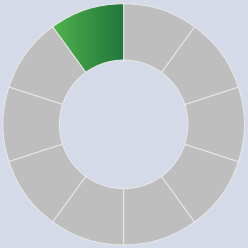
DEFENSE INDUSTRY INITIATIVE
DII
ON BUSINESS ETHICS AND CONDUCT

Small Business Toolkit

RESOURCE 6: SELF-AUDITING YOUR ETHICS AND COMPLIANCE PROGRAM

Purpose: The purpose of a self-audit is to assess whether an Ethics and Compliance Program is effective. This audit procedure examines the effectiveness of an ethics and compliance program against the ten steps noted below. You can use these procedures for the nine-step process or for only those steps that you have implemented in your company.



1. Leadership Commitment

Overview: *The visible commitment of your company's leadership at all levels is imperative to the success of your program. Leaders set the tone and culture of an organization, including its attitude about ethics. It is imperative that employees see that leaders are committed to the highest ethical standards. It is important for a leader to understand how his or her company's ethics program works, and how his or her role as a leader fits into the program and contributes to building and maintaining an ethical culture.*

Leadership includes not just the senior executives but also those at middle management. Employee perceptions about the company's commitment to ethics and the company's commitment to non-retaliation for reporting a concern are greatly influenced by the behavior of middle management.

Here are some steps you can perform to assess the level of leadership commitment in your company:

a. Ensure that the following organizational structure and activities exist to demonstrate leadership commitment:

1. Does the leader of the Ethics organization report directly into the Board of Directors or Chief Executive Officer? If that is not possible, does the leader have direct access to the Board or CEO to ensure issues can be properly escalated, if needed?
2. Is there a formal statement signed by the CEO to formalize your company's commitment to the highest ethical conduct in all aspects of your business?
3. Is there an Ethics and Compliance Committee that can provide leadership and oversight to the ethics program and review status of ethics-program-related activities?
4. Does the leadership of the Ethics and Compliance Committee reflect leadership commitment by having a senior executive as Chairman of that Committee? (The committee can consist of senior leaders from the Law Department, Human Resources, Internal Audit, Business Management, Operations, Communications, Security, Information Technology, and any other organization with which you may partner.)
5. Does the company's compensation and bonus structure include criteria tied to ethics and compliance performance, and does the company have clawback provisions for compensation paid to individuals who engage in misconduct?

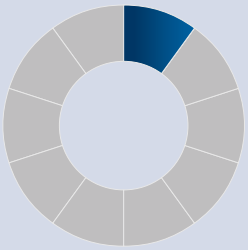
b. Select a random sample of your middle managers (e.g., department manager, site manager, district manager, area manager, regional manager) and ask about their role in implementing the Company's commitment to the highest ethical standards in all aspects of their responsibilities. They should say all or most of the following:

- Lead by example.
- Ensure that employees understand the company's ethics standards.
- Create a culture that encourages employees to comply with company policies and voice questions and concerns.
- Respond appropriately and immediately to concerns that are raised.
- Ensure that employees receive a copy of the Code of Conduct.

- Ensure that employees complete required training and certifications as required.
- Be cognizant of ethics exposures and take appropriate mitigating actions.

If the middle managers are not responding as noted above, that could indicate the message of ethical behavior has not flowed down to the middle-level managers who actually manage the company's business on a day-to-day basis. Therefore, you should recommend corrective actions such as additional training, communication, and coaching.

Prepare an opinion about leadership commitment based on the results of the above steps.



2. Company Values / Code of Conduct

Overview: *Your company values must be the foundation of your ethics and compliance program and should be communicated through your Code of Conduct ("Code"). The Code must also provide important business conduct information for your employees and others who represent your company. How do you know that your company has been effective in achieving these objectives?*

The following are audit steps you can use to assess the effectiveness of the communication of your values and the Code of Conduct.

a. Do you provide your Code of Conduct to all of your employees, Directors and agents?

