TSA ERM Capability Maturity Model

Maturity Levels	Initial/Ad Hoc 1	Fragmented 2	Comprehensive 3	Integrated 4	Strategic 5
Governance					
Governance & Oversight	• Authority and accountability for risk management are poorly defined and not documented. • Senior leadership and executive management have not defined tone at the top. • There is no separation of risk taking from risk oversight. • Segregation of duties are not in place. • Risk management is reactive. • Minimal controls in place.	• Authority and accountability for risk management may be defined within some program offices and for some risk types. • Senior leadership and executive management have not consistently communicated or enforced tone at the top. • Segregation of duties has been defined for some authority centers (committees, boards, functions, or positions granted authority). • Risk management may be reactive.	• Authority and accountability for risk management is defined and documented at the Administrator level and within all program offices. • Senior leadership and executive management have consistently communicated and enforced tone at the top regarding risk across the enterprise. • Segregation of duties has been defined for all relevant authority centers. • Risk management is proactive. • There is a designated risk committee with decision authority.	• The exercise of authority, accountability, and segregation of duties is efficient and effective across the enterprise, including for those mission and mission support activities that occur across organizational boundaries • Issues related to shared authorities are minimized.	• The enterprise is recognized by the public and stakeholders for good corporate citizenship and creating value. • External partners engaged to participate.

Maturity Levels	Initial/Ad Hoc 1	Fragmented 2	Comprehensive 3	Integrated 4	Strategic 5
Objective Setting	• Objective setting is informal or may not be documented. • There is no consideration of risk in the objective setting process.	• Objectives are set disparately across the program offices in silos with no clear alignment to an enterprise-level strategy. • Mission and strategic objectives and metrics are not clear or consistent across the Program offices. • Risk is considered in the objective setting process in some program offices for some risk types.	• Objectives and strategic plans exist for the enterprise and all program offices. • Risk appetite is defined and considered when planning and budgeting and evaluating new programs, products and services. • Progress against plans are monitored and communicated across the program offices. • Risk metrics are used to measure performance against objectives.	• Mission objectives are set for the enterprise, are adopted by all program offices, and are aligned with the enterprise's risk appetite. • Risk appetite drives risk tolerance levels and risk limits for the enterprise. • There are clear metrics to demonstrate performance. • Risk management objectives and strategy are developed dynamically in conjunction with overall mission strategy.	• Strategy is embedded into day-to-day office activities and fully integrates all risk types. • Management of risk is directly linked into key value drivers and performance measures. • Staff performance is linked to active risk management. Plans are updated throughout the year as events, emerging risks, and emerging opportunities warrant. Risk management strategy has demonstrably shifted from value preservation to value creation.
Policies	• Risk policies are undocumented or vague. • Risk policies are not maintained.	• Risk policies are documented by program offices without coordination. • Risk policies are limited to a subset of risk types. • Development of a high level enterprise risk policy may be initiated.	• Risk policies are developed by the enterprise and all program offices and include all relevant risk types. • Enterprise level risk policy may not reference program office policies.	• An enterprise-level risk policy has been implemented. • Program office risk policies are consistent with the enterprise risk policy. • Policies provide for the correlation and aggregation of risks across program offices and risk types. • The enterprise and program office risk policies specify risk tolerances and limits for all risk types.	• Risk policies are integrated into the agency/administration and fully reflect strategy. • Risk policies are revisited and updated during the strategic planning process to reflect accurately the enterprise's risk appetite, risk tolerance, and correlation of risks. Risk policies provide guidance on how to seize opportunities and exploit risks.

Maturity Levels	Initial/Ad Hoc 1	Fragmented 2	Comprehensive 3	Integrated 4	Strategic 5
Risk Taxonomy/ Lexicon	• There is no overall definition for major risk types. • The definitions used are inconsistent and not clearly understood throughout the enterprise.	• Some risk definitions exist, but they are applied or interpreted in an inconsistent manner across the program offices. • The definitions of risk types differ among program offices and are limited to a subset of risk types related to external threats and security.	• Risk taxonomy is expanded to include all widely recognized risk types in each program office. • The definitions are used consistently across the program offices and include hard-to-quantify operational mission support and strategic risks in addition to mission related risks. • The categorization framework is aligned to the organizational structure.	• All major risks and their correlations are defined across the enterprise to facilitate risk aggregation • Definitions include resolution of boundary issues between mission support and mission risks. • Risk taxonomy is integrated and actively used with threat taxonomy.	• There is a fully integrated definition that supports the governance, organization structure, and information management protocols. • The definition of risk includes both the downside and the upside of risk.

