F5, Inc.
Risk Committee Charter

As amended and restated by the Board of Directors of F5, Inc. as of July 23, 2026.

Purpose

The purpose of the Risk Committee (the "Committee") of the Board of Directors (the "**Board**") of F5, Inc. is to assist the Board in its oversight of management's responsibility to implement effective risk management reasonably designed to identify, assess, and manage the Company's Strategic, Operational, and Technology risk profile of F5, Inc. (the "Company"). The Committee's responsibilities include monitoring, reviewing, and providing guidance regarding applicable risk policies and processes, including certain associated frameworks, as well as providing feedback on related risk analysis and reporting, as established by management.

Composition

Membership and Appointment. The Committee shall consist of three or more members of the Board. Members of the Committee shall be appointed by the Board upon the recommendation of the Nominating and Governance Committee and may be removed by the Board with or without cause at its discretion. Each member of the Committee shall meet the independence requirements of the Nasdaq Stock Market LLC ("Nasdaq"), and regulations of the Securities and Exchange Commission (the "SEC").

Qualifications. The Committee membership shall, in the determination of the Board, consist of the appropriate backgrounds and experience to discharge the oversight duties and responsibilities of the Committee, and the Committee membership shall meet all applicable regulatory or legal requirements regarding expertise and other qualifications, if any.

Chairperson. The Board may designate a chairperson of the Committee. In the absence of that designation, the Committee may designate a chairperson by majority vote of the Committee members.

Meetings and Authority

The Committee shall meet at least four times each year (with additional meetings as often as it determines is appropriate or necessary). The chairperson shall preside at all meetings of the Committee and shall set the agenda. The Committee may act by written consent (which may include electronic consent), which shall constitute a valid action for the Committee if it has been approved by each Committee member and shows the date of approval. Any written consent will be effective on the date of last signature and will be filed with the minutes of the meetings of the Board.

The Committee shall keep written minutes of its proceedings, which minutes will be filed with the minutes of the meeting of the Board.

The Committee shall meet periodically with the Head of Enterprise Risk Management ("ERM") and other key risk management leaders (e.g., Chief Information Security Officer ("CISO"), Chief Compliance Officer, Chief Privacy Officer, Chief Digital Officer, Chief Product Officer, or Chief Human Resources Officer), as the Committee deems appropriate, including in private session to discuss any matters that the Committee or the key risk leaders believe should be so discussed. The Committee shall meet periodically in executive session.

The Committee may invite to its meetings any director, officer, or employee of the Company and such other persons as it deems appropriate to carry out its responsibilities. The Committee may also hold closed sessions or meet in executive session, including any individuals whose presence is required, as it deems appropriate to carry out its duties.

The Committee shall also exercise any other powers and carry out any other responsibilities, or perform any other functions, consistent with this charter, the purposes of the Committee, the Bylaws, applicable Nasdaq rules, and the laws of the state of Washington as the Committee or the Board deem appropriate.

The Committee is authorized to adopt its own rules of procedure for notice and conduct of its meetings, so long as they are not inconsistent with (a) any provision of this charter, (b) any provision of the Amended and Restated Bylaws of the Company (the "Bylaws") that are applicable to the Committee, or (c) the laws of the state of Washington.

Duties and Responsibilities

Specific Risk Domain Focus. The Committee is charged with directly reviewing key risk reporting on strategic, operational, and technology risk domains.

The Company's Enterprise Risk program divides risk into five major Domains (Financial, Legal & Regulatory, Strategic, Operational, and Technology). The Committee shall focus their review of risk reporting on Strategic, Operational, and Technology domains; provided, however, that oversight of People risks, a subsection of Operational Risk, shall be delegated to and reviewed by the Talent and Compensation Committee. Financial and Legal & Regulatory risks shall be reviewed by the Audit Committee.

The review of risk domain reporting shall include assessment of the company's risk exposure and evaluate the adequacy and effectiveness of related risk management processes and policies. Additional specific risk reporting may be reviewed. These risk reports may include emerging and dynamic risk areas including Artificial Intelligence, data privacy, cybersecurity, product/system management and development, and enterprise resilience, which have source risks in strategic, operational, and technology domains.

In connection with this specific domain focus, the Committee will:

1. Review and advise on the Company's strategic, technology, and operational risk strategies: cybersecurity, resiliency, crisis and incident management, and security-related information technology planning processes, and review strategy and implementation for investing in related systems, controls, and procedures with the Company's management.

2. Review the Company's compliance with applicable global data protection and security laws and regulations, and the Company's adoption and implementation of systems, controls and procedures designed to comply with such laws and regulations.

3. Review the plans and methodology for the periodic assessment of the Company's cybersecurity, technical, and operational risk and incident response and disaster recovery capabilities by outside professionals, any findings of such assessments and any remediation plans to address any material deficiencies or other material matters identified by such assessments.

4. Review analysis of the in-focus Company risks by management and third parties, as applicable; if issues develop between meetings of the Committee that the Chief Technology Operations Office ("CTOO") believes could have a material adverse impact on the company, the CISO or other key risk management leader will promptly report such issues to the chairperson of the Committee.

5. Review the Company's cybersecurity insurance program.

6. Evaluate the Company's disclosure controls and procedures related to cybersecurity to ensure timely and accurate reporting of cybersecurity and operational risks and incidents to SEC and stakeholders, as appropriate.

*Reporting to the Board of Directors***.** The Committee shall report regularly to the Board with respect to the Committee's activities.

Other Matters

Retention of Advisors. The Committee has authority to retain advisers when it deems appropriate, including approval of fees and terms of retention, without the prior permission of the Board or management, and shall be provided the necessary resources for such purposes.

Subcommittees. The Committee may, from time to time, delegate duties or responsibilities to subcommittees or to one member of the Committee.

Third Party Reports. The Committee may receive and, if appropriate, respond to third party (including attorney, auditor, consultant, or other provider) reports regarding cybersecurity or privacy incidents or other associated disclosure or related requirements. The Committee shall establish procedures for the confidential receipt, retention, and consideration of any such report.

Charter Review. The Committee shall review and assess the adequacy of this charter periodically and submit any recommended changes to the charter to the Board for approval.

Performance Review. Evaluate the Committee's own performance on a periodic basis.