THOMSON REUTERS
PRACTICAL LAW™

Acting as an Independent Compliance Monitor for a Financial Institution

by John F. Curran, Daniel J. Chirlin, and Rachel Brook, Walden Macht & Haran LLP, with Practical Law Securities Litigation & White Collar Crime

Status: **Maintained** | Jurisdiction: **United States**

This document is published by Practical Law and can be found at: **us.practicallaw.tr.com/w-024-8664**
Request a free trial and demonstration at: **us.practicallaw.tr.com/about/freetrial**

A Practice Note examining the key issues and best practices for an attorney acting as a compliance monitor for a financial institution. This Note explains the monitor's responsibilities, how to assemble and manage the monitor team, the contents of the monitor's reports, and how the monitor team conducts the monitorship so that the team can recommend enhancements to the compliance program and other remedial actions.

The government or a regulator may impose a compliance monitor as part of resolving a civil, criminal, or regulatory matter (including after a regulatory examination) where the financial institution had an inadequate compliance program that failed to identify or prevent misconduct. Many types of financial institutions have agreed to accept a compliance monitor, including retail and commercial banks, broker-dealers, insurance companies, investment advisers, asset managers, and mortgage lenders and servicers. The matter may be resolved through a non-prosecution agreement (NPA), deferred prosecution agreement (DPA), plea agreement, consent order or decree, or other settlement with the government or regulator (governing agreement).

The government or regulator proposes terms for the financial institution to accept that are intended to strengthen the institution's compliance processes and procedures and reduce the risk that the same or similar misconduct recurs (see Terms of the Monitorship). The compliance monitor's role is to assess the institution's satisfaction of the terms of the governing agreement between the institution and the government or regulator. The monitor must ensure that the institution develops an environment committed to systemic and sustainable change.

The compliance monitor is often an attorney but may be an accountant or other type of professional. This Practice Note focuses on an attorney acting as the compliance monitor. However, the contents may also apply to other types of professionals acting as a compliance monitor.

Unless there is a reason to differentiate, any references to the government include the Department of Justice (DOJ) and state and federal regulatory agencies, such as the Securities and Exchange Commission (SEC) or the New York Department of Financial Services (NY DFS).

Monitorship Types

The two types of monitorship are:

- **Enforcement monitorships.** An enforcement monitor is an impartial party appointed by the court or government to oversee and enforce the terms of the governing agreement. Enforcement monitorships are typically shorter in duration than compliance monitorships. Enforcement monitorships have a limited scope and tend to focus narrowly on remedying specific violations. The governing agreement usually contains detailed requirements and specific parameters for remediation. The monitor evaluates the financial institution's remediation on a pass or fail basis.
- **Compliance monitorships.** A compliance monitor (also called an independent examiner or independent compliance consultant) is an impartial party appointed by the government to detect the root causes of the financial institution's compliance failures. The monitor must also identify the possible enhancements to the institution's compliance program and recommend the ones that are best suited to prevent future misconduct. The purpose of the monitorship is not to punish the institution but to monitor, make recommendations, and drive the company

towards improving its compliance program. A compliance monitor's focus is not on addressing a particular compliance failure. A compliance monitor instead takes a holistic approach to ensure that the institution's compliance culture improves so that the institution sustains change after the monitorship term ends.

This Practice Note only covers compliance monitorships. However, some of the same principles apply to enforcement monitorships.

Monitorship Terms

The government and the financial institution negotiate the terms and conditions based on the particular facts, including the nature of the misconduct and the identified compliance program failures. After reaching an agreement, the government memorializes the terms between the institution and the government in the governing agreement.

The governing agreement usually includes:

- A description of:
  - the misconduct and compliance failings of the institution justifying the appointment of a monitor;
  - the monitor's required qualifications;
  - the monitor selection process, including the timing for completion (see Selecting the Monitor); and
  - the process for replacing the monitor during the monitorship term, for example, if the monitor cannot continue or if the government finds the monitor's work unsatisfactory.
- An explanation of the monitor's responsibilities and the scope of the monitorship (see Scope).
- The length of the monitorship (see Duration).

(See Memorandum on Selection of Monitors in Criminal Division Matters (Oct. 11, 2018) (Benczkowski Memo).)

A monitor should supplement the governing agreement by entering into an engagement agreement with the financial institution that covers additional terms and conditions for the monitorship that are not in the governing agreement (see Engagement Letter).

Scope

The governing agreement sets out the scope of the monitorship by broadly describing the monitor's responsibilities and objectives and identifying the relevant laws, regulations, and geographic locations involved. The scope generally focuses only on the type of misconduct the government found during its investigation. (Memorandum on Selection and Use of Monitors in Deferred Prosecution Agreements and Non-Prosecution Agreements with Corporations, at 5 (Mar. 7, 2008) (Morford Memo).)

The governing agreement may not provide a detailed description of the scope. Before beginning, the monitor should discuss with the parties their expectations on the scope to avoid any ambiguity or misunderstanding, which could lead to hostility toward the monitor (see Kickoff Meeting).

A monitor should only act to accomplish the objectives in the governing agreement and engagement letter. A monitor should not attempt to expand the scope beyond the governing agreement unless there is a factual basis, and the government agrees.

Selecting the Monitor

The governing agreement generally sets out the terms for selecting the monitor. Although each government agency or regulator may handle the process for selecting a monitor differently, they all typically:

- Allow the financial institution to suggest potential candidates and participate in the selection process.
- Require monitor candidates to:
  - respond to their questionnaires and questionnaires from the financial institution;
  - interview with them and the financial institution; and
  - submit a staffing plan.

(See Benczkowski Memo, at 5.)

The government typically looks to select a monitor who has:

- Previous monitorship experience, preferably as a monitor for a financial institution.
- Experience and expertise with the subject matter at issue.
- Adequate and sufficient resources available to conduct the monitorship.
- No potential conflicts, including recent work for the financial institution.

Duration

The governing agreement sets out the monitorship term, which typically runs from one to five years. The

monitorship term is often the same as the term of the governing agreement. To determine what monitorship term to impose, the government considers:

- The nature and seriousness of the underlying misconduct.
- The pervasiveness and duration of the misconduct, including whether senior management was complicit.
- The financial institution's history of similar misconduct.
- The financial institution's culture of compliance.
- The scale and complexity of any required remedial measures, including the size of the financial institution or business unit to monitor.
- The stage of the financial institution's design and implementation of remedial measures when the monitorship begins.

(Morford Memo, at 7-8.)

The governing agreement generally provides that the government may extend the monitorship term in its sole discretion. For example, the governing agreement may state that if the institution is slow to provide information or make resources available to the monitor, the monitorship term is tolled until the institution resolves those issues.

Although possible, the government rarely terminates the monitorship early. A monitor should not expect to conclude the monitorship before the end of the term, even with extraordinary progress and success.

Engagement Letter

The monitor and the financial institution enter into a written engagement letter, which establishes and governs the contractual relationship between the monitor and the institution. Either party may draft the letter, and the government must approve its terms. The terms must be consistent with the parameters set by the governing agreement. The letter must also detail the institution's obligations to cooperate with the monitor and the consequences of any failure.

