



## EM-31.9

**Category:** Board & Management Operations

**Topic:** Standards of Conduct, Whistleblower, & Criminal Referral

**Published:** 9/22/2023

---

### Overview

Standards of conduct (SOC) is a key component of board and management operations. A comprehensive evaluation of an institution's SOC program should address regulatory compliance and the program's effectiveness. FCA regulations provide both specific guidance and general principles for evaluating SOC programs. However, SOC is a complex area where usually no two circumstances will be identical. As such, while regulatory compliance is important, an institution's SOC program can be fully compliant and ineffective at the same time. Such situations can result in significant reputation risk and potential legal and financial risk for an institution, which underscores the importance of this area. Institutions must ensure SOC programs are both compliant with regulations and effective in practice. Whistleblower and criminal referral programs are also examined in conjunction with SOC programs and are addressed in this Examination Manual topic.

### Examination Procedures and Guidance

#### General

##### **1. SOC Program:**

Determine if the SOC program and related internal controls, including policies and procedures, Standards of Conduct Official's role, Code of Ethics, and training are appropriate and comply with FCA Regulations.

##### Guidance:

FCA Regulation [612.2135](#) includes certain standards of conduct (SOC) core principles with which each director and employee in the System must comply (excluding Farmer Mac). These core principles are the following:

- **Conduct** – A director or employee must maintain high ethical standards and act in the best interest of the institution. They must take actions to preserve both the institution's reputation and public confidence in the System and use good judgement in carrying out their duties and responsibilities. This includes proper and complete reporting to the Standards of Conduct Official (SOCO), effective identification and resolution of any real or potential conflicts of interest with the SOCO, and avoidance of the appearance of self-dealing (e.g., acceptance of inappropriate gifts or favors).
- **Responsibility** – Directors and employees must comply with the institution's SOC program, related policies and procedures, as well as the institution's Code of Ethics. In addition, they must comply with laws and regulations, and properly report any suspected illegal or unethical activity or violations of the institution's SOC program and Code of Ethics by others.

- Fiduciary Duties – Officers and directors must fulfill their fiduciary duties to the institution and stockholders.

The board and management are responsible for maintaining a sound SOC internal control environment that ensures compliance with these core principles. FCA Regulation [612.2137](#) establishes the board’s responsibility for implementation, oversight, and compliance with its SOC program which includes the following:

- Establish a SOC program.
- Appoint a SOCO.
- Adopt a written Code of Ethics.
- Develop SOC policies and procedures.
- Establish appropriate internal controls to monitor for SOC compliance.
- Establish a SOC training program for directors and employees.

Directors, employees, and the SOCO each have a role in complying with these requirements and expectations. Directors and employees are required to identify, disclose, and report to the SOCO any real or potential conflicts of interest they have. A conflict of interest can occur when a person has an interest in a transaction, relationship, or activity that could affect their ability to remain impartial when performing their duties. (Refer to FCA Regulation [612.2130](#) for definitions used when reading the SOC regulations.)

The SOCO assists directors and employees in understanding expectations for identifying and reporting conflicts of interest. The SOCO is also tasked with reviewing conflict of interest reports for material conflicts and conducting investigations of SOC violations, all in the manner determined by the institution's written policies and procedures. (Refer to FCA Regulation [612.2170](#) for a full listing of SOCO duties.)

Conflicts of interest, or the appearance thereof, can adversely affect an institution’s profitability and reputation for fiduciary integrity, which can undermine public confidence in the System. In addition, a conflict may result in financial loss to the institution if the individual involved considers self-interest and personal gain above the institution’s interests. The guidance below focuses on key controls required by FCA regulations. Importantly, proper controls are critical in helping the institution avoid the negative impacts SOC issues can create.

***Policies and Procedures:*** Effective SOC programs begin with the board setting an appropriate culture and tone at the top. SOC policies and procedures should be an outgrowth from this culture and tone, as well as reflect the importance of appropriate and ethical conduct. FCA Regulation [612.2137\(d\)](#) requires boards to develop policies and procedures implementing a SOC program. Importantly, these policies and procedures must promote public confidence, preserve the integrity and independence of the SOC program, and prevent improper use of official property, position, or information. The regulations provide specific details on items that must be included in policies and procedures. Evaluative questions and items to consider when examining SOC policies and procedures include:

- ***Policy and Procedure Content: Do policies and procedures support a culture of high ethical standards and comply with regulatory requirements?*** The board plays a key role in setting a strong and effective culture regarding appropriate and ethical conduct. This culture should be the driving force behind SOC policies and procedures. SOC policies and procedures should be reviewed and updated periodically to ensure they remain pertinent and appropriate as

conditions change. SOC policies and procedures should also include specific reporting elements to ensure the board has the proper awareness and information to oversee the SOC program effectively. SOC policies and procedures should include details on additional disclosure expectations (e.g., interim loan actions, relationships, financial interests). In addition, the institution's SOC policies and procedures should include the specific SOCO reporting expectations required by FCA Regulation [612.2170\(d\)\(2\)](#). Directors and employees are expected to comply with these policy and procedure requirements. FCA Regulation [612.2137\(d\)](#) requires policies and procedures to address, at a minimum, the following:

- Frequency of conflict of interest reporting for all directors and employees consistent with FCA Regulation [612.2145](#). At a minimum, each director and employee must annually report to the SOCO known conflicts occurring in the current fiscal year. (Note: Disclosure schedule should consider the reporting requirements for directors and senior officers in FCA Regulations [620.6 \(a\)](#), [\(e\)](#), and [\(f\)](#).)
- Explanation of what constitutes SOC program compliance, including setting criteria for documentation submitted with conflict of interest reports, and instructions that directors and employees will use to identify and report actual or apparent conflicts of interest. This includes an explanation of the following:
  - What transactions are likely to present real or potential conflicts which includes setting benchmarks and thresholds for both single and aggregate activities. A threshold is the point something becomes an issue and a benchmark is an example to use in comparing transactions (to determine if similar in nature). The explanation could include a discussion of transaction, activity, or relationship examples or scenarios considered as presenting conflicts.
  - What types of transactions the institution will treat as occurring in the ordinary course of business (as defined in FCA Regulation [612.2130](#)). The explanation could include examples or scenarios common in the institution's territory and amongst directors and employees.
  - How to identify if a conflict is material using benchmarks and thresholds. (Material, when applied to a financial interest or transaction, is defined in FCA Regulation [612.2130](#).) The explanation could include differentiating materiality based on type of relationship (e.g., director, employee, senior management, agent) or type of transaction (e.g., real estate, equipment, services, feed).
- Processes for resolving real and apparent conflicts of interest, including actions when a conflict cannot be resolved, and the SOCO's role and authorities in resolving conflicts.
- Conduct of third-party relationships, including specific third-party conflict of interest policies, safeguards for ethical conduct, expectations for disclosing known conflicts of interest, and implementing the requirements of FCA Regulation [612.2180](#) for agents (including a reference to FCA enforcement authorities over institution-affiliated parties).