Maturity Levels	Initial/Ad Hoc 1	Fragmented 2	Comprehensive 3	Integrated 4	Strategic 5
Risk Appetite	• There is no formal process in which to set risk appetite and tolerance. • Risk appetite concepts are not understood throughout the enterprise. • Vague articulation of risk appetite and tolerance is made by program offices on an ad hoc basis. • The risk appetite and tolerance vary from exposure to exposure. • Risk limits are not documented.	• Elements of risk appetite are defined in relevant risk policies for some risk types in some program offices. • There is some understanding of the overall risk appetite at the executive level and some at the management level, but this is not articulated into specific tolerance levels which can be allocated or communicated across the program offices. • Some risk measures and limits are documented. However, they are broad and have minimal impact on decision making or they are focused only on aviation passenger transportation or cargo, not both. • Risk measures and limits are not fully understood or complied with across the program offices	• Risk appetite is explicitly defined at an overall level for the enterprise. • Risk measures and limits are linked to the goals of the enterprise and the expectations of the senior leadership team and other stakeholders. • The enterprise has clearly documented risk measures and limits and standards for risk taking that are widely understood throughout the enterprise. • Conformance with risk appetite is a key criterion in the assessment of new programs, processes, or security measures.	• Risk measures and limits are set at the enterprise level and are allocated across program offices. • Risk appetite forms an integral part of overall strategy and is reviewed at regular intervals. • Increased sophistication is present in the use of quantitative and qualitative criteria to assess performance against appetite levels. • Risk exposures are calculated frequently and hierarchically within the organizational structure. • Limits and standards are communicated across program offices and their usage is widely embedded in day-to-day activities.	• Risk appetite forms an integral component of the enterprise's strategic objectives and plans. • An aggregate risk measure has been adopted and is used to guide decision-making. • Risk appetite is formulated on an integrated risk basis using quantitative and qualitative methods that allow for timely recalibration of limits as operating conditions change. There is clear understanding of the value drivers that influence risk appetite.

Maturity Levels	Initial/Ad Hoc 1	Fragmented 2	Comprehensive 3	Integrated 4	Strategic 5
Resource Allocation and Investment Decisions	Resources are allocated and investment or budgeting decisions made with limited regard to the level of risks.	Investments in projects exceeding a defined threshold are evaluated for some, but not necessarily all, risk types.	• All major investments are evaluated for all relevant risk types. • Resource allocation is calculated for all risk types • Understanding the individual layers of security drives resource allocation.	• Resource allocation is performed on a portfolio basis including the effects of correlation. • Resource allocation is revisited during the year as operating and threat conditions warrant. • Sections of the transportation system are considered in the portfolio review.	• A proactive risk and return strategy is set and compliance is monitored. • Program decisions at all levels utilize risk-adjusted metrics. • Resource allocation is revisited as opportunities arise. • Top-down and bottom-up risk levels are measured and reconciled. • The Transportation system as a whole is considered in portfolio reviews.

Maturity Levels	Initial/Ad Hoc 1	Fragmented 2	Comprehensive 3	Integrated 4	Strategic 5
Process					

Maturity Levels	Initial/Ad Hoc 1	Fragmented 2	Comprehensive 3	Integrated 4	Strategic 5
Establish the Context ▪ **Regulatory context** ▪ **Culture** ▪ **Structure** ▪ **Capabilities** ▪ **Goals & objectives** ▪ **Aligned risk management objectives**	▪ There are limited activities undertaken to identify or understand risks emanating from the external regulatory, political, or from the internal culture and organizational structure. ▪ Risk management is not defined relative to the goals or objectives of the enterprise or program offices. ▪ Risk management processes are not in place.	Risk management processes are implemented to manage some risk types in some program offices.	Program offices consider the external regulatory, political, stakeholder environment and internal environment and mission objectives in formulating risk management objectives and processes.	▪ Enterprise-level strategy and objectives inform the definition of the enterprise's risk appetite, risk management objectives. ▪ Enterprise risk appetite and risk management objectives inform the risk appetite and risk management objectives of the program offices in an integrated fashion and addresses segments of the transportation sector.	▪ Risk management objectives are inseparable from the enterprise's mission strategy and objectives. All risk management activities are designed to support achievement of the administration's missions and considers the entire transportation sector.