The engagement letter typically includes:

- Plain statements that:
  - the parties are subject to the terms of the governing agreement, including its scope;
  - the monitor is independent; and
  - the financial institution and the monitor are not entering into an attorney-client relationship (see Attorney-Client Privilege Inapplicable).
- The monitor's guidelines for:
  - onboarding the monitor team (see Onboard the Team);
  - requesting information from the financial institution (see Liaise with the Financial Institution);
  - handling confidential information (see Confidential Information); and
  - providing reports to the financial institution and the government (see Drafting Reports).
- The monitor's billing and payment protocols, including a statement that the financial institution's payment of the monitor's fees is not contingent on the outcome or final resolution of the engagement (see Billing).
- The specific tasks the financial institution must perform to facilitate the monitor's duties (see Handling the Monitorship and Conducting the Monitorship: Logistics).

The monitorship term begins to run from the date both parties sign the engagement letter.

Billing

At the outset, the monitor should agree on billing and expense guidelines and protocols with the financial institution. A monitor's billing practices typically include:

- Sending the invoices and supporting information for the work performed directly to the institution or its counsel. Unless requested, the monitor does not provide the invoices to the government.
- Uniform billing descriptions to avoid different descriptions for the same work.
- Excluding any confidential supervisory information (CSI) or other confidential information from the billing entries (see Confidential Supervisory Information).

Attorney-Client Privilege Inapplicable

The monitor's engagement does not form an attorney-client relationship between the monitor and the financial institution. The engagement letter should expressly state that the monitor and the institution agree to not enter into an attorney-client relationship. The communications between the monitor team and the institution and the work the monitor team performs therefore are not protected by the attorney-client privilege. However, the communications between the institution and the monitor team and the work product the monitor produces may be protected as CSI where the bank's supervising regulator is the other party to the governing agreement. In that case, the monitor created the communications

and work product in furtherance of the supervising regulator's investigatory or enforcement authority (for example, 12 C.F.R. §§ 261.2 and 261.20; see Confidential Supervisory Information).

During the monitorship, the monitor requests various categories of documents. The engagement letter should set out a mechanism for handling any privileged documents responsive to the monitor's requests. The engagement letter may require that the institution provide a privilege log to the monitor for any documents withheld on privilege grounds.

For information about waiver of the attorney-client privilege, see Practice Note, Attorney-Client Privilege: Waiver (Federal).

Initial Steps

Kickoff Meeting

At the beginning of the monitorship, the monitor should organize a kickoff meeting with the financial institution and the government. The monitor should promptly identify and raise any questions about scope where the governing agreement is silent or lacks sufficient detail. Doing so may avoid the institution asserting that the monitor is exceeding the scope of the monitorship.

The monitor should detail its intended approach to achieve its objectives. This includes a high-level description of the anticipated workflow, including, for example, interviews, document review, testing software and systems, and transaction review (see Conducting the Monitorship: Logistics). The monitor should include all these items in the work plan provided after this meeting (see Draft a Work Plan).

The monitor should ask the institution to give an informational presentation:

- Providing the relevant background information.
- Explaining the business, including its organizational structure and clientele.
- Describing the current state of the institution, the changes the institution has already made, and the institution's plans to improve its compliance program, including a timeline.

The monitor should typically request that the institution take them through the institution's systems and data. The monitor should then propose the necessary level of access they need to the institution's offices, data, and systems and discuss with the institution any limitations on the monitor's access and use of confidential information. The monitor should also determine the method and process the institution will use to produce documents to the monitor.

The parties may also go over:

- The information and data that the monitor wants from the financial institution (see Gather Information and Use Data Analytics).
- How the monitor intends to handle attorney-client privilege issues that may arise in document productions or interviews (see Attorney-Client Privilege Inapplicable).
- The budget and the overall work plan, including the dates for accomplishing tasks (see Draft a Work Plan).
- The monitor's practices to preserve the confidentiality of the financial institution's information and data (see Confidential Information).
- Whether the financial institution's counsel can attend witness interviews (see Attendance by Counsel for the Financial Institution).
- The financial institution's communications about the monitorship to its employees and relevant third parties, including agents, consultants, or vendors.
- Any travel or international concerns related to overseas locations, including:
  - the local regulatory authority and process;
  - the local labor laws;
  - the local data privacy laws;
  - any health and safety concerns; or
  - the need for local counsel or other local expertise.

Select the Monitor Team

The monitor should select team members who are experienced with investigating and evaluating compliance programs and can communicate and collaborate effectively with a financial institution. The team members should have or develop knowledge about issues relevant to financial institutions, such as:

- The applicable regulatory areas.
- The general operation of a financial institution, including knowledge about specialized products and services the financial institution offers, for example, foreign exchange, trade finance, commercial lending, or US dollar clearing.
- Customer due diligence (CDD) and Know Your Customer (KYC) protocols to onboard new customers and monitor existing customers, particularly where the governing agreement identifies anti-money laundering (AML)

and Customer Identification Program (CIP) compliance deficiencies.

- The relevant technology and data analytics for CDD, monitoring transactions, and screening and filtering for sanctions.
- The common compliance training programs financial institutions provide.
- The standards and procedures for auditing a financial institution.

The monitor must ensure that the team has the appropriate subject-matter expertise. For example, the monitor may conclude that the key areas for testing are financial controls, accounting, and compliance technology, in addition to traditional legal issues. In many cases, monitors can supplement teams with auditors, forensic accountants, and compliance technology experts.

The monitor should make these decisions about building out and supplementing the team at the outset. If issues arise that require additional areas of expertise, the monitor should quickly identify those needs and discuss with the government before supplementing the team.

Size of Team and Workstreams

The number of members on the monitorship team varies depending on the scope of the monitorship. The monitor should work in close coordination with the government and the institution to set clear expectations about the size of the team and workstreams. A global monitorship involving travel to multiple locations across the world requires a far larger and varied team than a monitorship of a single branch location. Similarly, a monitorship focused on narrow issues can be handled by a smaller team than a monitorship with a broad mandate.

Depending on the size and complexity of the monitorship, the monitor may divide the team into workstream groups by subject matter. For example, the monitor may create workstream groups for:

- Risk assessment.
- Corporate governance and management oversight.
- Compliance technology.
- KYC.
- Bank Secrecy Act (BSA) and AML suspicious activity monitoring.
- Office of Foreign Assets Control (OFAC) economic sanctions.
- Internal audits.
- Report writing.

The monitor may assign different team members to each workstream.

The size of workstream teams depends on the size, scope, and complexity of the monitorship and the workstream's subject matter. For example, the risk assessment team's role is to perform a risk assessment annually. That team therefore may be small while the compliance technology, CDD, and suspicious activity monitoring teams may be large because they must test the institution's general methodologies and workflow for investigating potentially suspicious activity and the compliance technology for the institution's past and ongoing business.

Team Hierarchy

The leadership structure and hierarchy depend on the nature, complexity, and scale of the work and the size of the monitor team. The monitor generally has a senior leadership team or individual who guides and oversees the monitor team's work and progress and makes decisions (with team input) as needed. The senior leadership team sets the tone for the monitorship. This team should ensure that the monitor team conducts the monitorship in a targeted, cost-efficient, and consistent way. In large monitorships, the monitor may assign one or more members of senior leadership to act as deputies and oversee the day-to-day progress of each workstream and other projects, such as transaction reviews, to ensure the work is progressing satisfactorily.

An executive committee, made up of the workstream team leads, may help senior leadership, particularly in large monitorships. The executive committee keeps senior leadership apprised of progress and developments of the work and any issues and decision points that arise.

Onboard the Team

The engagement letter usually describes the process for onboarding team members. Each team member, including third-party experts, must agree to:

- Follow the terms of the engagement letter, including the confidentiality obligations.
- Undergo a background check, if requested.
- Provide conflicts disclosures and update them if changes occur.
- Certify compliance with cybersecurity and other information technology requirements for accessing and reviewing the financial institution's information.