If so, examine evidence of acknowledgments of receiving the Code. This can be done by examining the acknowledgment cards, if submitted by the individuals who received the codes; or examining any electronic evidence of acknowledgment of the code if the code was distributed electronically. Examine at least 25% of such evidence selected at random.

b. What do you do to ensure that your employees understand the Code of Conduct and are familiar with its requirements?

Is there any training for employees to introduce them to the Code? If so, from the list of your company employees, select 25% of the names at random and examine evidence of their attendance at orientation training for the code. Such evidence, for example, can be signatures on sign-in-sheets noting employee name and employee number or other evidence as deemed appropriate.

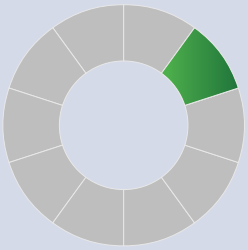
c. How do you know that the Code training provided to employees is effective in ensuring that the employees understand the Code and its requirements?

Select a random sample of employees (no more than 15 or no less than 10 per site) to interview, without the presence of their supervisors. The questionnaire should include the following:

1. Have they received the Company's Code?
2. Do they understand their role in complying with the standards established by the Code?
3. Do they believe the Company is serious about ethics and compliance? If not, why not?
4. What do they think are the Company's risks regarding ethics and compliance?

5. Do they know the name of their Ethics Officer or the person they can contact to report wrongdoing?

The answers to the above questions should be summarized to form an opinion regarding the effectiveness of the Code of Conduct training program.



3. Risk Assessment

Overview: *To build upon a foundation of ethics, many companies conduct a comprehensive risk assessment by looking closely at their business to determine areas of business ethics and legal risks on a periodic basis. The purpose of such assessment is to ensure that the ethics and compliance program is focusing on current business risks as a result of changes in organizations, business practices, and laws and regulations.*

Some risk areas may include:

Anti-Kickback/ Anti-Bribery	**Proprietary Information**	**Cost Accounting**	**Supply Chain Integrity**	**Government Contracting Issues**
Company Assets	**Time Charging**	**Foreign Corrupt Practices Act**	**Antitrust**	**Safety Rules/OSHA**
Environmental	**Nondiscrimination**	**Procurement Integrity/TINA**	**Conflicts of Interest**	**Non-harassment**
Cybersecurity and Data Protection	**Business Courtesies/ Gratuities**	**Teaming**	**Export Control**	**AI and Emerging Technology**

Compliance programs establish minimum acceptable conduct, whereas robust ethics and business conduct programs are the foundation upon which compliance programs and legal best practices are built. Compliance rules tend to cluster in discrete subject areas, and some areas may only concern a specific, targeted group of employees (e.g., export control issues, TINA, etc.). However, your compliance program may be integrated into your ethics and business conduct program, resulting in a cohesive, holistic Ethics and Compliance program. Here are the audit steps you can use to assess the effectiveness of your risk assessment programs:

a. What do you do to assess the risk of non-compliance with applicable laws and regulations and to assess the risk of fraudulent transactions by your employees and/or third parties?

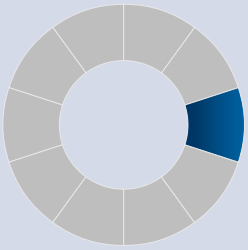
1. Is there a formal risk assessment process? If so, examine how the risk assessment is done to ensure that it is done objectively.

2. Did the risk assessment identify risks of fraud and/or non-compliance with laws and regulations? If so, are there plans for mitigating those risks? Such mitigation may include implementation of applicable policies, establishment or enhancement of internal controls, internal or external audits, segregation of duties, and training.

3. If there were risk mitigation plans, ensure that specific individuals have been identified to implement the risk mitigation plans. Seek opinions of subject matter experts (e.g., Law, Internal Audit, Controllership, IT, Corporate Security, Loss Prevention) regarding the adequacy of the risk mitigation plans.

4. Follow up on the action items after the planned implementation dates to ensure that the mitigating actions were implemented according to the plan.

Based on the above action items, provide an opinion regarding the adequacy and effectiveness of the risk assessment program in your company.

