Governance and Control Assurance Program

FHLBank
Chicago

FHLBank Chicago
Governance and Control Assurance Program

The Federal Home Loan Bank of Chicago (FHLBank Chicago; “the Bank”) appreciates the need for members and other business partners to receive assurance on the Governance and Control environment at the Bank. We are committed to building and maintaining an appropriate control environment for the risks undertaken by FHLBank Chicago. As a result, we have prepared this Governance and Control Assurance document to provide an overview of the Bank’s risk management, governance, and operational controls, and to focus on how we manage the risks associated with technology and vendors. It covers the controls identified by our members and their regulators as they seek assurance about their key business partners. This document should assist members and other business partners in meeting their own vendor's governance requirements and regulatory obligations.

As a strategy, we are not specific in our control descriptions within this document. FHLBank Chicago’s approach is deliberate and reflects that Bank staff continuously update our control implementations. We believe disclosure of detailed facts related to how we manage risks, such as specific vendors and tools, makes the Bank more vulnerable to an aggressive and constantly changing threat environment.

To ensure a well-managed and secure environment, we expect our members and partners to have robust governance and control environment. As such, we have identified some areas where we expect our members and business partners to have significant governance and control processes in place.

There are many aspects to the internal control environment of FHLBank Chicago, most of which are included on the following pages. Further information on the Bank’s risk and control structure is available in our SEC filings, which can be found online at http://sec.gov. And in various guides such as the MPF Guide (MPF Guides | FHLBMPF) and Wire Transfer Agreements.

Thank you for your request, and please feel free to contact FHLBank Chicago with any questions.

Regards,

Thomas H.W. Harper
Executive Vice President and General Auditor

This document has been prepared for the benefit of the Federal Home Loan Bank of Chicago’s business partners, including members, Mortgage Partnership Finance® (MPF®) Program Participating Financial Institutions, and FHLBanks and their regulators and auditors. This document should only be distributed by the Federal Home Loan Bank of Chicago. This document is confidential and proprietary to the Federal Home Loan Bank of Chicago.

Governance and Oversight

- The Board of Directors (Board) sets risk tolerance and provides risk oversight through its Operations and Technology, Risk Management, and Audit committees.

- Business area management identifies key controls over our activities. Appropriate business owners periodically attest that these controls are operating effectively and that no changes are needed to the control environment. Fiduciary areas such as MPF, safekeeping, member deposits, wire activity, and collateral are covered in this letter.

- The Bank's Operational Risk Oversight Committee oversees operational risk management processes. The Committee oversees risks related to financial reporting, legal compliance, fraud, models and technology

- Our risk management process includes identifying and ensuring we appropriately evaluate the risks to our data, including employee, member, and consumer data.

- The Chief Risk and Compliance Officer works with management to prepare periodic process risk assessments that evaluate the risks faced by the Bank and its control environment. Senior management and the Board's Risk Management Committee review these on a regular basis.

- Certain Bank officers oversee specific risks, such as business continuity, compliance, fraud, vendor management, and information security risks.

- Our Internal Audit Department, in accordance with the *International Standards for the Professional Practice of Internal Auditing*, has a program that assesses the Bank's risks and operations. It also conducts an audit program that evaluates the adequacy of the controls in place and their operating effectiveness. The Internal Audit Department reports the results of its assessment to senior management and the Board's Audit Committee. All significant control issues identified by internal and external auditors, management, and regulators impacting the bank are tracked and reported to the Board and senior management until successfully resolved.

Our partners are covered by a variety of regulators at a state and national level in addition to industry guidance. A short list of the key areas of regulatory guidance is listed at the end of this document.

- Our external auditors, business partners (such as MPF investors), and our federal regulator also examine the Bank and its control environment on a regular basis.
- Employees, business partners, contractors, and vendors can report ethics concerns or wrongful conduct confidentially through our whistleblower program.

Service Organization Control Reports

(Previously SAS 70 Reports)

- Service Organization Control (SOC) reports are internal control reports on the services provided by a service organization. The provisions of auditing standard AU 324, Service Organizations, are not intended to apply to situations in which the services provided are limited to executing client organization transactions that are specifically authorized by the client (Section 324.03). Since the services provided by the Bank are executed based upon authorizations from our members, the Bank does not fall under the definition of a service provider in this instance. As such, a SOC report in accordance with Statements on Standards for Attestation Engagements (SSAE) No.18, Reporting on Controls at a Service Organization, is not prepared for services provided by the Bank. Please note, however, that the Bank has established and maintains an effective internal control system that addresses the efficiency and effectiveness of our activities, the safeguarding of our assets, and the reliability, completeness, and timely reporting of financial and management information to the Board and outside parties.