The government may require that the monitor designate team members as either core or non-core team members. Core team members are involved throughout the monitorship and dedicate a larger portion of their availability to the matter. Non-core team members spend less time on the matter and may only work on discrete issues where they have specific expertise. This requirement helps ensure a consistent and knowledgeable core team throughout the monitorship.

For large monitorship teams, the workstream leads and the senior leadership team typically train the core team members on goals, processes, and tasks. The core team members then train the rest of the team on those issues and explain the institution's business, the conduct that led to the monitorship, and the legal and factual considerations for the relevant subject matters.

Draft a Work Plan

The monitor provides the financial institution and the government with a work plan that gives an overview of the information to review, tests to perform, and reports to prepare. The governing agreement may also set out the timeline for the monitor to provide the initial and subsequent work plans (for example, 60 days after being retained) and the timing for the parties to give comments (for example, 30 days after receipt of the work plan). The work plans should contain enough detail so that the parties are not surprised later. The work plan may also change because of changing circumstances, new information, or modifications to the governing agreement or the engagement letter.

The work plan typically includes:

- A description of:
  - the institution's policies and procedures to be evaluated; and
  - the data and systems to be analyzed.
- A list of:
  - individuals to be interviewed; and
  - locations to visit.
- A schedule of the reports the monitor team will prepare.
- A timeline for the monitor and the institution to achieve certain tasks to allow the parties to track progress (for example, deadlines for the monitor to request information and the institution to provide it).

The work plan should build in sufficient flexibility to address unanticipated issues. If something is completely unaddressed, the monitor should look to the governing agreement or discuss with the government the proper way to revise the work plan.

Budget

When providing the work plan, the monitor should include an estimated budget of the fees and expenses for each month to complete the work plan so the financial institution can plan its costs accordingly. While the monitor should try to avoid exceeding the budget, accomplishing certain tasks may require doing so. The monitor should advise the institution of any anticipated overages as soon as possible.

Disputes

If the monitor and financial institution disagree on the work plan or scope of the monitorship, the parties should try to reach a resolution. If they cannot reach an agreement, the government usually resolves the dispute. The monitor does not need to appease the institution but creating an adversarial relationship with the institution is unlikely to produce a successful monitorship.

Managing the Monitorship

The monitor should liaise with the designated people at the financial institution to request documents and information, access data, interview relevant individuals, and visit the relevant locations (see Liaise with the Financial Institution). The monitor should communicate regularly about the team's progress and any issues that arise with:

- The monitor team (see Communicate with the Monitor Team).
- The financial institution (see Communicate with the Financial Institution).
- The government (see Communicate with the Government).

Liaise with the Financial Institution

To accomplish the monitorship's objectives, the monitor must request documents, information, and access to the financial institution's systems. The institution typically designates one or more of its employees to act as a liaison or project manager for the monitorship. The institution's liaison passes on the monitor's requests to the appropriate institution employees. If granted, the liaison facilitates fulfilling the monitor's request.

The monitor typically designates one or more team members or engages a professional project manager to coordinate with the institution's liaison. The monitor's project manager should create mechanisms to track outstanding issues. For example, the project manager may create several comprehensive tracking spreadsheets, such as:

- A document request tracker.
- An interview request tracker.
- A query tracker listing follow-up questions and clarifying inquiries generated from interviews, document review, or observations during testing of the institution's compliance processes and systems.
- An issue and action tracker for outstanding action items that arise at any point. This tracker keeps a record of actions the institution promised. It may include items from the document, interview, or query trackers that remain unresolved for an unreasonable amount of time so that their progress is more closely tracked and possibly escalated within the institution or to the government.
- A recommendation and corrective action tracker to evaluate the institution's progress on the monitor's recommended remediations to the compliance program.

The project manager should record in the trackers the dates of each request and the response deadlines and highlight any past due items. The monitor may use the trackers to support a request to toll the monitorship because of the institution's delay or failure to comply with a request.

The project managers from the monitor team and the institution should speak or meet regularly to exchange updates, including whether the institution may miss any deadlines, and identify any outstanding issues, such as system access issues or problems with the institution's responsiveness to certain requests. If the project managers cannot resolve an issue, the monitor should escalate it further within the institution, such as to the institution's executive leadership or board of directors. If the issue persists, the monitor should raise it to the government.

Communicate with the Monitor Team

The monitor should appoint a team leader for each workstream to participate in regular executive committee meetings or check-ins to report on progress and potential roadblocks. Depending on the size of the monitorship and individual management styles, the full senior leadership team can participate in these meetings or rely on the deputies to attend and report any crucial information to the full senior leadership team.

Depending on the circumstances, the monitor may implement:

- Formal check-ins between the monitor, the deputies, and the workstream leads on at least a monthly basis. However, during more active periods, the check-ins should occur more frequently to discuss progress, impediments, and findings.
- Weekly calls between the workstream leads and the deputies to discuss weekly workflow, important developments or findings, and any impediments.
- A formal or ad hoc reporting process for the deputies to inform the monitor's senior leadership about any crucial issues when they arise.
- Regular daily meetings between workstream leads and their workstream teams.
- Weekly executive committee meetings between the monitor and deputies to discuss any important developments, strategic decisions, important deadlines, or reporting obligations.

Communicate with the Financial Institution

The monitor should schedule separate regular check-ins with the financial institution's management and its compliance department. These check-ins allow the monitor team and the institution to raise issues, communicate about progress, share thoughts or conclusions, and ask questions.

During particularly active periods, such as a testing phase, the compliance department check-ins should be weekly or daily, and at other times, they should be bi-weekly or monthly. Workstream leads should participate in the compliance department meetings related to their subject area.

Management check-ins should be bi-weekly or monthly unless there is a special need. The monitorship's senior leadership should participate in the management meetings.

Communicate with the Government

The monitor should have regularly scheduled check-ins with the government at least monthly, to disclose the progress made and discuss any new developments. The monitor may also:

- Ask for guidance on certain issues, for example, how to handle the financial institution asserting a privilege or refusing to provide specific information.
- Seek input on any areas of conflict with the financial institution.
- Preview a possible request to toll or extend the monitorship because of misconduct or a lack of cooperation.

Handling the Monitorship

The monitor team should:

- Foster a trustworthy and productive working relationship with the financial institution (see Build Trust and a Constructive Relationship While Maintaining Independence).
- Learn about the financial institution's business (see Understand the Business).
- Know the relevant compliance standards (see Understand the Applicable Standards).

Build Trust and a Constructive Relationship While Maintaining Independence

To create a positive working environment, the monitor team must build trust with the financial institution and refrain from acting as though the monitorship is a punishment. The monitor team should respect that the institution is an ongoing business and continues to operate. To avoid unnecessary hardship on the institution's employees, who are responding to the monitor's requests while continuing to perform their regular duties, the monitor should:

- Schedule interviews and meetings in advance.
- Be thoughtful and targeted with document requests.
- Limit repetitive interviews of the same individual.
- Keep interviews focused, if possible.
- Always be respectful toward employees.
- Avoid disrupting the business when working on-site, if possible.
- Set reasonable deadlines for the financial institution to:
  - provide documents and information; and
  - implement the monitor's recommended improvements to the compliance program.

Understand the Business

The monitor team must learn the financial institution's business operations and financial objectives by, for example:

- Meeting with the institution's management and employees.
- Visiting the institution's offices.
- Reviewing documents, such as the institution's business plans and regulatory filings.
- Conducting interviews (see Conduct Interviews).

