COSMOS
Navigate the Compliance Universe

CEP Magazine - March 2024

Renu Jha (renu.jha@ethic-ally.com, linkedin.com/in/renujha) is the Founder of Ethic-Ally Compliance and Audit Solutions in Delhi, India. She is also a Partner with the France-based international risk advisory firm Governances.

Determining what and when to audit

by Renu Jha, CA, CFAP

In the ever-evolving landscape of business and regulations, compliance auditing and monitoring are critical to ensure that companies operate within the confines of laws, regulations, and ethical standards.

As businesses navigate the complex environment of legal and ethical obligations, the strategic execution of audits at regular intervals becomes imperative to identify, rectify, and prevent potential compliance risks.

Compliance auditing and monitoring play a pivotal role in evaluating the effectiveness of a company's compliance program. When regulators assess these programs, they focus on three key criteria:

1. Is the company's compliance program well-designed?
2. Is it being applied in good faith (i.e., how well is it implemented)?
3. Even if it is well-designed and implemented, does it work? Is it effective, and what is the impact? [1]

To determine what and when to audit, we must first understand the objectives of compliance auditing and monitoring. For this, let's explore the three primary purposes of these activities that align with the seven elements of an effective compliance program as defined by the U.S. Sentencing Guidelines.

I. Prevention

Element 1: Written policies, procedures, and standards of conduct

An effective compliance program begins with well-documented policies, procedures, and standards of conduct, which set the foundation for ethical behavior and compliance with relevant laws and regulations.

Element 2: Designate a compliance officer and governance committee

The compliance officer and committee are responsible for overseeing and implementing the compliance program within the organization in alignment with the organization's values and goals.

Element 3: Provide regular and effective education

Regular training and communication are essential to ensure that employees understand compliance standards, guidelines, and processes, helping them grasp the dos and don'ts of the organization's operations.

II. Detection

Element 4: Reporting and investigation

This element focuses on creating a culture where employees feel comfortable reporting potential violations. Investigative procedures should be in place to examine reported issues thoroughly, ensuring non-retaliation and preventing adverse actions against those who report in good faith.

Element 5: Conduct internal auditing and monitoring

These proactive measures help identify compliance risks and weaknesses in the system. Regular assessments enable early detection and correction, contributing to the program's overall effectiveness.

III. Remediation

Element 6: Enforcement and discipline

When violations occur, a clear, fair, and transparent system of enforcement and discipline is crucial. It ensures breaches are addressed promptly and consistently, building trust with employees and business partners.

Element 7: Response and prevention

This element focuses on strategies for responding to violations and implementing preventive measures to avoid future breaches.

Auditing and monitoring processes can work together to help an organization understand its risk landscape and allocate resources accordingly. Trends observed at the organizational, regional, or country level can point to an area where a company may want to dig deeper through a process audit. The following are some examples:

- **Distributor margins**: Trend analysis done as part of monitoring distributor margins may show a sudden increase in a country or reveal wide variations between margins paid to similar distributors used by different business units in the same country. This may indicate that the higher margins distributors are being allowed to charge are helping to create a slush fund to be used for bribes. Auditors may want to dig deeper in the form of a special audit for distributor margins.
- **Channel stuffing**: If there is a spike in month-end sales to distributors, followed by a high number of products being returned at the beginning of the next month, this may indicate a deceptive business practice used by the company to inflate its sales and earnings figures. Observing such a trend may necessitate an audit of the sales incentives and bonus schemes to check how sales variables are tied to incentives and find the right balance to check these deceptive practices.
- **Gifts and hospitality**: Likewise, an audit may reveal process gaps around gifts and hospitality expenses and result in audit recommendations to regularly monitor such expenses.

While planning *what to audit*, it's essential to evaluate the *audit universe*—which means all the different kinds of reviews/audits for various areas, processes, and activities within an organization. We're talking about any kind of review that may be done by different functions in relation to compliance controls, as well as complementary internal controls.

