A Blueprint to Effective Enterprise Risk Management

Kenneth J Kepchar
Federal Aviation Administration
Kenneth.kepchar@faa.gov

Abstract.

Traditional risk management models have typically focused on the acquisition and operational phases of a product life cycle, with the second dimension of these models being that they are also system-centric. Modern transportation systems are defying the traditional system-centric approach to design, development, and deployment and represent an unprecedented level of complexity to be factored into decision making. This level of complexity, both in the solution space and at the organizational level, demands a more robust approach to risk and opportunity management than has traditionally been considered. This paper discusses the factors that must be addressed in establishing a viable opportunity and risk management presence in a Systems of Systems (SoS) context.

Introduction.

Much of our current and emerging transportation capability can be classified as widely distributed Systems-of-Systems (SoS). They are composed of multiple independently functioning systems of systems that are federated to deliver overall capabilities and services. In the case of air traffic management in the United States, this includes, but not limited to, communications and data-sharing, location determining, and flight planning, to approach surveillance systems. The National Airspace System (NAS), which is "today's air traffic control system, relies on ground-based communications, navigation and surveillance services that can no longer be scaled upward to handle growing demand. NextGen, led by the FAA, is the federal government's response to this challenge. It calls for fundamental changes in the concepts, systems, technologies, roles and responsibilities guiding the nation's air traffic system. The complex network that is the NAS requires a comprehensive set of services able to deliver benefits along several fronts. … Providing new capacity is not in itself sufficient to close NAS performance gaps. There are requirements in other areas that must simultaneously be met. Foremost among these is safety. Despite forecasted growth, aircraft and air traffic operations should maintain their current low accident and fatality rates across the system."[1]

The NAS is also a critical component of a broader aviation enterprise, including airport authorities, airlines, general aviation, and other federal agencies.[2] Each can be viewed as a System of Systems in their own right. This complexity extends to the organizational context itself through "the diversity of stakeholders associated with (this endeavor). Stakeholder groups will likely differ in viewpoint, which will be reflected in the needs and requirements. This

[1] OMB Performance Dashboard for NextGen – http://it.usaspending.gov
[2] Next Generation Air Transportation System, A report prepared by Stevens Institute of Technology (Aug 2009), Section 1.2

diversity must be effectively managed through a (disciplined and well-defined) governance process in order for (the endeavor) to be successful".[3]

The most daunting challenge in the development and deployment of widely distributed SoS is the massive coordination effort among the various stakeholders and the synchronization of activities to deliver early benefits and efficiencies. In the case of aviation, the extent of procurement of user equipage (aircraft in the case of aviation or cars/trucks in the case of intelligent surface transportation systems) coupled with ensuring the readiness of the infrastructure (including policy development/changes), presents a plethora of opportunities and risks. Few, if any, benefits from new technology accrue until a critical mass of equipped vehicles are in operation.

Management of opportunities and risks at the enterprise level is gaining acceptance in more and more board rooms across many industries. **For the purposes of this paper, the term "enterprise" is defined to include both the federation solution space (Systems of Systems) and/or the organizational community of participants and stakeholders involved.**

Program Elements.

The following elements and considerations are necessary for successful management of Risk / Opportunity in a complex SoS context, referred to as "Enterprise Risk Management" (ERM):

- **Strategy** – Statement of purpose and approach to managing opportunity/risk in the context of an SoS.
- **Plan** – Documentation to establish the operating scope, process, tools, documentation, and roles/responsibilities/authority (RAA).
- **Process Framework** – overall process structure to systematically and consistently identify, analyze, and manage enterprise level opportunities/risks.
- **Integration** – Interaction with other key enterprise management systems/processes such as the Enterprise Architecture (EA) Performance Management and Management Visibility systems.
- **Governance** – The policies and mechanisms to render decisions regarding enterprise level opportunities/risks that are addressed at the enterprise level.
- **Products & Tools** – A suite of products and tools is necessary to enable effective analysis and management of enterprise opportunities/risks. This includes software, a data repository, and outputs to support the governance process.
- **Training & Workforce Competencies** – Role based training is required for participants and interested parties spanning decision makers, practitioners, and affected stakeholders. This must be coupled with objective measures of practitioner competencies or skills.

[3] Next Generation Air Transportation System, A report prepared by Stevens Institute of Technology (Aug 2009)

- **Deployment** - The roll–out of a consistent ERM process should be staged to ensure that the participating organizations and functions achieve an appropriate level of maturity to allow them to improve their overall performance.

Benefits.