After learning about the financial institution's business, the monitor can:

- Identify the risks the institution faces.
- Assess the internal controls the institution uses to address its risks.
- Evaluate the institution's compliance program and existing controls.
- Recommend policies, procedures, and internal controls that make sense for the particular institution's business model and culture.

Understand the Applicable Standards

Before evaluating the current state of the compliance program, the monitor must understand the published guidance and standards from the relevant government agency or regulator and the American Bar Association (ABA), such as:

- The ABA Criminal Justice Standards for Monitors (ABA Standards for Monitors).
- The standards for an effective compliance program under the Federal Sentencing Guidelines for Organizations (U.S. Sentencing Guidelines § 8B2.1).
- The DOJ's guidance on compliance programs (see DOJ: Justice Manual § 9-28.800).
- The DOJ Criminal Division's guidance on compliance programs (see Practice Note, US Department of Justice Standards for Effective Corporate Compliance Programs).
- The SEC and DOJ's guidance on compliance programs in the Resource Guide to the US Foreign Corrupt Practices Act, Second Edition (July 2020).
- The SEC's guidance for reviewing a compliance program (see SEC: Questions Advisers Should Ask While Establishing or Reviewing Their Compliance Programs).

- Any applicable financial regulator's compliance program guidance, rulemaking, or other publications.

Review Compliance Program and Initial Report

The monitorship typically begins with the monitor's review of the financial institution's compliance program, which includes:

- Conducting a root cause analysis of the compliance failures and the misconduct committed that are the subject of the governing agreement (see Conduct a Root Cause Analysis).
- Examining senior management's oversight of compliance risks and the adequacy of the members of the compliance department (see Assess Compliance Governance).
- Assessing the institution's process for onboarding customers and the institution's ongoing monitoring of its customers (see Evaluating the Customer Due Diligence Process).
- Evaluating the institution's compliance systems (see Assess the Compliance Systems).
- Assessing how the compliance department checks the quality of the data the institution receives (see Evaluate the Data Governance).
- Evaluating the institution's processes for identifying potential suspicious transactions (see Assess the Transaction Monitoring for Suspicious Activity).

After this review, the monitor issues an initial report with findings and recommendations for the institution to address throughout the monitorship term. The governing agreement sets a deadline for when the initial report is due, which is usually within the first year.

The initial report is different from subsequent reports because it focuses on the state of the institution before the monitorship and the monitor's plan to accomplish the monitorship's objectives. The content in the initial report often overlaps with content in the work plan. The initial report serves as a benchmark to measure against the institution's future progress.

For information on drafting the report, see Initial Report.

Conduct a Root Cause Analysis

As part of many of these tasks, the monitor team conducts interviews to gather information and test the information they receive (see Conduct Interviews).

The monitor team should test the institution's compliance technology to determine whether it contributed to the failure. The monitor team should search for and review any complaints or allegations of the same or similar misconduct and how the institution addressed them. For each complaint or allegation, the monitor should evaluate:

- Whether the financial institution thoroughly investigated the complaint or allegation.
- The financial institution's findings.
- Any remedial actions the financial institution took.

The monitor team should learn about the causes of previous compliance failures by reviewing the government's findings and any internal documentation of compliance issues, which may identify persisting problems. For example, internal audit reports often contain a treasure trove of issues or compliance failures identified over time. The monitor team may also ask the relevant employees to identify or provide their opinions about the causes of previous compliance failures.

The monitor team should review the institution's compliance policies at the time the misconduct occurred to determine whether there were any gaps that allowed the misconduct to go undetected. The monitor team should also determine if the employees failed to follow the institution's compliance policies and procedures, for example, by skipping a necessary step in the transaction review process.

The monitor team should assess whether, at the time the misconduct occurred, the compliance personnel lacked the appropriate subject-matter expertise. The monitor may do so by conducting interviews and reviewing documents, such as personnel files, including performance reviews.

The monitor team should also examine if the compliance department had adequate staffing levels when the misconduct occurred. The monitor may evaluate the staffing levels by conducting interviews and reviewing documents, including the compliance logs showing how long employees spent to complete compliance activities.

Assess Compliance Governance

The monitor team must evaluate the financial institution's system of rules, practices, and processes for compliance issues that the institution put in place to ensure participation, accountability, transparency, and responsiveness. To do so, the monitor should explore, for example:

- The tone that management and the board of directors have set (see Evaluate the Tone from the Top).
- The culture for following the compliance structure (see Evaluate the Culture of Compliance).
- The adequacy of the compliance department's personnel (see Assess Compliance Department Personnel).
- The sufficiency of the compliance training provided (see Evaluate the Compliance Training).

For more information about effective compliance programs, see Practice Note, Developing a Legal Compliance Program.

Evaluate the Tone from the Top

The monitor team must evaluate whether the board of directors and the C-Suite or other senior management have set the appropriate tone through words and actions for employees and third parties that compliance is important, that is, that the financial institution prioritizes compliance processes and procedures.

To assess senior management, the monitor team should review senior management's written communications about compliance and its responses to escalations of compliance issues to assess whether senior management has:

- Effectively communicated the importance of compliance to all employees and third parties.
- Empowered all employees and third parties to identify and escalate compliance issues.
- Encouraged all employees and third parties to report any compliance issues that arise.
- Responded to compliance issues appropriately, in a timely manner, and in a way that demonstrates that the financial institution takes compliance issues seriously.

As part of its assessment, the monitor team should also assess senior management's reactions to the monitor team's presence and work, including its findings and recommendations. The monitor team should gauge whether senior management accepts that change is needed. Any substantial resistance to the monitor team's legitimate inquiries, findings, and recommendations may indicate that senior management does not accept full responsibility for its compliance failures or is not committed to remediating its compliance failures. Conversely, senior management's acknowledgment of the monitor team's findings and proactive engagement with the monitor team to address its recommendations may indicate a positive shift in the institution's compliance culture and trajectory.

To assess whether the board of directors plays an active role in compliance issues, the monitor team should review the compliance reports submitted to the board and the portions of the board meeting minutes dealing with compliance issues. The monitor team should also investigate whether the board had any further involvement in the compliance issues that reached the board.

For more information about the responsibilities of the board of directors, see Practice Note, Fiduciary Duties of the Board of Directors.

Evaluate the Culture of Compliance

The monitor team evaluates the financial institution's culture of compliance, that is, the social norms employees follow when performing their duties. Misconduct often comes about because of ethical blind spots, rationalizing, or self-deception rather than purposefully committing misconduct. Employees are more inclined to do what they see other employees doing or what management's messaging sets out, particularly about honesty and integrity. Acting ethically must be ingrained in the institution's culture.

The monitor team should interview current and former employees from all levels and parts of the business and third parties. The monitor team should assess, for example:

- The financial institution's communication of compliance policies to the employees or third parties and whether they follow them.
- Whether the employees and third parties have the necessary tools to understand their roles and responsibilities in dealing with the institution's compliance risks and the reporting lines and escalation procedures if a compliance issue arises.
- The ability of the employees and third parties to request and receive guidance on compliance issues in a timely manner.
- The frequency of compliance training.
- If the employees and third parties sufficiently acknowledge, own, and address the compliance risks related to their roles and responsibilities at the institution.
- Whether employees and third parties adequately follow the compliance policies.
- The employees' and third parties' perceptions of senior and middle management's commitment to compliance.

