

TECHNOLOGY AND CYBERSECURITY COMMITTEE CHARTER

Purpose

The Technology & Cybersecurity Committee (the “**Committee**”) is appointed by the Board of Directors (the “**Board**”) of Western Alliance Bancorporation (the “**Company**”) and each of its subsidiary banks and other subsidiaries to assist the Board in fulfilling its oversight responsibilities with respect to:

- Technology strategy, technology risk, information security, IT operations, and resilience, including business continuity and disaster recovery.
- Data governance and data management, including overseeing the data management framework and key data risks.
- Cybersecurity risk management, including operational, strategic, compliance and reputational risks related to cyber threats and incidents.
- Significant change management initiatives, such as new product development and acquisition opportunities, that include the adoption of new and emerging technologies
- Management’s implementation of an effective enterprise-level technology and cybersecurity risk management framework.

Authority and Delegation

The Committee has authority to:

- Access Information and Management:** Obtain information from and meet with members of management, including the Chief Information Security Officer (“**CISO**”), Chief Information Officer (“**CIO**”), Chief Risk Officer (“**CRO**”), and other relevant executives, at any time or in executive session when appropriate.
- Retain Advisors:** Engage independent advisors, consultants, or experts as necessary to fulfill its responsibilities, the compensation for which to be paid for by the Company.
- Delegate Responsibilities:** Delegate duties to subcommittees or management working groups as appropriate, consistent with Board authorization.

Composition and Organization

The Committee shall have three or more members appointed by the Company’s Board of Directors. Members may be removed and replaced by the Board at any time and shall serve until their successors are appointed. The Board shall designate one member of the Committee to act as Chair of the committee. The Committee chair shall set the agenda for, and preside at, meetings of the Committee.

The Committee shall meet as often as it determines necessary, but no less than four times per year. The Committee may meet in joint session with the Audit, Risk, or other Board committees when topics of common interest arise. The Committee will maintain minutes and provide regular reports to the Board summarizing key matters discussed and any recommendations.

Responsibilities and Duties

Among its specific duties and responsibilities, the Committee shall:

A. Technology Oversight.

1. Review the technology strategy, architecture, transformation initiatives, and alignment with business objectives.
2. Receive updates on information technology operations and performance, system resilience, and infrastructure.
3. Review technology risk, information security risk, and third-party assessment results and risk culture alignment.

B. Data Governance and Data Management Oversight.

1. Review and oversee the data governance framework and strategy, and its alignment with business strategy.
2. Monitor material range of data risks (such as security, privacy and regulatory), associated with the use of data, and have visibility into KPIs and other metrics that demonstrate management of data risk.

C. Cybersecurity Oversight.

1. Review the Company's cybersecurity program, including strategy, governance, resourcing, and effectiveness.
2. Monitor significant cyber risks, threat intelligence, incidents, response activities, and remediation plans—including MRAs, MRIAs, KRIs, and maturity assessments.
3. Review management's periodic cybersecurity assessments, including maturity models (e.g., CAT), gap analyses, and risk tolerance alignment.
4. Review GLBA Risk Assessment at least annually.
5. Oversee business continuity, disaster recovery, and incident response capabilities.

C. Change Management & Emerging Technologies.

1. Review the technology, data governance and cybersecurity aspects of significant projects, new products and services, business developments, and acquisition opportunities.
2. Assist the Board in identifying and understanding new and emerging technology issues, trends, opportunities, and threats that may impact the Company's overall business strategy.

D. Policies, Reporting, and Governance.

1. Review and approve relevant policies within its remit.
2. Receive periodic risk reports, including first-, second-, and third line assessments.

3. Coordinate with the Risk Committee to ensure consistent risk oversight, especially where responsibilities intersect.
4. Oversee compliance with applicable regulatory expectations related to cyber and technology governance.
5. Conduct an annual evaluation of its performance.
6. Review and assess the adequacy of this Charter annually, or more frequently as needed, and submit amendments to the Governance Committee and Board for approval.