

**STERLING BANCORP, INC.**  
**STERLING BANK AND TRUST, F.S.B.**  
**RISK COMMITTEE CHARTER**

---

**PURPOSE**

The Board of Directors of Sterling Bancorp, Inc. (“*Bancorp*”) has appointed the Risk Committee (the “*Committee*”) to assist the Board<sup>1</sup> in fulfilling its oversight responsibilities with regards to the overall risk management programs of Bancorp, Sterling Bank and Trust, F.S.B. (the “*Bank*”), and their respective subsidiaries (collectively, the “*Company*”). The Board understands that effective risk management is a key driver to the long-term safety and soundness of the Company. If the Board is to fully understand the Company’s strategic plan, it also needs to determine the risks inherent in that plan. The Committee also serves as the Risk Committee of the Board of Directors of the Bank.

The Committee shall assist the Board with regards to the Company’s risk management programs as follows:

- Evaluate the Company’s strategic plan as to the nature and magnitude of potential risk exposures;
- Provide an open and ongoing communication forum between management, third parties, and the Board to discuss risks and risk management;
- Oversee the risk management practices of the Company in relation to the identification, measurement, monitoring, controlling, and reporting of the Company’s principal business risks as defined within the Company’s enterprise risk management framework;
- Serve as the primary oversight committee for specified risk areas, to include strategic, operational, and regulatory risks; and
- Provide secondary oversight for risk areas allocated to other Board committees such as credit, financial, and reputational risks, including intersections with the Company’s strategic plan and objectives.

**MEMBERSHIP**

The Committee shall be comprised of three (3) Independent Directors, within the meaning of the Corporate Governance Guidelines, as determined by the Board. The Committee may not have more than two (2) Directors who also serve on the Audit Committee. All Committee members will maintain appropriate knowledge and expertise to remain educated with current risk management concepts. The Committee will include at least one (1) member with risk management experience who will serve as the Chair. Other Committee members may be representatives of the Credit, Asset/Liability, Ethics and Compliance, and Audit Committees. Membership on the Risk Committee is reviewed each year by the Nominating and

---

<sup>1</sup> Reference to the “Board” herein shall refer to the Board of Directors of each of Bancorp and the Bank, unless the context requires otherwise.

Corporate Governance Committee and approved by the Board, which also designates a Chair for the Committee.

## **MEETINGS**

The Committee will meet at the call of the Chair, and the Committee shall convene at least quarterly or more frequently, as needed. At least two (2) meetings shall include executive sessions, without any members of management present. Agendas for the meeting will be distributed to the Committee prior to the meeting date. The Committee shall be governed by the same rules regarding meetings (including meetings in person or by telephone or other similar communications equipment), action without meetings, notice, waiver of notice, and quorum and voting requirements as are applicable to the Board.

The Committee shall meet periodically with the Chief Risk Officer (“**CRO**”) in private sessions to discuss any matters that the Committee or the CRO believes should be discussed.

The Committee may ask any officer or employee of the Company to attend the Committee meeting or for such persons to meet with any members of, or advisors to, the Committee.

The Committee will select a Secretary who will be responsible for taking minutes of the meetings which will be approved at the subsequent meeting.

## **DUTIES AND RESPONSIBILITIES**

In carrying out its mission, the Committee will have the duties, responsibilities, and authority set forth below, as well as other matters specifically delegated to the Committee by the Board. The Committee may carry out additional functions and adopt such other procedures as may be appropriate in light of changing business, regulatory, or other conditions.

1. Ensure the development and oversight of the Company’s risk management framework.
2. Ensure that the Company has a robust risk governance system in place that is commensurate with the Company’s size and complexity.
3. Ensure that an appropriate policy governance process is in place to ensure risks are properly identified, controlled, quantified, and are within the Company’s risk appetite and risk tolerances, including material risks related to the Company’s compliance with all applicable laws and regulations, with relevant risk policies managed and approved at the appropriate Board committee. Such risks include, but are not limited to, capital risk, liquidity risk, credit risk, market risk, operational risk, technological and cybersecurity risks, legal risk, regulatory risk, reputational risk, and other emerging risks.
4. Monitor the Company’s risks and oversee risk management efforts of the Company. While primary oversight responsibility of certain risk categories may reside with a separate Board committee or the full Board, the Committee’s interest extends to all organizational risk types. To that end, the Committee may investigate or authorize a full investigation into any and all areas within its jurisdiction, as well as retain special legal, accounting, or other consultants to advise the Committee or management, as appropriate.
5. Oversee the development of appropriate risk capacity, risk appetite, and risk tolerances.
6. Engage management in an ongoing risk appetite dialogue vis-à-vis its strategic plan as conditions

and circumstances change and new opportunities arise.

7. Review the Company's risk appetite statement annually and approve any material amendments to the risk appetite statement.
8. Review the Company's actual risk profile and risk trending against its risk appetite based on management reports and analysis of its principal business risk categories.
9. Review material reporting on business continuity, vendor risk management, model risk management, and other operational risk programs.
10. Review and approve the selection of new vendors that have been identified as critical per the vendor management risk assessment.
11. Examine external data such as banking trends and economic indicators to gauge the Company's exposure/impact and recommend timely mitigation strategies as necessary.
12. Oversee management's processes regarding the proposal of new strategic initiatives, products, and services to ensure that such endeavors are within the Board's risk appetite and that any such risks are known and proactively mitigated.
13. Understand the Company's information security program, including cybersecurity, and ensure the development of the program as the Company grows and the cyber and information risks change.
14. Ensure the CRO has adequate stature, authority, and resources and is independent from individual business units within the Company. The Chair will provide input to the Chief Executive Officer as to the performance and effectiveness of the CRO as well as provide input into the CRO's succession planning.
15. Receive and review quarterly reports from the CRO and other members of management, as appropriate, to ensure that the Committee is sufficiently informed to effectively fulfill its responsibilities.

The Committee shall, together with the Audit Committee, review audit results prepared by Internal Audit assessing the effectiveness of the risk governance framework, and the Committee may also meet with the Audit Committee on such other topics of common interest or other matters as required by law, regulation, or agreement.

In carrying out these responsibilities and duties, the Committee shall foster an environment which encourages the CRO or any other Company employee to raise any risk issues or concerns freely and without concern for retribution. The CRO and the Chief Compliance Officer each shall have access to communicate with the Committee on any matter relevant to risk and compliance.

## **REPORTING**

The Committee will keep the Board apprised of its activities and shall directly advise the Board in detail of any of its material findings. The Committee shall also make a written report to the Board summarizing its activities, conclusions, and recommendations for the past year and its agenda for the upcoming year.

## **PERIODIC REVIEWS**

The Committee will review and reassess the adequacy of the Charter at least annually and recommend any proposed changes to the Board for approval. The Committee will periodically evaluate the Committee's own performance and present its performance evaluation to the Board.