Business Continuity Risk

- Business continuity risk is addressed in a variety of ways throughout the Bank. The Bank designs its systems and processes to be resilient, and, in the event of significant disruption, the Bank has back-up and/or alternative processing arrangements in place. Business continuity processes are tested regularly and reported to executive management and the Board.

Fraud and AML/BSA/OFAC

- FHLBank Chicago participates in relevant fraud and suspicious activity reporting protocols and complies with the U.S. Treasury's OFAC regulations, as applicable.

- FHLBank Chicago has:
  - Developed internal policies, procedures, and related controls.
  - Designated an AML/BSA, OFAC and Fraud Compliance Officers.
  - Implemented a thorough and ongoing training program.
  - Conducts regular independent reviews for compliance.

Vendor Risk Management

- FHLBank Chicago uses external parties to provide technology and other services. The Bank has implemented vendor management and security controls designed to ensure that external parties provide services in a manner consistent with the Bank's standards, especially for the security of information systems.

- FHLBank Chicago policy is that all data used in development is scrubbed of sensitive data elements.

- Vendors are subject to a formal vendor governance and management program and process, which includes assessment of vendor risks, data protection requirements, and ongoing monitoring protocols to assure us that vendors are fulfilling their obligations to the Bank. When warranted, FHLBank Chicago seeks independent third-party reports, such as System and Organization Controls (SOC) 1 and/or SOC 2 reports, on vendor performance. In addition, when appropriate, Bank staff visit vendors to assess their performance and control environment.

Artificial Intelligence and Machine Learning

AI Usage Policy

FHLBank Chicago enforces a formal Artificial Intelligence Usage Policy, managed by the AI/ML Center of Excellence (CoE). This policy applies to all employees, contractors, and temporary staff.

Core Risk Management and Control Activities

- **Business Case Approval** – AI initiatives require documented business justification and approval from the AI/ML CoE and Operational Risk Oversight Committee.
- **Inventory Management –** Centralized tracking of AI models, tools, and use cases.
- **Monitoring** – Oversight of AI models and usage to ensure compliance and performance.
- **Training** – Ongoing education on responsible AI practices for staff.

Scope and Principles

FHLBank Chicago's governance framework includes Generative AI and emphasizes responsible AI, ethical use, transparency, and compliance with regulatory standards. Generative AI outputs (text, image, audio, video) cannot be directly incorporated into Bank content without human review for accuracy and compliance.

Third-Party Risk Management

Many service providers and software vendors include AI functionality in their offerings. FHLBBank Chicago manages associated risks through:

- Contract reviews for AI-related clauses, liability, and data protection.
- Due diligence on the use of Bank data in training AI models.
- Tracking vendor-provided applications with AI capabilities through a centralized inventory.
- Security reviews for vendors, with additional considerations for those incorporating AI capabilities.

Audit and Assurance

Internal Audit evaluates AI governance, inventory, and monitoring capabilities. IAD tests preventive and detective controls to mitigate unauthorized AI use.

Member and Business Partner Responsibilities

As a cooperative serving our members and working with other business partners, our collective control environment involves responsibilities for all parties. Listed below are some critical responsibilities of members and other business partners with respect to our business together:

- Timely balancing and reconciliation of transactions with the Bank and prompt notification to the Bank of any discrepancies.

- Securing passwords, PINs, and other authentication mechanisms.

- Notifying FHLBank Chicago of any changes in personnel, lost authentication keys, or other events that could indicate or lead to a security incident.

- Implementation of Ethics policies and whistleblower protocols to ensure staff and business partners can notify the appropriate senior leadership of potentially damaging activity.

- Regular independent reviews of business and technology processes to ensure designed controls are adequate and operating effectively.

- Ensuring Anti-money laundering (AML), Bank Secrecy Act (BSA), and Office of Foreign Asset Control (OFAC) protocols are appropriately implemented.

- Business continuity plans that address major business functions and likely disruption and periodically appropriate testing of business continuity plans.

- Back-up of critical data.

- Adequate training in the use of Bank systems.

- Secure transmission and storage of data shared with the Bank.

- Configuring and periodically re-evaluating user access to Bank systems.

- Providing adequate physical security for technology and paper records

- Conducting periodic information.

- Security training and awareness.

