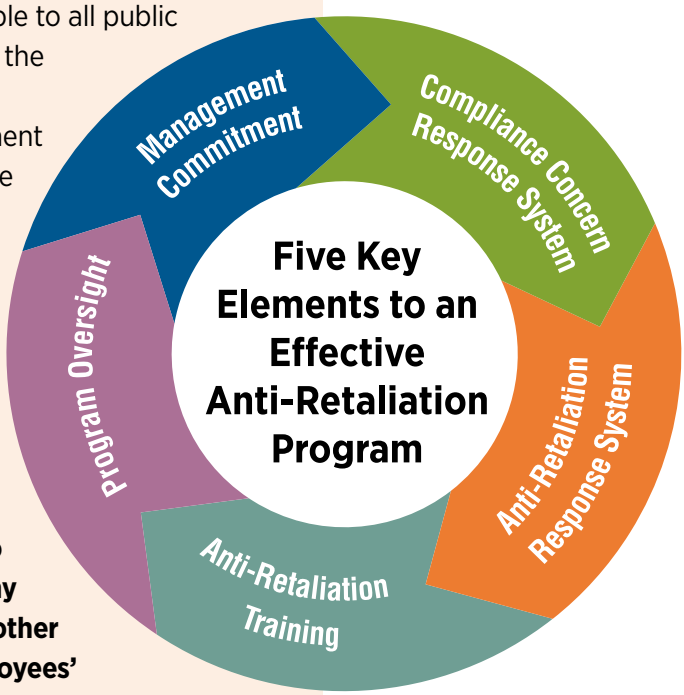
Recommended Practices for Anti-Retaliation Programs

How to Use These Recommended Practices

This set of recommendations is intended to assist employers in creating workplaces that are free of retaliation, including retaliation against employees who engage in activity protected under the 22 whistleblower laws that the Occupational Safety and Health Administration (OSHA) enforces. This document is advisory in nature and informational in content. It is not mandatory for employers, and does not interpret or create legal obligations.

These recommendations are intended to be broadly applicable to all public and private sector employers that may be covered by any of the whistleblower protection provisions enforced by OSHA. This recommended framework can be used to create and implement a new program, or to enhance an existing program. While the concepts outlined here are adaptable to most workplaces, employers may adjust these guidelines for such variables as employer size, the makeup of the workforce, and the type of work performed.[1]



This guidance is directed at employers that may be covered by the 22 whistleblower protection statutes that OSHA enforces, although the basic principles in this guidance could also be useful in circumstances where other anti-retaliation protections apply. **This guidance is not intended to advise employees about their rights or protections under any whistleblower protection statute enforced by OSHA or any other government agency. Information and resources about employees' rights under the whistleblower protection statutes that OSHA enforces can be found at www.whistleblowers.gov.**

Retaliation Is Against the Law

OSHA's Whistleblower Protection Program enforces the whistleblower provisions of 22 federal statutes protecting employees who raise or report concerns about hazards or violations of various workplace safety and health, airline, commercial motor carrier, consumer product, environmental, financial reform, food safety, health insurance reform, motor vehicle safety, nuclear, pipeline, public transportation agency, railroad, maritime, and securities laws (see list of statutes at the end of this document).

An employer must not retaliate against an employee for engaging in activities that are protected under these laws. Protected activities may include: filing a report about a

1 The core recommendations presented in this document were recommended unanimously by the Secretary of Labor's Whistleblower Protection Advisory Committee.

OSHA®
www.whistleblowers.gov
(800) 321-OSHA (6742)
OSHA 3905-01/2017

possible violation of the law with OSHA or other government agencies, reporting a concern about a possible violation of the law to the employer, reporting a workplace injury, illness, or hazard, cooperating with law enforcement, refusing to conduct tasks that would violate the law, or engaging in any other type of statutorily protected activity.

Preventing Retaliation Is Good for Workers and Good for Business

Retaliation against employees who raise or report concerns or otherwise exercise their rights under these laws is not only illegal, it is also bad for workers and bad for business. A proactive anti-retaliation program is designed to (1) receive and respond appropriately to employees' compliance concerns (i.e., concerns about hazards or potential employer violations of one of the 22 laws) and (2) prevent and address retaliation against employees who raise or report concerns. Without an effective program, problems in the workplace may go unreported because workers fear retaliation for reporting concerns or feel frustration over the lack of effective resolution of their concerns.

An anti-retaliation program that enables all members of the workforce, including permanent employees, contractors and temporary workers, to voice their concerns without fear of retaliation can help employers learn of problems and appropriately address them before they become more difficult to correct. A program based on this proactive approach not only helps employers ensure that they are following federal laws, but also helps create a positive workplace culture that prevents unlawful retaliation against employees. Furthermore, a successful anti-retaliation program improves employee satisfaction and engagement, and helps protect workers and members of the public from the harm of violations of federal laws and regulations.

A successful anti-retaliation program improves employee engagement, and helps protect workers and members of the public from violations of federal laws and regulations.

Employees' Rights to Report to the Government

While an anti-retaliation program that enables employees to communicate their compliance concerns to the employer can be beneficial to employers, workers, and the public, employers must also recognize that employees have the right to provide "tips" or file complaints about hazards or potential violations of the law with OSHA and other government agencies. Employer policies must not discourage employees from reporting concerns to a government agency, delay employee reports to government, or require employees to report concerns to the employer first. OSHA also cautions employers that an anti-retaliation program must not have the effect of discouraging or misleading employees about their right to report compliance concerns or retaliation externally. Anti-retaliation program policies and training for management and employees should clearly explain employees' rights to report hazards, violations of the law and retaliation externally, and that retaliation for reporting externally is against the law.

What Is Retaliation?

Retaliation occurs when an employer (through a manager, supervisor, or administrator) takes an adverse action against an employee because the employee engaged in protected activity, such as raising a concern about a workplace condition or activity that could have an adverse impact on the safety, health, or well-being of the reporting employee, other workers, or the public; or reporting a suspected violation of law. Retaliation also occurs when an employer takes an adverse action because an employee reported an injury or to dissuade an employee from reporting an injury. An adverse action is an action that could dissuade or intimidate a reasonable worker from raising a concern about a workplace condition or activity. Retaliation against an employee is not only harmful to the employee who experienced the adverse action, it can also have a negative impact on overall employee morale because of the chilling effect that retaliation can have on other employees' willingness to report concerns.

Because adverse action can be subtle, it may not always be easy to spot. Examples of adverse action include, but are not limited to:

- Firing or laying off
- Demoting
- Denying overtime or promotion
- Disciplining
- Denying benefits
- Failing to hire or rehire
- Intimidation
- Making threats
- Blacklisting (e.g., notifying other potential employers that an applicant should not be hired or refusing to consider applicants for employment who have reported concerns to previous employers)
- Reassignment to a less desirable position or actions affecting prospects for promotion (such as excluding an employee from training meetings)
- Reducing pay or hours
- More subtle actions, such as isolating, ostracizing, mocking, or falsely accusing the employee of poor performance.

Creating an Anti-Retaliation Program

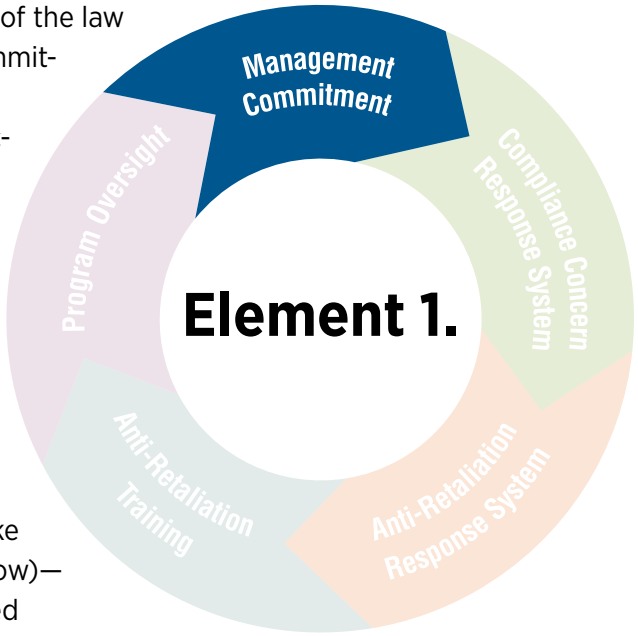
Implementing an effective anti-retaliation program is not intuitive and requires specific policies and commitments. There are five key elements to creating an effective anti-retaliation program:

1. Management leadership, commitment, and accountability
2. System for listening to and resolving employees' safety and compliance concerns
3. System for receiving and responding to reports of retaliation
4. Anti-retaliation training for employees and managers
5. Program oversight

In order to effectively support employee reporting and protect employees from retaliation, employers should integrate all five elements into a cohesive program.

Management Leadership, Commitment, and Accountability

To make preventing retaliation and following the law integral aspects of the workplace culture, it is important that senior management demonstrate leadership and commitment to these values. Senior management, such as the CEO and board (if applicable), should lead by example to demonstrate a culture of valuing and addressing employees' concerns regarding potential violations of the law and commitment to preventing retaliation. To demonstrate commitment, management should back up words with actions; written policies that are not actively practiced and enforced are ineffective. Managers at all levels should be held accountable for the quality of their response to employees' concerns, including reports of potential violations of the law, of safety hazards, and of retaliation.



How can management show commitment to preventing retaliation?

