From:	JR3 Consulting, LLC
To:	aiframework
Subject:	Response to RFI: Artificial Intelligence Risk Management Framework
Date:	Tuesday, August 10, 2021 1:40:07 PM
Attachments:	RM5 Method of risk management 02152021.doc AI RMF RFI Response JR3 Consulting.xlsx

---

Greetings:

Please see the attached response on the NIST-provided template (Item 10 only). As explanatory material for the response, I've also attached supporting research on a novel (journal-published) risk management framework which may benefit The Institute. The research was conducted while I supported the US Army as a contractor and was updated while I was a Professor of Digital Engineering at the Defense Acquisition University.

Thank you for the opportunity to provide feedback from industry on this important topic.

Regards,
John Rice

John Rice, President and Owner
JR3 Consulting, LLC

-
https://www.linkedin.com/in/jr3consulting

Adaptation of Organizational Models To Systems Engineering and Risk Management

John F. Rice

JR3 Consulting, LLC, Huntsville, AL 35758

ABSTRACT

Prominent tools for assessing and managing risk include Risk Matrices, Risk Burndown charts and Automated Risk Management software. They are generally lacking, however, in accommodating ideation and brainstorming to identify potential problems. A suggested approach for improving the process is to apply strategic management models -- many of which are directly applicable and adaptable to Systems Engineering. This paper presents traditional risk tools and introduces a complementary management model tailored to the identification, scoring and tracking of potential program issues. Additional management models are presented for further investigation and adaptation.

Key words: risk, management, model

1.0 INTRODUCTION

For decades management theorists have compared corporate organizations to 'systems'. [1] In the mid-1960s, Optner described organizational systems as follows: "A system is here defined as a set of objects together with relationships between the objects and between their attributes related to each other and to their environment so as to form a whole." [2]

Jenkins' definition of a system is a complex grouping of human beings and machines for which there is an overall objective. Extending these concepts to Systems Engineering (SE), Hall saw SE as "operating in the space between research and business, assuming the attitudes of both." [3]

Furthermore, typical SE models such as Work Breakdown Structures, Functional Flow Block Diagrams, and Risk Matrices are analogous to organizational hierarchies, enterprise flowcharts, and uncertainty matrices, respectively.

2.0 TRADITIONAL RISK MANAGEMENT

The topic addressed herein is the adaptation of a strategic management tool to model risk as part of a structured Systems Engineering (SE) process. Traditional Risk Management (RM) models have included Risk Matrices (Figure 1), Risk Burndown charts (Figure 2), and automated RM tools. By tailoring the management tool for RM, the Systems Engineer has another "tool in the toolbox" to perform the risk function or to complement existing methods.

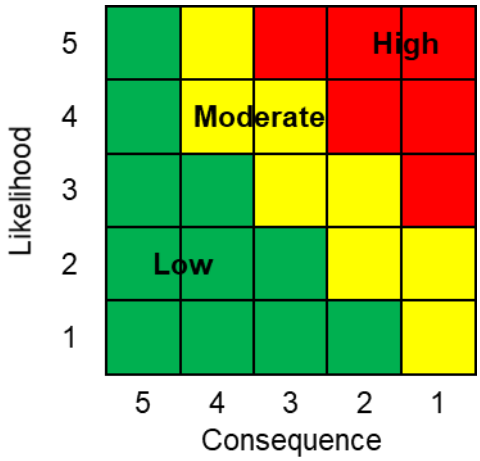

Figure 1. Risk Matrix [4]

