting of systems/analytics performance would be addressed in service level agreements with the relevant internal function or third-party service provider.

E. PRACTICAL CONSIDERATIONS

How & Where Will Program Effectiveness Testing Be Documented?

It is worth spending time thinking carefully about what form your program assurance will take:

- ⌞ Will standards and associated narrative reside in a document (e.g. a spreadsheet) or a platform?
- ⌞ Could your company's existing controls management platform be utilized, allowing you to upload supporting evidence as well?
- ⌞ Should the company invest in a dedicated platform that is specifically designed for self-assessment against program/audit standards and the assembly of supporting documentation?



Innovative technology providers are now utilizing artificial intelligence to undertake the initial assessment of a company's performance against pre-defined audit standards by undertaking the initial review of supporting evidence.

In determining this, it is worth reflecting on what functionality you wish the tool to have either now or in the future. For example:

- ⌞ Would you like to document the regulatory and other drivers for the standard?
- ⌞ Aside from the narrative, would you like the program owner to score the effectiveness of the standard?
- ⌞ Do you wish to have/preserve the ability of other peer reviewers/auditors to document their own assessment?
- ⌞ Can changes to the standard, narrative, scoring and supporting documentation be tracked?
- ⌞ Do you wish to specify upfront the required supporting documentation? And/or allow the program owner to describe the supporting documentation they have provided?
- ⌞ How do you wish to capture relevant metrics (particularly relevant for execution standards)? Are they manually updated or is there the ability to automatically update them? (e.g., an API connection to a learning management system)
- ⌞ Do you wish to capture planned improvements in relation to the standard? And the anticipated budget and status of such improvements?

As evidenced above, your assurance tool can be as simple or advanced as you require, mindful of your design and evidentiary requirements.

Unlocking The Benefits of Your Program Effectiveness Testing

With program assurance standards defined, narratives maintained and supporting evidence organized, you will reap multiple benefits:

- ⌞ Maintaining a narrative against standards helps program owners to identify opportunities for continuous improvement.

- ⚡ The chief compliance officer and other stakeholders are more easily able to keep up to speed with the program.
- ⚡ Facilitates program reporting and responding to third-party questionnaires.
- ⚡ Enhances the quality and expedites the conduct of independent program audits.
- ⚡ Supports metrics relating to not only program effectiveness, but also cultural health.
- ⚡ Represents a robust and defensible program assurance model in the event of a government investigation.

Artificial Intelligence Can Unlock Even More Value



The act of bringing together program assessment narratives, metrics and supporting documentation, and utilizing generative AI to interrogate it, can unlock even more value. By way of illustration, several gen AI use cases are provided below:

Generative AI Use Case	Example Query
Automatic generation of an initial program narrative based on its assessment of supporting evidence against the standards.	<i>"You'll see that I have now completed uploading the remaining supporting documentation in relation to our effectiveness assessment for the company's charitable donations program. Please review the evidence against the program assurance standards and identify documentation gaps where you have been unable to make an assessment."</i>
Identification of hitherto-unseen trends across the full range of program assurance data.	<i>"Please summarize the impact of the compliance team's efforts in 2024 to promote the speak up helpline on (a) the increase in the number of allegations reported; (b) the number of questions raised; and (c) any other type of employee engagement addressed in our various program assessments."</i>
Conversion of unstructured information into structured data that can be used in analytics.	<i>"I am uploading copies of emails sent by several country managers to their teams emphasizing the importance of compliance with our gifts & hospitality program. For each communication, I would like to extract the following data: communication date, name of sender, name of employee recipients and relevant country. For the sender/recipient information I would like you to correlate with our HR information management system and match the employee names to their id number. Please populate all of this information into [document/database/visualization tool] so that we can track the impact of this messaging"</i>
Assessment of the evolution of an individual program element over time.	<i>"Prepare a report summarizing the evolution of our antitrust training program over the past 5 years. In your report, consider how the substantive content has evolved, the audience size and make up has changed and the general level of employee engagement."</i>
Preparation of tailored reports or questionnaire responses for the multiple and increasing number of stakeholders that have an interest in the program.	<i>"Please prepare a draft response to this questionnaire on grievance mechanisms issued by a sustainability index. In your response you should draw from the program effectiveness assessments for (a) Code of Conduct speak up/investigation process;(b) community grievance mechanisms and (c) supply chain grievance mechanisms, as appropriate. Ensure the language style and use of terminology is consistent with that used in the company's last annual sustainability report. If there are inconsistencies in metrics included in the assessments and what was reported in our sustainability report, please let me know"</i>

