



Transportation Security Administration

# Transportation Security Administration Enterprise Risk Management

## ERM Policy Manual

August 2014



## Contents

Abbreviations .....	4
Introduction.....	5
Purpose of this document.....	6
ERM Objective .....	7
Enterprise Risk Management Policy Statement.....	8
ERM Roles and Responsibilities .....	9
TSA Administrator .....	9
Enterprise Risk Steering Committee (ERSC).....	9
Chief Risk Officer (CRO) .....	9
Assistant Administrators (AAs) .....	9
ERM Team .....	10
Program Office ERM Liaisons.....	10
ERM Working Group (ERMWG).....	10
Risk Analysis Integrated Project Team (IPT).....	10
Policy Review and Administration.....	10
Related Laws, Regulations, and Policy Exceptions .....	11
ERM Process Framework .....	12
Guide to Process Description Terms .....	13
Establish the Context.....	14
Identify Risks .....	18
Analyze Risks.....	21
Evaluate Risks .....	25
Respond to Risks.....	28
Monitor and Review .....	33
Communicate and Consult .....	37
Appendix 1: Risk assessment scales -notional.....	41
Appendix 2: Risk monitoring and reporting templates.....	46
Appendix 3: Executive Risk Steering Committee Charter .....	52
Appendix 4: TSA Risk Appetite Statement.....	56
Appendix 5: ERM Lexicon.....	58
Appendix 6: ERM Risk Taxonomy .....	61



## Document control information

### Document information

<b>Document name</b>	TSA Enterprise Risk Management (ERM) Policy Manual
<b>Document author</b>	TSA Chief Risk Officer
<b>Document version</b>	Version 1
<b>Document status</b>	Final
<b>Date released</b>	August 2014

### Document edit history

<b>Version</b>	<b>Date</b>	<b>Additions/modifications</b>	<b>Prepared/revised by</b>
1.0	August 2014	Initial Release	OCRO

### Document review/approval history

<b>Date</b>	<b>Name</b>	<b>Organization/title</b>	<b>Comments</b>



## Abbreviations

The following abbreviations are used throughout the document for conciseness:

<b>AA</b>	Assistant Administrator
<b>CMM</b>	Capability Maturity Model
<b>CRO</b>	Chief Risk Officer
<b>DHS</b>	Department of Homeland Security
<b>ERM</b>	Enterprise Risk Management
<b>ERSC</b>	Executive Risk Steering Committee
<b>GPRA</b>	Government Performance and Results Modernization Act
<b>HSE</b>	Health, Safety, and Environment
<b>KPI</b>	Key Performance Indicators
<b>KRI</b>	Key Risk Indicators
<b>OCRO</b>	Office of the Chief Risk Officer
<b>PAR</b>	DHS Performance Accountability Report
<b>TSA</b>	Transportation Security Administration
<b>TSA-RK</b>	Transportation Security Administration Risk Knowledge Center



## Introduction

TSA is developing an Enterprise Risk Management (ERM) capability to provide a structured, disciplined, and consistent approach to risk management that facilitates risk-informed decision making throughout the organization. ERM provides TSA with a means to align strategy, processes, people, technology, and knowledge for the purpose of evaluating and managing uncertainties in executing our counterterrorism mission. A consistent approach to risk management across the organization is essential for TSA leaders to identify and prioritize strategic risks and for prioritizing competing requirements. ERM enables TSA to more effectively manage enterprise level risks, and it enables agency leaders to consider the trade-offs between risks, associated costs, and value creation across the organization.

This manual explains the ERM process and provides actionable steps necessary for a mature and successful ERM program. As TSA's Chief Risk Officer (CRO), I have approved this approach to implementing ERM as the path to achieve mature and sustainable ERM activities and processes. By consistent use of ERM across the organization, TSA will be positioned to identify and assess risks within the current environment through a systematic process which evaluates the impact of risk on TSA's ability to achieve our mission and objectives in support of U.S. Department of Homeland Security (DHS) strategic objectives.

A handwritten signature in black ink, appearing to read "K. Fletcher".

Kenneth C. Fletcher  
Chief Risk Officer



## **Purpose of this document**

TSA's Enterprise Risk Management Manual (ERM Manual) has several purposes. First, the ERM Manual details the specific duties and responsibilities of TSA's CRO, ERM team, and risk management staff, and it provides information necessary for these individuals to effectively perform their ERM duties.

Next, the ERM Manual describes the ERM process and provides an overview of the seven-step closed loop process that defines TSA's ERM framework. Each process step is described separately and includes key objectives, "triggers" affecting the successive order of process steps, details around the corresponding activities, and the roles and responsibilities required of individuals involved in performing the activities. To familiarize users with context of each process step within the ERM framework, process flow diagrams accompany each section to illustrate the inter-relatedness of activities and interactions between activity owners.

Finally, the manual is intended for use by program offices to guide the development of risk management capacity using agency-wide processes and standardized assessment scales.

The contents of this document provide the initial blueprint for TSA's ongoing ERM program. Because TSA is in the initial stages of ERM implementation, some of the appendices are preliminary or remain under development. Updates to these appendices will occur as development efforts are completed and as the ERM program matures.



## ERM Objective

TSA's ERM framework provides the means to embed risk management as a core competency in TSA programs, enabling the agency to fully embed robust and consistent risk management practices at both the enterprise-wide level and within each Program Office in a way that facilitates risk-informed decision making at all levels.

The ERM objectives are to:

- Support TSA leadership through transparency and insight into risks that could impact the ability to execute TSA's mission through the implementation of well-defined and common risk management processes, tools, and techniques.
- Quickly identify both current and emerging risks and develop plans to respond to risks as well as to take advantage of opportunities.
- Increase the likelihood of success in achieving the objectives of TSA's mission and the DHS Strategic Plan.
- Build credibility and sustain confidence in TSA's governance and risk management by all stakeholders including industry, federal, state, and local partners, and the American people.
- Improve the understanding of interactions and relationships between risks.
- Establish clear accountability and ownership of risk.
- Develop the capacity for continuous monitoring and reporting of risk across the Agency from the operational level to the ERSC.
- Develop a common language and consistent approach across all Program Offices that help to establish the broad scope of risk and to organize risk management activities and reinforces TSA's risk culture.
- 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.

TSA recognizes that many risks within the organization are interrelated and cannot be effectively and efficiently managed independently within a given Program Office. Instead, these interconnected risks facing TSA must be managed across the organization and, in many instances, in tandem between the agency and its stakeholders. This manual sets forth guidance in the form of repeatable processes and activities to identify, analyze, evaluate, and respond and effectively manage the risks to TSA's mission.



## Enterprise Risk Management Policy Statement

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 the Transportation Security Administration (TSA). I firmly believe that implementing effective risk management principles across all aspects of TSA is essential to our successful execution of this mission in the long term.

Our risk management approach must support our ability to identify, analyze, and appropriately respond to strategic risks across the full spectrum of TSA activities. I have directed the Chief Risk Officer, working with the Executive Risk Steering Committee, to develop and implement Enterprise Risk Management (ERM) as the framework for risk management across the organization. Through ERM, we will:

- Provide a structured, disciplined, and consistent approach to assessing risk aligned with U.S. Department of Homeland Security guidance.
- 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.
- 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.
- Align our strategy, process, people, technology, and information to support agile risk management.
- Provide greater transparency into risk by improving our understanding of interactions and relationships between risks in support of improved risk-based decision making.
- Establish clear accountability and ownership of risk.

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. With your cooperation and commitment to this policy, TSA can best ensure the safety and security of the nation's transportation systems by providing the most effective security in the most efficient manner.

John S. Pistole  
Administrator





## **ERM Roles and Responsibilities**

### **TSA Administrator**

The TSA Administrator maintains ultimate accountability for the management of the agency's risks, 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.

### **Enterprise Risk Steering Committee (ERSC)**

The role of the ERSC, chaired by the 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, is to oversee the development and implementation of processes used to analyze, prioritize, and address risks across TSA. These risks include terrorism threats facing the entire transportation sector, along with non-operational risks that could impede TSA's ability to achieve its strategic objectives. The ERSC is broadly responsible for ensuring that risks are managed to create value for the Nation and in a manner consistent with established risk appetite and risk tolerances levels. Specific duties and responsibilities are depicted in the ERSC Charter attached as Appendix 3 to this manual.

### **Chief Risk Officer (CRO)**

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. The CRO is responsible for the design, development, and implementation of the ERM program at TSA. The CRO, in conjunction with the TSA ERM Team, will lead TSA in conducting regular enterprise risk assessments of TSA business processes or programs at least quarterly and will oversee the identification, assessment, prioritization, response, and monitoring of enterprise risks. The CRO will also lead TSA strategic planning and integration of risk-based security (RBS) and risk management (RM) principles across the enterprise. The CRO, in collaboration with the TSA Chief Architect, will develop the strategic risk architecture, and align systems and technical architecture efforts within respective Program Offices for proper integration.

### **Assistant Administrators (AAs)**

AAs, who comprise TSA's Senior Leadership Team (SLT), serve as ultimate risk owners in accordance with the ERSC Charter. Program Offices will adopt and follow the ERM framework and the TSA ERM Policy and participate in enterprise-wide risk management efforts and perform risk management activities within their individual office. AAs are responsible for implementing consistent risk management practices in alignment with this policy. 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. Program Offices and AAs will also



assist the ERM Team in creating ad-hoc risk analysis teams to serve as Subject Matter Experts (SMEs) during the risk identification and analysis process.

### **ERM Team**

The ERM Team resides within the Office of the Chief Risk Officer (OCRO) and leads ERM activities under the supervision of the CRO. Such activities include developing and maintaining ERM policies, processes, procedures, tools, and information systems; leading efforts to perform enterprise risk identification, assessment, prioritization, reporting, and monitoring; and, establishing ERM communication at all levels and for gathering data and developing risk reports.

### **Program Office ERM Liaisons**

Program Office ERM Liaisons are designated individuals within each TSA Program Office that serve as the primary representative to the ERM Team. ERM Liaisons are responsible for communicating with the ERM Team and supporting Program Office risk owners throughout the ERM process, as necessary.

### **ERM Working Group (ERMWG)**

The ERMWG is an advisory body that shares information and provides subject matter expertise to support ERM program activities, such as the identification, validation, and assessments of enterprise risks. This group also serves as the primary point of communication between the ERM Team and its members' respective Program Office. There shall be a core team of advisors on the ERMWG which represent each Program Office, but other TSA subject matter experts (SMEs) may be identified to participate on an as-needed basis.

### **Risk Analysis Integrated Project Team (IPT)**

Risk Analysis IPTs are comprised of cross-functional subject matter experts (SMEs) that are responsible for assessing a defined risk to identify cross-functional root causes and consequences. IPT members will assist the ERM Team and Risk Owners to develop event trees or scenarios, estimate probabilities and impacts, identify risk response options, perform cost-benefit analysis, identify Key Risk Indicators (KRIs), and develop recommendations for risk response and monitoring plans.

### **Policy Review and Administration**

The content and the level of detail of the ERM policy will evolve as the TSA ERM program matures. The CRO will review the TSA ERM policy every year at a minimum and provide recommended changes for consideration and comment by the ERSC prior to finalizing any future revisions.



**Related Laws, Regulations, and Policy Exceptions**

ERM policies, procedures, and activities must comply with Government Statutes and Laws as well as requirements dictated by the U.S. Congress, U.S. Department of Homeland Security (DHS), U.S. Government Accountability Office (GAO), and other relevant stakeholders. Any exception to this policy must be documented in writing and approved by the AA of the Program Office and forwarded to the CRO for notification, review, and approval. The Risk Management Division of the OCRO will track policy exceptions and report this status to the ERSC. Additionally, policy exceptions must be reviewed and approved by TSA's SLT.



## ERM Process Framework

The ERM process framework depicted below is being implemented by TSA. It is closely aligned with the DHS Risk Management Process<sup>1</sup> and incorporates elements from the International Standards Organization (ISO) 31000:2009 Risk Management — Principles and Guidelines, and the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management Integrated Framework (2004).

Figure 1: TSA Enterprise Risk Management Process



This risk management process provides a logical and systematic method for establishing the context for risks, as well as identifying, analyzing, evaluating, responding to, monitoring, and communicating them in a way that will allow TSA to make decisions and respond timely to risks and opportunities as they arise. This approach promotes comparability and a shared understanding of information and analysis in the decision process and facilitates a better risk

---

<sup>1</sup> Beers, R.,(2011), *Risk Management Fundamentals, Homeland Security Risk Management Doctrine*, U.S. Department of Homeland Security, Washington, D.C., April 2011, p. 15



management structure and risk-informed decision making. Details regarding each process within the context of the overall ERM Framework are contained in each section.

### **Guide to Process Description Terms**

To add to the understanding and use of the ERM process, each of the seven steps is described using a consistent format with each element described below. In addition, process flow diagrams accompany each sub-process to further explain responsibilities, relationships, and sequence of actions within each sub-process.

Overview: The Overview section provides a short description of the process describing its key elements. This contains a summary of the process to provide context and orient readers with the content.

Objectives: The Objectives section describes the purpose for performing the process. The objective statement is a high-level statement that explains the ‘why’ but not the ‘how’ of the process inputs being transformed into process outputs.

Triggers: The Triggers section describes what prompts or initiates the process to occur and when, if time dependent. A process must have at least one trigger, but may have many. In some cases the trigger may be a scheduled start date. For example, *Establish the Context* could be scheduled on an annual basis during a particular month. Another typical trigger would be the completion of the preceding process in the risk management framework. For example, *Analyze Risks* is performed upon the completion of *Identify Risks*.

Inputs: The Inputs section lists all materials, data, or information required to perform the process. Inputs can consist of: Output from a preceding or parallel process; publications, notifications, or formal communications; data from a database or other source; and documents or reports providing information or data.