- Criteria for accepting gifts not already prohibited by FCA regulations, including establishing a de minimis dollar threshold for all permissible gifts regardless of the gift giving reason (must apply both per gift and in the aggregate per recipient, per year), disclosure requirements for gifts received, and procedures for disposing of impermissible gifts.
- Appropriate actions that may be taken against directors or employees who violate SOC policies and procedures, Code of Ethics, or FCA regulations, including who is authorized to take action and when, and the SOCO's authority under FCA Regulation [612.2170](#) to investigate certain conduct issues.
- Provide for anonymous reporting of SOC program or Code of Ethics violations. See the *Whistleblower Program* procedure for additional guidance.
- **Prohibited Activities: Do policies and procedures clearly communicate prohibited conduct as described in FCA Regulation [612.2150](#)?** FCA Regulation [612.2150](#) specifies directors and employees must act consistent with the core principles detailed in FCA Regulation [612.2135](#). Directors and employees are expected to conduct official duties in a prudent and professional manner and to avoid conflicts of interest. In addition, directors and employees must not engage in activities (nor give the appearance thereof) which might impair judgment or objectivity, discredit themselves, or discredit the System. Policies and procedures should specifically address recusal expectations, processes, and controls to ensure directors and employees do not influence or engage in the decision-making process when defined relationships exist. A common example would be decisions impacting a director or employee loan or loans to their family, business partners or businesses in which they own a material percentage, or other close acquaintances. FCA Regulation [612.2150](#) includes specific director and employee prohibited activities; however, the board may decide to further limit activities based on their desired culture, risk tolerance, or other factors. FCA Regulation [612.2150](#) specifically prohibits the following for directors and employees:
  - Use position for personal gain or advantage.
  - Divulge confidential information.
  - Accept prohibited gifts.
  - Purchase property owned by the institution (see FCA Regulation [612.2150\(a\)\(4\)](#) for exceptions).
  - Enter into transactions with prohibited sources (see FCA Regulation [612.2150\(a\)\(5\)](#) for exceptions).
  - Purchase System obligations, including the purchase or retirement of any stock in advance of the release of material, non-public, information (see FCA Regulation [612.2150\(a\)\(6\)](#) for additional details and exceptions).
  - Employee only prohibitions include the following:
    - Serve as a director or employee of certain entities as outlined in FCA Regulation [612.2150\(b\)\(1\)](#).
    - Act as a real estate agent or broker.
    - Act as an insurance agent or broker.
    - Serve as a joint employee (see FCA Regulation [612.2150\(b\)\(4\)](#) for exceptions).
- **Agents: Do policies and procedures address SOC expectations for agents?** Agents include any person with the power to act for the institution and represent the institution in

contracts with third parties or provide professional services to the institution as defined in FCA Regulation [612.2130](#). The institution should identify and maintain a list of all agents and ensure directors and employees are aware of the rules regarding agents. The institution is responsible for administering relationships with its agents. This includes taking appropriate investigative and corrective action in cases of agent breach of fiduciary duties or failure to carry out duties required by contract, FCA regulations, or law. As discussed above, FCA Regulation [612.2137\(d\)\(4\)](#) requires SOC policies and procedures to address the conduct of third-party relationships which includes adopting specific conflict of interest policies and developing safeguards for ethical conduct with agents. SOC policies and procedures must set forth expectations for disclosing known conflict of interests and implement requirements of FCA Regulation [612.2180](#) for agents, which include the following:

- Institution agents must maintain high standards of honesty, integrity, and impartiality to ensure proper performance and continued public confidence in the System.
- Institutions must use safe and sound practices in the engagement and use of agents.
- Institutions must avoid or control sensitive situations, including employing agents who are related to directors or employees, soliciting or accepting gifts either to or from agents, and protecting information obtained by agents. While FCA regulations do not require individual SOC disclosures by agents, the institution may require it as a sound practice when addressing conduct of third-party relationships in policies and procedures. SOC policies and procedures should also address the engagement, use, and retention of agents.
- Agents are considered institution-affiliated parties subject to certain enforcement authorities of the Farm Credit Act of 1971, as amended.

Note: FCA Regulation [621.30](#) specifically requires institutions to have policies and procedures governing the engagement of external auditors that must incorporate the provisions of FCA Regulation [612.2180](#). Refer to the *Financial Reporting Controls* procedure in the *Financial & Shareholder Reporting* Examination Manual topic for examining compliance with FCA Regulation [621.30](#).

- ***Unincorporated Business Entities (UBEs): For institutions that use UBEs, do policies, procedures, or other control processes sufficiently address expectations on compliance with SOC regulations?*** FCA Regulation [611.1153\(c\)\(3\)](#) requires institutions to ensure transactions between a UBE and System institution directors, officers, employees, and agents are conducted at arm's length, in the interest of the System institution, and in compliance with SOC rules. Institution controls used to ensure compliance should be commensurate with the extent and type of its UBE activities. As such, if an institution is involved in a UBE that conducts business operations and has officers, employees, or agents, then policies and procedures should typically address compliance with the SOC requirements.
- ***SOC-Related Policies for Banks: Do bank policies sufficiently address the following SOC-related issues as required by FCA regulations?***

- **FCA Regulation [614.4460](#)** – Each bank board that delegates loan approval of official loans, and loans with potential conflicts to bank management, must have an established policy.
- **FCA Regulation [614.4900\(g\)](#)** – Personnel policies for each Agricultural Credit Bank (ACB) must include written standards of conduct for those involved with foreign exchange activities.

