COSMOS
Navigate the Compliance Universe

Corporate Compliance Forms and Tools
Compliance Program Risk Catalog and Assessment

The following is a general— not exclusive—list of potential compliance risk areas that an organization may face. Choose a likelihood (L) and impact (I) scale (e.g., 1–5 or 1–10) and calculate total inherent risk (L times I) based on input received from subject matter experts and interviews with different portions of your organization.

Assess the effectiveness of your controls (E) using the same numeric scale you chose for likelihood and impact, again based on input from subject matter experts and interviews with different business functions, and then subtract the effectiveness (E) from the inherent risk to determine your residual risk (R) for each risk event.

You can then use a heat map or other visual scale to depict the top risks for your organization. You may decide to conduct this assessment on an enterprise basis, a regional basis, a department or business unit basis, a country-level basis etc. It may be conducted annually, biannually, on a quarterly basis, or some other cadence. Choose the scope and cadence that best suits the needs of your organization.

Category	Risk Event	Likelihood (L)	Impact (I)	Inherent Risk (L x I)	Controls Effectiveness (E)	Residual Risk (R)
Accounting fraud/earnings management	Financial statement inaccuracy					
	Embezzlement					
	Books and records inaccuracy or off-the-books accounts					
	Revenue or cost figure manipulation					
Antitrust/competition law	Collusive conduct (e.g., price-fixing, bid-rigging, market allocation)					

	Unfair business practices or business torts (e.g., disparagement, inducing breach of contract, theft of trade secrets)					
	Monopolization or abuse of dominant market position					
	Price discrimination					
	Failure to make required pre-merger notifications					
	Prohibited tying or bundling of products					
Confidential information	Use of the confidential information of others					
	Failure to protect the organization's own confidential information					
	Inappropriate gathering of competitive information					
Conflicts of interest	Excessive entertainment given to or accepted from suppliers or service providers					
	Excessive gifts or gratuities given to or accepted from suppliers or service providers					
	Ownership interests in competitors, suppliers, or service providers					

	Conflicting outside employment					
	Co-opting of the organization's opportunities for personal gain					
	Family members reporting to each other					
Consumer protection and treatment/advertising	Discrimination against customers					
	Failure to provide accommodations for customers under the Americans with Disabilities Act					
	Consumer safety issues					
	Deceptive sales practices					
	Inaccurate advertising, including inaccurate pricing					
	Weight and measure accuracy					
	Failure to comply with telemarketing or mail order sales rules					
	Product warranty issues					
Record management/retention	Failure to retain documents as part of litigation holds					

	Use of ephemeral messaging apps that do not create a business record to conduct business					
	Failure to retain and destroy documents in accordance with record retention policy					
Employment and labor	Failure to accommodate employees under the Americans with Disabilities Act					
	Failure to accommodate employee religious practices and beliefs					
	Inaccurate or missing I-9 documentation and/or employment of ineligible persons					
	Failure to comply with National Labor Relations Board regulations related to unions and organizing					
	Failure to comply with Employee Retirement Income Security Act relating to employee benefits					
	Failure to comply with Family and Medical Leave Act					
	Discrimination in the workplace					
	Failure to abide by requirements of the Worker Adjustment and Retraining Notification Act					
	Failure to provide appropriate leave for military or military reserve service					

	Substance abuse by employees in the workplace, creating unsafe working conditions					
	Risk of gender-based pay gaps and discrimination					
Harassment	Sexual harassment of employees					
	Harassment of employees based on other protected class (e.g., gender, age, sexual orientation, religion, veteran status, pregnancy)					
	Failure to provide state-manded training to prevent harassment (e.g., California and Illinois)					
Workplace violence and security	Negligent hiring or failure to conduct adequate background checks					
	Failure to prevent weapons in the workplace					
	Failure to detect and prevent the potential for violence in the workplace					
Workplace safety and health	Failure to comply with federal Occupational Safety and Health Administration (OSHA) regulations, including injury reporting and remedying of unsafe conditions					
	Failure to comply with state OSHA regulations					

Wages and hours/Fair Labor Standards Act	Failure to comply with regulations related to hours of work, overtime, minimum wage, exempt status, and child labor					
Environmental	Failure to comply with Toxic Substances Control Act, including asbestos remediation					
	Failure to comply with regulations controlling the shipment of hazardous materials					
	Failure to dispose of hazardous substances in compliance with the Resource Conservation and Recovery Act					
	Failure to comply with the requirements of the Clean Air Act, including permit and reporting requirements					
	Failure to comply with requirements of the Clean Water Act, including permitting and release notification					
	Failure to comply with local right to know laws relating to environmental issues					
	Failure to remediate and report any underground tanks on company property					
	Failure to abide by endangered species or wildlife regulations					

