U.S. Commodity Futures Trading Commission
OFFICE OF INSPECTOR GENERAL

AUDIT OF CFTC's ENTERPRISE RISK MANAGEMENT PROGRAM (ERM)

Project Number: 24-AU-05

MARCH 5, 2025

U.S. Commodity Futures Trading Commission
OFFICE OF INSPECTOR GENERAL

MEMORANDUM

TO: Caroline Pham, Acting Chairman
Kristin Johnson, Commissioner
Christy Goldsmith Romero, Commissioner
Summer Mersinger, Commissioner

FROM: Christopher Skinner, Inspector General

DATE: March 5, 2025

SUBJECT: Performance Audit of CFTC's Enterprise Risk Management Program (ERM)

Attached is the Independent Auditor's Report of the U.S. Commodity Futures Trading Commission's (CFTC or Commission) Enterprise Risk Management (ERM) Program. We contracted with Williams, Adley & Company-DC, LLP (Williams Adley) to examine the effectiveness of the CFTC's ERM process as well as its maturity. Williams Adley conducted the audit in accordance with Generally Accepted Government Auditing Standards (GAGAS) and is responsible for the attached audit report and the conclusions expressed therein.[1] The OIG monitored the auditor's progress throughout the performance audit and reviewed the respective audit report and related documentation.

In summary, Williams Adley determined that the CFTC's ERM program requires substantial enhancements to achieve an acceptable level of maturity to be operational and effective. The auditor identified three findings related to the lack of proper governance and communication, lack of comprehensive policies and procedures, and lack of sufficient resources and processes for implementation of the program within the organization. In addition, Williams Adley reported twenty recommendations related to the findings in efforts to increase program maturity.

On January 27, 2025, we provided management with a draft report for review and comment. In its February 24, 2025, response, management concurred with all findings and recommendations. Williams Adley included management's response in Appendix 3 of this report.

We appreciate the cooperation and support received from CFTC personnel during the audit. If you have any further questions, please contact Miguel Castillo, assistant inspector general for audits or Branco Garcia, senior auditor.

[1] The OIG does not express opinions on the Commission's Enterprise Risk Management program or whether it complied substantially with OMB guidance.

Commodity Futures Trading Commission (CFTC)
Enterprise Risk Management Performance Audit
FY 2024

Contract No: 9523ZY24A0001
March 3, 2025

WILLIAMS ADLEY

March 3, 2025

Mr. Jeffrey Sutton
Executive Director
Commodity Futures Trading Commission
1155 21st Street, NW
Washington, DC 20581

Dear Mr. Sutton:

Williams, Adley & Company-DC, LLP (Williams Adley) conducted a performance audit of the Commodity Futures Trading Commission's (CFTC or "the Commission") Enterprise Risk Management (ERM) program. We conducted the performance audit under Order Number 9523ZY24A0001, dated July 23, 2024.

We conducted our audit in accordance with the applicable Government Auditing Standards, 2018 revision. The audit was a performance audit, as defined by Chapter 8 of the Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. The specific objectives of the audit were to 1) assess the effectiveness of the CFTC's ERM process with specific attention to governance and internal control integration and 2) determine CFTC's ERM program maturity using the Committee of Sponsoring Organizations of the Treadway Commission (COSO) model.

To accomplish our objectives, we interviewed personnel from the CFTC as well as reviewed applicable documents, policies, and procedures relevant to the ERM program. Appendix 1 provides a detailed description of our objectives, scope, and methodology. We appreciate the opportunity to have conducted this audit. Should you have any questions or need further assistance, please contact us at (202) 371-1397.

Leah Southers, CPA, CISA, CGFM, CFE
Partner

Contents

RESULTS IN BRIEF

Williams, Adley & Company-DC, LLP (Williams Adley) conducted an independent performance audit of the Commodity Futures Trading Commission's (CFTC or "the Commission") Enterprise Risk Management (ERM) program. Specifically, we examined the effectiveness of the CFTC's ERM process as well as its maturity.

Based on the procedures performed, we determined that most of the CFTC ERM policies and procedures are still in draft form and the program requires substantial enhancements to achieve an acceptable level of maturity to be operational and effective.

Specifically, we noted the following findings which management should address to ensure that the CFTC's ERM program reaches the level of acceptable maturity to be operational and effective.

Finding 1: CFTC lacks proper governance and communication over Its ERM program.

Finding 2: CFTC lacks comprehensive policies and procedures for its ERM program.

Finding 3: CFTC lacks sufficient resources and processes for implementation of the ERM within the organization.

We recommend CFTC takes the following actions:

Recommendation 1: Establish a Risk Management Committee and include key personnel and stakeholders from different CFTC Divisions.

Recommendation 2: Create the Governance Charter and hold regular meetings with the Risk Management Committee.

Recommendation 3: Update and finalize an ERM roadmap from 2020 which includes estimated and actual completion dates.

Recommendation 4: Develop Annual Risk Analysis Reports and distribute to the various divisions.

Recommendation 5: Implement an Enterprise Governance, Risk and Compliance (eGRC) Tool which will help aggregate risks across the enterprise and map them to strategic objectives.

Recommendation 6: Enhance ERM communication channels and hold regular meetings between the ERM team and divisions.

Recommendation 7: Increase CFTC leadership support and conduct regular briefings and workshops, and actively participate in ERM activities.

Recommendation 8: Foster a collaborative environment by appointing ERM liaisons within each division.

Recommendation 9: Conduct training sessions to educate employees about the ERM program and its benefits.

Recommendation 10: Develop a formal ERM policy that outlines the framework, objectives, and scope of the program. This policy should be approved by senior management and communicated across the organization.

Recommendation 11: Create standardized procedures to conduct ERM assessments including guidelines for risk identification, assessment, mitigation, and monitoring.

Recommendation 12: Define its ERM risk rating methodology to consistently evaluate and prioritize risks and align this methodology with the organization's risk appetite and tolerance levels.

Recommendation 13: Maintain a centralized risk register to document all identified risks as well as the risk owners, mitigation strategies, and monitoring plans.

Recommendation 14: Establish a timeline and criteria for conducting regular risk assessments and continuously monitoring and managing risk with at least an annual risk assessment.

Recommendation 15: Regularly review and update the ERM program to incorporate best practices and lessons learned to strive for continuous improvement.

Recommendation 16: Enhance its ERM team capacity and prioritize hiring skilled ERM professionals and provide ongoing training to existing staff. Further, the CFTC should integrate the ERM roles and responsibilities into existing job descriptions through cross-training and encourage participation in training, conferences, and other professional development opportunities. The CFTC should also leverage external expertise to provide support and guidance during the development phase of the ERM program.

Recommendation 17: Ensure ERM considerations are integrated into the strategic planning process with active involvement from senior executives.

Recommendation 18: Improve its processes by investing in technology that supports ERM activities, such as risk assessment tools and data analytics platforms. CFTC should also implement an Enterprise Governance, Risk, and Compliance (GRC) tool to aggregate risks across the enterprise and map them to overarching strategic objectives.

Recommendation 19: Address budget constraints by reevaluating the resources dedicated to the ERM program and alternative explore cost-effective solutions and tools to enhance the ERM program without significant financial investment.

Recommendation 20: Strengthen its organizational resilience by conducting regular risk awareness and training sessions for all employees to build a risk-aware culture and establish a feedback loop to continuously assess and improve the ERM program based on lessons learned and emerging best practices.

Management has reviewed the audit findings and they concur with the recommendations.

BACKGROUND

The CFTC is an independent federal agency with approximately 710 employees as of September 30, 2024. Congress created the CFTC as an independent agency via the Commodity Futures Trading Commission Act of 1974 with the mandate to regulate commodity futures and option markets in the United States. The Commodity Exchange Act was passed to serve the public interest by creating a self-regulating system of trading facilities, clearing systems, market participants, and market professionals with oversight from the CFTC. The agency's mandate has been renewed and expanded several times since then, most recently in July 2010 by the Dodd-Frank Wall Street Reform and Consumer Protection Act.

The mission of the CFTC is to promote the integrity, resilience, and vibrancy of the U.S. derivatives markets through sound regulation. CFTC fosters markets that accurately reflect the forces of supply and demand and are free of disruptive activity by overseeing trade execution facilities, derivatives clearing organizations, swap dealers, data repositories, futures commission merchants, introducing brokers, commodity pool operators, commodity trading advisors and other market participants. The CFTC conducts surveillance, reviews new exchange applications, and assures that market participants comply with the Commodity Exchange Act and Commission regulations, including requirements imposed by the Dodd-Frank Wall Street Reform and Consumer Protection Act.

Enterprise Risk Management (ERM) is a comprehensive, structured approach used by organizations to identify, assess, manage, and monitor risks across all aspects of the business to achieve strategic objectives and ensure long-term sustainability. ERM involves considering risks from all sources (financial, operational, strategic, regulatory, etc.) and developing strategies to mitigate or manage these risks.

ERM also plays a crucial role in the federal government by helping agencies and departments systematically identify, assess, manage, and monitor risks to ensure they can effectively achieve their missions and meet public service goals.

Office of Management and Budget (OMB) Circular No. A-123 requires agencies to integrate risk management and internal control functions. The Circular also establishes an assessment process based on the Government Accountability Office’s (GAO) Standards for Internal Control in the Federal Government (known as the Green Book) that management must implement in order to properly assess and improve internal controls over operations, reporting, and compliance.

The primary compliance indicators that management must consider when implementing OMB Circular No. A-123, include:

1. Management is responsible for the establishment of a governance structure to effectively implement, direct and oversee the implementation of the Circular and all the provisions of a robust process of risk management and internal control.
2. Implementation of the Circular should leverage existing offices or functions within the organization that currently monitor risks and the effectiveness of the organization’s internal control.

3. Agencies should develop a maturity model approach to the adoption of an ERM framework. For FY 2016, Agencies are encouraged to develop an approach to implement ERM. For FY 2017 and thereafter Agencies must continuously build risk identification capabilities into the framework to identify new or emerging risks, and/or changes in existing risks (See Section II.C. for additional details).
4. Management must evaluate the effectiveness of internal controls annually using GAO's Standards for Internal Control in the Federal Government. (The Green Book)[1]

Effective ERM and its components enable governments to continue meeting the needs of their citizens without unnecessary expenditures related to risk.

Periodically, the CFTC Office of Inspector General (OIG) identifies a program within the agency to audit, inspect, or evaluate. CFTC OIG contracted with Williams Adley to perform an audit of CFTC's ERM maturity posture and program capabilities. The objectives of our audit are to: 1) assess the effectiveness of the CFTC's ERM process with specific attention to Governance and Internal Control Integration and 2) determine CFTC's ERM program maturity using the COSO model.

Our performance audit was conducted in accordance with Generally Accepted Government Auditing Standards (Yellow Book or GAGAS) as promulgated by the U.S. Government Accountability Office (GAO).

AUDIT RESULTS

Our audit determined that the CFTC is in the emerging stages of establishing an ERM program, and the program has not yet achieved maturity. The majority of the agency's ERM policies and procedures remain in draft form and are not officially finalized. We observed deficiencies, including inadequate ERM governance and communication structures, an absence of fully documented policies and procedures, and insufficient resources and processes dedicated to ERM implementation. Furthermore, the internal control framework supporting the ERM program was not appropriately designed or consistently applied, particularly concerning performance reporting. Finally, utilizing the COSO model to evaluate the maturity of the ERM program, we concluded that the CFTC's ERM efforts are still in the early developmental phase and require substantial advancement to reach a maturity level that demonstrates compliance with sound agency-wide risk management program. Currently, the ERM maturity level at CFTC is at an ***initial*** level, which refers to a stage in the risk maturity model where the organization is aware of the need for a formal risk management approach but the current processes are incomplete and risk is managed in silos.

[1] White House, Office of Management and Budget. *OMB Memorandum M-16-17: OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control*, June 2, 2016.

Objective 1: Assess the Effectiveness of the ERM Program

Overall, we found the CFTC's ERM program to be **Not Effective**. Specifically, we found CFTC's ERM program lacks proper governance and communication, documented policies and procedures, and lacks resources and processes for ERM implementation as described in further detail below.

Finding 1: Lack of Proper ERM Governance and Communication

The CFTC is currently facing significant challenges in the governance and communication of its ERM program. The ERM team is small, consisting of one member, Risk Analyst. The Chief Risk Officer (CRO) position is currently open and because of this, the Risk Analyst reports to the Executive Director of the Division of Administration, who in turn reports to the whole Commission (four Commissioners and the Chairperson). The insufficient staffing within the ERM team leads to increased workload and reduced opportunity for communication. Additionally, there is misalignment of goals and priorities, and also lack of collaboration and knowledge sharing.

There is a notable lack of communication between the ERM team and various departments. Currently, departments do not report their risks to the ERM team and instead report them directly to executive leadership using various methods on a monthly basis. Further, departments have not been adequately informed about the ERM program and the need for their participation and input. Out of the 10 department leader interviews we conducted, eight had not received any communication from the ERM team in the past year.