**Code of Ethics, Internal Controls, and Training:** FCA Regulations [612.2137\(c\)](#), [\(e\)](#), and [\(f\)](#) require the board to adopt a written Code of Ethics, establish a system of internal controls to ensure compliance with regulatory requirements, and train institution personnel in their SOC and ethical responsibilities. Evaluative questions and items to consider when examining Code of Ethics, internal controls, and training include:

- **Code of Ethics: Did the institution adopt a written Code of Ethics which complies with FCA Regulation [612.2137\(c\)](#)?** The Code of Ethics must establish the institution’s values and expectations for ethical conduct of directors and employees with regard to business transactions. The Code of Ethics must also include a general statement of expectations for appropriate professional conduct. All directors, employees, agents, and shareholders must have access to the Code of Ethics. The institution’s website must include a statement about the adoption of a Code of Ethics, a summary of the Code, and the entire Code of Ethics is available, upon request, at no cost. If the entire Code of Ethics is posted on the external website, no summary or statement of the entire Code of Ethics being available at no cost is required.
- **Internal Controls: Is the SOC program monitored through appropriate internal controls as required by FCA Regulation [612.2137\(e\)](#)?** Internal controls should expand beyond required policies and procedures; they should also serve to ensure compliance with regulatory expectations. Controls should assess whether staff and directors are complying with the overall culture and intent of the program. FCA Regulation [612.2137\(e\)](#) requires the board to establish a system of internal controls that includes, at a minimum, processes to:
  - Protect against unauthorized disclosure of confidential information.
  - Conduct scheduled periodic reviews to determine continued adequacy of the program and consistency with institution practices, industry best practices, and FCA regulations.
  - Perform internal audits of the SOC program. The scope and depth of these audits, and who completes the audits, must be determined by the board, with the assistance of the SOCO and applicable board committees used for these processes (e.g., Audit Committee). FCA Regulation [612.2137\(e\)\(3\)](#) includes specific objectives a SOC audit must achieve. Refer to the *Audit* and *Transaction Testing* procedures for information on examining audit coverage and conducting transaction testing to validate controls are functioning as intended.
- **Training: Has formal SOC training been provided to all directors and employees as required by FCA Regulation [612.2137\(f\)](#)?** FCA Regulation [612.2137\(f\)](#) requires the board to establish a training program to ensure all directors and employees are informed of SOC regulatory requirements and related policies and procedures at least once a year. Training is an effective tool to communicate expectations and facilitate a proper ethical culture. FCA

Regulation [612.2137\(f\)](#) requires the SOCO to provide SOC training to new directors within 60 calendar days of assuming their position, new employees within 10 business days of beginning work, and periodic training for all directors and employees at least annually. The training must cover any updates or revisions to the SOC program or the Code of Ethics, if appropriate, and reinforce SOC requirements. The expectation is that the training cover what should be reported on the disclosure statements by providing clear examples of items to be reported, and informing staff of the potential penalties and remedies for noncompliance. FCA Regulation [612.2170\(c\)](#) requires the SOCO to obtain written certification of participation from directors and employees upon completion of SOC training.

**Standards of Conduct Disclosures:** As outlined in FCA Regulation [612.2135](#), directors and employees have a responsibility to achieve and maintain high ethical standards in carrying out their duties, obligations, and responsibilities and must avoid conflicts of interest (as defined in FCA Regulation [612.2130](#)). FCA Regulation [612.2145](#) outlines requirements for disclosing and reporting conflicts of interest. Disclosure statements are a key part of the process to identify and prevent conflicts of interest. Evaluative questions and items to consider when examining SOC disclosures include:

- **Reporting Conflicts of Interest: Are director and employee disclosures accurate and completed in accordance with FCA Regulation [612.2145\(b\)](#) and the institution’s policies and procedures?** Directors and employees must identify, disclose, and report any interest or circumstance that does or could constitute a real or potential conflict of interest, as defined by board policy. Director and employee coordination with the SOCO is required to ensure conflicts or potential conflicts are addressed. Directors and employees must refrain from participating in official action, discussion, voting, or influencing any decision on the matter, transaction, or activity deemed as a conflict of interest. Additionally, directors and employees must report any known or suspicious activity by a person affiliated with the institution that is illegal, unethical, or a violation of the SOC program or Code of Ethics. SOC disclosures must be signed and filed at least annually and at such other times as may be required by policies and procedures. The disclosures must be in sufficient detail for a reasonable person to make a conflict of interest determination and decide if the conflict is material (as defined in FCA Regulation [612.2130](#)). Directors and employees are expected to provide subsequent clarifying information when requested by the SOCO to assist in evaluating if conflicts (real or potential) exist. At a minimum, the director and employee disclosures must include the following:
  - Any interest in any business matter, including any loan or loan application, to be considered by the institution, or supervised or supervising institution in the current year.
  - All material financial interests (material is defined in FCA Regulation [612.2130](#)), including those arising in the ordinary course of business, with any director, employee, agent, or borrower of the institution, or a supervised or supervising institution.
  - The name(s) of reportable business entities (as defined in FCA Regulation [612.2130](#)) the director or employee knows or has reason to know, in the current year transacted business with:
    - the institution,
    - any supervised or supervising institution, or

- a borrower that transacts business with the institution, or any supervised or supervising institution.
- The name(s) of family members the director or employee knows or has reason to know transacted business with the institution or any supervised or supervising institution in the current year. (Family is defined in FCA Regulation [612.2130](#).)
- Reportable gifts received or disposed of under the institution's SOC program policies and procedures.
- Other required disclosures for directors and officers. Directors and officers must disclose to the SOCO at least annually (at issuance of the Annual Meeting Information Statement) the disclosures required under FCA Regulations [620.6 \(a\)](#), [\(e\)](#), and [\(f\)](#).

Note: Examiners should consider the results of any transaction testing (completed by FCA during an examination activity or by the institution's audit and review program) when concluding on disclosing and reporting conflicts of interest.