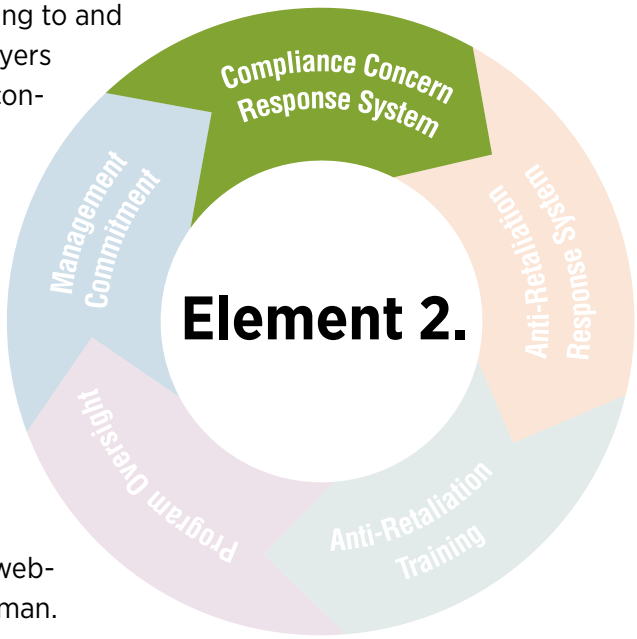
- Ensure that the systems for reporting hazards, compliance concerns and retaliation—including systems for maintaining the confidentiality of employees who make reports (discussed in more detail in elements 2 and 3 below)—are implemented, enforced, and evaluated by a designated manager who is responsible and accountable for these programs, and has access to top managers and the board (if applicable).
- Confer with workers and worker representatives (if any) about creating and improving management awareness and implementation of anti-retaliation policies and practices.
- Require training for managers and board members (if applicable) to make certain they understand what retaliation is, the employer's and their own legal obligations (including their obligation to maintain the confidentiality of employees who make reports), the organizational benefits of anti-retaliation practices, and what it takes programmatically to prevent retaliation. (For more information, see element 4 below.)
- Ensure that there is a mechanism for accurately evaluating employees' willingness to report concerns about the workplace and the employer's actual record in preventing retaliation against employees who report, and ensure that there is a means for accurately reporting to top management the results of such evaluation.
- If appropriate, and taking into account an employee's preference for confidentiality, publicly recognize the contribution of employees whose disclosures have made a positive difference for the employer, perhaps through an award that is publicized company-wide.

How can management be held accountable for preventing retaliation?

- Incorporate anti-retaliation measures (e.g., promptly and constructively addressing employee concerns, attending training, and championing anti-retaliation initiatives) in management performance standards and reviews.
- Implement strong codes of conduct and ethics programs that clearly identify whistleblower retaliation as a form of misconduct to ensure anti-retaliation policies and practices are enforceable.
- Apply appropriate consequences, such as discipline, to managers who retaliate or who violate the confidentiality of an employee who has made a report. These consequences should be sufficient to serve as a deterrent to future acts of retaliation.

System for Listening to and Resolving Employees' Safety and Compliance Concerns

To help prevent retaliation, employers should proactively foster an organizational culture in which raising concerns about workplace conditions and activities is valued. Employers can cultivate such an environment by listening to and resolving employees' compliance concerns. Specifically, employers should establish procedures that enable employees to report concerns (including through confidential or anonymous channels, when possible), provide for fair and transparent evaluation of concerns raised, offer a timely response, and ensure a fair and effective resolution of concerns. In developing these policies, employers should work with employees and worker representatives (if any).



What can employers do to enable employees to raise safety and compliance concerns?

- Create at least one or, preferably, multiple channels for reporting compliance concerns. Channels can include helplines, anonymous reporting through email boxes or websites, or reporting to a trusted official and/or an ombudsman.
- Protect the confidentiality or anonymity of employees who report concerns, and ensure that confidentiality is not used as a shield to prevent whistleblowers from having access to information needed to exercise their rights.[2]
- Give employees clear and accessible instructions on how they can report compliance concerns both internally and externally, and make clear that the employee has the right to choose which avenue to use to report concerns. Employees must not be penalized for reporting concerns to the employer by a means other than through these channels.
- Ensure that the program does not restrict or discourage employees from reporting allegations to the government or other appropriate regulatory and oversight agencies.

2 While an employee should be permitted to remain anonymous when reporting compliance concerns internally (i.e., within the company) or externally to a government agency, the 22 whistleblower statutes enforced by OSHA do not allow for an employee to anonymously file a retaliation complaint with OSHA.

- Provide employees with opportunities to share information informally and to ask questions at an early stage, before issues become more difficult to resolve.
- Eliminate or restructure formal and informal workplace incentives that may encourage or allow retaliation or discourage reporting. Examples of incentives that may discourage reporting or encourage retaliation include rewarding employee work units with prizes for low injury rates or directly linking supervisors' bonuses to lower reported injury rates.

  (For additional information on incentive programs, see OSHA's information on Employer Safety Incentive and Disincentive Policies and Practices, http://www.osha.gov/as/opa/whistleblowermemo.html, Revised VPP Memo #5: Further Improvements to the Voluntary Protection Programs, https://www.osha.gov/dcsp/vpp/policy_memo5.html, and incentive program guidance at https://www.osha.gov/recordkeeping/modernization_guidance.html.)

How should employers ensure prompt and fair resolution of compliance concerns?

Create at least one or, preferably, multiple channels for reporting compliance concerns.

- Have an independent investigator review reports of concerns promptly, thoroughly, and with transparency, including responding to the employee who brought forward the initial concern.
- Ensure that supervisors or managers respond in a constructive and timely manner upon receiving reports of concerns from employees.
- Guarantee that employee rights are protected even if the person is incorrect or unpleasant in raising a concern.
- Follow through on employee concerns, even if they appear to be trivial.
- Have a strong, enforceable policy of not punishing employees for reporting concerns or incidents or for engaging in any other protected activity.
- Help employees get unbiased, confidential advice or information about exercising whistleblower rights and coping with the stress of reporting concerns, such as by providing a list of resources.
- Ensure that any employment agreement or policy that requires employees to keep employer information confidential does not prohibit or discourage employees from reporting or taking the steps necessary to report information reasonably related to concerns about hazards or violations of the law to any government agency. Steps that may be necessary include conferring with legal counsel, union or other worker representatives, or with medical professionals regarding the employee's concerns. Employers should not use confidentiality or non-disclosure agreements to penalize, through lawsuits or otherwise, employees who report suspected violations of the law or take steps necessary to make such reports.
- Ensure that employment status changes, such as demotions and denials of promotions, are only made for legitimate non-retaliatory reasons and are not likely to be perceived as retaliatory.

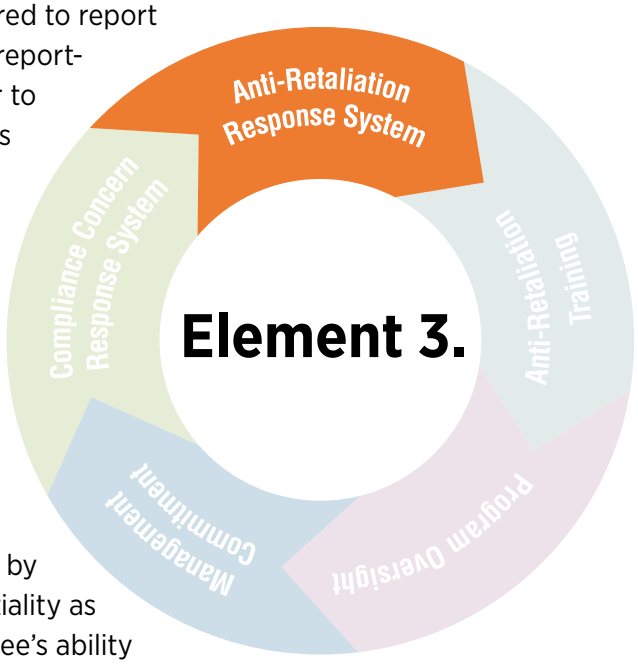
If an employee is disciplined after reporting a concern, injury, or other issue, how should the employer review the discipline to ensure that it is not retaliatory?

Ask questions such as:

- Did the employee's report influence the decision to initiate disciplinary action in any way?
- Has the employer disciplined other employees who engaged in the same conduct as the employee but who did not report a concern?
- Is the discipline imposed on the employee of the same severity as the employer's response to the same conduct by other employees who did not report a concern?
- Has the disciplinary action been independently reviewed by a manager who was not involved in the incident?
- If the employer uses progressive discipline, has it been appropriately used up to this point?
- Could the workforce perceive the punishment as retaliatory? If so, what actions can management take to mitigate the potential chilling effect?

System for Receiving and Responding to Reports of Retaliation

Employees who believe they have experienced retaliation should have independent channels for reporting the retaliation; they should not be required to report to the manager who they believe retaliated against them. The reporting employee should also have the ability to elevate the matter to higher levels, if necessary. There should be clearly defined roles and responsibilities for managers at all levels and others who are involved in responding to reports of retaliation, such as human resources or ethics and compliance personnel. The procedures should be known and accessible to all.