The monitor team should review employee performance reviews and the recent history of disciplinary actions to determine how the institution responded to employees who identified or failed to identify compliance issues, including changes to their compensation. For example, the team should investigate whether the institution rewarded employees' successful efforts to address compliance risks with promotions, raises, bonuses, and positive feedback and penalized employees who failed to sufficiently own and focus on compliance risks. The monitor team should also examine any employee upward reviews of their supervisors to assess the employees' experiences when reporting compliance issues.

The monitor team should review how the financial institution implemented its corporate and compliance governance frameworks. The monitor team should consider the frequency of the institution's training on the frameworks and the availability of the documented frameworks to staff.

The monitor team should evaluate how the staff communicate compliance issues to senior management. The monitor team should review the institution's policies and procedures setting out the reporting lines and escalation procedures when a compliance issue arises. The monitor team should interview the employees to determine if the actual practices were different from the official policies and procedures. The monitor team must determine whether the policies and procedures provide clear guidelines for identifying compliance issues and reporting them and whether the employees or third parties are comfortable following the policies and procedures.

If the institution has previously used anonymous surveys, the monitor team should review the employee submissions, the results of the surveys, and the institution's responses to any compliance issues identified. The monitor should also interview the individuals who managed the anonymous surveys to understand how they carried out the surveys, including:

- Who reviewed the surveys.
- How the feedback was solicited, for example, if the survey was announced by email or at a meeting attended by all employees.
- Whether employee participation was voluntary.
- What questions employees were asked.
- How results were reported to senior management to ensure that the institution effectively addresses any issues identified.
- How senior management responded to the feedback, including whether senior management was receptive to or dismissive of negative information.

If the institution has never used anonymous surveys, the monitor may encourage the institution to use anonymous surveys to assess employee perspectives on the compliance program.

Assess Compliance Department Personnel

The monitor team must evaluate the adequacy of the compliance department personnel, including the number of compliance employees, their experience, and their expertise. The monitor team must then determine whether the department contains an appropriately and sufficiently staffed and qualified team to handle the volume of transactions processed by the institution and the scope of the monitoring required for the types of transactions processed. For example, the monitor team may consider whether the institution employs enough staff to conduct a multi-level review of alerting transactions that may indicate suspicious activity. The monitor team should evaluate whether the institution's compliance personnel include subject-matter experts for the institution's areas of business risk.

The monitor should also assess whether the compliance department is sufficiently independent from senior management and if the Chief Compliance Officer (CCO) has ample input in compliance-related decisions. To do so, the monitor team should review the institution's policies, procedures, and practices for making decisions about compliance-related issues to see if the institution's protocols include:

- Reporting lines between compliance leadership and the institution's senior management.
- Escalation procedures for disagreements between the compliance and business departments on compliance issues.

However, the monitor must understand that the business side of the institution ultimately owns all compliance risks and must contribute to managing the risk.

If the parties agree, a member of the monitor team may observe the meetings between the compliance and business employees. Before doing so, the monitor should consider if the team member's presence is important enough to overcome the likely disruption their presence would cause. If the disruption would be too great, the monitor should instead rely on the interviews of the compliance and business employees.

If present at these meetings, the monitor team member should evaluate the compliance and business personnel's ability to discuss compliance issues and decide how to address the issues, particularly when faced with their competing concerns.

Evaluate the Compliance Training

The monitor team must evaluate the quality of the institution's compliance training. The monitor team should assess whether:

- The training fully describes the applicable issues and explains each employee's role and responsibility to identify, escalate, and address any issues that arise.
- The participants understood the training by, for example, conducting interviews or reviewing subsequent employee examinations on the training.

The monitor team should also evaluate whether the frequency of the trainings for each subject matter is sufficient and the methods for recording each individual's attendance, including the use of attendance sheets or other tracking mechanisms.

Evaluate the Customer Due Diligence Process

The monitor team must assess the adequacy of the institution's customer onboarding process and ongoing monitoring of existing customers. For example, the monitor should assess how the financial institution:

- Collects and verifies the necessary information to identify its customers to comply with its KYC and CIP obligations.
- Identifies and verifies the information its legal entity customers provide about their ultimate beneficial owners.
- Passes on information about any suspicious or potentially suspicious transactions to those responsible for the ongoing due diligence process.
- Maintains and updates customer information on a risk basis by, for example, regularly screening news stories and block lists (lists of persons or entities that are blocked from transacting with US persons, such as the Specially Designated Nationals and Blocked Persons List (SDN List)) for customer and beneficial owner names to uncover negative information about them.
- Appropriately addresses any customers or beneficial owners that raise red flags, including offboarding a customer.

The monitor team should also evaluate how the institution learns the nature and purpose of each customer relationship, which may include understanding the types of transactions in which a customer is likely to engage, so that the institution can develop an accurate customer risk profile. The institution's process to determine customer risk profiles should be sufficiently detailed to differentiate between significant variations in the money laundering and terrorist financing risks of its customers. An insufficient process can have a ripple effect in multiple areas of the institution's internal controls and weaken its entire compliance program.

For more information, see Practice Notes, US Anti-Money Laundering and Trade Sanctions Rules for Financial Institutions and Suspicious Activity Reporting Requirements for Financial Institutions.

Assess the Compliance Systems

The monitor team typically engages compliance technology experts to test and evaluate the financial institution's compliance systems. The testing requires technical experts with specific knowledge of coding and compliance technology software. The experts test the screening, filtering, and CDD technology and evaluate whether the institution's technology identifies industry-accepted red flags. The experts typically run scenarios through the institution's compliance program to identify weaknesses in the software or its implementation.

Evaluate the Data Governance

A financial institution's surveillance program that monitors transactions for possible money laundering or unusual and suspicious activity is only as good as the quality of its data. The institution's data governance is a crucial component of a compliance program. The monitor must assess the effectiveness of the institution's overall data governance.

The monitor should evaluate the flow of data from the source (for example, the repository of account statements showing all transactions into and out of each account) to the compliance systems. This analysis involves assessing:

- The integrity of the data flowing through the compliance systems, for example, whether the institution dedicates sufficient resources and attention to ensuring the data is complete based on the volume of information and transactions the institution regularly processes and monitors.

- The frequency that the institution performs data quality checks considering the size of the institution and the type and amount of data flowing through its compliance systems.
- The data management protocols for reporting the results of data quality testing to management and addressing any problems identified, by, for example, examining if all departments and personnel involved with or affected by the flow of data are sufficiently sharing information with each other to improve the quality of the data transmitted.
- The institution's data governance framework (the rules and processes for collecting, storing, and using data), including whether the personnel or third-party consultants responsible for testing and ensuring data quality have had sufficient experience or training.

Assess the Transaction Monitoring for Suspicious Activity

If the scope includes AML, complying with the BSA, or economic sanctions, the monitor team must review the financial institution's transactions for suspicious activity. The monitor team should evaluate the institution's processes in place to identify potentially suspicious activity, particularly how the institution manages false positives and the escalation of potentially problematic activity.

The monitor should also request access to the institution's SARs. Financial institutions file SARs with the Financial Crimes Enforcement Network (FinCEN) to document suspicious or potentially suspicious transactions that customers route through the institution. The institution must request approval from FinCEN to disclose the SARs to the monitor.

Reviewing the institution's SARs may help identify:

- Potential areas of compliance weakness.
- Potential screening and CDD weaknesses.
- Problematic customers or third parties for the monitor team to use when performing compliance testing and look-back analyses (see Assess the Compliance Systems and Review Historical Financial Transactions).
- Compliance failures for failing to file SARs on suspicious transactions identified during the monitor's review of financial transactions (see Review Historical Financial Transactions).

However, FinCEN may not grant the financial institution's request to give the monitor access to the SARs, depriving the monitor of the benefit of using the institution's past reporting to inform the monitor's testing.