The ERM program currently has minimal oversight and operates under the Division of Administration without supervision from a Risk Management Committee (RMC), which is a common practice within agencies with an effective ERM program, or other executive leadership. Effective governance requires active involvement from executive leadership which is currently lacking for the ERM program. In addition, there are no established reporting mechanisms or channels in place to facilitate executive oversight.

Senior leadership has not provided sufficient support or clear directives for the ERM program. This lack of support results in a weak organizational tone at the top. The ERM team has not received sufficient resources, such as budget and staffing, for program development and implementation. In addition, ERM policy and procedures were updated in 2020; however, they have not yet been approved by CFTC leadership.

Furthermore, there are no formal and consistent requests for risk assessments by the ERM team to the individual divisions, hindering the identification and management of risks. We also noted that the ERM process is not effectively integrated within the divisions, leading to a fragmented approach to risk management.

The lack of proper governance and communication results from Senior leadership not prioritizing the development of an ERM program and therefore not allocating sufficient time, resources, or funding to the ERM program. Despite the issuance of OMB Circular A-123 in 2016, requiring the establishment of an ERM program at federal agencies, CFTC's ERM program is still in its initial stages of creation and significant progress on the 2020 roadmap has not been made. In addition, the agency has not been able to hire a dedicated person for the ERM program to own and direct the program for successful execution.

Lack of proper governance and communications may result in:

1. **Increased Risk Exposure**: Without proper communication and integration, CFTC may fail to identify and manage risks effectively, leading to increased vulnerability to unforeseen events.
2. **Inefficiency and Redundancy**: Lack of coordination between the ERM team and various departments can result in duplicated efforts and inefficiencies, wasting valuable resources.
3. **Poor Decision-Making**: Without comprehensive risk assessments and executive oversight, leadership may make decisions based on incomplete or inaccurate information, potentially leading to adverse outcomes.
4. **Low Employee Engagement**: The absence of clear directives and support from senior leadership can result in low engagement and buy-in from employees, undermining the overall effectiveness of the ERM program.
5. **Reputation Damage**: Failure to manage risks appropriately can lead to incidents that damage the CFTC's reputation, eroding stakeholder trust and confidence.
6. **Regulatory Non-Compliance**: Inadequate risk management practices may result in non-compliance with regulatory requirements.
7. **Reliance Deficiency**: Divisions are not placing sufficient reliance on the ERM program. Leadership has not prioritized the ERM program and as such the program has not received the level of support needed to be effective and valuable to the organization.

Addressing these issues is crucial for the successful implementation and sustainability of the ERM program, ensuring that the CFTC can effectively manage risks and achieve its strategic objectives.

The Committee of Sponsoring Organizations (COSO)[2] releases guidance detailing the application of ERM. Specifically, in its recent guidance outlined in The Compliance Risk Management: Applying the COSO ERM Framework, the Treadway Commission states:

> "The COSO ERM framework, like the internal control framework, comprises five interrelated components: 1) Governance & culture 2) Strategy & objective-setting 3) Performance 4) Review and revision 5) Information, communication, and reporting."

Furthermore, the principles in the above-mentioned COSO guidance require management to do the following:

> "Have regular meetings/communications between compliance and business units (Principle 14), update compliance risk assessments on a periodic basis (Principle 16), review efficacy of the compliance risk assessment process on a periodic basis (Principle 17) and exercise Board Risk Oversight (Principle 1)."

[2] COSO ERM Framework

Office of Management and Budget (OMB) Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control states:

> "ERM and Internal Control are components of a governance framework. ERM as a discipline, deals with identifying, assessing, and managing risks. Through adequate risk management, agencies can concentrate efforts towards key points of failure and reduce or eliminate the potential for disruptive events. Internal control is a process effected by an entity's oversight body, management, and other personnel that provides reasonable assurance that the objectives of an entity will be achieved.
>
> ERM is viewed as a part of the overall governance process, and internal controls as an integral part of risk management and ERM.
>
> Establish Risk Management Council, develop "Risk Profiles" which identify risks arising from mission and mission-support operations, and consider those risks as part of the annual strategic review process.
>
> ERM provides an enterprise-wide, strategically-aligned portfolio view of organizational challenges that provides better insight about how to most effectively prioritize resource allocations to ensure successful mission delivery.
>
> ERM seeks to open channels of communication so that managers have access to the information they need to make sound decisions."

Recommendation: We recommend CFTC:

Recommendation 1: Establish a Risk Management Committee and include key personnel and stakeholders from different CFTC Divisions.

Recommendation 2: Create the Governance Charter and hold regular meetings with the Risk Management Committee.

Recommendation 3: Update and finalize an ERM roadmap from 2020 which includes estimated and actual completion dates.

Recommendation 4: Develop Annual Risk Analysis Reports and distribute to the various divisions.

Recommendation 5: Implement an Enterprise Governance, Risk and Compliance (eGRC) Tool which will help aggregate risks across the enterprise and map them to strategic objectives.

Recommendation 6: Enhance ERM communication channels and hold regular meetings between the ERM team and departments.

Recommendation 7: Increase CFTC leadership support and conduct regular briefings and workshops and actively participate in ERM activities.

Recommendation 8: Foster a collaborative environment by appointing ERM liaisons within each division.

Recommendation 9: Conduct training sessions to educate employees about the ERM program and its benefits.

Finding 2: Lack of Documented Policies and Procedures

The CFTC currently lacks comprehensive policies and procedures for its ERM program. Our audit procedures found that CFTC does not have a finalized ERM policy or established standard operating procedures for conducting ERM assessments. We also noted that an official risk rating methodology has not been developed, and the CFTC has not defined its risk appetite or risk tolerance levels. Currently, risks are not officially documented and they are mitigated in a siloed manner by individual departments.

Furthermore, the CFTC does not have a defined timeline or criteria for conducting annual risk assessments. While most of these documents have been drafted, at the time of our fieldwork, they had not been finalized or approved.

Senior leadership has not prioritized the development of an ERM program and therefore has not allocated sufficient time, resources, or funding to the ERM program to ensure its successful implementation. Although leadership developed an ERM roadmap in 2020, it has not been implemented or approved yet.

Lack of documented policies and procedures related to CFTC's ERM program could have several potential effects:

- **Increased Risk Exposure:** Without a formal ERM policy and risk rating methodology, the CFTC may not effectively identify, assess, and mitigate risks, leading to increased vulnerability to unforeseen events.
- **Lack of Coordination:** The absence of a Risk Committee and official procedures can result in fragmented risk management efforts, with individual divisions addressing risks in isolation rather than through a coordinated approach.
- **Inconsistent Risk Management:** Without documented risks and a defined risk appetite, there may be inconsistencies in how risks are managed across the organization, potentially leading to gaps in risk coverage.
- **Inefficient Resource Allocation:** The lack of a structured ERM framework can lead to inefficient use of resources, as efforts to manage risks may be duplicated or misaligned with the organization's strategic objectives.
- **Regulatory and Compliance Issues:** Inadequate risk management practices could result in non-compliance with regulatory requirements, potentially leading to legal and financial repercussions.
- **Delayed Response to Risks:** Without a defined timeline or criteria for conducting risk assessments, the organization may be slow to respond to emerging risks, impacting its ability to mitigate potential threats effectively.

The Compliance Risk Management: Appling the Committee of Sponsoring Organizations (COSO) ERM Framework_issued by the Committee of Sponsoring Organizations of the Treadway Commission states:

> "The COSO ERM framework, like the internal control framework, comprises five interrelated components: 1) Governance & culture 2) Strategy & objective-setting 3) Performance 4) Review and revision 5) Information, communication, and reporting"

The *Strategy & Objective-Setting for Compliance Risks* section states:

> "Management to consider its risk appetite as part of the organization's risk profile."

Further, the COSO states:

> "There should be regularly scheduled and periodic meetings, including sessions in which the board meets privately with the Chief Compliance Officer (CCO) without other members of senior management present.
>
> Additionally, agencies should document their policies and procedures specific to the operation, create a compliance risk assessment that gets updated periodically, and establish protocols/procedures for the escalation of significant compliance risk events."

Office of Management and Budget (OMB) Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* states that:

> "Senior management develops and implements core policies and procedures with respect to enterprise risk management, including developing a process to define risk appetite and establish risk thresholds accordingly.
>
> Ensuring the current risk levels and processes are consistent with the established risk tolerance thresholds and policies."

Recommendation: We recommend CFTC:

> **Recommendation 10:** Develop a formal ERM policy that outlines the framework, objectives, and scope of the program. This policy should be approved by senior management and communicated across the organization.
>
> **Recommendation 11:** Create standardized procedures to conduct ERM assessments including guidelines for risk identification, assessment, mitigation, and monitoring.
>
> **Recommendation 12:** Define its ERM risk rating methodology to consistently evaluate and prioritize risks and align this methodology with the organization's risk appetite and tolerance levels.
>
> **Recommendation 13:** Maintain a centralized risk register to document all identified risks as well as the risk owners, mitigation strategies, and monitoring plans.
>
> **Recommendation 14:** Establish a timeline and criteria for conducting regular risk assessments and continuously monitoring and managing risk with at least an annual risk assessment.

Recommendation 15: Regularly review and update the ERM program to incorporate best practices and lessons learned to strive for continuous improvement.

Finding 3: Lack of Resources and Process for ERM Implementation

The CFTC's ability to implement and effective ERM program is also hindered due to limitations in technology, resources, and processes. The ERM team is currently composed of two positions, Risk Analyst and Chief Risk Officer (CRO); however, the CRO position is currently vacant. CRO is responsible for reporting to the Executive Director under which the ERM office operates (Division of Administration). In addition, both the Risk Analyst and Executive Director have been in their positions for just over a year.

Additionally, we noted that the ERM program is not integrated into CFTC's strategic planning. And there is no process for divisions to report their risks to the ACRO for inclusion in the agency's risk register. Currently, CFTC does not have a risk register to capture all the risks identified.

Furthermore, the immaturity of the ERM program at CFTC leads to reluctance among departments to collaborate on risk mitigation efforts due to inadequate and inconsistent communication and a lack of a clear path forward.

Senior leadership has not prioritized the development of an ERM program and has therefore not allocated sufficient time, resources, or budget to the ERM program to ensure its success. As part of our audit procedures, we interviewed thirteen individuals within the CFTC divisions and all thirteen individuals interviewed expressed that budget constraints hinder the hiring of skilled personnel. Significant budget constraints and staffing attrition have resulted in smaller teams within the CFTC overall which has adversely impacted the ERM team's ability to hire knowledgeable and experienced personnel.

Lack of resources can have several significant effects on the CFTC's ERM program and the organization as a whole:

- **Limited Risk Management Capabilities:** A small ERM team and new executives constrain the ability to effectively identify, assess, and mitigate risks.
- **Strategic Misalignment:** Lack of integration of the ERM program into strategic planning can lead to misaligned priorities and missed opportunities for proactive risk management.
- **Operational Inefficiencies:** Budget constraints and staffing attrition can result in operational inefficiencies due to insufficient skilled personnel to manage and execute ERM activities.
- **Increased Vulnerability:** An immature ERM program can leave the organization more vulnerable to risks, as departments may be hesitant to collaborate on risk mitigation efforts, impacting organizational growth objectives.
- **Reduced Organizational Resilience:** Without a robust ERM framework, the organization may struggle to respond effectively to emerging risks, potentially impacting its overall resilience and stability.

The Compliance Risk Management: Appling the Committee of Sponsoring Organizations (COSO) ERM Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission states:

> "The COSO ERM framework, like the internal control framework, comprises five interrelated components: 1) Governance & culture 2) Strategy & objective-setting 3) Performance 4) Review and revision 5) Information, communication, and reporting."

Additionally, Principle 18 of the Framework provides the following characteristics of leveraging information and technology:

> "Ensure that compliance has access to all information relevant to effectively manage compliance risk.
>
> Provide compliance with relevant information technology/data analytics skills or access to such skills.
>
> Utilize data analytics in monitoring/auditing (monitor compliance and performance of internal controls).
>
> Create automated dashboards/reports for monitoring compliance.
>
> Leverage technology to provide for the delivery of effective compliance and ethics training.
>
> Utilize technology to facilitate risk assessment process (scoring, reporting, etc.). "

In addition, Principle 1 states:

> "The board should also ensure there is an effective compliance oversight infrastructure in place to support the Compliance and Ethics (C&E) program, to include adequate staffing and resources, as well as appropriate authority and empowerment to achieve the objectives of the program" and that organizations "ensure that sufficient resources are provided to support the program".

Office of Management and Budget (OMB) Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* states:

> "ERM provides an enterprise-wide, strategically aligned portfolio view of organizational challenges that provides better insight about how to most effectively prioritize resource allocations to ensure successful mission delivery.
>
> Effective Risk Management: a) is an integral part of all organizational processes b) takes human and cultural factors into account.
>
> The development of risk responses should be used to inform decision-making through existing management processes including the strategic reviews, development of the legislative and policy agenda, operational planning, and budget formulation.

