BANK OF AMERICA

GLOBAL INSTITUTIONAL CONSULTING

Risk management and cyber security framework

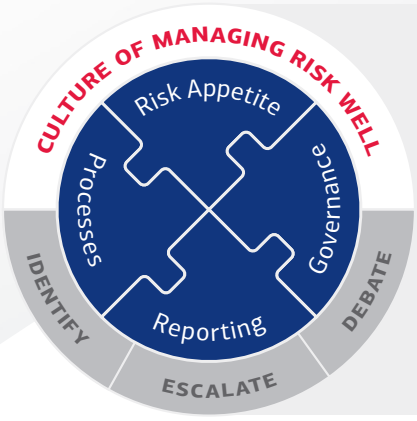
Throughout our organization, we strive to keep risk in check by devoting substantial time and extensive resources to staying ahead of challenges like cyber threats and information security.

How we help protect your institution's information

At Bank of America, we understand the important role you play in helping your institution pursue its goals, and our ability to manage risk well is foundational to our work in helping you fulfill that responsibility. Throughout our organization, we strive to keep risk in check with intense focus, substantial time and extensive resources devoted to staying ahead of challenges like cyber threats and information security.

While risk is an inherent part of business, we feel it is critical to be proactive in identifying, measuring, monitoring and controlling risk. Risk management is central to our organization — from strategic planning and liquidity considerations to data management and information security. We have created a risk culture that focuses on risk in all our business activities and clearly establishes that managing risk is core to our company.

We will employ a broad range of technology and skilled people, create policies and procedures, and implement strong governance and oversight. We invest in resources comparable to the size and strength of our organization to help protect your institution's interests.



Key risk types

- Strategic
- Credit
- Market
- Liquidity
- Operational
- Compliance
- Reputational

We look at risk from multiple angles in the work we do.

Our Risk Framework provides direction and accountability

Our goal is to proactively address concerns about risk head-on, so you can stay focused on the priorities of your institution. We have established our Risk Framework, which defines risk, outlines how the company manages it proactively and sets the responsibilities for risk management for every part of our organization. Our network of financial advisors is also responsible for adhering to our Risk Framework and assuring compliance with industry regulations, with oversight from local branch office leadership. This framework is instrumental in helping to create a culture of ownership and accountability for risk while building risk management skills throughout the company.

The Risk Framework is consistent with regulatory expectations, including the U.S. Federal Reserve Board's Enhanced Prudential Standards final rule and Office of the Comptroller of Currency's Heightened Standards final guidelines. The Risk Framework is owned by the Company's Chief Risk Officer (CRO), who is held accountable by Bank of America's Chief Executive Officer and the board of directors.

Protecting your institution's information

Information security is a critical component of Bank of America's Risk Framework and our corporate risk culture. The Bank of America Information Security Policy is designed to protect the integrity and availability of information assets and resources. This policy is based on regulatory requirements; federal, state, and local laws; industry standards and best practices; and is subject to ongoing regulatory oversight and examination. The policy applies to all members of the Bank of America corporate family as well as vendor and other third-party partners who are authorized users of Bank of America systems, facilities or information.[1]

In a dynamic threat and risk environment, we constantly assess and evolve our information security program, test our response capabilities and validate the effectiveness of our controls while continuously monitoring for emerging risks. We proactively look for ways to build stronger defenses, ensure our technology design process takes cyber risks into consideration and integrate layers of security into our infrastructure. In addition, we're committed to keeping clients' personal and financial information protected and secure through responsible information collection, processing, and use practices. Our fraud prevention and security systems help protect clients with features including encryption technology and secure email communications. We are committed to fraud and identity safety, with strong performance in fraud prevention, detection, and resolution, based on industry assessments by Javelin.[2]

Cyber security in action

Because we understand that the threat of cyber attacks in today's digital landscape can be a cause for concern, the Global Information Security (GIS) team remains vigilant in its work to maintain and enhance the many layers of security we've built to protect information, proprietary and confidential data and information systems. The team uses a proactive strategy, an agile operating model, innovative controls and a highly proficient information security workforce.

The Global Information Security team has 2,564 employees in 15 countries[3] working to keep information safe.