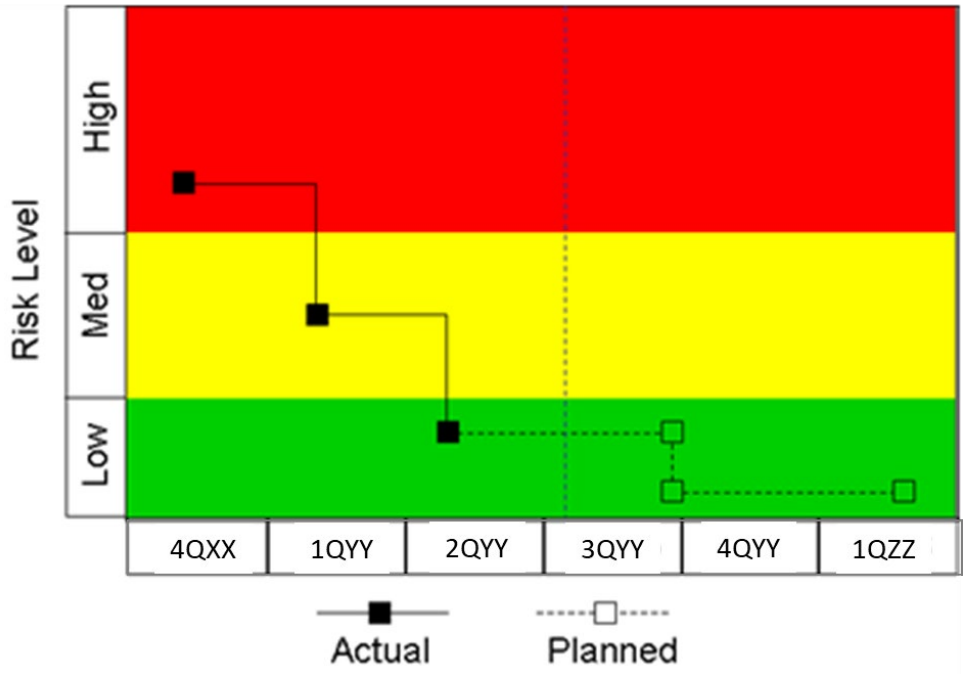

Figure 2. Risk Burndown Chart [4]

3.0 FIVE FORCES MODEL

The strategic management model of interest is known as the Five Forces model. [4] Its originator is Dr. Michael Porter, Harvard University Business School professor, who developed the tool for competitive advantage analysis within specific industries. [Other

management tools adaptable to Risk Management / Systems Engineering functions are described under 7.0 ADDITIONAL MODELS].

As shown in Figure 3, the center block depicts intensity of rivalry among industry competitors. The external forces – new entrants, bargaining power of buyers and suppliers, and substitutes – are shown as the threats acting on the industry.

4.0 ADAPTATION TO RISK MANAGEMENT

Adapting the 5 Forces model to RM involves replacing intra-industry rivalries and competitive threats with the following risk "forces":

- Internal organization
- Industry
- Information
- Infrastructure
- Influences

Internal organization risks include enterprise functions such as task sharing, personnel loads, cross training, assignment duration, and related parameters. Industry risks are associated with contractor and subcontractor organizations, product maturity and support, contractual matters, and so forth.

Information risks include software availability and functionality, information system backup, network security, and the like. Infrastructure refers to physical security, communications networks, event recovery, safety, and related issues. Influences include external demands (e.g. meetings, travel), senior leadership support, policy mandates, and similar risks.

