Gartner

Improve Compliance Risk Monitoring Using Data & Analytics

As focus on compliance risk oversight and data-driven risk monitoring expands, chief compliance and ethics officers (CCEOs) are facing increasing pressure to better utilize available enterprise data sources for compliance risk monitoring. In fact, 87% of CCEOs report experiencing greater pressure from regulators. [1] To address this, CCEOs have been leveraging readily available data, like training completion rates and helpline call volumes, to drive risk response strategies and continuous monitoring efforts. However, this data can be one-dimensional and provide limited insight.

CCEOs are also often constrained by a lack of investment in tools and resources to create necessary data infrastructure to monitor their programs. Such investments ultimately enable the CCEO to build defensible oversight of their compliance program and more effectively allocate scarce resources to mitigate high risks as continuous monitoring enables real-time response.

To create a more informed risk monitoring strategy, CCEOs must prioritize data-driven decision making that allocates resources to high-risk areas more efficiently and demonstrates oversight of compliance programs.

Analysis

Understand and evaluate enterprise data sources

Prior to selecting KRIs and KPIs to monitor their compliance risks, CCEOs should document the data sources required for monitoring compliance risk. This can include both data sources they own directly (e.g., hotline, training completion) or data from other sources (e.g., travel and expense [T&E] data, payment transactions). When building a roadmap for a compliance risk monitoring program, understanding what data is readily available allows CCEOs to obtain quick wins.

Preparing a map of data can also help facilitate a strategic roadmap for compliance risk monitoring. Documenting quick wins with easily accessible data can demonstrate oversight, while the CCEO partners with the chief data and analytics officer (CDAO) and other leaders to access new resources.

While the volume of data in organizations may be overwhelming, it is crucial to start with what is available. This helps avoid selecting a risk monitoring project that is not feasible because the data does not exist.

Table 1: Data sources

Type of data	Definition	Examples
Structured	Data that has a standard, tabular format making it efficient for humans and machines to process (e.g., .csv or .xlsx files that are extracted from an enterprise or compliance management system)	Hotline data, payment transaction data, T&E data
Semistructured	Data that does not follow a fixed schema but contains some elements that make it easier to analyze such as metadata tags	Legal matters such as employment litigation, training logs in SharePoint
Unstructured	Data that does not have any predefined format	Observations, focus groups, culture surveys, videos

Source: Gartner

CCEOs should keep in mind that using a single data source to track a compliance risk may not yield the best results. Reviewing multiple data sources can provide better insight into the effectiveness of key compliance risks, frameworks and controls.

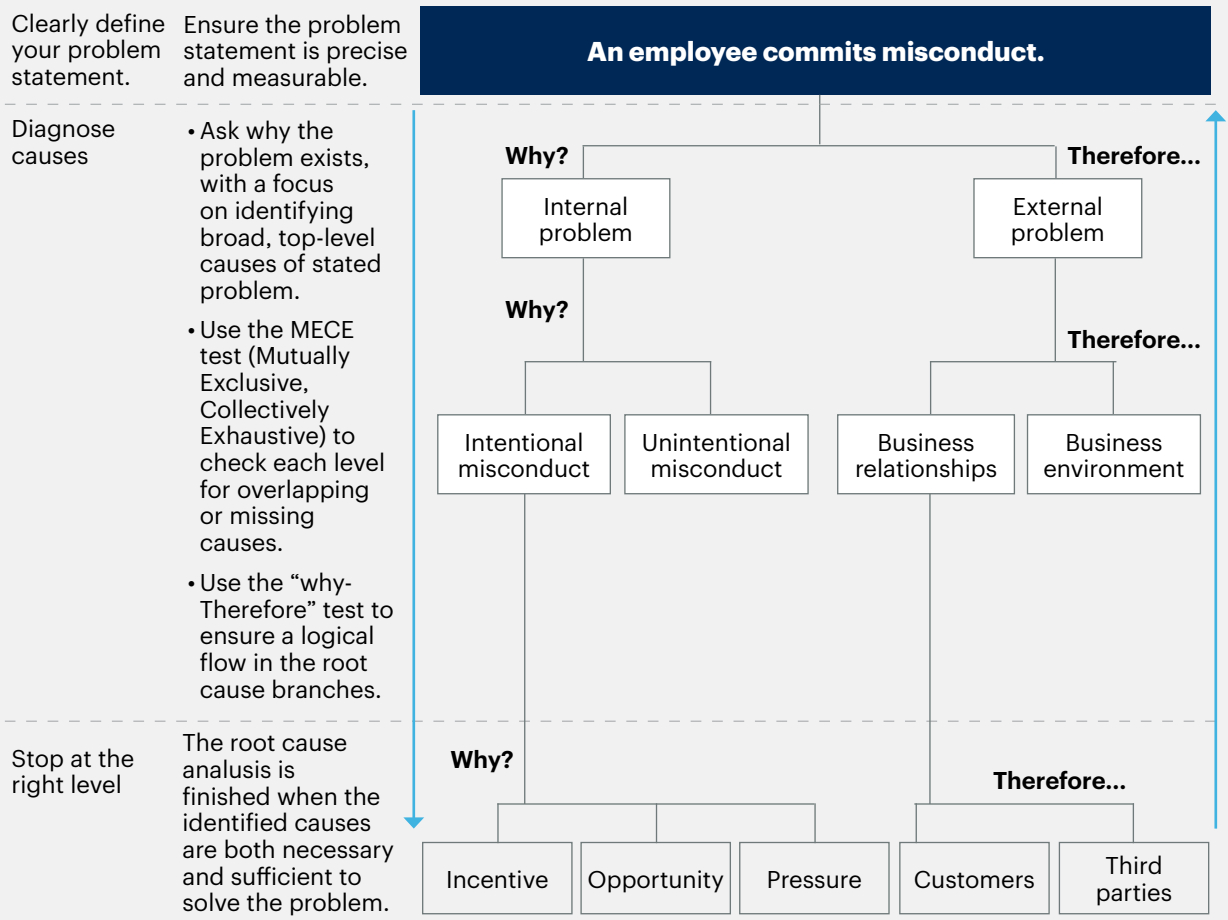
Select the right KRIs through root cause analysis

