

TRAINING COURSES — Summaries

Discrimination and Harassment

Anti-Harassment Policy Certification
Preventing Discrimination and Harassment
Questionable Interview Questions
Workplace Bullying
Workplace Diversity

Financial Integrity

Avoiding Insider Trading
Finance Basics for Managers
Fraud Awareness and Detection
Internal Controls
Money Laundering
Regulation FD

General Business

Antitrust Basics
Appropriate Internet Use
Careful Communication
Code of Conduct
Compliance Certification
Conflicts of Interest Questionnaire
Contract Law Basics
Ethics and Compliance Basics
FAR Code of Conduct

Healthcare

Healthcare Fraud and Abuse
Whistleblowing (Deficit Reduction Act) Compliance

Data Privacy and Security

CPNI
FACTA "Red Flags"
Gramm-Leach-Bliley Act (GLBA) Privacy
HIPAA Privacy and Security
Information Security
PCI-DSS Compliance
Protecting Personal Information
Record Management
Safe Harbor Privacy Primer

International Business

Canadian Competition Law
EU Competition Law
Export Controls Basics
Foreign Corrupt Practices Act/Anti-Corruption
OFAC Sanctions and Trade Embargoes

Workplace

Americans with Disabilities Act
Fair Labor Standards Act (FLSA)
Family and Medical Leave Act (FMLA)
HazCom/Right To Know
Maintaining a Cooperative Workforce
Preventing Workplace Violence

Americans with Disabilities Act

The Americans with Disabilities Act (ADA) was enacted in 1990 with the goal of ending discrimination against individuals with disabilities. Title I of the ADA prohibits employers from discriminating in all aspects of the employment relationship — application, testing, medical examinations, hiring, training, assignments, evaluations, disciplinary actions, promotions, layoffs and terminations, as well as compensation, leave and other benefits. The ADA was revised substantially in 2009.

Since the law went into effect, enforcement by the U.S. Equal Employment Opportunity Commission (EEOC) has resulted in payments of more than \$300 million by businesses to more than 20,000 individuals. Recent cases resulting in punitive-damage awards up to \$13 million make the importance of understanding and complying with the ADA clear.

Course Summary

This 35-minute course explains the basic requirements of the ADA in simple, understandable terms. It includes pop-quizzes, news clippings and a final quiz highlighting real-world compliance issues that employees should learn to recognize and deal with appropriately.

The topics covered in the course include —

- Overview of the ADA
- Persons with disabilities
- Impairments
- Major life activities
- Records and perceptions of a disability
- Essential job functions
- Reasonable accommodation
- Undue hardship
- Qualification standards
- Safety standards
- The hiring process
- Medical exams and questions
- The ADA on the job
- Evaluations and promotions

Anti-Harassment Policy Certification

Most organizations now understand the importance of (a) having an anti-harassment policy and (b) being able to show that employees were made aware of the policy and the complaint procedure. For many organizations, computer-based policy-certification and training are de rigueur — or at least should be. WeComply offers a top-notch online course developed in collaboration with Proskauer Rose LLP, a preeminent labor and employment law firm.

But for organizations with large numbers of employees who don't have computer access or skills, e-learning may not be an option. While some of these organizations have managed to push policies and training out to their far-flung workforce, proving that particular employees received them has been nearly impossible. This can leave these organizations defenseless before the EEOC or a jury — even when they had done all the right things.

WeComply developed a telephone-based anti-harassment policy certification to address this problem. From any phone, employees call a toll-free number and follow the IVR (interactive-voice-response) prompts to authenticate themselves. They are then engaged in an interactive quiz and policy certification that takes about five minutes. Results are tracked just like an online WeComply training course and reported in real-time to your organization's training administrator. (Employees who do have computer access/skills can do the same certification online if they prefer.)

Course Summary

This five-minute Certification provides trackable proof that employees received, read and agreed to abide by your organization's anti-harassment policy. It also quizzes employees on basic issues of what harassment is, what a victim should do about it, and what your organization will do in response to a complaint. Finally, it provides employees with an option to report an incident of discrimination or harassment.

The certification is available in English and Spanish. It can be customized and/or made available in other languages if needed.

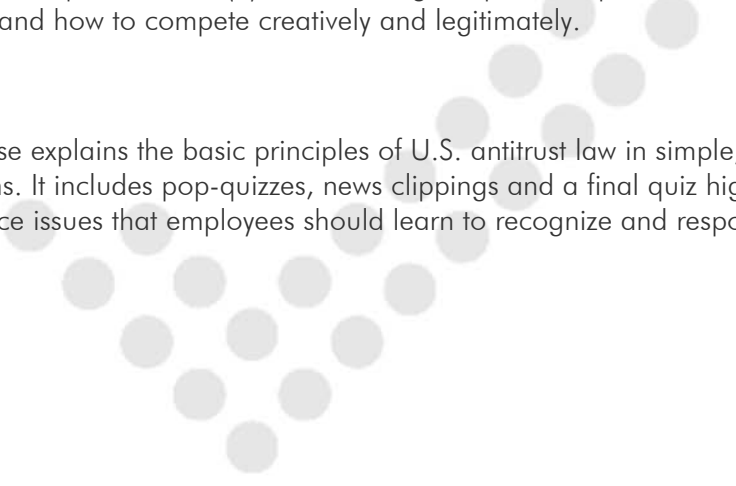
Antitrust Basics

As the complexities of the business world multiply, so do potential antitrust problems for a business enterprise up and down its organizational chain. An intricate web of federal, state and international statutes and regulations poses significant dangers for both intentional and inadvertent antitrust violations — organizations are fined, mergers and acquisitions are thwarted, enormous litigation costs pile up, and people go to jail. Just as important, organizations and their employees become afraid to be inventive, aggressive and competitive in completely legitimate ways.

Thus, it is crucial that organizations train their employees on the basic what, why and how of antitrust enforcement: (1) what are the basic legal principles, and what problems can occur in the real world in dealings with colleagues, customers, competitors, suppliers and business partners; (2) why is compliance with antitrust law important to your organization's business goals and the free-enterprise system in general, and why avoiding violations and civil and criminal penalties is so important; and (3) how to recognize potential problems and deal with them appropriately, and how to compete creatively and legitimately.

Course Summary

This 40-minute course explains the basic principles of U.S. antitrust law in simple, understandable terms. It includes pop-quizzes, news clippings and a final quiz highlighting real-world compliance issues that employees should learn to recognize and respond to appropriately.



Antitrust Basics (cont'd.)

The topics covered in the course include —

- Overview of U.S. antitrust law
- Recognizing "red flags"
- Relationships with competitors
- Price-fixing
 - Allocating markets or customers
 - Boycotts
 - Other improper competitor contacts
 - Price-related restrictions
 - Geographic or customer restrictions
- Relationships with customers
 - Exclusive dealing
 - Tying
 - Reciprocal dealing
 - Dual Distribution
- Mergers and acquisitions
 - Pre-merger reporting
 - Pre-closing sharing of information
- Monopolistic behavior
 - Predatory pricing
 - Refusals to deal
- Price discrimination
 - Meeting competition
 - Promotional services
- Exemptions from the antitrust laws
 - Lobbying activities
 - Labor-related activities
 - State action
 - Regulated industries
- Special industries
 - Insurance
 - Healthcare
- Antitrust in other contexts
 - Government contracting
 - Foreign trade

Appropriate Internet Use

Without a doubt, the Internet has revolutionized the workplace. According to the Pew Research Center, 62% of American employees now use the Internet for their work, with 27% reporting "constant" use. With an Internet connection, a laptop or netbook, and a cell phone or PDA, many employees are fully equipped for their work wherever they are. Indeed, nearly half of employed Americans now work from home at least some of the time — and 18% do so every day or almost every day.

