FEDERAL COMMUNICATIONS COMMISSION Washington, D.C. 20554 **FCC DIRECTIVE**	**Title** **Enterprise Risk Management**	
	Directive Number: FCCINST 1481.1	**Effective Date:** November 2021

1. PURPOSE:

   To set forth the policies, procedures, and responsibilities for improving the accountability and effectiveness of the Federal Communications Commission (FCC)'s programs and operations by: identifying and managing risks; establishing accountability for assessing, correcting, and reporting on the effectiveness of internal controls; and maintaining an Enterprise Risk Management (ERM) program. The overall objective of this directive and the FCC's ERM program is to ensure public confidence in the FCC by: (1) managing the full spectrum of the FCC's significant risks as an interrelated portfolio; (2) governing enterprise risks to effectively and efficiently accomplish the FCC's broader mission and strategic goals; and (3) promoting an open and transparent culture that encourages risk information flow and a collaborative response to identified risks.

2. BACKGROUND:

   Every federal agency is required to establish and maintain an ERM program in order to improve the efficiency and effectiveness of the Government. Risks include, but are not limited to, those associated with strategy, operations, reporting, compliance, reputation, safety, privacy, supply chain, cybersecurity, improper payments, and fraud. FCC leadership has the responsibility to holistically manage the combined set of risks as part of its ERM program.

3. SCOPE:

   This directive applies to all Bureaus and Offices within the FCC.

4. AUTHORITY:

   A. Government Accountability Office, Standards for Internal Control in the Federal Government, GAO-14-704G (Sept. 10, 2014) (Green Book).

   B. Government Accountability Office, A Framework for Managing Fraud Risks in Federal Programs, GAO-15-593SP (July 28, 2015).

   C. Office of Management and Budget, Management's Responsibility for Enterprise Risk Management and Internal Control, OMB Circular A-123 (July 15, 2016).

D. Office of Management and Budget, Management's Responsibility for Enterprise Risk Management and Internal Control, OMB Circular A-123 Appendix A, Management of Reporting and Data Integrity Risk (June 6, 2018).

E. Office of Management and Budget, Preparation, Submission, and Execution of the Budget, OMB Circular A-11.

F. Office of Management and Budget, Financial Reporting Requirements, OMB Circular A-136.

G. Federal Managers' Financial Integrity Act of 1982 (FMFIA), Pub. L. No. 97-255, 96 Stat. 814, 31 U.S.C. § 3512.

H. GPRA Modernization Act (GPRAMA), Pub. L. No. 111–352, 124 Stat. 3866, .

5. DEFINITIONS:

A. Enterprise Risk Management (ERM). An effective agency-wide approach to addressing the full spectrum of the organization's significant risks by considering the combined array of risks as an interrelated portfolio, rather than addressing risks only within silos.

B. Risk. The effect of uncertainty on objectives. Risks are both positive (opportunities) and negative (threats).

C. Risk Profile. A prioritized inventory of the most significant risks identified and assessed through the risk assessment process versus a complete inventory of risks.

D. Inherent Risk. The exposure arising from a specific risk before any action has been taken to manage it beyond normal operations.

E. Residual Risk. The exposure remaining from an inherent risk after action has been taken to manage it, using the same assessment standards as the inherent assessment.

F. Risk Acceptance: One of the risk responses where no action is taken to respond to the risk due to the insignificance of the risk or where the risk is knowingly assumed by the organization to seize an opportunity.

6. POLICY:

The FCC shall continuously and strategically mitigate the likelihood and impact of all significant enterprise risks that have been identified by factoring in the cost and benefit analysis as well as budget limitations. The FCC's ERM efforts are intended to facilitate achievement of its broader mission and strategic goals by helping to ensure that funds are spent effectively, services fulfill their intended purpose, and assets are safeguarded. FCC policy for ERM relates to the following areas:

A. ERM Practice: Consistent with the Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government* and *Framework for Managing Fraud Risk in*

Federal Programs and other federal guidance, the FCC shall ensure that its Office of Managing Director (OMD):

(1) Follows leading practices for FCC's risk management activities;

(2) Incorporates fraud and cybersecurity assessment as part of its enterprise risk assessment process; and

(3) Assesses and tailors its risk assessment process, as needed, to enhance FCC's risk maturity.

B. Annual Assertion Letter and Risk Assessment: The FCC shall require all Bureau and Office Chiefs to provide an annual assertion letter describing the overall effectiveness of internal controls in their organization, as well as any risks, issues or concerns. The annual assertion letter shall include:

(1) An assessment of the strength of their internal controls over operations, reporting and compliance;

(2) The status of enterprise level risks faced by their Bureau or Office;

(3) A list of their enterprise level risks that have been deemed "accepted risks" based on an assessment by their Bureau or Office; and

(4) A list of their open audit findings along with estimated dates of completion.

The assertion letters provided by the Bureau and Office Chiefs shall form the basis for the FCC Chairperson to sign the assertion letter that is included in the Annual Agency Financial Report.