- Regularly scanning and remediating vulnerabilities.

- Documenting cybersecurity incident response procedures.

- Notifying FHLBBank Chicago of loss of Bank or personally identifiable information (PII).

Technology, Cyber Risks, and Confidential Data Protection

The confidentiality, integrity, and availability of our environment is very important. Our technology team has processes in place to ensure that systems are maintained to an appropriate level; this includes frequent monitoring and regular maintenance. All technology operated by FHLBank Chicago can be supported by the Bank's staff or our vendors.

The Bank maintains policies, standards, and procedures as well as the allocation of resources for a formal, dedicated IT security organization.

Data Centers

- Leading vendors that are rated the equivalent of "Tier 3" or better by the Uptime Institute provide data centers to the Bank. Key features include redundant incoming power, redundant UPS systems and generators, and redundant HVAC. Safety systems include fire detection systems, fire suppression systems, and leak detection systems.

- Our primary data center provider has a number of compliance certifications, including but not limited to FedRAMPSM, PCI DSS Level 1, ISO 9001, DOD SRG Levels 2 and 4, and NIST.

- Data center providers are regularly reviewed and subject to independent inspection and reporting.

- The Bank uses US-based service providers for its core operations and, as a strategy, maintains all data in the US. The Bank and some of our service providers have offshore operations, mostly for development and support, and we have protocols to protect sensitive information if production data needs to go offshore including ensuring it is deleted as soon as practical.

Inventory of Authorized and Unauthorized Devices or Software

- FHLBank Chicago allows authorized devices to access its network and authorized software to run on its end points. We monitor these processes centrally.

Threat Intelligence

- The Bank develops knowledge about our adversaries, motivations, and tactics to proactively mitigate and respond to evolving threats.

Vulnerability Assessment and Remediation

- FHLBank CHicago has established processes and procedures to perform frequent vulnerability scans of its systems. These procedures specify the use of vulnerability scanning software, the creation of vulnerability assessment reports, and the presentation of vulnerability scanning results to the information security team and Bank leadership.

- The Bank has baseline security configurations and corresponding tools to manage the deployment and compliance of these configurations.

- FHLBank Chicago continually reviews patches and application updates as they are released to determine their criticality. Patches released on a regular schedule are applied following the release; off-cycle or other patches determined to be critical to the Bank's environment are applied as needed to ensure protection from vulnerabilities.

Technology, Cyber Risks, and Confidential Data Protection
continued

Maintenance, Monitoring, and Analysis of Audit Logs

- The Bank maintains audit logs for servers and network devices that log the occurrence of system faults and security events to facilitate examination of abnormal activities. Logs are collected in a central security information and event management system to prevent modification or removal of administrative and user activities. Audit logs are monitored regularly.

- The Bank has an independent IT compliance team that monitors compliance with activity across our technological environment.

Email and Web Browser Protections

- The Bank uses a hosted email solution to filter incoming email for spam and malware.

- The Bank has deployed and regularly updates a URL filtering solution that blocks access to high-risk categorized websites or websites the Bank deems inappropriate for business use.

Malware Defenses

- FHLBank Chicago uses malware prevention software on all end points to support a secure computing environment. These solutions are centrally managed and configured to receive updates on a regular basis.

- The Bank leverages intrusion detection/prevention software to detect malicious activity.

Data Recovery Capability

- Data is backed up and retained for disaster recovery and record retention purposes. These capabilities are supported by documented policies and procedures.

- Telecom services are provided by dual carriers. The Bank's network is architected with resiliency and performance as key criteria.

- The Bank has a disaster recovery plan and tests this plan on a regular basis to ensure our systems can be recovered in the event of a disaster.

Change and Configuration Management

- The Bank's IT organization has established and maintains a change control process which includes risk assessment, test and recovery procedures, and communication. planning, management review, and approval components.

- The Bank maintains separate development, test, and production environments. The Bank has established procedures requiring the use of the change management process to transfer changes from development to test and production.

Boundary Defense

- The Bank maintains redundant firewalls that inspect and filter all ingress and egress of network traffic.

- Intrusion prevention and detection software has been placed at strategic points on the network. The intrusion detection system is centrally monitored 24/7.

- The Bank blocks network communications from countries where we don't do business.

Data Protection

FHLBank Chicago has established policies and procedures that are designed to meet the requirements of applicable laws and regulations involving data protection.