But with all of the potentially positive uses of the Internet come potential abuses, as well. Of 1,200 companies surveyed about Internet usage, 54% reported that they had caught employees browsing Web sites that were unrelated to their work — some up to eight hours per day! Another survey found that of the 30% of employers who fire employees for web-related violations, 84% cited the reason as the viewing or uploading of inappropriate material.

In addition, improper or indiscriminate use of e-mail, text- or instant-messaging, postings to blogs, Facebook, Twitter, etc., can lead to issues of workplace discrimination (including sexual harassment), copyright infringement, securities-law violations, antitrust violations, the loss of company trade secrets, and many other legal and practical problems.

Course Summary

This 30-minute course explains the basic rules and guidelines for appropriate use of the organization's electronic-communication systems. The topics covered in the course include —

- Overview
- E-communications
- Monitoring and access
- Personal use
- Social networking
- Inappropriate communications
- Prohibited Internet use
- Passwords
- Working remotely
- Violations

Avoiding Insider Trading

Investing in the stock market has become an important factor in the financial lives of millions of people across many income levels. News reports of fortunes being won and lost in the stock market can tempt employees to try to capitalize on "inside" information that they learn at work before it is available to the general public. But whether these employees buy or sell stock themselves or "tip" others to do so, their activities could violate federal securities laws and lead to severe fines and even prison sentences — for themselves, their supervisors, friends and family, and their company.

Thus, it is essential that public companies — and businesses that come in contact with material, nonpublic information about public companies — provide their employees with a basic understanding of insider-trading law and policy.

Course Summary

This 25-minute course explains the laws prohibiting insider trading in simple, understandable terms. It includes pop-quizzes, news clippings and a final quiz highlighting real-world compliance issues that employees should learn to recognize and respond to appropriately.

The topics covered in the course include —

- Overview of insider trading
- What information is "material"?
- What is "non-public" information?
- Who may be liable for insider trading?
- Civil and criminal penalties for insider-trading violations
- Insider trading and Regulation FD

Canadian Competition Law

Canada's Competition Act is the oldest competition statute in the western world. Although similar to its U.S. corollary — known as "antitrust law" — Canada's competition law differs in several important respects and was amended substantially in 2009.

As commerce becomes increasingly global, an understanding of the laws of various countries is necessary to do business and avoid unnecessary litigation, fines and even prison. A web of international rules poses significant dangers for both intentional and inadvertent competition-law violations. Consequently, organizations and their employees may become afraid to be inventive, aggressive and competitive in completely legitimate ways.

Thus, it is crucial that organizations train their employees on the basic what, why and how of competition-law enforcement: (1) what are the basic legal principles, and what problems can occur in the real world in dealings with colleagues, customers, competitors, suppliers and business partners; (2) why is compliance with antitrust law important to your organization's business goals and the free-enterprise system in general, and why avoiding violations and civil and criminal penalties is so important; and (3) how to recognize potential problems and deal with them appropriately, and how to compete creatively and legitimately.

Course Summary

This 35-minute course explains the basic principles of Canadian competition law in simple, understandable terms. It includes pop-quizzes, news clippings and a final quiz highlighting real-world compliance issues that employees should learn to recognize and respond to appropriately.

Canadian Competition Law (cont'd)

The topics covered in the course include —

- Overview of Canadian competition law
 - Relationships with competitors
 - Price-fixing
 - Market allocation
 - Bid-rigging
 - Boycotts
 - Agreements about quality or quantity
 - Reviewable trade practices
 - Market restriction
 - Refusals to deal
 - Resale price maintenance
 - Exclusive dealing
 - Tied selling
 - Abuse of dominance
 - Price discrimination
 - Predatory pricing
 - Promotional allowances
 - Merger control and review
- 

Careful Communication

With the arrival of the Information Age and the explosion of high technology, communication is getting faster but not necessarily better. Many employees believe that if they act with integrity and simply follow their bosses' or customers' instructions, their good intentions will keep their communications from becoming a legal "smoking gun."

In reality, however, nothing could be further from the truth. Almost everything an employee says or does on behalf of his or her organization can be used as evidence against the individual and/or the organization at a later date. Documents, both paper and electronic, create a paper trail that lawyers can use to "connect the dots" to paint a picture that may not be very pretty. But by following a few simple guidelines, such as those outlined in this course, these dangers can often be reduced or eliminated.

Course Summary

This 30-minute course explains the following eight tips for avoiding — or at least minimizing — the many lurking "smoking guns" of business communications:

- Recognizing that you can't always know your audience
- Understanding the law that applies to your organization's business
- Recognizing the limits of your own knowledge
- Meaning what you say and saying what you mean
- Managing the closure process
- Being consistent with record retention
- Understanding the attorney-client privilege
- Working to improve your writing

Code of Conduct Training

It's widely agreed that every company needs to have a policy statement on legal and ethical conduct. The Organizational Sentencing Guidelines require that a company "must have taken steps to communicate effectively its standards and procedures to all employees and other agents, e.g., by requiring participation in training courses or by disseminating publications that explain in a practical manner what is required." Thus, if a company hopes to qualify for more lenient treatment under the Guidelines in the event of employee or corporate misconduct, having, disseminating and enforcing a Code of Conduct are essential.

Think about it — in most companies, a new employee is given a copy of the Code on his or her first day of work, signs the acknowledgment page, and puts the Code in a bottom desk drawer, never to be opened again. But if legal or ethical issues arise down the road, what standard of conduct will the company be held to? The Code of Conduct. Code of Conduct training lifts your company's Code out of employees' bottom drawers and makes it a resource for dealing with important issues that arise in the workplace.

Course Summary

This 40-minute course provides basic training on the most important topics found in almost every company's Code of Conduct. The topics covered in the course include —

- Honesty and fairness
- Diversity and respect
- Conflicts of interest
- Information security
- Business records
- Electronic communications
- Health, safety and the environment
- Alcohol and drug abuse
- Workplace violence
- Political activity
- Insider trading
- Fair disclosure
- Anti-competitive conduct
- Bribery and kickbacks
- Sanctions and trade embargoes
- Working with integrity
- Reporting violations
- Acknowledgment

Compliance Certification

More and more companies are instituting annual compliance certification by managers as part of their corporate-governance process. For global companies, this can be a daunting task — disseminating the certification in multiple languages worldwide, following up to ensure a timely 100% completion rate, reporting on the results, and identifying and responding to exceptions.

Use our fully automated Compliance Certification module to implement your process electronically — with customized questions and policy links, periodic e-mail "reminders," and real-time tracking and reporting of responses — in as many languages as you need.

Your process may require more of managers than a simple acknowledgment that they read company policies. Use our Certification module to ask as many multiple-choice questions and/or solicit as many free-form text responses as your needs dictate. Include "trigger questions" to make it easy for managers to complete the Certification in a matter of seconds if they have no exceptions to report.