ERM reflects forward-looking management decisions and balancing risks and returns so an Agency enhances its value to the taxpayer and increases its ability to achieve its strategic objectives.

Risk must be analyzed in relation to achievement of the strategic objectives established in the Agency strategic plan (See OMB Circular No. A-11, Section 230), as well as risk in relation to appropriate operational objectives. Specific objectives must be identified and documented to facilitate identification of risks to strategic, operations, reporting, and compliance.

The management of risk must be regularly reviewed to monitor whether or not the risk profile has changed and to gain assurance that risk management is effective or if further action is necessary. In addition, processes must be put in place to review whether risks still exist, whether new risks have arisen, whether the likelihood and impact of risks have changed, to report significant changes that adjust risk priorities, and deliver assurance on the effectiveness of control. In addition, the overall risk management process must be subjected to regular review to deliver assurance that it remains appropriate and effective.

At a minimum, management's risk management review processes must: 1) ensure that all aspects of the risk management process are reviewed at least once a year 2) ensure that risks themselves are subjected to review with appropriate frequency; and 3) make provisions for alerting the appropriate level of management to new or emerging risks, as well as changes in already identified risks, so that the change can be appropriately addressed."

Recommendation: We recommend the CFTC:

Recommendation 16: Enhance its ERM team capacity and prioritize hiring skilled ERM professionals and provide ongoing training to existing staff. Further, the CFTC should integrate the ERM roles and responsibilities into existing job descriptions through cross-training and encourage participation in training, conferences, and other professional development opportunities. The CFTC should also leverage external expertise to provide support and guidance during the development phase of the ERM program.

Recommendation 17: Ensure ERM considerations are integrated into the strategic planning process with active involvement from senior executives.

Recommendation 18: In addition to recommending CFTC to implement an Enterprise Governance, Risk, and Compliance (GRC) tool (See recommendation 5) we suggest CFTC to also Improve its processes by investing in technology that supports ERM activities, such as risk assessment tools and data analytics platforms.

Recommendation 19: Address budget constraints by reevaluating the resources dedicated to the ERM program and exploring cost-effective solutions and tools to enhance the ERM program without significant financial investment.

Recommendation 20: Strengthen its organizational resilience by conducting regular risk awareness and training sessions for all employees to build a risk-aware culture and establish a feedback loop to continuously assess and improve the ERM program based on lessons learned and emerging best practices.

Objective 2: Determine CFTC's ERM Program Maturity

To determine the maturity of the ERM program at the CFTC we interviewed key individuals within the ERM program, requested and reviewed all applicable ERM-related documents, and documented our assessment of CFTC ERM maturity utilizing an internally developed tool based on the American Institute of Certified Public Accountants (AICPA) and Chartered Institute of Management Accountants (CIMA)'s ERM Maturity Assessment Tool.

We evaluated the Commission's ERM maturity level against ten risk objectives. These risk objectives were:

- Risk Culture
- Risk Identification
- Risk Assessment
- Articulation of Risk Appetite
- Risk Response
- Internal Controls
- Governance
- Risk Reporting
- Integration with Strategic Planning
- Assessment of ERM Effectiveness

For each of these ten risk objectives, we assigned a score of 1 – Not Effective, 2 – Somewhat Effective, 3 – Effective, 4 – Highly Effective, and 5 – Exceptional.

We asked the CFTC ERM team to provide us a self-assessment based on where they believe the ERM program is currently. We also conducted our own assessment based on the results of our audit.

We calculated the delta between the CFTC's self-assessment and our assessment. This variance helps us to analyze the differences and suggest areas for further improvement and documentation which are needed for the purposes of maturing the ERM program. Then, we calculated the average score of each risk category by taking the average of the score assigned by our team and calculated the percentage score for each risk category.

The table below provides an overall assessment of each risk category:

Risk Category	Highest Possible Score	CFTC Self-Assessment Score	Auditor Assessment Score	Delta	Average Initial Score	Percentage Score for Category	Desired End Score
Risk Culture	55	24	21	3	22.5	41%	33
Risk Identification	45	22	20	2	21	47%	27
Risk Assessment	65	28	22	6	25	38%	39
Articulation of Risk Appetite	25	5	5	0	5	20%	15
Risk Response	60	24	15	9	19.5	33%	36
Internal Controls	45	21	14	7	17.5	39%	27
Governance	40	15	10	5	12.5	31%	24
Risk Reporting	20	4	4	0	4	20%	12
Integration with Strategic Planning	45	20	14	6	17	38%	27
Assessment of ERM Effectiveness	35	14	11	3	12.5	36%	21
Total Score	**435**	**177**	**136**	**41**	**156.5**		**261**
Percentage	**100%**	**41%**	**31%**		**36%**		**60%**

Table 1 – Overall Maturity Assessment of the CFTC ERM Program

The desired end score for each risk category (Risk Culture, Risk Identification, etc.) has been calculated by allocating a rating scale of 3 – Effective, for each of the risk category key elements. For instance, the risk category of "Governance" has eight key elements, as shown in Appendix 2 – ERM Maturity Assessment, and by allocating a desired rating score of three (Effective) to each of these eight key elements, we achieve the total desired end score of twenty-four, as shown in table 1 above.

Additionally, the desired end percentage of 60%, has been calculated by dividing the total desired end score of 261 by the highest possible score of 435. The figure below illustrates various ERM maturity levels and the corresponding desired end score.

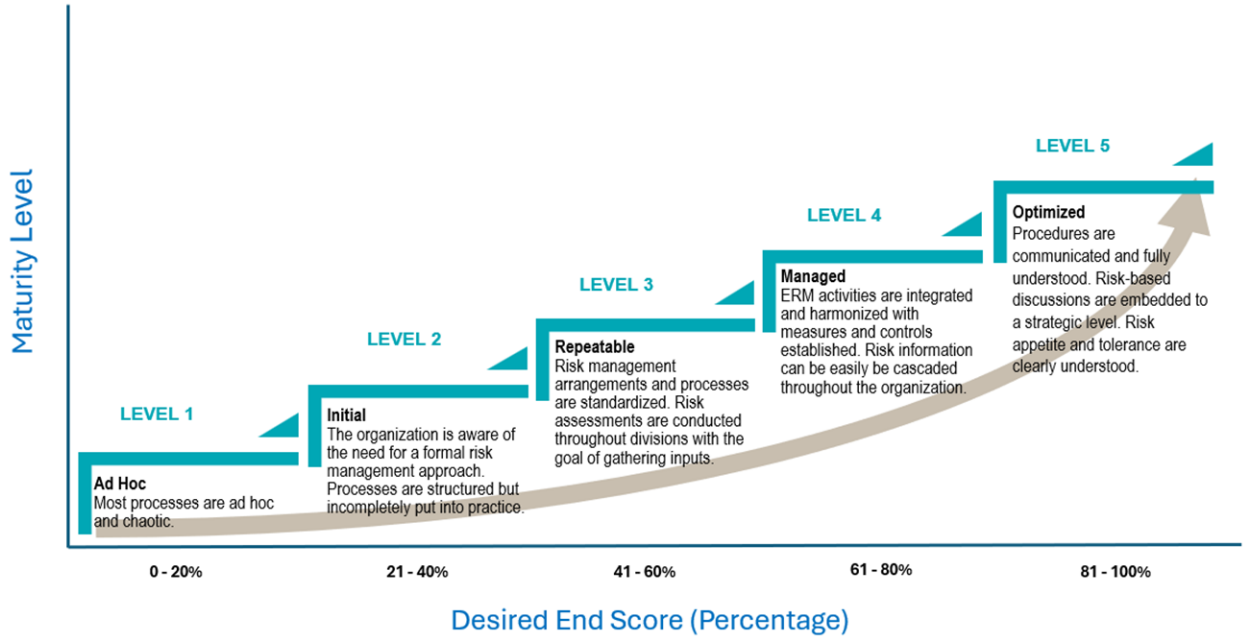

Figure 1 – ERM Maturity Level

The graph below represents an overall maturity assessment of the CFTC risk categories identified above compared to the desired goals.

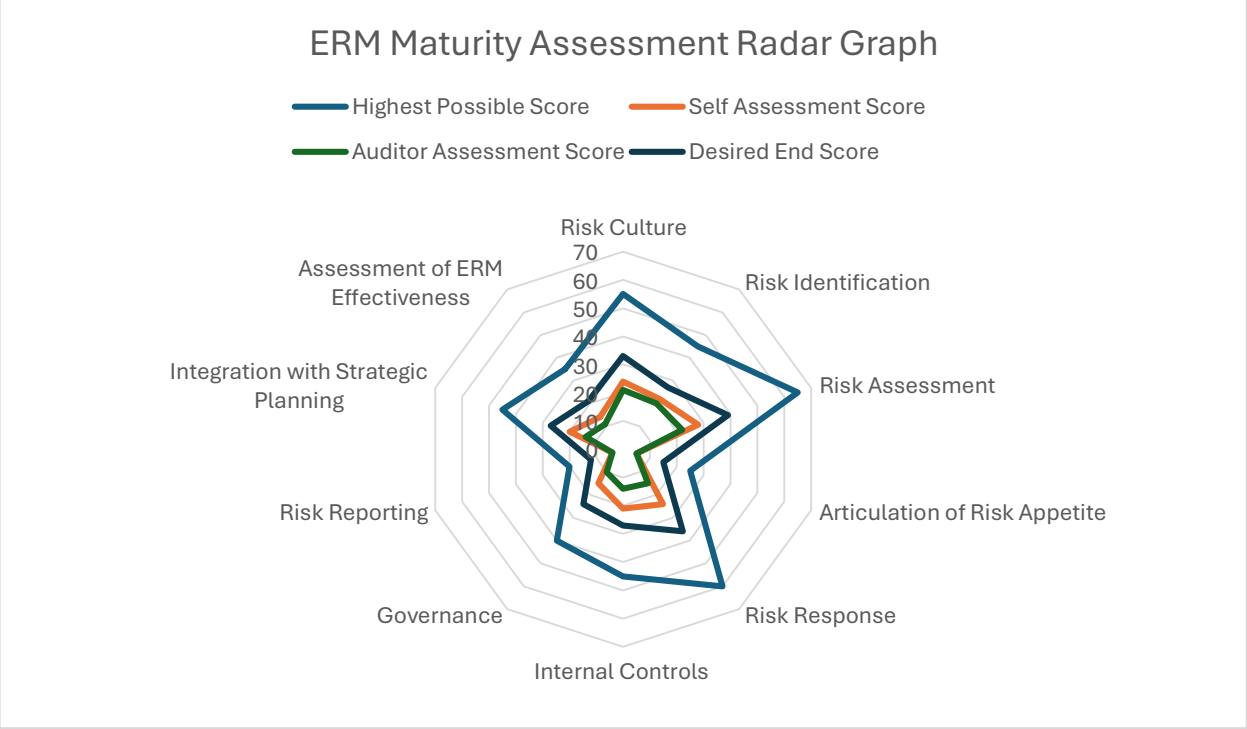

Figure 2 – CFTC ERM Maturity Assessment Radar Graph

Based on the assessment of the maturity performed above, we determined the ERM program is at the **initial** level being in its early stages of development and CFTC desires to achieve a repeatable level for its ERM Program. Appendix 2 – ERM *Maturity Assessment* provides further details on each of risk category objectives as well as the individual score obtained for considering the maturity level.

APPENDIX 1: OBJECTIVES, SCOPE AND METHODOLOGY

Audit Objectives

Our audit examined the ERM program at the CFTC for the specific objectives of 1) assessing the effectiveness of the CFTC's ERM process with specific attention to Governance and Internal Control Integration and 2) determining CFTC's ERM program maturity using the COSO model. The Chartered Institute of Management Accountants (CIMA)'s ERM Maturity Assessment Tool links with the Committee of Sponsoring Organizations of the Treadway Commission (COSO) ERM framework as it has, Key Principles from COSO model, Maturity Levels Linked to COSO's Principles, Emphasizes on Continuous Improvement and assesses areas that reflect COSO's approach to risk governance.

The performance audit was conducted in accordance with Government Auditing Standards, 2018 revision, also known as generally accepted government auditing standards (GAGAS), issued by the Comptroller General of the United States (GAO-21-368G), general and performance audit chapters 1, 2, 3, 4, 5, 8 and 9.

Audit Scope

The scope of the performance audit covered the current stage of CFTC ERM during Fiscal Year 2024.

Audit Methodology

To execute this audit, we designed a risk-based methodology to ensure that audit resources were deployed to the areas determined to have the highest risk while minimizing redundant efforts and CFTC resources. Our performance audit consisted of three phases: Planning, Fieldwork, and Reporting.

