Eleos Governance, Risk & Compliance (eGRC) Policy

Purpose:

The purpose of Eleos' GRC program is to provide a comprehensive framework designed to strategically identify, manage, and mitigate risk in order to enhance individual health, safety, and protection from harm, and optimize meeting the goals of individuals. This includes improving the ability to identify and reduce risk to individuals and to ensure a high quality of support services that we deliver. Additionally, the policy covers potential risks associated with non-compliance with applicable federal, state, and local regulations and laws, DDD guidelines, and Eleos' internal policies and procedures.

Scope:

This policy is organization-wide, as such it applies to all functional areas - divisions, departments and staff regardless of position or rank.

Policy Statement:

The GRC program is overseen by the Board, President and Executive Management Team, with day-to-day management delegated to the Compliance Manager. The Compliance Manager is responsible for developing and implementing the GRC program, in coordination with other key stakeholders across the organization.

The GRC program is designed to be an ongoing process of risk assessment, mitigation, and monitoring. It is important to note that risk is an ever-changing landscape, and the GRC program must be flexible enough to adapt to new risks and changing circumstances.

Review & Revisions:

This policy should be reviewed and updated regularly to ensure its effectiveness in addressing evolving risks and challenges. The policy will be reviewed for potential updates at a frequency of no less than once annually, however certain factors such as our organization's size, regulations and risk profile, may require ad-hoc updates.

Governance, Risk Management & Compliance Policy Outline

Continuous Assessment: Assessing our organization's current governance, risk management, and compliance practices.

Define Objectives: GRC will define the objectives of the GRC framework. These objectives should align with the organization's overall strategic goals and objectives.

Identify Risks: Conduct a thorough risk assessment to identify and prioritize the key risks facing the organization. Risks can include operational, financial, legal, regulatory, reputational, and strategic risks.

Establish Policies and Procedures: Develop comprehensive policies and procedures to address governance, risk management, and compliance requirements.

Policies and Procedures: Comprehensive policies and procedures to address the identified risks and ensure compliance with regulations.

Implement Controls: Implement controls to mitigate identified risks and ensure compliance with policies and regulations. Controls can include preventive, detective, and corrective measures designed to reduce the likelihood and impact of risks.

Assign Responsibility: Clearly define roles and responsibilities for managing governance, risk, and compliance within the organization. Establish accountability for implementing and maintaining the GRC framework, including oversight from senior management and the board of directors.

Provide Training and Awareness: Ensure that employees receive adequate training and awareness programs on the organization's GRC policies, procedures, and expectations. Training should be tailored to different roles and responsibilities within the organization and should emphasize the importance of compliance and risk management.

Monitor and Review: Establish processes for monitoring and reviewing the effectiveness of the GRC framework on an ongoing basis. This includes conducting periodic risk assessments, evaluating control effectiveness, monitoring compliance with policies and regulations, and assessing the impact of changes in the internal or external environment.

Report and Communicate: Implement reporting mechanisms to communicate key GRC-related information to relevant stakeholders, including senior management, the board of directors, regulators, and external auditors. Reports should provide insight into the organization's risk profile, compliance status, and the effectiveness of control measures.

Continuous Improvement: Continuously evaluate and improve the GRC framework based on feedback, lessons learned, and changes in the business environment. This includes updating policies and procedures as needed, enhancing control measures, and adapting to evolving risks and regulatory requirements.

Please reference our Eleos Risk Management Plan 2024 for more information.

What is a GRC Framework?

A GRC framework is a structured approach that helps Eleos to manage governance, risk, and compliance (GRC) effectively. The right framework, when implemented effectively and monitored continuously, can improve efficiency, ensure compliance, and promote responsible decision-making.

What are the Key Capabilities of GRC?

- Capabilities of the GRC solution include:

Governance

- Enterprise risk management and assessment
- Board compliance capabilities such as options policy compliance, ethics and policy compliance, etc.
- Business performance reporting such as balanced scorecards, risk scorecards, operational controls dashboards, etc.
- Policy management, documentation, and communication

Risk Management

- Risk identification and reporting
- Risk assessment of Risk analysis and prioritization
- Root cause analysis of issues and mitigation
- Risk analytics and trend analysis

Compliance

- Flexible controls hierarchy
- Assessments and audits
- Issue tracking and remediation
- Analytics
- Integrated policy and document management capability that should cut across all GRC departments

What are GRC Controls?

GRC controls refer to the policies, procedures, and activities implemented within our organization Governance, Risk, and Compliance (GRC) framework to manage their risks effectively, maintain compliance with regulations, and achieve strategic goals ethically, effectively and responsibly. Additional information related to our controls can be found within our Risk Management Plan document.