Risk management is often incorrectly viewed as an impediment to achieving an organization's goals. Striking the proper balance between risk and performance turns risk management into a proactive decision tool, especially when coupled with pursuit of potential opportunities. Investment in this capability directly supports the goals of effective communication across the stakeholder community in the support of major operational/organizational decisions e.g. future strategic direction, program approval, or capital investment approval and offers the following benefits for the organizations involved:

- **Consistency** - Given the organizational diversity of the stakeholder community, a standard framework provides a consistent shared view of risks, especially from entities touching the enterprise. There is also an opportunity to share policies, metrics, mitigations, and enforcement of decisions.

- **Knowledge database** - A shared knowledge base reduces the number of redundant risks and controls that members of the extended community must deal with. It also provides transparency through common information being available and used by all parties.

- **Understanding** - A shared view of the problem space and actions being taken facilitates effective dialogue across organizations and with stakeholders. Improved understanding of available mitigation options allows the federated SoS solution to achieve balance between alternative treatment strategies, thus enabling rational risks to be taken from an informed and controlled basis. Enterprise-wide awareness and sharing increases the confidence and investment each member of the extended community has in succeeding.

- **Credibility** - Decisions based on facts and objective criteria across the extended enterprise provides credibility to decisions being made, regardless of the organization(s) involved. Additionally, this approach reflects emerging trends in industry practice of risk management at the enterprise level vs a more traditional system-centric approach.

- **Efficiency** - The individual entities that make up the enterprise are networked to a degree that risks are shared across these networks whether they realize it or not. Consolidated risk treatment, documentation, and reporting provides efficient and effective decision making across all participants. It also allows for allocation of mitigation resources across the implementing organizations and stakeholders.

- **Compliance** – US Government organizations have responsibilities under the Federal Information Security Management Act (FISMA)[4] that requires compliance with specific regulations and standards, both present and emerging. For example, the Office of

[4] Public Law (P.L.) 107-347

Management and Budget (OMB) has issued guidelines in Circular A-130, and NIST Special Publication 800-53, Rev 3 (Aug 2009) (Controls RA-3 and PM-09). Emerging concepts for enterprise level risk management are found in NIST SP 800-37 Rev 1 (Feb 2010). The extent that these and similar standards are also applicable to the private sector is under consideration in pending US legislation.

Strategy.

A federation of System of Systems emcompasses considerably more than acquisition and/or implementation. Traditional risk frameworks need to be adapted to satisfy the enterprise's needs. Enterprise Risk Management (ERM) is focused at the enterprise level rather than project/system level, and is structured to address the complexity and integration issues arising from a System of Systems (SoS) endeavor.

While adaptation of an existing framework is necessary for an SoS application, certain fundamental tenets are still applicable. These form the basis for a successful Enterprise Risk Management approach:

1. Opportunity and risk are managed through the same framework across the **lifecycle**. This is illustrated in Figure 1. In addition, opportunity and risk are managed in the same manner across the **enterprise,** through an Enterprise Risk Management framework. This includes policy, process, criteria, and dissemination of enterprise risk information.
2. All opportunities/risks are measured against delivering the capabilities of the SoS. This constitutes "success" as defined by the SoS stakeholders.
3. The ERM governance model is based on existing organizational decision making mechanisms.
4. Management of enterprise opportunities/risks builds on and complements ongoing efforts. Program implementation risks become enterprise risk(s) when the impact transcends program scope/boundaries *(same criteria as CM Class I).*
5. A risk tool that is capable of scaling to the enterprise level (multiple organizations and/or SoS sets) and integrates into the management tool suite used by the lead integration organization is needed to manage opportunities/risks at the SoS level.
6. Enterprise Risk Management builds upon and is compatible with existing enterprise mechanisms such as portfolios, Performance Management Systems (PMS), and Management Visibility Systems.
7. Since degree of risk treatment tends to key on color changes (red, yellow, green risk levels), prior agreed upon definitions and formal validation of color changes must be established to enforce a consistent portrayal of risk and opportunity levels to all participants and stakeholders.

Enterprise Risk Management Plan (ERMP).

An Enterprise Risk Management plan is developed and maintained by the lead integration organization. This document should address the elements discussed herein in sufficient detail to enable effective enterprise risk management to be applied across the enterprise. The ERMP should address the following areas, as a minimum, for both enterprise risks and

opportunities: operating scope, process, roles/responsibilities/authority (RAA), tools, status reporting (frequency, format, etc), and documentation.