- **Disclosure Form Templates: Do the disclosure form templates clearly and effectively address items required by FCA Regulation [612.2145](#) and the institution's policies and procedures?** The forms should include appropriately worded questions that enable the individual completing the disclosure to understand what must be reported. The institution should also have a process for periodically reviewing the forms to determine if changes to the questions are needed to help individuals better understand conflict of interest situations and prohibitions.

**Standards of Conduct Official Role:** As required by FCA Regulation [612.2137\(b\)](#), the board must appoint a SOCO to comply with the responsibilities of the role detailed in FCA Regulation [612.2170](#). This includes having the necessary authority and resources to fulfill the role, implement the program appropriately, and train employees and board members on individual responsibilities and expectations for program compliance, which is dependent upon the policies set by the board. An institution can appoint one of its officers to this position or the board may outsource this role to a third party, but the board remains accountable for ensuring the SOCO complies with regulatory requirements. An institution may share a SOCO with other System institutions when each institution has a separate confidential relationship with the person serving as the SOCO. Refer to the *Third-Party Risk Management* procedure in the *Direction & Control of Operations* Examination Manual topic for information on examining an institution's outsourcing processes. FCA Regulation [612.2170](#) outlines the SOCO's specific duties and responsibilities. To accurately assess SOC program effectiveness, examiners must understand and evaluate the SOCO's role within the program. Evaluative questions and items to consider when examining the SOCO role include:

- **SOCO Designation and Authority: Did the board appoint a SOCO and grant authorities as required by FCA Regulation [612.2170\(a\)](#)?** FCA Regulations [612.2170](#) and [612.2137\(b\)](#) require the board to appoint a SOCO to carry out responsibilities over the SOC program. As required by FCA Regulation [612.2170\(a\)](#), the board must authorize the following for the SOCO:
  - Direct access to the board to discuss matters related to the SOC program and Code of Ethics.
  - Authority to carry out SOC responsibilities.



- Access to all directors, employees, and agents.
  - Legal authority to receive confidential SOC communications.
  - Adequate resources to implement a successful SOC program.
- **SOC Administration: Is the SOCO administering the SOC program in accordance with policies, procedures, and FCA regulations?** The SOCO must administer the SOC program as determined by policies, procedures, and FCA regulations. FCA Regulation [612.2170\(b\)](#) outlines various program administration responsibilities which may include providing guidance and assistance to directors and employees on conflicts of interest and receiving disclosure reports. The SOCO reviews and acts upon all disclosure reports, as necessary, based on resolved and unresolved conflicts of interest. The SOCO also conducts investigations as required and reports promptly to the board. (See guidance below for specifics on SOCO review, investigations, and reporting). Additionally, the SOCO maintains all SOC program records for a minimum of 6 years as required by FCA Regulation [612.2137\(a\)](#). The SOCO is also required to conduct training for all directors and employees per FCA Regulations [612.2170\(c\)](#) and [612.2137\(f\)](#). (See guidance discussed earlier on training expectations.)
  - **SOCO Review: Does the SOCO complete a thorough, timely, and documented review of annual and ongoing director and employee disclosures?** The SOCO's role involves more than just distributing and collecting disclosure forms. It includes active involvement in helping directors and employees understand the disclosure requirements by providing relevant information and guidance. This includes aiding in identifying a reportable conflict of interest or financial interest, applying board-determined materiality thresholds and benchmarks to a reported conflict, and deciding how to resolve conflicts so directors and employees can comply with regulations, policies, and procedures. After receiving the completed disclosure forms, the SOCO should follow a structured process to ensure reported matters are properly evaluated, seeking additional information if needed. The review should be thorough, sufficiently documented (including the resolution), and discussed with the director or employee, as needed. Other sound practices to consider for an effective SOC program include the following:
    - The SOCO notifying individuals, in writing, of an identified conflict of interest situation and the recommended method of resolving the conflict. The institution's policies and procedures need to determine the SOCO's role and authorities in resolving conflicts. This could include how the SOCO or others in the institution (e.g., human resources) will handle the actual conflict resolution measures (e.g., recusal, reassignment of tasks, additional reporting, separation).
    - The SOCO being authorized access to director and employee loan files and similar resources if needed when reviewing conflict of interest disclosures. Access may be necessary to accurately capture conflicts and potential conflicts so that remediation efforts properly address the conflict or potential conflict. Access to these institution resources would not need to be unlimited (i.e., full-time, unrestricted access), but should employ reasonable controls much like internal credit review. This access may need to be expanded for SOCO investigations conducted under FCA Regulation [612.2170\(d\)](#). When the SOCO is not an institution employee, a recommended safeguard is to have the SOCO sign a confidentiality agreement notating FCA enforcement authorities as described in FCA Regulation [612.2180](#).

- Institution personnel consulting with the SOCO on potential conflict situations that they identify while working on business transactions (e.g., loans) as a means of proactively identifying, and preventing conflicts of interest. This may help ensure preferential treatment is not occurring in institution business transactions.
  - The board designating a member of the board or impartial qualified individual who is best situated to review the SOCO's individual disclosures and follow up as needed.
  - The SOCO being provided access to a current and complete list of the institution's agents and ensuring the SOCO has a process in place to implement the SOC requirements for agents as outlined in FCA Regulation [612.2180](#).
- ***SOCO Investigations: Does the SOCO conduct SOC investigations, as necessary, as authorized by FCA Regulation [612.2170\(d\)](#), policies, and procedures?*** The SOCO is responsible for investigating complaints alleging misconduct or possible criminal behavior by the institution, its directors, or its employees. FCA Regulation [612.2170\(d\)\(1\)](#) outlines cases where the SOCO must investigate or cause to be investigated (i.e., hire investigative team or firm). These include possible violations of criminal statutes, prohibited conduct regulations, FCA SOC regulations, institution policies and procedures; as well as complaints of misconduct or suspected activities of a sensitive nature. FCA Regulation [612.2170\(d\)\(2\)](#) requires the SOCO to report to the board and FCA's Office of General Counsel investigations initiated under [Part 612 Subpart B](#) (i.e., investigations resulting in the preliminary identification of a criminal violation, the removal of a director or employee, or violations negatively impacting public confidence in the System). These reports are required whether or not a criminal referral was actually made. An investigation initiated under [Part 612 Subpart B](#) is one where there is known or suspected criminal activity, potential loss to the institution, or unsafe or unsound actions resulting from the behavior of a director or employee and that behavior involves the assets, operations, or affairs of the institution (which may include SOC or Code of Ethics violations).
  - ***SOCO Reporting: Does the SOCO effectively carry out board reporting responsibilities as required by FCA regulations, policies, and procedures?*** Timely and complete reporting on SOC issues and compliance is a key control for the board to effectively carry out its oversight responsibilities. The SOCO should periodically meet with the board (or designated board committee) to discuss SOC activities. FCA Regulations [612.2170\(b\)\(7\)](#) and [\(8\)](#) require the SOCO to formally report to the board (or designated board committee) all SOC program or Code of Ethics matters, conflicts of interest, current investigations or complaints, and any other issues required by regulations, policies, and procedures. The board should receive sufficient information in reports to carry out its oversight responsibilities. SOCO reporting helps the board engage in the SOC process and provides the SOCO with the necessary resources. In addition, a direct reporting line to the board reduces the potential for undue management influence on SOCO conclusions.
  - ***SOCO Qualifications and Training: Does the SOCO have the qualifications and training to conduct his or her duties in an appropriate manner?*** The SOCO should possess an in-depth knowledge of FCA SOC regulations and the institution's SOC-related policies and procedures. The SOCO must also reflect strong ethics and maintain high standards of honesty, integrity, and impartiality to effectively serve in the role. This person should have the qualifications needed to make SOC determinations, document actions taken, and explain the basis for such actions. The SOCO's qualifications are a strong indicator of an institution's SOC culture, as an