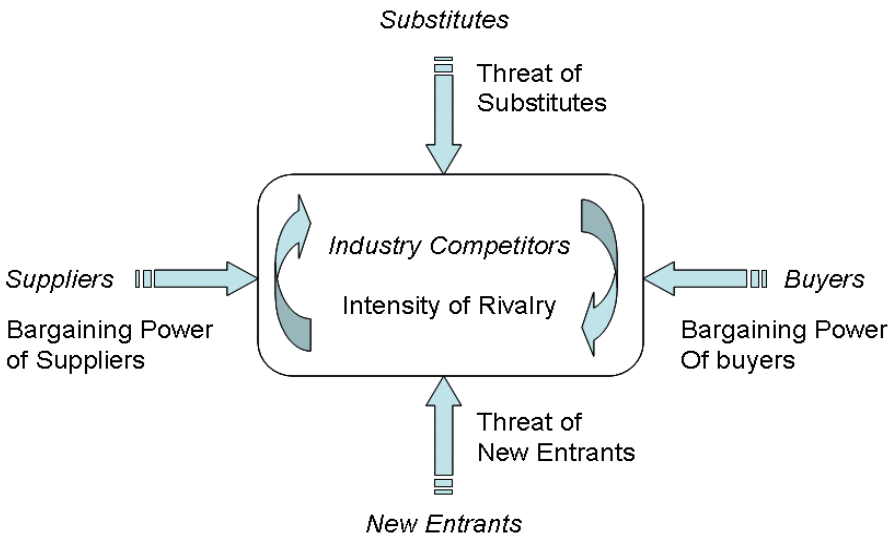

Figure 3. Porter's Five Forces Model

It should be noted that the tailoring of Porter's model to this application involves more than a change in nomenclature. It requires a change of perspective from an industry view to an enterprise view. Additionally, the perspective should be defined at a particular management level to be valid. And the forces are no longer competitive in nature, but risk-related.

The RM version of the Five Forces model, hereafter called *RM5*, has numerous benefits including the ability to:

- perform 'back of the envelope' cursory analyses,
- promote and capture brainstorming among groups,
- document the identification of potential risks from the brainstorm session,
- categorize the risks into one of the five I's,
- measure the impact of each risk using a consensus scoring approach, and
- track risk trends through comparison of historical versions.

The author initially utilized *RM5* to assess risk for a US Army program. As shown in Figure 4, each of the I's was examined for candidate risks such as contractor (Industry), communications (Information), budget (Influences), personnel (Internal), and system risks (Infrastructure).

The identification of risks is generated from subject matter experts, experienced systems engineers, and brainstorm sessions. Initially, some of the submitted risks may be of low significance or relevance. Through iterative reviews, the candidates can be critiqued and validated.

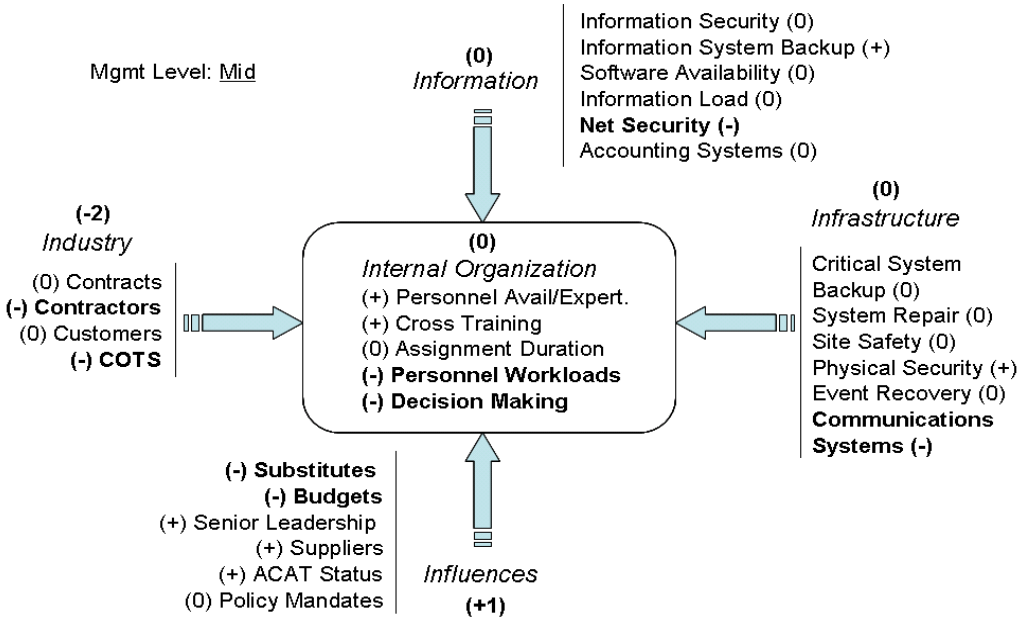

Figure 4. RM5 Model

Scoring and weighting of risks are also features of *RM5*. Scoring is performed in a manner similar to Porter's model where +, 0 and – are used to indicate a positive, neutral, or negative condition. In risk terminology, this is stated as a positive trend, unlikely / unknown risk, or negative trend.