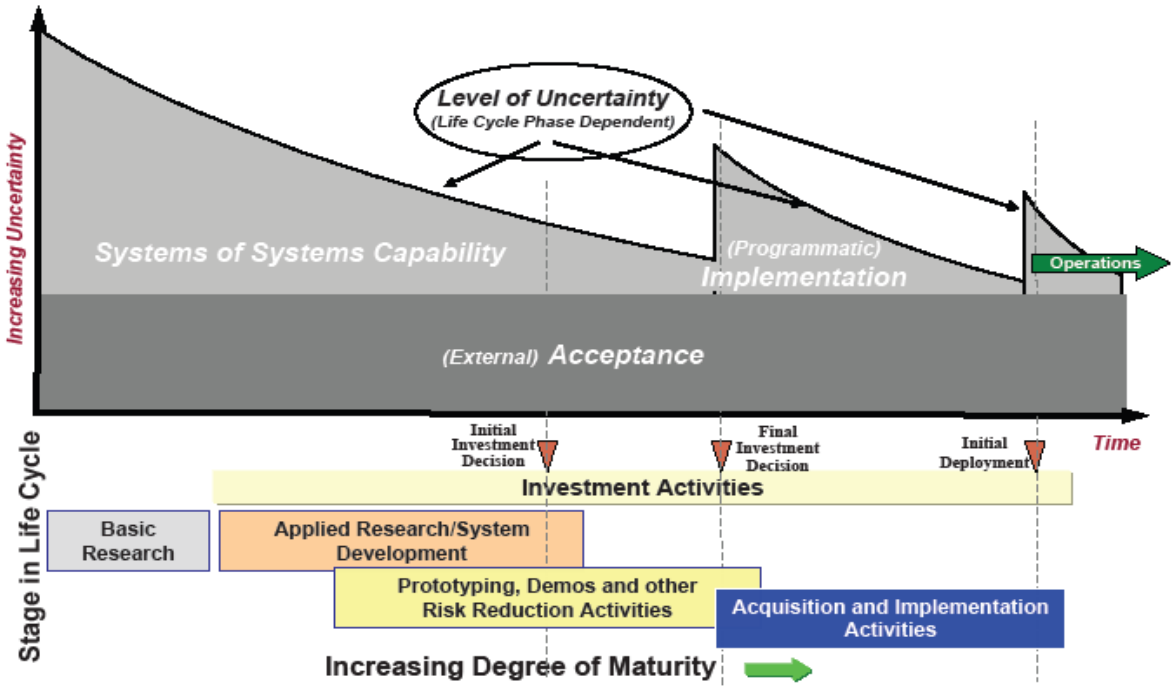

Figure 1 – Enterprise Risk Management Framework Spans the Full Life Cycle

Process Framework.

This framework is based on a traditional risk management process model, adapted to an SoS context for both opportunity and risk. It focuses on identification, analysis and treatment/pursuit as shown in Figure 2 for both risks and opportunities. The use of this process framework during the planning, development, and deployment of the SoS has three primary objectives:

1. Inclusion of opportunity/risk in the SoS architectural framework ensures that the concepts and courses of action with extreme risk are generally avoided and/or filtered out of the various architectural features generating these risks as they are identified. Alternatively, subsequent approaches that are developed to evaluate the features of candidate concepts and approaches are designed specifically to eliminate or mitigate such risks, while exploring potentially attractive outcomes.
2. Risks which remain are considered when developing implementation approaches, including focused research, development, or assessment designed to mitigate such risks, vice immediate implementation of a high risk feature.
3. The residual opportunities and risks are documented, and should be considered during subsequent life cycle phases or activities such as far term implementation planning.