unqualified person in this role would suggest SOC is not a priority to the board and management. The SOCO should participate in regular training to maintain the needed skills as a subject matter expert.

## 2. Whistleblower Program:

Determine if the institution has an effective whistleblower program that allows an individual to confidentially report complaints or tips about a violation of law, regulation, or policy, as well as fraud, corruption, or operational weaknesses, for investigation and resolution.

### Guidance:

FCA Regulation [612.2137\(d\)\(7\)](#) requires the institution to provide for anonymous reporting by individuals of known or suspected violations of the institution's SOC program or Code of Ethics, such as through a hotline or similar venue. A whistleblower (WB) program, or a similar program by another name (e.g., Ethics, Standards of Conduct, Anonymous Reporting), provides ways to anonymously and confidentially report complaints or tips about a violation of law, regulation, or policy, as well as fraud, corruption, or operational weaknesses. Examples include lending fraud, ethical concerns, and financial reporting irregularities. A WB program is a key component of an effective internal control process as required by FCA Regulation [618.8430](#). FCA issued an Informational Memorandum on [Whistleblower Programs](#) dated July 9, 2015, to provide additional guidance and criteria in this area.

Evaluative questions and items to consider when examining WB programs include:

- **Program Structure and Confidentiality: Does the institution have a formalized WB program that provides for confidential and anonymous reporting from both inside and outside the institution?** A WB program should provide anonymous and confidential methods for internal and external sources to provide complaints or tips on suspicious activity as required by FCA Regulation [612.2137\(d\)\(7\)](#) for SOC and ethical complaints. This is typically, and most effectively, accomplished with a telephone hotline or other electronic means for directly communicating a complaint or tip to a third party.
  - WB programs should not be limited to employees. Industry best practices expand WB programs to include external parties, such as customers, loan applicants, appraisers, vendors, and others.
  - Using a third-party WB hotline provider is a key way to ensure confidentiality and anonymity, which should reduce the fear of retribution for making a report. The WB service provider should have experience in handling WB issues and provide a reasonable process for reporting complaints and tips to ensure anonymity. Refer to the *Third-Party Risk Management* procedure in the *Direction & Control of Operations* Examination Manual topic for information on examining an institution's outsourcing processes.
  - If the institution does not have an externally administered WB program, an alternative process must be in place to ensure confidential and effective WB reporting for SOC and Code of Ethics matters. While alternative solutions may prove to be effective, institutions should be strongly encouraged to contract this service with a third party. Examiners should discuss with the institution potential drawbacks related to confidentiality and effectiveness with an internally administered process. Example drawbacks may include potential conflicts of interest and reduced

reporting due to confidentiality concerns, fear of retribution, and an intimidation factor. Cost should not be a primary deterrent as third-party services are generally inexpensive.

- **Policy Guidance: Does the institution have adequate written WB policy guidance, including an anti-retaliation policy?** Institutions must have written WB policy guidance that clearly communicates board expectations to management and staff as required by FCA Regulation [612.2137\(d\)\(7\)](#). The policy should address key items such as internal and external access, investigation processes, routing and reporting expectations, and documentation expectations for WB complaints and investigations (including retention requirements). Policy guidance should also address anti-retaliation expectations to provide appropriate assurance that any person who submits a WB complaint or tip will not be subject to retaliation or retribution from the board of directors, institution management, or its employees. An effective policy will help the board hold management accountable for installing and properly administering the WB program.
- **Reporting, Investigating, and Resolving: Are processes sufficient to ensure complaints and tips are reported to the appropriate parties, investigated, and resolved?** Institutions should assign specific board, committee, and managerial positions with responsibility for following up on WB complaints and tips. Institutions should also consider the SOCO's role as outlined in FCA Regulation [612.2170\(d\)](#) for investigating complaints received against directors, employees, or agents of the institution regarding SOC or Code of Ethics matters. Well-defined processes should exist for screening, routing, and tracking complaints and tips, including an escalation structure that ensures a party named in the complaint is not sent a notification. This is important for managing potential conflicts of interest. Notices should be provided to the person(s) identified in the SOC and WB policies and procedures. Effective programs include a thorough screening process, secure tracking system, timely followup, proper investigation, adequate resolution, and final closure of the issue. Regular status updates on complaints and tips should be shared with those identified in SOC and WB policy and procedures, including notice if there were no items to report. Institutions should also have protocols to keep FCA informed of complaints and tips received and investigative efforts, and to file criminal referrals when necessary. Depending on the complaint or tip, the SOCO may need experts (e.g., human resource professionals, attorneys) to provide advice, provide input on scope, or even complete the full investigation under the oversight of the SOCO to ensure proper independence and confidentiality.
- **Education and Awareness: Is WB program information effectively disseminated to staff, the board, customers, and the public through training programs and other communications?** The board and management should promote the WB program and provide the necessary training and other communications to support it.
  - A formal training program should be in place for all employees and board members. As a sound business practice, training should be provided annually, and also as part of new employee and director orientation. Training should promote awareness of the WB program, provide information on reporting processes, and address what should be reported. Furthermore, training should emphasize confidentiality to ensure staff understands how the process works and protects anonymity. Board training should also ensure that directors fully understand their crucial role in establishing a healthy, ethical culture that supports the WB program. If the WB program is informal or not highly visible (e.g., through annual staff training, posters

in the break room, or other means), the culture may discourage staff from using the program.