For more information on BSA/AML and SARs requirements, see Practice Notes, US Anti-Money Laundering and Trade Sanctions Rules for Financial Institutions and Suspicious Activity Reporting Requirements for Financial Institutions.

Conducting the Monitorship: Logistics

A monitor uses several methods to achieve the monitorship's objectives and test the effectiveness of the financial institution's compliance program, such as interviewing people and reviewing data and information, including financial transactions.

Conduct Interviews

The monitor team conducts interviews to learn about the financial institution's operations, culture, compliance risks, compliance program, and employee practices. For information on interviewing witnesses generally, see Conducting Internal Corporate Investigations Toolkit: Conducting the Interviews and Investigation.

Identifying Interviewees

The monitor team initially identifies interviewees by reviewing the financial institution's organizational chart and list of third parties. As the monitorship progresses, the monitor team identifies additional interviewees from, for example, the initial interviews and the document and data review. The monitor team may interview, for example:

- Current or former employees, including officers, managers, and members of the compliance department.
- Current or former directors.
- Third parties, including external vendors or auditors.

Arranging Interviews

For current employees and third parties, the monitor should request the institution's project manager or liaison to contact the employee or third party to schedule the interview. The monitor may contact former employees directly without notifying the institution. However, the monitor should consult with the government beforehand to ensure the monitor is not exceeding the scope of the monitorship and to discuss any additional confidentiality measures that the monitor may need to take.

If an interviewee wants their attorney at the interview, the monitor may consult with the interviewee's attorney or the government to decide whether to allow the attorney to attend.

Attendance by Counsel for the Financial Institution

Counsel for the financial institution may want to attend the interviews to learn the information at the same time the monitor learns it. Before the interview stage (and again later if circumstances warrant), the monitor, after consulting with the government, should determine whether to allow the institution's in-house or outside counsel to attend some of or all the interviews. Accounting for all the facts, the monitor considers whether the institution's counsel's presence during certain or all interviews could prevent the witnesses from being candid because they fear retaliation from the institution. For example, if the monitor learns of a breach in the institution's cooperation obligations, it may want to interview employees about the relevant events outside the presence of the institution's counsel to ensure the employees feel comfortable being fully candid.

If the monitor allows the institution's counsel to attend the interviews, the monitor may restrict counsel's presence to interviews of current employees because former employees typically feel more comfortable speaking without a representative from their former employer present.

If the interviewee contacted the monitor as an anonymous whistleblower, the monitor must interview them without the institution's counsel present to protect the whistleblower's identity (see Whistleblowers).

Confidentiality of Interviewee Disclosures

The governing agreement usually gives the monitor the ability to collect information confidentially or otherwise protect the identity of persons providing information (see ABA Standards for Monitors § 24-4.2(4)(d)). The monitor team may conduct sensitive interviews without informing the institution's counsel. In these cases, the monitor should consider whether to share any information from the interview with the institution's counsel. The monitor should balance the need to provide the institution with sufficient information to address any problems identified during the interviews with maintaining the anonymity of the witnesses to ensure they feel comfortable making full disclosures.

The monitor should inform the interviewee that what information they disclose will remain confidential or anonymized and about what the monitor must do with the information. For example, the monitor should inform the interviewee that their statements:

- Do not act as notice to the financial institution about the information provided unless the institution's counsel attended the interview.
- Are not privileged.
- May be disclosed to the government.

(See ABA Standards for Monitors § 24-4.2(4)(e).)

Gather Information and Use Data Analytics

The monitor team requests the information and data they have identified for review to evaluate the institution's compliance program. The financial institution then collects the information and makes it available through the appropriate medium. The monitor team may review a variety of types of information and data, including:

- Policies and procedures, business plans, risk assessments, and compliance evaluations, which the institution usually provides through a document-sharing platform that the monitor team can access remotely.
- Customer information or data, which the monitor must access through on-site computers at the financial institution.
- Confidential employee reviews, complaints, and disciplinary actions, which the financial institution may only make available for in-person review.
- Telephone call recordings, emails, or text messages between employees and customers, which the financial institution may provide in a variety of ways, such as through a secure document-sharing platform.

If the monitor plans to only test a sample of the institution's data rather than all the data, the monitor team may request summary data before selecting a sample. The monitor typically uses sampling where the volume of transaction data or information is large. Depending on the circumstances and goal of the review, the monitor may try to identify either:

- A representative sample, meaning a sample of the overall transaction population.
- A risk-based sample, meaning a sample that is selected to include only the higher risk countries, jurisdictions, counterparties, or transaction types so that the monitor can identify the most likely candidates for suspicious activity.

Based on the outcome of the sample testing, the monitor team may request additional data or information. For example, if the monitor finds a pattern in the initial sample of transactions (such as a specific red flag), it may request additional data that targets characteristics of the transactions relevant to the pattern to confirm that the trend exists on a larger scale.

A monitor usually uses:

- A third-party vendor to host certain less-sensitive documents on a platform. The financial institution can upload its policies, procedures, and other information requested by the monitor for its review and evaluation to this platform. The monitor team can also host its work product on this platform.
- On-site air-gapped computers (meaning they have no access to the internet or outside networks) provided by the financial institution that can directly access certain systems and sensitive customer and transaction data. The financial institution uses these computers in its normal course of business to avoid sharing highly confidential banking information (such as customer data and transaction details) outside of their own systems.

The monitor and the institution should agree on the third-party vendor document-sharing platform for the monitor to use. The platform should contain a separate restricted space for the monitor to maintain its work product. The platform vendor must ensure each team member receives appropriate access.

The monitor must have effective cybersecurity and data privacy policies and procedures and ensure that the monitor team follows them.

Site Visits

The monitor team should conduct on-site inspections of all the institution's crucial locations, such as branches or offices involved in any of the misconduct that led to the monitorship. Site visits allow the monitor team to personally observe the institution handle its compliance processes, including the institution's review of the incoming data and other relevant documentation for financial transactions. Site visits also help facilitate in-person interviews of employees directly involved in the relevant activity and related remediation work.

However, the monitor may not be able to visit certain locations due to circumstances outside of the monitor's or the institution's control, such as health or safety reasons or local regulatory concerns. For example, the local regulatory authority in a particular country may not approve of a monitor operating in its territory. If the monitor team is unable to access certain locations, the monitor should note that in its reports.

Review Historical Financial Transactions

If the financial institution's compliance program likely failed to identify suspicious or improper transactions, the governing agreement often requires the institution or the monitor to perform a look-back analysis of historical transactions to identify the scope of the previous failings. If the institution undertakes the analysis, the monitor team reviews the results. Depending on when the monitor conducts the root cause analysis, the results of the look-back review may also inform or confirm the monitor's root cause analysis of past compliance problems (see Conduct a Root Cause Analysis).

This look-back is distinct from sampling and testing the current effectiveness of the transaction monitoring, sanctions, or KYC programs. If the monitor conducts the review, the monitor team reviews the institution's historical transaction activity, including transactions with correspondent or intermediary banks. The review includes analyzing the transaction data with the institution's compliance tools, verifying that the data matches the compliance work product, and reconciling the institution's data against data available through other third-party tools, such as World-Check, real-time vessel tracking tools, customs data aggregators, or sanctions screening lists.

