Effective Disclosure Management

14 Key Requirements

Refresher:
Conflicts of Interest

Conflict of Interest (COI): "Any personal business or professional activity that would create a conflict between personal interests and the interests of the employer."
- Institute for Supply Management

Common Conflicts of Interest

Gifts	A procurement manager accepts season tickets from a potential vendor.
	An elected official goes on a private vacation paid for by a CEO.
Personal Relationships	A supervisor is involved in a romantic relationship with a direct report.
	A manager sits on the hiring committee for a position his nephew is applying for.
Personal Investments	A manager is a major investor in a company he selects as a supplier.
	An auditor owns stock in the company he is auditing.
Outside Employment/ Competition	An employee performs consulting work for a competitor of her full-time employer.
	An employee forms a company that competes with his current employer.
Revolving Door	A company executive leaves his post for a government appointment related to his former industry.
	A regulatory official leaves public service and joins a private sector firm in the industry she regulated.

What is Disclosure Management?

Disclosure Management: The process of collecting, reviewing and maintaining relationship disclosure information, and responding to and monitoring potential conflicts of interest.

Why Disclosures?

"Sunlight is said to be the best of disinfectants; electric light the most efficient policeman." –U.S. Supreme Court Justice Louis Brandeis

An effective relationship disclosure program:

- Creates transparency within the organization
  - Allows organizational leaders to gain awareness of a potential conflict and appropriately monitor employee activity related to the conflict of interest (COI)
- Potentially hampers unethical behavior
- Can be a less burdensome and more feasible form of COI management than outright elimination or avoidance of all potential conflicts
  - Allows leaders to keep performing their duties (under scrutiny)
  - Allows individuals with industry knowledge and experience to share their expertise and leverage networks while avoiding COI risk

14 Key Requirements

1. Risk-Based Design
2. A Robust Disclosure Policy
3. Organization-Wide Coverage
4. Clear Communication
5. Ease of Disclosure
6. Intimidation-Free
7. Consistent Disclosure Review
8. Data Centralization and Integration
9. Flexible
10. Complexity-Capable
11. Confidentiality Protection
12. Ongoing Monitoring
13. Reporting-Ready
14. Periodic Program Review

Requirement 1
Risk-Based Design

An effective disclosure program is designed to mitigate organizational risks.

- Scan the industry, organizational structure and operations for areas where COIs create or enhance risk, such as:
  - Functional areas or offices especially vulnerable to conflicts (e.g., sales)
  - Business relationships or transactions that may breed conflicts
  - Industry practices that lend themselves to potential conflicts
  - Geographic-specific risks areas (e.g., countries where gift-giving is customary)
- Ensure that your COI program covers you against these risk exposures

Example: Identifying COI Risks
National Restaurant Chain

POTENTIAL RISK AREA		POTENTIAL CONFLICT OF INTEREST
Functional area vulnerable to conflicts of interest	Construction project management	Personal relationships between subcontractors and the construction project manager
Business relationships or transactions that may breed conflicts	Purchasing relationships	A supplier offers purchasing staff discount on personal purchases
Geographic area of operations vulnerable to conflicts of interest	Overseas expansion plans in countries where bribery is common practice for establishing business operations	Employees or agents of the company may give bribes to local government officials

Requirement 2
A Robust Disclosure Policy

A robust disclosure policy forms the foundation of your disclosure and COI management program.

While developing a disclosure policy, consider the following:

- How will the policy cover your risk areas?
- Who should disclosures be mandatory for? Board members? Executives? Employees in select departments? Contractors?
- Which situations warrant completion of a disclosure?
  - Personal financial investments greater than $15,000?
  - A relative in senior management with a company vendor?
  - A romantic relationship with a co-worker?
- How frequently should disclosures be updated or confirmed?
- What, if any, penalties will be enforced for failure to disclose potential conflicts?

Requirement 3 **Organization-Wide Coverage**

Only 48% of compliance executives surveyed say their company provides contractors with a copy of the organization's code of conduct, and only 39% require contractors to sign anti-corruption agreements.*

To be successful, a disclosure program must cover the entire organization.