Activities: The Activities section lists and describes each activity represented in the process flow diagrams. Each activity within the process is a task or set of tasks required to produce the desired outputs from the inputs. Activities having a manual component may require a procedure per the guidance in the introduction. Activities are best defined for a single organizational unit to simplify procedure-writing. However, certain activities require close interaction among two departments or functions. These should be evaluated on a case-by-case basis.

Process owner(s): The Process Owners section outlines those individuals with accountability for the outlined activity. These individuals oversee the activity to be performed and have sufficient authority to enforce policies and procedures and authorize the resources to carry out span of activity.

Process participants: The Process Participants section lists the roles of individuals required to perform the activities. The key process participants are represented by the swim lanes in the process flow diagrams. However, there may be other process participants, and they will be listed in each section. Descriptions of the roles of each of the process participants are defined in the ERM Accountabilities and Responsibilities section above.



**Outputs:** The Outputs section lists the materials, information, or data produced by the process. Outputs can consist of: Input to another process; publications or formal communications; alerts or notifications; interfaces to another process; data written to a database or other source; documentation or reports providing information or data.

## **Establish the Context**

### **Overview**

The *Establish the Context* process step involves understanding and articulating the internal and external environment of the organization. During this step is where TSA defines its objectives, evaluates the external and internal parameters to be taken into account when managing risk, makes changes to the risk management process, and develops risk criteria.

### **Objectives**

To establish the scope of the risk management process by reviewing TSA's strategic objectives, environment, risk management objectives, and the criteria against which risks will be assessed.

### **Triggers**

These are some of the triggers for conducting this step of the process:

- Annual context review performed each July
- Major changes in organizational structure, such as the formation of a new Program Office
- Congressional, Administration, or DHS mandates affecting risk management processes
- Occurrence of a major risk event where "major" refers to risk events having a high degree of severity on the enterprise impact scale

### **Inputs**

- TSA mission statement, vision, strategic goals, and objectives
- Analysis of risk response options and controls effectiveness
- Financial audit reports and findings
- DHS Strategic Plan, Quadrennial Homeland Security Review (QHSR)
- TSA ERM Policy, risk appetite statements, roles and responsibilities, organizational structure charts, and ERSC Charter
- Existing ERM process documentation
- GPRA measures, including DHS Annual Performance Report (APR)
- Information about major changes in external or internal environment affecting strategic objectives or risk profile
- Scope of risk assessments (from previous year or last time developed)
- Stakeholder analyses and inputs



## Process participants

- ERSC
- CRO
- ERM Team
- ERM Liaisons
- Risk Owners

## Activities

1. Evaluate external, internal, and risk management context (ERSC, CRO, ERM Team, ERM Liaisons, Risk Owners). Review existing DHS and TSA risk documentation, including the risk lexicon (see inputs), to assess whether current policies and procedures are sufficient, or if additional criteria and policies should be developed. Review should include changes in TSA's internal and external environment such as: Newly-identified emerging risks, industry volatility, and changes to characteristics of the flying public, new threats or technologies, organizational changes, etc.
2. Adjust risk assessment criteria, policies, and charters (CRO, ERM Team, ERM Liaisons). Identify the types of impacts which are most critical to TSA through interviews with TSA leadership and ERSC members. Ensure definitions of levels of impacts are relevant to appropriately reflect TSA's risk appetite and tolerance. Obtain guidance and approval for changes from appropriate parties, including ERSC members.
3. Approve risk criteria, policies, and charters (CRO and ERSC). Review proposed policy, charter, and risk criteria revisions submitted by the ERM Team. Provide comments and feedback to the ERM Team. Communicate development of changes and confirmed revisions to the SLT to endorse agreed revisions.
4. Propose risk assessment scope (ERM Team). Determine the scope of risk identification and assessment activities for the year by annual review of the Risk Register. Review any changes to the internal and external risk management context, and identify business activities requiring a re-assessment of risks. Input and guidance should be sought from Risk Owners in defining the scope for the risk assessments. Obtain agreement from Risk Owners as to whether or not risks in their area require re-assessment during the coming year.
5. Define risk assessment scope (Risk Owners). Review anticipated mission and business operations for the coming year and determine if any changes in the external context (e.g., new threats or technologies, changing laws or regulations, etc.), should trigger a re-evaluation of existing risks, or the identification of new and emerging risks. Review proposed risk assessment scope provided by ERM Team and provide input.
6. Approve TSA risk assessment scope (ERSC). Review the risk assessment scope proposed by ERM Team and reviewed by Risk Owners, provide input and guidance, attend meetings, and vote on the endorsement.
7. Update ERM Risk Register (ERM Team). Review the structure and elements of TSA's Risk Register and other risk management systems and tools in light of the previous activities. Determine if any changes need to be made, update processes and procedures to reflect the changes, and communicate the changes to affected parties.



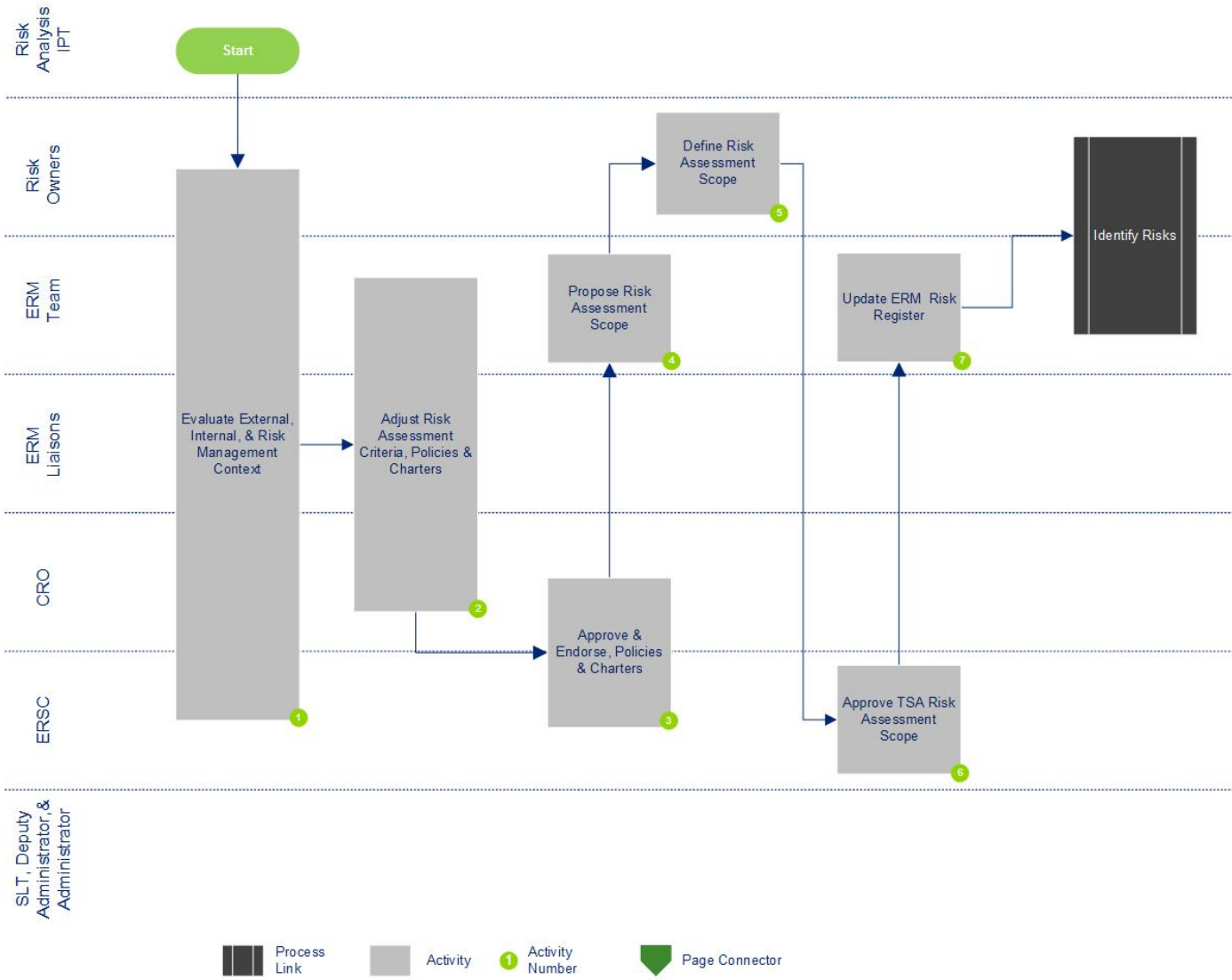
## Outputs

- Updated ERM Policy, risk appetite statements, roles and responsibilities, organizational structure charts, and ERSC Charter
- Updated impact, likelihood scales, and tolerance thresholds
- Risk assessment scope (for current year)





Figure 2: Establish the context process flow diagram





## Identify Risks

### Overview

During the *Identify Risks* process step, TSA seeks to identify enterprise-level risks to be managed using a structured, systematic process called the Enterprise Risk Register. This process specifies what risks can occur, as well as where, when, why, and how they may occur. At this stage in the overall framework, the primary concern is to identify as many risks to achieving the TSA's mission and vision as possible, the sources of the risks, and the impacts. The list of risks identified through this process is preliminary and subject to further qualification and refinement as part of the following *Analyze Risks* process. The *Identify Risks* process captures risks using TSA's enterprise risk taxonomy and then progressively narrows the list to the most critical using first qualitative and then quantitative techniques in the *Analyze Risks* process.

### Objectives

To identify a comprehensive list of risks and events that may potentially impact the achievement of TSA's mission and strategic objectives.

### Triggers

- Completion of *Establish the Context* process

### Process participants

- ERSC
- CRO
- ERM Team
- ERM Liaisons
- Risk Owners

### Inputs

- Audit reports and findings
- Stakeholder analyses and inputs
- Updated ERM Policy, risk appetite statements, roles and responsibilities, organizational structure charts, and ERSC Charter
- Updated impact, likelihood scales, and tolerance thresholds (if applicable)
- Processes
- Intelligence information
- GAO reports
- TSA Risk Map



## Activities

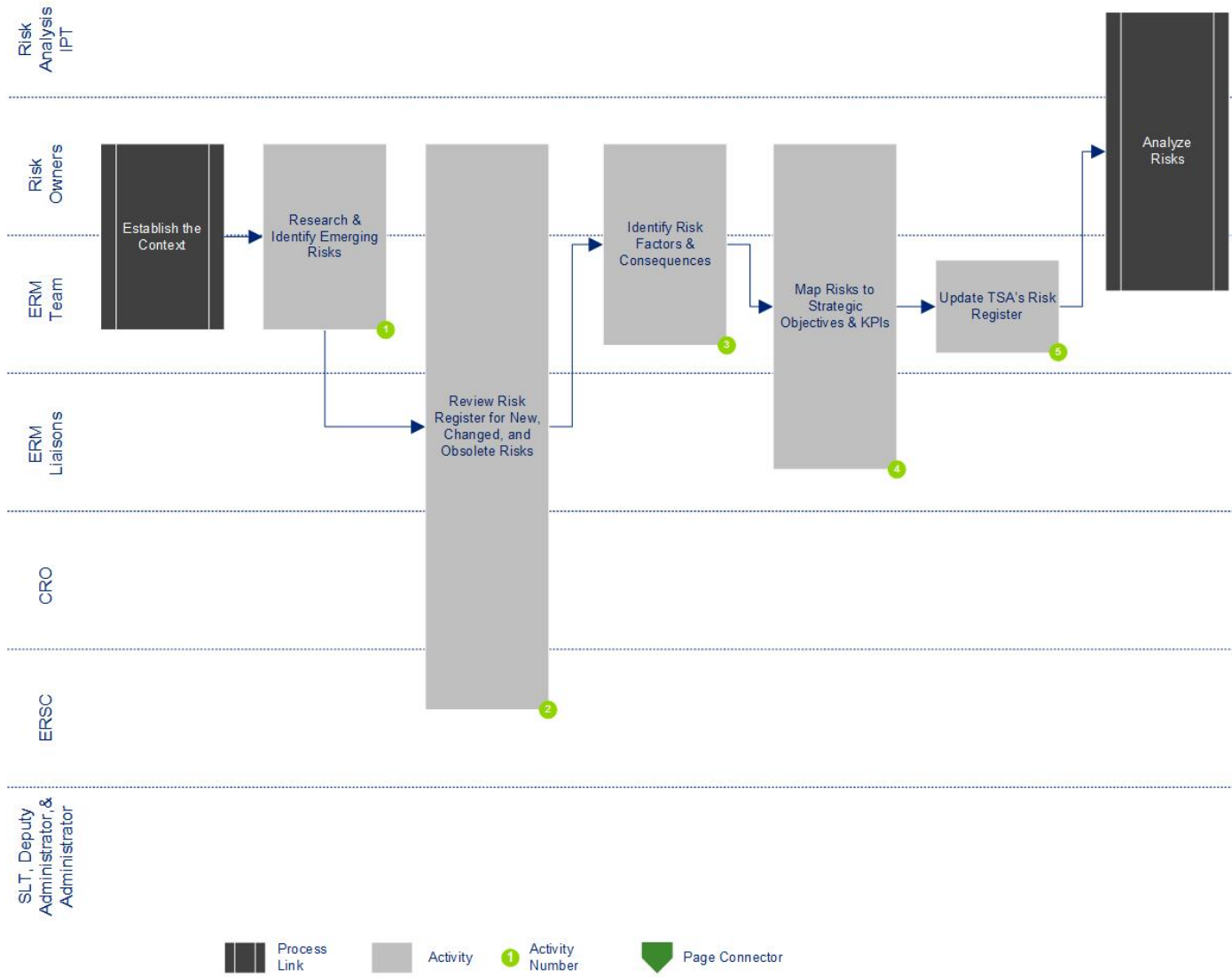
1. Research and identify emerging risks (ERM Team and Risk Owners). Perform scenario analysis exercises periodically, and review the major risks associated with existing Key Performance Indicators (KPIs) or other performance metrics associated with achieving mission success. Review the scenario analyses from similar organizations (e.g., other Federal agencies in the transportation sector, international transportation authorities) if available, as well as companies in the transportation industry.
2. Review the Risk Register for new, changed, and obsolete risks (ERSC, CRO, ERM Team, ERM Liaisons, Risk Owners). Review risk taxonomy to identify risk types on which to focus the risk identification and review activities. Risk Owners will perform this process for their Program Office or Division, and the ERM Team will perform this at the AA Program Office level. Conduct cross-functional workshops to further identify which risks are new, changed, or obsolete in terms of their impact or likelihood.
3. Identify risk factors and consequences (ERM Team and Risk Owners). Develop preliminary lists of risk factors and consequences. Assist TSA's ERM Team with identifying the Risk Owner for new risks and confirm the Risk Owner for changed risks. Assist with the identification of staff that will be able to identify and quantify the risk factors and consequences. If the risk is determined to be high enough to be elevated to the TSA's Risk Register, then this initial list of risk factors and consequences will be used as the starting point for an expert panel to build out event trees.
4. Map risks to strategic objectives, KPIs, and processes (ERM Team, ERM Liaisons, Risk Owners). Specify the strategic objective to which the risk applies. Identify and capture the KPIs used to measure the risk. These should be drawn from existing KPIs specified as part of the performance goals. If new KPIs are identified during the risk management process, then these should be communicated to the affected staff for incorporation into process documentation and departmental objectives and performance measures. Specify the risk tolerance for each KPI. The risk tolerance can be expressed as a threshold that is not to be breached or as an acceptable band depending on the particular KPI in question.
5. Update TSA's Risk Register (ERM Team). Update the information in TSA's Risk Register for existing risks. Add new risks and preliminary information to be elaborated and validated during the risk evaluation. Delete obsolete risks and document the reason. Map each risk to the operational activities or processes it resides in.

