TSA MANAGEMENT DIRECTIVE No. 100.8
Enterprise Risk Management

To enhance mission performance, TSA is committed to promoting a culture founded on its values of Integrity, Innovation and Team Spirit.

1. **PURPOSE:** This directive provides TSA policy and procedures for enterprise risk management (ERM).

2. **SCOPE:** This directive applies to all TSA Program Offices and risk management staff that support the development and implementation of ERM at TSA.

3. **AUTHORITIES:** Office of Management and Budget (OMB) Circular A-11 Sections 270.24 – 270.29

4. **DEFINITIONS:**

   A. Enterprise Risk Management (ERM): Comprehensive approach to risk management that engages organizational systems and processes together to improve the quality of decision making for managing risks that may hinder an organization's ability to achieve its objectives.

   B. Executive Risk Steering Committee (ERSC): Governing body that retains overarching responsibility for defining strategy and managing risk at an enterprise level. The ERSC is chaired by the Chief Risk Officer (CRO) and composed of Assistant Administrators (AAs) from the Offices of Acquisition, Finance and Administration, Human Capital, Information Technology, Global Strategies, Intelligence and Analysis, Law Enforcement/Federal Air Marshal Service, Security Capabilities, Security Operations, and Security Policy and Industry Engagement.

   C. Key Risk Indicator (KRI): Measures that provide an early warning system that a risk is occurring or has occurred.

   D. Risk: Potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and associated consequences.

   E. Risk Appetite: Amount and type of risk that an organization is willing to pursue or retain.

   F. Risk Owner: Person or entity with the accountability and authority to manage a risk.

   G. Issue: An existing event or condition that an organization must address to achieve its mission.

5. **RESPONSIBILITIES:**

   A. The TSA Administrator is responsible for maintaining ultimate accountability for the management of the agency's portfolio of risks across the enterprise, including issuing directives for their management. The Administrator also authorizes and owns the TSA ERM Policy and issues final approval of the ERM risk appetite statements.

B. The Chief Risk Officer (CRO) is responsible for the design, development, and implementation of the ERM program at TSA. The CRO serves as the principal advisor to the Administrator and Deputy Administrator on all risk matters that could impact TSA's ability to perform its mission.

C. Assistant Administrators (AAs) are responsible for:

(1) Serving as ultimate risk owners in accordance with the ERSC Charter;

(2) Ensuring that Program Offices adopt and follow the ERM framework and the TSA ERM directive and participate in enterprise-wide risk management efforts within their individual office; and

(3) Implementing consistent risk management practices in alignment with this directive.

NOTE: It will be the responsibility of the Program Offices to disaggregate the enterprise level risk appetite statements into Program Office-specific risk limits, where applicable.

D. The Executive Risk Steering Committee (ERSC) is responsible for:

(1) Overseeing the development and implementation of processes used to analyze, prioritize, and address risks across TSA to include terrorism threats facing the entire transportation sector, along with non-operational risks that could impede TSA's ability to achieve its strategic objectives; and

(2) Ensuring risks are managed to create value for the Nation and in a manner consistent with established risk appetite and risk tolerances levels.

E. The ERM Team is responsible for:

(1) Leading ERM activities under the supervision of the CRO;

(2) Developing and maintaining ERM policies, processes, procedures, tools, and information systems;

(3) Leading efforts to perform enterprise risk identification, assessment, prioritization, reporting, and monitoring; and

(4) Overseeing the process for establishing ERM communication at all levels for gathering data and developing risk reports.

F. TSA Program Office ERM Liaisons are responsible for serving as the primary representative to the ERM Team, communicating with the ERM Team, and supporting Program Office risk owners throughout the ERM process, as necessary.

G. The ERM Working Group (ERMWG) is responsible for:

(1) Sharing information and providing subject matter expertise to support ERM program activities, such as the identification, validation, and assessments of enterprise risks; and

(2) Serving as the primary point of communication between the ERM Team and its members' respective Program Office.

H. Risk Analysis Integrated Project Teams (IPT) are responsible for assessing a defined risk to identify cross-functional root causes and consequences, and coordinate with the ERM Team and risk owners to develop recommendations for risk response and monitoring plans.