When retaliation is reported, employers should investigate the claim promptly and thoroughly, utilizing an established retaliation response system. Such investigations should:

- Take all reports of retaliation seriously.
- Maintain employee confidentiality as much as possible to protect the employee from further retaliation or isolation by coworkers. However, employers should not use confidentiality as a shield to impede a government agency's or the employee's ability to successfully resolve the retaliation claim.
- Be transparent to the employee alleging retaliation about how investigations are conducted, including the roles and independence of the investigators.
- Investigate claims using an objective, independent complaint review process; focus on evaluating the circumstances surrounding the employment decision objectively rather than on defending against the claim; and listen to all sides before making a judgment.

- Ensure that investigations of alleged retaliation are not tainted by preconceptions about what happened.
- Utilize conflict of interest protections.
- Involve senior managers and others who recognize the organizational impact, benefits, risks, and policy ramifications of both the reported concern and the need to prevent retaliation against the reporting employee.
- Ensure that the program does not restrict or discourage employees from reporting retaliation allegations to the government or other appropriate regulatory and oversight agencies.
- Keep the reporting employee and management representatives informed of developments throughout the investigation and ensure respectful, proper closure of the issue.
- After the reported problem has been investigated and resolved, periodically follow up with the reporting employee for a reasonable amount of time to ensure continued protection from retaliation.
- Use third-party, independent investigators if the employer can support it and the circumstances warrant it (e.g., when the allegations involve particularly polarizing or high-stakes issues).
- If possible, make the anti-retaliation investigation completely independent from the corporation's legal counsel, who is obligated to protect the employer's interests. If the employer's legal representative is involved in conducting the investigation, fully inform the whistleblower that the investigator represents the employer's interests and that any attorney-client privilege will only extend to the employer.
- Consider using early dispute resolution techniques when significant disputes arise about an employee's disclosures or when considering implementing adverse actions like termination or demotion.
- Ensure that employees understand that they may file a retaliation complaint with OSHA and, if applicable, another government agency and that any internal investigation by the employer or attempts at early dispute resolution by the employer will not automatically delay or toll the deadline for filing a retaliation complaint with OSHA or another government agency. In certain circumstances, employers should consider whether offering to formally delay the deadline to file would be appropriate.
- Be attuned to the potential for a chilling effect caused by the workforce's perception that management's actions were retaliatory, and if likely, address such a perception through timely and effective communications or other mitigating strategies.

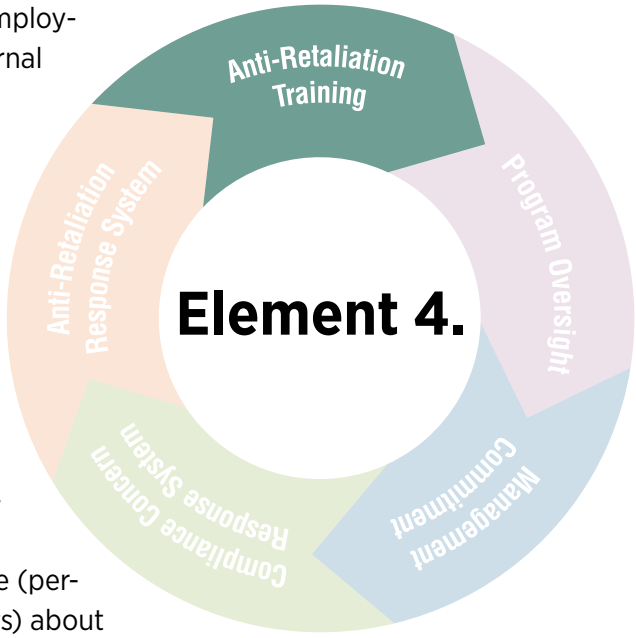
Take all reports of retaliation seriously.

Employers should respond quickly to reports of retaliation. Failure to do so can discourage employees from reporting concerns about workplace conditions or activities.

If the employer confirms that retaliation took place, it should remedy the retaliation and review its anti-retaliation program to determine why the system failed and what changes may be needed to prevent future retaliation. Workers and worker representatives (if any) should be integrally involved in this evaluation.

Anti-Retaliation Training for Employees and Managers

Effective training of employees and all levels of management and the board (if applicable) is key to any anti-retaliation program. Training is essential because it provides management and employees with the knowledge, skills, and tools they need to recognize, report, prevent, and/or properly address hazards, potential violations of the law, and retaliation. Training should be tailored to teach workers and managers about the specific federal whistleblower protection laws and company policies that apply to them, employees' rights under the laws, how employees can exercise their rights using available internal and external protection programs, and the organizational benefits of such programs. Managers should learn these concepts as well as related skills, behaviors, and obligations to act.



Training should be provided in accessible language(s) and at a level that can be easily understood by the intended audience.

Anti-retaliation training for employees, at a minimum, should include coverage of:

- Relevant laws and regulations.
- An explanation of the employer's commitment to creating an organizational culture of complying with the law, addressing concerns from all members of the workforce (permanent employees, contractors, and temporary workers) about potential hazards and violations of the law, and complying with its code of ethics, including prohibitions on retaliation.
- Employees' rights and obligations, if any, to report potential hazards and violations of the law externally to law enforcement, including OSHA and other government agencies, regardless of whether the employee first reported the violation to the employer.
- Statutory rights to be protected from retaliation for reporting potential violations.
- The elements of the employer's anti-retaliation program, including roles and responsibilities, how to report concerns internally and externally, options for confidential or anonymous reporting, and how to elevate a concern internally when supervisors or others do not respond.
- What constitutes retaliation, including actions such as firing or laying off, demoting, denying overtime or promotion, disciplining, denying benefits, failure to hire or rehire, reducing pay or hours, and blacklisting, along with common but less overt behaviors, such as ostracizing, mocking, intimidating, and making false accusations of poor performance.

In addition to the employee training topics described above, anti-retaliation training for managers should include, at a minimum:

- Skills for defusing conflict, problem solving, and stopping retaliation in a work group.

- How to respond to a report of a workplace concern while protecting an employee's confidentiality and without engaging in retaliation, appearing to engage in retaliation, or questioning the motives for the report.
- How to separate annoying or inappropriate behavior from the concern itself.
- Consequences for managers who fail to follow anti-retaliation policies or respond to concerns inappropriately.
- How to recognize that an employee believes there has been retaliation, when employers are required to act, and the potential legal consequences the employer and the manager face for inaction.
- Other issues specific to the employer.

Legal requirements can change. Employers should create a process for staying up to date on changes to anti-retaliation laws and regulations and update their training and policies accordingly. Refresher training should be conducted on a regular basis and as needed, such as when there is a change in legal requirements, when retaliation has occurred, or when program oversight reveals that it is needed. Concepts from the training should not only be discussed during the designated training sessions, but should be reinforced frequently using other types of communications in order to make it part of the workplace culture.

Effective training is key to any anti-retaliation program.

Program Oversight

A well-designed anti-retaliation program needs rigorous oversight to ensure that it is effective and working as intended. Employers should develop and implement a plan for oversight of the anti-retaliation program, review oversight findings, and ensure that the program is improved and modified as needed.

What are some methods of oversight that can be used to assess the anti-retaliation program?

Monitoring and audits are two forms of oversight that can help employers gain insight into a program's strengths and weaknesses and reveal whether program improvements are needed.

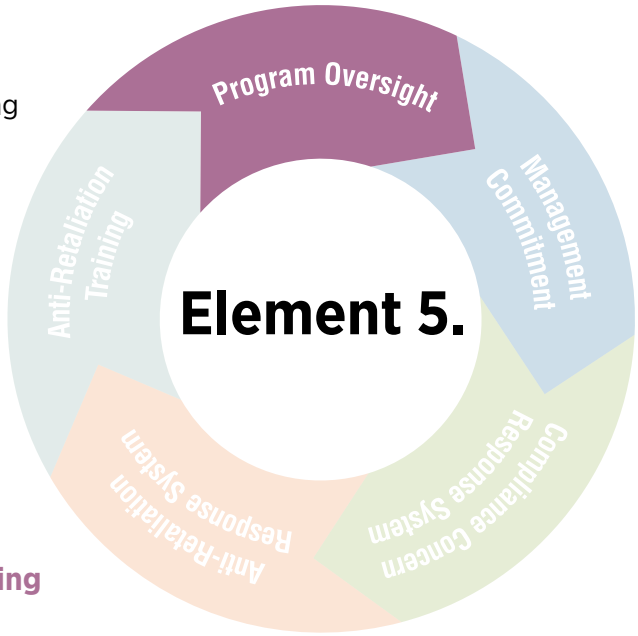
- Monitoring is an ongoing analysis of whether the program processes in place are achieving the organization's planned results and program goals.
- Auditing is an independent, formal, and systematic approach designed to determine whether program processes are efficient, effective, and working as intended. Audits should be conducted by individuals who are independent of the process being audited.

The functions of monitoring and auditing may overlap, and results from any one activity can be used to direct efforts of the other activities.

What issues should employers assess using oversight tools like monitoring and auditing?

Oversight tools like monitoring and auditing should be tailored to meet an organization's specific needs. Examples of the types of anti-retaliation program topics that may be assessed using oversight include:

- Trends in issue reporting and resolution, including anonymous reporting;
- Whether managers are following program policies;
- Whether workers are unafraid of retaliation and coming forward with concerns; and
- Whether the types of measurements that are used to track issue response and reward improvement could have the effect of discouraging reporting rather than incentivizing it.



Note that when new anti-retaliation programs are implemented, the numbers of reported incidents may rise at first. This often means that employees are more comfortable reporting, not that there are a larger number of concerns to report.