You can customize the questions to survey employees about conflicts of interest, get feedback on training courses they've taken, solicit suggestions for improvement, etc. You can roll out the Compliance Certification module by itself, or append it seamlessly to annual Code of Conduct training — whichever will make your job easier!

Course Summary

This two-minute Certification addresses the topics listed below. Where employee responses indicate an exception, they are asked to provide details.

- Whether the employee conducted his/her business practices in accordance with the Code of Conduct;
- Whether the employee is aware of any business-practice issue that has not been addressed or properly resolved;
- Whether the employee feels he/she can openly discuss business-practice concerns without fear of retaliation; and
- Code of Conduct acknowledgment.

Conflicts of Interest Questionnaire

More and more companies are instituting an annual conflicts-of-interest questionnaire by employees as part of their corporate-governance process. For global companies, this can be a daunting task — disseminating the questionnaire in multiple languages worldwide, following up to ensure a timely 100% completion rate, reporting on the results, and identifying and responding to exceptions.

Use our fully automated Conflicts of Interest Questionnaire to implement your process electronically — with customized questions and policy links, periodic e-mail "reminders," and real-time tracking and reporting of responses — in as many languages you need. You can customize it to ask as many multiple-choice questions and/or solicit as many free-form text responses as your needs dictate. Include "trigger questions" to make it easy for managers to complete the Questionnaire in a matter of seconds if they have no exceptions to report. Roll out the Questionnaire by itself, or append it seamlessly to annual Code of Conduct training — whichever will make your job easier!

Course Summary

This two-minute Questionnaire addresses the topics listed below. Where employee responses indicate an exception, they are asked to provide details.

- Whether the employee or a family member works for anyone that does or is seeking to do business with the organization;
- Whether the employee or a family member has accepted benefits from anyone that does or is seeking to do business with the organization;
- Whether the employee has disclosed confidential information outside of the scope of his/her employment or used such information in any way to promote his/her own interest or the interests of others;
- Whether the employee or a family member has any other interest or arrangement that may represent a conflict of interest; and
- Conflicts of interest policy acknowledgment.

Contract Law Basics

Business people deal with contracts in many different contexts — purchasing, sales, marketing, distribution, employment and others — almost every day. A contract serves, in effect, as the "private law" of the parties on whatever subjects it covers. This is a powerful tool, since the law gives parties tremendous flexibility in defining their contractual relationships. Whatever terms the parties agree to include (within broad legal limits) define their respective rights and obligations for the duration of the contract.

Because every valid contract gives rise to legal rights and obligations, it is important to understand how contracts are (and are not) formed and enforced. Dire consequences may await those who fail to form a valid contract when intended, or who bind themselves or their organization to a contract inadvertently.

Course Summary

This 35-minute course provides an overview of contract law — what makes a contract valid and enforceable, what remedies are available in the event of a breach, and what employees should look for in their real-world dealings with business contracts. The topics covered in the course include —

- What is a contract?
- Forming a contract — the offer
- Responding to an offer
- Consideration
- Defenses to enforcement
- Breach
- Remedies
- Important contract terms
- Real-world considerations

Customer Proprietary Network Information (CPNI)

Pursuant to the Telecommunications Act of 1996, the Federal Communications Commission (FCC) requires that telecommunications companies protect consumer privacy by (1) obtaining customer approval before divulging customer proprietary network information (CPNI); and (2) using certain specified security measures. In 2007 the FCC issued security rules that included customer authentication and notification requirements.

All telecommunications employees with access to consumer data are required to receive annual training on the proper handling of CPNI in both sales transactions and everyday customer interactions. A telecommunications company's failure to provide its employees with this training puts the company at risk of substantial FCC fines.

Course Summary

This 30-minute course explains the legal requirements for how CPNI can be used and accessed, including the rules contained in the FCC's 2007 order on protecting the confidentiality of call-detail information.

The topics covered in the course include —

- What is CPNI?
- The Telecommunications Act of 1996
- FCC rules
- Telecommunications service categories (TSCs)
- Other CPNI use
- Customer approval
- Opt-out and opt-in customers
- Informed consent
- Authentication requirements
- Customer account passwords
- Changes to accounts
- Security breaches
- Recordkeeping
- Annual certifications
- Enforcement

Ethics and Compliance Basics

Reinforcing ethical principles and educating employees about compliance with the law are ongoing and important responsibilities. An organization is only as ethical and compliant as its officers, managers and employees. Training is helpful for encouraging appropriate behavior, setting expectations, demonstrating the organization's commitment, and informing employees of laws or regulatory principles that may not be common knowledge.

Integrity and scruples not only keep us out of court and out of prison, but they are good for business. One study found that companies making "an explicit commitment to doing business ethically" have produced profit/turnover ratios at 18% higher than those without a similar commitment. Conversely, a bad reputation can ruin a business.

Course Summary

This 35-minute course is, in essence, a "Code of Conduct Training" course for organizations that do not have a formalized Code of Conduct. It covers the same legal/ethical/compliance principles, but without reference to a Code.

The topics covered in the course include —

- Honesty and fairness
- Diversity and respect
- Conflicts of interest
- Information security
- Business records
- Electronic communications
- Health, safety and the environment
- Alcohol and drug abuse
- Workplace violence
- Political activity
- Anti-competitive conduct
- Bribery and kickbacks
- Working with integrity
- Reporting violations

EU Competition Law

As the complexities of the business world multiply and commerce becomes increasingly global, the need to understand issues of antitrust law — commonly referred to as "competition law" in the European Union — becomes more important. A web of international rules poses significant dangers for both intentional and inadvertent competition-law violations. As a result, businesses and their employees may become afraid to be inventive, aggressive and competitive in completely legitimate ways.

Thus, it is crucial that organisations doing business in the EU and/or with EU member states train their employees on the what, why and how of competition-law enforcement: (1) what the basic legal principles are, and what problems can occur in the real world in dealings with colleagues, customers, competitors, suppliers and business partners; (2) why compliance with competition law is important to your organisation's business goals and the free-enterprise system in general, and why avoiding violations and civil and criminal penalties is so important; and (3) how to recognize potential problems and deal with them appropriately, and how to compete creatively and legitimately.

Course Summary

This one-hour course explains the basic principles of EU competition law in simple, understandable terms. It includes pop-quizzes, news clippings and a final quiz highlighting real-world compliance issues that employees should learn to recognize and respond to appropriately.

EU Competition Law (cont'd)

The topics covered in the course include —

- Introduction to the European Union
 - EU institutions
 - Enforcement of competition law
 - Consequences of non-compliance
 - Overview of EU competition law
 - Article 101 TFEU: purpose and rationale
 - What is an anti-competitive agreement?
 - Consequences of Article 101 violations
 - Recognising "red flags"
 - Relationships with competitors
 - Cartels, price-fixing, market-sharing, etc.
 - Vertical agreements
 - Verticals Block Exemption Regulation
 - Resale price maintenance, market-partitioning, etc.
 - Relationships with licensees
 - Article 102 TFEU: abuse of market dominance
 - Investigation and enforcement
 - "Dawn raids"
 - Leniency programme
 - The need for "careful communication"
- 

Export Control Basics

Exporting — that is, the shipment or transmission of items or material outside of the U.S. — is heavily regulated by federal laws and regulations referred to collectively as "export controls." These controls affect the export of commodities (goods and materials), technology (technical data and know-how) and software from the U.S. to a foreign country. They also affect the re-export of any such U.S. items from one foreign country to another, as well as products made outside the U.S. by or for a U.S. company.