- In addition to internal WB program awareness, institutions should take adequate actions to ensure customers and the public are aware of how to report complaints or tips. Information and links on the institution's website could be used in addition to including information in quarterly financial reports, newsletters, or other documents mailed to customers or vendors.
- **Testing and Audit Coverage: Are WB programs tested periodically and included in audit plans?** WB programs should be tested periodically to ensure the reporting and routing mechanisms are functioning as intended and are easy to use. For example, testing should ensure a party named in the complaint is not sent a notification. Furthermore, a busy phone line, a complicated set of menus, a break of confidentiality, or an unanswered email may cause the WB process to fail or be less effective. Additionally, WB programs must be included in the internal audit program's risk assessment process and audit plans as required by FCA Regulation [612.2137\(e\)](#). Audit coverage should address all aspects of the program to ensure controls are sufficient and processes are working as intended. This would include the reliability and responsiveness of a third-party hotline provider. If audit personnel are involved in administering the WB program, an independent evaluation should be completed. Refer to the *Audit* procedure for examining audit coverage.

### **3. Criminal Referral:**

Evaluate the adequacy of policies, procedures, and controls to ensure compliance with criminal referral regulations.

#### Guidance:

System institutions have the responsibility to detect and report known or suspected criminal activity involving their assets, operations, or affairs. FCA Regulations in [Part 612 Subpart B](#), promote consistency, efficiency, and timeliness in addressing known or suspected criminal activities. This helps to reduce potential losses, ensure the institution's safety and soundness, and ensure the public's confidence in the System. The regulations require institutions to notify law enforcement agencies of known or suspected criminal violations that meet certain criteria. For state and local crimes, institutions must notify the applicable state or local law enforcement authorities. When the crime relates to United States Code, reporting to the applicable law enforcement agencies and FCA must be completed using the FCA Criminal Referral Form. This must be completed within 30 days of determining that a known or suspected violation has occurred (even in certain situations where the suspect(s) is not known). Generally, institutions must report if there appears to be a reasonable basis to conclude that a criminal violation has been committed that meets the criteria outlined in the regulations. Examples include (but are not limited to) diversion of proceeds, filing of false financial statements, collateral conversions, money laundering, check fraud and kiting, computer intrusion, wire transfer fraud, mortgage and consumer loan fraud, embezzlement, misuse of position or self-dealing, and identity theft. An institution may not consider whether the activity is worthy of prosecution when determining the need to file. Once it is determined that a known or suspected criminal act has occurred meeting the reporting thresholds, a criminal referral must be filed. Refer to section [EM-1.5](#) in the Examination Manual for the FCA Criminal Referral Form filing instructions and a link to FCA's Criminal Referral System.

As required by FCA Regulation [612.2170\(d\)](#), the SOCO is responsible for investigating complaints alleging misconduct or possible criminal behavior by the institution, its directors, or its employees. Additionally, the SOCO serves as the reporting official for all cases investigated that involve possible violations of criminal statutes, those resulting in removal or discharge of an employee or director based on conduct issues, and those where there was an adverse impact to the institution's reputation. In this capacity, the SOCO must report to both the institution's board and the Farm Credit Administration's Office of General Counsel as required by FCA Regulation [612.2170\(d\)\(2\)](#). If a criminal referral is not filed when a reasonable person could question a situation, institutions are responsible for thoroughly documenting determinations not to file as evidence of completing their due diligence and making a good faith effort to comply with the regulatory requirements. Refer to FCA Bookletter [BL-073](#) for some of the most frequently asked questions about FCA's criminal referral regulations and filing requirements. It may also be beneficial for an institution making a criminal referral determination to consult with either its examiners or the FCA Office of General Counsel, as needed.

Evaluative questions and items to consider when examining criminal referral policies, procedures, and controls include:

- ***Policy and Procedures: Does the institution have effective criminal referral policies and procedures as required by FCA Regulation [612.2303](#)?*** Each institution must establish effective policies and procedures to ensure compliance with FCA Regulations on referral of known or suspected criminal violations, including, but not limited to, adequate internal controls. An effective policy will help the board hold management accountable for installing and properly administering the criminal referral reporting process and related controls. Policies and procedures should establish clear lines of authorities and responsibilities for appropriate discovery and reporting of any known or suspected criminal activities in accordance with FCA Regulations. This includes guidance on preparation, review, and approval of the FCA Criminal Referral Form and the related documentation that must be collected, organized, and retained in accordance with the FCA Criminal Referral Form instructions outlined in Examination Manual section [EM-1.5](#). In addition, guidance should address the SOC Official's role as outlined in FCA Regulation [612.2170\(d\)](#) for investigating and reporting possible violations of criminal statutes by insiders. FCA Bookletter [BL-073](#) (question 1) identifies several specific items that should be included in policies and procedures or addressed as part of the institution's internal control processes. Examiners should ensure that policies and procedures sufficiently address internal controls and are designed to ensure compliance with requirements in the following regulations:
  - FCA Regulation [612.2300](#) – Purpose and scope.
  - FCA Regulation [612.2301](#) – Referrals.
  - FCA Regulation [612.2302](#) – Notification of board of directors and bonding company.
- ***Training, Testing, and Audit: Has the institution conducted appropriate training, testing, and audits of criminal referral processes?*** The board and management should promote a culture that supports the criminal referral reporting processes, which includes providing the necessary training and other communications to staff. Training should be conducted annually for staff and the board. It should cover activities that require criminal referrals to be made, and the processes for preparing criminal referrals. Criminal referral processes should also be monitored and tested periodically to ensure the discovery and reporting mechanisms are functioning as intended. For example, management should test these processes by watching for and following up on indicators of suspect activities that may

warrant a criminal referral filing when reviewing internal audit or review reports, loan committee minutes, high risk asset reports, chargeoff lists, wire transfer activity, or other information. If an institution has not filed a criminal referral over an extended period of time, examiners should ensure these processes are occurring and working as intended. Additionally, criminal referral policies, procedures, and processes should be included in the internal audit program's risk assessment and audit plans. Audit coverage should assess all key aspects of the area to validate controls are sufficient and processes are working as intended. Refer to the *Audit* and *Transaction Testing* procedures for examining audit coverage and conducting transaction testing.