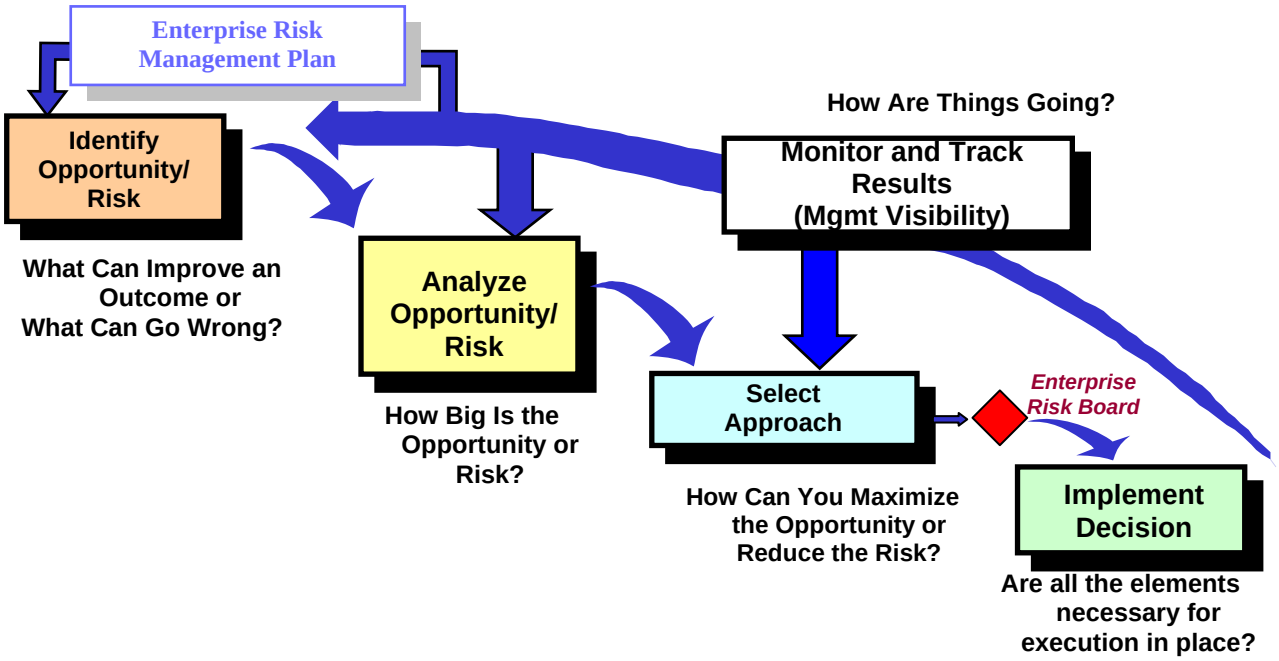

Figure 2 – Enterprise Risk Management Process

Opportunity Management.

The objective of the Opportunity Management portion of the Enterprise Risk Management framework is to exploit situations involving upside uncertainties to success while providing a proper balance between risk and opportunity. It seeks to understand the potential opportunities to an endeavor, and to take a proactive and well-planned role in anticipating them and capitalizing on them if they occur. **Opportunity is defined as a future situation or circumstance with a realistic (non-zero nor 100 percent) likelihood/probability of occurring and which may create a favorable outcome toward advancing enterprise objectives.**

Opportunity Management is an organized, systematic decision-support process that identifies opportunities (and attendant risks), assesses or analyzes potential benefits, and effectively pursues situations that advance enterprise objectives. Opportunity management is a continual process throughout the federated SoS life cycle. Opportunities within the overall solution space are defined, assessed and pursued following a structured process, and reviewed on a regular basis for the purpose of informing decision making at all levels. This framework is based on and in concert with standard risk management processes adapted to the enterprise context.

Opportunities need to address whether they improve the desired results for the enterprise. For example in the case of Air Traffic Management, the impact of each opportunity is judged through the perspectives of safety, efficiency, and capacity. The actual measures of success are developed through the enterprise Performance Management System.

Risk Management.

The objective of the Risk Management component of the Enterprise Risk framework is to manage downside uncertainty while providing a proper balance between risk and opportunity. It seeks to understand the potential risks to an endeavor, and to take a proactive and well-planned role in anticipating them and responding to them if they occur. **Risk is defined as a future event or situation with a realistic (non-zero nor 100 percent) likelihood/probability of occurring and an unfavorable consequence/impact to the successful accomplishment of well-defined goals if it occurs.**

Risk Management is an organized, systematic decision-support process that identifies risks, assesses or analyzes risks, and effectively mitigates or eliminates risks to achieve objectives. Risk management is a continual process throughout the federated SoS life cycle. Risks to the overall SoS solution set are defined, assessed and mitigated following a structured process, and reviewed on a regular basis for the purpose of informing enterprise decision making at all levels.

A traditional view of risk frameworks classifies each risk according to the root cause of the risk event, typically in the categories of technical, schedule, and cost. While these dimensions are useful and easy to understand, they need to be expanded and tailored to make the discussion of risk meaningful for a System of Systems (SoS) context. In a similar manner , risk evaluation criteria must be adapted to support enterprise needs rather than any single system or organization.

For an enterprise, it is more useful to view the root cause of a risk beyond the traditional terms of (system) performance, schedule, and cost, since these metrics effectively only measure implementation success and don't address the balance of the larger enterprise nor life cycle shown in Figure 1. In this context risks are categorized in terms of (1) SoS **capabilities** of the concepts captured in the architecture, (2) programmatics of **implementing** the solutions associated with these concepts and capabilities, or (3) external forces that influence the realization of the architectural components such as stakeholder **acceptance**, shown in Figure 3.

These categories are each decomposed over time into a Risk Breakdown Structure that supports an enterprise work breakdown Structure (WBS). This ensures that all risk information developed at any level of the enterprise has line of sight by all affected parties.

Integration with Organizational Management Systems.

The Enterprise Risk framework needs to be mutually compatible with and support other management systems. The primary intersection is with the Enterprise Architecture. However, ERM has to effectively interface and support Performance Management, Knowledge Management, and Management Visibility at the enterprise level, including its visibility portal.