- All parties involved in business operations should be subject to your COI policy, directly or indirectly:
  - Require joint venture partners, distributors, agents, suppliers and other contractors to attest to a code of conduct
- In evaluating potential vendors, look at their COI and ethics policies and their track record in these areas

*Deloitte & Touche LLP and Compliance Week, "In Focus: Compliance Trends Survey 2014," http://deloitte.wsj.com/cfo/files/2014/07/Compliance_Week_Compliance_Survey_2014.pdf

Requirement 4
Clear Communication

To facilitate organization-wide understanding and adherence to your COI policy, successful communication and training is vital.

- All employees and contractors—new and old—should receive training on your disclosure policies
- Provide additional, in-person training to managers, senior leaders and board members
  - They should know your policies and procedures backwards and forwards and be ready to handle COI misconduct reports
- Post your policy online and make it easily accessible in other formats
- If your company operates globally, provide your COI policy, training and disclosure form to employees in their local language
- Build a year-long communication plan to reinforce your commitment to ethical conduct
- Maintain tone at the top and middle—senior leaders and front-line managers must walk the walk and talk the talk of ethical behavior

Requirement 5
Ease of Disclosure

Disclosure should be a painless process.

- Disclosure forms should be:
  - Easily accessible through an employee portal or other central system that employees can access independently
  - Easy to complete and update at any time
  - Submitted and maintained electronically for record-keeping efficiency
- To help employees and managers navigate the COI world, establish a compliance contact or advisory body to answer employee inquiries and provide guidance on relationships and COIs

Checklist: Painless Disclosure Process

Does your disclosure program…

- ✓ Allow employees to add, update or cancel active relationship disclosures in your system?
- ✓ Allow authorized compliance staff and managers to submit proxy disclosures for employees?
- ✓ Enable employees to report potential conflicts immediately after new-hire/annual policy attestation and training?
- ✓ Ask employees to confirm or edit disclosures on file each year?

Requirement 6
Intimidation-Free

Hotlines and other reporting channels are often associated with wrongdoing. By asking employees to submit relationship disclosures through your hotline, you may inadvertently discourage employees from candidly disclosing all potential conflicts.

To encourage open, transparent communication of relationships, offer a disclosure channel that's independent of other reporting channels.

Offering an independent disclosure reporting channel will:

- Take the intimidation out of the relationship disclosure process
- Ensure that your disclosure process does not put employees on the defensive
- Enable proactive management of COIs

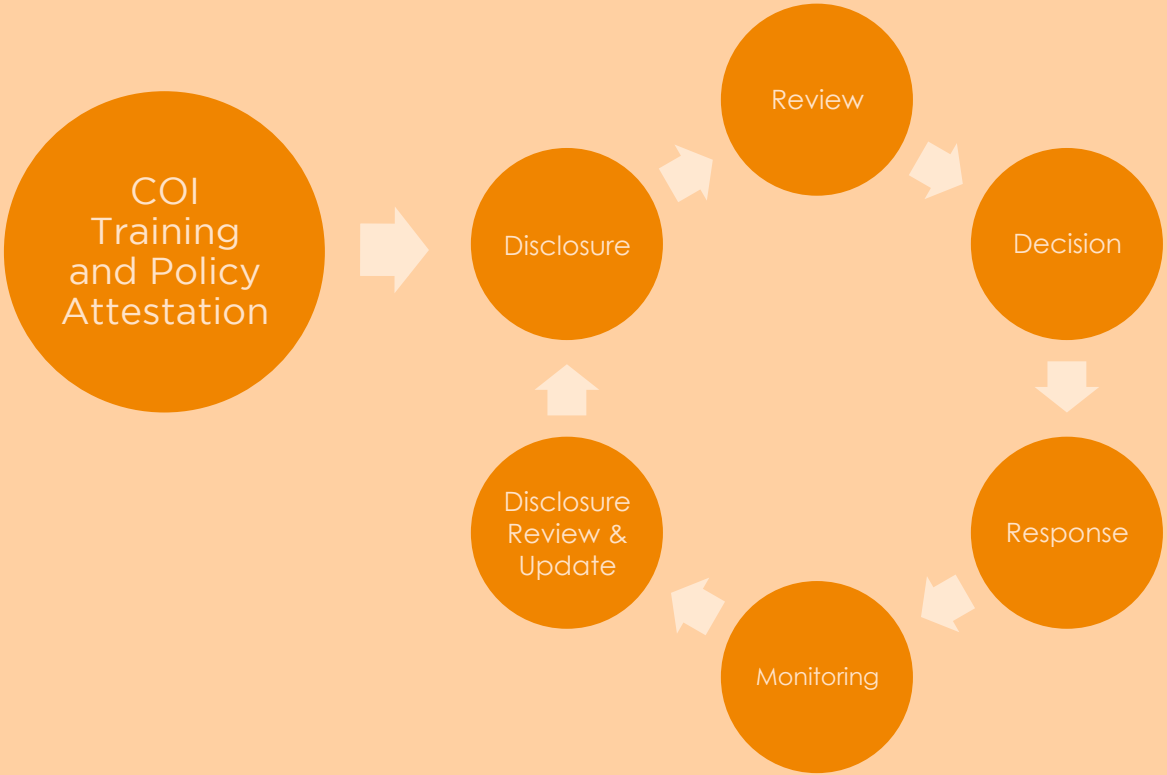
By connecting your compliance program initiatives and information behind the scenes, through a central platform, you can still associate relationships with these initiatives and program data, while ensuring you have the most complete and accurate understanding of COI risk.