Maturity Levels	Initial/Ad Hoc 1	Fragmented 2	Comprehensive 3	Integrated 4	Strategic 5
Identify Risks	▪ Management reacts to risks as they occur. ▪ Management relies on personal experience or past organizational experience, reports, or checklists to identify risks. ▪ Review of historical events and proactive contingency planning do not take place. ▪ There is no formal or consistent practice to continuously identify enterprise risks or to document risks and their impacts. ▪ Formal responsibility for risk identification has not been assigned	▪ Risks are identified for some program offices for some risk types. ▪ Risk identification focuses only on external threats and security risk. ▪ Identification techniques rely primarily on past risk events. ▪ Risk management databases may be implemented within some program offices for some risk types.	▪ A well-structured systematic process is set up to generate a comprehensive list of risk factors across the enterprise. ▪ Risk management databases are implemented in all program offices and maintenance is enforced. ▪ Management identifies both internal and external sources of risk that could significantly, adversely affect the attainment of TSA's key objectives, projects, processes, functions, or systems. ▪ Risks are considered as chains of events rather than as isolated incidents. New and emerging risks are identified by means of review of external information sources.	▪ Improved and consistent techniques of risk identification are used across the enterprise. ▪ Interrelationships of risks across risk types and program offices are captured using techniques such as event tree analysis and structured scenario analysis. ▪ New and emerging risks are identified by means of scenario planning or other visioning techniques.	▪ Risks and opportunities are identified to seize opportunities and create value. ▪ Risk identification process is forward looking and there is real time dynamic reporting to executives and risk owners. ▪ Both upside and downside risks are identified and their interrelationships are well understood and exploited.

Maturity Levels	Initial/Ad Hoc 1	Fragmented 2	Comprehensive 3	Integrated 4	Strategic 5
Analyze Risks	Qualitative assessments are used to provide a general understanding of risk.	▪ Quantitative analysis is developed for a few more prevalent risk types in the operational and program areas. ▪ Program offices and divisions assess risks individually with an internal focus.	▪ Quantitative analysis is developed for prioritized risk types including those that are traditionally harder to quantify such as operational, regulatory, strategic, and political risks. ▪ Analysis techniques are more refined (e.g. structured scenario analysis, game theory, and real options). Different risk models may be used for different risk types, such as deterministic models for some and probabilistic models for others. ▪ Assumptions and weaknesses are clearly stated and understood. ▪ Multi-disciplinary groups are involved in the risk analysis. ▪ Risk interactions are addressed qualitatively. ▪ Sensitivity analysis may be performed. ▪ Risk interactions are recognized and analyzed qualitatively. ▪ Risk analysis informs decision making	▪ Sophisticated risk measures are used that allow aggregation across risk types and across program offices are used to analyze all risk types. ▪ Events are evaluated relating to the impact across the enterprise. ▪ Correlation matrices are developed to quantify the inter-relationships of risks. ▪ Structural simulation models are used that explicitly recognize cause and effect linkages based on data, where available and pertinent, and on expert opinion to fill in gaps. ▪ Sensitivity analysis is expanded to all relevant risks. ▪ The use of a common risk measure makes it possible for risk aggregation across all risk types and across all program office. ▪ All risks are aggregated reflecting correlations and portfolio effects expressing the results in terms of the impact on the enterprise's key performance indicators. Risks are aggressively analyzed for off-setting or mutually amplifying interactions.	▪ Risk analysis is integrated with mission planning. ▪ Structural simulation models allow management to exploit their knowledge of cause and effect relationships and correlations to dynamically model the effect of different decisions on mission outcomes and the risk portfolio. ▪ An open environment is created to share information about a risk within the enterprise in order to arrive at the best possible understanding. ▪ A robust and dynamic risk aggregation solution exists across the administration for all risk types and program offices. Aggregation is linked to risk appetite and limit allocation across program offices.