To review financial transactions, the monitor team usually:

- Develops a methodology that must be approved by the government and disclosed to the financial institution. The methodology details the scope of the review, including whether it includes all transactions, only high-risk transactions, or a sampling of transactions.
- Submits requests for relevant data and access to the relevant systems.
- Trains the transaction review team retained by the monitor on the specific information necessary for the review, such as:
  - the compliance failings that led to the monitorship;
  - the compliance tools the financial institution uses;
  - the red flags to look for; and
  - the monitor's objectives for the review.
- Provides real-time information sharing with the financial institution about any suspected violations the transaction review team discovers.

Drafting Reports

Drafting reports is one of the most important and time-consuming tasks the monitor must perform. The work plan should include ample time for drafting reports. Monitors may designate a team whose primary responsibility is to coordinate the workstream leads' drafting of the sections of the report related to their work.

The monitor team must draft reports that accurately provide their assessment of the financial institution's actions, both positive and negative. The monitor's reports are a primary means for the government to assess the monitorship's effectiveness and the institution's progress. The institution and its board of directors use the reports to assess the institution's progress and continued weaknesses.

To draft a report, the drafter should schedule regular check-ins with each workstream team to learn their findings and if they have found any new developments. The drafter should then prepare a high-level topical outline by theme or workstream with the assistance of the workstream teams. They should then convert the high-level outline into a detailed report that includes support for key findings, themes, and recommendations. The drafter should ensure that the report addresses all key areas in the governing agreement and does not include findings that are outside the scope of the monitorship.

Reports should be balanced and acknowledge program enhancements that the institution has effectively deployed, where appropriate. Rather than focusing primarily on the institution's failings and areas for improvement, a balanced approach provides the government with a fulsome understanding of the state of the institution's compliance program and the relative significance of any negative findings.

Each report should describe:

- The key findings, themes, and conclusions or recommendations.
- The work the monitor team performed since the last report and the methodologies the monitor used.
- Any interviews the monitor team conducted, including each individual's function and level.
- Any site visits the monitor team conducted.
- Any past or external work the monitor relied on to reach its conclusions, for example, previous compliance evaluations or audits.
- Any improvements the financial institution made to its compliance program.
- Any negative findings with supporting evidence and, if applicable, the financial institution's acceptance of the findings.
- The monitor's recommendations and conclusions with supporting evidence.
- The schedule for the financial institution to implement the recommendations.

The reports usually contain confidential information. However, the monitor team should anonymize certain confidential information where possible, such as employee and customer names.

The governing agreement may allow or require the monitor to share a draft of each report with the institution for feedback before the monitor submits it to the government. The preview ensures the institution is not surprised by the monitor's findings and recommendations. Providing a preview also gives the institution the opportunity to point out any factual errors or give input on the feasibility of the monitor's recommendations. (See ABA Standards for Monitors § 24-4.3(1)(d).)

If the monitor finds that any of the institution's requested changes correct or clarify facts reflected in the monitor's reporting, the monitor must decide whether to make the suggested changes or to merely reference the institution's comments in the final version. The governing agreement may also give the institution an opportunity to submit comments in writing either in the report or appended to it.

The governing agreement typically classifies the monitor's reports as confidential documents. Other interested parties, including the media, have tried to obtain access to a monitor's reports without success (see, for example, *United States v. HSBC Bank USA, N.A.*, 863 F.3d 125, 135-42 (2d Cir. 2017) (holding that the district court could not disclose the monitor's report because the report is not a judicial document)). For more information on monitor reports, see ABA Standards for Monitors § 24-4.3(4).

Initial Report

The initial report usually contains:

- An introduction section and an executive summary of the key provisional findings, themes, and conclusions of the initial evaluation of the financial institution's compliance program.
- A background section describing the financial institution's structure at the start of the monitorship, any relevant regulatory issues, and any changes or enhancements the financial institution made to its compliance program since it discovered the misconduct.

- A high-level description of:
  - interviews;
  - site visits;
  - document review; and
  - data testing or analysis.
- Initial findings.
- Initial recommendations and corrective actions with supporting information.
- The monitor's plan and schedule to review the financial institution's compliance processes, procedures, and organizational culture, which may be separated by theme or workstream (see Size of Team and Workstreams).

Annual and Interim Reports

The governing agreement instructs the monitor about when it must provide subsequent reports, which is usually annually. The monitor may also prepare interim reports outside of the schedule to address any new issues that arise that the monitor believes warrant more immediate reporting.

Annual and interim reports are much shorter and more targeted than the initial or final report. The monitor usually organizes them by theme or workstream. The monitor describes the institution's progress, the work the monitor performed, any notable developments, the corrective actions implemented, and the monitor's recommendations for changes the institution should make to comply with the governing agreement. The reports also note whether the institution is complying with the terms of the governing agreement. (See Morford Memo, at 6.)

Special Issues

Confidential Information

The monitor team routinely accesses the financial institution's customer information, transaction data, and other highly confidential information, including CSI (see Confidential Supervisory Information). The monitor must comply with all applicable federal and local laws for protecting each type of confidential information (for example, 12 C.F.R. § 261.20 (CSI) and N.Y. Banking Law § 36(10) (examination and investigation materials)). The engagement letter usually sets out additional requirements and conditions for the monitor to adhere to when handling confidential information (see Engagement Letter).

The engagement letter typically requires the monitor to:

- Only use the institution's confidential information to carry out its monitorship duties and responsibilities.
- Implement or confirm the existence of comprehensive protocols and trainings for team members on handling and protecting confidential information.
- Inform the government or financial institution about any:
  - breach of confidentiality; or
  - request for the disclosure of the institution's confidential information from third parties, such as civil litigants or other government agencies.
- Return or destroy confidential information when the monitorship ends, except for records that the monitor must retain under a law or regulation or as part of the monitor's general firm document retention policies applied in its normal course of business. On confirmation from the government that the monitorship has ended, the monitor and the institution typically negotiate a date by which the monitor must return or destroy confidential information, subject to the government's approval.

Confidential Supervisory Information

In the course of its review, the monitor team may review CSI, which is typically information prepared by or for financial regulators (12 C.F.R. § 261.2; see Practice Note, Bank Supervision and Examinations: Confidentiality Issues). The monitor must comply with state and federal requirements to access CSI (see Confidential Information). The institution must request a waiver from the financial regulator to allow the institution to give the monitor access to the CSI.

CSI can be some of the most valuable information the monitor team reviews because it includes the reports of regulatory examinations and any written responses the financial institution submitted. This information provides context and background for any deficiencies or other issues previously identified with the institution's compliance program.

Data Privacy

A monitor may encounter multiple applicable sets of laws because the financial institution's transactions, data, information technology (IT) systems, compliance frameworks, customer information, and other aspects of its business likely cross into other states or countries. When seeking access to the institution's data and

information, the monitor must consider US laws and regulations, international privacy laws, blocking statutes, or other regime-based restrictions. When confronted with multiple applicable sets of laws, the monitor should consult with local counsel in the various jurisdictions involved. Where multiple laws conflict, the monitor should consult with the government about how best to proceed within each jurisdiction.

In some instances, to obtain certain protected data or information, the government may need to request that a separate governmental or regulatory authority grant the monitor access.

For information on data privacy issues, see Practice Notes, Global Data Localization Laws: Overview and Blocking Statutes Chart: Overview.

Whistleblowers

At the outset, the monitor must ensure that the financial institution distributes the monitor's contact information to all employees and informs them that they may reach out to the monitor directly, if they want. This creates a communication channel for potential whistleblowers to contact the monitor without fear of retaliation from the institution. After interviewing a whistleblower, the monitor must inform the government about the information gathered in the interview.

Alternatively, a whistleblower may contact the government with information about potential misconduct. The government may then inform the monitor about the whistleblower's report.