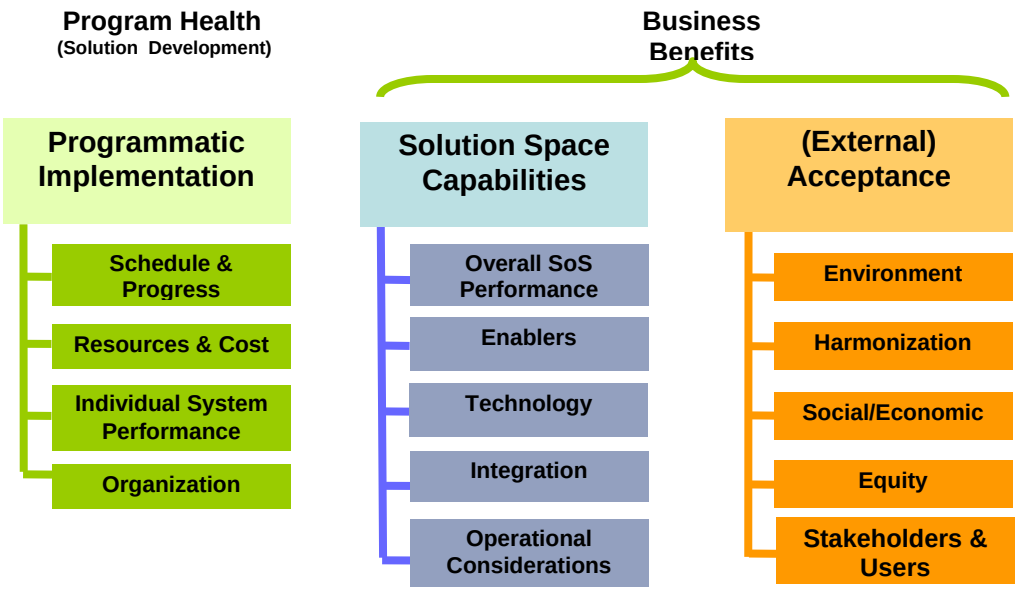

Figure 3 – Enterprise Risk Categories

Governance.

The effort to address opportunity/risk at the enterprise level is a federated responsibility that requires effective and extensive collaboration. Individuals and/or organizations are charged with contributing to this effort in various manners, ranging from management of the process, ownership of contents, through development of opportunity/risk artifacts.

Policy.

ERM mechanisms to render decisions regarding enterprise level opportunities/risks require an organizational environment that includes a strategic policy structure that enforces consistent application of the framework to produce the benefits that are envisioned in this strategy. Execution of an enterprise risk management strategic policy provides policy makers consistent and creditable information to base enterprise decisions. Cultural differences across the participating organizations are probably the largest obstacles to success. Effective governance won't happen in the face of incompatible or clashing organizational cultures and decision styles. A further discussion of policy should be included in the Enterprise Risk Management Plan.

Decision Model.

The basic tenant in the enterprise risk decision model is that decisions occur at the lowest level practical. The goal is the reduction of overall risks to the success of the SoS. Assessing risks that are specific to a program/system is NOT a goal of this framework. In practice, this means that risks should be dealt with where the concomitant responsibility, accountability, and authority (RAA) resides. For example, risks that are within the scope of an implementation program or

organization are handled by that organization. If the risk impact extends beyond that scope, the decision must be escalated to a level that is commensurate with the scope of the risk. This is the same principle followed in implementing effective Configuration Management. Figure 4 depicts this Enterprise Risk governance model.

Figure 4 –Enterprise Risk Management Governance

Enterprise Risk Management Execution.

An enterprise risk management function must be established within the Lead Integrator's organization. This function shall include an Enterprise Risk Manager and appropriate staff to maintain & manage the effort on a continuous basis. In NIST SP800-37, this function is referred to as the "Risk Executive Function". This function should be responsible to the Enterprise Risk Board for all opportunity/risk information necessary to support enterprise level decisions. This includes the Enterprise Risk Management Plan (ERMP), database and all opportunity/risk products defined in the ERMP. In general, the risk executive function:

- Provides senior leadership input and oversight for all opportunity and risk management activities across the enterprise to help ensure consistent decisions on risk acceptance and pursuit of opportunities;
- Ensures that individual authorization decisions by authorizing officials consider all factors necessary for enterprise-wide mission and business success;
- Provides an enterprise-wide forum and visibility to consider all sources of risk (including aggregated risk from individual systems) to organizational operations and assets, individuals, other organizations, and stakeholders;

- Promotes cooperation and collaboration among organizations in the enterprise to include authorization actions requiring shared responsibility;
- Identifies the overall enterprise risk posture based on the aggregated risk from each of the systems and supporting infrastructures for which the organization is responsible;
- Ensures that the shared responsibility for supporting organizational mission/business functions using external providers of systems, information, and services receives the needed visibility and is elevated to the appropriate decision-making authorities, and
- Measures the effectiveness of mitigation efforts through the Enterprise Performance Measurement System.