During the Planning Phase, we developed our overall strategy for the expected scope and timing of audit procedures. The planning phase objectives were to develop an understanding of the entity and the objectives of the audit, to identify questions, and to develop testing steps to address the audit objectives. The purpose of this phase was to ensure we obtained and reviewed pertinent background information and conducted meetings and interviews with key CFTC ERM personnel so that we could confirm and update our understanding of the environment and the objectives relevant to the engagement.

In the Fieldwork Phase, we obtained sufficient evidence related to the objectives identified in the planning phase. Our fieldwork phase consisted of obtaining an understanding of the internal control environment and governance structure surrounding CFTC's ERM Program. Our fieldwork activities provide sufficient evidence to assess the effectiveness and maturity of CFTC's ERM program.

To determine whether the CFTC ERM program is effective we interviewed key individuals within the ERM program including the Acting Chief Risk Office and the Executive Director to gain an initial understanding of the program. We also selected and interviewed additional key personnel outside of the ERM program office within the Commission to gain a better understanding of the

ERM implementation and awareness across the agency. Our assessment of effectiveness was based on the following rating scale.

Rating Scale	Rating Scale Description
1. Not Effective	The CFTC ERM Program lacks understanding of risk management, there is no documented ERM strategy and is reactive and ad hoc. The program does not meet the objectives of this key element.
2. Somewhat Effective	The CFTC ERM Program applies Risk Management but does not do it strategically and is siloed and inconsistent. The program partially achieves the objectives of this key element.
3. Effective	The CFTC ERM Program has documented framework and processes but lacks visibility across the organization. Most processes are consistent. The program achieves the objectives of this key element.
4. Highly Effective	The CFTC ERM Program has the program integrated across the enterprise. The ERM tools are implemented and the ERM process is monitored and improved. The program repeatedly achieves the objectives of the key element consistently.
5. Exceptional	The CFTC ERM Program is in a highly matured stage. The strategic ERM Program is integrated across the enterprise, the ERM processes are tied to value creation and optimized risk scenarios. The program consistently achieves the objectives of the key element and looks for ways to improve.

Table 2 – ERM Rating Scale

To determine ERM program maturity, we conducted interviews with CFTC personnel, performed an analysis and evaluation of the CFTC's policies and procedures related to the ERM program and assessed the maturity of the CFTC ERM program using an internally developed tool and assigned a score using the following maturity rating scale.

Maturity Levels	Maturity Level Description
Ad Hoc (1)	The organization may be compliant with legal and regulatory requirements, but without consistent, formalized or documented risk management arrangements or processes. Implies an extremely primitive level of ERM maturity where risk management typically depends on the actions of specific individuals, with improvised procedures and poorly understood processes.
Initial (2)	The organization is aware of the need for a more formal risk management approach. Risk management arrangements and processes are structured, but incompletely put into practice. Formalization is on-going but not fully accepted in the organization. Risk is managed independently, with little integration or risk gathering from all parts of the organization. Processes typically lack discipline and rigor. Risk definitions often vary across the organization. Risk is managed in silos, with little integration or risk aggregation. Processes typically lack discipline and rigor. Risk definitions often vary across the silos.

Maturity Levels	Maturity Level Description
Repeatable (3)	Risk management arrangements and processes are standardized with defined and documented procedures. Risk management awareness may be included in organizational training. A standardized procedure is generally in place with the senior levels of the organization being provided with risk overviews/reports. Risk management is aligned with the organization's external and internal environment, as well as the organization's risk profile. The risk management arrangements and processes are established and repeatable as a standard organizational approach. Risk assessments are conducted throughout Divisions with the goal of gathering input from the frontline. Information is aggregated to the Executive Directors/Division Heads, senior management, committees and regulators for risk overviews. Approaches to risk management are established and repeatable.
Managed (4)	Enterprise-wide risk management activities, such as monitoring, measurement and reporting are integrated and harmonized with measures and controls established. Risk arrangements, assessments, and treatments are organized, monitored, and managed at many levels of the organization. Risk information is structured in a manner that it can easily be cascaded throughout the organization for information collection and aggregated for senior level reporting. Measurement metrics are standardized and incorporated into the organization's performance metrics. Risk procedures are communicated and fully understood throughout the organization with the risk management principles integrated fully within the management process. Mechanisms are in place for alerting management about changes in the organization's risk profile that may affect the organization's objectives.
Optimized (5)	Risk procedures are communicated and fully understood throughout the organization with the risk management principles integrated fully within the management process. Risk-based discussions are embedded to a strategic level, such as long-term planning, budget allocation and decision-making. Risk appetite (risk/reward) and tolerances are clearly understood with alerts in place to ensure the Executive Directors/Division Heads and senior management is made aware when set thresholds are exceeded. Planned critical review of the risk management program provides guidance for adjusting/improving application of the risk management principles, arrangements and processes across the organization to advance objectives.

Table 3 – ERM Maturity Levels

The purpose of the Reporting Phase was to communicate the results of the audit. Our reporting approach involved an assessment of audit evidence and summarizing the results of testing to support audit conclusions. We followed the applicable audit standards and gathered sufficient evidence to support the audit conclusions. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We conducted this performance audit between September 3, 2024 and January 21, 2025 in accordance with GAGAS. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions

based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

APPENDIX 2: ERM MATURITY ASSESSMENT

The following section provides further details on each of risk category objectives as well as the individual score obtained. For each of the risk objectives, we assigned a score of 1 – Not Effective, 2 – Somewhat Effective, 3 – Effective, 4 – Highly Effective, and 5 – Exceptional.

RISK CULTURE (RC)

Risk culture refers to the collective values, beliefs, attitudes, and practices within an organization that influence how risk is perceived, managed, and addressed. The strong endorsement by the Executive Directors/Division Heads and senior management of the value of investing time and infrastructure into better understanding the organization's most significant risk exposures is an important and necessary condition that must be in place. Without that endorsement, the organization is not likely to be supportive of any efforts to obtain an enterprise-wide perspective of risks most likely to impact organizational objectives. Instead, risk management may be relegated to a low-value initiative that is viewed by management and employees as compliance oriented and bureaucratic.

In our assessment of the CFTC Risk Culture, we took the following key elements into consideration:

Key Element ID	Description of Key Elements
RC-1	Directors/Division Heads have a clear understanding of the objectives of ERM relative to traditional approaches to risk management.
RC-2	The Chairman embraces the need and provides adequate endorsement of an enterprise-wide approach to risk oversight that seeks to obtain a top-down view of major risk exposures.
RC-3	The Directors/Division Heads are supportive of management's efforts to implement an enterprise-wide approach to risk oversight.
RC-4	Directors/Division Heads view the organization's efforts to obtain an enterprise perspective on the collection of risks as an important strategic tool for the organization.
RC-5	The organization has explicitly assigned enterprise-wide risk management authority and responsibility to a senior executive or senior management committee (e.g., identified an internal 'risk champion' or 'risk management leader').
RC-6	The senior executive with explicit responsibilities for enterprise-wide risk management leadership is a direct report of the Chairman (or, a Senior Executive Risk Committee is used to provide that leadership and the Committee Chair reports to the Chairman).
RC-7	Enterprise-wide risk management principles and guidelines have been identified and defined by executive management and formally communicated to all Divisions.
RC-8	Senior management has effective risk management capabilities and competencies.

Key Element ID	Description of Key Elements
RC-9	Senior management has formally presented an overview to the Directors/Division Heads about the organization's processes that represent its approach to ERM.
RC-10	The Directors/Division Heads sets aside agenda time at regular intervals (annually at a minimum) in its meetings to discuss the most significant risks facing the organization.
RC-11	Both the Directors/Division Heads and senior management view ERM as an ongoing process that will continually evolve over time.

Table 4 – Risk Culture Key Elements and Descriptions

The table below illustrates the Risk Culture Maturity assessment performed by the CFTC ERM team as well as Williams Adley.

Risk Culture Maturity Summary					
Key Element	**CFTC ERM Self-Assessment Score**	**Auditor Assessment Score**	**Delta**	**Average Initial Score**	**Desired End Score**
RC-1	2	2	0	2	3
RC-2	2	1	1	1.5	3
RC-3	2	2	0	2	3
RC-4	2	2	0	2	3
RC-5	2	2	0	2	3
RC-6	3	3	0	3	3
RC-7	2	1	1	1.5	3
RC-8	2	2	0	2	3
RC-9	3	2	1	2.5	3
RC-10	2	2	0	2	3
RC-11	2	2	0	2	3
Total Raw Score	**24**	**21**	**3**	**22.5**	**33**
Percentage Score (Raw Score divided by 55)	**44%**	**38%**		**41%**	**60%**

Table 5 – Risk Culture Maturity Summary

The following chart displays the key elements above using a maturity assessment rating of 1-5.

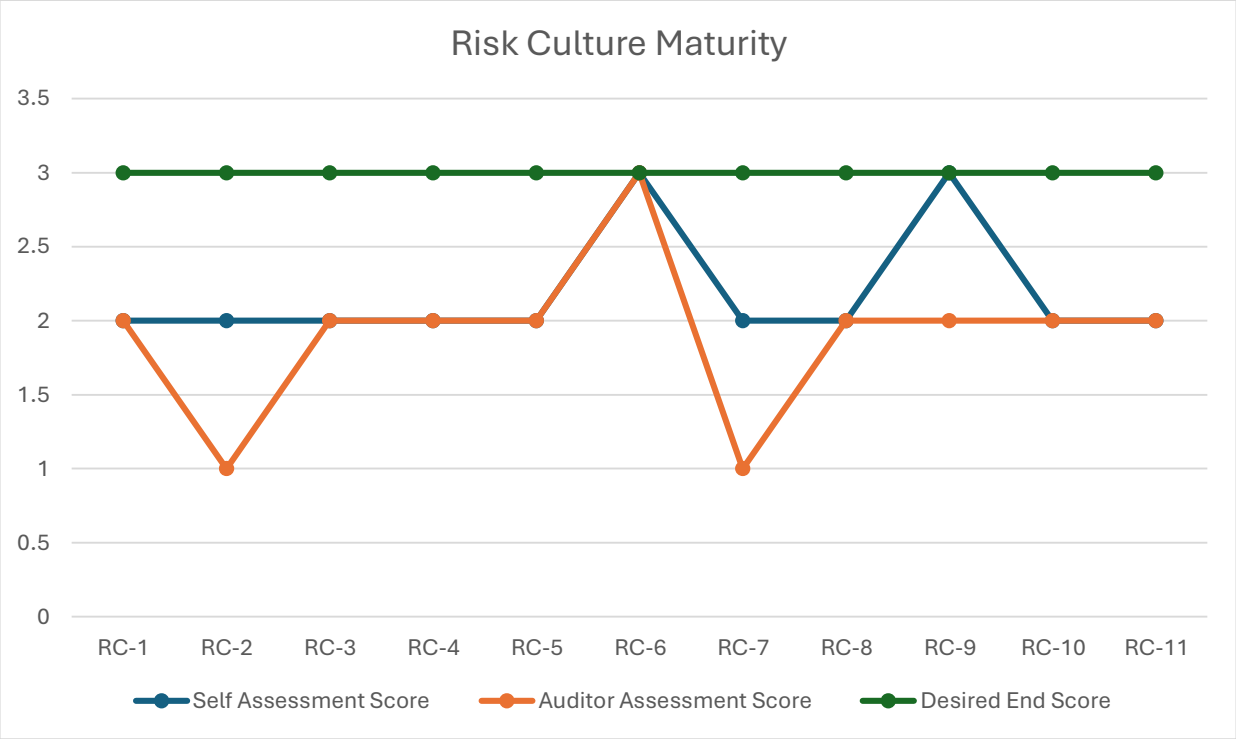

Figure 3 – Risk Culture Maturity Graph

RISK IDENTIFICATION (RI)

Many organizations believe ad hoc and informal approaches to the identification and assessment of risks are sufficient. Therefore, they conclude that there is little benefit in implementing definable, robust, and repeatable processes which encourage the Executive Directors/Division Heads and senior management to regularly think about risks and opportunities that may emerge and affect the organization's achievement of objectives.

In our assessment of the CFTC Risk Identification, we took the following key elements into consideration:

Key Element	Description of Key Elements
RI-1	The organization has defined and widely communicated to Directors/Division Heads what it means by the term “risk.”
RI-2	Risks have been described in terms of events that would affect the achievement of goals, rather than simply a failure to meet goals (i.e., risks can have both positive and negative aspects to the organization).
RI-3	The organization engages in explicit (e.g., identifiable, defined, formal, etc.) efforts to identify the organization’s top risks at least annually.
RI-4	The organization has identified a broad range of risks that may arise both internally and externally, including risks that can be controlled or prevented, as well as those over which the organization has no control (i.e., focus on more than just known risks such as IT risk, legal risk, external risk).

