# The CyberGov™Framework – Optimizing Your Cybersecurity Posture v. 8.0, 14 Dec 2023

**Principle 1.0:** **Establish**

**Practice 1.1**: Board members acknowledge their role as fiduciaries.

**Practice 1.2:** Risk management identification as part of the organization’s mission is understood and communicated. GV.OC-01

**Practice 1.3:** Legal, regulatory, and contractual requirements regarding cybersecurity are understood and communicated. GV.OC-03

**Practice 1.4:** Develop agreed upon written and electronic protocols for effective communication between board and staff to facilitate efficient decision making.

**Principle 2.0:** **Plan**

**Practice 2.1:** Organizational cybersecurity policies, processes, and procedures are established, communicated, and enforced. GV-PO (formerly ID.GV-01)

**Practice 2.2:** Risk appetite and risk tolerance statements are determined, communicated, and maintained. (formerly ID.RM-02, ID.RM-03)

**Practice 2.3:** Overall risk management objectives and tolerances are defined and agreed upon by board/staff and updated at least annually.

**Practice 2.4:** Use standardized criteriatoreview threat vulnerabilities assessments briefings by staff at least semiannually.

**Practice 2.5:** Include ongoing education to help employees to be aware of nontechnical risks and know how to spot them. GV.RR-04

**Practice 2.6:**  Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties. GV.RM-05

**Practice 2.7**: A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks to include the supply chain is established and communicated. GV.R|M-02

**Practice 2.8**: Strategic opportunities (i.e., positive risks) are identified and included in organizational cybersecurity risk discussions. GV.SC-02

**Practice 2.9:** Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally. Formerly ID.AM-06

**Principle 3.0:** **Do**

**Practice 3.1**: Establish an overall enterprise risk management committee to include HR as a subset of the board and include a member knowledgeable in cybersecurity.

**Practice 3.1:** Regularly monitor the legal and regulatory environments for changes and updates affecting compliance and reporting.

**Practice 3.2:** Provide a means for senior staff and the board to monitor issues globally, by region, country and/or company on an ongoing basis.

**Practice 3.3:** Include relevant suppliers and other third parties in incident planning, response, and recovery activities. Formerly ID.SC-05

**Practice 3.4:** Confirm that cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes. Formerly ID.SC-02

**Practice 3.5:** Confirm that the company is meeting the administrative requirements for reporting to the SEC and other agencies making sure to include detailed reports on a timely basis in case of a cyber breach or ransomware attack.

**Practice 3.6:** Establish cyber protocols for use in merges and/or acquisitions to be used to assess risk prior to acquisition.

**Practice 3.7:** Confirm that suppliers and other third parties are included in incident planning, response, and recovery activities. Formerly ID.SC-05

**Practice 3.8**: Identify the most likely cyber threats (bad actors, nation states, etc) and conduct regular testing.

**Practice 3.9:** Cybersecurity is included in human resources practices. CV.RR-04

**Principle 4.0: Incidence response and crisis management**

**Practice 4.1:** Policies, processes, and procedures for managing cyber breaches internally are established and reviewed at least annually.

**Practice 4.2:** Maintain an ongoing audit-like record of the who, what, where, when, and how the issues are resolved.

**Practice 4.3:** Establish internal crisis management team together with outsider experts, to include designated person to brief the board.

**Practice 4.4:** Develop an incidence response team, together with outside experts, to include an action plan, a check list to follow, and point person for reporting to the board.

**Practice 4.5:** Conduct regular practice sessions in anticipation of when a cyber event will take place. Use real data in planning practice.

**Practice 4.6:** Establish a crisis management teamto coordinate with expert advisors to represent the company in the public domain and include regular training and simulated event response.