- **Other Internal Controls: Are other internal controls established by the board and management effective?** The board and management are responsible for sound controls to discover and report criminal activity. In addition to the controls already discussed in the evaluative questions above, other controls that can help to accomplish this effectively include strong management information systems, which can help to identify potential criminal activity, and having a designated person responsible for overseeing criminal referral processes. On a macro level, it is important for institutions to provide timely board reporting, establish strong overall risk management practices, ensure appropriate staffing, and provide sufficient management oversight with respect to suspicious activity monitoring and reporting.

#### 4. Audit:

Determine if the institution conducts an effective audit (scope, reporting, and followup) of standard of conduct, whistleblower, and criminal referral programs and processes.

##### Guidance:

The internal audit and review program is a key mechanism for ensuring effective standard of conduct, whistleblower, and criminal referral programs and processes and compliance with regulatory requirements. The internal auditor or other qualified, independent party should review the adequacy of processes to ensure compliance with applicable criteria. The audit risk assessment and scope should address direction and control of operations topics, and audit or review frequency should be commensurate with the complexity of the institution's operations and risk profile. A reliable audit program provides the board reasonable assurance that SOC, WB, and criminal referral programs and processes are sound and that reporting is complete and accurate.

Note: This procedure focuses on evaluating the reliability and effectiveness of internal audits and reviews in this topical area. Refer to the *Audit & Review Programs* topic in the Examination Manual for guidance on examining the overall internal audit and review program.

Evaluative questions and items to consider when examining the audit or review of SOC, WB, and criminal referral include:

- **Audit Coverage: Is there periodic audit or review coverage of SOC, WB, and criminal referral programs and processes?** Audit or review coverage and frequency should be appropriate relative to risks, changes in the operating environment, regulatory requirements, and periodic testing needs. Coverage should also be consistent with the institution's risk assessment results and annual audit plan. FCA Regulation [612.2137\(e\)\(3\)](#) requires internal audits over the SOC program.

- **Scope and Depth: Are audit or review scope and depth sufficient to conclude on the adequacy, completeness, and timeliness of SOC, WB, and criminal referral programs and processes?** The scope and depth of work, including transaction testing, should cover the primary processes and controls within the area being audited or reviewed and be sufficient to determine if internal controls are functioning as intended and regulatory requirements are met. The scope and depth of coverage should be documented and consistent with the approved audit or review plan and engagement contract (if applicable). FCA Regulation [612.2137\(e\)\(3\)](#) requires the board, with SOCO and other assistance (e.g., Chief Audit Executive (CAE)), to determine the scope and depth of SOC audits. Audit or review workpapers should be examined to verify the actual scope and depth of work performed. The workpapers may indicate the scope and depth deviated from what was identified (or implied) in the audit plan. For example, workpapers may indicate the work performed was limited to evaluating the existence of policies and procedures and didn't include reviewing other controls, such as training or reporting, or testing compliance with regulations or institution guidance. If the work deviated materially from the original planned scope, internal audit should notify the board (or Audit Committee, if so delegated) of the reasons for the change. FCA Regulation [612.2137\(e\)\(3\)](#) requires SOC audits to review the effectiveness of advancing core principles, identify weaknesses, recommend and report necessary corrective actions, and cover the entire SOC program, including unincorporated business entity activity. Additionally, other items that should also be considered in the audit or review scope include:

  - Policies and procedures for all SOC processes, including:
    - SOCO activities
    - WB programs
    - Criminal referral processes
  - Compliance with SOC, WB, and criminal referral related policies, procedures, FCA Regulations, and other FCA guidance.
  - Monitoring and control processes (e.g., reporting, management oversight, delegated authorities, separation of duties, staffing, management information systems).
  - Sufficient transaction testing for insider loans and criminal referrals to ensure established criteria are followed.
  - Fraud-related threats and vulnerabilities, as well as anti-fraud controls.
- **Reliability of Results: Did FCA identify any concerns with audit or review reliability?** It is important to understand the scope and depth of the audit or review being examined, as discussed above, when evaluating audit or review reliability. With this understanding, the following are key considerations when evaluating the reliability of audit or review results:

  - *FCA Testing* – Evaluate the reliability of internal audit or review work by comparing the results to FCA's examination results in this area. This comparison often includes FCA testing transactions that were covered in the internal audit or review (transactions are often loans or loan applications, but may include other types of transactional activity, as well). In addition to the audit or review report, examiners should request and review the workpapers and hold discussions with the auditor to obtain a more thorough understanding of work completed. This can be especially



important if the audit or review report is not sufficiently detailed or FCA's examination work and testing identifies potential concerns. Auditors and reviewers complete line sheets, flowcharts, control matrices, standard work programs, workpaper forms, or other relevant audit evidence when conducting and supporting their work. (IIA Standards 2240, 2300, 2310, and 2320) Workpapers should adequately document the work performed and support the final report. If FCA identifies weaknesses that were not identified in the audit or review, the cause for any discrepancy should be determined.