What sources of information should be examined during program oversight?

Program oversight may examine a variety of sources, such as: anonymous surveys; confidential interviews with employees who reported compliance concerns or retaliation; narratives from injury or error reports; case studies of investigated issues and responses; claims department or risk management case files related to injuries or errors; and complaint files relating to reporting requirements.

Employers can also cross-check the data obtained as part of monitoring or auditing with other sources of relevant information, such as information reported to workers' compensation, in grievances, to outside agencies, or in exit interviews. Cross-checking these other sources of information could reveal whether a policy is creating a chilling effect or other barrier that is discouraging or preventing employees from reporting compliance concerns or retaliation.

How should employers use the results or findings of program oversight?

The results of oversight activities like monitoring and auditing should be reported directly to the top managers and the board (if applicable). The results should also be shared with all levels of management and the workers covered by the program.

Top-level managers and board members (if applicable) should review in-depth results of monitoring and auditing, including dashboard reports on all program measurements. Management should also periodically discuss the program with employees and worker representatives (if applicable) to get ideas and feedback.

Employers should use monitoring results as a basis for program improvements and accountability. If the results identify problems, employers should determine whether possible system failures led to the problem and make changes to the reporting system if warranted. Managers should create plans to improve work groups or facilities that have trends indicating room for improvement.

How OSHA Can Help

Filing a complaint

Employees who believe that they have been retaliated against in violation of any of the 22 whistleblower protection statutes that OSHA enforces may file a complaint with OSHA. Employees must file a complaint with OSHA before the filing deadline under the relevant statute (filing deadlines vary by statute). For example, a complaint of retaliation under the Occupational Safety and Health Act must be filed within 30 days of the alleged retaliation. For more information about the filing deadlines for the whistleblower statutes that OSHA enforces, view our "Whistleblower Statutes Desk Aid" at www.whistleblowers.gov/whistleblower_acts-desk_reference.pdf.

Complaints may be filed with OSHA by visiting or calling the local OSHA office at 1-800-321-OSHA (6742), or may be filed in writing by sending a written complaint to the closest OSHA regional or area office, or by filing a complaint online at www.whistleblowers.gov/complaint_page.html. Written complaints may be filed by facsimile, electronic communication, hand delivery during normal business hours, U.S. mail (confirmation services recommended), or other third-party commercial carrier.

Further information

For more information on filing a complaint under the 22 whistleblower statutes that OSHA enforces, please visit www.whistleblowers.gov. You can also call OSHA at 1-800-321-OSHA (6742) if you have questions or need more information.

OSHA enforces the whistleblower provisions of the following statutes: (1) Occupational Safety and Health Act (OSHA 11(c)), 29 U.S.C. § 660(c); (2) Surface Transportation Assistance Act (STAA), 49 U.S.C. § 31105; (3) Asbestos Hazard Emergency Response Act (AHERA), 15 U.S.C. § 2651; (4) International Safe Container Act (ISCA), 46 U.S.C. § 80507; (5) Safe Drinking Water Act (SDWA), 42 U.S.C. § 300j-9(i); (6) Federal Water Pollution Control Act (FWPCA), 33 U.S.C. § 1367; (7) Toxic Substances Control Act (TSCA), 15 U.S.C. § 2622; (8) Solid Waste Disposal Act (SWDA), 42 U.S.C. § 6971; (9) Clean Air Act (CAA), 42 U.S.C. § 7622; (10) Comprehensive Environmental Response, Compensation and Liability Act (CERCLA), 42 U.S.C. § 9610; (11) Energy Reorganization Act (ERA), 42 U.S.C. § 5851; (12) Wendell H. Ford Aviation Investment and Reform Act for the 21st Century (AIR21), 49 U.S.C. § 42121; (13) Sarbanes Oxley Act (SOX), 18 U.S.C. § 1514A; (14) Pipeline Safety Improvement Act (PSIA), 49 U.S.C. § 60129; (15) Federal Railroad Safety Act (FRSA), 49 U.S.C. § 20109; (16) National Transit Systems Security Act (NTSSA), 6 U.S.C. § 1142; (17) Consumer Product Safety Improvement Act (CPSIA), 15 U.S.C. § 2087; (18) Affordable Care Act (ACA), 29 U.S.C. § 218C; (19) Consumer Financial Protection Act of 2010 (CFPA), 12 U.S.C. § 5567; (20) Seaman's Protection Act, 46 U.S.C. § 2114 (SPA); (21) FDA Food Safety Modernization Act (FSMA), 21 U.S.C. § 399d; and (22) Moving Ahead for Progress in the 21st Century Act (MAP- 21), 49 U.S.C. § 30171.

OSHA®
www.whistleblowers.gov
(800) 321-OSHA (6742)
OSHA 3905-01/2017

International Labour Organization

IGDS Number 551 (version 2)

Office directive

Date: 5 March 2021

Reporting misconduct and protection from retaliation

I. Introduction

1. In accordance with the provisions of the Constitution of the International Labour Organisation, service with the International Labour Office is subject to the highest standards of conduct and integrity and all staff are required to comply with ILO internal rules and procedures.

2. Providing channels for reporting misconduct ("whistleblowing") and affording protection to staff members who report such cases or cooperate with duly authorized audits or investigations is essential for ensuring respect for applicable standards of conduct and compliance with ILO internal rules and procedures.

3. The present Directive specifies the appropriate channels for reporting misconduct and establishes arrangements for prevention of and protection from retaliation to ensure that all staff can report misconduct and cooperate with audits and investigations without fear of retaliation. The Directive should be read in conjunction with:

   (a) the Staff Regulations;

   (b) the Financial Rules and the Financial Regulations;

   (c) the Standards of Conduct for the International Civil Service issued by the International Civil Service Commission (ICSC); [1]

   (d) the Principles of Conduct for Staff of the International Labour Office; [2]

   (e) Office Directive, *Ethics in the Office*, IGDS No. 76;

   (f) Office Directive, *Anti-fraud and anti-corruption policy*, IGDS No. 69; and

   (g) Office Directive, *Prevention and response to sexual exploitation and abuse*, IGDS No. 568.

4. The Directive is issued pursuant to article 8 of the Constitution of the ILO, article 30 of the Financial Regulations and article 1.2 of the Staff Regulations.

5. The Directive supersedes Office Procedure, *Ethics in the Office: Whistle-blower protection*, IGDS No. 186 (version 1), of 8 September 2010.

[1] The Standards of Conduct are available at www.ilo.org/ethics and on the ICSC website https://icsc.un.org/Resources/General/Publications/standardsE.pdf?r=03326915.

[2] The Principles of Conduct are available at www.ilo.org/ethics.

6. The Directive applies to all ILO staff irrespective of service category or type of contract. It also addresses reporting of misconduct by external parties such as interns, consultants, service providers or implementing partners.

7. This Directive is effective as of its date of issue.

II. Definitions

8. For the purposes of this Directive:

   (i) "Misconduct" is understood as the failure to comply with the Staff Regulations, Financial Regulations, Financial Rules or other relevant internal rules and procedures or to observe the standards of conduct required of an international civil servant. Submission of grievances under Chapter XIII of the Staff Regulations other than harassment grievances under article 13.4 is not considered as reporting misconduct under this Directive.

   (ii) "Retaliation" and "retaliatory action" refers to any direct or indirect detrimental action that adversely affects the employment or working conditions of a staff member, where such action has been threatened or taken for the purpose of punishing, intimidating or injuring an individual because that individual engaged in a protected activity. Retaliation in itself constitutes misconduct and may result in disciplinary or other appropriate action.

   (iii) "Protected activity" is understood as the reporting by staff members of misconduct in good faith and through the channels specified in paragraphs 9–16 below or the cooperation with a duly authorized audit or investigation. The transmission or dissemination of unsubstantiated rumours is not a protected activity. Making a report or providing information that is intentionally false or misleading constitutes misconduct and may result in disciplinary or other appropriate action.

III. Reporting misconduct

Reporting misconduct through internal mechanisms

9. All ILO staff have a duty to report situations involving possible misconduct through the appropriate internal mechanism for receiving such reports as described in the present Directive. [3] Reports may also be received anonymously.

10. The Chief Internal Auditor receives directly from individual staff members reports, complaints or information concerning possible misconduct, [4] including sexual exploitation and abuse of project beneficiaries possibly perpetrated by other staff members, interns, consultants, service providers or implementing partners and their employees. [5] Any such report, complaint or information concerning possible misconduct should be brought to the attention of the Chief Internal Auditor in person, by telephone or in writing, including by email (investigations@ilo.org).

11. The Chief Internal Auditor and the Treasurer (TRCF@ilo.org) receive reports and information concerning any suspected case of fraud, presumption of fraud or attempted fraud. [6]

12. Staff members who consider having been subject to harassment, including sexual harassment, may file a grievance with the Director of the Human Resources Development Department (HRD) under article 13.4 of the Staff Regulations. Other staff members who become aware of situations possibly involving harassment, including sexual harassment, perpetrated by staff members should inform the Director of HRD (HRD@ilo.org).

[3] Standards of Conduct for the International Civil Service, para. 20.

[4] See Standard Operating Procedure Investigations (https://www.ilo.org/global/about-the-ilo/how-the-ilo-works/accountability-and-transparency/iao/WCMS_686602/lang--en/index.htm), Financial Rule 14.30(iii).