## Outputs

- KPIs and risk tolerance thresholds
- Updated and new mappings to operational activities or processes
- Updated Risk Owners
- Updated TSA's Enterprise Risk Register



Figure 3: Identify risks flow diagram





## Analyze Risks

### Overview

The *Analyze Risks* process involves consideration of the causes and sources of risk, the probability that the risk event will occur, their positive or negative consequences and magnitude, and the likelihood that those consequences may occur. Risk analysis provides the basis for evaluation and decisions regarding risk response or treatment. Each risk identified during the *Identify Risks* process is subjected to a qualitative evaluation of its likelihood and impacts. The list of risks is then narrowed and refined based on the criticality of the risk. Those risks falling below a defined threshold may continue to be monitored and managed within TSA, but will not be reported at the executive level as part of the Enterprise Risk Register.

After the initial screening using qualitative techniques, a determination will be made regarding how accurate the estimates of likelihood and impact are for prioritizing, measuring, and reporting the risk and to select the appropriate risk response options. Risk assessment techniques range along a spectrum. Qualitative risk assessment techniques use scales representing ranges of likelihood and impact, more quantitative techniques may include what-if scenario analyses using complex quantitative models. Initially, TSA will rely more heavily on qualitative assessments until quantitative measures are developed and implemented. TSA's risk assessment tools and techniques will evolve over time, and as the ERM program matures a shift to more quantitative analysis is expected. The assessment scales used to qualitatively assess the risks are in contained in Attachment A.

### Objectives

To estimate the magnitude of the likelihood and impact of risks using qualitative and deterministic quantitative methods while laying the foundation for future quantitative risk modeling.

### Triggers

- Completion of *Identify Risks*
- Occurrence of a risk event(s)
- The publication of a risk assessment by internal or external stakeholders supporting different conclusions regarding the likelihood or impact of a risk or the effectiveness of existing controls
- To be performed annually or more often if events warrant as specified in the triggers for *Establish the Context*.

### Inputs

- Qualitative assessment scales
- Advanced risk modeling testing results, if applicable
- Internal and external audit reports
- Internal and external data and information sources (e.g., TSA-RK Center)



- Stakeholder input
- Updated TSA Risk Register

### Process Participants

- ERM Team
- ERM Liaisons
- Risk Analysis IPTs
- Risk Owners

### Activities

1. Facilitate qualitative assessment and assign risk ratings (ERM Team, Risk Analysis IPTs, Risk Owners). For risks that have causal links or impacts that affect more than one Program Office, it is likely that the staff best qualified to estimate likelihood and impact will come from multiple Program Offices. In this case, solicit the assistance of the ERSC members if necessary, to assist with securing resources across TSA, and build the appropriate reporting relationships.
2. Aggregate and prioritize risks (ERM Team). Assign a rating of severity and likelihood to each risk and record the risk rating in the Risk Register. Assess all risks with risk ratings of high severity and high likelihood at TSA's level and prioritize the risks for various types of analysis. For visualization purposes, risks may be plotted on a heat map based on the defined impact and likelihood scales for TSA.
3. Develop or update event trees (Risk Analysis IPTs and Risk Owners). Identify risk analysis IPTs of individuals intimately familiar with the select risk to develop causal chains of events that could lead to the risk. Organize these as "triggering events" that lead to secondary risk factors ultimately leading to the risk event. Identify the chains of impacts resulting from the risk occurrence and link secondary impacts to primary impacts. For existing event trees, reconvene with the appropriate expert staff to identify if the risk factors and impacts shown still apply.
4. Facilitate event tree development and updates (ERM Team). Provide training on how to develop event trees as required. Provide assistance with facilitating expert panel sessions if requested. Review the likelihood and impact data for reasonableness and alert the Risk Owners and Risk Analysis Team of any potential issues. Assist the Risk Owner and Risk Analysis IPT with identifying Key Risk Indicators (KRIs).
5. Quantify selected risks (ERM Team, Risk Owners, ERM Liaisons). For each causal chain of risk factors in a new event tree, estimate the annual frequency of the trigger event, the probability that the second risk factor will occur if the trigger occurs, and the severity of the loss should the second risk factor occur. For each impact, estimate the probability of occurrence.
6. Develop TSA's risk portfolio (ERM Team). After all the risk factors and consequences have been quantified, calculate various risk measures to express all risks as an enterprise-wide risk measure such as "percent of budget at risk" or "percent of security effectiveness at risk."

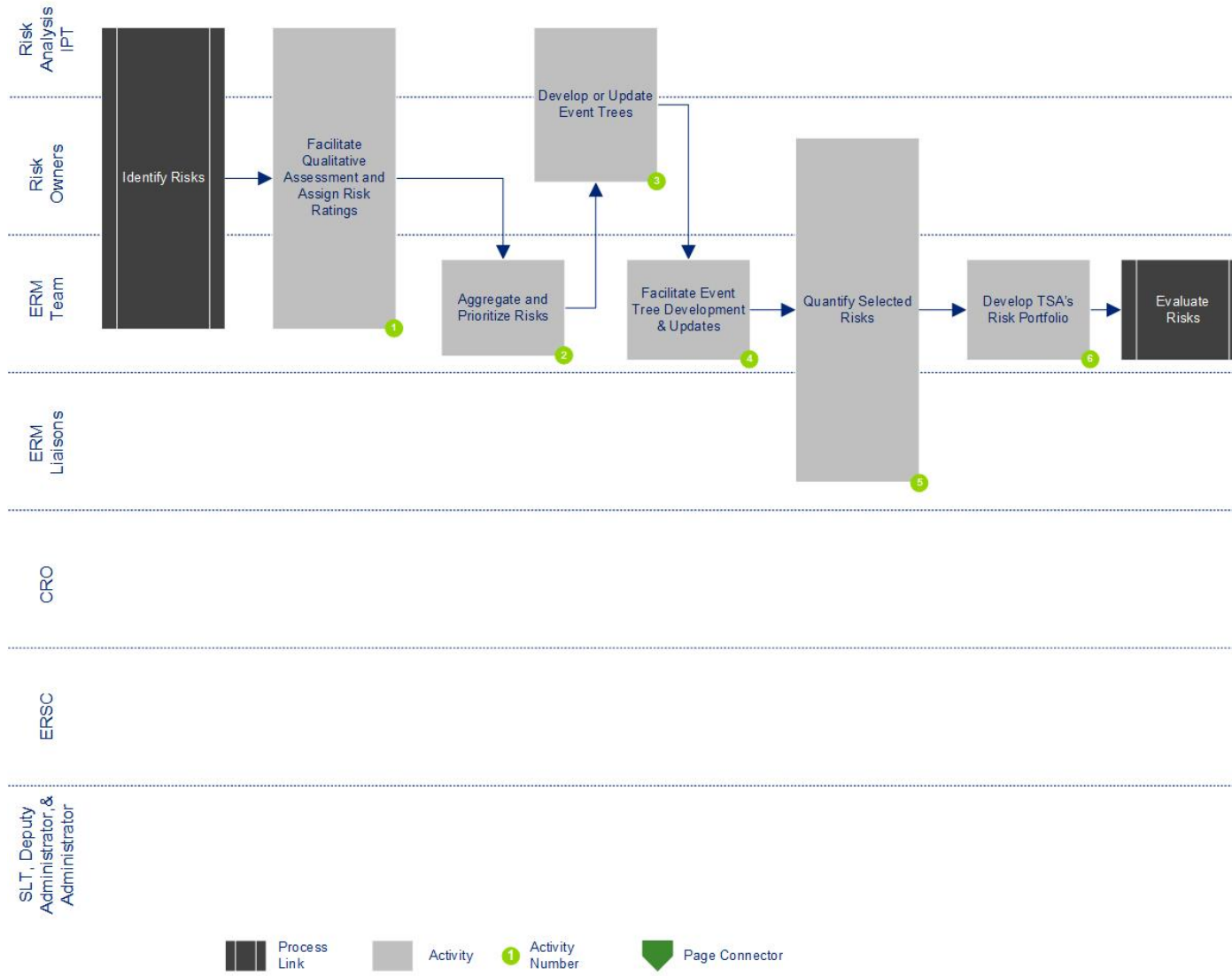


## Outputs

- Enterprise-wide risk measures for the TSA's complete portfolio of risks
- Event trees analysis
- Identified relationships between risks
- KRIs
- Qualitative and quantitative analysis
- Updated TSA Risk Map and Risk Register



Figure 4: Analyze risks flow diagram







## Evaluate Risks

### Overview

The *Evaluate Risks* process uses the qualitative risk analysis generated in the preceding *Analyze Risk* process to rank and prioritize enterprise level risks. The focus of ERM is not to try and identify and analyze every risk facing TSA, but to identify those risks that rise to the enterprise-wide level. By prioritizing the enterprise-level risks, TSA leadership can respond as appropriate with strategic allocation of resources in the *Respond to Risks* process. Usually, risk managers find that responding to a few critical risks results in dramatic reductions in residual risk. At this stage, TSA leadership should have more enterprise-wide quantitative information regarding risks from across the organization that may not have been available earlier during the *Establish the Context* or *Identify Risks* processes. During *Evaluate Risks*, TSA leadership should revisit the documented risk tolerances in light of their overall risk portfolio and make adjustments.

### Objectives

To develop a prioritized list of enterprise-level risks for response options.

### Triggers

- Completion of *Analyze Risks*
- To be performed annually or more often if events warrant (as specified in the triggers for *Establish the Context*)

### Process Participants

- ERSC
- ERM Team
- ERM Liaisons
- Risk Analysis IPTs
- Risk Owners

### Inputs

- Analysis of risk response and controls effectiveness
- Calculated enterprise-wide risk measures for the TSA's complete portfolio of risks
- Event trees analysis
- Identified relationships and correlations between risks
- KRIs and KPIs
- Qualitative and quantitative analysis
- Risk tolerance thresholds
- Stakeholder Input
- Updated TSA Risk Map and Risk Register