Regardless of who does the auditing and/or monitoring work—internal audit, compliance, or an external consultant—involvement of the compliance function is essential while deciding *what and when to audit*.

If the compliance function is not developing the compliance auditing and monitoring plan, it would be good to ask that the plan include how priority risks are evaluated and ongoing monitoring occurs. It is also important to focus on how compliance will be integrated into another function's process of forming and implementing the compliance auditing and monitoring plan.

Questions to ask

Organizations should ask questions like, "What other internal and external reviews have been done for common auditable areas?" For example, peer reviews may be done by the compliance team—a compliance officer of one country reviews the compliance program of another country and vice versa. Similarly, internal controls may be reviewing marketing expenses and payment processes, and compliance may also look at these expenses from an anti-bribery perspective.

"When and with what frequency are these reviews conducted?" If different groups are reviewing the same auditees for a common area under review, and if these reviews are done too close together, it may result in duplication of efforts and annoyance to auditees since they must provide almost the same set of documents for reviews held one after another.

Other questions include, "What areas did the other reviews cover?" and "What were the outcomes of these reviews?"

Based on the quality of other reviews done and how much reliance the auditor thinks they can place on the outcomes of such reviews, the auditor may choose to either expand or reduce the extent of their audit into that particular area.

The auditor may also check whether other reviews identified any compliance issues. If so, what remedial measures were put in place to address them? For example:

- Performing compliance due diligence is a compliance control and is key before making third-party payments. There are also internal controls around payment processing, like purchase orders, invoices, approval matrices, etc.
- Monetary thresholds for gifts and hospitality are compliance controls, and there are also controls related to procurement, marketing expenses, budget approvals, etc.

We will now discuss the key critical aspects of an ethics and compliance program that audits should focus on.

Audit of compliance program design

It is vital to audit whether essential compliance policies have been designed to adequately address the compliance and integrity risks of the organization.

Culture and tone at the top

The foundation of a strong compliance program starts with the organization's culture and the tone set by its leadership.

- Does the organization promote a culture of integrity and compliance? Is there a commitment to doing the right thing at all levels?
- What is the tone at the top? Does leadership—including senior management and the board—demonstrate a clear commitment to compliance and ethical behavior?

- What is the quality of the leadership team and talent and performance management systems? Does the organization promote compliance principles, ethics, fairness, and transparency?
- Is there effective talent management to ensure the organization hires, trains, and retains employees who align with the compliance culture?
- Are performance goals set and assessed to include compliance and ethical considerations?
- Does the organization identify, monitor, and mitigate behaviors that could lead to compliance breaches?
- Are compensation, rewards, and incentives structured to ensure they do not encourage unethical or noncompliant behavior?

By auditing culture, leadership, talent, behavior risks, and compensation, organizations can strengthen their compliance programs, foster ethical behavior, and minimize compliance risks.

Reviewing management communications

Are messages from middle and senior management consistent with the organization's commitment to compliance, ethics, and regulatory adherence while also being tied to the organization's mission and key business objectives?

Corporate governance structure

Auditing the corporate governance structure means that you must assess what kind of governing bodies are in place to oversee compliance-related matters, how disciplinary actions are decided and enforced, and how behaviors are rewarded or discouraged.

Organizational structure, authority, independence, and staffing

Evaluate whether the compliance function has the right placement within the organization. Does it possess the authority, independence, and sufficient resources to actually operate effectively and autonomously? Does compliance have an independent budget? What is the reporting structure of the compliance function in relation to business/country leaders?

Effective training and communication

Ensure employees receive the necessary education to understand and adhere to compliance standards. Is training being done, what is the quality of training delivered, and what is the credibility and competence of the trainer?

Review compliance communications to assess the clarity and accessibility of information being communicated regarding compliance policies and procedures.

