COSMOS
Navigate the Compliance Universe

The Complete Compliance and Ethics Manual 2024
Appendix 3-A: Compliance Program Implementation Checklist

Actions	Responsible Party	Best Practice	Completion Date
Appointment of Compliance Officer and Committee			
Select and appoint a chief compliance officer (CCO)	CEO/governing board	High-level authority; position of power equivalent to business functions; "independent"/does not report to chief financial officer or general counsel	
Select and appoint compliance committee(s) (CC): • Create CC charter to include scope of CC responsibilities, compliance officer, and board of directors • Provide compliance and risk area training, including the three lines of defense model, to the compliance committee members • Identify specific compliance subtopics for implementation • Create subcommittees or task forces • Assign each task force to a specific compliance subtopic	CEO/governing board/CCO	Ideally lead by CEO/CCO. Should include representative of all key business functions, including finance, human resources, audit, risk management, legal, and data security	
Ensure CC meets on a regular basis after implementation • Ensure CC minutes are created and retained for each meeting	CCO	Should meet no less than quarterly	

Compliance Risk Assessment (once CC is in place)			
Conduct a compliance risk assessment and prioritize findings: • Identify industry-specific risk areas • Identify all relevant laws, regulations, and government or regulatory body guidance • Identify areas of previous compliance issues within the organization • Agree upon risk definitions • Determine metrics to be used (e.g., impact, severity, frequency, effectiveness of controls, gross risk v. net risk) • Determine methodology to be used (questionnaire, interviews, both) • Identify subject matter experts and risk owners in the first line of defense to participate in assessment • Conduct assessment phase using methodology selected • Collect and tabulate results of assessment to identify top risks/emerging risks/well-controlled risks • Create a risk matrix • Share risk matrix with members of senior management and board of directors and obtain feedback • Develop risk management/mitigation plans for all top risks and assign responsibility for each plan • Track progress of implementation of risk mitigation/management plans and document	CC	Initial risk assessment should be conducted as soon as feasible as the CC's first order of business	

Developing Code of Conduct, Policies and Procedures			
Create and distribute code of conduct: • Draft compliance code of conduct • Obtain approval of code of conduct • Adoption of code of conduct by CC/board of directors • Translation of code into all company languages • Distribute code electronically with communication campaign and explain to all employees the key points of the code and how to access/find it • Provide training on content of the code to all employees • Provide employees without computer access with access to printed copy upon request • Obtain signed acknowledgement of code of conduct from all employees	CC/CCO	CCO and their team often take the lead in initial code drafting and reviews with the CC Source of the code should be the organizational values adopted by the company, aligned closely with the organization's mission statement Code is written in affirmative voice (e.g., "we behave this way") as opposed to a prohibitive voice (e.g., "you may not"). It must be easily understood, without legalese. Attestation to be obtained no less than annually	

Draft structural policies and procedures: • Mission/goals/directives of compliance program • Policy/procedure for creation and approval of new policies • Conflicts-of-interest disclosure policy and procedure • Compliance education policy • Testing of compliance education retention • Anonymous reporting mechanism • Investigative policy, including mechanism for feedback to reporters/protection of confidentiality where possible • Open-door/speak-up policy • Nonretaliation policy • Anti-bribery/anti-corruption policy • Gift policy (both giving and receiving) • Nondiscrimination/workplace respect policy • Auditing and monitoring of compliance program policy • Auditing work plan/procedure • Auditor independence • Conducting background checks • Disciplinary action guidelines • Enforcement of disciplinary action ◦ Regulatory response plan/policy (i.e., responding to dawn raids, search warrants, visits, subpoenas, and document requests from regulators)	CC/CCO	CCO and their team often take the lead in initial drafting of policies and procedures for review and approval by CC	