## Activities

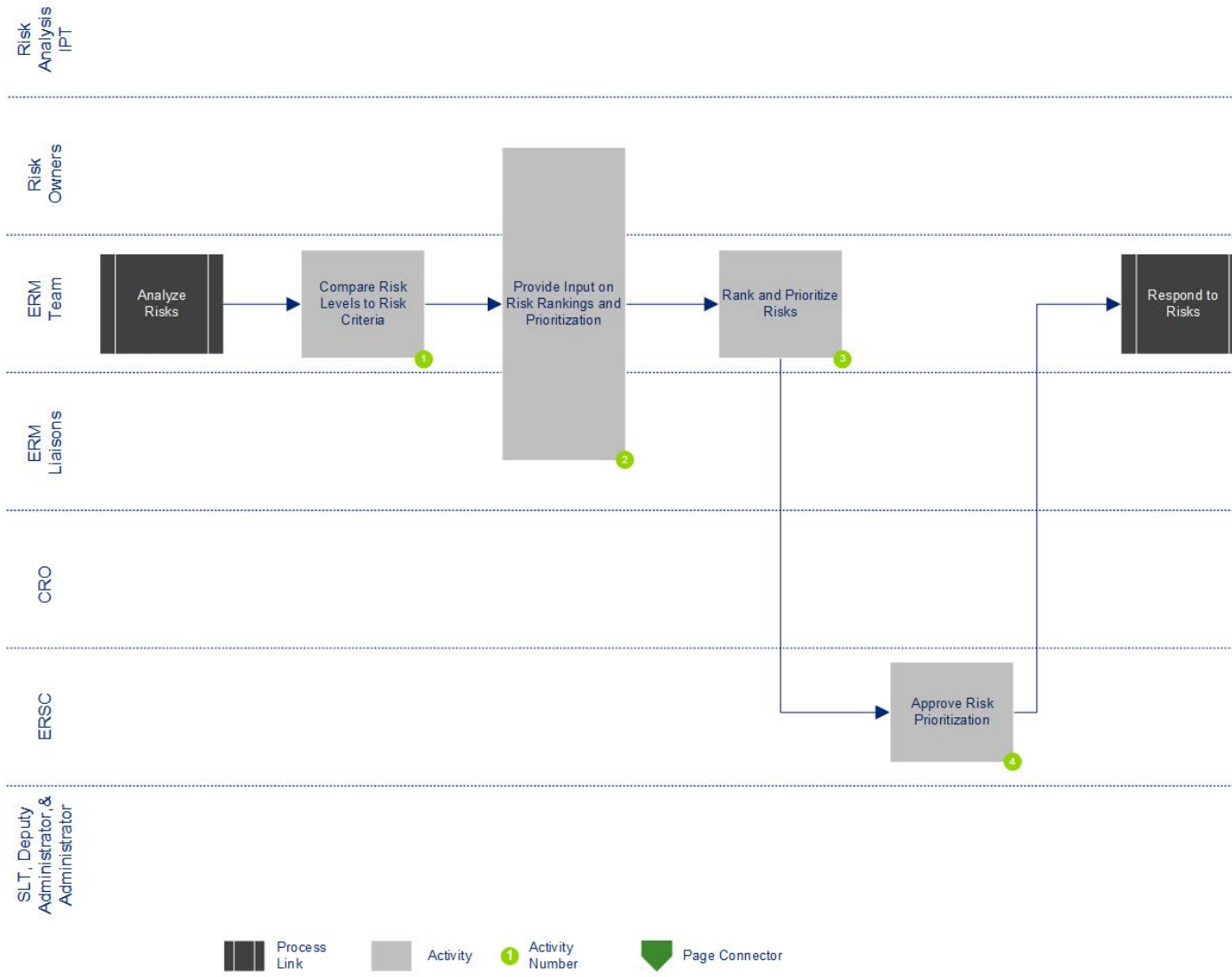
1. Compare risk levels to risk criteria (ERM Team). For each risk factor, risks, and risk consequence identified, compare the calculated risk measures to the risk tolerance thresholds defined as part of the *Identify Risks* process.
2. Provide input on risk rankings and prioritization (Risk Owners, ERM Team, ERM Liaisons). Provide any additional required input on qualitative impacts, mission objectives, risk tolerance, or threshold criteria, and any other considerations that would impact the relative ranking and prioritization of risks for response options. Review event trees and risk correlations in order to understand the interrelated nature of risks and how they might impact risk prioritization.
3. Rank and prioritize risks (ERM Team). Prioritize TSA's risks for risk response options. Involve Risk Owners and Program Office Staff responsible for managing the risks. Review event trees and risk correlations to prepare a report on the ranked list of risks and the approach and rationale used to rank the risks and present it to the ERSC for endorsement. Update information about TSA's risks and enter their rankings in the Enterprise Risk Register.
4. Approve risk prioritization (ERSC). Review the report on the ranked list of risks that will be considered for risk response options. Offer guidance on any pending management decisions, planned projects, changes to strategic direction, or other factors that might impact the ranking of the risks. Request and review changes from the ERM Team, and vote to endorse the ranked list prior to presenting it to the SLT, Administrator, or Deputy Administrator for approval.

## Outputs

- Prioritized list of quantified risks requiring response options
- Stakeholder Input
- Updated TSA Risk Register



Figure 5: Evaluate risks flow diagram





## Respond to Risks

### Overview

The *Respond to Risks* process involves identifying and assessing the range of risk response options and preparing implementation plans for selected response options. Responding to risks includes both the seizing of opportunities to achieve mission success as well as efforts to minimize the adverse impacts of risk. Using a prioritized list of quantified risks requiring response options from the *Evaluate Risks* process, TSA leadership can make informed strategic decisions about how to allocate resources to programs and projects reflected in the enterprise risk register.

### Objectives

To select a combination of risk response options that will optimize TSA's limited resources in managing its portfolio of risks within the bounds of a predefined risk appetite.

### Triggers

- Completion of *Evaluate Risks*
- To be performed annually or more often if events warrant (as specified in the triggers for *Establish the Context*)

### Inputs

- Analysis of previous and current risk response strategy effectiveness
- Existing crisis management plans (this should include crisis management plans as mandated by DHS)
- Previous communication and training plans
- Prioritized list of risks requiring response options
- Relevant laws and regulations
- Stakeholder analysis

### Process participants

- CRO
- ERSC
- ERM Liaisons
- Risk Analysis IPTs
- Risk Owners

### Activities

1. Identify risk response options (Risk Owners and Risk Analysis IPTs). Review event trees for those risks listed in the prioritized list of risks requiring response options and identify risk factors that can be mitigated or eliminated to reduce likelihood and severity. Identify consequences that can be mitigated or avoided to reduce likelihood and impact and



review existing risk response strategies and controls and insurance policies and analyze their effectiveness. Pinpoint any projects in progress that will impact the existence, likelihood, or magnitude of the risk and observe the project timeline to determine when the risk will be impacted. Document all identified response options for those risk factors and consequences selected.

2. Coordinate risk response option identification (ERM Team). Provide Risk Owners with information about existing risk response options. Assist them in identifying cost-effective options including opportunities to extend current risk management activities. Identify opportunities to leverage risk response across Program Offices to optimize risk management efforts and eliminate any duplicative efforts.
3. Assess risk response options (Risk Owners). Determine the cost of implementing the identified risk response options and evaluate the qualitative impacts that would be reduced or eliminated by the various risk response options using the qualitative impact scales. Compare the residual risk calculation to the risk tolerance level. If the residual risk still exceeds the risk tolerance level, then consider additional risk response options until the estimated residual risk is reduced below the risk tolerance level. Select the most cost-effective combination of risk response options that reduces the estimated risk to an acceptable level below TSA’s risk tolerance. Additionally, review the risk response options for compliance with relevant laws and regulations.

Figure 6: Risk response strategies to consider

<b>Avoid risk</b>	<p><b>Discontinue</b> operations or activities in a particular area.</p> <p><b>Prohibit</b> unacceptably high-risk activities and asset exposures through appropriate policies.</p> <p><b>Stop</b> specific activities by redefining objectives, refocusing strategic plans and policies, or redirecting resources.</p> <p><b>Screen</b> alternative projects and budgeted investments to avoid off-strategy and unacceptably high-risk initiatives.</p> <p><b>Eliminate</b> at the source by designing and implementing internal preventive processes.</p>
<b>Accept risk</b>	<p><b>Retain</b> risk at its present level, taking no further action.</p>
<b>Reduce risk</b>	<p><b>Disperse</b> financial, physical, or information assets to reduce risk of unacceptable catastrophic losses.</p> <p><b>Control</b> risk through internal processes or actions that reduce the likelihood of undesirable events occurring to an acceptable level (as defined by management’s risk tolerance).</p> <p><b>Respond</b> to well-defined contingencies by documenting an effective plan and empowering appropriate personnel to make decisions; periodically test and, if necessary, execute the plan.</p> <p><b>Diminish</b> the magnitude of the activity that drives the risk.</p> <p><b>Isolate</b> differentiating characteristics of proprietary assets to reduce risk of loss through imitation, obsolescence, or other competitive pressures.</p> <p><b>Test</b> strategies and implemented measures on a limited basis to evaluate results</p>



	<p>under conditions that will not influence perceptions of the broader traveling public.</p> <p><b>Improve</b> capabilities to manage a desired exposure.</p> <p><b>Relocate</b> operations in order to transfer risk from one location, in which it cannot be well managed, to another location in which it can.</p> <p><b>Redesign</b> the TSA’s approach to managing the risk (i.e., its unique combination of assets and technologies for creating opportunities to achieve mission success).</p> <p><b>Diversify</b> organizational assets that TSA currently implements for mission and business operations.</p>
<b>Transfer risk</b>	<p><b>Outsource</b> non-core processes (a viable risk transfer option only when risk is contractually transferred).</p> <p><b>Delegate</b> risk by entering into arrangements with independent, capable authorities.</p>

4. Review risk response options with stakeholders (ERM Team and ERM Liaisons). Develop an overall risk response strategy. Consult broadly about risk response with stakeholders. Many response options need to be acceptable to stakeholders or those involved in implementation if they are to be effective and sustainable. Present the risk response options, their costs and benefits, and the recommended risk response strategy to the ERSC for their review and approval.
5. Approve risk response options (CRO and ERSC). Review proposed risk response strategy and selected risk response options and cost-benefit analysis submitted by the ERM Team. Provide comments and feedback to the ERM Team. Obtain permission from the SLT, Administrator, or Deputy Administrator to secure funding and resources to implement the risk response plans as necessary. In some instances, TSA may need to obtain permission of DHS, OMB, or Congress in order to secure or re-align funding.
6. Prepare risk response option plans (Risk Owners). Develop a detailed risk response action plan including the person responsible for implementing the risk response options, the primary activities, required resources, schedule, budget, reviewer, and status.
7. Implement risk response plans (Risk Owners). The Risk Owners will be responsible for working with the Chief Financial Officer (CFO) to secure the budget to implement the risk response plan. Once budget is secured, Risk Owners begin implementation of the risk response and report progress to the reviewer and other identified stakeholders.
8. Monitor risk response option plan implementation (ERM Team). Update information regarding the risk factors and impacts of the risks including annual frequencies, probabilities, impacts, and existing response strategies and controls in the Risk Register. Monitor the status of risk response plans against agreed milestones as recorded. Alert responsible party if deadlines are likely to be or have been missed. Determine and implement corrective action such as reassigning work, identifying additional resources to assist with the activity, or communicating with the appropriate individuals to reassign work. See *Appendix 1: Risk monitoring and reporting templates* for examples of reports that can be used to report on the status of risk response plan implementation.
9. Enforce implementation deadlines (ERSC). Take corrective action to resolve issues, remove implementation barriers, or address missed deadlines. Set the expectation that deadlines will be met and expected residual risk levels will be achieved.
10. Assess risk response effectiveness (CRO, ERM Team, ERM Liaisons). Assess whether the reduced probabilities or impacts or other expected benefits have been realized. Make



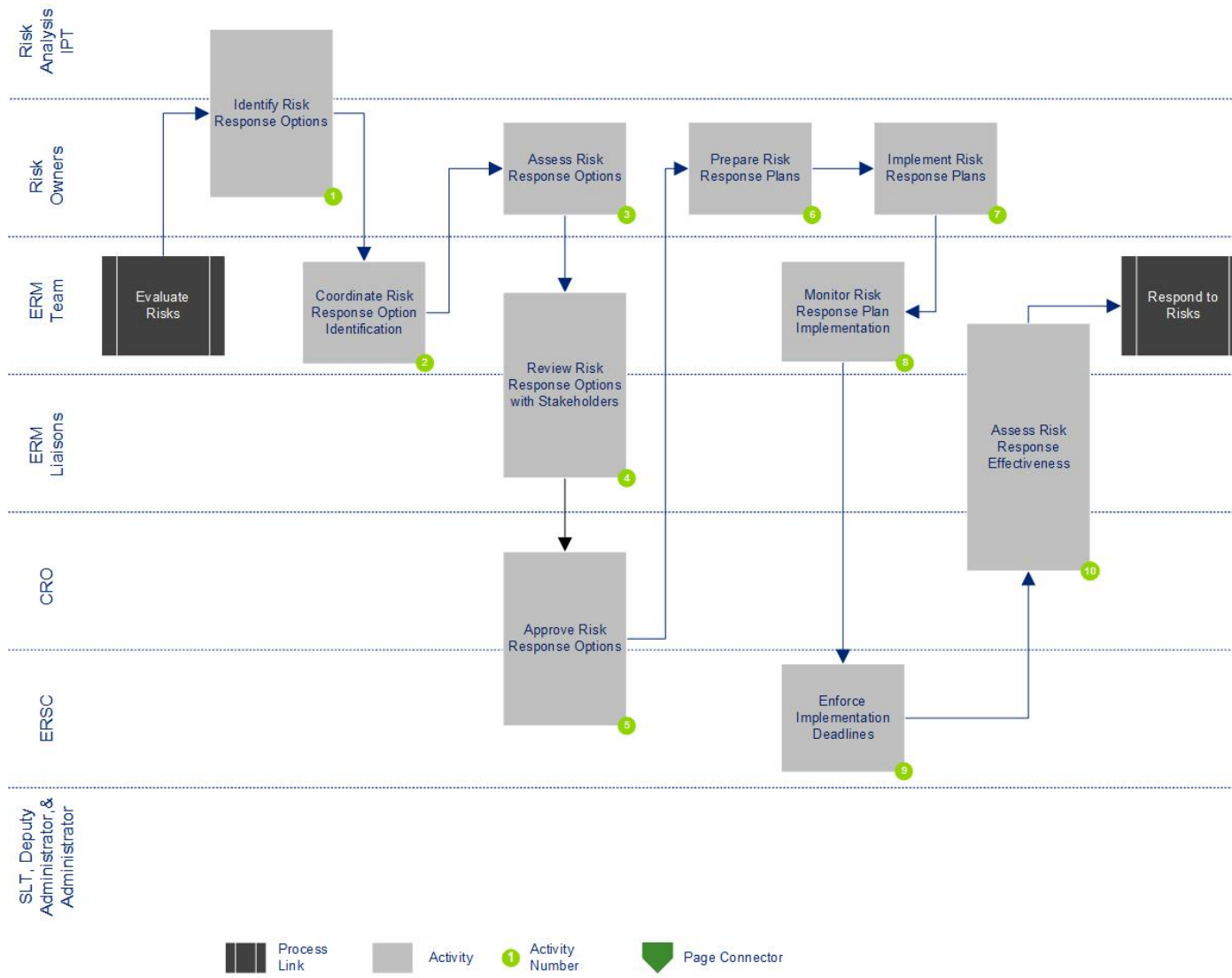
adjustments to the event tree as necessary to reflect actual conditions. Compare the expected benefits and costs of risk response to the actual benefits and costs. Calculate the residual risk and compare it to the risk tolerance levels to determine if additional risk responses will be necessary. Determine the timeline for any additional risk response plans.

### **Outputs**

- Risk response strategies and plans which include the analyzed costs and timelines for development and implementation
- Updated Risk Register with quantified residual risks



Figure 7: Respond to risks flow diagram







## **Monitor and Review**

### **Overview**

The *Monitor and Review* process involves ongoing review of risks to ensure that risk management efforts and response strategies remain relevant and effective. Factors that may affect the likelihood and consequences of an outcome may change over time, as may the factors that affect the suitability or cost of the selected response options. It is therefore necessary to repeat the risk management cycle regularly. Actual progress against risk response option plans provides an important performance measure and should be incorporated into the TSA's performance management and reporting processes. *Monitor and Review* also involves benchmarking actual ERM risk management outcomes against expected or required performance levels.