[5] Office Directive IGDS No. 568.

[6] Financial Rule 13.10.

13. Situations involving possible misconduct may also be reported by staff to management, including heads of departments, units, bureaux or offices. The managers receiving such reports must forward them immediately to the competent authority indicated in paragraphs 10–12 above. Management should not undertake investigations into the possible misconduct reported, unless it is under the guidance of the Office of the Internal Audit and Oversight (IAO). Staff may also report directly to the competent authorities.

14. Allegations of fraud or other misconduct concerning the Chief Internal Auditor shall be reported to the Director-General, who will inform the Chairperson of the Governing Body and the Chairperson of the Independent Oversight Advisory Committee (IOAC), and will make the appropriate recommendations on how to deal with the allegations. [7]

15. Allegations of fraud or other misconduct concerning the Director-General shall be reported to the Chairperson of the Governing Body, either directly or through the Treasurer, the Chief Internal Auditor, or the Chairperson of the IOAC. [8]

Reporting misconduct through external mechanisms

16. Protection against retaliation will be extended to a staff member who reports misconduct to an entity or individual outside of the established internal mechanisms, where the criteria set out in subparagraphs (a), (b) and (c) below are satisfied:

    (a) such reporting is necessary to avoid:

        (i) a significant threat to public health and safety; or

        (ii) substantive damage to the Organization's operations; or

        (iii) violations of national or international law; and

    (b) the use of internal mechanisms is not possible because:

        (i) at the time the report is made, the individual has grounds to believe that he/she will be subjected to retaliation by the person(s) he/she should report to pursuant to the established internal mechanism; or

        (ii) it is likely that evidence relating to the misconduct will be concealed or destroyed if the individual reports to the person(s) he/she should report to pursuant to the established internal mechanisms; or

        (iii) the individual has previously reported the same information through the established internal mechanisms, and the Office has failed to acknowledge the receipt of the report or to inform the individual, upon her or his request, in writing of the status of the matter; and

    (c) the individual does not accept payment or any other benefit from any party for such report.

17. External reporting by a staff member in accordance with the Directive does not constitute a breach of the staff member's obligations regarding confidentiality and discretion under the Staff Regulations.

IV. Prevention of and protection from retaliation

Action to prevent retaliation

18. The IAO and HRD shall inform the Ethics Officer of any report of alleged misconduct received by them which they consider posing a retaliation risk, subject to the consent of the staff member who made the report.

[7] See Standard Operating Procedure Investigations.

[8] https://www.ilo.org/public/english/edmas/ioac/index.htm.

19. When informed of the risk of retaliation, the Ethics Officer shall consult with the staff member who made the report on appropriate retaliation prevention action. With the person's consent, such action may include engagement by the Ethics Officer with the person's senior management or the Director of HRD to ensure monitoring of the person's workplace situation with a view to preventing any retaliatory action against the staff member as a consequence of her or his engagement in a protected activity.

Request for protection from retaliation

20. Staff members who believe that retaliatory action has been threatened or taken against them because they have reported misconduct or cooperated with an audit or investigation may submit to the Ethics Officer a request for protection against retaliation in person, by phone or in writing, including by email at ethics@ilo.org. They should forward all information and documentation available to them to support their request to the Ethics Officer as soon as possible.

21. The staff member's request for protection must be submitted to the Ethics Officer not later than six months after the date on which the individual knew, or in the opinion of the Ethics Officer should have known, that the alleged retaliation was threatened or taken.

22. Allegations of retaliation concerning the Director-General shall be reported to the Chairperson of the Governing Body either directly or via the Chairperson of the IOAC.

Preliminary review

23. Upon receipt of a request for protection, the Ethics Officer shall send an acknowledgement of receipt to the staff member, register the request and undertake a preliminary review to determine whether:

    (a) the staff member engaged in a protected activity;

    (b) the action alleged to be retaliatory did take place; and

    (c) there is a prima facie case that the staff member's engagement in the protected activity was a contributing factor in causing the action or threat alleged to be retaliatory.

24. The Ethics Officer shall complete the preliminary review within 30 days of receiving all information requested concerning a claim of retaliation. Where in exceptional circumstances the Ethics Officer is unable to conclude the preliminary review within 30 days, she or he shall inform the staff member and set a new timeline.

25. The Ethics Officer shall maintain the confidentiality of all communications received from staff members who request protection against retaliation, and from all relevant third parties. Staff members may authorize the Ethics Officer to contact any office or other staff members to obtain additional information and/or records related to the request for protection.

26. The Ethics Officer may, at any time during the preliminary review period or, as the case may be, during the time period of a subsequent investigation by the IAO as provided below, recommend measures to HRD, or to other relevant units, to protect the staff member from the risk of further retaliation. Such measures can include, but are not limited to, temporary suspension of the implementation of the action reported as retaliatory; with the consent of the complainant, temporary reassignment of the complainant and/or change of reporting lines; or placement of the complainant on special leave with full pay.

27. All offices and staff members shall cooperate with the Ethics Officer and provide access to any and all records and documents requested by the Ethics Officer with the exception of medical records that are not available without the express consent of the official concerned and records that are subject to confidentiality requirements.

Action in case of a prima facie determination of retaliation

28. If the Ethics Officer determines that there is a prima facie case of retaliation or threat of retaliation, she or he shall refer the matter in writing to the IAO for investigation and shall immediately inform the staff member in writing. The IAO shall seek to complete its investigation and submit its report to the Director-General within 120 days, with a copy to the Ethics Officer.

29. Upon receiving the IAO's fact-finding report, the Ethics Officer shall make a determination whether retaliation has occurred or not. Retaliation shall be deemed to have taken place unless it is established with clear and convincing evidence that the Organization would have taken the same action regardless of the protected activity, or that the alleged retaliatory action was not made for the purpose of punishing, intimidating or injuring the staff member. In this respect, this Directive is without prejudice to the legitimate application of regulations, rules and administrative procedures, including those governing evaluation of performance, non-extension or termination of appointment or contract. The Ethics Officer shall, wherever possible within 30 days, inform the Director-General and the staff member of whether or not retaliation is considered to have occurred.

30. If the Ethics Officer considers that retaliation has occurred, his/her recommendations to the Director-General, after consultation with the complainant, may include possible measures aimed at correcting negative consequences suffered as a result of the retaliatory action and protecting the complainant from any further retaliation. These measures may include, but are not limited to, rescission of the retaliatory decision, including reinstatement, or, if requested by the complainant, transfer to another office and/or function and/or change in reporting lines, or subject to due process rights and relevant staff rules, transfer of the person who allegedly engaged in retaliation.

31. The Director-General shall communicate a written decision to the staff member within 60 days of receipt of the Ethics Officer's recommendations, with a copy to the Ethics Officer. The written decision shall inform the staff member of the appeals available in accordance with paragraph 41 below.

Action where there is no prima facie case of retaliation

32. In cases where the Ethics Officer, following the preliminary review of the requests of protection from retaliation, finds that there is no prima facie case of retaliation, the Ethics Officer shall notify the staff member accordingly.

33. Should the Ethics Officer determine in such cases that there is an interpersonal problem within a particular office it may advise the complainant on the available channels for informal conflict resolution, including the Office of the Mediator. The Ethics Officer may also inform the Director-General if she or he considers there to be a managerial problem relating to a particular office.

34. Within 30 days of notification of the determination that there is no prima facie case of retaliation, the staff member may request the Ethics Officer, to refer the matter to an external and independent expert for further review. For this purpose, the Director-General establishes a list of qualified experts with experience regarding protection from retaliation in the UN system.

35. Following receipt of a request for further review, the Ethics Officer shall refer the matter to an expert from the above-mentioned list and shall inform the staff member accordingly. The expert may seek further information from the staff member, the Ethics Officer, and, with the consent of the staff member, other ILO units. The independent expert shall be tasked with making a recommendation as to whether the matter should be referred to the IAO for investigation under paragraph 28 above. If recommended so, the Ethics Officer shall refer the matter for investigation.

Disciplinary action against staff that engaged in retaliation

36. In cases where the Director-General, following the IAO investigation, determines that there had been retaliation, the Director-General will refer the case to the Director of HRD for consideration of appropriate disciplinary action under Chapter XII of the Staff Regulations against the staff member who engaged in retaliation.

37. HRD shall inform the staff member who made the claim of retaliation, the Ethics Officer and the IAO on a confidential basis of any sanction applied to the staff member who engaged in retaliation.

V. Reporting of misconduct by external parties

38. External parties engaged in dealings with the ILO such as interns, consultants, service providers or implementing partners can and are encouraged to report misconduct of ILO staff members to the IAO (investigations@ilo.org). Reports may also be received anonymously.

39. External parties engaged in dealings with the ILO who consider that they have been subject to detrimental action taken by an ILO staff member because they have reported misconduct to the ILO may raise the matter with the Ethics Officer (ethics@ilo.org). The Ethics Officer shall review the matter and refer it to the IAO in case there are reasonable grounds to investigate the matter further. If it is established that any retaliatory measures were taken by an ILO staff member against such an external party because she or he reported misconduct to the ILO, this in itself constitutes misconduct and may lead to disciplinary or other appropriate action.

VI. General matters

Appeals

40. Staff members are reminded that they may file a grievance under article 13.2(1) of the Staff Regulations with HRD on the grounds that they have been treated in a manner incompatible with their terms and conditions of employment, including in order to challenge any action or inaction by the Office that they consider to be retaliatory, within six months of the treatment complained of.