Opportunities/risks can be identified by anyone involved or interested in the enterprise solution set. Prior to commitment to the master repository and potential subsequent effort, each proposed risk and/or opportunity is screened for relevance and validated as meeting enterprise criteria. Validation includes an assessment of the magnitude of the opportunity/risk. In the case of proposed opportunities, the enterprise risk management function should utilize the expertise of the business management community within the lead integrator through an Initial Opportunity Review. For enterprise risks, the Enterprise Risk Manager should chair a Risk Review Group, which has representation from the enterprise organizations. This group validates the proposed risks, analyzes and scores them per established assessment criteria, and generates a recommended approach for handling the risk and proposed mitigation organizational RAA. A representative view of the Enterprise Risk Management function is shown in Figure 5.

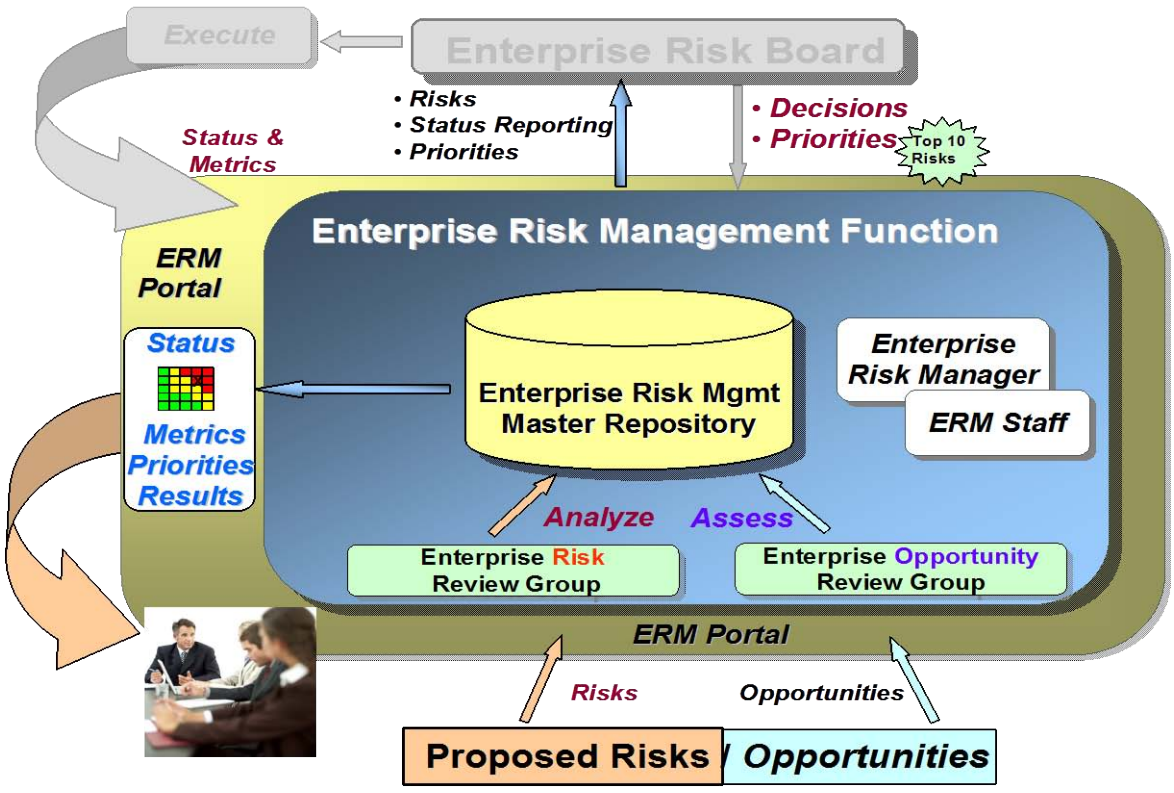

Figure 5 – Enterprise Risk Management Function

Risk Board.

The governance model discussed here envisions a multi-layed approach to Risk and Opportunity. There are many opportunities/risks that will be too low a level for consideration at the enterprise review board. It is envisioned that sub - risk and opportunity boards can be established or data from existing boards can be escalated as appropriate to the NextGen level. This means that the criteria for enterprise level managed risks needs to be clearly established and only those situations that satisfy this criteria are handled at the enterprise level. A useful analogy is found in Configuration Management best practices. Changes handled at the enterprise Configuration Change Board (CCB) satisfy specific change criteria ("Class I changes"). Any change not satisfying this criteria is de-escalated to the appropriate sub-board or organization for consideration ("Class II changes") rather than being managed at the enterprise level.