Weighting can be applied by assigning multiple notations (e.g. + +) based on consensus or expertise, or through numerical methods such as regression analysis. Using chronological versions of the model, a trend analysis can be performed and plotted as curves, Gantt charts or similar illustration.

5.0 MODEL RESULTS

For the noted project, risks pertaining to the Internal Organization's performance are:

- Personnel Availability
- Personnel Expertise
- Cross Training
- Assignment Duration
- Personnel Workloads
- Decision Making

Project risks pertaining to Information handling, processing and storage are:

- Information Security
- Information System Backup
- Software Availability
- Information Load
- Net Security
- Accounting Systems

Those risks involving Industry forces include:

- Contracts
- Contractor organization
- Customer organization
- COTS[1] Market Risks

Risks related to external Influences consist of:

- Program/Product Substitutes
- Budgets
- Senior Leadership Support
- Suppliers

[1] Commercial Off The Shelf (Non-Developmental)

- ACAT[2] Status
- Policy Mandates

and Infrastructure risks include:

- Critical System Backup
- System Repair
- Site Safety
- Physical Security
- Event Recovery
- Communications Systems

For illustration, *hypothetical* scores (+, 0, -) have been assigned and tallied where + is a +1, 0 is zero, and – is a -1. Summing these values for each category yields a cumulative numerical risk. For example, Industry's composite score is -2 which indicates a relative degree of risk resulting from contractor performance and COTS products. Conversely, the other categories are neutral or favorable in comparison, as shown by their composite scores.

Composite scores could be totaled strictly as minuses to highlight the degree of negative risk. In this case, the results would be:

Internal Organization (-2)
Information (-1)
Industry (-2)
Influences (-2)
Infrastructure (-1)

As a consequence, it can be shown that all categories have some degree of risk and those items could be targeted for mitigation. The risks for either approach could be weighted to underscore their importance.

6.0 OTHER MODEL USES

Other uses for the model include applying it specifically to identification of existing, rather than projected, program issues. This could provide managers a snapshot of information that would otherwise escape attention and provide them with the insight to head off problems. Likewise, *RM5* could be used to identify strengths or opportunities which were previously unrecognized and could support or provide visibility to a program.

In all of the above cases, the potential for cost savings or revenue generation is apparent since reducing risks or capturing opportunities are means to improving the bottom line.

[2] Acquisition Category used by the Department of Defense to prioritize programs

Furthermore, having a model to complement existing SE tools provides an additional decision aid to validate current assumptions or to promote ideation for new process / product development.

7.0 ADDITIONAL MODELS

Other management tools adaptable to Risk Management or Systems Engineering functions include, but are not limited to,:

- SWOT analysis for requirements development;[5]
- Gap analysis for trade studies;[6] and
- Value Chain analysis for determining value added from technical processes.[7]

SWOT (Figure 5) -- Strengths, Weaknesses, Opportunities, and Threats -- can be performed by compiling a list of organizational attributes applied to each of these categories. This allows management to determine where resources need to be allocated to either shore up or scale back attributes to optimize program performance. For example, the strength of market demand for a product could be impacted by production bottlenecks or limitations. A remediation opportunity could be outsourcing the production, although a negative outcome of that action may be reduced quality.

Strengths	Weaknesses	Opportunities	Threats
Subject matter experts	Insufficient funding	Contract personnel	Budget cuts
Certified processes	Process software outdated	Develop S/W internally	International stds
Market demand	Production limitations	Outsource production	Loss in quality

Figure 5. SWOT Analysis

Gap analysis (Figure 6) employs a two-axis, four-quadrant graphic depicting variables of interest to the systems engineer. Variables could be metrics relating to cost, schedule and performance, for example; however, the axes are not restricted to specific categories. The systems engineer determines what is of value or interest.