41. A staff member that has sought protection from retaliation under the present Directive may file a grievance against the decision taken under paragraph 31 above to the Joint Advisory Appeals Board (JAAB) within 30 days of its receipt. In the absence of an express decision within the time allowed under the same provision, a staff member may file a grievance with the JAAB within 30 days of the expiration of the time allowed.

Conflict of interest

42. In case the Ethics Officer has a potential, perceived or real conflict of interest preventing the exercise of his or her functions under this Directive in a particular matter, he or she shall recuse him/herself therefrom, and designate an expert from the list referred to in paragraph 34 above to act in his or her stead. The complainant shall be informed accordingly.

43. Where the Ethics Officer or the IAO consider that there may be a conflict of interest in the IAO conducting the investigation into a prima facie case of retaliation, they may recommend to the Director-General that the matter be investigated by a qualified external investigator and inform the staff member that requested protection that such a recommendation was made to the Director-General.

44. In case the Director-General has a potential, perceived or real conflict of interest preventing the exercise of his or her functions related to protection from retaliation in a particular matter, he or she shall recuse him/herself therefrom, and designate another appropriate official to act in his or her stead and inform the Chairperson of the Governing Body and the IOAC of such designation.

Reporting on whistleblowing and retaliation cases

45. Summary information on the reports of misconduct and retaliation received by the IAO is included in the report of the Chief Internal Auditor to the Governing Body.

46. The Ethics Officer makes available information on the number and status of cases of retaliation in the function's Annual Report.

47. Information on sanctions applied to staff members that engaged in retaliatory action is included in the periodic information notes on disciplinary cases issued by the Office.

Information and advice

48. Staff and external parties who wish to seek information and advice with regard to reporting misconduct and available protection from retaliation may contact the Ethics Officer (ethics@ilo.org) or the IAO (investigations@ilo.org).

Review of implementation

49. The Ethics Officer, in consultation with the IAO, HRD, other units concerned and the Staff Union, shall review and assess the terms and implementation of the present Directive every two years, and may make recommendations to the Director-General for its updating, as may be warranted.

Guy Ryder
Director-General

Module No. 5

5.1. Safety and security of employees

The Safety and Security function deals with both enterprise and employee safety and security. It includes the organization's efforts to prevent and/or mitigate loss, risks to or from staff, threats to its physical assets, damage to its technology and intellectual property, or risks of any other kind arising from all elements surrounding the work environment. Safety and security encompasses two overlapping areas of practice, sometimes treated separately and sometimes combined, as appropriate.

WORKPLACE SAFETY

Workplace safety is a process that seeks to eliminate or reduce risks of injury or illness to employees. The chief aim of workplace safety is to protect an organization's most valuable asset—its people. Workplace safety is achieved through a variety of methods, including policies, procedures and specific hazard control techniques.

Policies and procedures are devised and integrated into the organization's overall management and administrative processes. They usually involve specific job task procedures established for working with or around equipment, hazardous environments or other forms of high-hazard conditions. Safety procedures and policies include accountability requirements to ensure that prescribed practices are followed.

Safety professionals apply a well-recognized hierarchy of measures to eliminate or control specific workplace hazards. The measures are applied as part of an orderly decision-making process, as follows:

Substitution. Can the existing process, material or equipment be replaced with a less hazardous process, material or equipment?

Isolation. Can barriers or limits be placed between people and the hazard? This could be physical barriers, time separation or distance.

Ventilation. Can the potential hazardous airborne substances be ventilated through dilution or capture?

Administrative controls. Can the hazards be effectively mitigated through specialized operating practices? Examples include restricting access to certain high-hazard areas to authorized personnel only, adjusting work schedules or adopting preventive maintenance programs to address potential equipment breakdown.

Personal protective equipment. If the preceding methods are not sufficient or feasible, can personal protective equipment be provided (e.g., safety glasses, gloves, hard hats, hearing protection, safety footwear, respirators)?

WORKPLACE SECURITY

The chief aim of workplace security is to protect employees from internal and external security risks. Workplace security has gained much attention in the last several years due to an increase in workplace violence, the necessity of background investigations of prospective and current employees, Internet- and technology-based security needs, threats of terrorism, and increased legal liability to organizations for not taking reasonable measures to safeguard the workplace due to security threats.

Workplace security risks vary depending on an organization's business, its location and its hours of operation. A fundamental element of any workplace security initiative is a security risk assessment. Risks need to be properly identified to establish appropriate methods, either procedural or physical barriers and systems.

The scope of workplace security has continued to expand. Depending on the nature of the business and related security risks, organizations may need to address the following:

- Establishing a formal security function.
- Establishing computer, e-mail, and Internet policies and procedures.
- Including non-compete agreements and other types of clauses in employment contracts for the protection of proprietary information and intellectual property.
- Developing crisis management and contingency plans.
- Establishing theft and fraud prevention procedures.
- Developing workplace violence prevention procedures.
- Installing premises security systems.
- Developing restricted-access policies and key-control procedures.

5.2. Prevention of workplace violence

With violence in society a growing problem, the importance of taking measures to prevent workplace violence has become increasingly urgent to businesses that want to protect the safety of their employees.

According to the Bureau of Labor Statistics, between the years of 2011 and 2018, a total of 5,746 injuries resulting from workplace violence were reported. Of these, 3,584 were workplace homicides and 2,825 of these homicides were the result of a shooting by another person.

While violence is one of the major causes of death in the workplace, nonfatal cases are more common. Overall, the Occupational Health and Safety Administration estimates there are about 2 million cases of workplace violence a year. The surprisingly high number of incidents varies between verbal and physical abuse to homicides. It is also estimated that about 25 percent of workplace violence goes unreported.

These statistics are a strong reminder that violence in the workplace is more common than we might think, but workplaces can take specific measures to prevent and lessen the impact of violence. When you know how to prevent workplace violence, you can be part of the solution and make your company a safer place for all employees.

1. Complete background checks on new employees.

Workplace violence prevention begins with hiring. Conducting a thorough background check on potential employees (after they access a job offer) can reveal whether the candidate has a violent past. If something comes up, ask for an explanation and make sure it's consistent with the report. They that have a recent violence conviction, you may decide to retract the job offer to avoid that kind of behavior in your workplace.

2. Create a policy that prevents harassment.

Harassment is repeated persecution, bullying and/or troubling behavior that intimidates others. It creates an offensive work environment and the behavior often serves as a warning for violence. That's why creating a policy to prevent harassment is a crucial step in preventing the possibility of violence. This policy should include a set of procedures that addresses any workplace complaints efficiently and privately. While creating this policy, it's important to involve each level of the facility, including managers, employees, and executives. Keep all individuals informed by distributing the new policy across your organization and take the time to ensure every employee understands it.

3. Create an effective line of communication.

Effective communication is a key factor in preventing workplace violence. If your employees have access to a workplace communication network, it can help them understand, recognize and report the early signs of potential violence, rather than passively sweeping them under the rug in favor of getting back to work. Giving them access to conflict-resolution resources makes they feel more responsible to communicate. Also, providing an open line of communication to management, HR and other key members of your company will help create an environment where employees can make sure their grievances are heard and properly responded to.

4. Training and awareness are key factors in workplace violence prevention.

Take the time to have training sessions about how to respond to a violent incident so your staff knows how to react when it occurs. ALICE Training teaches people what to do when they recognize danger. Being trained properly so that decisive action can be taken quickly gives a team member the confidence needed to respond in a controlled and responsible way during a violent incident.

5. Establish a strict anti-violence policy.

Prevent workplace violence by creating firm policies that empower your team to report violent and harassing behaviors and other signs of danger. This kind of policy eliminates undesirable employee behavior and leaves no room for favoritism – managers must apply swift and consistent punishment no matter who violates the policy. Make sure all employees are aware of the consequences for violating the policy. This firm stance helps to show your company's commitment to preventing violence.

6. Encourage your employees to accept individual differences.

Personality clashes or leadership style differences exist in every workplace. If left unresolved, these issues could result in job dissatisfaction or depression, and even violence (in the form of verbal abuse, sabotage, or worse). Persistent issues result in high turnover and culture problems or your organization. Help negate conflict by organizing activities to help the tea get to know each other, and acknowledging differences as positive attributes. This could help people see that their individual differences play a vital role in the team's strengths as a whole.

7. Prevent conflicts from turning into harassment or violence.

Tense situations like employee layoffs or firings can create extreme anger. Sometimes, that anger builds a desire to "get revenge." You can help prevent these conflicts from turning into violence by immediately alerting staff and building security of the angry departure to prepare them for possible escalation. This allows them to be on the lookout for ex-employees who return without invitation and be more prepared to take action if needed.

8. Manage visitors and provide security monitoring

Monitoring visitors – and managing them when possible – is a smart way to prevent violence in the workplace. Whether security guards are patrolling your facility/parking lot, capturing video surveillance, or overseeing a visitor check-in desk, these are all extra layers of security that can deter someone from performing a violent incident. This is especially important in situations where people work alone or in confined spaces, or provide services involving money or alcohol. Also consider providing after hours escorts for workers in parking lots who become easier targets when alone.

9. Encourage everyone to report any and all violent incidents.

A great way to start preventing workplace violence is to establish trust between you and your employees. Ensure your employees of the confidentiality in which they can report incidents, and assure each of them that no retaliation will be made against anyone reporting acts of violence.