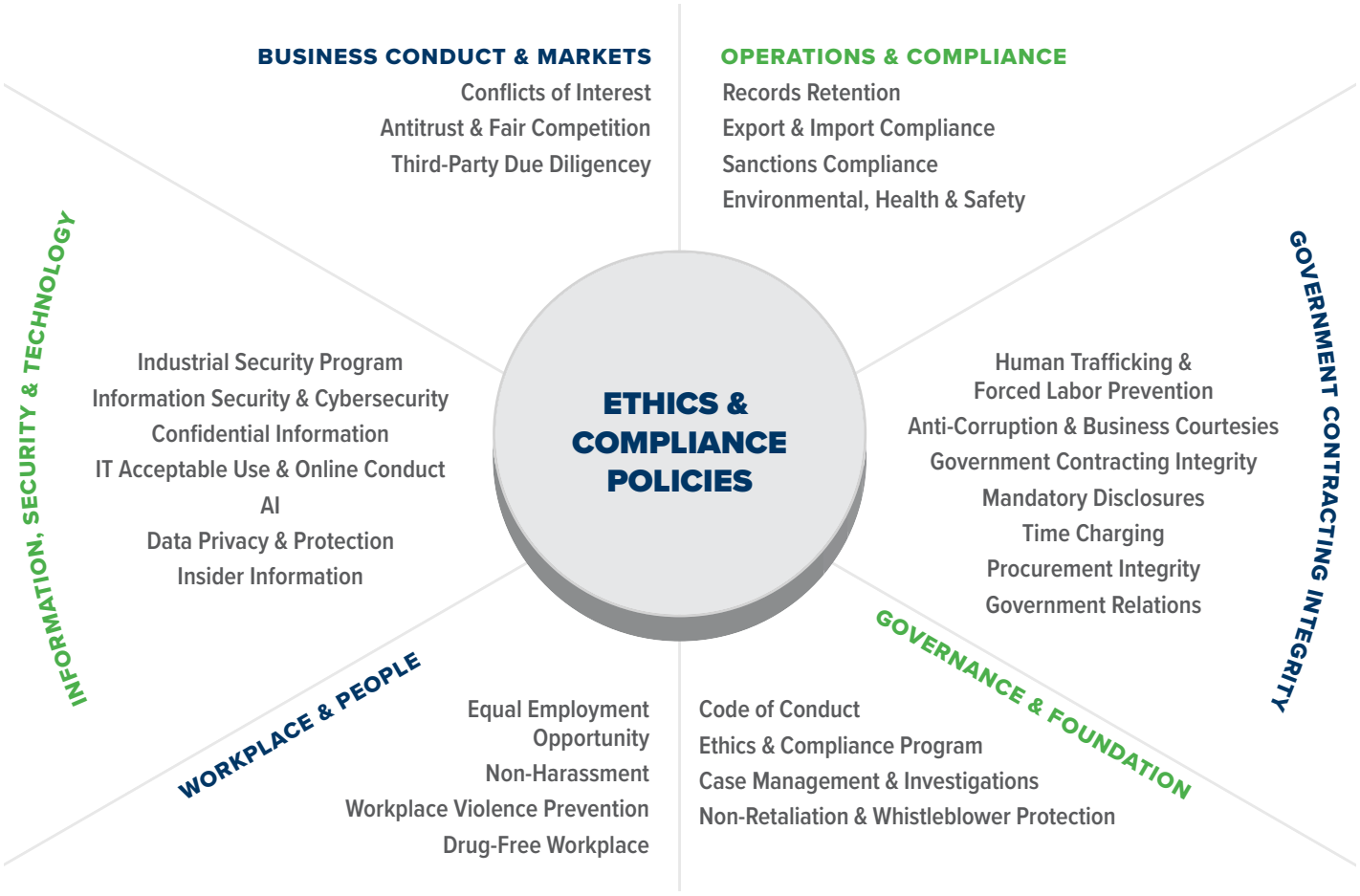


4. Ethics and Business Conduct Policies

Overview: *Your company's policies and procedures should include a statement from your CEO on ethics and business conduct. This formalizes your Company's commitment to the highest ethical conduct in all aspects of your business.*

The company's policies and procedures are the execution plans for the values and standards established in the Company's Code. Do you have policies and procedures addressing all areas of your Code to ensure that the employees understand their responsibilities to carry out the Company's commitments and to implement the standards established in the Code?