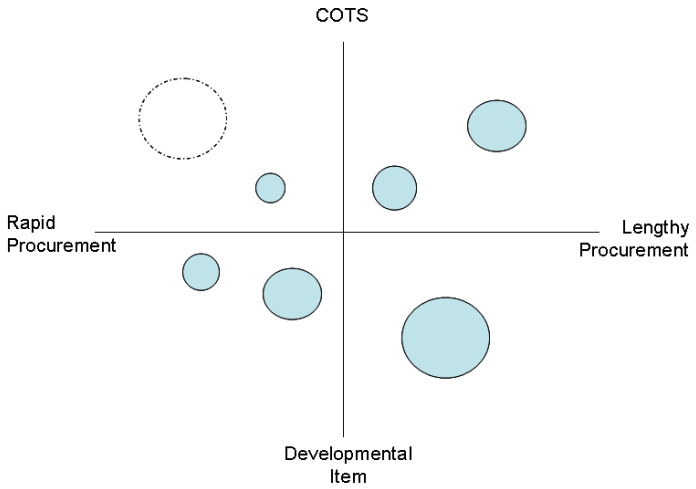

Figure 6. Gap Map

The space is populated to show occurrences of the variables or lack thereof. Should a particular quadrant, for example, be void of data points, this could be an indication of an opportunity or perhaps a deficiency in the enterprise. To demonstrate the scale of an occurrence, symbols (e.g. circle) are sized accordingly. For instance, if many COTS systems were identified in a quadrant, the size of the symbol would be indicative. Conversely, few occurrences would be represented as a small symbol. Finally, an opportunity or deficiency could be shown as a dashed, unfilled symbol -- scaled to show the magnitude of the gap.

Finally, Value Chain analysis (Figure 7) illustrates the functions performed to create a product or service, with a margin depicted to highlight the value added for the customer. This would be a useful model for trade studies to represent alternative approaches and determine which produces the greatest margin or best value.

Figure 7. Value Chain

The elements of the value chain are defined as follows: [7]

"Firm infrastructure – Support of entire value chain, such as general management, planning, finance, accounting, legal services, government affairs, and quality management.

Human resource management – Recruiting, hiring, training, and development.

Technology development – Improving product and manufacturing process.

Procurement – Function or purchasing input.

Inbound logistics – Materials receiving, storing and distribution to manufacturing premises.

Operations – Transforming inputs into finished products.

Outbound logistics – Storing and distributing products.

Marketing and sales – Promotion and sales force.

Service – Service to maintain or enhance product value."

8.0 CONCLUSION

The multidisciplinary aspects of strategic management tools lend themselves to other uses, when adapted appropriately. This paper focused on one tool to present this approach as it pertains to risk management. However, it is apparent from the other models presented that the overlap between strategic management and systems engineering yields opportunities for similar analyses. Expanding this approach to other disciplines including Systems Engineering Management; System Integration; Configuration Management; Data Management; Reliability, Maintainability and Testability; System Safety; Human Factors Engineering (HFE); Test and Evaluation; and Integrated Logistic Support (ILS) would be professionally and academically valuable.

ACKNOWLEDGMENTS

The author would also like to thank The University of Alabama in Huntsville, School of Administrative Science, for introducing business models in the Management of Technology graduate degree program.

REFERENCES

1. BERTALANFFY, L. (1968), The *Origin of General Systems Theory*, American Association for the Advancement of Science.
2. COMPONATION, P., (2004), *Systems Engineering Overview*, The University of Alabama in Huntsville.
3. CHECKLAND, P. (1993), *Systems Thinking, Systems Practice*, Wiley.
4. Risk Management Guide for DoD Acquisition 2003 (Fifth Edition, Version 2.0), < http://www.dau.mil/pubs/gdbks/risk_management.asp>, April 5, 2005
5. ROBBINS, S., MARY COULTER (1996), *Management*, pp. 264-265, Prentice Hall.
6. CRAWFORD, C. MERLE (1997), New Products Management, pp. 480-481, Irwin/McGraw-Hill.
7. PORTER, MICHAEL E., VICTOR E. MILLAR, "How Information Gives You Competitive Advantage," *Harvard Business Review*, July-August 1985, pg. 151.