10. Deter robbers with limited assets on hand.

Workplace violence often occurs in conjunction with crimes like robbery and shoplifting. In fact, 85 percent of workplace homicides fall into this category where the criminal has no known relation to the business or its employees. You can reduce the risk of robbery and potential violence by keeping the amount of assets at your facility to a minimum. Use electronic pay systems to reduce cash on hand and install a locked drop safe. It may also help to keep your facility well lit and ask law enforcement officers to visit occasionally. Always be alert and pay attention to customers acting strangely.

11. Identify organizational risk factors that could lead to violence.

What areas or concerns in your organization are potential risk factors that could lead to workplace violence? When combined with the stress of a personal situation employees bring to work, they may become aggressive and lash out. Assess your operation to become aware of these factors like working while understaffed, inadequate security, the perception that violence is tolerated or that victims are unable to properly report incidents, and many others.

12. After an incident or near miss, perform a thorough analysis.

In the event that your workplace does experience a violent situation or is able to prevent one from occurring, follow up with an analysis. Who was affected and what, if any, warning signs were present? Were existing procedures and operations followed and if not, why? Were team members adequately trained? What new procedures and operations would help to improve staff safety and security? Answering these questions can help you modify your existing plans and ensure your business is able to effectively prevent workplace violence.

5.3. Sexual harassments

Sexual harassment includes unwelcome sexual advances, requests for sexual favors, and other verbal or physical harassment of a sexual nature in the workplace or learning environment, according to the Equal Employment Opportunity Commission (EEOC). Sexual harassment does not always have to be specifically about sexual behavior or directed at a specific person. For example, negative comments about women as a group may be a form of sexual harassment.

Although sexual harassment laws do not usually cover teasing or offhand comments, these behaviors can also be upsetting and have a negative emotional effect.

Some forms of sexual harassment include:

- Making conditions of employment or advancement dependent on sexual favors, either explicitly or implicitly.
- Physical acts of sexual assault.

- Requests for sexual favors.
- Verbal harassment of a sexual nature, including jokes referring to sexual acts or sexual orientation.
- Unwanted touching or physical contact.
- Unwelcome sexual advances.
- Discussing sexual relations/stories/fantasies at work, school, or in other inappropriate places.
- Feeling pressured to engage with someone sexually.
- Exposing oneself or performing sexual acts on oneself.
- Unwanted sexually explicit photos, emails, or text messages.

5.4. Protection from retaliation

Retaliation occurs when an employer punishes an employee for engaging in legally protected activity. Retaliation can include any negative job action, such as demotion, discipline, firing, salary reduction, or job or shift reassignment. But retaliation can also be more subtle.

5.5. HR data security

The 4 most common HR data security issues

Some HR data security threats, such as chatbots, have arisen more recently, while others have been consistent issues for some time. Here are some of the HR data security issues that occur most frequently.

1. Remote work

Remote work is arguably one of the greatest threats to a company's security, and HR employees working outside the office makes it difficult to ensure the security and privacy of sensitive employee records. For example, an HR professional may decide to work for an afternoon at a coffee shop with unsecured Wi-Fi, which could lead to others accessing employee data.

HR management must learn how to properly handle employee data in a remote environment and ensure HR employees are following those best practices.

2. Chatbots

HR departments are now using chatbots for recruitment, benefits process automation and employee interaction. However, chatbots bring security risks.

If employees send sensitive information through chatbot channels, the information could subsequently be exposed via web browser caches and server log files or even exploited via malware.

Employees should carefully consider the data they send using chatbots to attempt to prevent future problems.

Other potential security problems include criminals compromising the chatbot system or creating a fake system to gain further network access and lure unsuspecting users into divulging sensitive information.

3. Employee carelessness

Like other departments, HR can face security risks because of employees not following general cyber security best practices, which could compromise data across the company. However, HR staff are well positioned to help prevent this.

Because HR communicates often with employees about other topics, workers may pay more attention to HR messages about security and privacy. HR staff should take advantage of this and frequently remind company employees about security best practices.

4. HR systems

Some of an enterprise's most vulnerable systems are internal and third-party, or cloud, web applications that process HR and payroll records. Laptops and other mobile devices such as HR professionals' phones and tablets are also vulnerable. Any weakness involving passwords, SQL injection or unencrypted devices presents sizable business risks.

HR staff must alert technical staff about any potential areas of concern. Computer or application vulnerabilities involving authentication, access control and even system oversight -- logging and alerting -- often surface without technical staff being aware of the problem.

5.6. HRM in cross border mergers and acquisitions

The term human resource management (HRM) is used to describe an organization's systematic efforts to shape the actions of its employees. Managing human resources is a crucial strategic challenge for all firms, but especially so for those engaged in cross-border Mergers and Acquisitions, since employee behaviour has a significant impact on profitability, customer satisfaction, and other essential metrics of organizational success. Human resource management encompasses a wide range of actions any company takes, no matter how big or small. Both strategic plans and routine procedures for supervising employees are part of human resource management. All organizations need to have policies in place that lay out the ground rules for managing employees. Mergers and acquisitions are recognized as significant factor that affects talent management strategies. Talent management is all about finding, keeping, inspiring, and rewarding a company's most talented managers so that they can keep up their competitive edge. Human resource management may benefit Mergers and Acquisitions by using talent management initiatives. Retention is a crucial aspect of M&A human resource management. Once the company's leadership has been established, HR professionals should begin working on a plan to keep its most valuable employees from leaving. Many top employees of an acquired organization leave during the acquisition transition because their status is diminished in comparison to the competitors of the acquiring company.

Developing and implementing comprehensive compensation strategies helps to retain talented managers. To ensure the success of the new synergy, it is essential that the leadership team first identifies the most valuable personnel and then designs a remuneration package that will not only keep them happy at work but also substantially motivate them. The acquiring firm's human resources policies and reward system tend to have the most significant impact on winning over the target company's workforce and facilitating a smooth transition. Understanding that pay packages are utilized to incentivize personnel towards the new integrated vision is fundamental to designing effective compensation methods. Appropriate compensation is a well-documented inducement for managers to stay with their organization. In most cases, the most contentious parts of negotiation are the terms of employment, including remuneration, benefits, and retention strategies. The structure of the transaction and the treatment of employees may be affected by the political and legal climate in which the Merger and Acquisition deal is reached. To come up with an effective retention and compensation strategy, HR managers need to be familiar with the functions of unions and the varying approaches to employment relations regulation across countries. For example, the stricter regulations on M&A deals imposed by European Union labour rules make doing business in Europe more difficult than in the United States. This is due to stricter laws and limits on employee dismissals for M&As that occur within European borders. Due to the lack of powerful trade unions like those seen in Europe, the United States has a far more transient approach to hiring and firing.

Effective communication is one of the most important ways for a combined firm to get the most out of its people. To successfully implement an M&A, it is necessary to convince employees that they would personally profit from the company's continued growth. One of the safest and most productive strategies is using numerous communication channels simultaneously. To successfully integrate the two organizations and win over the affected workers' confidence, it's crucial that they have a clear understanding that the integration process is fair, impartial, and reflective of their shared interests. Communication reduces employees' concerns and confusion regarding M&As, builds trust, and promotes integration. The ability to communicate more effectively was determined to be a critical factor in the combined company's success. It was identified that the connection between communication and performance varied between acquirers from different countries. The purchasing business must successfully deal with these difficulties to achieve M&A performance.

The outcome of Mergers and Acquisitions can be affected by human resource management at any time during the procedure. Human resource management's primary concern in the lead-up to a merger is

usually to ensure that all applicable laws and regulations are being followed, particularly those pertaining to equal employment opportunity and collective bargaining agreements. Human resources managers can get to work on the merger preparations immediately after a deal is announced by doing things like handling retention agreements and evaluating pay scale disparities. Human resources managers have been shown to have the most significant impact on Mergers and Acquisitions during the integration phase, which is when M&A processes and policies are put into effect. Human resources managers are crucial after an acquisition, especially if there are cultural differences. In many cases, the type of integration varies from country to country, which will impact business practices and policies.

5.7. Motives behind mergers and acquisitions

1. Value creation

Two companies may undertake a merger to increase the wealth of their shareholders. Generally, the consolidation of two businesses results in synergies that increase the value of a newly created business entity. Essentially, synergy means that the value of a merged company exceeds the sum of the values of two individual companies. Note that there are two types of synergies:

- **Revenue synergies**: Synergies that primarily improve the company's revenue-generating ability. For example, market expansion, production diversification, and R&D activities are only a few factors that can create revenue synergies.
- **Cost synergies**: Synergies that reduce the company's cost structure. Generally, a successful merger may result in economies of scale, access to new technologies, and even elimination of certain costs. All these events may improve the cost structure of a company.

2. Diversification

Mergers are frequently undertaken for diversification reasons. For example, a company may use a merger to diversify its business operations by entering into new markets or offering new products or services. Additionally, it is common that the managers of a company may arrange a merger deal to diversify risks relating to the company's operations.

Note that shareholders are not always content with situations when the merger deal is primarily motivated by the objective of risk diversification. In many cases, the shareholders can easily diversify their risks through investment portfolios while a merger of two companies is typically a long and risky transaction. Market-extension, product-extension, and conglomerate mergers are typically motivated by diversification objectives.