Technology, Cyber Risks, and Confidential Data Protection
continued

- These policies and procedures address information handling requirements throughout the information life cycle.
- Most users are unable to use removable media. Those users with specific job requirements are issued encrypted USB drives for business use only.
- Access to Bank email via mobile devices is only permitted when configured in accordance with the Bank's security policy.
- The Bank has implemented tools to manage the egress of sensitive information via email and web access.
- Non-Bank managed mobile devices cannot access Bank data. Visitors are provided with a limited connection to an Internet-only wireless guest network, which requires sponsorship from authorized Bank personnel.
- The Bank has minimized the use of fully functional laptops when operating our business, which reduces the risk of data leaving the Bank unintentionally and/or being mislaid through loss of a physical device. All Bank staff use special purpose laptops that are hardened, restricted to very limited functions, and contain no sensitive local Bank content.
- All environments run a security suite that includes virus protection, anti-spyware, host intrusion detection These controls are centrally managed.
- The Bank complies with all relevant regulations regarding confidential information. Protocols are provided to ensure the appropriate parties, including members and business partners, are notified in the event information is breached.
- Data the Bank deems sensitive is encrypted at rest and in transit with industry standard encryption protocols such as TLS, IPSec and AES256.
- Secure paper disposal and locked printing are used to protect the accidental loss of physical data.
- Physical access to the Bank's office and data center environments is limited to approved personnel.
- Personally Identifiable Information (PII) is masked on the screens of appropriate applications.

Wireless Access Control

- Only IT-approved and managed wireless devices are permitted on the Bank's network. Technologies are in place to identify and disable ports with unauthorized rogue wireless networks attached.

Access Management

- End users use two-factor authentication, strong passwords, and encrypted methods to access our environment.
- There are processes established to limit third-party remote access to FHLBank Chicago systems. Such access requires approval from the security organization and access is limited to those systems required for the third party to complete their task.

The Bank uses a documented access management process that defines the responsibilities and steps for onboarding, transferring, and off-boarding users and access rights.

Technology, Cyber Risks, and Confidential Data Protection
continued

- Access is attested to by business managers on a regular basis. Automated and manual processes execute changes based on attestation results.

- The Bank has access controls designed to prevent a single user from moving funds, making trades, or performing other high-risk transactions.

- Privileged accounts are monitored by both Information Security and Information Technology Compliance departments.

Information Security Team, Skills, and Training

- FHLBank Chicago has a dedicated Information Security Program led by a Chief Information Security Officer (CISO). The Information Security teams supporting the program include specialists in threat and vulnerability management, incident response, and technology risk management. These security professionals hold a variety of technology certifications. Newly hired personnel, including interns, temporary hires, and contractors, undergo pre-employment background checks.

- All workers are required to sign non-disclosure agreements as a condition of employment.

- All workers are required to complete security and privacy awareness training. This training addresses the proper use of computer security systems and the importance of protecting confidential information. All workers are required to understand their roles and responsibilities regarding confidentiality, business ethics, appropriate usage, and professional standards through the completion of training.

- The Bank provides its staff with technology security policies and guidelines to communicate individual responsibility with respect to safeguarding technology resources. These policies are communicated to staff and easily accessible through the Bank's intranet portal.

- Workers connecting to the Bank network are required by policy to conduct themselves in a manner consistent with the Bank's guidelines.

- Staff are required to be away from the Bank for a minimum period of time each year to address staff wellness, resiliency and other operational risks including fraudulent activity.

- The Bank conducts regular security awareness training to ensure awareness of potential threats.

Application Software Security

- To implement new solutions, the Bank follows a documented process for project requests. This process includes review and approval by members of IT leadership, including the IT security organization. Security requirements are artifacts of every project plan.

- Member- and Participating Financial Institution-facing applications and interfaces include in their user documentation descriptions of specific controls and requirements, as well as the obligations of parties using them, to manage transactions and user access.

- The Bank's software development life cycle includes processes that support the identification and remediation of security issues. These processes are governed by a structured approach to identifying business risk and application security standards to address higher risks with stronger security.

Technology, Cyber Risks, and Confidential Data Protection
continued

Incident Response Management

- FHLBank Chicago has a documented Cyber Security Incident Response Plan (CSIRP) that is practiced and refined on a regular basis.
- The Bank periodically revalidates its CSIRP plan through integrated testing. The plan includes protocols and procedures to ensure that the Bank complies with applicable notification requirements should the incident involve sensitive information including PII.