### **Objectives**

To continuously monitor the progress of risk response strategies and anticipate and respond to risk events as they occur. Improve TSA's risk management capabilities, ensure the performance of risk management activities, monitor the progress of risk response strategies, and anticipate and respond to risk events as they occur.

### **Triggers**

- Predetermined timelines for activities as maintained in the risk management calendar
- Occurrence of major risk events or risk factor triggers

### **Inputs**

- KPIs, KRIs, and risk tolerance thresholds
- Risk response strategies and plans which include the analyzed costs and timelines for development and implementation
- Stakeholder input
- Updated ERM Policy, risk appetite statements, roles and responsibilities, organizational structure charts, and ERSC Charter
- Updated Risk Register with quantified residual risks

### **Process participants**

- ERSC
- CRO
- ERM Team
- ERM Liaisons
- Risk Owners



## Activities

1. Develop risk monitoring plans (Risk Owners and ERM Team). Develop a risk monitoring plan listing each KRI and KPI. Identify individuals responsible for monitoring the indicators, the associated threshold values, the timing for the monitoring, the required actions should the KRI or KPI breach the threshold, and required alerts and notifications in the event of a breach. Design risk monitoring and reporting templates for internal use and to be provided to a pre-determined audience. The ERM Team will assist in identifying KRIs and KPIs mapped to multiple risks and resolving any issues around the span of control and monitoring responsibilities. See *Appendix 1: Risk monitoring and reporting templates* for examples of monitoring dashboards and reports.
2. Monitor KRIs and respond to changes in risks (Risk Owners). Monitor whether the defined thresholds are breached, or if there has been a change in the indicator signaling a trend, whereby the thresholds might be breached or a risk event might occur. Communicate any breaches or trends requiring corrective action, and take or direct corrective action as appropriate.
3. Coordinate communications and responses to changes in risks (ERM Team). In the event of a KRI or KPI threshold breach or change, determine if the probability of a risk event occurrence has changed that warrants further analysis. Depending on the circumstances, it may be necessary to trigger another process such as *Establish the Context*. Assist the Risk Owners by identifying the broader impacts of a KRI or KPI threshold breach.
4. Record and analyze risk events (Risk Owners, ERM Team, ERM Liaisons). Record any risk events or near misses to the risk event occurring. Include a description of the event, person responsible for tracking and analysis, the risk category and root cause. Analyze data to identify trends events that could indicate a need for a broader analysis and corrective action beyond the individual risk event in question. The ERM Team will assist in documenting and analyzing risk events and near misses, as well as determining what, if any, corrective action needs to be taken.
5. Review risk event analysis and enforce corrective action (ERSC). For significant risk events related to TSA's risks, review the risk event analysis paying particular attention to the root cause and timing. Review proposed corrective action and provide input and guidance. The ERSC will perform these steps and inform the Administrator should major risk events occur.
6. Prepare scheduled and ad hoc reports (Risk Owners and ERM Team). Prepare daily, weekly, monthly, quarterly, and annual risk reports. Distribute reports to agreed audience groups according to the agreed schedule. Prepare ad hoc reports for TSA leadership or Risk Owners upon request.
7. Review and respond to reports (ERSC). Review scheduled and ad hoc risk reports. Note any items requiring corrective action such as risk tolerance or limit breaches, or risk events or near misses. Note changes in the overall enterprise risk profile, in underlying risk types, their root causes, and any trends in changes to risks. Determine if corrective action needs to be taken, the affected parties, and what communications outside of regular channels might be required. Endorse corrective actions and assist in identifying and deploying cross-Program Office resources to investigate risk events or sudden changes or developing trends.

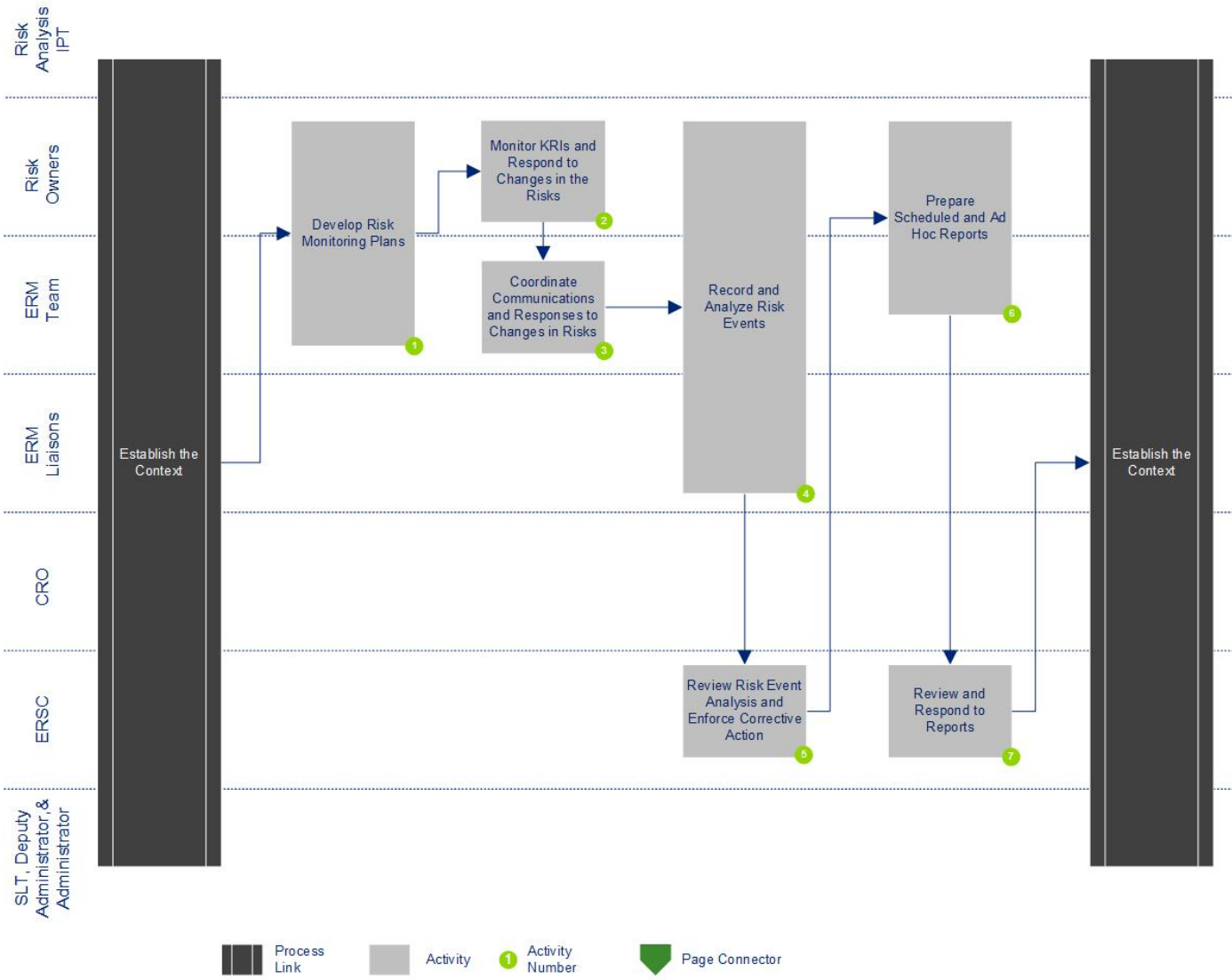


## Outputs

- Analysis of ERM program effectiveness
- Analysis of the effectiveness of risk response strategies and plans
- Analysis, documentation, and escalation of major risk events
- Changes and enhancements to risk management processes and systems
- ERM Program calendar
- Identified communication and training needs
- Information on major changes in external or internal environment affecting strategic objectives or risk profile
- KRI breaches and risk events
- Scheduled and ad hoc risk reports



Figure 8: Monitor and review risks flow diagram





## **Communicate and Consult**

### **Overview**

*Communication and Consultation* are intrinsic to the risk management process and should be considered at each step. An important aspect of the *Establish the Context* process is to identify stakeholders and seek and consider their needs. A communications plan can then be developed to specify the purpose or goal for particular communication needs, identify who is to be consulted and by whom, when communication will take place, how the process will occur, and how it will be evaluated. Within TSA, clear communication channels will be essential in fully integrating all Program Offices in risk management and in developing a culture where the positive and negative dimensions of risk are recognized and valued.

### **Objectives**

To improve understanding of risks and the risk management process, ensure that the varied views of stakeholders are considered and build awareness among participants of their active risk management roles and responsibilities.

### **Triggers**

- Annual stakeholder review to be performed each July
- Major change in organizational structure such as a new Program Office formed
- New requirements, laws, and regulations which TSA must adhere to
- Occurrence of a major risk event

### **Inputs**

- Calculated enterprise-wide risk measures for the TSA's complete portfolio of risks
- Changes and enhancements to risk management processes and systems
- ERM staff and other personnel training needs
- Prioritized list of quantified risks, residual risks, and their interdependencies
- Risk response strategies and plans
- Update Risk Owners
- Updated ERM Policy, risk appetite statements, roles and responsibilities, organizational structure charts, and ERSC Charter
- Updated Risk Register

### **Process participants**

- ERM Team
- ERM Liaisons
- Risk Owners



## Activities

1. Manage risk management workflow and schedule (ERM Team). Maintain a calendar of risk management activities for the year beginning with the *Establish the Context* process. Agree on an ERM calendar to communicate schedules, milestones, and expectations of the program. The calendar will need to be updated at defined intervals as the scope of work is elaborated with TSA's developing ERM capabilities.
2. Enhance ERM capabilities (ERM Team). Monitor emerging risk management best practices by subscribing to publications, joining consortia and dedicated industry groups, attending conferences, and consulting with other risk professionals at other organizations. Evaluate the effectiveness of existing risk management processes, tools, and techniques. Develop recommendations for enhancements to TSA's risk management capabilities. Involve the Risk Owners within TSA and present the recommendations for approval from the SLT, Administrator, or Deputy Administrator as necessary.
3. Approve ERM capability enhancements (ERSC). Review the proposed risk management capability improvements understanding the benefits and costs. Resolve issues related to performance of the risk management processes raised by the ERM Team.
4. Identify stakeholders, communication, and training needs (ERM Team and ERM Liaisons). Review stakeholder analysis from the previous year and determine if the stakeholder groups have changed. Include both internal and external stakeholders to determine the communication and training needs for each stakeholder group.
5. Provide input on stakeholders, communication, and training needs (Risk Owners). Assist the ERM Team in identifying relevant stakeholders and their communication and training needs. Assist in the development of communication and training content as required. Communicate training needs to the ERM Team and participate in training programs if requested.
6. Develop and deliver communication and training (ERM Team). Develop a detailed communication and detailed training plan including the target audience, the sender, the timing, the communication channel (e-mail, newsletter, meeting, webcast, etc.), the message, and responsibilities for developing and managing the delivery of the content. Develop and deliver the communication and training materials according to plans.
7. Deliver reinforcing messages (ERSC). Review, provide input on, and deliver messages prepared by the ERM Teams. Request endorsing messages from the Administrator as necessary. The purpose is to demonstrate leadership sponsorship for ERM and to promote ERM objectives and benefits to achieving mission success.
8. Maintain ERM iShare site and process documentation (ERM Team). Maintain the TSA ERM website. Designate an individual within the ERM Team as the website coordinator. The website coordinator will gather the required content and provide periodic updates to the website.

## Outputs

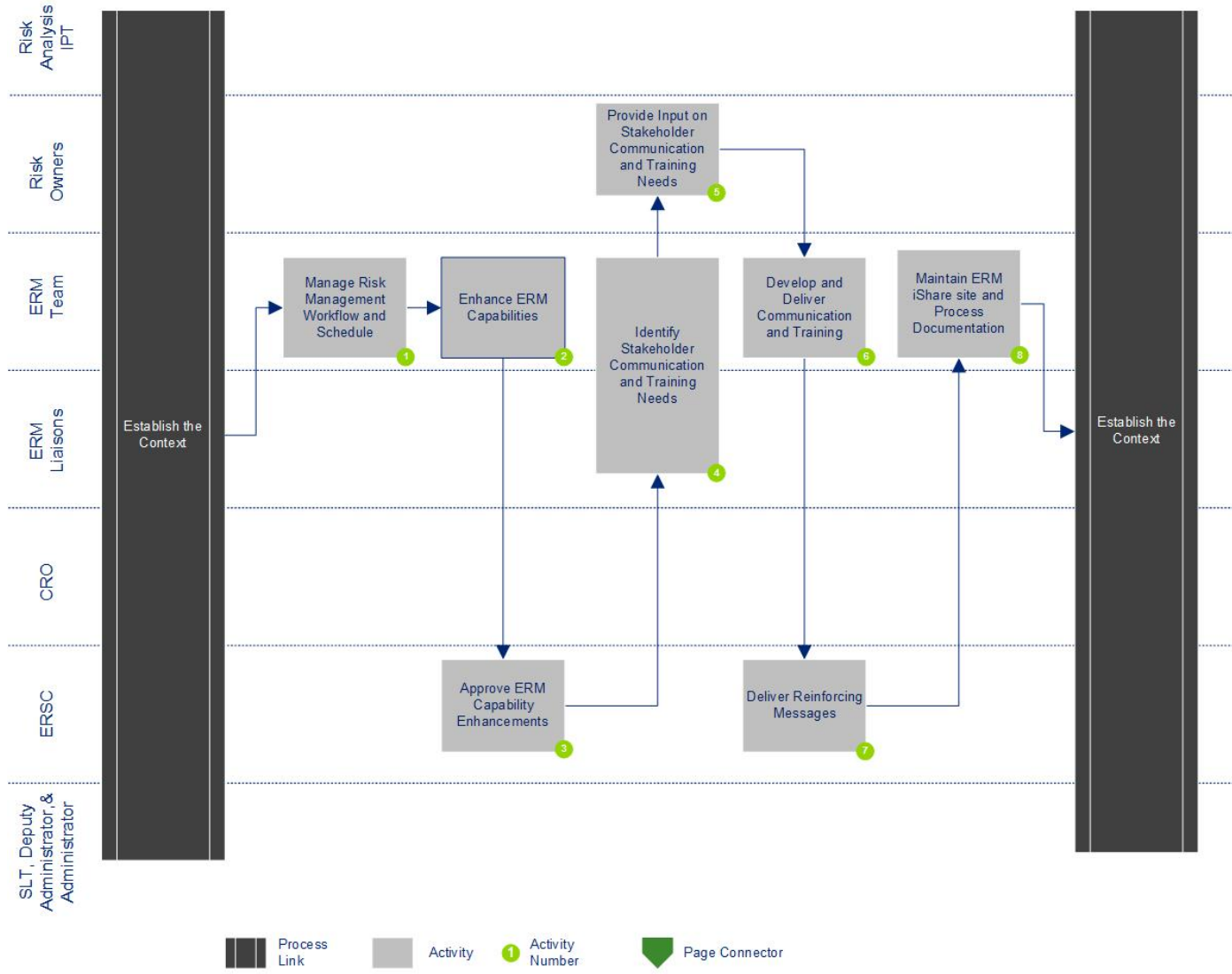
- Changes and enhancements to risk management processes and systems and ERM organizational structure
- Communication and training plans
- ERM website development via the TSA Intranet