An effective Ethics and Compliance Program should include Policies and Procedures addressing the particular risks facing the company, such as:

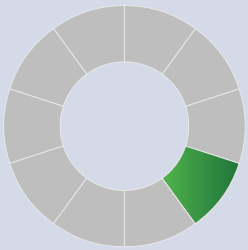


Examine your list of policies and see if all of the above risk areas are addressed. If not, recommend the establishment of such policies to facilitate compliance with relevant laws, regulations, and/or the Company's standards or guidelines. If all or some of the policies listed above exist, how do you know that the employees are aware of such policies and are knowledgeable about their roles in complying with the requirements of those policies?

In the employee interviews mentioned in audit step 1c above, ask the following questions for each of the policies relevant to your Code. The following is a suggested format for such questions:

1. I am going to read you a list of items and I'd like you to tell me how well you understand your own responsibilities in connection with each of them. It might be that you understand your responsibilities "Well," or you understand them "Somewhat," or you "Don't Really Understand Your Responsibilities," or that the item "Just Doesn't Apply To You." (Read each item and wait for the employee's response.) The questions relate to the employee's overall awareness on these issues based on their understanding of the Code and the Company's Policies and Procedures identified above in section 3.
2. If an employee says he/she is not aware of the Company's guidelines on a topic listed above, refer him/her to the specific section of the Code of Conduct.
3. Based on the results of the above interviews, prepare an opinion regarding employee awareness of your policies and procedures.

Recommend what actions, if any, need to be taken to address any deficiencies. For example, if the majority of interviewees answer "somewhat" or "don't know" to your questions about Human Rights and Conflicts of Interest, you should recommend that awareness of those policies be increased through additional training and/or communication.



5. Inquiry and Reporting Mechanisms

Overview: *It is important that your ethics and compliance program includes at least one mechanism in place for your employees, suppliers, customers, and others who do business with your company to ask questions or raise areas of concern.*

a. Do you have a process for employees to report their concerns about ethics or about violations of laws, regulations, and Company policies? If so, who is responsible for receiving employee calls or concerns? The best practice is to use a third party to receive such calls live on a toll-free line so that there is no concern about the complainant being identified.

b. If you have a Hotline number, how is it communicated to employees? Ensure that the following are done:

1. Posters with the toll-free hotline number are displayed prominently at locations where employees gather frequently (e.g., cafeteria and other common areas).

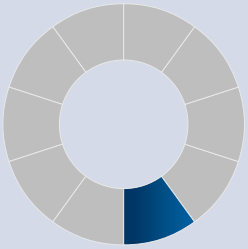
2. The name and contact information of the appropriate Ethics Officer or other appropriate person are noted to allow employees to report a concern in person if they wish to do so.
3. Ensure that the posters state that the concerns can be reported anonymously.
4. Ensure that the hotline poster states that there will be no retaliation for reporting a concern even if it turns out to be unsubstantiated.
5. Ensure that the posters are changed periodically in designs and colors so that they continue to remain noticeable.

c. Assess the effectiveness of the above reporting mechanism by asking the following questions during the interviews mentioned in 1c above:

1. Do they know that there is a hotline number they can use to report concerns?
2. Do they know where to find the hotline number?
3. Do they know that there will be no retaliation for reporting a concern if it turns out to be unsubstantiated?
4. Do they know the name and contact info of their Ethics Officer?

d. Do the company's confidentiality, severance, and employee agreements include carve-outs preserving employees' rights to report concerns to government regulators (including the SEC, EEOC, DOL, and similar agencies)?

e. Does the company periodically assess employees' willingness to report concerns (for example, through survey questions) and identify any factors that may chill reporting?