3. Acquisition of assets

A merger can be motivated by a desire to acquire certain assets that cannot be obtained using other methods. In M&A transactions, it is quite common that some companies arrange mergers to gain access to assets that are unique or to assets that usually take a long time to develop internally. For example, access to new technologies is a frequent objective in many mergers.

4. Increase in financial capacity

Every company faces a maximum financial capacity to finance its operations through either debt or equity markets. Lacking adequate financial capacity, a company may merge with another. As a result, a consolidated entity will secure a higher financial capacity that can be employed in further business development processes.

5. Tax purposes

If a company generates significant taxable income, it can merge with a company with substantial carry forward tax losses. After the merger, the total tax liability of the consolidated company will be much lower than the tax liability of the independent company.

6. Incentives for managers

Sometimes, mergers are primarily motivated by the personal interests and goals of the top management of a company. For example, a company created as a result of a merger guarantees more power and prestige that can be viewed favorably by managers.

Such a motive can also be reinforced by the managers' ego, as well as their intention to build the biggest company in the industry in terms of size. Such a phenomenon can be referred to as "empire building," which happens when the managers of a company start favoring the size of a company more than its actual performance.

Additionally, managers may prefer mergers because empirical evidence suggests that the size of a company and the compensation of managers are correlated. Although modern compensation packages consist of a base salary, performance bonuses, stocks, and options, the base salary still represents the largest portion of the package. Note that the bigger companies can afford to offer higher salaries and bonuses to their managers.

Achieve faster growth

The major benefit of a merger or acquisition deal can be calculated by evaluating the **growth graph**. Such deals have the potential to exponentially increase the growth of the company due to the high rise of the resources.

It is just simple math that when 2 companies combine, then their corresponding **assets**, as well as **market share**, are also merged and this widens opportunities for growth. And the increased market power is directly proportional to more yearly **turnovers**.

Attain positive synergy

The concept of synergy states that the combined return of two companies will be greater than the sum of the returns of the companies as individuals. A merger & acquisition process helps to increase the company's performance for its **shareholders**.

The potential synergy from the merger & acquisition between two or more companies is **evaluated** before the **final agreement** is signed. Positive and greater synergy is often the main motive for a merger or acquisition.

Exploitation of the market

No market is perfect and there are always **loopholes** that businesses utilize for their own **profit**. Acquiring or merging of two similar companies help to form a dominant place in the existing market. This allows them to achieve a **monopoly** over its **competitors**.

A merger & acquisition deal also increases the **market power** of the involved companies by reducing their dependence on other companies for raw materials. There is enough scope for a company to have authority over:

Facilitates transfer of technology

When the two companies involved in a merger & acquisition are **technology-driven**, then a possible motive is the transfer of technology. The companies must be using unique technologies and sharing them could empower them a larger market share.

Developing new technologies may require a lot of time and revenue, which may not prove profitable. Through mergers and acquisitions, the development process can be done in a easier and **cost-effective** manner.

Achieve diversification

Mergers and acquisitions allow companies to attain diversification in their business. There are both **risks** and profit in acquiring different businesses. Entering into different fields helps the company to maintain a positive impact in the **share market**.

Suppose, there is a drop in one business and rise in another, then the company has an option to recover from the profitable business. So, it is better to invest in acquiring for diversifying your **business portfolio**, rather than being stuck with a single platform.

5.8. HR Interventions

HR Interventions targeted at developing , Integreting and supporting the employees in an organization. Theses Interventions operates on the premise that employee development and well being can lead to increased organizational performance.

Human process interventions

Human process interventions are the earliest and most well-known OD intervention types related to interpersonal relations, group, and organizational dynamics. It is important to note that, though concerned with improving workforce performance; organizational development strategy should not be mistaken for human resource development. HR development focuses more on an employee's personal growth, whereas human process interventions focus on developing the organization's processes to improve organizational effectiveness. There are many different human process interventions but let's expand on four.

1. Individual interventions

These interventions are targeted at the individual employee, often around improving communication with others. During this intervention, the individual will be given direction to better understand their own and others' emotions, motivations, and behaviors. The employee may also have support to identify their career needs, set complementary career goals, and resolve conflict.

A real-world example is Amazon, which recently stated that its organization would *"spend more than $700 million to provide 100,000 employees with new skills for the digital age by 2025,"* according to an article from CBSNews. The number of companies investing in individual interventions will continue to climb to retrain its workforce to stay competitive in the changing economy.

2. Group interventions

OD group interventions help teams and groups within a company become more effective. These interventions are usually aimed at the group's content, structure, or processes.

For example, to understand more about the group, the department responsible for OD will ask team members to analyze their group's performance, what the team needs to do to improve, and discuss possible solutions to any challenges they have.

3. Team building

Team building is one of the best-known organizational development interventions. It refers to activities that help teams improve productivity, communication, performance, and employee engagement.

4. Intergroup relations interventions

Inter-group interventions are incorporated into OD strategy to facilitate collaboration and efficiency between different teams within a business towards a common goal. You can generally see these interventions in larger companies when departments need to fight for limited resources or are unaware of each other's needs.

How does this work in an organization? First, different team leaders/managers are brought together to make sure they are committed to the intervention. Then, the teams make a list of their feelings about the other team. After, the groups will meet to share their lists with each other. And lastly, the teams meet to discuss the problems and to find possible solutions that will help both squads.

5. Technostructural interventions

The significance of technology in business cannot be understated. Organizations worldwide rely on new technologies to help improve their competitive advantage and drive growth. Technostructural interventions focus on

improving organizational effectiveness and employee performance by focusing on technology and the structure of the organization.

6. Organizational (structural) design

Organizational design refers to how an organization is structured to achieve its strategic plan and goals. This structure is essential to how the company will operate. There are many different classifications of organizational structure, such as hierarchical, divisional, matrix, process, customer-centric, and network.

According to Deloitte, nowadays, *"companies are decentralizing authority, moving toward product- and customer-centric organizations, and forming dynamic networks of highly empowered teams that communicate and coordinate activities in unique and powerful ways."*

Within OD strategy, organizational design is about reengineering and rightsizing. Therefore, an organization needs to rethink how it works and restructure it around the new business methods.

7. Total quality management

Total quality management is also known as continuous process improvement, lean, and six-sigma. It is an approach that seeks to improve quality and performance by placing customer satisfaction at the center. To achieve this, there is a strong focus on complete employee involvement in the ongoing improvement of products, processes, and workplace culture.

Ford Motor Company is one of the best-known companies to practice TQM. They had a vision of developing better products, having a more stable environment, effective management, and increasing profitability. Ford's Chief Engineer at the time, Art Hyde, used the DMAIC (Define, Measure, Analyze, Improve, and Control) process to detect problems before selling the product to the consumer.

8. Work design

Work design impacts an organization's outcomes, with well-designed work contributing to improved productivity and financial growth. It can also affect how an employee feels about their job, such as if they feel motivated, engaged, bored, or stressed at work.

Sometimes, an organization needs work redesign to achieve its goals. That's where the techno-structural interventions come in. However, redesigning work doesn't necessarily require company-wide changes to the way things are done. Instead, small changes to the way tasks are completed, or the way employees communicate at work can have substantial outcomes for both staff and the organization.

9. Job enrichment

According to American psychologist Frederick Herzberg, job enrichment aims to enhance job efficiency and employee satisfaction by creating a more significant scope of more challenging work, greater autonomy, better professional achievement, and recognition, as well as more opportunities for advancement and growth.

Examples of job enrichment that you can implement in your business are:

- **Variety of tasks.** Give your employee new tasks or ones that go beyond their everyday duties.
- **Giving autonomy.** Empower employees to make decisions about their work.
- **Employee feedback**. Make sure your team receives input regarding their performance, skills, and ability to work within a group.
- **Assigning meaningful work.** Help employees make sense of their work by showing them how it benefits the company and how they contribute to overall organizational goals.
- **Creating incentive programs.** Create recognition for a job well done through incentive programs like bonuses or extra days off.

10. Transformational change

Transformational changes are those you make to thoroughly reshape your business strategy and processes, which often results in a shift in work culture. Some examples of transformational change are

- **Restructuring:** Changing your business's structural chart by adding, removing, or combining departments.
- **Retrenchment:** Decreasing employee headcount by closing an office or division of the company.
- **Turnaround:** Replacing all top management within a failing business to turn things around.

- **Outsourcing:** Hiring another company to complete tasks for your own company. This is common in customer service departments.
- **Spin-off:** Breaking up a company into distinct, smaller companies. Google is well-known for this when it created its umbrella organization, Alphabet Inc., and now owns many household name companies such as Nest and YouTube.

11. Continuous change

This intervention encourages companies to improve gradually over time by making small changes. The best-known example of continuous change is a learning organization. Businesses that shift from the top-down hierarchical structure to a learning model have a higher chance of collaboration, risk-taking, and growth and are more competitive in the ever-changing work environment.

In addition, this technique places importance on experimentation and learning from mistakes and failures rather than punishing them.

12. Trans organizational change

Trans organizational change involves interventions that include two or more organizations. This can be in the form of mergers or acquisitions but also businesses working together to achieve their objectives.

13. Wellness interventions

A wellness intervention combines strategies developed to create behavior changes or improve health status and wellbeing among individual employees or the entire staff. Organizations need to understand their teams' specific needs. It is vital to pinpoint which wellness interventions would best serve their needs and allow the individual to learn to manage their own health and wellbeing.