- Stakeholder analyses and stakeholder inputs
- Trainings and communications delivered to the appropriate stakeholders



Figure 9: Communicate and consult risks flow diagram







## Appendix 1: Risk assessment scales -notional

Figure 10: Impact/consequence Scale

Descriptor	Description
<b>Very High</b>	Event could be expected to have catastrophic adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
<b>High</b>	Event could be expected to have a severe adverse effect on organization operations, organizational assets, individuals, other organizations, or the Nation. A severe or catastrophic adverse effect means that the event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions for a significant period of time; (ii) severely undermine the ability to perform one or more of the primary functions for a significant period of time; (iii) result in major damage to organizational, critical infrastructure, or national security assets; (iv) result in major financial loss; or (v) result in severe harm to individuals exceeding mission expectations.
<b>Moderate</b>	Event could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A serious adverse effect means that the event might: (i) cause a significant degradation in or loss of mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of those functions is significantly reduced; (ii) result in significant damage to organizational, critical infrastructure, or national security assets; (iii) result in major financial loss; or (iv) result in significant harm to individuals exceeding mission expectations.
<b>Low</b>	Event could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. Limited adverse effect means that the event might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of those functions is noticeably reduced; (ii) result in minor damage to organizational, critical infrastructure, or national security assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
<b>Very Low</b>	Event could be expected to have a negligible adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

Source: Adapted from U.S. Department of Homeland Security (DHS) *National Security Systems Policy Standard Number: 4300B.103-2*, 2013, p. 49.



Figure 11: Impact/Consequence Scale Application Examples

Descriptor	Application
<p><b>Very High</b></p>	<ul style="list-style-type: none"> <li>• Security event valued at greater than or equal to \$1B in direct costs or \$XB in indirect costs<sup>1</sup></li> <li>• Cost impact greater than or equal to 15% of TSA’s budget</li> <li>• 40% of key leadership or mission critical staff are unavailable for duty</li> <li>• Complete degradation of the confidentiality, integrity, or availability of mission critical system(s)</li> <li>• Complete inability to maintain continuity of operations at mission-critical location(s) or function(s)</li> </ul>
<p><b>High</b></p>	<ul style="list-style-type: none"> <li>• Security event valued at greater than or equal to \$800M up to \$1B in direct costs or \$XB up to \$XB in indirect costs<sup>1</sup></li> <li>• Cost impact greater than or equal to 10% up to 15% of TSA’s budget</li> <li>• 20% - 40% of key leadership or mission critical staff are unavailable for duty</li> <li>• Severely compromised confidentiality, integrity, or availability of mission critical system(s)</li> <li>• Severely compromised ability to maintain continuity of operations at mission-critical location(s) or function(s)</li> </ul>
<p><b>Moderate</b></p>	<ul style="list-style-type: none"> <li>• Security event valued at greater than or equal to \$400M up to \$800M in direct costs or \$XB up to \$XB in indirect costs<sup>1</sup></li> <li>• Cost impact greater than or equal to 5% up to 10% of TSA’s budget</li> <li>• 15% increase in staff turnover or low staff morale</li> <li>• Disrupted confidentiality, integrity, or availability of mission critical system(s)</li> <li>• Disrupted ability to maintain continuity of operations at mission-critical location(s) or function(s)</li> </ul>
<p><b>Low</b></p>	<ul style="list-style-type: none"> <li>• Security event valued at greater than or equal to \$100M up to \$400M in direct costs or \$XB up to \$XB in indirect costs<sup>1</sup></li> <li>• Cost impact greater than or equal to 1% up to 5% of TSA’s budget</li> <li>• 5% increase in staff turnover or general staff morale problems</li> <li>• Minimal degradation to the confidentiality, integrity, or availability of mission critical system(s)</li> <li>• Minor disruptions to continuity of operations at non-mission-critical location(s) or function(s)</li> </ul>
<p><b>Very Low</b></p>	<ul style="list-style-type: none"> <li>• Security event valued at less than \$100M in direct costs or \$XB up to \$XB in indirect costs<sup>1</sup></li> <li>• Cost impact less than 1% of TSA’s budget</li> <li>• Negligible or isolated staff dissatisfaction</li> <li>• Little to no degradation to the confidentiality, integrity, or availability of mission critical system(s)</li> <li>• Minimally disrupted ability to maintain continuity of operations at non-mission-critical location(s) or function(s)</li> </ul>

<sup>1</sup>Direct costs include immediate economic damage and loss of life and injuries, and indirect costs include aggregated secondary macro- and micro-economic impacts.



Figure 12: Probability/likelihood scale

Qualitative values	Best estimate
Certain	.99
Almost Certain	.93
Probable	.75
Chances About Even	.5
Probably Not	.25
Almost Certainly Not	.07
Impossible	.01

Source: U.S. Department of Homeland Security (DHS) *Transportation Sector Security Risk Assessment (TSSRA)*, 2013, p. 49.



Figure 13: Vulnerability scale

Qualitative values	Description
Very High	<ul style="list-style-type: none"> <li>•Countermeasure effectiveness is very low (e.g., vulnerability estimate of .93)</li> <li>•Controls, policies, and procedures are ineffective or insufficient</li> <li>•Resources and tools are unavailable or do not meet mission-critical needs</li> <li>•No contingency, crisis management plans, or scenario plans in place</li> <li>•One or more major weaknesses exist that render an asset, database, or IT system extremely susceptible to failure or attack</li> </ul>
High	<ul style="list-style-type: none"> <li>•Countermeasure effectiveness is low (e.g., vulnerability estimate of .75)</li> <li>•Controls, policies, and procedures are mostly ineffective or insufficient</li> <li>•Resources and tools are inconsistently available for mission-critical needs</li> <li>•Some contingency, crisis management plans, or scenario plans in place</li> <li>•One or more major weaknesses exist that render an asset, database, or IT system susceptible to failure or attack</li> </ul>
Moderate	<ul style="list-style-type: none"> <li>•Countermeasure effectiveness is medium (e.g., vulnerability estimate of .5)</li> <li>•Controls, policies, and procedures are somewhat ineffective or insufficient</li> <li>•Resources and tools are available for mission-critical needs but are not optimized</li> <li>•Most contingency, crisis management plans, or scenario plans are in place with limited rehearsals</li> <li>•One or more weaknesses exist that render an asset, database, or IT system somewhat susceptible to failure or attack in select areas that can be contained</li> </ul>
Low	<ul style="list-style-type: none"> <li>•Countermeasure effectiveness is high (e.g., vulnerability estimate of .25)</li> <li>•Controls, policies, and procedures are mostly effective or sufficient</li> <li>•Resources and tools are available and optimized for mission-critical needs but to a lesser degree for non-mission-critical needs</li> <li>•Contingency, crisis management plans, or scenario plans are in place with some rehearsals</li> <li>•Few, easily remediable weaknesses exist that render an asset, database, or IT system susceptible to failure or attack in select areas of lesser consequence</li> </ul>
Very Low	<ul style="list-style-type: none"> <li>•Countermeasure effectiveness is very high (e.g., vulnerability estimate of .07)</li> <li>•Controls, policies, and procedures are effective or sufficient</li> <li>•Resources and tools are available and optimized for both mission-critical and non-mission-critical needs</li> <li>•Contingency, crisis management plans, or scenario plans are in place that are rehearsed regularly</li> <li>•Very few, minor weaknesses exist that render an asset, database, or IT system susceptible to failure or attack</li> </ul>



Table 14: Speed of onset scale

Qualitative values	Definition
<b>Very High</b>	Very rapid onset, little or no warning, instantaneous
<b>High</b>	Onset occurs in a matter of days to a few weeks
<b>Moderate</b>	Onset occurs in a matter of two to three months
<b>Low</b>	Onset occurs in a matter of three to four months
<b>Very Low</b>	Very slow onset, more than four months year to occur

Source: Committee of Sponsoring Organizations of the Treadway Commission (COSO) *Risk Assessment in Practice*, 2004.



## Appendix 2: Risk monitoring and reporting templates

Figure 15: Sample risk register

ID	Risk Owner Name	Risk area	Risk category	Risk name	Risk description	Causal factors	Impacts
1	John Doe	Business Operations	Human Resources & Employee Relations	Inability to attract, develop, or retain qualified staff	The risk that TSA may be unable to attract, develop, or retain qualified staff	Competing organizations or industries Non-competitive pay or benefits	High employee turnover Increased hiring and training costs
2							
3							

\*\* The information in the sample risk register above is not intended to represent an actual risk at TSA.



Figure 16: Sample ERSC top 10 risk snapshot report

Risk name	Very Low	Low	Moderate	High	Very High	Status and comments	Action
	Remote	Unlikely	Possible	Probable	Almost Certain		
1. Inability to attract, develop, or retain qualified staff						[Need to set desired risk tolerance levels using red sliders.]	Reduce
2. <Risk name>						[Status and comment]	[Action]
3. <Risk name>						[Status and comment]	[Action]
4. <Risk name>						[Status and comment]	[Action]
5. <Risk name>						[Status and comment]	[Action]
6. <Risk name>						[Status and comment]	[Action]
7. <Risk name>						[Status and comment]	[Action]
8. <Risk name>						[Status and comment]	[Action]
9. <Risk name>						[Status and comment]	[Action]
10. <Risk name>						[Status and comment]	[Action]

Key: Impact  Likelihood  Impact/likelihood score  Impact/likelihood capacity

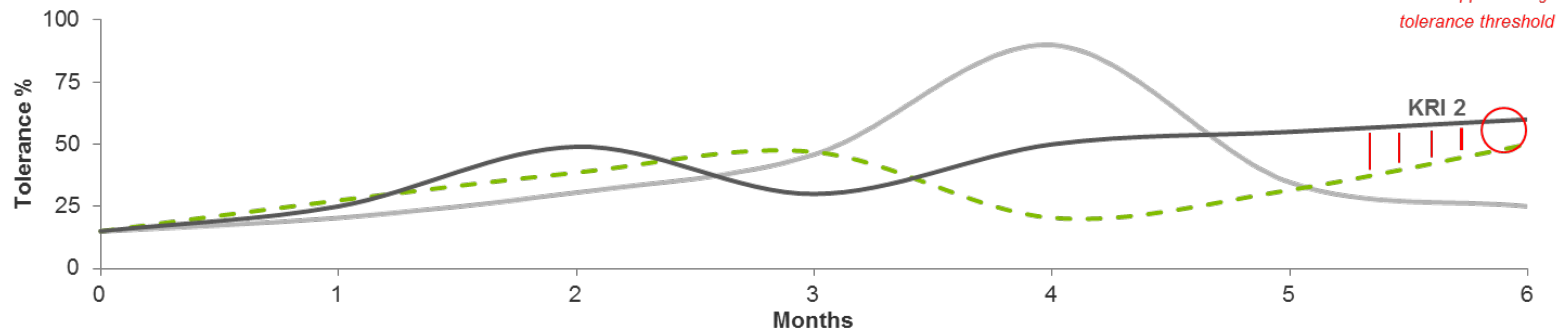
Risk response highlights	Issues
<ul style="list-style-type: none"> <li>[Highlight]</li> <li>[Highlight]</li> </ul>	<ul style="list-style-type: none"> <li>[Issue]</li> <li>[Issue]</li> </ul>
Upcoming milestones	Program Office action required
<ul style="list-style-type: none"> <li>[Milestone]</li> <li>[Milestone]</li> </ul>	<ul style="list-style-type: none"> <li>[Action]</li> <li>[Action]</li> </ul>



Figure 17: Sample individual risk report

[Risk name]				
<b>Risk description</b>	Inability to attract, develop, or retain qualified staff	<b>Risk rating</b>	<b>Probability</b>	<b>Impact</b>
<b>Risk owner</b>	John Doe	<b>Risk interdependencies</b>		

Risk specific KRIs



<b>Overall status</b>	<b>Changes in KRIs</b>
<ul style="list-style-type: none"> <li>During the FY15 Q1-Q2 period there have been relatively no changes to the impact and likelihood status of the risk</li> <li>Risk response plans currently under development</li> <li>[Insert status]</li> </ul>	<ul style="list-style-type: none"> <li>KRI 3 "number of industry requirements breaches" approaches tolerance threshold</li> <li>[insert change in KRI]</li> <li>[insert change in KRI]</li> <li>[insert change in KRI]</li> </ul>
<b>Milestones and issues</b>	<b>Decisions and actions required</b>
<ul style="list-style-type: none"> <li>Risk management project assessment phase completed on 5/17</li> <li>KRI 3 approaching tolerance threshold</li> <li>[Milestone/issue]</li> </ul>	<ul style="list-style-type: none"> <li>Approve finalized risk response options</li> <li>Review any immediate actions required to alleviate KRI 3 issue</li> <li>[Action]</li> </ul>