Draft substantive policies and procedures: • Complete risk assessment (described earlier) • Draft specific substantive policies and procedures that address identified risk areas	Risk owners with guidance from CCO and CC	Risk owners should follow the guidelines included in the "policy on policies" and use the approved policy template to draft appropriate policies to address/mitigate risks they own	
Obtain approval of policies and procedures from CC	Risk owners and CCO	Risk owners to follow prescribed policy approval procedure	
Obtain approval of policies and procedures from executive committee where needed	Risk owners, CC, and CCO		
Obtain approval of policies and procedures from board of directors where needed	CCO and CC		
Distribute policies and procedures, ensure accessibility in a policy/procedure library, and provide training and tools to all affected employees	CCO	CCO and their team to work with IT and internal communications teams to ensure availability of all policies and procedures to employees as well as with the training and development team to develop and deliver appropriate employee training	
Obtain signed certification of receipt and understanding of policies and procedures and initial conflicts of interest disclosures from all affected employees	CCO	CCO and their team to work with IT and HR to ensure attestation/certification/disclosure	

Annual review of compliance policies, processes, and procedures: • Review all compliance-related policies, processes, and procedures for applicability and accuracy and to ensure consistency • Validate policy ownership has not changed • Update policies, processes, and procedures as needed • Create new policies, processes, and procedures for new risk areas identified • Obtain required approvals for revised policies, processes, and procedures • Document proof of review for all nonrevised policies, processes, and procedures • Track review and revision dates for each • Distribute any revised policies, processes, and procedures to all appropriate employees/contractors • Obtain signed certification of receipt and understanding for all applicable revised policies, processes, and procedures	CCO	CCO and their team typically handle this annual review and revalidation	

Review policies, processes, and procedures owned by functions other than compliance: • Prepare a policy, process, and procedure request memo (upon creation/implementation of the compliance program and annually thereafter) • Designate a task force or delegate review of specific policies, processes, and procedures to various task forces to recommend any revisions to each • Provide recommendations to the departments with a timeline for each one to submit its revisions or a written explanation of why it believes the policy, process, or procedure should not be revised • Documentation of each revision and each policy, process, and procedure that does not require revision	CCO/CC	Memo should request copies of all operational, financial, or other compliance-related department-specific policies, processes, and procedures from all departments	
Creation of Reporting Channels/Systems			

Determine reporting channels to be offered: • Ensure channels are available in all company languages • Ensure at least one channel allows for reporting of issues outside of chain of command • Ensure at least one channel allows for confidentiality of reporting • Allow for different methods of reporting (telephonic, online, in writing, verbal, face-to-face) to accommodate varying levels of reporter access and skill • How will reports from all reporting channels be captured and input into one issue management system for tracking/resolution?	CC/CCO	Multiple internal reporting channels should be offered, including direct reporting to manager, HR, Compliance, or Legal, as well as an option to report confidentially to helpline (either over-the-phone or web-based)	
Develop issue management process/system to track the handling of all incoming reports: • Choose a third party to host outside helpline • Choose issue management tool/system to be used and configure/customize system for your organization • Determine issue types to be tracked • Determine issue metrics to be tracked, including issue volume; time to close for investigations; materiality metrics; regional, geographic, or business unit metrics; or subject matter metrics • Determine staffing for tracking and investigation of issues • Consider creation of an investigations committee (IC) comprising control function representatives to oversee handling of issue reports and	CC/CCO	Users may fear retaliation/identification unless external third party–hosted option is provided If no dedicated investigator staff is available, consider training existing members of other control functions to serve as investigations, such as Audit, HR, Legal, and Compliance Be aware of the potential for conflicts of interest between investigators and subjects and require an objectivity certification from each investigator Some issues will have the potential to cause loss of life and/or severe injury or material financial loss; you will need an escalation protocol for immediate notice to senior management Materiality criteria may include level of implicated person, potential financial loss, issue type, and more Ensure data privacy concerns are properly accounted for before initiating electronic searches of any kind Investigation reports should be reviewed prior to case closure to ensure they are well documented, thorough, and complete	

investigations • Create list of persons qualified to act as investigators • Develop investigations training for persons chosen to serve as investigators • Conduct training for all investigators • Create objectivity certification for all investigators • Determine issue reporting metrics to be tracked and format for reporting • Create standard forms including standard issue report, investigation report, root cause analysis, mitigation plan, and resolution report • Develop escalation protocol for emergency situations where loss of life or serious injury are reported • Develop materiality criteria and escalation protocol for material matters that should be immediately brought to the attention of the CC and/or the board of directors • Develop a mechanism for providing feedback to anonymous reporters regarding progress of issue investigation and ultimate resolution • Develop process to obtain approval for retrieval of electronic data from information systems including laptops and cell phones in conjunction with IT and Legal • Develop case closure process to ensure all investigations are well documented and complete.			