In recent years, the government has stepped up its enforcement of export controls — 50% in 2007 alone. At the same time, the government has increased penalties dramatically. Fines for intentional violations have jumped from \$50,000 to \$1 million per violation, while fines for other violations have increased from \$11,000 to the greater of \$250,000 per violation or twice the value of the improper export transaction.

Course Summary

This 35-minute course provides an overview of U.S. export controls and the most common "red flags" — situations presenting a risk of export-control violations. It includes pop-quizzes, news clippings and a final quiz highlighting real-world compliance issues that employees should learn to recognize and deal with appropriately.

The topics covered in the course include —

- Overview of export controls
- Export control agencies
- What is an "export"?
- Defense exports under the ITAR
- Commercial exports under the EAR
- Anti-boycott and embargo rules
- Recordkeeping and reporting
- Red-flag issues
- Penalties

FACTA Red Flags

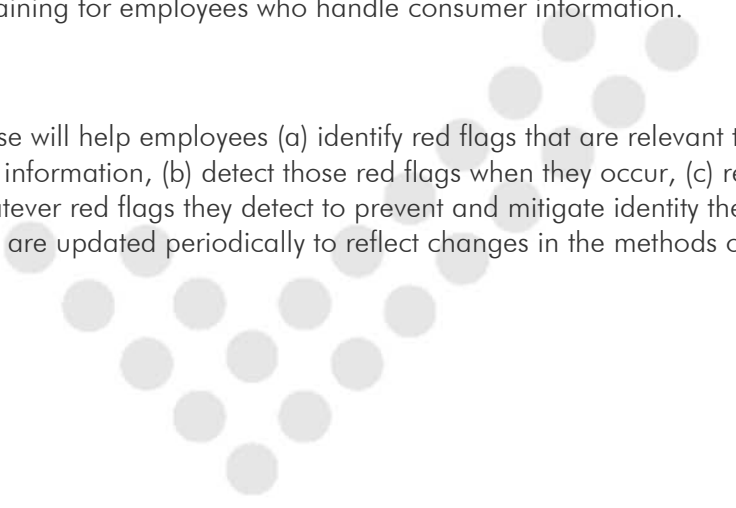
Identity theft is a huge problem for consumers and the companies that serve them. In the U.S. alone, five percent of adults — about 10 million — are victimized each year, with total losses of about \$50 billion. U.S. companies spend another \$50 billion a year on identity-theft-prevention measures.

Companies that handle personal and business account information are a common target of identity thieves. If these companies aren't careful with this information, they can be used as instruments of identity theft by clever criminals. But if they are alert to the "red flags" of identity theft, they can do much to prevent it, detect it early if it does occur, and mitigate the damage it can cause.

New Federal Trade Commission (FTC) regulations under the federal Fair and Accurate Credit Transactions Act (FACTA) require companies to have an Identity Theft Prevention Program that includes "red flag" training for employees who handle consumer information.

Course Summary

This 40-minute course will help employees (a) identify red flags that are relevant to their handling of account information, (b) detect those red flags when they occur, (c) respond appropriately to whatever red flags they detect to prevent and mitigate identity theft, and (d) ensure that red flags are updated periodically to reflect changes in the methods of identity theft.



FACTA Red Flags (cont'd)

The topics covered in the course include —

- What is identity theft?
- Fighting identity theft with FACTA
- Identifying and detecting red flags
- Warnings from consumer reporting agencies
- Suspicious documents
- Suspicious personal identifying information
- Suspicious account activity
- Notice or alerts of identity theft
- Low-tech red flags
- Responding to red flags
- Other information-security practices
- Address discrepancies
- Change of address requests
- Identity theft — a moving target



Fair Labor Standards Act (FLSA)

Consider this: In a recent decision, a federal appellate court upheld a \$24,000 judgment against a property-management company for failing to pay overtime to one employee as required by the Fair Labor Standards Act (FLSA). In another case, a maid service was ordered to pay almost \$4.5 million in back wages and other damages to 385 employees; when it failed to pay those damages, the court ordered to it pay thousands of dollars per day in additional fines. The FLSA is definitely a trap for the unwary — and unethical — employer.

The FLSA is arguably the labor law most often violated by employers. Violations are likely to become even more prevalent as Congress and the courts broaden the scope of the law to apply to more types of workers. As the make-up of a company's workforce becomes increasingly varied, it is more crucial than ever to be aware of how the FLSA works.

Course Summary

This 30-minute course explains the basic requirements of the FLSA in simple, understandable terms. It includes pop-quizzes, news clippings and a final quiz highlighting real-world compliance issues that employees should learn to recognize and deal with appropriately.

The topics covered in the course include —

- An overview of the FLSA
- Minimum-wage requirements
- Overtime rules and how overtime pay is calculated
- Employees who are exempt from the requirements of the FLSA
- What workers are considered independent contractors under the FLSA
- Restrictions on the use of child labor
- Recordkeeping requirements
- Penalties for violations of the FLSA
- FLSA hot spots

Family and Medical Leave Act

The Family and Medical Leave Act (FMLA) was passed in 1993 and expanded in 2008 and 2009. It guarantees employees a certain amount of unpaid annual leave for medical reasons, the birth or adoption of a child, exigencies related to a family member's active-duty military service, or caring for a relative who suffered serious injuries or illnesses during military service. In addition, employers generally must maintain insurance coverage for employees who are on FMLA leave and must reinstate them to the same or equivalent job positions when their leave concludes.

Familiarity with the FMLA is important for two reasons. First, knowing the eligibility requirements and reinstatement policies will help your organization minimize the disruption caused by employees who must be absent from work for family or medical reasons. Second, failing to abide by the provisions of the FMLA can expose an organization to significant legal liability.

Course Summary

This 40-minute course explains the basic requirements of the FMLA in simple, understandable terms. It includes pop-quizzes, news clippings and a final quiz highlighting real-world compliance issues that employees should learn to recognize and deal with appropriately.

The topics covered in the course include —

- An overview of the FMLA
- The scope and coverage of the FMLA
- Covered employers
- Eligible employees
- Entitlement to leave
- Spouses with the same employer
- Paid leave
- Intermittent leave and reduced schedules
- Serious health conditions
- Certification
- Company notice requirements
- Employee notice requirements
- Continuing benefits
- Job restoration
- Other issues

FAR Code of Conduct

In 2007 the U.S. Department of Defense, the General Services Administration and the National Aeronautics and Space Administration developed a set of rules for federal contractors and subcontractors to (1) adopt and promote a Code of Business Ethics and Conduct, and (2) implement internal controls to encourage the reporting of misconduct through awareness training, among other things.

These rules are part of the Federal Acquisition Regulation (FAR) and serve as a guide for all federal contractors and subcontractors. They are mandatory when (1) the value of the contract is expected to exceed \$5,000,000, and (2) the performance period is 120 days or more.