Three Lines of Defense (3LOD)

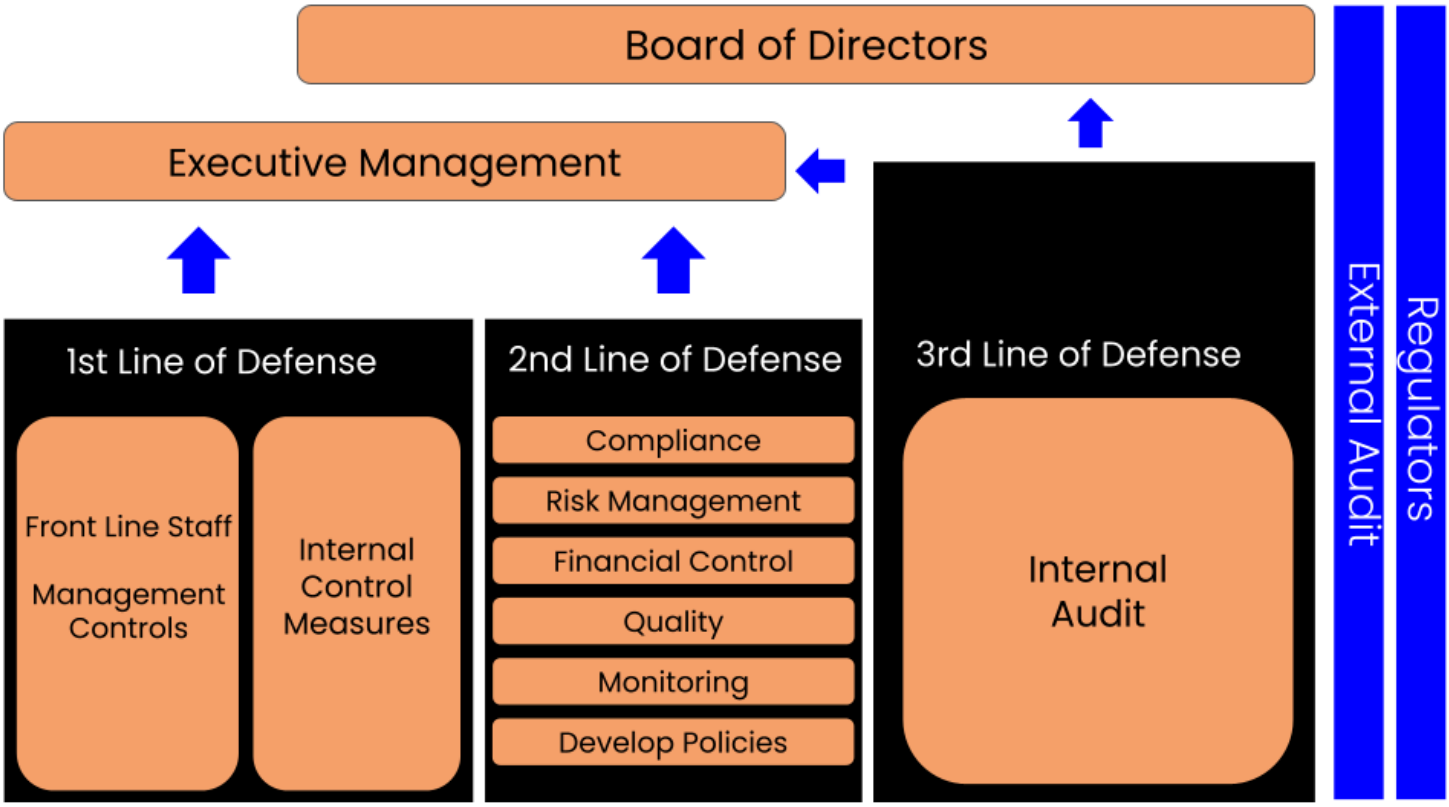
A "line of defense" refers to a distinct level within our organization responsible for managing and mitigating risks, with each line having specific roles and responsibilities in ensuring adherence to regulations, policies and procedures, typically categorized as the first line (frontline staff, management), second line (compliance and risk management), and third line (internal audit) which independently assesses the effectiveness of the other lines; essentially acting as a layered approach to risk management.