Bank of America's Global Information Security team operates around the clock and around the globe to identify and mitigate information security risks, including:

- 24/7 global team to monitor cyber threats.
- Plan proactively for a cyber security event and develop well thought-out and tested incident response plans.
- Application security evaluations following protection practices such as ethical hacking assessments and vulnerability scanning.
- Security protocols used throughout our entire organization that help create a safe environment for information and data transfer.
- Ongoing work with industry professionals and government officials to enhance cyber security and financial sector resilience as demonstrated by our leadership in the creation of the Financial Systemic Analysis and Resilience Center (FSARC) and ongoing activities with the Financial Services Information Sharing and Analysis Center (FS-ISAC).[4]
- Bank of America has aligned its information security controls and annual policy management cycle to the National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) and the International Organization for Standardization (ISO) series 27002:2013 (Code of Practice for Information Security Management).
- The GIS team strives to set the gold standard in cyber security. In 2018, GIS won SC Magazine's Professional Award for Best Security Team.[5]

Bank of America's threat-centric framework is based on a five-fold model. The framework is predicated on the prevention of data exfiltration, data and system destruction and manipulation, as well as system and transactional disruption.

Prepare	Prevent	Detect	Mitigate	Respond/Recover
We constantly analyze the threat environment to identify attacks before they happen	Understanding how our adversaries might attack us means we can take steps to reduce the number of security incidents	We are continuously monitoring for potential attacks—whether they come through networks, applications or business partners	If there is an incident, we have a well-rehearsed plan of action to ensure it's contained	By having a recovery plan in place we can quickly restore any services that were harmed

This framework helps the firm manage cyber security risk by organizing information, enabling risk management decisions, addressing threats and learning from previous activities. This also aligns with existing methodologies for incident management. The Threat Response team actively monitors the infrastructure to help ensure comprehensive threat monitoring and detection.

Limiting down time

Our ability to protect your institution's proprietary information includes our resilience to a wide variety of challenges to our business operations—from small occurrences, such as single building power outages, to large disasters, such as major hurricanes or tsunamis. Our Business Continuity and Disaster Recovery programs help us prepare for the loss of facilities and technologies and to resume normal business as quickly as possible.

Complying with applicable rules and regulations

We have a strong risk management and governance culture. Our Risk Framework is consistent with regulatory expectations including the U.S. Federal Reserve Board and Office of the Comptroller of the Currency.

Our ongoing commitment

Our team is dedicated to helping alleviate risk concerns and to keeping your institution's information safe. For questions or to learn more, please contact your Global Institutional Consultant.

[1] Bank of America Corporation information security policy is maintained by Global Information Security (GIS) who manages performance to the policy which is supported by standard requirements (standards) and baselines that provide additional requirements or guidance for carrying out the bank's information security program.

[2] Javelin Strategy & Research, 2018 Online Banking Award, Bank of America Ranks "Best in Class" for Second Year in Row.
Methodology: Javelin's 2018 Online Banking Scorecard measures the availability of 250 criteria at 28 of the nation's largest retail FIs by total deposits, excluding banks focused on investment banking. Data was collected from April through June, and 75% of the FIs validated their results. Javelin analysts weight individual features based on their strategic value, tactical necessity, and industry and consumer trends. The overall score was a composite of six categories weighted by consumers' responses about what is most important to their satisfaction with online banking: Ease of Use (28%), Security Empowerment (20%), Money Movement and Financial Fitness (17% each), Customer Service (12%), and Account Opening (6%).

[3] As of June 2019.

[4] Financial Systemic Analysis & Resilience Center (FSARC) established 2016. For more information: https://www.fsisac.com/sites/default/files/news/FS-ISAC%20Announces%20the%20Formation%20of%20the%20Financial%20Systemic%20Analysis%20%28FSARC%29.pdf.

[5] On April 19, 2018, Bank of America announced that its Global Information Security group won the SC Magazine Professional Award for Best Security Team. The 2018 Professional Award winners were chosen by a panel of judges comprised of recognized security professionals and leaders from a variety of backgrounds and vertical markets. The individuals, programs and teams chosen as winners in the Professional Award categories go through a rigorous judging process that includes testimonials, industry assessment and additional research. For more information: https://newsroom.bankofamerica.com/press-releases/awards-and-recognition/bank-americas-cyber-team-named-best-sc-magazine.