

UNISYS CORPORATION

SECURITY AND RISK COMMITTEE CHARTER (Approved May 1, 2024)

Purpose

The Security and Risk Committee (the “Committee”) is appointed by the Board of Directors (the “Board”) of Unisys Corporation (the “Corporation”) to assist the Board in its oversight responsibilities with regard to the Corporation’s company-wide security and enterprise risk management practices, including overseeing the practices, procedures and controls that management uses to identify, manage and mitigate risks related to cybersecurity, privacy, disaster recovery, and other key enterprise risks that the Corporation faces such as strategic, commercial, physical security, property, work place safety, legal, regulatory, and reputational risks.

Membership

The Committee shall consist of at least three directors, each of whom shall meet the independence requirements of the New York Stock Exchange. Any action taken by the Committee during a period in which one or more of the members subsequently is determined to have failed to meet the membership qualifications shall nevertheless constitute duly authorized actions of the Committee and shall be valid and effective for all purposes, except to the extent required by law or determined appropriate by the Committee to satisfy regulatory requirements.

The members of the Committee shall be appointed and replaced by the Board.

Responsibilities

Management of the Corporation has responsibility to manage the Corporation’s security and enterprise risk management practices, procedures and controls. The Committee has an oversight role, and in fulfilling that role, may rely on reviews and reports provided by management and the Committee’s advisors. In performing its oversight responsibilities, the Committee shall:

1. Review management’s implementation of cybersecurity programs, privacy programs and risk policies and procedures and management’s actions to (a) safeguard the effectiveness of such programs and policies and the integrity of the Corporation’s electronic systems and facilities and (b) prevent, detect and respond to cyber-attacks or information or data breaches involving the Corporation’s electronic information, intellectual property and data.
2. Receive information from the Chief Information Security Officer (the “CISO”) regarding matters related to the management of cybersecurity risk and information from the chief privacy officer regarding matters related to the management of privacy risks, in each case as the Committee deems appropriate.

3. Review management's crisis preparedness and incident response plans (including policies and procedures regarding public disclosure of any such incidents) and the Corporation's disaster recovery capabilities.
4. Receive and review summaries of any incidents or activities that are required to be reported to the Board or the Committee pursuant to any escalation policies applicable to the CISO.
5. Monitor the Corporation's enterprise risk profile, its ongoing and potential exposure to risks of various types, and, in doing so, the Committee recognizes the responsibilities delegated to other committees by the Board and understands that the other committees may emphasize specific risk monitoring through their respective activities. Specifically, the Compensation and Human Resources Committee shall continue to have oversight responsibility for risks relating to the Corporation's compensation arrangements (including risks related to the Corporation's pension, welfare and employee benefit plans), senior executive succession planning and talent management and the Audit and Finance Committee shall continue to have oversight responsibility for risks relating to the Corporation's financial reporting (including internal control over financial reporting), capital structure, financial and budgeting requirements, financial risks related to the Corporation's pension, savings and welfare plans, investor relations, violations of the Corporation's Code of Ethics and Business Conduct, taxes and acquisitions and dispositions.
6. Receive and review information from management regarding the activities of the Corporation and discuss matters related to the Corporation's risk profile as appropriate, including a risk heat map identifying the risks to the Corporation and the potential for occurrence and expected impact on the Corporation for each identified risk.
7. Review and discuss with management the effectiveness of the Corporation's risk management programs and its practices for identifying, managing and mitigating risks across all business functions and recommend improvements, where appropriate.
8. Review and approve the framework for adopting policies and procedures establishing risk-management governance, risk-management procedures, and risk control infrastructure.
9. Oversee the processes and systems for implementing and monitoring compliance with risk-management and risk-control policies and procedures, including:
 - a. Processes and systems for identifying and reporting risks (including emerging risks) and risk management deficiencies, and implementation of actions to address risk-management deficiencies; and
 - b. Processes and systems to integrate risk management and associated controls with management goals.

10. Review significant investments and expenditures the Corporation proposes to make to manage or mitigate enterprise risks and make recommendations, where appropriate.
11. Receive and review reports and presentations from management and the Committee's advisors, including outside experts, regarding the management of enterprise risk programs.
12. Review and address, as appropriate, management's corrective actions for deficiencies that arise with respect to the effectiveness of enterprise risk management programs.
13. Review the adequacy of the Corporation's insurance programs to determine if the coverages are sufficient, consistent with market conditions, to protect the Corporation.
14. Review, with the Corporation's general counsel or their designee, any legal matter that could have a significant impact on the Corporation's business or reputation.
15. Address other matters as the Committee Chair or other members of the Committee determine relevant to the Committee's oversight of enterprise risk assessment and management.

Meetings; Operational Matters and Reports

The Committee is to meet periodically in separate executive sessions with such members of management, including the Corporation's COO, CISO and chief privacy officer as the Committee deems appropriate, and shall have other direct and independent interaction with them from time to time as the Committee deems appropriate.

The Committee may form and delegate authority to subcommittees when appropriate.

In connection with its duties and responsibilities, the Committee shall have full access to all books, records, facilities and personnel of the Corporation as deemed necessary or appropriate by any member of the Committee to discharge his or her responsibilities hereunder. The Committee shall also have authority to pay, at the expense of the Corporation, ordinary administrative expenses that, as determined by the Committee, are necessary or appropriate in carrying out its duties. The Committee shall have the authority to retain outside legal, accounting or other advisors, including the authority to approve the fees payable by the Corporation to such advisors and other retention terms. The Corporation shall provide the funding for the payment of such fees.

The Committee shall annually review its performance. In addition, the Committee shall review and reassess the adequacy of this Charter annually and recommend to the Board any changes it considers necessary or advisable.

The Committee shall make regular reports to the Board.