Requirement 7
Consistent Disclosure Review

The organization must develop a standard procedure for reviewing disclosures and issuing decisions.

- Form a committee or designate a compliance professional to review disclosures
- After reviewing disclosures, determine the organization's response:
  - Accept and monitor the COI risk
  - Eliminate the risk through conditional approval or operational adjustments
  - Determine the potential COI is not a significant concern
- Within the review procedure, outline a process for re-reviewing disclosures as employees change roles and responsibilities or as business operations change (e.g., business is pursued in new geographic regions)

Disclosure Management Process



Requirement 8
Data Centralization and Integration

For best efficiency, maintain all disclosures and related COI documentation on one central platform, integrated with other compliance program initiatives.

- Maintain historical records of disclosure policy training and attestation
  - Your organization may need to prove an employee received and attested to your policy
- Leverage technology to manage disclosures electronically
  - Maintain employee disclosure information, review decisions and records of organizational response
  - Attach notes and relevant documentation
- Connect your disclosure management program with other risk and compliance program initiatives
  - Tie COI disclosures to identified organizational risk areas to better monitor and flag disclosures of concern
  - Link employee disclosure information to policies, hotline and incidents to measure the effectiveness of your initiatives
  - Link disclosures to relevant HR data for further insight

Compliance Program Integration in Action

Jim, a purchasing manager at ABC Company, completes his annual COI training and policy attestation. He does not disclose that his brother is a major investor in a new office supply company competing for a contract with ABC.

Jim reviews the new firm's bid to provide office supplies for ABC and approves a contract with them.

A purchasing agent in Jim's department learns of Jim's conflict of interest and reports it through the company hotline.

The hotline manager logs the report in ABC's compliance management system and routes it to the appropriate party for investigation.

The investigating staff receives the report and enters ABC's compliance management dashboard. In seconds, he is able to see that:

- Jim has completed COI training and attested to ABC's COI policy three times;
- Jim has not filed any disclosures; and
- Jim was investigated last year for a separate code of conduct violation.