Ensure employees know and understand the consequences of noncompliance: • Develop clear disciplinary guidelines for compliance violations and failures • Communicate disciplinary guidelines to all employees and make them available for review on demand • Ensure the fact finder in investigation is separate and apart from the disciplinary decision-maker • Consider creation of multi-function disciplinary committee to ensure consistent application of discipline across the organization and unbiased administration of the disciplinary guidelines • Develop audit plan to ensure consistency of disciplinary action for similar violations across the organization to avoid discriminatory application of guidelines	CC/HR	Levels of discipline will likely vary depending on severity and materiality Discipline options should be agreed upon with HR and may include verbal reprimand, written warning, written reprimand, suspension, and termination	

Develop communication campaign to announce and educate constituents on availability of and expectations related to reporting channels and on investigations process: • Ensure communications are available in all company languages • Emphasize retaliation prohibition • Educate all managers on how to handle reports received from employees and open-door practices and whom they should escalate to in order to ensure issue is added to tracking system • Educate all control functions on how to handle incoming reports and how to ensure issues are entered into the chosen issue-tracking system (develop standard operating procedures and work instructions) • Educate CC and board of directors on reporting channels and emphasize that more reporting is better	CC/CCO with Internal Communications	Encourage reporting from both employees and third parties Make sure all issues are captured and tracked in one issue-tracking system Management and the board may believe fewer reports means fewer problems. Educate them that "silence is not golden" when it comes to reporting channels, and that silence is an indicator of culture problems, hiding of issues, and a fear of retaliation.	
Launch reporting channels	CC/CCO	Monitor launch carefully to ensure systems are working correctly. Consider testing external phone numbers and web reporting systems from different company locations and countries to ensure functionality.	
Investigation of Reported Issues			

Investigate all reported issues in a timely manner: • Ask investigator to create a written investigations plan • Best practice is having investigator have someone take notes for them during all interviews • Interview reporter • Interview personnel identified in investigations plan • Determine whether data collection from computer systems is warranted/required/allowed and gather if appropriate • Conduct site visits and walk-throughs as specified in the investigations plan • Review policies, processes, procedures, laws, regulations, and guidance identified in investigations plan • Obtain legal opinions where needed	IC/CCO	If matter is material, consider whether investigation should be run under attorney–client privilege and whether there is the potential of a conflict of interest between the reporter and the organization. If so, provide Upjohn warning.	
Create investigation case file and report: • Ensure careful documentation of every portion of the investigation • Interview notes should be created for each interview • Facts and supporting documents should be carefully summarized		Documentation should include interview notes, all documents, and applicable policies and regulations that were reviewed as part of the investigation This is a fact-finding stage only	

Determine findings of the investigation: • Do the facts collected indicate the allegation has been substantiated, partially substantiated, not substantiated, is not a compliance issue, or that reporter has not provided enough information to investigate? • If issue is substantiated in whole or in part, determine root cause and develop corrective action plan (see below) and provide details of same in final investigation report • If issue is substantiated in whole or in part, provide facts to disciplinary committee for determination of whether discipline is appropriate and creation of disciplinary action plan • If discipline is administered, ensure case closure process is completed, including description of disciplinary measures taken in the final report • If issue is not a compliance issue, refer to appropriate function for review • If reporter has not supplied sufficient information, make a request for same • If issue is not substantiated, ensure case closure process is completed	IC	Not all cases will involve misconduct. Some will involve misunderstanding or lack of information or an unclear policy or procedure. In some cases, employee discipline is not necessary but employee training may be.	