6. Investigation of Reported Concerns

Overview: *Once a concern is reported, how you investigate it determines whether employees will trust the program and continue to come forward. An effective investigation process is prompt, objective, consistently applied, and conducted by trained individuals who are independent of the matter under review. The following audit steps will help you assess whether your investigation process meets those standards.*

a. What is your process for investigating the concerns reported through your reporting mechanisms such as the company's hotline?

b. Is there a formal protocol for deciding who investigates what? Do you verify that the investigator is independent and objective and has had some training in conducting investigations?

c. Are the investigations documented in formal reports? If so, examine a sample or all of the reports completed during the past 12 months and determine if the investigations are done in accordance with the Company's protocol.

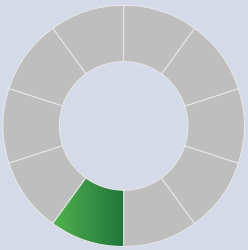
d. Is there a prioritization of concerns (e.g., A, B, C) received based on the severity of the issues raised? If so, was

there a timeline for completion of the investigation based on this categorization?

1. Were the investigations completed in accordance with the established timeline?
2. Were the investigations thorough enough to reach a conclusion regarding the validity of the concerns?
3. Was there any explanation for actions taken or not taken as a result of the concerns received?
4. Were the concerns acknowledged to assure the caller that their concerns were taken seriously and will be investigated timely and thoroughly?
5. Were the callers made aware of the results of the investigations?

e. Are confidentiality instructions to witnesses and complainants narrowly tailored to the specific investigation (for example, limited to the duration of the investigation and to specific categories of information), rather than blanket prohibitions on discussion?

Prepare an opinion about the adequacy and effectiveness of your Inquiry and Reporting Mechanisms based on the results of the above audit procedures.



7. Awareness Training

Overview: *In addition to publishing a Code, it is necessary to continue to communicate your company's commitment to ethics to your employees. Employee awareness can be achieved through something as formal as one hour of live ethics training each year or through a variety of ethics awareness initiatives that can be presented to employees periodically on a more informal basis, such as incorporating ethics discussions into regular staff meetings, safety meetings, or employee forums.*

One effective method of training is top-down, cascaded training that begins with the company's president or CEO training his or her staff. The training is then cascaded down through the entire company, with each leader training his or her direct reports so each employee hears the company's ethics message directly from his or her immediate supervisor.

Other examples of ethics training materials include videos, on-line training provided by training vendors, and live classroom training.

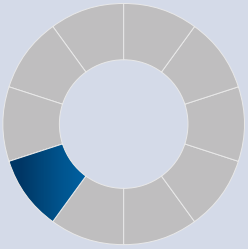
Do you have a program to train your employees to make them aware of Ethics and Compliance issues relevant to your Company? If yes:

a. How is this training delivered to employees? Is it an on-line program or live sessions? Is the delivery method adequate to reach all employees who must take the ethics and compliance courses?

b. How is one considered to have completed a course? Is there a quiz after a training course with a minimum score requirement?

c. If a tracking mechanism is used to see the completion status of required courses, what percent of the employees have completed their required courses? A best-practice ethics program will have 100% completion status.

Prepare an opinion regarding the adequacy of the Awareness Training program based on the results of the above audit steps.



8. Communication Program

Overview: *Developing a comprehensive communication plan for your ethics and compliance program allows you to manage the task of communicating your program's elements to your employees. A communication plan ensures that you are able to engage all audiences with specific messages using a variety of media.*

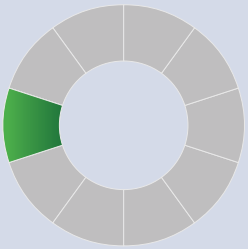
a. Does the communication of your company's commitment to ethical conduct include consistent messages delivered in engaging and diverse manners such as email, posters, company newsletters, company intranet, and other existing company communications?

b. Do all levels of leadership in your company use every available opportunity to verbalize a personal commitment to the company's ethical standards? Examine evidence of such communications (e.g., speeches, presentations, discussions on ethics topics at staff meetings, safety meetings, and All-Hands meetings).

c. Examine how often messages described above are delivered. Such messages should be frequent enough to be constant reminders for ethical behavior in all aspects of the Company's business.

d. Does the program address business communications conducted on personal devices and messaging applications (including ephemeral messaging applications)? Does the company have a policy directing the preservation of business-related communications on employees' personal devices?