Key Element	Description of Key Elements
RI-5	The organization engages in identifiable processes to regularly scan the environment in an effort to identify unknown, but potentially emerging risks such as new laws & regulations and risks in known risk areas such as IT risk, legal risk, external risk, etc.
RI-6	Senior management has a documented process to accumulate information about risks identified across the organization to create an aggregate inventory of enterprise-wide risks.
RI-7	Senior Management links risks identified by the ERM process to strategic goals in the organization's strategic plan to evaluate the impact of those risks on the strategic success of the organization.
RI-8	Each member of the Directors/Division Heads has provided input into the risk identification process.
RI-9	Employees below the Directors/Division Heads have provided input into the risk identification process.

Table 6 – Risk Identification Key Elements and Descriptions

The graph below illustrates the Risk identification assessment performed by the CFTC ERM Team as well as Williams Adley.

Risk Identification Maturity Summary					
Key Element	**CFTC ERM Self-Assessment Score**	**Auditor Assessment Score**	**Delta**	**Average Initial Score**	**Desired End Score**
RI-1	3	2	1	2.5	3
RI-2	3	3	0	3	3
RI-3	2	2	0	2	3
RI-4	3	3	0	3	3
RI-5	3	3	0	3	3
RI-6	2	1	1	1.5	3
RI-7	2	2	0	2	3
RI-8	2	2	0	2	3
RI-9	2	2	0	2	3
Total Raw Score	**22**	**20**	**2**	**21**	**27**
Percentage Score (Raw Score divided by 45)	**49%**	**44%**		**47%**	**60%**

Table 7 – Risk Identification Maturity Summary

The following chart displays the key elements above using a maturity assessment rating of 1-5.

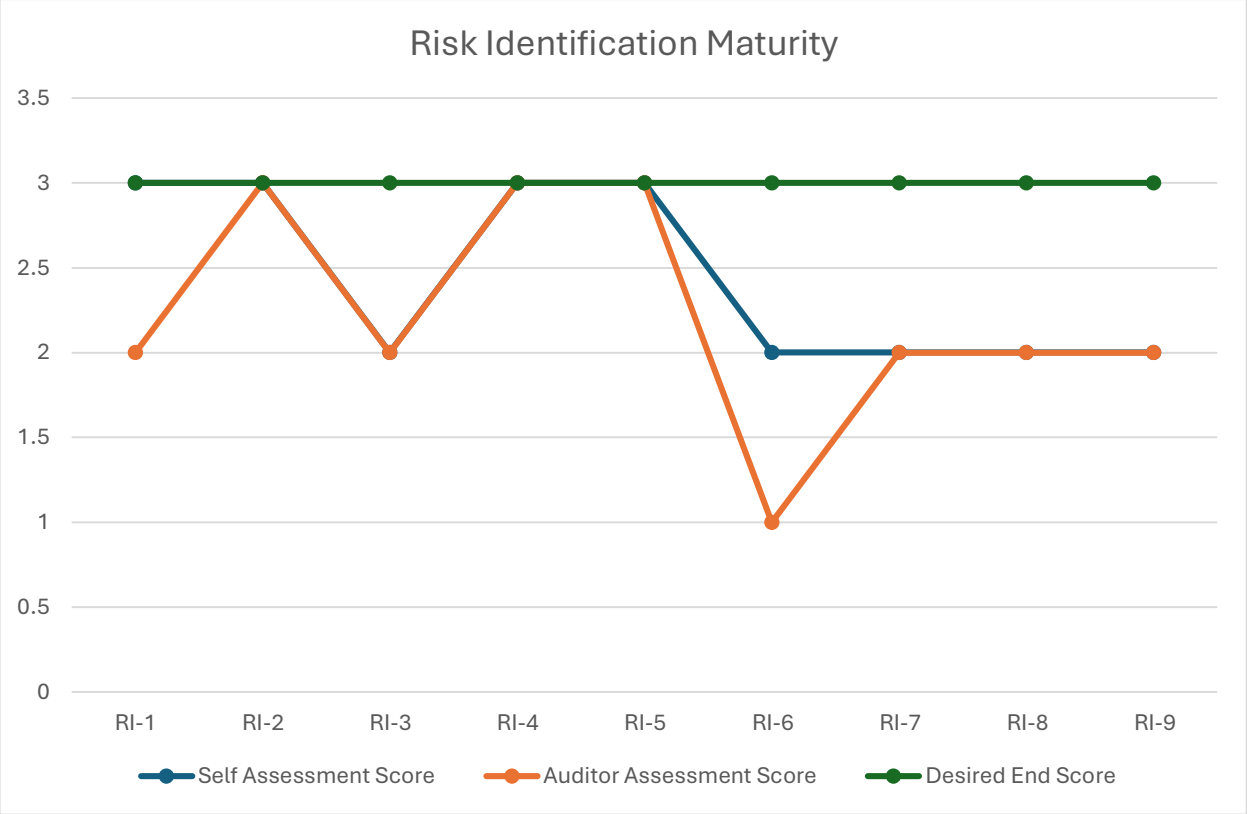

Figure 4 – Risk Identification Maturity Graph

RISK ASSESSMENT (RA)

Many organizations find that when they engage in activities to identify risks, they identify a large number of potential risk events, sometimes numbering into the hundreds or thousands. While all risks identified may have relevance to the organization, some risks are notably more important to the achievement of objectives than others. Therefore, organizations need some method to prioritize risks that encourages a consistent consideration of both the likelihood of the risk occurring and the impact of the event to the organization, if the risk occurs.

In our assessment of the CFTC Risk Assessment Maturity, we took the following key elements into consideration:

Key Element	Description of Key Elements
RA-1	The organization defines the time period over which risks should be assessed (e.g., the next 3 years) to ensure consistency in management's evaluations.
RA-2	The organization strives to assess inherent risk (i.e., the level of the risk before taking into account the organization's activities to manage the risk).
RA-3	The organization assesses not only the likelihood of a risk event occurring but also the impact of the risk to the organization.

Key Element	Description of Key Elements
RA-4	Guidelines or metric scales have been defined and provided to help individuals assess both likelihood and impact so that assessments are consistently applied across the organization.
RA-5	The organization considers an integrated score that incorporates both the likelihood and impact assessments to create some kind of risk rating that helps prioritize the organization's most significant risk exposures.
RA-6	The organization's ERM processes encourage Directors/Division Heads to consider any low probability, but catastrophic events (i.e., "black swan" or "tail" events).
RA-7	The organization considers other dimensions, in addition to likelihood and impact, (such as speed of onset or velocity of a risk or the persistence of a risk event) when assessing risks.
RA-8	Each member of the Directors/Division Heads has provided his or her independent assessments of each risk identified.
RA-9	The Directors/Division Heads (or other similar group with an enterprise view of the organization) has met formally to review the results of the independent assessments and to discuss significant differences in individual risk assessments.
RA-10	Division Heads (or other similar group which would have an enterprise view of the organization) have reached a consensus on the most significant (somewhere between 8–12 critical risks) risks facing the organization.
RA-11	The Directors/Division Heads have concurred with the assessment of the risks completed by senior management.
RA-12	Directors/Division Heads analyzes its portfolio of risks to determine whether any risks are interrelated or whether a single event may have cascading impacts.
RA-13	The ERM process encourages monitoring on a regular basis, any events substantially impacting the assessments of likelihood and impact.

Table 8 – Risk Assessment Key Elements and Descriptions

The graph below illustrates the Risk Assessment Maturity assessment performed by the CFTC ERM Team as well as Williams Adley.

Risk Assessment Maturity Summary					
Key Element	CFTC ERM Self-Assessment Score	Auditor Assessment Score	Delta	Average Initial Score	Desired End Score
RA-1	2	1	1	1.5	3
RA-2	2	2	0	2	3
RA-3	2	2	0	2	3
RA-4	2	1	1	1.5	3
RA-5	2	1	1	1.5	3
RA-6	3	2	1	2.5	3
RA-7	2	2	0	2	3
RA-8	2	2	0	2	3
RA-9	2	2	0	2	3
RA-10	2	2	0	2	3
RA-11	3	2	1	2.5	3
RA-12	2	2	0	2	3

Risk Assessment Maturity Summary					
RA-13	2	1	1	1.5	3
Total Raw Score	**28**	**22**	**6**	**25**	**39**
Percentage Score (Raw Score divided by 65)	**43%**	**34%**		**38%**	**60%**

Table 9 – Risk Assessment Maturity Summary

The following chart displays the key elements above using a maturity assessment rating of 1-5.

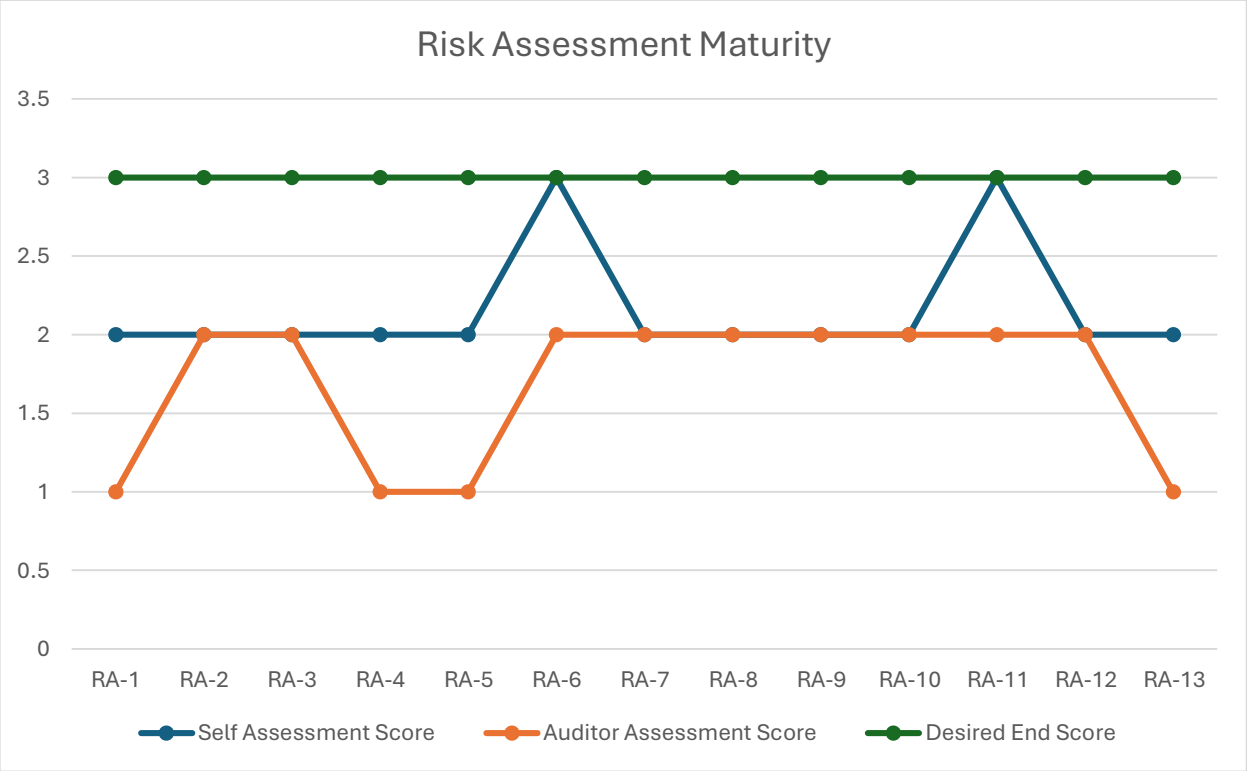

Figure 5 – Risk Assessment Maturity Graph

ARTICULATION OF RISK APPETITE (ARA)

The Articulation of Risk Appetite maturity is when the full benefits of identifying and assessing risks can only be realized if the organization has articulated its risk appetite. Without some description of the organization's willingness to take on risks as it seeks to achieve its objectives, the Executive Directors/Division Heads and senior management are unable to know when risks should be taken or when risks should be managed. While determining the organization's appetite for risk taking can be challenging, it is important that the Executive Directors/Division Heads and senior management make some attempt to articulate its overall appetite for risk taking.

In our assessment of the CFTC Articulation of Risk Appetite Maturity, we took the following key elements into consideration:

Key Element	Description of Key Elements
ARA-1	Senior management has engaged in discussions to articulate the organization's overall appetite for risk taking.
ARA-2	The Chairman has concurred with the organization's risk appetite.
ARA-3	The organization has separately defined its risk appetite for different types of risks (e.g., IT risk, legal risk, external risk).
ARA-4	The organization has expressed in writing its overall appetite for risk taking.
ARA-5	The organization has used at least some quantitative measures in defining its risk appetite.

Table 10 – Articulation of Risk Appetite Key Elements and Descriptions

The graph below illustrates the Articulation of Risk Appetite Maturity assessment performed by the CFTC ERM Team as well as Williams Adley.