All active new and high risks at the enterprise level are compiled by the enterprise risk executive function and presented monthly to the Enterprise Risk Board (ERB). All new opportunities that meet enterprise investment criteria (established by the enterprise participant organizations) are also presented to the ERB. The ERB reviews the recommended actions for performance & implementation opportunities/risks and provides appropriate guidance. The membership of this board should be at a level in the participating organizations that can commit that organization to both internal implementation of Risk Board decisions and commitments to outside stakeholders.

A recommended priority list for enterprise risks are also presented by the Enterprise Risk Manager to the Enterprise Risk Board for concurrence. The agreed upon guidance and priority list (top 10 in rank order) is recorded in the enterprise risk database and shared with all participants and stakeholders through an ERM portal. The criteria for establishing the priority list for both opportunities and risks should be agreed upon in advance by the ERB and maintained in the Enterprise Risk Management Plan.

The Enterprise Risk Board assigns the organizational RAA for mitigating each risk on the enterprise risk priority list. Risk mitigation status is reported to the Enterprise Risk Board monthly, at which time the ERB provides any additional guidance to the implementing organization(s). This information is also used by the board to determine the ongoing enterprise risk priorities.

Products and Tools.

NextGen enterprise risk information is managed through a risk tool suite capable being deployed across the enterprise organizations. Products to be produced by this tool suite are defined in the Enterprise Risk Management Plan. This includes content, format, frequency, etc. for each product.

A central enterprise risk database should be established and maintained by the enterprise risk executive function within the lead integration organization. The database should reflect all active enterprise risks that are the responsibility of a given participating organization to include description, impacts, current status, history, decisions (including rationale) actions taken, and organizational responsibilities assigned. Links to risk repositories maintained by other

organizations should be established over time in accordance with the deployment strategy agreed upon by the enterprise participating organizations. A historical archive of all risks considered during the life of the enterprise should be maintained. The single authoritative source for all enterprise risk information and decisions should be the Master Enterprise Risk Database.

Risk information should also be integrated into an information portal as shown in Figure 5. This portal can either be integrated into or complementary to the Management Visibility System used by the enterprise. In any case, it should contain current and sufficient relevant information to be the single authoritative source for risks and opportunities across the enterprise for the partners and stakeholders.

Baseline deployment should address a core capability within the lead integration organization, with expansion beyond the lead integrator as shown in Figure 6.