Maturity Levels	Initial/Ad Hoc 1	Fragmented 2	Comprehensive 3	Integrated 4	Strategic 5
Evaluate Risks	There is no evaluation and prioritization of risks.	Program offices prioritize among a subset of risks using simple, predetermined criteria. Risks are evaluated using qualitative or semi-quantitative estimations (to include threat, vulnerability, and consequence or probability and impact).	▪ Enterprise risks are evaluated and prioritized using pre-defined and standardized criteria. •	▪ More sophisticated ranking and prioritization techniques are possible facilitated by the robust characterization and quantification of risk correlations and the ability to aggregate risks. ▪ The marginal contribution of each individual risk factor to the overall risk profile of the enterprise can be determined, e.g. flight by flight or cargo.	The impact of particular risk factors on the attainment of mission objectives are isolated and quantified and incorporated into strategic and program planning and used to identify areas requiring further analysis and specific risk responses.
Treat Risks/Develop strategies	▪ Managers and staff perform reactive "damage control" as events occur. Response plans are not formulated or documented.	▪ Individual program offices may have risk response plans for some risk types, but they are not well-coordinated across offices ▪ Response options are selected mainly based on past experience and may not be rigorously analyzed across all offices relative to risk appetite, tolerance, limits and cost-benefit analysis. •	▪ Risk response plans are developed within each program office for all risk types. ▪ The enterprise has a more complete picture of its risks through insight into risks and the associated risk response plans at program offices •	▪ Management considers the entire portfolio view of risks and risk response options when treating risks, including all risk types in all program offices. ▪ There is consensus and alignment across TSA regarding possible actions. ▪ Whenever a risk response impacts the likelihood or impact of a risk, a new evaluation of the risk portfolio is undertaken to assess the impact on the overall risk profile. Response options are analyzed and selected relative to desired risk appetite, tolerance, and limits thresholds	▪ Response plans are integrated with the management and budgetary processes of the enterprise. Risk responses embody leading practices and are reviewed on a regular basis for potential improvement.

Maturity Levels	Initial/Ad Hoc 1	Fragmented 2	Comprehensive 3	Integrated 4	Strategic 5
Monitor & Review	▪ There is no regular monitoring of key risk indicators or enforcement of compliance with a formal risk management framework. ▪ There is no formal annual review of all risk activities. ▪ Monitor and review is reactionary and ad-hoc.	▪ Each program office operates its own monitor and review practices. ▪ Post-event analysis is performed for some risks, and lessons learned are incorporated into risk response plans. Post-event analysis is performed for failed projects.	▪ All risk types are monitored and reviewed within all program offices. ▪ Key risk indicators are documented and monitoring plans and alert and notification protocols are in place. ▪ Key performance indicators are documented allowing monitoring and control against defined risk tolerances and limits. ▪ Post-event analysis is performed for all risk events and failed projects, and lessons learned are incorporated into risk response plans. ▪ A comprehensive database is maintained for all risk events and near misses.	▪ Active portfolio management undertaken across risk types and program offices thorough understanding of risk dependencies, causal links, and interdependencies allows the impact of risk events to be quickly assessed for the enterprise as a whole. ▪ Scenario analysis and mock crisis events are used to assess and improve readiness. ▪ Risk tolerance and limit violations are reported and corrective action taken timely.	▪ The enterprise risk portfolio is continuously monitored relative to defined risk appetite and tolerance levels. ▪ Changes in the enterprise's risk profile are assessed relative to the achievement of business objectives, and strategic course corrections are implemented quickly. ▪ Lessons learned and control deficiencies drive improvement initiatives, which are implemented and reported across the enterprise. A monitoring and review program is developed for the enterprise with a focus on sustainability and continuous improvement.
Communication	▪ Communication is informal and infrequent with a long lag time in most situations.	▪ Communication flows within program offices and to some external stakeholders; however, communication may not include all necessary offices and stakeholders. ▪ Communication quality varies by program office and situation.	▪ Quality and comprehensive communication exists within the program offices and flows up to the enterprise level and out to external stakeholders.	▪ Effective communication flow with internal and external stakeholders exists throughout the enterprise.	▪ Communication effectiveness is measured and continuously improved.