Figure 18: Sample risk progress report dashboard

Risk Title						
Risk description	Inability to attract, develop or retain qualified staff			Risk rating	Probability	Impact
Risk owner	Jane Doe			Risk interdependencies		

Summary of key action plan								
Causal factors	Risk response plans	Expected completion	Resource planning		Status	Causal factor KRI change		Causal factor KRI trend
						Prev. QTR	Prev. Yr.	
Lack of career path strategy	<ul style="list-style-type: none"> <li>Formed committee formally define workforce planning strategy</li> </ul>	FY16 Q4	5 FTEs	\$20,000	On-track	+ 1.295%	+ 1.75%	
	<ul style="list-style-type: none"> <li>Define career paths for critical position</li> </ul>	FY16 Q3	3 FTEs	\$75,000	Off-track	- .8%	- .11%	
[Enter causal factor 2]	<ul style="list-style-type: none"> <li>[Description]</li> </ul>	[Date]	[Source]	[\$ Amt.]	[Status]	[+/--%]	[+/--%]	[Trend]
	<ul style="list-style-type: none"> <li>[Description]</li> </ul>	[Date]	[Source]	[\$ Amt.]	[Status]	[+/--%]	[+/--%]	
[Enter causal factor 3]	<ul style="list-style-type: none"> <li>[Description]</li> </ul>	[Date]	[Source]	[\$ Amt.]	[Status]	[+/--%]	[+/--%]	[Trend]

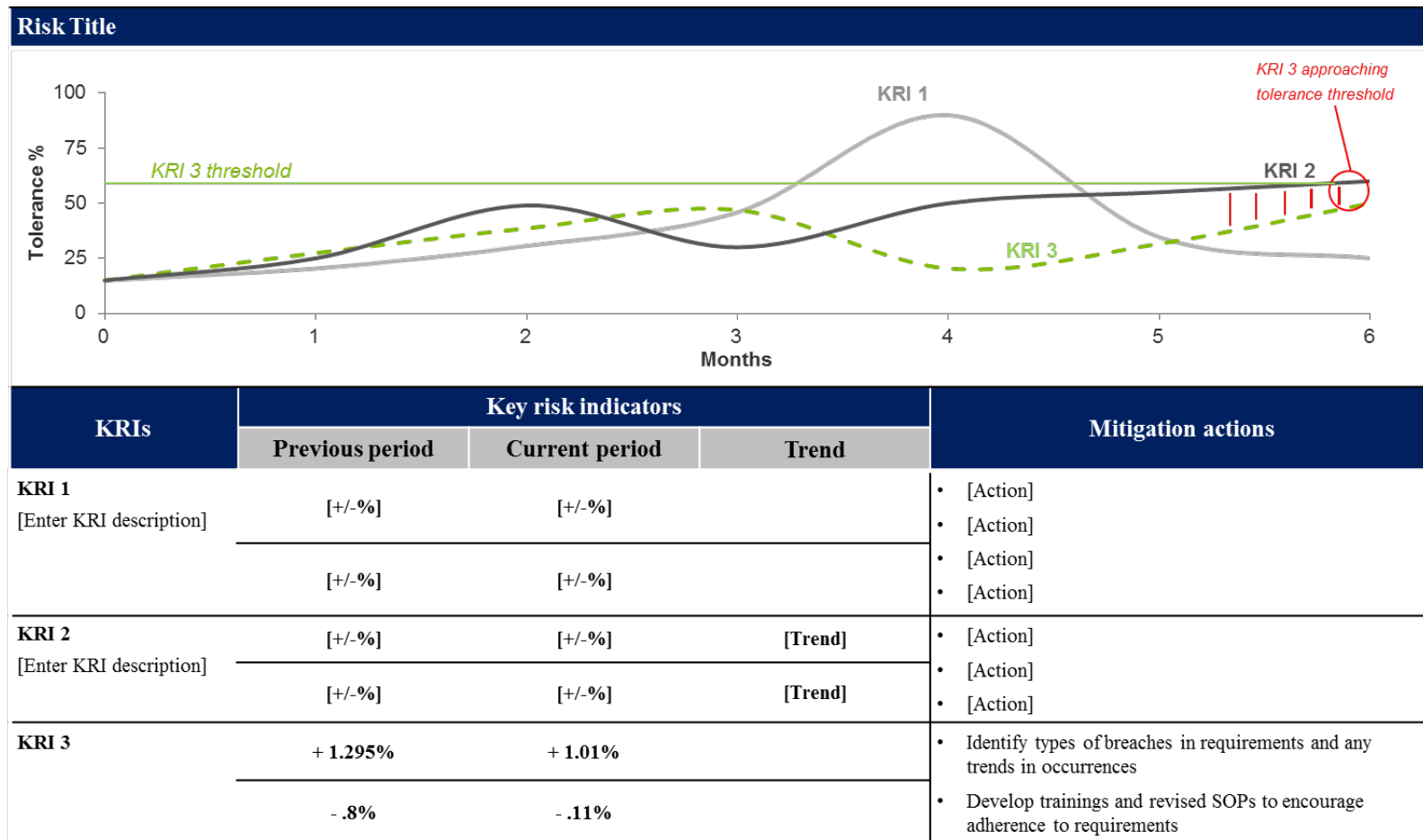


Figure 19: Sample risk response report dashboard

Risk		Risk owner		
Inability to attract, develop, or retain qualified staff		Jane Doe		
Current state/issue noted:		Future state/outcome:		
For example: Note any KRIs approaching threshold		7 risk response actions expected to reduce KRIs by 50% of determined KRI thresholds, and develop plans to reduce impact severity and likelihood levels		
Risk response action	Current State	Due Date	Response action owner(s)	Action results/details
1. Formed committee to develop workforce planning strategy		FY16 Q4	Dell MacApple (Program Office ABC) Roger McDonald (Program Office XYZ) Paul Denim (Program Office LMN)	<ul style="list-style-type: none"> <li>Held 7 meetings to date</li> <li>Developed stakeholder outreach plan</li> <li>Obtained strategy approval</li> </ul>
2. Define career path for critical positions		FY16 Q3	Kale Arugula (Program Office HIJ) Holly Mistletoe (Program Office EFG)	<ul style="list-style-type: none"> <li>Critical positions identified</li> <li>Workforce strategy developed</li> </ul>
[Enter response action plan 3]		[Date]	[enter individuals from Program Office responsible for action]	[enter action plan details]
[Enter response action plan 4]		[Date]	[enter individuals from Program Office responsible for action]	[enter action plan details]
[Enter response action plan 5]		[Date]	[enter individuals from Program Office responsible for action]	[enter action plan details]
[Enter response action plan 6]		[Date]	[enter individuals from Program Office responsible for action]	[enter action plan details]



Figure 20: Sample KRI monitoring dashboard





## Appendix 3: Executive Risk Steering Committee Charter

An effective Enterprise Risk Management (ERM) program requires the clear setting of roles and responsibilities for the management of risks. The Executive Risk Steering Committee (ERSC) is designated as the governing body at the Transportation Security Administration (TSA) responsible for developing risk management strategy across the organization.

### **Transportation Security Administration Executive Risk Steering Committee Charter March 2014**

#### **I. Purpose**

The purpose of this charter is to establish the ERSC's overarching responsibility for defining strategy and managing risk at an enterprise level. The ERSC oversees the development and implementation of processes used to analyze, prioritize, and address risks across TSA. These risks include terrorism threats facing the entire transportation sector, along with non-operational risks that could impede TSA's ability to achieve its strategic objectives. The ERSC is broadly responsible for ensuring that risks are managed to create value for the Nation and in a manner consistent with established risk appetite and risk tolerances levels. The ERSC has the powers set forth in this charter, but the responsibility of risk ownership and execution of risk management shall remain in the program offices.

#### **II. Background**

Risk management is a key driver for TSA and affects all aspects of TSA's operations, policies, and processes. In addition, the proliferation of tools and methodologies used to measure risk and associated risk management activities throughout TSA, the U.S Department of Homeland Security (DHS), and the private sector combined with TSA's goal of using intelligence and information necessitates the establishment of an executive-level risk governance structure.

#### **III. Function**

As TSA executives, ERSC members are responsible for managing risks within their respective program offices. However, when participating as a member of the ERSC, they are responsible for considering risk management from an Agency-wide perspective. The primary functions of the ERSC are to assist the Administrator and Deputy Administrator in oversight of key Agency risks through:

- The development, implementation and application of the TSA Enterprise Risk Management (ERM) Policy;
- Ensuring the effective operation of the TSA ERM Framework and setting the tone for ERM throughout TSA;



- Establishing the risk appetite for each major category of risk and the risk tolerance levels for area of risk associated with TSA strategic objectives;
- Identifying and reporting of the top strategic enterprise risks; and
- Constant monitoring of TSA's strategic enterprise risks and the associated response strategies.

The ERSC will fulfill these functions by carrying out the activities detailed in this charter.

#### **IV. Responsibilities and Duties of the ERSC**

The ERSC:

- In conjunction with the Chief Risk Officer (CRO), defines TSA's Enterprise Risk Management Framework
- Defines enterprise risk management priorities based on risk, threat environment, and opportunities to enhance value for the Nation through changes to TSA's approach to operations
- Sets the risk-based security and risk management strategies for TSA and provides strategic oversight
- Provides recommendations to the Administrator and Deputy Administrator regarding the enterprise risk appetite and risk tolerance thresholds
- Reviews alignment and provides direction for risk strategies based on risk appetite and enterprise risk portfolio
- Provides recommendations to the Administrator and Deputy Administrator regarding alignment of Agency resources to meet risk strategy objectives and strategic vision
- Identifies, prioritizes, and monitors the most significant enterprise risks through the strategic risk register and ensures appropriate risk response and mitigation plans are working to achieve desired outcomes
- Informs the Senior Leadership Team (SLT) of key risk-based security and risk management decisions
- Sponsors and provides oversight, direction, and review for the TSA Pre✓™ Risk Assessment working group

#### Limitation of Responsibilities and Duties of the ERSC:

While the ERSC has the responsibilities and powers set forth in this Charter, the responsibility of risk ownership shall remain in the program offices.

#### **V. Objectives**

The overall goal of the ERSC is to determine an appropriate risk-based, crosscutting strategy that will enable the use of threat, vulnerability, and consequence information to make risk-informed policy and resource allocation decisions across all TSA functions.



The ERSC's primary objective is to develop and oversee an enterprise risk management strategy that achieves the following outcomes:

- **Identify risks** - Compile a unified set of transportation security risks by risk category. Cast a wide net to understand the universe of risks making up TSA's risk profile.
- **Develop vulnerability assessment standards and enterprise risk assessment thresholds** - Develop a common set of assessment standards across the organization, assessed on likelihood and impact to the security system.
- **Assess risk** - Assign values to each risk using the defined criteria. Initially, the ERSC may use qualitative techniques and then use quantitative analysis for select risks.
- **Assess risk interactions** - Develop a holistic view of risks using techniques such as risk interaction matrices, bow-tie diagrams, and aggregated probability distributions.
- **Prioritize risks** - Determine risk management priorities by comparing the level of risk against predetermined target risk levels, risk appetite, and tolerance thresholds.
- **Respond to risks** - Examine response options (accept, mitigate, share, or avoid), perform cost-benefit analyses, formulate a response strategy, and develop risk response plans.
- **Create or enhance value** - Use the defined risk appetite and risk thresholds to inform decision-making and define the value created by TSA (e.g., enhanced stakeholder engagements, increased operational efficiency, and enhanced security effectiveness) in accomplishing TSA's missions and achieving strategic objectives.
- **Charter Integrated Project Teams (IPTs) that implement high-priority initiatives:**
  - Coordinate and implement internally, as directed, on internal risk management strategies and procedures.
  - Coordinate with the various DHS risk-related efforts and those set forth by the TSA Administrator, including working groups and other DHS components as appropriate.

## VI. Organization

The ERSC's Chair is the CRO (or designated ERSC Assistant Administrator when the CRO is not available) and reports to the Deputy Administrator. A project management staff supports the Chair in preparing for and conducting the ERSC meetings. As required, the ERSC oversees the progress of working groups that will consist of executive- and staff-level participants. Working groups develop detailed plans defining milestones and key deliverables that meet requirements and tasks from the ERSC.

The ERSC consists of the following primary members:

Chief Risk Officer (Chair)  
Assistant Administrator, Office of Security Operations  
Assistant Administrator, Office of Law Enforcement/Federal Air Marshal Service  
Assistant Administrator, Office of Global Strategies  
Assistant Administrator, Office of Security Policy and Industry Engagement



Assistant Administrator, Office of Intelligence and Analysis  
Assistant Administrator, Office of Security Capabilities  
Assistant Administrator, Office of Finance and Administration  
Assistant Administrator, Office of Information Technology  
Assistant Administrator, Office of Acquisitions  
Assistant Administrator, Office of Human Capital

- Participants in specific ERSC meetings may include other program offices
- Assistant Administrators and subject matter experts as deemed necessary and approved by the ERSC primary members and CRO
- Other Assistant Administrators may attend ERSC meetings as a nonvoting member.
- As the organization changes, the ERSC membership will adjust accordingly.

Responsibilities and Duties of ERSC Members

At a minimum, the ERSC shall meet in person on a monthly basis. Additionally, the chair may schedule ad hoc meetings at his or her discretion. ERSC members have the following responsibilities:


- Attend ERSC meetings in person or virtually if possible. If an ERSC member cannot attend for any reason, he or she must appoint a designated alternate empowered to make decisions on his or her behalf. Should this person be below Deputy level, prior approval from the CRO must be obtained.
- Appoint knowledgeable and empowered representatives and a designated alternate to participate in IPTs established by the ERSC.
- Elevate major risk-related decisions to the full ERSC as necessary.
- Review read-ahead materials prior to the meeting.
- Facilitate ERM-related communications within their respective program offices.