Course Summary

This 40-minute course provides basic FAR Code of Business Ethics and Conduct training on the most essential government-contracting topics. The topics covered in the course include —

- Federal Acquisition Regulation
- Honesty and fairness
- Communication with government customers
- Pricing Mandates
- Government supply contracts
- Other government contracts
- Conflicts of interest
- Rules for procurements
- Hiring government employees
- Record management
- Cooperation with government audits
- Improper Payments
- Lobbying restrictions
- Violations
- Retaliation
- Acknowledgment

Foreign Corrupt Practices Act/Anti-Corruption

With the increasing globalization of our economy, companies are faced with new challenges, as well as new opportunities. Part of this new environment is compliance with laws such as the Foreign Corrupt Practices Act, or FCPA, that regulate the way U.S. companies transact international business. Enacted in 1977, the FCPA was a response to government findings that hundreds of U.S. companies, including many of the Fortune 500, were using cash and "slush funds" to make questionable or illegal payments to foreign government officials, politicians and political parties. The purpose of the FCPA is to halt the bribery of foreign officials and restore public confidence in the integrity of the American business system.

Recent international initiatives, including the Inter-American Convention against Corruption and the OECD's Convention on Combating Bribery of Foreign Public Officials in International Business Transactions, have refocused the world's attention on anti-corruption issues. Major U.S. trading partners are enacting legislation similar to the FCPA. These international efforts to battle corruption mean that U.S. companies can compete on the merits with increasing certainty that they will not be undercut by a competitor's illicit payment to a foreign-government purchaser. They also mean that there is an increased emphasis on enforcement of anti-corruption legislation worldwide, and particularly of the FCPA within the U.S., making company compliance more important than ever.

Course Summary

This 35-minute course explains FCPA and global anti-corruption measures in simple, understandable terms. It includes pop-quizzes, news clippings and a final quiz highlighting real-world compliance issues that employees should learn to recognize and respond to appropriately. The topics covered in the program include —

- FCPA overview
- Why anti-corruption is important
- Scope of the FCPA
- Prohibited recipients and payments
- Intent and the "knowing" standard
- Due diligence and "red flags"
- Exceptions and defenses
- Accounting and recordkeeping
- Penalties for FCPA violations

Finance Basics for Managers

Many of the important decisions that an organization makes depend on its current and future financial health. Every manager needs a working knowledge of finance and accounting principles to understand and contribute effectively to the organization's decision-making and management processes.

It is not at all unusual for there to be a "cultural divide" between the accounting department and the rest of an organization. Because accounting deals with an organization's past performance, it is fairly precise and conservative in nature. An organization uses the financial information prepared by its accountants to make forecasts and budgets, which tend to be imprecise and more optimistic in nature. The better an organization's managers understand the financial aspects of the operation, the better their chances of bridging this divide.

Course Summary

This 30-minute course explains the basics of finance in simple, understandable terms. It includes pop-quizzes, news clippings and a final quiz highlighting real-world finance issues that managers should be conversant with.

The topics covered in the course include —

- Understanding financial information
- The balance sheet
- The income statement
- Statement of cash flows
- Other information sources
- Analyzing financial information
- Return on investment
- Using financial information
- Budgeting
- Managing for profitability

Fraud Awareness and Detection

Corporate fraud is on the rise. Losses attributable to corporate fraud were estimated at \$600 billion in 2002, up from \$400 billion in 1996. Employee theft alone costs American businesses between \$60 and \$120 billion a year. Aside from unscrupulous employees and third parties, a major contributing factor to corporate fraud is simply a lack of awareness of it.

Dishonest employees prey on unsuspecting co-workers and supervisors, and clever third parties use so-called "social engineering" tactics to penetrate a company's defenses. Because successful fraud schemes are hard to detect, everyone from rank-and-file employees to executives needs at least a basic knowledge of how these schemes work and what the warning signs are.

Course Summary

This 35-minute course is intended not only to instill in employees a sense of responsibility to comply with the law and report misconduct, but also to make employees aware of fraud so that it can be detected and nipped in the bud. The course covers the most common types of fraud used to siphon millions of dollars from corporations every day.

The topics covered in the program include —

- Fraud overview
- Billing schemes and their warning signs
- Skimming
- Check tampering and its warning signs
- Red flags of bribery and kickbacks
- Expense-reimbursement schemes
- Payroll fraud
- Non-cash misappropriations
- Cash larceny
- Social engineering
- Reporting fraudulent conduct

GLBA Privacy Primer

Advances in "information technology" have enabled companies to collect, compile, analyze and deliver data around the world much more quickly and cheaply than ever before. These advances have given consumers better access to information, and they've given companies lower-cost and better-targeted opportunities to market and provide their goods and services.

But these technological advances have also brought new challenges to protecting information privacy. In response, Congress passed the "Financial Services Modernization Act" (also known as the Gramm-Leach-Bliley Act (GLBA) after its Senate sponsors), which imposes significant information-privacy requirements on a broad array of "financial institutions." The GLBA applies not only to banks, securities firms and insurance companies, but also to other providers of financial products and services — retailers issuing credit cards, money transmitters, check cashers, mortgage brokers, real-estate settlement services, appraisers, tax-preparation services, and even online companies that offer aggregation, funds-transfer or payment services.

Course Summary

This 30-minute course explains the most important GLBA requirements in simple, understandable terms. It includes pop-quizzes, news clippings and a final quiz highlighting real-world compliance issues that employees should learn to recognize and deal with appropriately.

The topics covered in this course include —

- Overview of the GLBA
- Protected information
- Notice of usage
- Opt-out choice
- Opt-out exceptions
- Delivering notice
- Protecting personal information
- Social engineering
- Unauthorized access and misuse
- Providing notice of an incident
- Enforcement

HazCom/Right To Know

More than 30 million American workers are exposed to hazardous chemicals in their workplaces. To ensure that workers are informed about these chemicals and any health and safety hazards they present, the federal Occupational Safety and Health Administration (OSHA) developed standards for "Hazard Communication" (also known as "HazCom") covering some 650,000 chemical products found in more than three million workplaces.

HazCom/Right To Know affects all employees, regardless of their position, job function or responsibility. Besides providing important workplace safety procedures, HazCom/Right To Know is the law. The failure to offer required training or comply with applicable laws and regulations can lead to substantial fines and penalties.

Course Summary

This 30-minute course is intended to provide the information and training on HazCom required by OSHA regulations (and New York State "Right To Know" laws). The topics covered in the course include —

- What's ahead...
- Purpose
- Chemical basics
- Recognizing chemical hazards
- Hazardous chemicals in your workplace;
- Material Safety Data Sheets (MSDS);
- Reading labels and tags
- Preventing chemical exposure
- Dealing with chemical exposure
- Other employer responsibilities

Healthcare Fraud and Abuse

According to the Government Accounting Office, healthcare fraud and abuse account for three to ten percent of all healthcare costs — well over \$100 billion annually. Whatever the cost, fraud and abuse waste much-needed resources and seriously undermine our healthcare system.

The healthcare industry is subject to many different laws that concern fraud, including the False Claims Act, the Stark Law, the Anti-Kickback Statute, HIPAA and the Prescription Drug Marketing Act. On top of this legislative infrastructure, government agencies and trade organizations have created a patchwork of guidelines and codes. Together, these laws, guidelines and codes present a significant compliance challenge.