F. OUR CALL TO ACTION

In recent years we have been accustomed to the periodic elevation of U.S. prosecutor expectations with regards to compliance programs. The current pause in FCPA enforcement might temporarily quiet the drumbeat of government expectation, but this is not the time to slow down.

The case for continuous improvement does not rest solely on government enforcement. It is reinforced by an expanding set of risks, and the expectations of a broader group of stakeholders each with their own unique evidentiary and assurance requirements.

But, in the peace of the stilled drums, we do have an opportunity. A moment to reflect on what's working, what's not, and where we can experiment, simplify, and improve. This article has argued for a more intentional and sustainable approach to program effectiveness, by explicitly considering and documenting the standards and evidence by which compliance programs should be assessed. We should proactively ask ourselves:

- ⌞ What elements of our compliance programs truly drive ethical behavior and effectively mitigate risk?
- ⌞ Are our measurement and assurance processes rigorous enough to withstand scrutiny, not just from government agencies but from other stakeholders?
- ⌞ How can we harness technologies such as advanced analytics and artificial intelligence, not merely as supplemental tools, but as integral components in our compliance assessment framework?

Doing this well requires partnership—with Legal, Finance, IT, HR and other functions. This call to action also extends to outside counsel, auditors, technology and other service providers that support ethics & compliance teams. Providers must question if their products and services genuinely facilitate the full effectiveness assessment of their clients' compliance programs:

Technology Providers

- ⌞ Does your product provide end-to-end coverage of the relevant compliance process you support? For example:
 - if you operate a due diligence platform, do you focus purely on the due diligence process or can you support the delivery of training to third parties, and the tracking and reporting of other remediation?
 - If you operate an investigation case management platform, is it sufficiently flexible to manage human rights grievances as well as allegations relating to a client's code of conduct? Can clients align the classification of allegations in your platform to their own internal taxonomy? How robust is your root cause analysis and remediation tracking?
 - If you are an eLearning provider, can your LMS support the delivery of third-party training products, the tracking of in-person training and non-system-generated communications?
- ⌞ Can your platform serve as the system of record for evidence of program assurance? Can evidence relating to the design and empowerment of the relevant process you administer be maintained in your platform? Can you provide metrics relating to the administration of the process in your platform?



- ⌞ How can artificial intelligence unlock greater value from the information your platform contains?
How can you support ethics & compliance teams wanting to conduct “cross-over” data analytics, combining data from multiple internal sources and third-party platforms?

Outside Counsel, Auditors & Consultants:

- ⌞ Are you being clear as to the standards by which you are assessing a compliance program?
- ⌞ If you currently apply an exception-based approach, can it be expanded to include a narrative against all standards, including those that are working?
- ⌞ Can you identify the opportunities and challenges arising from intersections between different areas of compliance?
- ⌞ Do you have the requisite experience to assess compliance systems, business processes and systems, analytics models and metadata architecture?
- ⌞ Is your work product in a format that clients can update themselves going forward?

A compliance program does more than reduce risk. It builds trust with employees, communities, investors, and other stakeholders. It gives companies the confidence to operate with integrity in an increasingly complex world. But that trust and confidence must be earned and sustained through evidence. Testing the effectiveness of your compliance program is critical to both and serves as a catalyst for continuous improvement. Now is the time to test whether your compliance programs are truly working.