Maturity Levels	Initial/Ad Hoc 1	Fragmented 2	Comprehensive 3	Integrated 4	Strategic 5
People					
Organizational Structure	No formalized structure has been set up for the senior leadership team or executive management for risk management.	▪ Risk management is decentralized. The authority and responsibilities reside within each program office. ▪ Governance may be specified for only some risk types. ▪ No Chief Risk Officer position or committee structures (at either board or senior management levels) are in place for the enterprise as a whole although these may exist in some or all program offices	▪ The Chief Risk Officer position exists. ▪ Committee structures exist at the executive leadership levels. ▪ The enterprise has made a decision about the degree of risk management centralization and has designed an organizational structure accordingly. ▪ Program offices may or may not have their own risk managers/officers and risk committees depending on the degree of centralization or decentralization.	▪ An optimal balance between centralized and decentralized risk management has been attained. ▪ Reporting relationships between the senior leadership team, the enterprise Chief Risk Officer, and senior management risk committees, and any program office risk officers and risk committees have been clarified.	Enterprise is recognized as best in class by external parties with respect to separation or risk taking and risk oversight functions and activities.
Roles & Responsibilities	▪ The senior leadership team is not engaged in enterprise risk management. ▪ Enterprise does not have dedicated risk resources and depends on the initiative of individuals to react to risk events as they occur. ▪ Risk owners are not defined.	▪ Risk owners for some risk types are defined and supported with staff. ▪ Specific individuals are designated with defined roles, responsibilities, and authorities. ▪ There is weak accountability because reporting is not rigorous to hold individuals accountable for results. ▪ Coordination across offices and divisions is challenging.	▪ Risk is on the agenda of the senior leadership team. ▪ The senior leadership team fully supports the initiative and direct risk appetite and risk reporting for all risk types. ▪ More rigorous methodologies and reporting protocols provide clarity to accountability.	▪ Roles and responsibilities are clearly defined and consistent across the enterprise, with a central function coordinating efforts, minimizing duplication, and providing appropriate backup capabilities. ▪ Dedicated risk professionals have a wide array of skills to assess multiple risk types across program offices. ▪ Integrated teams are formed across program offices where efficiencies can be gained.	▪ Individual performance incentives are linked to enterprise risk strategies. Integrated teams operate seamlessly across program offices and at the enterprise level.

Maturity Levels	Initial/Ad Hoc 1	Fragmented 2	Comprehensive 3	Integrated 4	Strategic 5
ERM Knowledge, Skills, and Abilities	Some individuals do not understand enterprise risk principles or utilize common risk terminology.	▪ Individuals are trained in the risk management process. ▪ Individuals have deep subject matter expertise limited in scope	▪ Requisite knowledge, skills, and abilities are in place for all risk types. ▪ Risk professionals are trained in enterprise risk management, and are embedded in all business units or program offices.	▪ Risk management professionals understand how risks are aggregated and correlated. ▪ Dedicated risk management professionals keep abreast of industry developments, and receive regular external training.	▪ Executives and managers understand how to evaluate opportunities in light of the risks they pose. ▪ All employees have a basic understanding of risk management and the roles they play. Risk management specialists engage in industry eminence-building activities.
Culture	▪ Risk management is generally viewed as a non-value adding activity. ▪ Raising and discussing risks are not encouraged by senior management.	▪ Tone is not set at the top. ▪ There is limited buy-in from program offices for enterprise-wide risk management. ▪ A risk management culture within program offices may be strong, but may vary from office to office. ▪ Within a program office there may be very different cultures for different risk types.	▪ Senior management commitment to risk management is explicitly communicated within the program offices. ▪ Staff throughout the organization (both at headquarters and at field offices) are aware of the increased emphasis on enterprise risk management and are beginning to be more aware of how risks need to be better integrated into the culture.	▪ Integrated enterprise-wide risk management practices are embedded in business processes and reinforced by the "tone at the top." ▪ Program offices do not resist executive guidance. ▪ The entire enterprise can articulate the enterprise's risk management strategy, vision, objectives, and risk appetite and tolerance levels. ▪ There is a commitment to competence to ensure that all individuals have the necessary knowledge and skills to perform their duties ▪ Risk culture is regularly measured to determine degradation.	▪ There is an open environment that fosters objective discussion about risks across the enterprise. ▪ Risk management is everyone's job. ▪ The enterprise focuses on value creation as well as preservation.