Course Summary

This 40-minute course explains the basic rules regarding healthcare fraud and abuse in simple, understandable terms. It includes pop-quizzes, news clippings and a final quiz highlighting real-world compliance issues that employees should learn to recognize and deal with appropriately.

The topics covered in the course include —

- Fraud and abuse overview
- Possible penalties
- Fraud and abuse contexts
- Gifts and business courtesies
- Free goods and services
- Discounts and rebates
- Price reporting
- Administrative fees to GPOs
- Purchasing from customers
- Preceptorships
- Educational grants
- Support of scientific research
- Sponsorships of charitable activities

HIPAA Privacy and Security

The privacy and security of personal information is something everyone should be concerned about. This is especially true in the area of healthcare, where individuals share details of their health, personal lives and finances when they are at their most vulnerable. The Health Insurance Portability and Accountability Act ("HIPAA") addresses these issues by imposing stringent privacy and security requirements on healthcare providers and their business associates.

Newly revised federal regulations require "covered entities" — healthcare providers, health insurance plans, healthcare clearinghouses, and "business associates" who contract with these entities — to create and implement information-security policies covering protected health information that is electronically transmitted or maintained. The work needed to comply with these regulations presents a tremendous challenge for all organizations that handle healthcare information.

Course Summary

This 40-minute course explains the basic principles of HIPAA privacy and security in simple, understandable terms. It includes pop-quizzes, news clippings and a final quiz highlighting real-world compliance issues that employees should learn to recognize and respond to appropriately.

The topics covered in the course include —

- What is HIPAA?
- Who is subject to HIPAA?
- Protected health information (PHI)
- HIPAA privacy
- Notice of privacy practices
- Reasonable safeguards
- Using PHI for marketing
- HIPAA security
- Administrative safeguards
- Physical safeguards
- Technical safeguards
- Handling PHI
- Security breach
- PHI rights of individuals
- Enforcement

Information Security

Along with music and movies, information is increasingly digital, making it easy to transmit and copy — and easy to misuse. While the entertainment industry scrambles to find ways to protect its copyrights, other organizations are likewise struggling to protect their confidential information and to keep pace with the increasingly stringent laws that protect consumer and employee privacy.

Although teenage hackers from faraway countries make the headlines, ordinary breaches of information security often start with things such as an intruder in the workspace, an unscrupulous co-worker or a stolen laptop. A password scrawled on a post-it note under an employee's desk or an un-shredded, discarded memo may be the keys to security breaches that cause grave damage to an organization's financial status and reputation.

Laws such as HIPAA and the Gramm-Leach-Bliley Act demand that employees take specific precautions with certain types of personal information they handle. But even organizations that are not subject to these laws must be sure that their employees understand and follow internal policies for protecting proprietary and/or confidential data in all forms.

Course Summary

This 30-minute course explains the basic principles of information security in simple, understandable terms. It includes pop-quizzes, news clippings and a final quiz highlighting real-world compliance issues that employees should learn to recognize and respond to appropriately.

The topics covered in the program include —

- Information security overview
- Electronic IDs and passwords
- Avoiding identity theft
- Information classification
- Computer viruses and hoaxes
- E-mail and Internet use
- Extra e-mail precautions
- Workspace security
- Social engineering
- Business continuity plans

Internal Controls

Good internal controls help assure the accomplishment of an organization's goals and objectives while protecting its employees and assets. Internal controls provide reliable financial reporting for management decisions, and they ensure compliance with applicable laws and regulations. Poor or excessive internal controls reduce productivity, increase the complexity of everyday transactions, and add no value to the organization's activities.

An important aspect of every internal-controls program is to train employees so that they have a solid awareness and understanding of internal-control standards. Employees who recognize their role in the organization's internal-controls course can help prevent problems from occurring and detect issues as they arise.

Course Summary

This 30-minute course explains the basics of internal controls in simple, understandable terms. It includes pop-quizzes, news clippings and a final quiz highlighting real-world internal-control issues that employees should learn to recognize and deal with appropriately.

The topics covered in the course include —

- What are internal controls?
- Types of controls
- Internal-control standards
- Risk
- Handling risk
- Security
- Employee responsibilities
- Wrap-up

Maintaining a Cooperative Workforce

The National Labor Relations Act (NLRA) grants labor unions the legal status to represent a particular workforce when certain conditions are met. A bill before Congress called the "Employee Free Choice Act" (EFCA) may soon amend the NLRA to make unionization easier and more likely.

Regardless of EFCA, unions appear to be gaining in popularity already. In 2007, U.S. union membership rose for the first time in more than 25 years and has continued to rise since. Consequently, many employers are preparing themselves for increased unionization efforts.

Statistics show that employees choose to unionize when they feel that they are receiving unequal treatment and a lack of respect, rather than because of wages or benefits.

Course Summary

This 40-minute course explains how managers can help create a more respectful work environment so that employees will not feel compelled to join a union. It also details the effects of unionization and ways to respond to unionization efforts without violating the NLRA.

The topics covered in the course include —

- Overview of labor unions
- Effects of unionization
- Recognizing unionizing efforts
- Responding to unionizing efforts
- Employee Free Choice Act
- Team-oriented management
- Fostering a supportive workplace
- Effective communication
- Feedback and reviews

Money Laundering

Have you ever seen a drug dealer pull out a credit-card machine to accept payment for a dime bag? Ever known someone to pay for a TV they bought off the back of a truck with a personal check? Probably not. Most criminals conduct their business in cash. This creates an obvious problem — cash is bulky, heavy and risky to carry around. (One million dollars in twenties weighs about one hundred pounds.) As a result, criminals need to find a way to "launder" their ill-gotten gains. "Money laundering" is the process that criminals use to disguise the true origin and ownership of cash by introducing it into legitimate enterprises. Laundering money is a lucrative and sophisticated business, both in the U.S. and overseas. Some sources estimate that more than \$300 billion is laundered annually worldwide.

You might say, "We're not a bank, so why do we need to be worried?" There are several reasons why it is important to have some familiarity with the money-laundering process, the laws that make it illegal, and our legal responsibilities to help prevent it. As banks and financial institutions become more closely scrutinized by law enforcement in connection with money-laundering activity, criminals are forced to become more creative in finding ways to introduce their ill-gotten gains into the legitimate economy. Increasingly, they are using other types of businesses in the laundering process. Therefore, every organization is more vulnerable than ever.

Course Summary

This 30-minute course is intended to familiarize employees with the process of money laundering and the laws that make it a crime. The topics covered in the course include —

- Defining "money laundering"
- The money-laundering process
- Section 1956 of the Money Laundering Control Act
- Section 1957 of the Money Laundering Control Act
- Reporting requirements
- Anti-structuring rules
- Red flags
- Tips for preventing money laundering

OFAC Sanctions and Embargoes

The U.S. Government has used economic sanctions and trade embargoes since its earliest days to further various foreign-policy, national-security and safety objectives. These sanctions programs are administered by the Office of Foreign Assets Control (OFAC), a division of the U.S. Department of the Treasury.

Every U.S. company and citizen must comply with all applicable sanction and embargo regulations. This means that people and companies subject to OFAC regulations are prohibited from facilitating or assisting foreign companies with transactions in which they themselves could not participate directly. Violations of OFAC sanctions programs can lead to substantial criminal and civil penalties for the company — and in some cases the individual employees involved.