The Risk Management Framework at Eleos employs a three lines of defense model:

- **First Line of Defense: (Frontline Staff, Supervisors & Management)**
  Operational management is responsible for the daily identification, assessment, and mitigation of risks. They are responsible for identifying, assessing, and mitigating risks on a day-to-day basis. They also have to implement corrective actions.
- **Second Line of Defense: (Governance, Risk Management, Compliance (GRC))**
  This is the risk management and compliance functions. The Compliance Manager oversees risk management activities, develops policies, and implements procedures and controls and the subsequent training. GRC is responsible for overseeing the risk management activities of the first line of defense.
- **Third Line of Defense: (Governance, Risk Management, Compliance (GRC))** Internal audit provides independent assurance to the board and senior management regarding the effectiveness of the risk management framework. This is the internal audit function. The internal audit function provides independent assurance to the board and senior management that the risk management framework is operating effectively.

This framework ensures a comprehensive approach to risk management within the organization.

The three lines of defense model is a helpful tool for our organization. By adhering to the three lines of defense model, Eleos will ensure strong and robust risk management capabilities and reduce the likelihood of non compliance and adverse events.



Internal Audit

Internal audits are a critical part of our company and the compliance and risk management program. Internal audits help to identify weaknesses in internal controls and ensure that the organization is meeting all applicable laws and regulations. Internal audits can also help to identify areas where the organization can improve its efficiency and effectiveness.

GRC Roles and Responsibilities

A successful GRC program integrates into the organization culture, ethics, and principles. Compliance is not just about rules; it is about behavior and attitude. Management at all and various levels of the organization, like Board, President, Executive Director and Operations Manager are an important nexus of GRC insight across the organization and will need to work together and communicate regularly.

Board & Executive Management

Cultivating a culture of compliance and maintaining a high level of integrity among staff members are growing challenges today due to greater regulatory oversight and potential risk factors. The Board & Executive Management helps staff members to adopt policies and procedures, follow the code of ethics, and adhere to principles of corporate governance.

Below is a high-level overview of a few executive roles that are usually considered by our organization to take up the challenge to maintain a world-class GRC program across the organization:

Board of Directors:

- **Oversight:** GRC framework should include "oversight from senior management and the board of directors." This suggests that the Board is responsible for overseeing the implementation and effectiveness of the GRC program.
- **Reporting:** GRC-related information should be communicated to senior management, the board of directors, regulators, and external auditors as is applicable and appropriate. This implies that the Board receives regular reports on the organization's risk profile, compliance status, and the effectiveness of control measures.
- **Accountability:** Accountability for implementing and maintaining the GRC framework. While this responsibility is shared with senior management, the Board's oversight role suggests that they hold the ultimate accountability for the program's success.

President & Executive Director

- Financial reporting, performance management, budgeting, and other financial processes provide the Board & Senior Management with detailed insight into the workings of virtually each division and department within the organization. Further, as the advantages and potential pitfalls of managing the financial processes and enterprise compliance are quite similar, it follows that the President & Executive Director could provide leadership in the area of organization-wide financial compliance.

Compliance Manager

Compliance Managers are entrusted with ensuring that the organization has the processes and controls to meet the requirements imposed by governmental bodies, regulators, industry mandates like Anti-Money Laundering, Foreign Corrupt Practices Act, cGMP, GLBA or internal policies. However, as the multiple compliance initiatives become more intertwined from regulatory and organizational perspectives, Chief Compliance Officers are also focusing on effective rationalization of controls to provide a clear, unambiguous process for compliance management

and to deliver a single point of reference for the organization.

- Compliance Manager's role has evolved from that of managing a predetermined set of risk exposures to identifying core business areas where the organization should be willing to retain risks to seize growth opportunities while ensuring compliance with applicable regulations. This ties risk management to business performance and changes the risk management from an exclusive centralized function to a federated, top-down approach aligned centrally with business objectives and reporting and assessments are distributed to lines of business for ownership, execution and accountability. By managing risk appetite and response to risks, Compliance drives organizational behavior.

- Internal Auditers are accountable for monitoring risks and ensure compliance across organizational silos and the role is evolving into an independent and horizontal function. This requires a common framework for all types of audits – financial, risk, operations, internal, suppliers, and compliance –such that auditing priorities are determined by an enterprise-level risk-based approach and not departmental and tactical imperatives.

- Cultivating a culture of compliance and maintaining a high level of integrity among staff members are growing challenges today due to greater regulatory oversight and investor activism. Compliance helps staff members to adopt policies and procedures, follow the code of ethics, and adhere to principles of corporate governance.

Human Resources Director

Providing guidelines, monitoring processes and providing constant access to information, rigorous training and awareness programs on compliance and ethics is proving essential to ensure effective implementation of governance programs. Most HR managers provide an integrated training platform to ensure compliance with HR policies and procedures, compliance with governmental health and safety regulations, and compliance training and certification.

Version	Date	Author	Changes
0.1	February 2023	Marquis Johnson	First Draft
0.2	November 2024	Marquis Johnson	Added Controls, LOD