CCEOs rely on KRIs to assess program performance; however, this on its own is not a sufficient measure of effectiveness. [1] The best KRIs are leading indicators whose movement definitively and independently signals increasing or decreasing risk exposure; however, only 13% of compliance functions establish KRIs that way.[2]

An example of a KRI is the number of hotline complaints in a particular location. This KRI doesn't say anything definitively except whether a concern was raised or not. A better KRI is the number of anonymous complaints — typically when those are high it definitively signals concerns about retaliation.

To build an effective monitoring program, CCEOs should select KRIs using a root cause tree (see Figure 1). The root cause tree allows CCEOs to break down compliance risks into measurable KRIs to facilitate ongoing monitoring and trend analysis.

Figure 1: Sample root cause tree



Source: Gartner

Using the example KRI of hotline complaints: If there are a lot of complaints or if there are zero complaints, both can signal an issue. Using root causing, one reason for zero complaints could be retaliation. A better way to measure the KRI would be to tie the hotline complaint to HR complaints and employment litigation for that particular location to visualize the health of speak-up culture and related compliance issues.

However, if employment litigation data is unavailable to the CCEO, using HR data such as open-door complaints would still give a better picture than just relying on HR complaints alone. Therefore, having knowledge of available data sources can help drive better decision making at the root cause level.

Gartner

Enhance program effectiveness by evaluating and expanding existing KRIs

While KRIs can signal a change in risk, KPIs indicate how effectively an organization is achieving its compliance and risk management goals. The term KPI is often used for metrics to determine employee or business performance against goals. KPIs include a set of targets, objectives or benchmark data from peers. Both KRIs and KPIs consist of metrics, but a KRI's performance against stakeholder objectives cannot be measured without a KPI (see Figure 2).

CCEOs can extract the most out of periodic or continuous monitoring by leveraging KPIs as a measurement of success. Our research finds that quality standards is one KPI that exceeds others in assisting compliance with risk monitoring from the perspective of employees.[1]

> Quality standards are documented principles, specifications, guidelines or characteristics used consistently to guide the design, development, execution, monitoring and improvement of compliance activities to promote compliant behavior and reduce compliance risk.

Consider the example of how compliance teams currently measure training completion rates. They often set a high bar for a 100% completion rate. This can be used only to demonstrate whether training was completed but gives no insight into its effectiveness. Instead, in addition to completion rates, compliance should measure performance of its training against a set of quality standards.

Case in point: Design-based training impact tests (AbbVie)

One company that provides reliable and proactive mechanisms for evaluating compliance programs is AbbVie, where the CCEO continually evaluates how well their compliance training performs. AbbVie's leaders start by articulating hypotheses on the desired impact of training design changes on employee behaviors. Next, they align these hypotheses to training assessments. AbbVie's set of hypotheses inform a set of standards that direct the design and evaluation of their training across the following categories: governance, content, audience and modality. This process can be adapted for assessing different types of compliance risk mitigation activities.

In 2023, AbbVie applied this methodology to Conflicts of Interest (CoI) booster training that was tailored to address personal relationships of healthcare professionals with healthcare providers. AbbVie analyzed responses to postsurvey questions that surveyed on training design choice. AbbVie also reviewed the volume and types of CoI inquiries raised by the target group. As a result, AbbVie observed an upward trend in terms of employee understanding of the training.

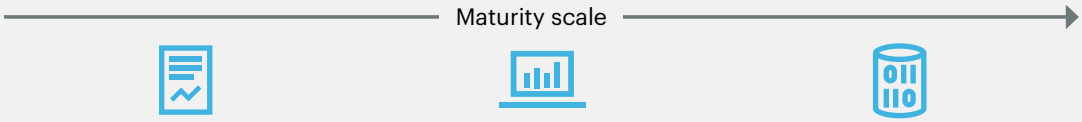
Mature risk monitoring through data and analytics

CCEOs must devise a solution that meets their long-term objectives for compliance monitoring and resist reactive approaches to responding to risk. We have observed three data and analytics maturity levels (see Figure 2):

1. Nascent
2. Emerging
3. Mature

Data and analytics maturity levels are additive, not linear. We have observed that clients continue to mature their programs at every level.