Course Summary

This 30-minute course provides an overview of OFAC sanctions programs and their key provisions and targets. It includes pop-quizzes, news clippings and a final quiz highlighting real-world compliance issues that employees should learn to recognize and deal with appropriately.

The topics covered in the course include —

- Overview of OFAC regulations
- Who must comply
- Key terms
- Targets
- Specially Designated Nationals
- Reporting and recordkeeping requirements
- Penalties for noncompliance
- Practical application of OFAC regulations

PCI-DSS Compliance

The Payment Card Industry Data Security Standard (PCI-DSS) was adopted in 2004 by five major credit-card companies. Its purposes are to promote consistent global security standards and to protect cardholder data from fraud and security breaches. All merchants or service providers who store, process or transmit payment card account numbers are subject to PCI-DSS.

PCI-DSS is not just a technical concern. Its compliance mandates are also directed at "low-tech" positions, such as cashiers or anyone else who processes credit-card information. Even with all the right technical safeguards, human error or ignorance can be the cause of severe security lapses.

A security breach can affect the whole organization in profound ways — fines, loss of reputation or business, and even our ability to accept major payment cards, to name a few. This course instructs employees who handle payment-card information how to do so in accordance with PCI-DSS.

Course Summary

This 40-minute course will explain the basic principles of PCI-DSS compliance and how they apply on the job. The topics covered in the course include —

- An overview of PCI-DSS
- PCI-DSS objectives and requirements
- Costs of non-compliance
- Sensitive Authentication Data
- Hard-copy storage
- Protecting cardholder information
- Payment-card transactions
- Remote access
- Good work practices
- Security incidents
- Restricted computer access
- Restricted physical access
- Tracking and monitoring
- Social engineering

Preventing Discrimination and Harassment

Dating back to the late 1800s, common law in the U.S. defined the employment relationship as "at will," meaning that employers were free to hire and fire at will. Employers could, for example, refuse to hire minorities, segregate the workforce, assign unpleasant work to women, and deny such groups opportunities for advancement. That's all changed. Federal laws now prohibit discrimination and harassment in the workplace on the basis of age, sex, race, religion, national origin, disability, pregnancy and genetic information, and some state and local laws protect even more characteristics.

Training employees to prevent workplace discrimination and harassment is nothing less than essential. Not only can workplace discrimination and harassment affect employee productivity, it can divert resources from the organization's real business. Improper conduct can also lead to liability for the organization and/or individual employees for workplace discrimination and harassment. The U.S. Supreme Court has established legal standards that employers must meet to avoid — or at least minimize — incidents of discrimination and harassment and avoid liability for punitive damages. Employee training is a key part of the defense.

Course Summary

There are separate training courses for managerial (45 minutes) and nonmanagerial (35 minutes) employees. Both include pop-quizzes, news clippings and a final quiz highlighting real-world compliance issues that employees should learn to recognize and deal with appropriately.

Preventing Discrimination and Harassment (cont'd)

The "employee" course covers the following topics:

- Reasons for concern
- Anti-discrimination laws
- Sexual harassment defined
- Types of sexual harassment
- Walking the fine line
- Consensual relationships
- Considering all of the circumstances
- Conduct to be avoided
- Internet and e-mail harassment
- Other protected characteristics
- Other conduct to be avoided
- Retaliation
- What you should do
- Maintaining a respectful work environment

The "manager" course covers the topics listed above and the following additional topics:

- Liability for supervisor misconduct
- Liability for other misconduct
- Supervisor responsibilities
- Set the right tone
- Document employee actions
- Documentation tips
- Respond properly to complaints
- Assist with the investigation
- Prevent retaliation

Preventing Workplace Violence

Every workday 16,400 threats are made, and 723 workers are attacked. One of four full-time workers has been harassed, threatened or attacked on the job. Workplace violence, which costs American businesses an estimated \$36 billion annually, is the second leading cause of job-related deaths for all workers (behind only motor-vehicle deaths) and the leading cause for women. No wonder the Centers for Disease Control has called workplace violence "epidemic."

There are often signposts — clues — that point toward potential violence, if only we know where to look. Employees can, with proper training, learn to spot those clues and forestall violent acts.

Course Summary

This 35-minute course is intended for all audiences, including employees of both private- and public-sector organizations. The topics covered in the course include —

- What is workplace violence?
- Types of violence
- Risk factors
- Prevention methods
- Security measures
- Zero tolerance
- Red flags
- Dealing with a volatile situation
- Weapons
- Reporting procedures
- Response plan
- Other elements

Protecting Personal Information (Massachusetts 201 CMR 17.00)

Identity theft is a huge problem for consumers and the companies that serve them. In the U.S. alone, five percent of adults — about 10 million — are victimized each year, with total losses of about \$50 billion. U.S. companies spend another \$50 billion a year on identity-theft-prevention measures.

In response, the Commonwealth of Massachusetts now requires organizations that handle the "personal information" of any Massachusetts resident to implement certain safeguards to protect that information against identity theft and other misuse. The Massachusetts data-security regulation (201 CMR 17.00) requires that employees receive training annually on administrative, technical and physical safeguards for the handling of such information.

Course Summary

Using the new Massachusetts data-security regulation as a framework, this 25-minute course explains the basic principles of protecting the personal information of all individuals, regardless of their state of residence. It includes pop-quizzes, news clippings and a final quiz highlighting real-world compliance issues that employees should learn to recognize and respond to appropriately.

The topics covered in the course include —

- Overview
- What information is covered?
- Why is this important?
- Physical safeguards
- Administrative safeguards
- Technical safeguards
- Encryption
- Handling personal information
- Electronic ID and passwords
- Social engineering
- Security Incidents

Questionable Interview Questions

Many aspects of employment are heavily regulated in the U.S., but none more than the interviewing and hiring process. State and federal statutes and court decisions prohibit employers from discriminating against certain groups of people and from taking actions that impact those groups adversely and unfairly.

Employees involved in the recruiting, interviewing and hiring process need to be aware of the laws that govern the questions they ask applicants so that they can (1) avoid the questions that could get them or your organization into legal trouble, and (2) phrase their questions within legal limits to elicit the information the organization needs.

Course Summary

This 30-minute course explains the key issues of employment-discrimination law in simple, understandable terms. It includes pop-quizzes, news clippings and a final quiz highlighting real-world interviewing issues that employees should learn to recognize and deal with appropriately.

The topics covered in the course include —

- Overview
- Federal anti-discrimination laws
- State and local anti-discrimination laws
- EEOC recommendations
- Questions about physical attributes
- Personal questions
- National origin, ethnicity and citizenship
- Questions about health and disabilities
- Bona fide occupational qualifications

Record Management

A company's corporate records are one of its most important and valuable assets. Almost every employee is responsible for creating or maintaining corporate records of some kind, whether in the form of paper, computer data, microfilm, electronic mail or voice-mail. Letters, memoranda and contracts are obviously corporate records, as are things such as a desk calendar, an appointment book or an expense record.

Companies are required by law to maintain certain types of corporate records, usually for a specified period of time. The failure to retain such documents for these minimum periods can subject a company to penalties, fines or other sanctions or could put it at a serious disadvantage in litigation. Accordingly, every company should establish a Record Management Policy to provide guidelines for maintaining complete and accurate corporate records — that is, to help employees understand what records to keep and for how long, what records to dispose of, and how to dispose of them.