6. POLICY: The security of the Nation's transportation systems is vital to the economic health and security of America. Ensuring transportation security while promoting the freedom of movement of legitimate travelers and commerce is a critical counter-terrorism mission assigned to TSA. Risk management approach must support TSA's ability to identify, analyze, and appropriately respond to strategic risks across the full spectrum of TSA activities.

A. The Chief Risk Officer, working with the Executive Risk Steering Committee, shall develop and implement ERM as the framework for risk management across the organization. Through ERM, we will:

(1) Provide a structured, disciplined, and consistent approach to assessing risk aligned with U.S. Department of Homeland Security guidance.

(2) Identify strategic risks that threaten TSA's achievement of our long-term objectives and goals, and manage those risks at the enterprise level through the ERSC.

(3) Ensure that risks are managed in a manner that maximizes the value TSA provides to the nation consistent with defined risk appetite and risk tolerance levels.

(4) Align our strategy, process, people, technology, and information to support agile risk management.

(5) Provide greater transparency into risk by improving our understanding of interactions and relationships between risks in support of improved risk-based decision making.

(6) Establish clear accountability and ownership of risk.

B. Risk management is central to TSA's mission, vision, and culture. All employees are expected to adopt the principles of risk management developed through the ERM program, and to apply the standards, tools, and techniques within their assigned responsibilities.

C. TSA creates value by protecting the Nation's transportation systems while enabling the movement of legitimate travelers and goods. TSA seeks practical and cost-effective solutions to effectively reduce the most significant transportation security risks.

D. TSA has different appetites for different risk types expressed in the following statements:

(1) TSA is strongly averse to security risks that could result in catastrophic consequences.

(2) TSA is strongly averse to the compromise of classified information and averse with regard to the compromise of Sensitive Security Information (SSI) and Personally Identifiable Information (PII).

(3) TSA is averse to workforce-related risks pertaining to integrity, performance, health and safety, and regulatory compliance.

(4) TSA is averse to events that could damage its standing and reputation with the traveling public, U.S. Congress, and other federal and industry stakeholders.

(5) TSA is risk neutral with regard to other mission and business operational enterprise risks.

(6) TSA is risk tolerant to programs that enhance the movement of legitimate travelers and goods.

E. TSA makes risk-informed decisions to achieve its mission within the parameters of its risk appetite:

(1) TSA evaluates and manages risks to the five transportation modes for which it is responsible arising from international terrorists, homegrown violent extremists, insiders, or other adversaries.

(2) TSA considers the interconnected and interdependent nature of the physical, human, and cyber components of the transportation infrastructure when assessing risks and response plans.

(3) TSA recognizes the need to balance security effectiveness with operational efficiency, cost, industry vitality, and passenger satisfaction by taking a systems approach to risk management.

(4) TSA evaluates the highest risk scenarios and the effectiveness of layered security counter-measures using advanced computational techniques to apply finite resources commensurate with the risk level.

(5) TSA strikes a balance between countering known risks and hedging against unknown risks by using strategies such as deploying random security countermeasures and enhancing system resiliency.

(6) TSA maintains a flexible capability to focus resources on the basis of real-time threat information.

(7) TSA takes decisive action to respond to imminent threats with potentially catastrophic consequences and security effectiveness may take precedence over other considerations.

(8) TSA evaluates risk levels and implements risk responses and monitoring to bring the risk within tolerance without over-controlling non-security-related enterprise risks.

(9) TSA embraces innovation to address adaptive adversaries and changing targets. TSA understands that innovation requires experimentation and balances the need for timely deployment with appropriate testing.

7. PROCEDURES: See TSA ERM Manual.

8. APPROVAL AND EFFECTIVE DATE: This policy is approved and effective the date of signature unless otherwise specified.

APPROVAL

Signed October 22, 2014

Kenneth C. Fletcher
Chief Risk Officer

Date

EFFECTIVE

Date

Distribution: Senior Management Officials and Business Management Offices (BMOs)
Point-of-Contact: Enterprise Risk Management, OCRORiskManagement@tsa.dhs.gov