Figure 2: Compliance risk monitoring maturity



	Nascent	Emerging	Mature
How	Join terms in Excel	Ingest structured data into GRC or business intelligence tool for reporting	Automated reporting using a business intelligence tool fed from a data lake; use of AI/ML and algorithms
Pro	All skill levels can access and manipulate data	Provides some level of automation	Real-time reporting can drive actionable risk response
Con	Lost time from manual effort	Limited data governance	Resource-intensive to build
Typical use case	Simple KRIs using one or two sources of data	Analyzing control effectiveness	Holistic ongoing monitoring of both risks and controls

Source: Gartner

Nascent

Most CCEOs get started with available data by using a spreadsheet-based, low-tech approach to organize and describe information. Maturity at this level includes manual data collection and preparation.

The process can be time-consuming and difficult to scale long term. However, having access to the insights outweighs the cost of time investment when getting started. This process is most effective for:

- Logging observations from a single data source. For example, the number of hotline complaints.
- Tying together two or more fragmented data sources that are joined on a common data element. For example, a CCEO may tie together training data from the learning management system (LMS) with sign-ins for live training. The data element this would be "joined" on could be the employee's name or role to provide a report related to role-based training completions.

Emerging

CCEOs who exhibit emerging maturity are partially automating data and analytics, and reporting to diagnose compliance risks. These solutions can reduce the amount of time spent analyzing data and determine the "why" of compliance risks. Markers of maturity include:

- A governance, risk and compliance (GRC) tool that can serve as an intermediary step for a data lake. These tools can, via an API, ingest data (either manually or using some automation) into the platform and provide a view of some compliance risks. These solutions are, however, limited to the types of compliance risks managed within the tool.
- Business intelligence tools that can be used to ingest multiple sources of information manually, or by leveraging some limited automation via an API. These solutions can ingest structured or semistructured data from sources both within and external to the organization.
- Progressive users of GRC and business intelligence technology could consider alignment across their assurance teams in compliance, risk and audit. The teams can jointly create a series of dashboards that provide consistent taxonomy and information within an aligned assurance model that provides more holistic insight into risk.

Mature

An observation of a mature program includes predictive and prescriptive analytics. Markers of maturity include:

- Continuous monitoring dashboards that pull data from enterprise systems on a near-real-time basis. These dashboards are often built on top of a data lake, or a centralized repository designed to store, process and secure large amounts of structured, semistructured and unstructured data. The data lake in a mature organization would likely be fed by compliance-owned tools such as GRC and data from enterprise systems.
- Predictive analytics involves technologies like machine learning, algorithms and AI. AI enhances data analysis by quickly analyzing and extracting insights from large datasets to identify trends, patterns and correlations that can detect and predict changes in risk.

Intel's corruption risk assessment system leverages data-driven insights and algorithms to strategically allocate resources to reduce anti-corruption risks and inform compliance audits.

Step 1: Intel scoped and built a "how and why" business case to help stakeholders understand the larger context of a proposed corruption risk intelligence system (CRIS).

Steps 2 and 3: Compliance staff identified the right data to be leveraged for CRIS and assigned risk weights to data sources. Intel determined an algorithm and threshold of high-risk deals for staff to audit and investigate with an ability to review the algorithm's accuracy when necessary.

CRIS helps Intel strategically allocate resources for audits and investigations of high-risk business deals. It also enhances the efficiency of risk assessment by leveraging algorithms to automate the identification of high-risk business transactions. Intel pulls data from CRIS to conduct ongoing proactive monitoring. This enables Intel to identify risks and take remedial actions on a near-real-time basis.

With sufficient use data compiled, CRIS creates an opportunity for compliance predictive analysis.

Evidence

[1] Gartner 2023 Compliance Effectiveness Client Survey
[2] Gartner 2024 Compliance Score

Disclaimer: The organization (or organizations) profiled in this research is (or are) provided for illustrative purposes only, and does (or do) not constitute an exhaustive list of examples in this field nor an endorsement by Gartner of the organization or its offerings.

Actionable, objective insight

Position your organization for success. Explore these additional complimentary resources and tools:

Webinar

Join a Virtual Event

Hear from Gartner legal, risk and compliance experts at an upcoming or recorded event.

Register Now

Research

Define the Leadership Vision for Your Role

Achieve personal and enterprise success with actionable insight.

Learn More

Research

Strategic Planning for Your Function

Turn your strategy into action with these tools and templates.

Download Now

How We Help

Gartner for Compliance

Discover how we can help you tackle your most-critical priorities.

Learn More

Already a client?
Get access to even more resources in your client portal. Log In

Connect With Us

Get actionable, objective insight that drives smarter decisions and stronger performance on your mission-critical priorities. Contact us to become a client:

U.S.: 1 855 811 7593

International: +44 (0) 3330 607 044

Become a Client

Learn more about Gartner for Legal, Risk & Compliance
gartner.com/en/legal-compliance/products/gartner-for-legal

Stay connected to the latest insight

Attend a Gartner conference
View Conference

Gartner®