Penetration Tests

- FHLBank Chicago conducts network, host, and application penetration tests on a regular basis to find vulnerabilities an attacker could exploit.
- The Bank evaluates these tests, prepares appropriate remediation plans, and tracks issues until they are resolved.

Insurance

- FHLBank Chicago carries customary insurance coverage for a financial institution including Directors and Officers, Errors and Omissions, and Blanket Bond coverage. The Bank also has a Cybersecurity insurance policy. Insurance coverage is determined after consultation with our brokers and underwriters and is reviewed by executive management and the Board annually.

List of Key Regulatory pronouncements on Third-Party and supply chain risks (this list is not exhaustive; each business partner should consider their governance, risk management and regulatory oversight and requirements):

Regulator / sector	Scope	Type	Key date (latest major action)
Federal Reserve, FDIC, OCC (banking)	Interagency Guidance on Third-Party Relationships: Risk Management lifecycle framework (planning, due diligence, contracting, ongoing monitoring, termination) for all third-party relationships; replaces earlier agency-specific guidance.	Final interagency guidance	June 9, 2023 (Federal Register publication)
OCC (national banks & FSAs)	OCC Bulletin 2023-17 Third-Party Relationships: Interagency Guidance on Risk Management OCCs transmittal of the interagency guidance clarifies applicability to national banks, FSAs, federal branches.	Supervisory bulletin	June 6, 2023
OCC (national banks & FSAs)	OCC Bulletin 2024-11: Third-Party Risk Management: A Guide for Community Banks Resource for community banks on implementing third-party risk management practices.	Supervisory bulletin	
FDIC (insured banks)	FIL-29-2023 Interagency Guidance on Third-Party Relationships: Risk Management FDICs issuance of the interagency guidance; rescinds FIL-44-2008 and related prior third-party letters.	Financial Institution Letter	June 6, 2023
Federal Reserve (Fed-supervised banks)	SR 23-4 / CA 23-4 & CA Letter 24-02 Interagency Guidance on Third-Party Relationships: Risk Management Fed implementation of the interagency guidance and clarification that applies to institutions of all sizes.	Supervisory / consumer-affairs letters	June 7, 2023 (SR 23-4); May 8, 2024 (CA 24-02 applicability)
FFIEC (all federally supervised FIs)	FFIEC IT Examination Handbook Business Continuity Management (BCM) booklet updated BCM expectations, including identification and management of third-party dependencies and supply-chain single points of failure.	Interagency examiner handbook	Nov 14, 2019 (revised booklet release)
FFIEC (all federally supervised FIs)	FFIEC IT Examination Handbook Development, Acquisition, and Maintenance (DA&M) booklet updated IT development / acquisition guidance with dedicated sections on third-party risk management and supply-chain considerations (e.g., inventories of critical third-party relationships, risk assessments of supply chains).	Interagency examiner handbook	Aug 29, 2024
NCUA (federally insured credit unions)	Letter to Credit Unions 07-CU-13 & Supervisory Letter 07-01 Evaluating Third Party Relationships foundational framework for CU third-party risk (risk assessment, due diligence, contract review, oversight). Still cited as primary vendor-risk guidance.	Supervisory letter + examiner guidance	2007 (Letter 07-CU-13; posted Nov 14, 2007)

Regulator / sector	Scope	Type	Key date (latest major action)
NCUA (credit unions)	Due Diligence Over Third-Party Service Providers (01-CU-20) early guidance emphasizing CU board/management responsibilities for due diligence and controls over third-party arrangements. Often referenced alongside 07-CU-13.	Supervisory guidance	2001 (legacy letter; still available)
CFPB (consumer-financial products & services)	Compliance Bulletin and Policy Guidance 2016-02 Service Providers set expectations that supervised banks and non-banks must oversee service providers to ensure compliance with federal consumer-finance law (risk-based due diligence, contract provisions, ongoing monitoring).	Supervisory bulletin / policy guidance	Oct 26, 2016 (Federal Register publication)
NAIC (National Guidance for Insurance Regulation)	Insurance Data Security Model Law (668) Establishes cybersecurity standards for insurers and requires oversight of third-party service providers.	Model Law	
NAIC (National Guidance for Insurance Regulation)	Risk Management and Own Risk and Solvency Assessment (ORSA) Model Act (505) Requires insurers to maintain a risk management framework, including risks from third-party relationships.	Model Law	
NAIC (National Guidance for Insurance Regulation)	Third-Party Data and Models Task Force Framework (Proposed) Developing regulatory oversight for third-party data, predictive models, and AI used by insurers.	Proposal	