Decision Making

Each member shall have one vote. The quorum for decision-making is two-thirds of the members or designated alternatives present. A simple majority of the attendees is required to bring a decision forward to the Administrator and Deputy Administrator. Unanimous concurrence is not required, and contrary opinions will be brought forward to the Administrator and Deputy Administrator for their consideration in making a final decision.

**VII. Approval**

The TSA Administrator has approved and signed this charter as of the date below.

  
\_\_\_\_\_  
John S. Pistole  
Administrator

3/31/14  
Date



## Appendix 4: TSA Risk Appetite Statement

The TSA ERM policy specifies ERM practices and applies to all TSA Program Offices at headquarters, in the field, and to employees at every level of the organization. This appendix consists of the appetite statements presented in that policy.

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.

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

- TSA is strongly averse to security risks that could result in catastrophic consequences.
- 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).
- TSA is averse to workforce-related risks pertaining to integrity, performance, health and safety, and regulatory compliance.
- 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.
- TSA is risk neutral with regard to other mission and business operational enterprise risks.
- TSA is risk tolerant to programs that enhance the movement of legitimate travelers and goods.

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

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





- 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.
- TSA maintains a flexible capability to focus resources on the basis of real-time threat information.
- TSA takes decisive action to respond to imminent threats with potentially catastrophic consequences and security effectiveness that may take precedence over other considerations.
- TSA evaluates risk levels and implements risk responses and monitoring to bring the risk within tolerance without over-controlling non-security related enterprise risks.
- 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.

A handwritten signature in black ink that reads "John S. Pistole".

John S. Pistole  
Administrator



## Appendix 5: ERM Lexicon

The following terms describe core concepts and terms that provide the basis for the TSA ERM framework and are used extensively throughout the risk management processes outlined in this manual. Many of these terms and definitions are derived from the DHS risk lexicon and have been expanded to apply to an ERM framework appropriate for TSA.

Figure 21: Proposed risk lexicon

Term	Definition
Accidental hazard	Source of harm or difficulty created by negligence, error, or unintended failure
Adversary	Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities
Control	Strategy or action that is modifying risk
Enterprise risk management	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
Establishing the context	Defining the external and internal parameters to be taken into account when managing risk and setting the scope and risk criteria for the risk management policy
Event	An incident or situation that occurs in a particular place during a particular interval of time
Event tree	Graphic tool used to illustrate the range and probabilities of possible outcomes that arise from an initiating event
Exposure	Extent to which an organization and/or stakeholder is subject to an event
External context	External environment in which the organization seeks to achieve its objectives
Fault tree	Graphic tool used to illustrate the range, probability, and interaction of causal occurrences that lead to a final outcome
Economic consequence	Effect of an incident, event, or occurrence on the value of property or on the production, trade, distribution, or use of income, wealth, or commodities
Hazard	Natural or man-made source or cause of harm or difficulty, may be intentional or accidental
Impact	The extent to which a risk event would affect the enterprise
Intentional hazard	Source of harm, duress, or difficulty created by a deliberate action or a planned course of action
Internal context	Internal environment in which the organization seeks to achieve its objectives



Term	Definition
Key performance indicator (KPI)	Measures on the progress or the achievement of objectives and activities
Key risk indicator (KRI)	Measures that provide an early warning system that a risk is occurring or has occurred.
Level of risk	Magnitude of a risk or combination of risks expressed in terms of the combination of consequences and their likelihood
Likelihood	Represents the possibility that a given event will occur
Monitoring	Continual checking, supervising, critically observing, or determining the status in order to identify change from the performance level required or expected
Natural hazard	Source of harm or difficulty created by a meteorological, environmental, or geological phenomenon or combination of phenomena
Probability	Measure of the chance of occurrence expressed as a number between 0 and 1, where 0 is impossibility and 1 is absolute certainty
Residual risk	Risk that remains after risk management measures have been implemented
Opportunity	The possibility that an event will occur and positively affect the achievement of objectives
Resilience	Ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption
Risk	Potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences
Risk acceptance	Explicit or implicit decision not to take an action that would affect all or part of a particular risk
Risk aggregation	The collection of risk (their categories and impact) to develop a more complete understanding of the overall risk
Risk analysis	Systematic examination of the components and characteristics of risk
Risk appetite	Amount and type of risk that an organization is willing to pursue or retain
Risk assessment	Product or process which collects information and assigns values to risks for the purpose of informing priorities, developing or comparing courses of action, and informing decision making
Risk avoidance	Informed decision not to be involved in, or to withdraw from, an activity in order not to be exposed to a particular risk
Risk criteria	Terms of reference against which the significance of a risk is evaluated
Risk description	Structured statement of risk usually containing five elements: sources, events, causes, consequences, and target (if applicable)
Risk identification	Process of finding, recognizing, and describing potential risks
Risk management	Coordinated activities to direct and control an organization with regard to risk
Risk map	Graphic tool used to illustrate areas of risk exposure



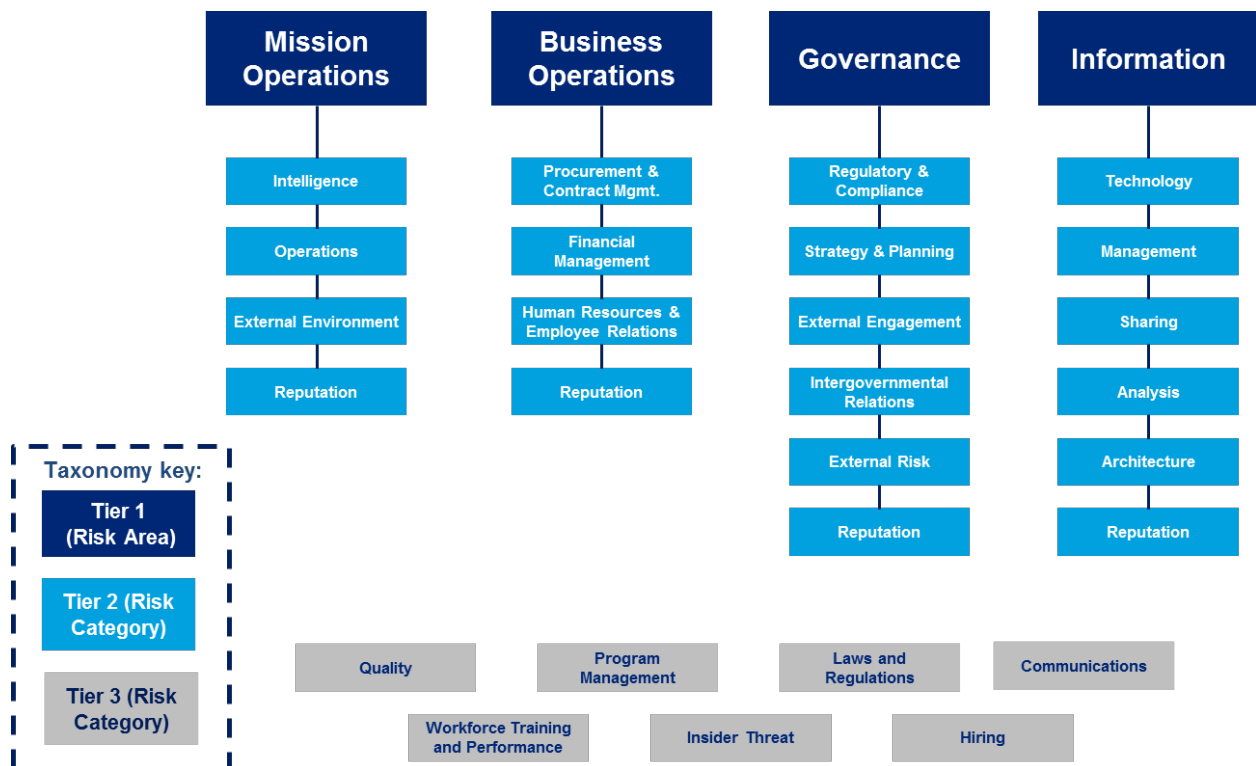
<b>Term</b>	<b>Definition</b>
<b>Risk matrix</b>	Tool for ranking and displaying components of risk in an array
<b>Risk owner</b>	Person or entity with the accountability and authority to manage a risk
<b>Risk profile</b>	Description of any set of risks
<b>Risk register</b>	Record of information about identified risks
<b>Risk reporting</b>	Form of communication intended to inform particular internal or external stakeholders by providing information regarding the current state of risk and its management
<b>Risk response</b>	Actions defining an organization's approach to an identified risk
<b>Risk sharing</b>	Form of risk response involving the agreed distribution of risk with other parties
<b>Risk source</b>	Element which alone or in combination has the intrinsic potential to give rise to risk
<b>Risk tolerance</b>	Organization's or stakeholder's readiness to bear the risk after risk response in order to achieve its objectives
<b>Risk transfer</b>	Action taken to manage risk that shifts some or all of the risk to another entity, asset, system, network, or geographic area
<b>Speed of onset</b>	The time it takes for a risk event to manifest, or the time that elapses between the occurrence of an event and the point at which the enterprise first feels its effects
<b>Stakeholder</b>	Person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity
<b>Target</b>	Asset, network, system or geographic area chosen by an adversary to be impacted by an attack
<b>Threat</b>	Natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property
<b>Vulnerability</b>	Susceptibility of the entity to a risk event in terms of environmental factors related to the entity's preparedness, agility, and adaptability



## Appendix 6: ERM Risk Taxonomy

The ERM Risk taxonomy organizes risk into categories to promote consistent identification, assessment, measurement, and monitoring of risks across the organization. Using a common and consistent risk taxonomy across the entire organization enables TSA to determine the relationships between various risks in a manner that allows improved assessment of the overall impact to the organization. Figure 2 illustrates TSA’s proposed ERM risk taxonomy, including 3 tiers of risk categories. The four tables that follow further define the Tier 2 risk categories within each Tier 1 risk area. Taxonomy tiers are intended to provide increasing levels of detail for a specific risk, and do not denote levels of importance.

Figure 22: Proposed risk taxonomy





### Taxonomy risk area and risk category descriptions

Figure 23: Proposed risk taxonomy category — *Mission*

<b>Mission operations</b>	<b>Fundamental areas that are central to, or will influence, TSA’s approach to its mission of ensuring freedom of movement for people and commerce</b>
<b>Intelligence</b>	The collection, analysis, production, dissemination, and use of information which allows TSA to effectively achieve mission success.
<b>Operations</b>	Programs and services (e.g., security screening, regulatory compliance, air cargo, intermodal, international relationships, law enforcement, canine programs) through which TSA implements mission objectives.
<b>External environment</b>	Externalities which affect implementation of TSA mission objectives (e.g., threats, hazards, economic conditions).
<b>Reputation</b>	The common perception that TSA’s stakeholders (e.g., Congress, the traveling public) have about TSA’s mission operations.

Figure 24: Proposed risk taxonomy category — *Business operations*

<b>Business operations</b>	<b>Core functions or elements that serve to enable how TSA will carry out its mission through its Programs and Services</b>
<b>Procurement &amp; Contract Management</b>	Procurement, investment and contract management activities performed to support Programs and Services.
<b>Financial Management</b>	Accounting, budget, and financial reporting functions performed to support Programs and Services.
<b>Human Resources &amp; Employee Relations</b>	Workforce recruiting, hiring, training, and deployment to support Programs and Services.
<b>Reputation</b>	The common perception that TSA’s stakeholders (e.g., Congress, the traveling public) have about TSA’s business operations.



**Figure 25: Proposed risk taxonomy category — Governance**

<b>Governance</b>	<b>Laws, regulations, and policies which provide the structure and composition for TSA, including the internal activities and policies for which senior leadership allocates specific aspects of oversight and responsibility.</b>
<b>Regulatory &amp; Compliance</b>	Laws, regulations, statutes, Executive Orders, and departmental policies that TSA is required to comply with in order to carry out operations in support of Programs and Services; this includes reports required by OMB, Congress, GAO and DHS, including internal and external audits, GPRA reporting, and other required metrics and assessments.
<b>Strategy &amp; Planning</b>	The planning or methods TSA leadership implements for achieving mission goals (usually over the long-term).
<b>External Engagement</b>	The nature of TSA’s third-party relationships (including geopolitics and alliances) affecting the implementation of TSA’s mission goals.
<b>Intergovernmental Relations</b>	Coordination with other federal (to include Congressional and Administrative branches of government), state, local, tribal, and international governmental bodies and entities on key TSA initiatives, policies, and programs, as well as rulemaking and legal advisory services to support Programs and Services.
<b>External Risk</b>	Externalities which affect implementation of TSA operations and governance activities (e.g., political balance, changes in laws and regulations).
<b>Reputation</b>	Management and promotion of a positive public image and stakeholder beliefs (e.g., Congress, OMB, GAO, and other governing authorities) and opinions of TSA’s mission and mission support activities.

**Figure 26: Proposed risk taxonomy category —Information**

<b>Information</b>	<b>The technology and functions central to TSA communications that directly impacts the ability to carry out their mission, business operations, or functions .</b>
<b>Technology</b>	The collection of tools – including hardware, software, and modifications to methods and procedures – to address mission and business operational needs.
<b>Management</b>	Technical processes, methods, or policies (including information security) enacted to support Programs and Services with which TSA accomplishes a mission or business operation objective.
<b>Sharing</b>	Communication, coordination, and information sharing between TSA components and among stakeholders to promote successful performance of TSA’s mission.
<b>Analysis</b>	Examination and synthesis of information collected and used in mission and business operations.
<b>Architecture</b>	The environment of technology processes and platforms used to collect, manage, share, and organize information to enable mission and business operations.
<b>Reputation</b>	The perception of TSA’s stakeholders regarding TSA’s ability to appropriately secure articulate important information.