Articulation of Risk Appetite Maturity Summary					
Key Element	**CFTC ERM Self-Assessment Score**	**Auditor Assessment Score**	**Delta**	**Average Initial Score**	**Desired End Score**
ARA-1	1	1	0	1	3
ARA-2	1	1	0	1	3
ARA-3	1	1	0	1	3
ARA-4	1	1	0	1	3
ARA-5	1	1	0	1	3
Total Raw Score	**5**	**5**	**0**	**5**	**15**
Percentage Score (Raw Score divided by 25)	**20%**	**20%**		**20%**	**60%**

Table 11 – Articulation of Risk Appetite Maturity Summary

The following chart displays the key elements above using a maturity assessment rating of 1-5.

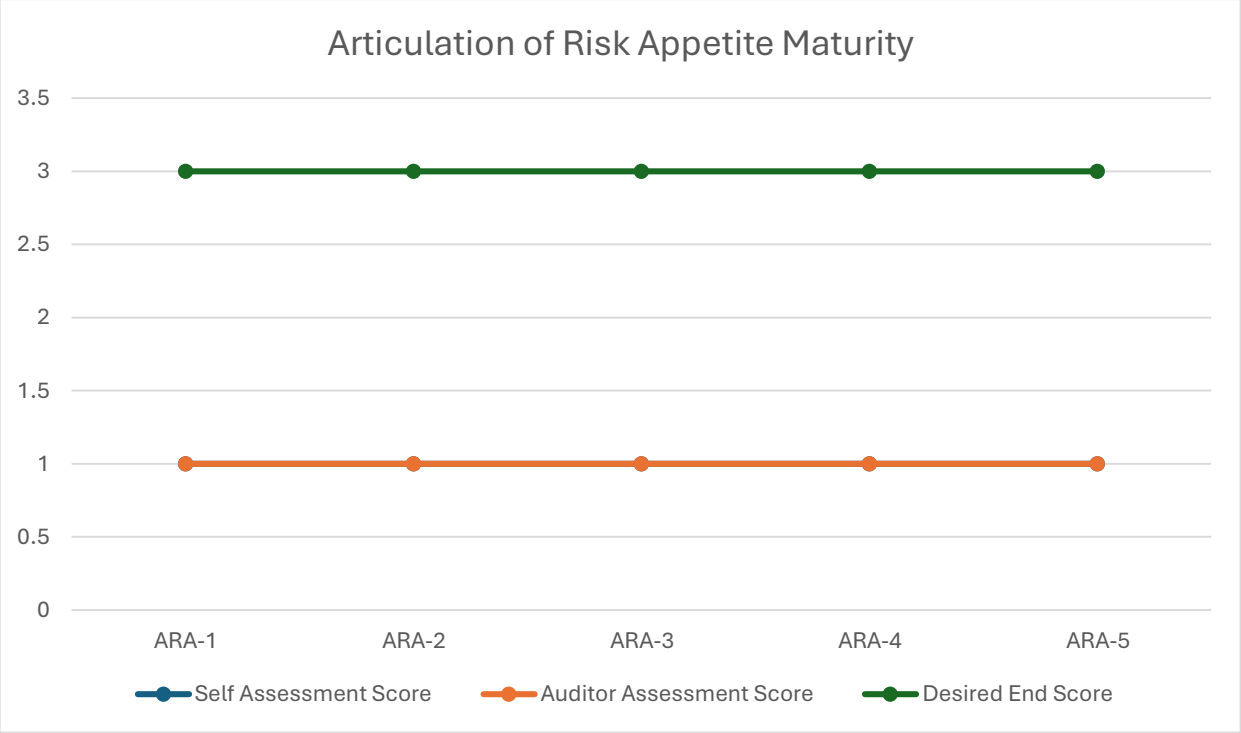

Figure 6 – Articulation of Risk Appetite Maturity Graph

RISK RESPONSE (RR)

The Risk Response Maturity is not utilized until the organization implements its desired response to manage risks that have been identified and assessed, the organization's ERM efforts will be of little value towards the achievement of objectives. Organizations may choose to accept certain risks, avoid others, adopt processes to reduce the exposures to risks, or share risks with external parties. Of utmost importance, however, is to ensure that an appropriate risk response (like those mentioned above) is implemented, and then to ensure that the response is working as intended. Periodic evaluation of whether identified risk responses are effectively being carried out will ensure an effective ongoing ERM process.

In our assessment of the CFTC Risk Response Maturity, we took the following key elements into consideration:

Key Element	Description of Key Elements
RRS-1	Senior management has identified risk owners with responsibility for each of its most significant risks (i.e., its top 8–12 risks).
RRS-2	Senior management has identified a risk owner for other risks identified outside the top 8–12 risks that organization believes are important to monitor.
RRS-3	The organization has documented the existing response(s) to its most significant risks (i.e., its top 8–12 risks).

Key Element	Description of Key Elements
RRS-4	The organization has documented the risk responses for each of the other risks identified outside those deemed as the top 8–12 most significant enterprise-wide risks.
RRS-5	The organization has evaluated whether the existing response is sufficient to manage the risks to be within the organization's risk appetite.
RRS-6	The organization has developed and is implementing plans to address those risks where the current response is insufficient.
RRS-7	The organization has separately evaluated the potential cost of the risk response relative to the benefit provided by the response towards either reducing the impact or reducing the probability of occurrence of the risk event.
RRS-8	The organization documents risk acceptance statements when the cost of mitigating, avoiding and sharing/transferring a risk, is higher than the benefit it provides.
RRS-9	The organization re-evaluates its risk responses at least annually.
RRS-10	The organization's ERM process helps identify potential overlaps or duplications in risk responses across the enterprise.
RRS-11	The organization conducts table top drills or other exercises to test whether responses to its most significant risks (i.e., its top 8–12 risks) are working as intended.
RRS-12	The organization has objectively assessed the effectiveness of risk response plans for its most significant risks (i.e., its top 8–12 risks).
RRS-13	The organization has objectively assessed the effectiveness of risk response plans for other risks that management believes are important to monitor that are outside the top 8–12.

Table 12 – Risk Response Key Elements and Descriptions

The graph below illustrates the Risk Response Maturity assessment performed by the CFTC ERM Team as well as Williams Adley.

Risk Response Maturity Summary					
Key Element	CFTC ERM Self-Assessment Score	Auditor Assessment Score	Delta	Average Initial Score	Desired End Score
RRS-1	2	2	0	2	3
RRS-2	2	2	0	2	3
RRS-3	2	1	1	1.5	3
RRS-4	2	1	1	1.5	3
RRS-5	2	1	1	1.5	3
RRS-6	2	1	1	1.5	3
RRS-7	2	1	1	1.5	3
RRS-8	2	1	1	1.5	3
RRS-9	2	1	1	1.5	3
RRS-10	2	2	0	2	3
RRS-11	2	1	1	1.5	3
RRS-12	2	1	1	1.5	3
Total Raw Score	**24**	**15**	**9**	**19.5**	**36**

Risk Response Maturity Summary					
Key Element	CFTC ERM Self-Assessment Score	Auditor Assessment Score	Delta	Average Initial Score	Desired End Score
Percentage Score (Raw Score divided by 60)	40%	25%		33%	60%

Table 13 – Risk Response Maturity Summary

The following chart displays the key elements above using a maturity assessment rating of 1-5.

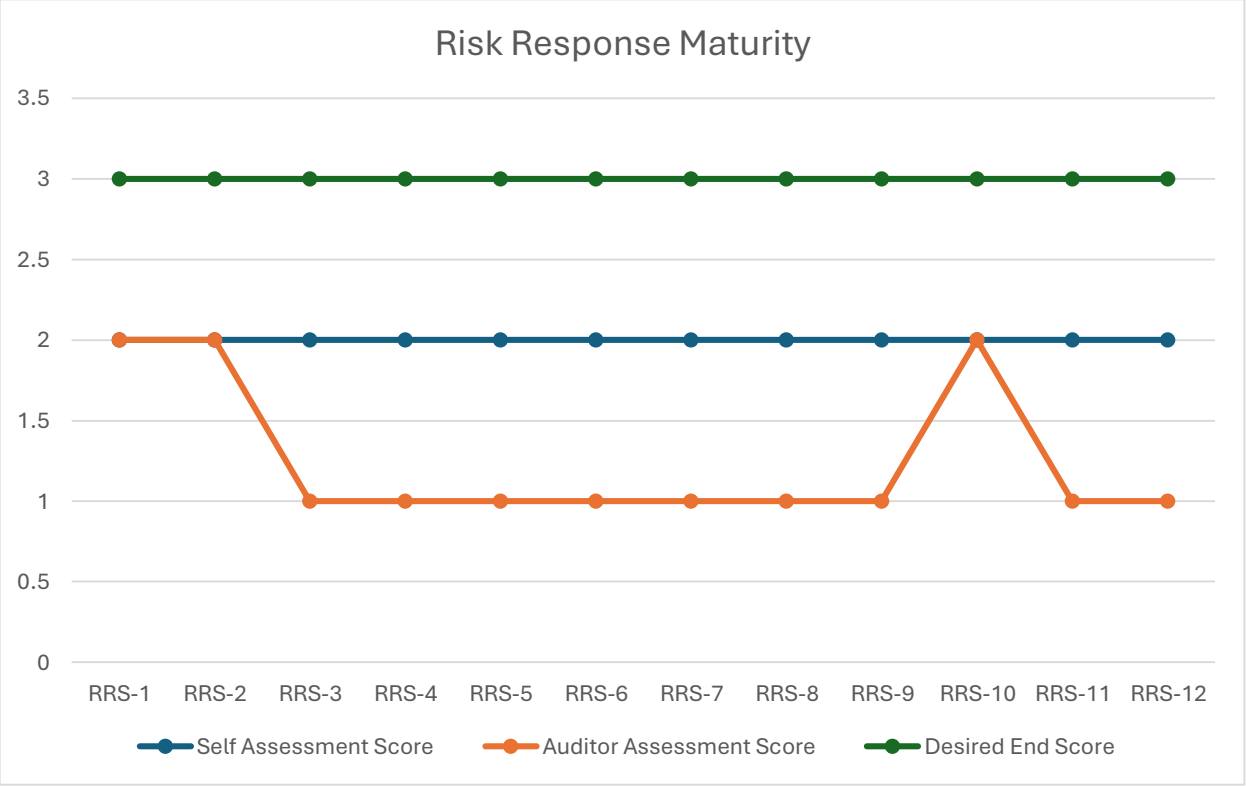

Figure 7 – Risk Response Maturity Graph

INTERNAL CONTROLS (IC)

Internal control is a process effected by an entity's oversight body, management, and other personnel that provides reasonable assurance that the objectives of an entity will be achieved.

In our assessment of the CFTC Internal Controls Maturity, we took the following key elements into consideration:

Key Element	Description of Key Elements
IC-1	The Directors/Division Heads have developed effective standard operating procedures for developing controls related to its most significant risks (i.e., its top 8–12 risks).

Key Element	Description of Key Elements
IC-2	The Directors/Division Heads have control operator/owner identified for controls related to its most significant risks (i.e., its top 8–12 risks).
IC-3	The Directors/Division Heads have control reviewer/approver identified for controls related to its most significant risks (i.e., its top 8–12 risks).
IC-4	The Directors/Division Heads have developed a contingency plan for operation and review of controls in the event of an absence of the standard owner/approver for controls related to its most significant risks (i.e., its top 8–12 risks).
IC-5	The Directors/Division Heads have evaluated whether existing controls are sufficient to mitigate its most significant risks (i.e., its top 8–12 risks).
IC-6	The Directors/Division Heads have objectively assessed the design of controls for its most significant risks (i.e., its top 8–12 risks).
IC-7	The Directors/Division Heads have objectively assessed the operating effectiveness of controls for its most significant risks (i.e., its top 8–12 risks).

Table 14 – Internal Control Key Elements and Descriptions

The graph below illustrates the Internal Controls Maturity assessment performed by the CFTC ERM Team as well as Williams Adley.

Internal Controls Maturity Summary					
Key Element	**CFTC ERM Self-Assessment Score**	**Auditor Assessment Score**	**Delta**	**Average Initial Score**	**Desired End Score**
IC-1	3	2	1	2.5	3
IC-2	3	2	1	2.5	3
IC-3	3	2	1	2.5	3
IC-4	3	2	1	2.5	3
IC-5	3	2	1	2.5	3
IC-6	3	2	1	2.5	3
IC-7	3	2	1	2.5	3
Total Raw Score	**21**	**14**	**7**	**17.5**	**21**
Percentage Score (Raw Score divided by 45)	**47%**	**31%**		**39%**	**47%**

Table 15 – Internal Control Maturity Summary

The following chart displays the key elements above using a maturity assessment rating of 1-5.