	Risk of being identified as a responsible party under the Comprehensive Environmental Response, Compensation, and Liability Act for a superfund cleanup site					
Government contracting	Illegal bid-rigging					
	Violation of the Anti-Kickback Statute					
	Fraud or false claims, including failure to properly document costs for cost-plus contracts					
	Record keeping or time recording violations					
	Failure to abide by "revolving door" limitations related to the hiring of former government employees					
	Giving of gifts or entertainment to government employees in violation of applicable laws					
	Failure to comply with requirements of the Office of Federal Contract Compliance Programs, including affirmative action requirements					
	Failure to abide by Made in USA requirements for federal contracts					
	Failure to comply with requirements of the Defense Contract Management Agency					

Government investigations and dealings	Failure to timely respond to an inquiry from a government agency					
Intellectual property	Infringement on intellectual property of another, including software, copyrights, patents, and trademarks					
	Theft or misuse of the proprietary information of others					
	Use of music or other intellectual property without proper license					
Trade compliance	Failure to comply with Foreign Corrupt Practices Act and other bribery and corruption prevention laws					
	Failure to comply with Export Administration Regulations, International Traffic in Arms Regulations, and other export control laws					
	Failure to comply with Office of Foreign Assets Control regulations and other economic sanction and boycott laws					
	Failure to comply with U.S. Customs and Border Protection regulations, tariff, and other import laws					
	Failure to comply with national security and espionage prevention laws					

	Failure to abide by anti-money laundering, know-your-customer, and other financial regulations					
	Risk of underpayment of duties and penalties resulting therefrom					
	Risk of fraud or corruption by customs brokers and service providers					
Political contributions/lobbying	Failure to abide by lobbying, reporting, and disclosure laws and limitations					
	Failure to abide by political action committee rules and limitations					
Product warranty and safety	Failure to comply with product warranty requirements, including reporting and disclosure requirements					
	Product safety issues and violations					
	Quality control issues resulting in consumer complaints or litigation					
Privacy	Failure to abide by jurisdiction-specific regulations (e.g., General Data Protection Regulation, California Consumer Privacy Act)					
	Failure to provide privacy and opt-out notices for consumers					
	Failure to protect employee privacy					

	Failure to provide required disclosures and notices related to monitoring of employee email and instant messages					
	Failure to discover a data breach					
	Failure to provide timely notice to regulators of a data privacy breach					
	Reputational damage resulting from data breach					
	Consumer complaints and litigation resulting from a data breach					
Supply chain	Risk of undisclosed conflicts of interest resulting in self-dealing and unnecessarily high pricing					
	Risk of employees demanding a kickback in order to choose or continue to use a supplier					
	Risk of supply chain disruptions due to weather, climate change, labor shortages, or other issues					
	Risk of human trafficking and forced labor in your supply chain and reputational damage resulting therefrom					
	Risk of supplier insolvency					
	Risk of supplier quality issues or fraud					

	Risk of fraud, accidents, or safety violations by logistics, transportation, and warehousing service providers					
	Risk of using conflict minerals in the manufacture of goods					
Taxes	Improper reporting and payment of sales and use taxes					
	Failure to account for duty impact of advanced transfer pricing agreements entered into with foreign tax officials					
	Errors in employee tax withholding					
	Use of aggressive tax deferral and savings strategies that carry risk of regulatory scrutiny and penalties					
Securities laws	Errors in compliance with Section 16 of the Securities Exchange Act					
	Risk of insider trading					
	Failure to comply with Sarbanes–Oxley internal control requirements					
	Failure to comply with stock exchange disclosure, reporting, and listing requirements (e.g., New York Stock Exchange, NASDAQ)					

	Failure to abide by internal governance requirements (e.g., board of directors, shareholder meeting, and other similar requirements)					
	Failure to abide by employee stock plan requirements					
	Failure to abide by executive compensation disclosure and calculation requirements					
Industry-specific regulations	Consider whether your industry has specific regulatory requirements that create additional risk in the event of noncompliance: • Pharmaceuticals • Aviation • Securities • Healthcare • Banking • Power/energy • Telecommunications • Agriculture • Food processing and safety • Transportation • Technology • Education					