- Does the company have a *code of conduct* that sets out the ethical standards for an organization, and is it communicated effectively to all employees?
- Have clear *anti-bribery* and *anti-corruption* policies been established? Has adequate training been developed in them, and are employees being provided regular training?
- Check what mechanisms have been designed to ensure adherence to anti-trust regulations.
- Have robust *third-party risk management practices* been established? Are third parties—including suppliers,

distributors, service providers, and business partners—put through due diligence and ongoing monitoring? Is there adherence to third-party compliance policies and processes?

Policies and processes

Similarly, it is necessary to have effective policies and auditing processes around:

- Sanctions, anti-boycott regulations, and export controls
- Anti-money laundering and countering terrorist financing
- Modern slavery and human rights
- Data privacy and data protection
- Fraud prevention and detection
- Travel and entertainment
- Contract management
- Employee selection and verification
- Occupational health and safety
- Employee selection and background verification

Internal reporting

An ethics helpline or internal alerting mechanism is a lifeline for employees to report concerns or allegations of misconduct. The audit should check the functionality and accessibility of the helpline.

- Is it easily accessible to all employees, including those in remote locations?
- Does the helpline offer options for anonymity and guarantee confidentiality to encourage open reporting?

Handling misconduct

Audit the efficiency of the investigative process for handling misconduct allegations.

- Are investigations conducted promptly and thoroughly?
- Does the investigative team have the necessary expertise, and are they independent from the alleged misconduct?

Disciplinary actions

Audit the consistency of disciplinary actions taken and remedial measures put in place.

- Are penalties commensurate with the severity of the misconduct?
- What remedial actions have been put in place to prevent similar misconduct?

Remedial measures

Evaluate the effectiveness of remedial measures put in place to prevent future misconduct and prevent any retaliation against whistleblowers.

- Does the organization provide ways for employees to get unbiased, confidential advice about exercising whistleblower rights?
- Check for any action taken that can be viewed as punishment for unrelated reasons (e.g., retaliatory changes in employee's location, duties, reporting structures, assignments handled, resignation, nondisclosure agreements signed) soon after a reported incident.

Sales and procurement

Sales and procurement processes are crucial to an organization's compliance efforts.

- Are these processes well-documented and aligned with compliance standards?
- What controls are in place for both sales and procurement activities?

Prevention

Are there measures to prevent unethical behavior?

- Are accurate books and records maintained? Do record-keeping practices meet regulatory requirements?
- Have systems and controls been audited to ensure data accuracy? Do the controls prevent errors or misrepresentations?

Integration

Audit the integration of complementary internal controls with compliance controls to ensure seamless operation.

- What is the testing methodology for validating compliance controls, and how are these different from the testing done for complementary internal controls?
- Where audit results show failed controls in internal control testing, are these results taken into consideration while testing the compliance controls for that same area?

Audit of the implementation of the compliance program

A detailed and focused review should be done on the actual implementation of the company's compliance and ethics policies, procedures, processes, and practices.

The auditing methodology primarily involves data collection and tracking because this provides trend analysis and serves as a good measure of progress.

The compliance officer or auditor may consider the following techniques:

1. Perform on-site visits and spot checks on certain high-risk areas.
2. Conduct interviews of personnel in management, operations, contracting, marketing, finance, and other related activities, which provides a good indication of risk areas and the organization's culture.