Course Summary

This 25-minute course explains the basic principles of record management in simple, understandable terms. It includes pop-quizzes, news clippings and a final quiz highlighting real-world compliance issues that employees should learn to recognize and deal with appropriately.

The topics covered in the course include —

- Our records
- What are "records"?
- Who reads our records?
- Electronic communication
- Creating accurate records
- Legal requirements
- Purpose and scope of policy
- Suspension of record destruction
- Record disposal
- Related issues

Regulation FD

Regulation FD, for "Fair Disclosure," dictates how public companies and their representatives disclose "inside" information about the company. In essence, Regulation FD requires that a public company's communication of material, nonpublic information be made in approved forms of public disclosure. The purpose of the regulation is to make all material information about a company available to all investors at the same time.

Regulation FD addresses a practice known as "selective disclosure," in which companies provide inside information to market analysts, other securities-market professionals and shareholders before announcing the information publicly. Selective disclosure is very similar to the phenomenon of "tipping" that is at the heart of insider trading — that is, they enable a privileged few to acquire information that they can use to turn a profit or avoid a loss, rather than having to rely on their skill, business acumen and/or diligence.

But while "tipping" and other forms of insider trading have long been subject to severe punishments under the anti-fraud provisions of the federal securities laws, selective disclosure was not expressly prohibited until the SEC's enactment of Regulation FD in 1990.

Course Summary

This 30-minute course explains the basic principles of Regulation FD in simple, understandable terms. It includes pop-quizzes, news clippings and a final quiz highlighting real-world compliance issues that employees should learn to recognize and respond to appropriately. The topics covered in the course include —

- Overview of Regulation FD
- Regulation FD and insider trading
- Regulation FD in a nutshell
- Who is subject to Regulation FD?
- What is material, nonpublic information?
- To whom are disclosures prohibited?
- Fair disclosure methods
- Fair disclosure safeguards
- Other communications
- Violations

Safe Harbor Privacy Primer

Advances in information technology have enabled companies to collect, compile, analyze and deliver data around the world much more quickly and cheaply than ever before. But these technological advances have also brought new challenges to protecting "information privacy." In fact, some experts believe that privacy concerns will slow the growth of the Internet generally and electronic commerce in particular.

Different countries view privacy issues differently. In the U.S., for example, companies have largely been allowed to "self-regulate." In Europe, by contrast, protection of consumer privacy is the subject of extensive legislation, including a comprehensive Data Protection Directive that took effect in 1998. Foreign companies wishing to receive personal information about European citizens from companies in the European Union (EU) must have policies in place that ensure an adequate level of privacy protection.

In November 2000, the Commerce Department (in consultation with the European Commission) created a "Safe Harbor" program for U.S. companies. A fundamental requirement of the safe harbor program is that companies have a Privacy Policy that addresses seven specific privacy/security principles. Companies that choose to participate in the Safe Harbor program must provide training on their Privacy Policy to employees who handle personal information of consumers. Once certified as a participant in the Safe Harbor program, a U.S. company can receive personal information from EU countries, Switzerland and Canada.

Course Summary

This 25-minute course explains the Safe Harbor program and its seven privacy/security principles in simple, understandable terms. It includes pop-quizzes, news clippings and a final quiz highlighting real-world compliance issues that employees should learn to recognize and deal with appropriately. The topics covered in this course include —

- "Safe Harbor" overview
- Safe Harbor principles
- Notice
- Choice
- Transfers to third parties
- Access
- Security
- Data integrity
- Enforcement

Whistleblowing (DRA Compliance)

Of the half-trillion dollars the federal government will spend on medical care this year, \$50 billion will be spent on fraudulent claims under courses such as Medicaid. In an effort to reduce Medicaid fraud, Congress included a provision in the Deficit Reduction Act of 2005 (DRA) requiring organizations that receive \$5 million or more in Medicaid reimbursements to inform their employees of the federal False Claims Act (FCA) and whistleblower-protection laws, as well as similar state laws.

Dating back to the Civil War Era, the FCA penalizes organizations that submit false claims for government funds. It provides significant financial incentives for employees to make a report — that is, to "blow the whistle" — if they believe that their employer has engaged in fraud.

Course Summary

This 25-minute course is intended to explain to employees when, how and why to use the whistleblowing provisions of the FCA as part of complying with the DRA. The topics covered in the course include —

- Healthcare fraud: The big picture
- Training requirements
- The False Claims Act
- *Qui tam*
- Administrative remedies
- Fraud in the healthcare context
- Evaluating a possible fraud claim
- Whistleblower protection
- Reporting fraud

Workplace Bullying

According to a recent poll, 37% of workers in the U.S. reported that they've been bullied at work (Workplace Bullying Institute and Zogby International). Another survey found that 29% of HR executives had one or more employees in their workplaces resign due to workplace bullying (Challenger Gray & Christmas). Between 12% and 18% of psychological-based disability claims are directly related to bullying. Books and movies such as *The Devil Wears Prada* are raising awareness about an issue that is anything but fiction.

Both business executives and lawmakers are taking action to define and address workplace bullying. Anti-bullying laws are already a reality in Australia, parts of Canada and in several European countries, including the U.K. Starting with California in 2003, state lawmakers nationwide in the U.S. have considered bills that would provide a cause of action based on an "abusive work environment."

Wise employers aren't waiting for public mandates and are implementing anti-bullying policies as a way to retain employees, stimulate recruitment and maintain a healthy, happy and more productive workforce.

Course Summary

This 30-minute course describes what workplace bullying is and details the various forms it takes. It addresses abusive bosses, clients and vendors, as well as bullying between co-workers. It explains both how to avoid bullying behavior and how to respond to it in others. The topics covered in the course include —

- What is workplace bullying?
- The toll
- Anti-bullying law and policy
- Forms of bullying, including hostility, abuse, abuse of power, deceit and sabotage
- Psychological causes of bullying
- Bullying as a violation of company policy
- Enforcement

Workplace Diversity

Dramatic cultural and social changes in the mid-twentieth century altered Western society in a way that affected the workforce and the customer base that companies serve. The emergence of a global economy and revolutionary advances in telecommunications later in the century made the world a much "smaller" place.

In the new millennium, the corporate world finds itself in an environment in which people of a wide variety of races, cultures, religions, ages and lifestyles interact regularly on the same level both within and outside the workplace. The norms that dictated behavior between men and women a half-century ago are transforming, as well.

Diversity is evermore apparent in everything from our names to the types of food we eat, and long-taboo subjects are now discussed freely. People in wheelchairs work alongside openly gay co-workers, and a variety of languages is spoken by employees and customers alike. Human conditions from obesity and dwarfism to mental illness and alcoholism are treated with increasing sensitivity and openness.

Our laws on the federal, state and local level have added a level of legal protection in the workplace that all employees need to be aware of. Diversity-awareness training covers these protections, and it goes on to (1) emphasize the importance of treating everyone with respect and dignity and (2) demonstrate how embracing diversity can be a sound business strategy.

Course Summary

The course covers the following topics —

- Historical background
- Diversity is good for business
- Illegal discrimination and harassment
- Consequences of discrimination and harassment
- Conduct to be avoided