



**Old Second**  
NATIONAL BANK

# Information Technology Steering Committee

ITSC Charter



## Contents

- MISSION ..... 3
- MEMBERSHIP ..... 3
- MEETINGS ..... 3
- FUNCTIONS & RESPONSIBILITES ..... 3
- I.T. STRATEGY & PROJECTS..... 3
- I.T. SECURITY/INTERNAL CONTROLS..... 4
- ADVISORY ROLE..... 4
- DOCUMENT MANAGEMENT – INFORMATION TECHNOLOGY STEERING COMMITTEE..... 5

# Information Technology Steering Committee

## MISSION

The Information Technology Steering Committee (the “Committee”) is a standing Committee of the Board of Directors of Old Second National Bank (the “Board”). The Committee sets the tone and direction for the Bank's use of IT. The Committee approves the IT strategic plan, information security program, and other IT-related policies.

In addition, the Committee performs the following;

- Annually, approves an IT strategic plan that aligns with the overall business strategy and includes an information security strategy to protect the institution from ongoing and emerging threats, including those related to cybersecurity.
- Promotes effective IT governance.
- Oversee processes for approving the institution's third-party providers, including the third parties' financial condition, business resilience, and IT security posture.
- Oversee and receive update on major IT projects, IT budgets, IT priorities, and overall IT performance.
- Oversee the adequacy and allocation of IT resources for funding and personnel.
- Approve policies to escalate and report significant security incidents to the board of directors, steering committee, government agencies, and law enforcement, as appropriate.
- Hold management accountable for identifying, measuring, and mitigating IT risks.
- Provide for independent, comprehensive, and effective audit coverage of IT controls.

## MEMBERSHIP

The Committee shall consist of the CFO/COO and three or more directors, who shall be appointed from time to time by the Board based on the recommendation of Old Second Bancorp, Inc.'s Nominating and Corporate Governance Committee. A majority of the Committee's composition shall consist of independent directors. One of these directors shall serve as the Committee Chairperson. All members of the Committee shall have a basic understanding of Information Technology management practices, specifically those relevant to the financial services industry. Members of management of the Bank, including the CEO, CTO, the Information Security Officer and Risk Officer, may meet with the Committee as necessary but shall not be considered Committee members.

## MEETINGS

The Committee shall meet with such frequency and at such intervals as it shall determine necessary to carry out its duties and responsibilities, but in no event shall the Committee meet less than three times each year. The Committee shall, at its discretion, meet without members of management present. The Committee may also meet periodically with the Risk Committee or other Board Committees to discuss matters of mutual interest and importance.

The Committee shall maintain minutes of its meetings and records relating to those meetings and the Committee's activities, and shall provide copies of such minutes to the Bank's Board of Directors. The Committee shall determine its rules of procedure.

## FUNCTIONS & RESPONSIBILITIES

The Committee's critical functions and responsibilities include:

### I.T. STRATEGY & PROJECTS

1. Evaluate the Bank's I.T. strategies and the financial, tactical and strategic benefits of proposed major I.T.-related projects and technology architecture alternatives.

2. Critically review and assess the progress of major I.T.-related projects and technology architecture decisions.
3. Discuss I.T. costs and internal processes for approval of major I.T.-related capital expenditures.
4. Make recommendations to the Board with respect to significant I.T.-related projects and investments that require Board approval.
5. Review and approve Critical Vendor list.
6. The Committee maintains the authority to engage independent advisors or consultants, paid for by the Bank, as it deems necessary to make informed decisions regarding the Bank's I.T. initiatives.

## I.T. SECURITY/INTERNAL CONTROLS

1. Review and approve IT and IS related policies.
2. Monitor the quality and effectiveness of the Bank's IT security, and ensure that the Bank has a formal information security process in place, in compliance with the Gramm- Leach-Bliley Act. Specifically, GLBA requires a written information security plan that details the Bank's program to protect customer information.
3. Discuss with the Bank's Information Security Officer high-level executive summary of compliance-related activities with the Information Security program, including mediations to the security program that have been identified.
4. Ensure that the Bank maintains a formal I.T. contingency plan and reviews testing of critical components of this plan at least annually.
5. Holds management accountable for the identification, measurement and mitigation of IT risks in accordance with the Bank's Risk Appetite.
6. Review regular reports regarding Key Risk and Performance Indicators as well as status updates on Regulatory and audit findings.

## ADVISORY ROLE

1. As required, consult with the Bank's senior I.T. management team.
2. Through the Bank's senior I.T. management team, stay informed regarding new technologies, applications and systems that relate to or affect the Bank's I.T. strategy or business plan.
3. Provide input regarding the overall effectiveness of the Bank's I.T. management team.

The Committee shall review and reassess the performance of the Committee and the Committee's role and responsibilities on an annual basis.