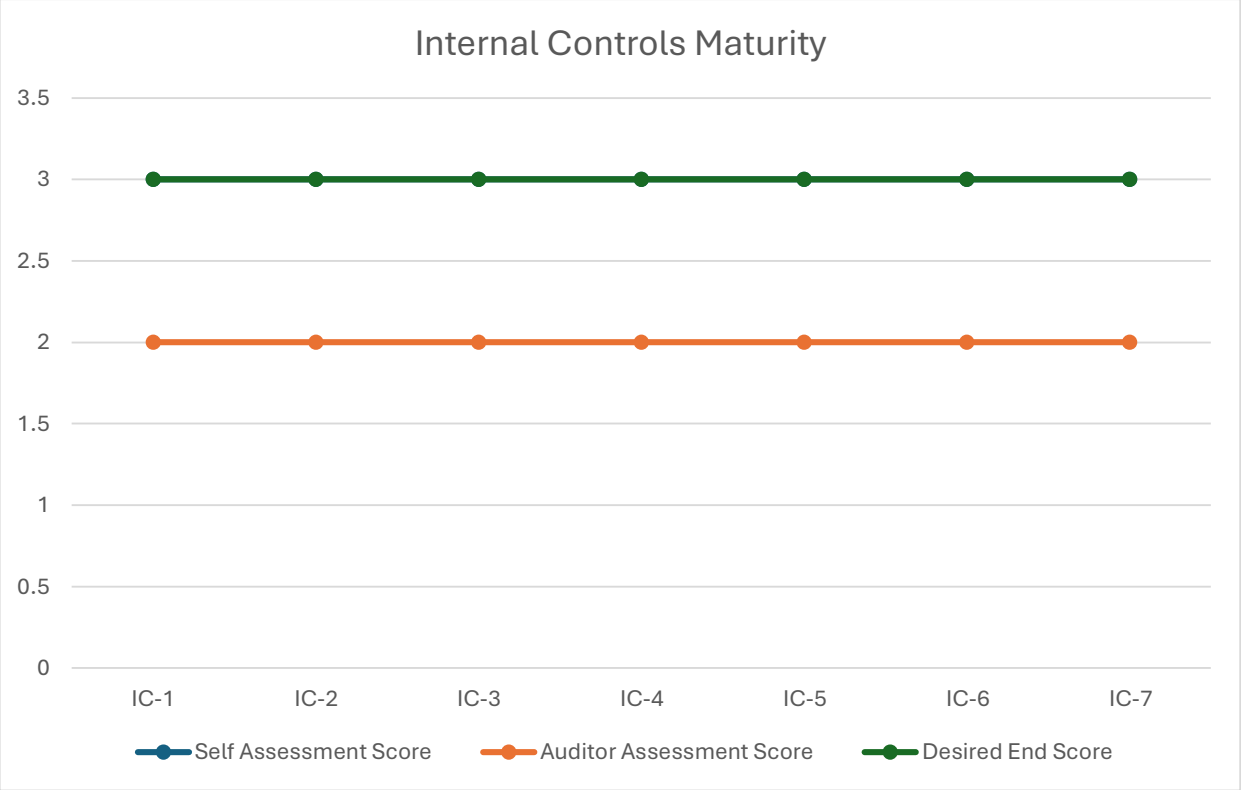

Figure 8– Internal Control Maturity Graph

GOVERNANCE (GV)

Governance is "the act of governing or overseeing the control and direction of an organization" in order to guide necessary decisions to deliver the desired stakeholder value. To achieve that objective, the governance structure aligns organizational efforts in setting direction, allocating limited resources, and managing risks. Enterprise risk governance provides the overall control and direction of risk management activities in a manner that maximizes organizational value. Specifically, the governing body ensures the organization identifies, assesses, treats, monitors, and communicates information about internal and external risks facing the organization that could enable or inhibit achieving key goals and objectives.

In our assessment of the CFTC Governance Maturity, we took the following key elements into consideration:

Key Element	Description of Key Elements
GV-1	The organization has developed a formal Risk Management Board or Risk Advisory Committee that oversees ERM implementation.
GV-2	The organization has developed a formal ERM framework or policies that are aligned with COSO or other best practices.
GV-3	The organization has a charter governing the Risk Management Board or Risk Advisory Committee.

Key Element	Description of Key Elements
GV-4	The organization has well-defined roles for governance and procedures in place to execute oversight.
GV-5	The organization has a structured process for regular reporting of risk information to a Risk Management Board, Risk Advisory Committee, or other governing body.
GV-6	The organization has designed an ERM program monitoring and reporting system that complies with relevant laws, regulations, and guidelines applicable to CFTC.
GV-7	The organization has developed an ongoing training program for ERM program staff and related stakeholders.
GV-8	The organization reviews governance framework for any necessary updates to reflect organizational changes and evolving risk landscapes, at least annually.

Table 16 – Governance Key Elements and Descriptions

The graph below illustrates the Governance assessment performed by the CFTC ERM Team as well as Williams Adley.

Governance Maturity Summary					
Key Element	CFTC ERM Self-Assessment Score	Auditor Assessment Score	Delta	Average Initial Score	Desired End Score
GV-1	1	1	0	1	3
GV-2	2	1	1	1.5	3
GV-3	2	1	1	1.5	3
GV-4	2	2	0	2	3
GV-5	2	1	1	1.5	3
GV-6	2	1	1	1.5	3
GV-7	2	1	1	1.5	3
GV-8	2	2	0	2	3
Total Raw Score	**15**	**10**	**5**	**12.5**	**24**
Percentage Score (Raw Score divided by 40)	**38%**	**25%**		**31%**	**60%**

Table 17 – Governance Maturity Summary

The following chart displays the key elements above using a maturity assessment rating of 1-5.

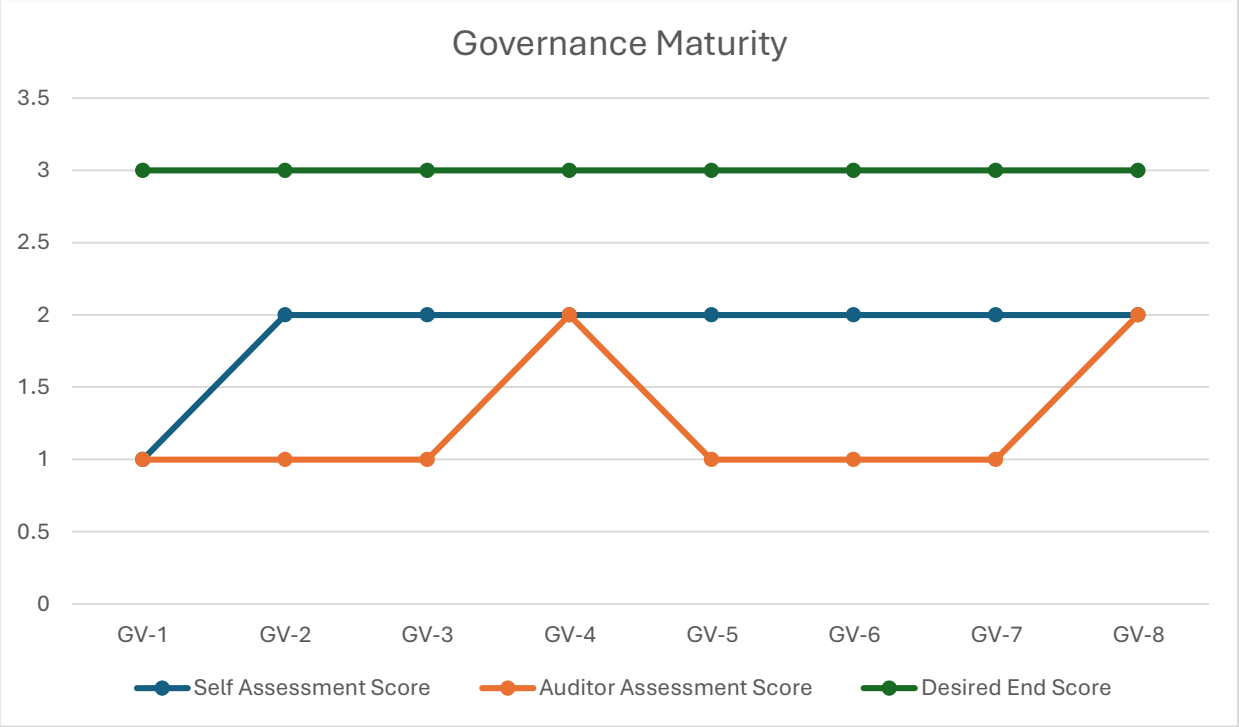

Figure 9 – Governance Maturity Graph

RISK REPORTING (RRP)

An objective of any ERM process is to provide information to senior management and the Executive Directors/Division Heads about the organization's portfolio of risks and related response to those risks. As risks are identified and assessed across the organization, processes are needed to facilitate the communication of risk-related information so that an aggregate view of important risks and their related risk responses are provided to senior management, Executive Directors/Division Heads, and to critical stakeholders.

In our assessment of the CFTC Risk Reporting Maturity, we took the following key elements into consideration:

Key Element	Description of Key Elements
RRP-1	Senior management has developed and monitors critical risk indicators that are lagging in nature (i.e., metrics that show when risk events have occurred, are escalating, or provide some indication that a risk event is more likely to occur in the future).
RRP-2	Senior management regularly receives and reviews a “dashboard” or other reports that provide the status of critical risks and/or risk response plans.
RRP-3	Senior management has identified thresholds or trigger points whereby risk metrics indicate that an emerging risk warrants greater management and/or board attention.
RRP-4	Output from the organization’s ERM processes about significant risk exposures are considered by management and leadership in making organizational risk disclosures to critical stakeholders.

Table 18 – Risk Reporting Key Elements and Descriptions

The graph below illustrates the Risk Reporting Maturity assessment performed by the CFTC ERM Team as well as Williams Adley.

Risk Reporting Maturity Summary					
Key Element	**CFTC ERM Self-Assessment Score**	**Auditor Assessment Score**	**Delta**	**Average Initial Score**	**Desired End Score**
RRP-1	1	1	0	1	3
RRP-2	1	1	0	1	3
RRP-3	1	1	0	1	3
RRP-4	1	1	0	1	3
Total Raw Score	**4**	**4**	**0**	**4**	**12**
Percentage Score (Raw Score divided by 20)	**20%**	**20%**		**20%**	**60%**

Table 19 – Risk Reporting Maturity Summary

The following chart displays the key elements above using a maturity assessment rating of 1-5.

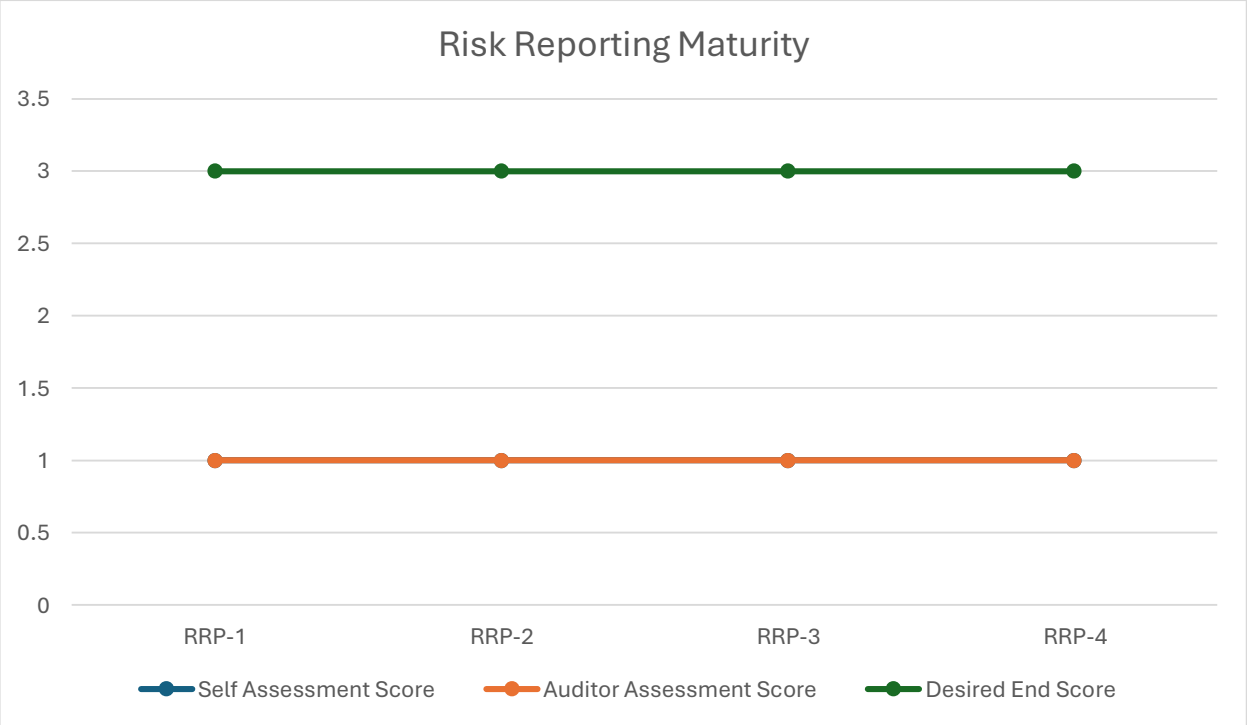

Figure 10 – Risk Reporting Maturity Graph

INTEGRATION WITH STRATEGIC PLANNING (ISP)

Integration with Strategic Planning is only useful when, the organization's efforts related to risk management and the efforts related to strategic planning are not distinct and separate activities. Effective ERM can be an important input and consideration into the determination and execution of any organization's strategy. ERM provides critical insights into the portfolio of existing and emerging risk exposures that can contribute to the strategic success of the organization.