Develop a corrective action plan:
• Conduct root cause analysis to determine factors that caused the issue
• Create time-bound corrective action plan to ensure:
  ◦ Creation or revision of policies and procedures to ensure misconduct is not repeated
  ◦ Creation or revision of forms that may have contributed to the issue
  ◦ Training is provided to involved employees as needed
  ◦ Revision of flow charts or entire processes are made as needed
• Assign responsibility for implementation and completion of corrective action plan
• Implement the corrective action plan and ensure timely completion
• Regularly audit and monitor processes affected to ensure future compliance
	IC/CC		

Training and Education			
Build initial compliance training program. Use results of compliance risk assessment to: • Identify employees for whom initial compliance education will be required • Identify employees for whom specific subject matter compliance education will be required • Identify vendors, contractors, and	CCO/CC	Consider a combination of in-person, online, facilitator-lead, and self-study approaches Consider use of written materials, posters, facilitator guides, articles in company publications or on company intranet, blog posts, PowerPoint presentations, emails, podcasts, videos, and communication campaigns Candidates to conduct training: compliance officer/compliance staff, HR partners, Legal, outside	

customers for whom compliance education is desired • Identify other stakeholders or other entities for which compliance education is desired • Determine content and duration of compliance education courses for each audience • Determine frequency of training required for each audience • Determine most appropriate mode of training for each audience • Determine most appropriate persons to conduct training • Develop training materials and translate into all company languages • Determine mechanism for tracking who has and has not completed required education courses • Will you create a penalty for failure to timely complete courses? • Determine responsibility for follow-up and tracking of persons who have failed to complete courses • Determine mechanism for obtaining participant feedback on the course • Determine how to measure effectiveness of training. Will there be a "before and after" knowledge check? A quiz they must pass in order to complete the course? A knowledge retention measure days/weeks after course completion? • Document training and education plan as well as a schedule developed through above activities		consultants Content can be developed internally by compliance staff, purchased from a vendor and used as is, purchased externally but customized, prepared by consultants, created by internal communications/education or subject matter expert teams, or made through a combination of approaches Consider a penalty for failure to timely complete courses. Provide managers with list of their employees who have failed to timely complete. Consider having manager contact tardy participants directly to request completion. Consider written reprimand/warning for failure to complete. Consider cutting off systems access as a consequence of failure.	

Conduct initial compliance education campaign: • Track completion data • Track effectiveness metrics • Report data and metrics to CC and associated risk owners • Collect course evaluations and synthesize feedback to create action items to improve next education campaign	CCO/CC	Data and metrics should be reported to the CC and, where appropriate, to the senior leadership team and/or board of directors Target course completion rate should be 100%, excepting those on approved leaves of absence	
Ongoing education program development and enhancement: • Track who has and has not been offered education courses • Identify audiences to be targeted for future compliance education efforts • Identify alternative education methods for those without systems access or in remote locations • Develop additional content for such audiences and translate into local languages as needed • Implement alternative training/education methods and track completion and effectiveness metrics	CCO/CC	Once initial education program has been completed, look to enhance and grow the program using a risk-based approach Consider in-person education sessions combined with compliance town halls to ensure nonremote employees have personal access to compliance officer and staff Consider conducting climate and culture surveys as part of in-person visits	

Train managers to discuss compliance during their staff meetings: • Provide them with discussion guides and "train the trainer" materials • Provide a case study of a compliance failure in your industry • Provide a case study of a compliance failure at our company and how it was handled • Provide managers with issue metrics from their areas to educate their employees on potential compliance vulnerabilities • Provide managers with risk assessment results to educate their teams about compliance risks in their areas	CCO/CC	Compliance training shouldn't only come from compliance and is often more meaningful when coming directly from an employee's supervisor and team Managers can feel ill equipped to discuss compliance and like they don't have the expertise needed to do so. Give them the tools and make it easy to include compliance topics in their team meetings.	
Continuing education/compliance expertise: • CO and CC members regularly attend high-level continuing education and compliance conferences/seminars • Subscribe to compliance journals/newsletters/blogs • Join compliance-related organizations • Subscribe to government and other mailing lists	CCO/CC	Continuing education is vital to ensure compliance leadership has most current information on regulations and enforcement actions that may change the organization's risk profile	
Auditing			
Complete risk assessment (described earlier)	CC/CCO		