Maturity Levels	Initial/Ad Hoc 1	Fragmented 2	Comprehensive 3	Integrated 4	Strategic 5
Technology					
Data	▪ Data are incomplete, out-of-date, inaccurate, or late. ▪ There is no formalized or coordinated collection and sharing of risk data across the enterprise. ▪ Costs of data gathering and reconciliations are high.	▪ There is improved data quality for a few selected risks. ▪ Some risk data collection is formalized, coordinated, and shared but is not consistent across the enterprise. ▪ Historical data are collected for risk events and near misses by some program offices for some risk types.	▪ Data are captured for all risk types and program offices. However, data and methods may be risk or program office specific and not consistent across the enterprise. ▪ Data capture is integrated and shared with ongoing business and mission operations activities so that data are captured at the source. ▪ Historical data are collected for risk events and near misses by all program offices consistently for all risk types. ▪ External data sources are used to identify emerging risks.	▪ Risk analysis systems collect data as part of normal business routines. ▪ An enterprise-wide risk management system can access risk data from across the enterprise either through a centralized risk data warehouse or using metadata solutions. ▪ Risk data from all program offices are available for centralized, enterprise-level reporting. ▪ Backup and data integrity issues are addressed.	Data for strategic planning, budgeting, and resource allocation flow seamlessly.
Systems	▪ Systems are unstable and not scalable (for example, spreadsheets) and provide no audit trail. ▪ System architecture is not conducive in providing information for decision making.	▪ There are multiple systems that collectively have important functionality gaps. ▪ Systems enable quantitative analysis for limited priority risk types. ▪ Risk registers or repositories exist in some program offices for some risk types and are not integrated with other systems and program offices. ▪ There is no system for enterprise risk management.	▪ Systems are more stable and scalable with improved functionality. ▪ Systems enable quantitative analysis for applicable/relevant risk types. ▪ Robust risk registers are maintained by all program offices for all risk types and at the enterprise level.	▪ Systems are integrated with dashboard reporting and drill-down capabilities. ▪ Risk analytics are built into decision support systems. ▪ Systems enable quantitative analysis, correlations between individual risks and their aggregations to be modeled for all risk types and all program offices.	▪ Integrated systems are improved continuously. Systems for strategic planning, budgeting and resource allocation are integrated with those for enterprise risk management.

Maturity Levels	Initial/Ad Hoc 1	Fragmented 2	Comprehensive 3	Integrated 4	Strategic 5
Reports	▪ Management reports are sporadic, ad hoc, informal, incomplete and/or inconsistent.	▪ Some reports are formally defined for management at the enterprise level and are issued consistently and timely with limited supporting detail. ▪ Reports are defined for some risk types in some program offices. Report availability and relevance at enterprise level may not meet management needs.	▪ Integrated management reports are prepared for all risk types across all program offices at regular predefined intervals such as monthly. ▪ Predefined reports are prepared for a Risk Management Committee (RMC) on a regular basis such as monthly and the senior leadership team quarterly. ▪ Exceptions, events, "near misses" and emerging risks are reported in a timely manner.	▪ There is consistent reporting of objectives, targets, performance and risks across the enterprise. ▪ Reports for the enterprise provide for the correlation and aggregation of the risks in a portfolio view. ▪ Portfolio view enables integration of risk reports from classified and unclassified systems. ▪ Data visualization is utilized	▪ "What if" scenarios conducted and reported. ▪ Real-time and dynamic monitoring is used for risk reporting