In our assessment of the CFTC Integration with Strategic Planning Maturity, we took the following key elements into consideration:

Key Element	Description of Key Elements
ISP-1	The organization has a formal strategic planning process.
ISP-2	The strategic plan is updated at least annually.
ISP-3	The organization's existing risk profile (i.e., output from the ERM processes) is an important input for the strategic planning process.
ISP-4	Senior management links the top risk exposures to strategic objectives to determine which objectives face the greatest number of risks and to determine which risks impact the greatest number of objectives.
ISP-5	When evaluating a range of strategic options, consideration is given to the potential impact of each option on the organization's existing enterprise-wide risk profile.
ISP-6	The senior executive with explicit responsibility for enterprise-wide risk management leadership (or the chair of the committee with that responsibility) is actively engaged in the strategic planning process.
ISP-7	The organization's ERM processes encourage the consideration of opportunities where the organization can take informed risks to generate incremental returns.
ISP-8	The organization's risk appetite statement guides the goal setting process
ISP-9	The organization's strategic plan has been communicated to employees so that they can understand how their actions can create or prevent risks to the achievement of strategic objectives.

Table 20 – Integration with Strategic Planning Key Elements and Descriptions

The graph below illustrates the Integration with Strategic Planning assessment performed by the CFTC ERM Team as well as Williams Adley.

Integration with Strategic Planning Maturity Summary					
Key Element	CFTC ERM Self-Assessment Score	Auditor Assessment Score	Delta	Average Initial Score	Desired End Score
ISP-1	3	2	1	2.5	3
ISP-2	2	1	1	1.5	3
ISP-3	2	2	0	2	3
ISP-4	2	1	1	1.5	3
ISP-5	2	1	1	1.5	3
ISP-6	3	3	0	3	3
ISP-7	2	1	1	1.5	3

Integration with Strategic Planning Maturity Summary					
Key Element	CFTC ERM Self-Assessment Score	Auditor Assessment Score	Delta	Average Initial Score	Desired End Score
ISP-8	1	1	0	1	3
ISP-9	3	2	1	2.5	3
Total Raw Score	**20**	**14**	**6**	**17**	**27**
Percentage Score (Raw Score divided by 45)	**44%**	**31%**		**38%**	**60%**

Table 21 – Integration with Strategic Planning Maturity Summary

The following chart displays the key elements above using a maturity assessment rating of 1-5.

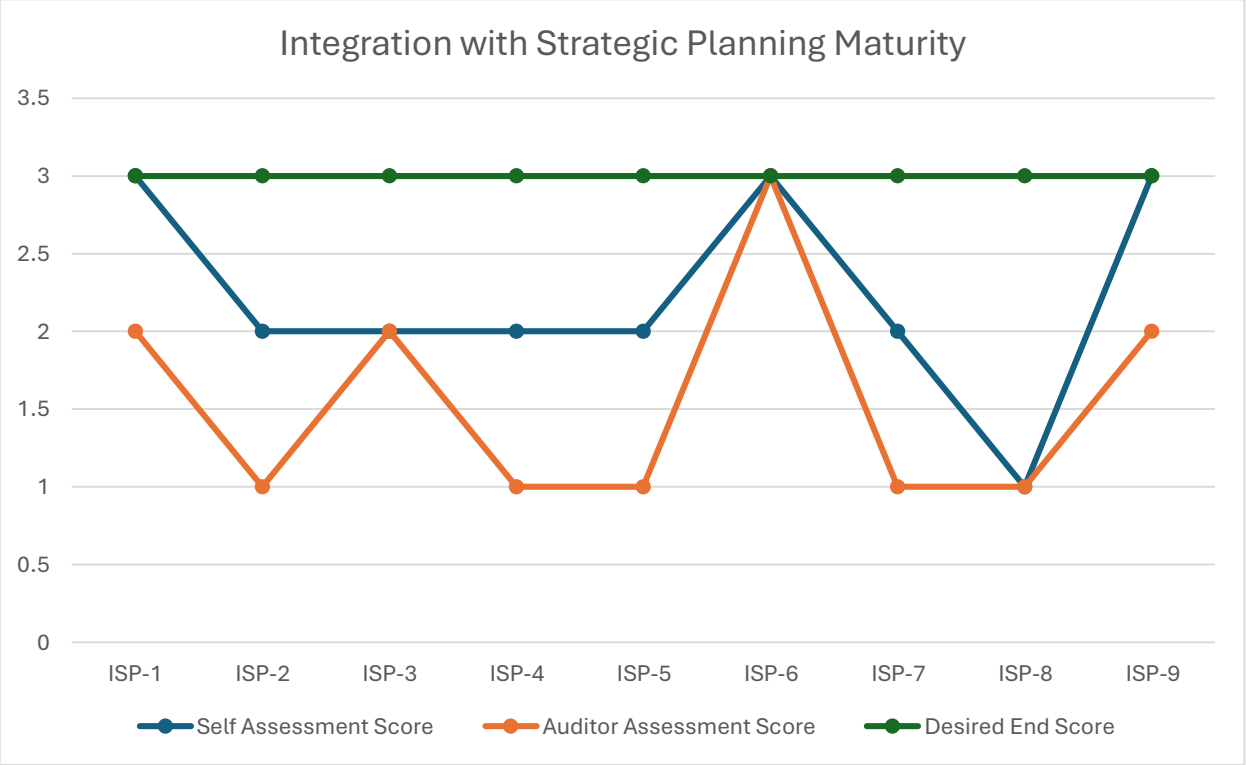

Figure 11 – Integration with Strategic Planning Maturity Graph

ASSESSMENT OF ERM EFFECTIVENESS (AEE)

While awareness of the concept of ERM has been growing over the last decade, processes and techniques involved in any ERM implementation continue to evolve and mature. Additionally, as the complexity of the federal environment continues to increase, new methodologies and procedures will be needed to effectively manage the portfolio of risks organizations will face in the future. As a result, senior management and Executive Directors/Division Heads need to view ERM as an evolution, not a point-in-time project to be implemented.

In our assessment of the Assessment of Effectiveness Maturity, we took the following elements into consideration:

Key Element	Description of Key Elements
AEE-1	The organization regards ERM as an ongoing process rather than just a project.
AEE-2	Senior management seeks to understand and monitor emerging ERM best practices.
AEE-3	Senior management has engaged in ERM related training or other knowledge enhancing activities.
AEE-4	Adequate resources have been dedicated to support the ERM function.
AEE-5	The organization periodically obtains an objective assessment of its ERM processes (e.g., through internal audit or third party ERM expert evaluations).
AEE-6	The organization evaluates risk events that have occurred to better understand why the risk occurred and whether there were failures in the organization's ERM processes.
AEE-7	The organization identifies and subsequently implements changes to improve its ERM processes.

Table 22 – Assessment of ERM Effectiveness Key Elements and Descriptions

The graph below illustrates the Assessment of ERM Effectiveness assessment performed by the CFTC ERM Team as well as Williams Adley.

Assessment of ERM Effectiveness Maturity Summary					
Key Element	**CFTC ERM Self-Assessment Score**	**Auditor Assessment Score**	**Delta**	**Average Initial Score**	**Desired End Score**
AEE-1	2	1	1	1.5	3
AEE-2	3	3	0	3	3
AEE-3	2	2	0	2	3
AEE-4	2	1	1	1.5	3
AEE-5	1	1	0	1	3
AEE-6	2	2	0	2	3
AEE-7	2	1	1	1.5	3
Total Raw Score	**14**	**11**	**3**	**12.5**	**21**
Percentage Score (Raw Score divided by 35)	**40%**	**31%**		**36%**	**60%**

Table 23 – Assessment of ERM Effectiveness Maturity Summary

The following chart displays the key elements above using a maturity assessment rating of 1-5.

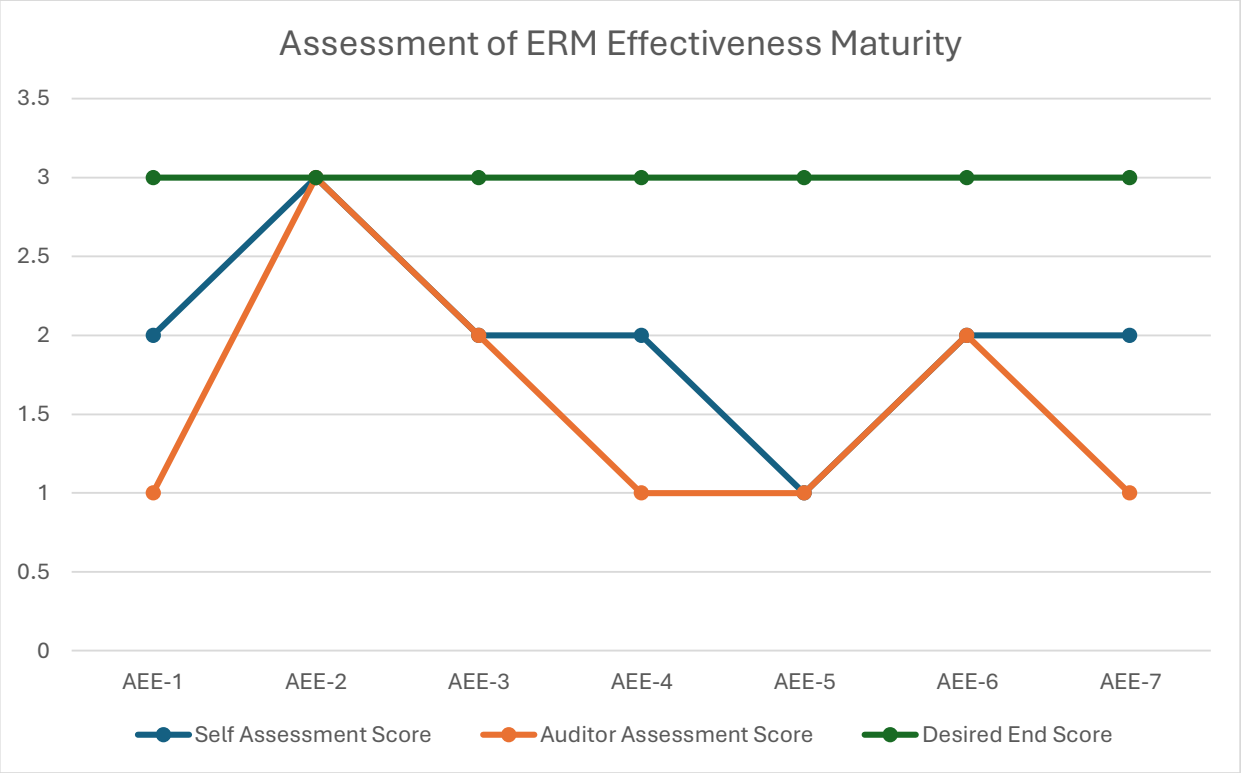

Figure 12 – Assessment of ERM Effectiveness Maturity Graph

APPENDIX 3: MANAGEMENT RESPONSE

U.S. COMMODITY FUTURES TRADING COMMISSION
Three Lafayette Centre
1155 21st Street, NW, Washington, DC 20581
Telephone: (202) 418-5000
Facsimile: (202) 418-5521
www.cftc.gov

MEMORANDUM

TO: Christopher Skinner
Inspector General
Office of the Inspector General

FROM: Jeffrey Sutton
Executive Director
Division of Administration

DATE: February 24, 2025

SUBJECT: Commodity Futures Trading Commission (CFTC) Management's Response to Draft Report on Enterprise Risk Management Performance Audit FY 2024

Thank you for providing us with the opportunity to comment on the Office of the Inspector General's (OIG) Draft FY 2024 Enterprise Risk Management (ERM) Performance Audit Report. We appreciate the thoroughness and professionalism of your review, and we value the OIG's role in helping us strengthen our risk management processes for the CFTC.

Management has carefully reviewed the audit findings outlined in the report and we concur with recommendations. Management takes the findings seriously and is committed to creating a corrective action plan to address these findings.

We appreciate the dialogue we have had throughout this review and thank the OIG for its valuable input. If you require further assistance, please contact Karrenthya Simmons, Acting Chief Risk Officer at (202) 418-5134.

CC:
Karrenthya Simmons
Acting Chief Risk Officer
Division of Administration


COMMODITY FUTURES TRADING COMMISSION
CFTC
OIG
OFFICE OF INSPECTOR GENERAL