Corporate Governance
After lax or dishonest corporate governance practices caused the failure of several major corporations in the late 1990s and early 2000s, Congress enacted the Sarbanes-Oxley Act (SOX) in 2002 to strengthen corporate governance. The act imposed significant new responsibilities on boards of directors, corporate executives, audit committees, and internal and external auditors of public companies. SOX applies only to publicly owned corporations, but all banks, whether publicly owned or privately held, are subject to corporate governance and financial reporting requirements that are very similar. SOX and the Dodd-Frank Wall Street Reform and Consumer Protection Act also encourage whistleblowers to report financial fraud and other corporate misconduct, offering whistleblowers anti-retaliation protections and financial rewards in some circumstances.

Pre-Employment Screening
Most banks have applicants fingerprinted and send the prints to the FBI to be checked against FBI records. The Federal Deposit Insurance Corporation (FDIC) also recommends that banks check applicants’ names against each federal banking agency’s list of individuals who have been assessed civil money penalties (CMPs) or have been prohibited from being employed by or associated with a bank. The Federal Deposit Insurance Act prohibits a person convicted of a criminal offense involving dishonesty, breach of trust, or money laundering from working at a bank unless the FDIC gives prior approval.

Under the Fair Credit Reporting Act, the bank must have the applicant’s written consent before obtaining a credit report for employment purposes. If the applicant is denied employment because of negative credit report information, the bank must provide contact information for the credit reporting agency and any third-party screening company used. Applicants have the right to correct credit report information and to review their credit report file.

Recognizing the important role banks play with regard to national security, the USA PATRIOT Act gives banks additional latitude to share employment information of suspected criminal activity. A bank can disclose, in written employment references provided to another insured depository institution at its request, information about a current or former employee’s suspected involvement in unlawful activity. The disclosures in the employment references cannot be knowingly false or made with malice or reckless disregard for the truth.

Bank employees who are considered mortgage loan originators (MLOs) under the Secure and Fair Enforcement for Mortgage Licensing Act (SAFE Act) are required to register with the Nationwide Mortgage Licensing System and Registry, which maintains fingerprints and identifying information for registered MLOs. Regulated institutions must not permit employees who are not properly registered to act as MLOs.

Bank Security Systems
Banks are required by law to have security systems and equipment that discourage crime and physical damage to bank structures. Under the Bank Protection Act, enacted in 1968, banks must select, test, operate, and maintain security devices, including:

- Vaults to protect cash or other liquid assets
- Lighting systems to make areas such as the vault visible from within and outside the building
- An alarm or similar system to notify the nearest law enforcement officers of an attempted robbery or burglary
- Tamper-resistant locks on exterior doors and windows that could be opened
Emergency Preparedness

After the September 11 terrorist attacks, detecting and reporting suspicious activities became a national imperative, especially because of the close link between money laundering and the funding of terrorist activities. In 2001, Congress enacted the USA PATRIOT Act. Its anti-money laundering provisions include a requirement for financial institutions to establish anti-money laundering compliance programs that include training, a designated compliance officer, policies, procedures, and internal controls, and an independent review. New customer identification program requirements imposed significant mandatory procedures for identifying both loan and deposit customers.

The importance of disaster recovery programs and business contingency plans was also emphasized following Hurricane Katrina in 2005, one of the greatest natural disasters in recent history. Hurricane Katrina severely tested the ability of banks in the Gulf Coast region to remain functioning after the infrastructure of the affected area was damaged or destroyed.

In the aftermath of Hurricane Katrina, the federal and state governments and the banking industry revaluated their emergency preparedness and response efforts. The Federal Financial Institutions Examination Council (FFIEC), its member regulatory agencies, and the Conference of State Bank Supervisors analyzed bank experiences during and after the storm and found:

- Communications outages made it difficult to locate missing personnel
- Access to, and reliable transportation into, restricted areas were not always available
- Lack of electrical power or fuel for generators rendered computer systems inoperable
- Many facilities were destroyed outright or sustained significant damage
- Some branches and ATMs were underwater for weeks
- Mail service in some areas was interrupted for months

In response, the banking industry and the government formulated planning tools and guidelines to help banks better prepare for and respond to emergencies. Recommendations included restoring communications, partnering with local agencies, distributing financial assistance, anticipating emergencies and the needed response, mitigating the economic impact, and preparing for unique emergencies, such as a pandemic.

Bank Secrecy Act

Since the passage of the Bank Secrecy Act (BSA) more than 30 years ago, BSA has been amended often to expand its scope. For example, in 1986 Congress made money laundering a federal crime, allowed laundered funds to be seized and forfeited, and required banks to have a formal BSA compliance program. In 1990, Congress created the Financial Crimes Enforcement Network (FinCEN) to detect financial crimes, and in 1994 FinCEN took over responsibility for BSA. In the late 1990s, regulatory agencies shifted their emphasis from the technicalities of reporting large currency transactions to monitoring and reporting suspicious activities.