Draft audit plans for each risk area identified: • Determine the objectives of the audit • Determine the appropriate sample selection method for each audit • Determine which policies, processes, and procedures will be audited • Determine the audit criteria ◦ Determine if legal counsel should be involved in the audit process	Internal Audit (IA)/CC	IA should ensure the controls and mitigation strategies designed for each identified risk have been appropriately implemented and are working in practice	
Develop an audit schedule using a risk-based prioritization	IA	Frequency of each audit, how many audits at once, expected duration of each audit should be set as part of the schedule	
Determine the appropriate party to conduct each audit	IA/CC	Internal audit, outside consultant, legal counsel, CC representative, CCO Take care that no function is auditing itself. The function that owns a risk cannot also audit its mitigation of same.	
Certify the independence/objectivity of the auditor	IA/CC	Consider having auditor self-certify to objectivity and absence of any conflict actual or perceived Be aware of potential to corrupt an audit if auditor is not completely independent	
Conduct the audit	IA	Audit should not be scheduled until an appropriate amount of time has passed after implementation of controls/mitigation measures following the risk assessment. Functions need time to implement and maintain controls prior to being audited on same. Suggested cadence is no sooner than six months following control/mitigation implementation.	

Determine the appropriate corrective action plan for any problems identified	IA/CC	Ensure plan is time-bound, documented in writing, approved by CC, and ensure specific action plan owner is assigned responsibility for implementation of corrections	
Prepare a written audit report	IA	Written report should be completed as soon as is reasonable. Recommended cadence is no more than 10 business days following audit completion.	
Determine whether legal counsel should be involved in the audit resolution based on findings	IA/CC	Be aware of potential need for attorney–client privilege protection prior to issuance and need for limited distribution depending on results of audit	
Ongoing Compliance Monitoring			
Develop compliance and culture surveys for specific audiences: • Determine what you want to know from whom • Choose your audiences based on risk • Choose your inquiries based on risk • Involve members of local management to ensure local sponsorship and buy-in	CC/CCO	Employees, customers, suppliers, dealers/distributors, board of directors	
Survey employees, customers, and other constituencies on compliance issues: • Ensure local language is used • Consider holding in-person roundtables regarding compliance • Provide written surveys • Consider allowing anonymous responses	CC/CCO	Ask whether they are aware of policies, processes, and procedures and whether they know where to go for assistance. Consider asking whether they are aware of potential violations and whether they have witnessed any failures to enforce policies, processes, or procedures.	

Review business processes: • Develop flow charts for specific processes • Consider having user experience tested and reported back to you • Identify potential compliance weaknesses in processes • Identify areas that lack sufficient checks and balances • Look for separation of duties and approvals • Add potential problem areas identified to audit plan/schedule • Revise processes as needed • Update process flow charts with corrected process • Educate affected employees on changes	CCO/Risk owners	Ensure risk owners are involved in process review and aware of the need for potential revisions	
Forms review: • Request forms used by each department for review to determine whether any create a potential compliance problem • Review the forms • Provide recommendations for revisions and improvements to forms, as needed ◦ Review the revised forms on a regular cadence		Examples include billing worksheets, dunning cycle statements, expense tracking forms, gift approval forms, time and effort tracking forms	
Effective Compliance Communications			

Publicize compliance metrics throughout the organization: • Consider annual reporting of issue metrics including volume, issue type, geography, and outcome • Consider issuance of regular "Help Me Understand" publications with clear explanations of specific compliance policies, topics, or risks • Consider a compliance department or officer blog with regular updates about the things the compliance team is working on • Work with your internal communications team to develop compliance-related content for internal company publications and the intranet	CCO/CC	Ensuring transparency of compliance program operations adds to a culture of organizational justice and builds trust	
Maintain open lines of communication: • Advocate for open-door/speak-up policy adoption • Give people managers a tool kit and educate them on how to behave in ways that encourage open communication on their teams • Educate people managers on the importance of diversity of opinion and the concept of psychological safety and their close connection to a culture of compliance	CCO/CC		

Ensure that processes are in place to protect employees from retaliation: • Adopt retaliation prohibition policy • Create retaliation audit program to review employment terminations/job eliminations against issue reporters • Create retaliation audit program to review performance appraisal data against all issue reports to detect any signs of retaliatory review • Consider making all allegations of retaliation automatically material under your issue escalation criteria	CCO/CC		