Discovery of Unrelated Misconduct

If the monitor discovers misconduct unrelated to the scope of the monitorship, the monitor's course of action depends on the nature and seriousness of the misconduct and the monitor's trust in the financial institution's current leadership. For serious misconduct that implicates the financial institution's compliance with the governing agreement's terms or the applicable laws or regulations, the monitor should immediately inform the government and ask for its guidance on how to proceed. For less serious unrelated misconduct, the monitor may choose to first notify the institution to allow it to investigate and remediate the misconduct before the monitor notifies the government.

The monitor usually should not investigate unrelated misconduct unless the government instructs the monitor to do so. If the institution conducts an internal investigation into the unrelated misconduct, the governing agreement's terms may not obligate the institution to share its findings with the monitor. If the institution does not share the results, the monitor may inform the government about the unrelated misconduct.

Make Findings and Recommendations

After conducting a root cause analysis and evaluating the compliance program, the monitor issues its findings and recommends actions the financial institution should take to improve or enhance its culture and compliance program to deter or prevent future misconduct. The monitor's recommendations are tailored to the institution's business needs and culture and the applicable laws and regulations. The monitor's findings and recommendations should be memorialized in reports to the government (see Drafting Reports).

The monitor must provide support for its findings and recommendations to explain to the institution why they are warranted and necessary. The government or institution may provide feedback on the monitor's findings and proposed recommendations, particularly if the monitor's recommended remediation work is likely to take longer to institute than the remainder of the monitorship term.

The monitor's recommendations typically require the institution to implement policies and procedures that ensure the compliance program prevents or detects future misconduct. The monitor's recommendations should:

- Build on any remediation work the financial institution has already begun, where possible.
- Seek to improve the financial institution's existing compliance program rather than perform a complete overhaul, where possible.
- Be practical considering the financial institution's business and culture.
- Avoid fundamentally altering the way the financial institution does business.

A monitor's recommendations to improve or enhance the compliance program may be specific to certain subject-matter areas or apply to the compliance program generally. Recommendations may include:

- Replacing or supplementing members of the compliance department.
- Improving or drafting new compliance policies and procedures.

- Updating, reconfiguring, or replacing technology.
- Transforming the tone from the top to emphasize the importance of acting ethically.

If the monitor finds that the institution's compliance culture is to follow the rules and procedures and not to try to circumvent them, the monitor can focus on strengthening the substantive compliance program. If the compliance culture is poor, the monitor must also recommend changes to improve the culture so that it promotes acting ethically and complying with all rules, laws, and regulations.

Strengthening an institution's compliance culture is a gradual and complicated process. Progress is hard to measure. To guide the institution in reforming its compliance culture, the monitor should identify potential causes, for example, gaps in governance frameworks, lack of effective forums for reporting issues to the compliance department or management, low morale, or insufficient staffing.

The monitor should also help create or improve existing employee feedback systems. An effective employee feedback system measures employee sentiment toward compliance responsibilities and provides a way for employees to report any concerns. For example, the monitor should consider recommending that the institution implement:

- Anonymous employee surveys.
- Secure means for whistleblowers to report potential misconduct anonymously.
- Regular peer meetings to discuss compliance issues.
- A compliance component tied to employee evaluation and compensation.
- Upward reviews of managers by employees.

The monitor should pay close attention to whether management is resistant to addressing any compliance issues the monitor identifies for remediation. The monitor should report any unjustified push back in its reports.

Financial Institution Rejection of a Recommendation

If the financial institution rejects one of the monitor's recommendations, the institution or the monitor should inform the government of the rejection and the reasons for it. The government evaluates the recommendation and the reasons for its rejection to decide whether the institution is complying with the governing agreement. (See Morford Memo, at 6.)

Potential Breach of the Governing Agreement

If the monitor team discovers that the misconduct at issue continued after the financial institution entered into the governing agreement, the monitor must follow the agreement's instructions on how to handle, such as immediately informing the government. If the agreement is silent on how to address ongoing misconduct, the monitor should immediately raise the issue with the government.

The monitor should recommend how to correct any ongoing misconduct or non-compliance with the governing agreement. If the misconduct or issue persists over the course of the monitorship, corrective actions should become more specific and targeted. For example, if the institution's screening technology repeatedly fails the monitor's testing, the monitor may recommend that the institution replace the system.

Tracking and Assessing the Institution's Remediation

After the monitor issues the initial report with its recommendations and any subsequent report with recommendations, the monitor team evaluates how the institution is implementing the recommended remedial steps and testing whether the remedial steps achieve their purpose. The monitor issues annual (and sometimes interim) reports documenting the institution's progress, any new recommendations, and any other issues that arise (see Annual and Interim Reports).

Track the Institution's Progress

The monitor team should create a system to track the institution's remediation progress. The tracker should identify each recommendation and set a reasonable timeline for the institution to implement it. The monitor team may share the tracker with the institution.

The monitor team and the institution should also maintain an open dialogue and work together to remediate the compliance program. The monitor may, for example, schedule weekly meetings with management and the compliance department to discuss the institution's progress and any challenges the institution has encountered.

If the institution fails to implement the recommendations in a timely fashion, the monitor should raise the issue within the institution. If the issue persists, the monitor should raise it to the government.

Assess the Improvements to the Compliance Program

To evaluate the changes made, the monitor team engages in many of the same activities it did during its initial assessment, such as conducting interviews, reviewing documents, using data analytics, and testing the institution's compliance systems (see Review Compliance Program and Initial Report and Conducting the Monitorship: Logistics). The monitor team may, for example:

- Review the new policies or procedures to determine whether they address the deficiencies the monitor team identified.
- Evaluate the changes to the compliance department's funding and personnel.
- Assess the improvements made to providing and tracking compliance trainings.
- Continue to use the compliance technology experts to test and evaluate the remade compliance system to determine if:
  - the improvements are working as designed; and
  - any further upgrades can be made.
- Interview employees to determine whether the tone from the top and middle management is emphasizing the value of compliance by, for example:
  - issuing regular reminders about the importance of honesty and expectation that all employees act with integrity; or
  - rewarding ethical conduct with promotions.
- Sample customer information and financial transactions (with help from the compliance technology experts) to identify any red flags that the compliance program failed to identify.

Concluding the Monitorship

As the monitorship term nears the end, the monitor meets with the financial institution with greater frequency. The monitor either closes out the remaining issues or recommends additional monitoring.

The monitor also communicates with the government more often to keep them apprised of the status of any outstanding issues. The monitor's discussions typically address:

- The status of the institution's remediation work.
- Any outstanding issues and additional corrective actions needed to ensure the institution's continued compliance and the sustainability of the institution's remediation.
- Whether any outstanding issues are severe enough to warrant extending the monitorship, either in full or only for a limited purpose.
- Any issues or corrective actions that will be transitioned to the government to monitor going forward.

Before the monitor issues its final report, the monitor, the institution, and the government meet to ensure that all parties agree about the status of the monitorship. The monitor previews its final findings, including any additional corrective actions. The institution provides its perspective and plan going forward. The government may ask the monitor or the institution for information, details, or clarifications.

The final report should:

- Set out the key findings identified throughout the monitorship.
- Assess the financial institution's progress, in particular, in implementing the monitor's recommendations.
- Discuss the remaining open issues.
- Suggest any corrective actions to ensure continued compliance and the sustainability of the financial institution's remediation.

After the monitor issues its final report, the government may follow up with questions. If the monitorship term is not extended, the government may monitor the institution's continued progress through regular examinations and reporting.