C. Strategy, Performance and Budget Integration: To maximize its mission impact and increase effectiveness and efficiency of its operations, the FCC shall integrate enterprise risks in its:

(1) Strategic planning and review;

(2) Performance review; and

(3) Budget planning and allocation.

D. Monitoring and Evaluation: The FCC's enterprise risks and internal control strength shall be subject to ongoing and periodic review by the Managing Director and the Senior Management Council. This information shall be used to continuously improve the controls and risk responses for the effective and efficient realization of the FCC's mission goals.

E. Risk Awareness: The FCC shall utilize the FCC University and its ERM team to enhance the enterprise wide risk awareness for the FCC staff with the goal to embed and enhance the risk aware decision making culture at all levels within the organization.

F. Crisis Management: In case a crisis hits the FCC with impact to multiple Bureaus and/or Offices, the Managing Director shall assemble a team that is best equipped to address the situation and lead the path to organizational recovery.

The FCC's Continuity of Operations (COOP) shall be invoked depending upon the extent of impact. The COOP shall be developed and led by the Public Safety and Homeland Security Bureau (PSHSB). In support of the COOP, IT shall be responsible for conducting annual Disaster Recovery Planning (DRP)/Plugs-out testing in coordination with all the Bureaus and Offices.

7. ROLES AND RESPONSIBILITIES:

A. The Office of Managing Director will:

(1) Work with the relevant Bureaus and Offices to ensure that risk management, including fraud and cybersecurity risk management, are a continuous process at the FCC resulting in necessary internal control improvements and preparedness for enterprise risks;

(2) Maintain and update this directive, as necessary, due to changes at the FCC or as new government-wide guidance becomes available;

(3) Ensure that employees are notified annually regarding the mandatory risk trainings;

(4) Ensure that risk is integrated in strategy, performance and budgetary decision making;

(5) Enable the ERM team to become the integrator of all risk management activities for the FCC;

(6) Facilitate FCC's Senior Management Council (SMC) discussions; and

(7) Lead the organizational recovery from crisis.

B. The Chief Financial Officer will:

(1) Oversee the FCC's annual enterprise wide risk assessment process, including the fraud risk assessment and integration of the Office of the Chief Information Officer (OCIO)'s cybersecurity risk assessment;

(2) Chair the SMC and organize its meetings;

(3) Provide to the FCC's senior management an analysis of the results of the annual risk assessment process, including any information related to the fraud and cybersecurity risk assessments;

(4) Provide support to the ERM team to effectively discharge its function as the integrator of all risk management activities within FCC; and

(5) Enable the process to include risk information in the budgetary decision-making process.

C. The Chief Risk Officer will:

(1) Ensure a comprehensive enterprise wide approach to risk management;

(2) Coordinate the FCC's annual enterprise wide risk assessment process, including the fraud risk assessment, and coordination with OCIO regarding the cybersecurity risk assessment;

(3) Ensure timely completion of the annual risk assessment analysis, including any information related to fraud and cybersecurity risks;

(4) Establish a process to include risk information in the budgetary decision-making process; and

(5) Engage with relevant stakeholders to elevate the organizational risk maturity over time.

D. The SMC will:

(1) Serve as the governing body for enterprise wide actions related to enterprise risk management;

(2) Enable a comprehensive approach to identifying, reporting, and responding to a combined set of risks, including operations, reporting, compliance, strategy, improper payments, fraud, cyber, privacy, and data risks;

(3) Ensure that risks are incorporated in decision-making activities and accountability for all risks is clearly established and maintained;

(4) Promote communication, collaboration, and integration across risk management activities;

(5) Provide ongoing guidance and support in addressing corrective actions and in refining the FCC's risk management framework;

(6) Support integration of risk with strategy, performance and budget; and

(7) Include as its members, the Managing Director, Chief Financial Officer, Chief Information Officer, Chief Risk Officer, Senior Agency Official for Privacy (SAOP), Chief Information Security Officer, Performance Improvement Officer,

Chief Data Officer, Chief of Staff from all Bureaus and Offices, Office Chiefs of small FCC offices and OMD Division Chiefs.

E. The Bureaus and Offices Chiefs will:

(1) Integrate risk with strategy, performance and budget within their Bureaus and Offices;

(2) Establish a culture of risk transparency for enhanced risk-aware decision making;

(3) Assess the effectiveness and efficiency of internal controls and risk management activities for continuous improvement actions at least annually;

(4) Involve the ERM team and other relevant stakeholders as new enterprise risks emerge, or any new enterprise level risks are being accepted by the Bureau or Office needing no action;

(5) Maintain adequate documentation and be the custodian for their Bureau or Office risk management actions, including accepted risks;

(6) Support ERM efforts by actively engaging their Bureaus or Office at the SMC and other offline ERM workgroups; and

(7) Support the COOP efforts including development/update of the COOP plan and annual DRP/Plugs-out testing.

8. EFFECTIVE DATE AND IMPLEMENTATION:

This directive is effective immediately and shall be implemented promptly upon distribution.

Mark Stephens
Digitally signed by Mark Stephens
Date: 2021.11.08 08:26:39 -05'00'

Mark Stephens
Managing Director