Requirement 9
Flexible

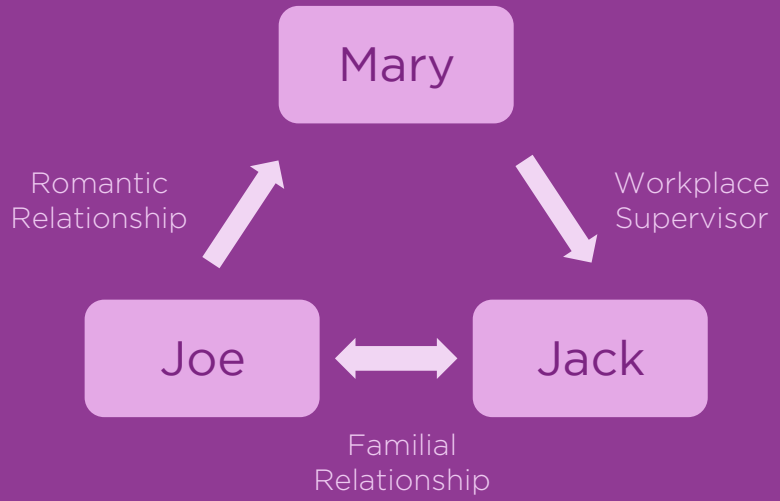
As business operations, employee roles and personal relationships evolve, disclosures need to be updated or reevaluated. Your disclosure management system must be agile enough to handle updates without missing a beat.

A flexible disclosure management program:

- Enables quick, easy disclosure updates by the employee at any time
- Allows authorized administrators to create and update disclosure decisions in the system (i.e., approval, disapproval or conditional approval)
- Allows information to be organized and practically to ensure security and confidentiality of disclosures

Requirement 10 **Complexity-Capable**

Relationships are complicated. Indirect relationships that involve multiple parties are more difficult to understand—and the risks they present more challenging to anticipate and manage. Your disclosure management system should be capable of tracking complex, multi-party relationships.



Potential COIs can breed real or perceived favoritism

Requirement 11
Confidential

Because disclosures may contain sensitive personal information, this information provided in disclosures must be protected.

At a minimum, adopt these data protection practices:

- Electronic disclosure information should be maintained in a secure, password-protected system with restricted user access
- Authorized users must agree to maintain employee confidentiality and uphold the organization's data security standards
- Any hard copies retained should be kept in secure storage, only accessible by authorized personnel

Requirement 12
Ongoing Monitoring

Disclose it and forget it? Not quite.

Effective disclosure management requires continuous monitoring. This means:

- Tracking relationship disclosures flagged as posing a high COI risk
- Reviewing disclosures for heightened risk concerns as business operations or employee roles/responsibilities change
- Monitoring hotline and management reports for hot spots and emerging risks
- Staying on top of risk profile changes and their connection to conflicts of interest

Requirement 13
Reporting-Ready

18% of compliance executives surveyed are not confident their organizations' IT systems collect and report the compliance data needed to evaluate compliance program effectiveness.*

Pulling together data for annual compliance program reports can be a time-consuming, difficult process if your disclosure and compliance management system is not set up to be reporting-ready.

- Implementing a platform capable of automating your data reporting will improve reporting efficiency by leaps and bounds, enable a more proactive approach to risk management and facilitate more effective program oversight by senior leaders.

*Deloitte & Touche LLP and Compliance Week, "In Focus: Compliance Trends Survey 2014," http://deloitte.wsj.com/cfo/files/2014/07/Compliance_Week_Compliance_Survey_2014.pdf

Quarterly Reporting

- Risk areas:
  Bangalore and Beijing, where zero disclosures are on file
- As policy acknowledgements increase, incidents trend downward

COI and Disclosure Management Program Sample Report

Requirement 14
Periodic Program Review

For continuous improvement, review your disclosure program annually or as conditions warrant.

- Review all program initiatives:
  - Policy
  - Procedures for:
    - Accepting and reviewing disclosures
    - Issuing decisions to approve or disapprove of conflicts
    - Recording decisions
    - Updating disclosure records and attaching notes and documentation
  - Training effectiveness
  - Data maintenance and monitoring
  - Gaps evident from hotline reports, manager reports and investigations

About Convercent

Convercent's risk-based global compliance solution enables the design, implementation and measurement of an effective compliance program. Delivering an intuitive user experience with actionable executive reporting, Convercent integrates the management of corporate compliance risks, cases, disclosures, training and policies. With hundreds of customers in more than 130 countries—including Philip Morris International, CH2M Hill and Under Armour—Convercent's award-winning GRC solution safeguards the financial and reputational health of your company. Backed by Azure Capital, Sapphire Ventures (formerly SAP Ventures), Mantucket Capital and Rho Capital Partners, and based in Denver, Colorado, Convercent will revolutionize your company's compliance program.

www.convercent.com.