3. Develop questionnaires or surveys to solicit impressions from a broad cross-section of the organization's employees (for example, a culture survey).
4. Review written materials and documentation prepared by different divisions within the organization.
5. Conduct trend analyses in specific areas over a given period and review the internal and external complaints filed, internal audits, observations, and findings. Trends and analyses of whistleblower hotline calls are good ways to check program implementation.
6. Review the regulatory activity in the company's industry and/or geographic market.
7. Include compliance-related questions in exit interviews (responses to these questions should be reported to the compliance officer), such as:
    a. How do you feel about communications in your unit?
    b. How about communications overall?
    c. How do you think the organization lives up to its code of conduct?
    d. Did you have any concerns about ethical issues or compliance-related practices? If so, please explain.
8. Audit the board's oversight of compliance to ensure a clear structure to support governance responsibilities.
9. Review management roles and responsibilities to ensure accountability for compliance implementation.
10. Audit the organization's tone at the top and culture to gauge how much it fosters compliance and ethical conduct.
11. Scrutinize charitable contributions, donations, and sponsorships to prevent any misuse of funds.
12. Audit the handling of gifts, hospitality, entertainment, travel, and expenses and how they align with policies and procedures.
13. Audit the incident reporting and investigation processes to ensure that incidents of noncompliance are thoroughly examined.
14. Review the due diligence procedures for third-party selection to minimize compliance risks. Audit contracts and payments to third parties to ensure they align with compliance standards.
15. Assess the effectiveness of internal controls to identify and mitigate risks.
16. Audit the record-keeping practices to ensure they meet regulatory standards.
17. Evaluate the effectiveness of ethics and compliance training programs.
18. Audit the response mechanisms and measures in place to address misconduct and prevent its recurrence.

By thoroughly reviewing all these areas, you can assess whether the culture of ethics and compliance has percolated throughout the organization and is not just an on-paper compliance program.

Timing and frequency of audits

The timing and frequency of ethics and compliance audits are not a one-size-fits-all schedule. They should align with the company's unique needs, industry standards, and risk factors.

It's best for each company to determine its audit timing and frequency based on specific circumstances because no one knows the organization better than its leaders. Some processes may require more frequent auditing due to higher inherent risks. This is where a risk-based approach comes into play.

1. Conduct a comprehensive review of the ethics and compliance program annually to allow for a thorough evaluation.
2. Depending on the identified risks, certain processes may be audited regularly—quarterly, biannually, or annually—to ensure ongoing compliance.
3. Special or ad hoc audits may be conducted as required. These audits are usually triggered by specific events, upon management request, or by emerging risks that need immediate attention.

Key criteria for timing

Timing should align with the company's objectives, industry standards, and risk landscape and reflect the company's dynamic environment and priorities.

1. One significant criterion is the complexity of the processes involved. Complex processes may require more frequent audits to ensure adherence to compliance standards.
2. Process maturity also matters. Well-established processes may need less frequent auditing than newly implemented or evolving ones.
3. Changes in business conditions—such as mergers and acquisitions, the introduction of new business models, or expansion into new locations— can trigger the need for audits to ensure compliance in the evolving landscape.
4. Consider the findings and recommendations from previous audits, reviews, or investigations. If issues were identified, follow-up audits may be necessary.
5. Budgets play a role in determining audit timing. Companies must allocate resources to conduct audits effectively.
6. Compliance with regulatory and customer requirements often dictates audit timing. Failure to comply can result in penalties or loss of business.

Conclusion

For effectively planning what and when to audit, assessing the organization's risks and control environment is crucial.

Compliance audits focus on the design and real-life application of ethics and compliance policies, procedures, and processes. The timing and frequency of such audits should align with specific organizational requirements.

Audits go beyond paperwork to confirm real-world implementation and add value by supporting the organization in continually improving.

Takeaways

- Before conducting audits, it's essential to thoroughly assess the organization's objectives and the associated risks and overall control environment.
- Auditors must have a clear understanding of the audit universe, which covers the various processes, departments, and functions that fall under the scope of compliance audits.
- Compliance audits should focus on evaluating the design of policies, procedures, processes, training programs, and communication strategies.
- Beyond design, audits should also assess the actual implementation of compliance policies, procedures, and processes.
- The frequency and timing of audits should be determined based on specific criteria tailored to the organization's needs.

1 U.S. Department of Justice, Criminal Division, *Evaluation of Corporate Compliance Programs*, updated March 2023, https://www.justice.gov/criminal-fraud/page/file/937501/download.