

## **TIAA RISK AND COMPLIANCE COMMITTEE CHARTER**

*Amended as of December 19, 2024*

### **1. Purpose**

The TIAA Risk and Compliance Committee (“Committee”) is a standing committee of the Board of Trustees (“Board”) of TIAA (“Company”), established to assist the Board in fulfilling its responsibilities relating to (i) the design and implementation of the company’s enterprise wide risk management and compliance frameworks including risk appetite and limits, risk governance and culture, risk and compliance policies, and risk management capabilities established by management to identify, assess, manage and mitigate risk; (ii) the review of management’s assessment of the Company’s risk profile including the major risks facing the Company and associated mitigation plans; (iii) the promotion of ethical behavior and compliance with applicable laws and regulations; (iv) the oversight of the TIAA Corporate Compliance Policy; and (v) any other matters delegated by the Board.

### **2. Responsibilities**

In carrying out the Committee’s responsibilities, each member shall be entitled to rely, in good faith, on information, opinions, reports or statements that are prepared and presented by persons who the Committee members reasonably believe to be reliable and competent in the matters presented, which persons may include, as applicable: (i) one or more officers of the Company or other members of management; (ii) compliance officers and legal counsel or other persons as to matters within the person’s professional or expert competence; or (iii) another committee of the Board.

The Committee’s responsibilities include:

- Promoting the development of appropriate governance, accountability, and transparent processes that foster a culture of risk management, compliance and ethics in the Company’s business activities;
- Setting an appropriate culture of risk management, compliance and tone at the top within the Company by holding management accountable for establishing clear policies regarding the management of compliance matters;
- Overseeing the Company’s Enterprise Risk Management Framework, including reviewing the Enterprise Risk Management Policy and reviewing and monitoring the Company’s Enterprise Risk Appetite Statement and Guidelines and recommending such items or proposed material changes to the Board for approval;

- Reviewing the Company's risk profile and its alignment with the Company's Strategic Plan, objectives, and Enterprise Risk Appetite Statement and Guidelines;
- Reviewing the primary themes of risk across the firm: financial, operational, strategic, compliance, legal and regulatory, and reputational risks and the programs and policies developed to mitigate those risks;
- Reviewing technology-related risks, including cybersecurity and artificial intelligence risks, significant cybersecurity events, and related public disclosure as necessary; approving annually the TIAA Cybersecurity Plan; and monitoring management updates on cybersecurity matters and remediation plans annually or at regular intervals and reporting to the Board as necessary;
- Overseeing the development and management of external consumer data and information sources (ECDIS) and artificial intelligence systems (AIS), including ensuring that appropriate lines of reporting are in place, along with regular, quality reporting; and reviewing and approving the ECDIS and AIS-related policies and procedures at least annually to ensure that they are kept current with changes in use of ECDIS and AIS and best practices in the industry;
- Reviewing the Company's key insurance programs;
- Reviewing annually the enterprise-wide risk management and compliance frameworks including the staffing, independence and reporting structure;
- Reviewing those key risk and compliance policies requiring Board approval, as material changes to such policies occur, and making recommendations for approval to the Board;
- Approving those key risk and compliance policies, approval of which can be provided by the Committee, as material changes to such policies occur;
- Promoting the development of a climate risk management framework, approving enterprise-level climate risk-related policies as material changes occur, and reviewing periodic reports on climate risk and progress on the Company's climate risk program;
- Overseeing enterprise conduct risk, including risk management's conduct risk oversight activities, and risk management components of the Company's culture;
- Reviewing reports of any ethical violations of the Company's policies and allegations of fraudulent conduct or any significant fraud-related incidents involving management, employees, agents or third parties, and all action plans developed in response thereto;
- Reviewing reports of any significant misconduct, integrity concerns and allegations of criminal conduct involving management, employees, agents or third parties;

- Reviewing the TIAA Corporate Compliance Policy and approving as material changes occur. Overseeing its execution including ensuring that compliance issues are resolved effectively and expeditiously by senior management with the assistance of the office of the Chief Risk and Compliance Officer;
- Reviewing summary reports of the confidential or anonymous complaints received from the Company's employees and third parties, along with the status and resolution of the complaints, noting any trending;
- Ensuring through oversight that its views about the importance of risk management and compliance are understood and communicated by senior management across, and at all levels of, the organization through ongoing training and other means;
- Ensuring that the corporate risk and compliance function has an effective and prominent status within the organization including its staffing, independence and reporting structures;
- Reviewing the results of the annual independent compliance risk assessments to understand the enterprise compliance risk profile and its impact to the related Compliance Risk Appetite and Tolerance levels;
- Reviewing reports on the effectiveness of key compliance programs, including the Company's anti-money laundering program, at least annually;
- Reviewing periodic reports from the Chief Risk and Compliance Officer concerning the Company's compliance with applicable laws, regulations and ethical conduct codes and policies, including the Company's Code of Business Conduct and reports of material compliance failures; and
- Reviewing with the Chief Legal Officer legal matters which could be material.

#### Coordination with Certain Other Board Committees and Management

In addition to the Committee's oversight of the Company's material risks, the Audit Committee, the Human Resources Committee, the Nominating and Governance Committee, and the Investment Committee also exercise direct oversight over aspects of the Company's enterprise risk management that fall within each committee's area of responsibility.

The Committee will coordinate with the Audit Committee, the Human Resources Committee, the Nominating and Governance Committee, the Investment Committee, and other committees of the Board, as appropriate, and management, including the Chief Risk and Compliance Officer, to help ensure that the committees have received the information necessary to permit them to fulfill their duties and responsibilities with respect to oversight of risk management and risk assessment guidelines and policies.

### **3. Membership and Organization**

- The Committee shall consist of at least four members of the Board.
- The members of the Committee shall be appointed by the Board and shall serve one-year terms or until their successors are appointed and qualified.
- The Board shall appoint members for a period shorter than one year in the event of a vacancy.
- The Committee may delegate its authority to a subcommittee or subcommittees consisting of the Committee's members.
- The Committee shall promptly inform the Board of the actions taken or issues discussed at its meetings.
- The Committee shall review and reassess this charter periodically and recommend changes to the Nominating and Governance Committee.

### **4. Meetings**

- The Committee shall meet at least four times per year.
- The Chair of the Committee may call a special meeting of the Committee upon due notice to the Corporate Secretary and each other member at least 48 hours prior to the meeting.
- A majority of members shall constitute a quorum.
- A majority of the members present shall decide any question brought before the Committee.

### **5. Advisors**

- The Committee shall have the authority, at the expense of the Company, to retain such risk or compliance professionals, lawyers or other advisors as it shall deem appropriate without prior management approval.

### **6. Performance Review**

- The Committee shall evaluate its performance annually and report its conclusions to the Nominating and Governance Committee.

*The Risk and Compliance Committee's responsibilities and powers as delegated by the Board are set forth in this charter. The Committee relies to a significant extent on information and advice provided by management and independent advisors. Whenever the Committee takes action, it exercises its independent judgment on an informed basis that the action is in the best interests of the Company.*