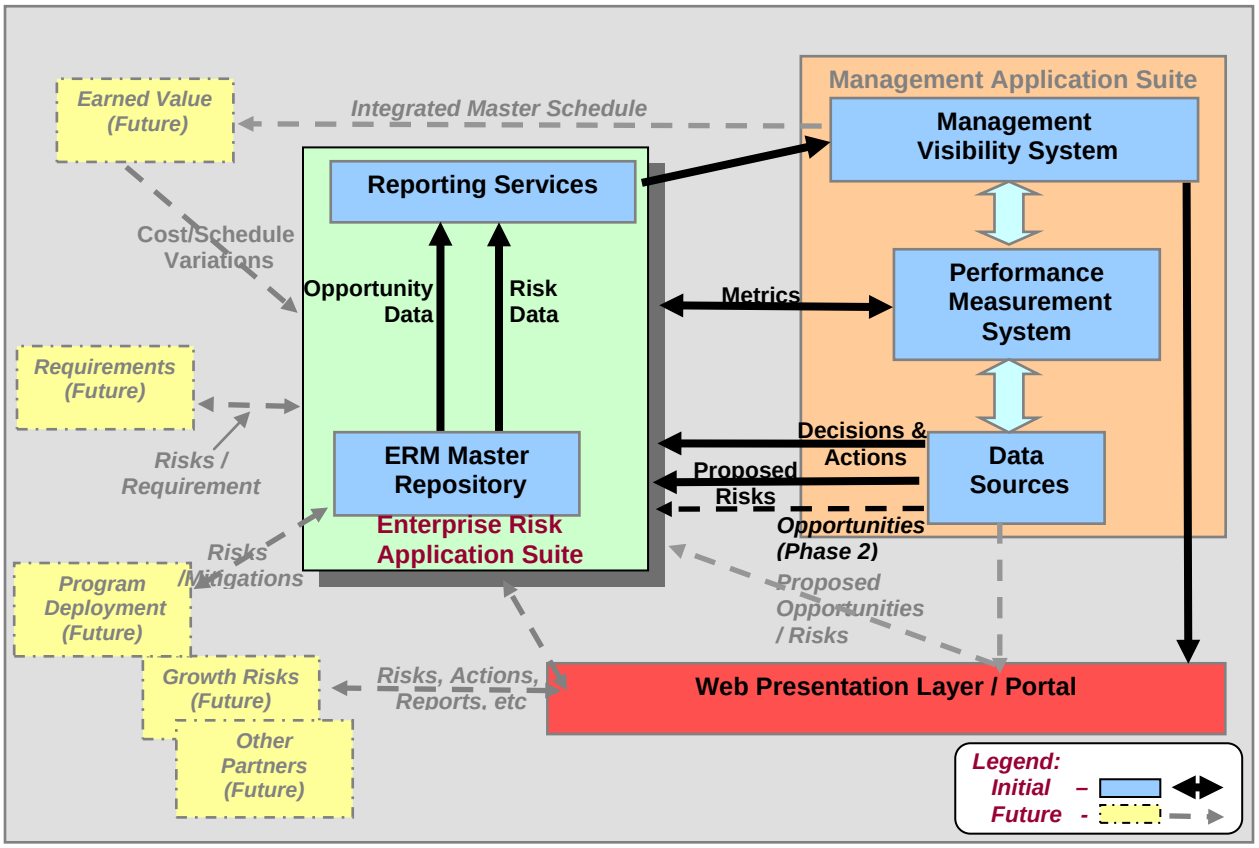

Figure 6 – ERM Tool Suite IT Integration

Training & Workforce Competencies.

A comprehensive training program should be established to provide role based training. This will range from an overview awareness course through in-depth practitioner workshops. It should take advantage of current training delivery mechanisms ranging from face to face classroom instruction through distance learning opportunities or self teaching materials.

Training should be conducted on an enterprise-specific basis as well as integrated into the appropriate existing training opportunities within the enterprise organizations.

Based on organizational needs and workforce competency plans, this training is useful as the basis for establishing measurement of Enterprise Risk Management skill levels, such as through third party certification.

Deployment.

The deployment of enterprise risk management should be staged over a 24 to 36 month period to ensure that the participating organizations and functions achieve an appropriate level of maturity to allow them to improve their overall performance.

The initial phase provides enterprise risk capability within the lead integrator. The objective of this phase is to provide the basic infrastructure to support enterprise decision making at the existing board level(s) shown in Figure 5. This deployment includes a risk management IT capability that supports all risk process functions from risk register handling to the creation of risk adjusted business plans.

The 2nd phase builds on the lessons learned from the initial effort to include opportunities as well as risks. This phase is aimed at supporting the same infrastructure and level of NextGen decision making as the initial deployment.

Subsequent phases extend this capability to include other enterprise organizations and implementation programs, as well selected outside stakeholders. A detailed plan and deployment schedule should be developed by the lead integrator to coordinate the planning, investment, and deployment of the enterprise risk capability to match deployment of the SoS solution.

Conclusions.

Deploying a system to address risk & opportunity in a Systems of Systems context entails more than simply buying a software application and distributing some reports with red, yellow, and green grids. The unprecedented level of complexity and degree of networking complicates enterprise-level decision making. This level of complexity, both in the solution space and at the organizational level, demands a more robust approach to risk and opportunity management than has traditionally been considered. In addition, all the facets outlined in this paper are required to provide a robust ERM presence that effectively serves the needs for decision making in this environment. Close attention must be paid to the organizational dimension since different organizations make decisions differently, and not always consistently. The issue of organizational cultures, the extent of disparity across the participating organizations, and energy necessary to integrate them into a homogeneous community cannot be ignored or underestimated. Combine that with the outside environment that the SoS enterprise partners and participants live in seriously constrains the alternatives available for a successful outcome.

Author Biography. Ken Kepchar is the Chief Systems Engineer for Integration and Information System Security within the NextGen Integration Office of the FAA Air Traffic

Organization. In this position, he is a member of the FAA Technical Review Board, which is the technical arm of the NAS Enterprise Architecture Board. He is the lead instructor for System Engineering, Risk Management, and Information System Security for System Engineers within the FAA. Ken has over 40 years of technical experience in the aviation industry, 25 of those years in management.

Ken has held numerous positions at the Chapter and International levels of the International Council of Systems Engineering (INCOSE). He has served on the INCOSE Board of Directors and recently as the initial Program manager and Chair of the Certification Advisory Group for the INCOSE Certified System Engineering Professional (CSEP) program.

Ken holds a B.S. (Aeronautics and Astronautics) from the Massachusetts Institute of Technology and an M.S. (Engineering Management) from the University of Missouri – Rolla. Ken is an INCOSE Expert System Engineering Professional (ESEP) and a registered Certified Information System Security Professional (CISSP).