BANK OF AMERICA

FINANCIAL LIFE BENEFITS®

Department of Labor Cybersecurity Guidance

Earlier in 2021, the Government Accountability Office (GAO) released a report titled *Federal Guidance Could Help Mitigate Cybersecurity Risks in 401(k) and Other Retirement Plans*. As part of the GAO report, they recommended that the Department of Labor (DOL) issue cybersecurity guidance for plan sponsors, plan participants and service providers. The week of April 12, 2021, the DOL released their guidance in the form of recommended best practices.

For service providers, the DOL guidance is a list of 12 recommended best practices for a cybersecurity program. Bank of America's Global Information Security division reviewed the guidance and confirmed that we have a robust information security program that is consistent with the DOL guidance.

Following is more detail about Bank of America's Global Information Security (GIS) program in response to each of the 12 categories in the DOL guidance.

1. Formal documented cyber security program

The GIS team, under the leadership of the Chief Information Security Officer (CISO), develops and executes a strategic company-wide Information Security Program to protect Bank of America and its clients' information. As part of this role, the CISO manages the development, implementation, and maintenance of the information security infrastructure; oversees the protection of Bank of America's computer-based assets by providing monitoring, detection, analysis, event handling, and containment of security incidents; monitors information security trends internally and externally; and informs senior leadership about information security-related issues and activities affecting the organization.

Our Information Security Policy supports the Bank of America Risk Framework by establishing the requirements for a proactive Information Security Program. This program protects the company through preventative and detective measures that mitigate current and emerging information security risks. As threats and technology evolve, we continuously update the policy to build upon best practices, leveraging a risk-based approach.

2. Prudent annual risk assessments

Information security is a critical part of our corporate risk culture, and we leverage both internal and external assessments and partnerships with industry leaders to ensure we are taking a holistic approach to this vital issue.

The Global Information Security team conducts rigorous, ongoing testing of its control processes to assess the overall environment, continually conducts internal assessment to ensure adherence to relevant information security standards and incorporates independent assessment by industry leading third parties to assess enterprise process control capabilities.

3. A reliable annual third-party audit of security controls

Information security is a critical part of our corporate risk culture, and we leverage both internal and external assessments and partnerships with industry leaders to ensure we are taking a holistic approach to this vital issue.

Bank of America is regulated at the state, federal and international level. The bank's Information Security program is continuously evaluated and examined by the Office of the Comptroller of the Currency and the Federal Reserve Board, as they represent our primary regulatory oversight. The Global Compliance and Operational Risk team independently assesses, monitor and test compliance and operational risk.

The Global Information Security team conducts rigorous, ongoing testing of its control processes to assess the overall environment, continually conducts internal assessment to ensure adherence to relevant information security standards and incorporates independent assessment by industry leading third parties to assess enterprise process control capabilities.

4. Clearly defined and assigned information security roles and responsibilities

At Bank of America, our Risk Framework serves as the foundation for consistent and effective management of risk across all our lines of business. The Risk Framework establishes clear roles, responsibilities, and accountability for the management of risk.

5. Strong access control procedures

As information owners and custodians, lines of business are required to manage who is permitted access to such information. Access requests must be approved by a manager and are assigned by a "least-privileged" guiding principle — giving users, programs or processes the minimum privileges necessary to perform a function. In accordance with the Bank of America's Information Security Policy, access is certified for appropriateness through access reviews. All access controls are continually monitored and reported to drive sustainability and accountability across the firm.

6. Assets or data stored in a cloud or managed by a third-party service provider are subject to appropriate security reviews and independent security assessments

Our commitment to information security extends beyond the Bank of America corporate family to our trusted third parties. Third parties are subject to our comprehensive Third Party Information Security Program. This incorporates both security requirements and regular assessments in order to ensure that every party privy to any of our clients' information meets our standards.

Our third-party providers are key partners for the conduct of our business operations and how we execute our Information Security Program. Bank of America maintains a comprehensive enterprise program that defines requirements for the planning, sourcing, management, and oversight of third-party relationships. Bank of America also requires our third parties conduct background checks on their personnel prior to performing services for Bank of America and comply with our internal requirements for training on an ongoing basis.

7. Cyber security awareness training conducted at least annually for all personnel and updated to reflect risks identified by the most recent risk assessment

Information security is a critical role for all of our personnel, and we are constantly investing in our culture of security. Individuals who access our computer systems and information are required to complete an annual information security training course, which covers key themes such as social engineering, data classification, securing work stations and email encryption. Annual training is supplemented with additional educational content, to include internal exercises, that reinforces desired employee behaviors, creates a heightened level of accountability, acknowledges good behavior, and provides additional training and coaching as needed.

8. Secure System Development Life Cycle program (SDLC)

Integrating security throughout the software development life-cycle is a core component of the Bank of America application security strategy. Developers receive required annual training on secure code development ensuring appropriate information security practices are leveraged. Applications receive a penetration test prior to production deployment and upon release of subsequent significant changes or at a minimum annually.

9. A business resiliency program which effectively addresses business continuity, disaster recovery, and incident response

Business continuity and disaster recovery planning at Bank of America are supported by an extensive Disaster Recovery Program and are incorporated into virtually every aspect of our business processes. The Business Continuity Program balances reasonable assessments of risk, placing the highest priority on the physical safety and security of our customers, clients, and employees, while preparing for loss of facilities and technologies.

Further, Bank of America's experienced Global Information Security response teams actively monitor for sophisticated cyber threats to ensure rapid response to any attempts to subvert or compromise confidentiality, integrity or availability of our systems and data. Bank of America utilizes Security Operation Centers (SOC) with advanced capabilities that are positioned globally in each of the regions where we have operations and employ a 24/7 "follow the sun" model to ensure around-the-clock coverage.

10. Encryption of sensitive data stored and in transit

Encryption is used as appropriate to protect the confidentiality of information. We use several forms of encryption in tailored, risk-based solutions, including business-to-business Virtual Private Networks (VPNs), secure email encryption, database encryption, and hardware security modules (HSMs). Bank of America encrypts records and files containing personally identifiable information that are transmitted or sent wirelessly across public networks, stored on laptops, where technically practicable, and stored on allowed portable devices.

11. Strong technical controls implementing best security practices

Over the years, we have established a robust and proactive Information Security Program that we continue to refine as the ever-evolving landscape of cyber security changes. In the current dynamic threat and risk environment, we constantly assess and evolve our program to deliver best in class protection. In addition to making strategic, and significant, investments in our technology and people, we continuously test our response capabilities and validate the effectiveness of our controls. Through this process, we strengthen our multiple layers of protection to provide end-to-end delivery of information and data security.

12. Responsiveness to cyber security incidents or breaches

Bank of America's experienced Global Information Security response teams actively monitor for sophisticated cyber threats to ensure rapid response to any attempts to subvert or compromise confidentiality, integrity or availability of our systems and data. Bank of America utilizes Security Operation Centers (SOC) with advanced capabilities that are positioned globally in each of the regions where we have operations and employ a 24/7 "follow the sun" model to ensure around-the-clock coverage.

For plan sponsor and consultant use only.