- *Audit/Review Staffing* – Whether internal or outsourced, auditors and reviewers conducting the work need to be qualified, independent, and objective to ensure reliable results. They should have the right mix of knowledge, skills, and other competencies needed to perform the work. (IIA Standard 2230) Additionally, auditors and reviewers need to be independent of the activities they audit so they can carry out their work freely and objectively. (IIA Standards 1100, 1112, 1120, and 1130) For example, audit and review staff should not be involved in developing and installing procedures, preparing records, operating a system of internal controls, or engaging in any other activity that they would normally review. Examiners should evaluate the staffing on the individual audit or review being examined as part of determining the reliability of results. (Note: FCA Regulation [612.2137\(e\)\(3\)](#) requires the board to identify who will conduct the SOC internal audit.)
- *Institution Review of Work Performed* – The institution should complete an independent review of the workpapers to ensure audit or review objectives and scope were met and the results and conclusions were reliable and supported. (IIA Standard 2340) Examples could include a supervisory review of in-house audit work by the CAE or other audit staff, or a review of outsourced work by the CAE or audit coordinator. Examiners should consider whether the institution completed these reviews, and if any concerns were identified, when concluding on audit or review reliability.
- **Reports: Does the internal audit or review report sufficiently communicate SOC, WB, and criminal referral review results and recommendations, if applicable?** Examiners should consider the following when evaluating the audit or review report:
  - Is the report prepared and communicated in accordance with the institution's guidelines? (Note: FCA Regulation [612.2137\(e\)\(3\)](#) requires the SOC audit findings to be given directly to the board or designated board committee.)
  - Is an executive summary or overview included to provide the board with a general conclusion on audit or review results?
  - Is the report accurate, concise, supported, and timely in communicating the audit or review objectives, scope, results, conclusions, and recommendations? (IIA Standards 2330, 2400, 2410, 2420, 2440, and 2450)
  - Are conclusions and recommendations realistic and reasonable, with material and higher risk issues clearly identified and prioritized?
  - Are conclusions and recommendations supported by convincing evidence and persuasive arguments (condition, criteria, cause, and effect)?

- Do results in the workpapers align with report conclusions?
- Does the report conclude whether the institution adheres to policies, procedures, and applicable laws or regulations, and whether operating processes and internal controls are effective?
- Does the report address potential vulnerabilities to fraud, if applicable?
- **Corrective Action: Are management responses to audit or review findings in this area reasonable, complete, and timely? Have corrective actions been effective?** Audits and reviews are only effective if corrective action is taken to remedy the weaknesses identified. As such, there should be a reasonable, complete, and timely management response to the audit or review report. Management commitments and agreements or any areas of disagreement should be documented in the report or in a separate memo or tracking system. (IIA Standards 2500 and 2600) If corrective actions are not resolving the issues or concerns in a timely manner, examiners should further investigate the reasons. For example, this could indicate the audit or review did not sufficiently identify the underlying causes or materiality of weaknesses, sufficient resources are not being directed toward corrective actions, or weaknesses exist in the institution's corrective action process, including board oversight of the process.

#### **5. Transaction Testing:**

Examine individual loans and other transactions to verify effectiveness of institution control processes, accuracy of disclosure statements, and compliance with SOC and criminal referral regulations.

##### Guidance:

Examiners should always be attentive to any transaction or activity that may represent an SOC concern or potential criminal activity. Besides conflict of interest situations, SOC concerns would include ensuring insiders (directors, employees, and agents) are not using their position, or information acquired in their position, to obtain favorable treatment or derive personal benefit. For example, when reviewing board minutes, examiners should ensure directors are following board policies and procedures for recusing themselves from decisions impacting their personal interests or the interests of parties related to them. Examiners should watch for indications of SOC concerns or criminal activity by any party involved in a transaction. While loan actions are the most common transaction to examine, other types of transactions to consider testing include, but are not limited to, related services, property sales, and institution personnel actions.

When identifying potential transactions specifically for criminal referral process testing, examiners should ask management about any potential criminal activity (by borrowers, insiders, or unknown parties) that has not been reported. This may reveal situations where the institution decided not to file a criminal referral. Whether the activity is worthy of prosecution is not a consideration when determining the need to file. Once it is determined that a known or suspected criminal act meeting the reporting thresholds has occurred, a criminal referral must be filed. As such, examiners should validate management's responses and follow up, as needed, through the transaction testing process. To assist in validating management's responses and identifying potential transactions to test, examiners should review chargeoff lists, high-risk asset reports, internal audit or review reports, loan

committee minutes, board materials, or other information for indicators of potential criminal activities.

When examining individual transactions to test SOC and criminal referral processes, including the accuracy of internal audit or review testing and related conclusions, consider the following:

- **Loans** – Watch for evidence of potential criminal activities on any loan examined to ensure compliance with criminal referral processes and requirements. Specifically, examiners should be alert for common types of potential criminal situations (e.g., collateral diversion that surfaces when loans are in collection, or misstatements that become evident on a borrower’s or applicant’s financial statements).
- **Insider Loans** – Cross-check loan file information against the director and employee disclosures to confirm that all relevant information was accurately disclosed in compliance with FCA Regulation [612.2145](#). Look at names on file documents (lease agreements, private promissory notes, receivables, payables, sales contracts, bill of sales, financial statements, etc.) to identify relationships or transactions that were not disclosed. In addition, look for signs of preferential treatment, such as in loan pricing or conditions, and ensure that loan approval requirements in FCA Regulations [614.4460](#) and [614.4470](#) are met. This should also include determining that recusals due to potential conflicts of interest are being carried out effectively. Insiders should not inappropriately influence or be involved in loans to themselves or their affiliated organizations and family members (e.g., involvement in the loan analysis, collateral evaluation, approval, or disbursement). Ensure appropriate SOC Official involvement, as needed.
- **Personnel Actions** – Review personnel actions (resignations, terminations, reprimands, etc.) for employees and directors to identify issues related to suspicion of wrong-doing, SOC violations, or criminal activity. Ensure appropriate SOC Official involvement and institution filing of criminal referrals, if warranted.
- **Criminal Referrals** – Review criminal referrals the institution has reported to test compliance with regulations and the institution’s criminal referral processes.
- **Sales of Acquired Properties** – Determine who purchased the property to ensure there are no director, employee, or agent conflicts of interest. Cross-check against director and employee disclosures and ensure appropriate SOC Official involvement, as needed. If it was an entity (limited liability company, corporation, partnership, etc.), look for entity or other documents that identify the individuals involved (officers, shareholders, partners, etc.).
- **Related Services** – Ensure that directors, employees, and agents are not receiving preferential treatment and there are no conflicts of interest. Cross-check against director and employee disclosures and ensure appropriate SOC Official involvement, as needed.