The effectiveness of the above-mentioned communication initiatives will also be reflected in the employee interviews mentioned in step 1c above. Prepare an opinion on the adequacy of your Company's communication initiatives based on the results of the above audit steps and the employee interviews.



9. Program Assessment and Evaluation

Overview: *Part of maintaining an effective Ethics and Compliance Program is conducting regular program assessments and evaluations. Performing the audit procedures described in this document is one way to assess the effectiveness of your ethics and compliance program.*

You should inquire about the following question:

a. Was there any internal or external audit of your program?

b. Who conducted the audit and how was the audit team composed? Was there an appropriate mix of internal personnel, external consultants, and subject-matter experts (such as legal, accounting, or industry specialists), and were team members independent of the activities being audited?

Internal and external audits of your program addressing all areas of your program can help your company avoid noncompliance and should be conducted regularly. This may be particularly useful when there is a new business venture, downsizing or personnel changes have taken place, or complacency has become evident.

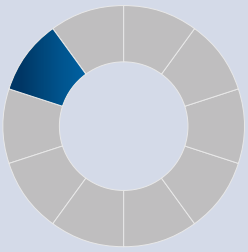
c. How often are the internal controls tested to ensure that they are adequate to prevent or detect fraud and/or non-compliance with laws and regulations?

d. Does the ethics and compliance function have appropriate access to company data (financial, HR, IT, third-party) needed to identify and assess compliance risks?

e. After completing the audit, did the company implement a follow-up review (typically three to six months later) to confirm that corrective actions were applied and that compliance improvements have been sustained?

Based on discussions with your controllers, ensure that internal controls are kept up to date and effective and that corrective action was taken when misconduct or potential for misconduct was identified.

You may also use employee surveys (separate from Human Resources surveys) and focus groups to measure the ethics culture of your company and spotlight areas for improvement in your program. Assessment surveys can also be done through external resources to ensure objectivity and independence in the expression of an opinion regarding the adequacy and effectiveness of your program in instilling ethical values, ethical leadership, and an overall ethical culture.



10. Discipline and Incentives

Overview: *An effective ethics and compliance program is reinforced through both consequences for misconduct and rewards for ethical behavior. Discipline should apply not only to those who engage in improper conduct, but also to supervisors and managers who fail to take reasonable steps to prevent or detect it. Incentives — including compensation, recognition, and advancement opportunities — should reward employees who demonstrate commitment to the program.*

a. Does the company have written standards for disciplinary action that apply to misconduct in connection with Government contracts? Confirm that discipline is available not only for the employee who engaged in improper conduct, but also for any supervisor or manager who failed to take reasonable steps to prevent or detect the conduct.

b. Is discipline applied consistently? Examine a sample of disciplinary actions taken over the past 12–24 months to confirm that similar misconduct results in similar consequences across levels of seniority and across business units.

c. Does the company's compensation structure reinforce compliance? Determine whether:

1. Eligibility for bonuses, raises, and other discretionary compensation is conditioned on meeting ethics and compliance expectations;

2. The company has clawback or recoupment provisions for compensation paid to individuals later found to have engaged in misconduct or to have supervised others who did; and

3. Ethics and compliance performance is a factor in promotion and succession decisions.

d. Does the company recognize and reward employees who demonstrate commitment to the ethics and compliance program — for example, through performance evaluations, formal recognition, or eligibility for advancement?

Prepare an opinion regarding the adequacy and effectiveness of the company's discipline and incentive practices based on the results of the above audit steps.

Conclusion: Prepare an overall summary of your findings based on the results of the above audit steps and provide an opinion about the adequacy and effectiveness of your ethics and compliance program. Provide recommendations for corrective actions if needed. The recommended corrective actions should identify individuals responsible for implementing those actions with expected completion dates.