John Rice is the owner and president of JR3 Consulting, LLC in Huntsville, Alabama. Mr. Rice's subject matter knowledge was developed through thirty-two years of systems engineering, project management and business development experience. He worked for the Department of Defense as a civilian employee with the Defense Acquisition University and with the Missile Defense Agency. Prior to Government service, he was employed by Teledyne Brown Engineering, Jacobs Engineering, Tyco International and Wyle Laboratories. The specific topic of risk management is an area he researched and applied in a systems engineering position for a US Army program. Mr. Rice holds a BS degree in Mechanical Engineering from Auburn University and a MS degree in Management of Technology from The University of Alabama in Huntsville (UAH).

All comments will be made public as-is, with no edits information, otherwise sensitive or prote

Comment Template for Responses to NIST Artifical Intelligence Risk Management Framework

General RFI Topics (Use as many lines as you like)	**Response #**	**Responding organization**	**Responder's name**	**Paper Section (if applicable)**
Please see item 10 below for suggested framework				
Responses to Specific Request for information (pages 11,12, 13 and 14 of the RFI)				

1. The greatest challenges in improving how AI actors manage AI-related risks – where “manage” means identify, assess, prioritize, respond to, or communicate those risks;				
2. How organizations currently define and manage characteristics of AI trustworthiness and whether there are important characteristics which should be considered in the Framework besides: accuracy, explainability and interpretability, reliability, privacy, robustness, safety, security (resilience), and mitigation of harmful bias, or harmful outcomes from misuse of the AI;				

3. How organizations currently define and manage principles of AI trustworthiness and whether there are important principles which should be considered in the Framework besides: transparency, fairness, and accountability;				
4. The extent to which AI risks are incorporated into different organizations' overarching enterprise risk management – including, but not limited to, the management of risks related to cybersecurity, privacy, and safety;				
5. Standards, frameworks, models, methodologies, tools, guidelines and best practices, and principles to identify, assess, prioritize, mitigate, or communicate AI risk and whether any currently meet the minimum attributes described above;				

6. How current regulatory or regulatory reporting requirements (e.g., local, state, national, international) relate to the use of AI standards, frameworks, models, methodologies, tools, guidelines and best practices, and principles;				
7. AI risk management standards, frameworks, models, methodologies, tools, guidelines and best practices, principles, and practices which NIST should consider to ensure that the AI RMF aligns with and supports other efforts;				

8. How organizations take into account benefits and issues related to inclusiveness in AI design, development, use and evaluation – and how AI design and development may be carried out in a way that reduces or manages the risk of potential negative impact on individuals, groups, and society.				
9. The appropriateness of the attributes NIST has developed for the AI Risk Management Framework. (See above, “AI RMF Development and Attributes”);				

10. Effective ways to structure the Framework to achieve the desired goals, including, but not limited to, integrating AI risk management processes with organizational processes for developing products and services for better outcomes in terms of trustworthiness and management of AI risks. Respondents are asked to identify any current models which would be effective. These could include – but are not limited to – the NIST Cybersecurity Framework or Privacy Framework, which focus on outcomes, functions, categories and subcategories and also offer options for developing profiles reflecting current and desired approaches as well as tiers to describe degree of framework implementation; and	1	JR3 Consulting, LLC	John Rice	

11. How the Framework could be developed to advance the recruitment, hiring, development, and retention of a knowledgeable and skilled workforce necessary to perform AI-related functions within organizations.				
12. The extent to which the Framework should include governance issues, including but not limited to make up of design and development teams, monitoring and evaluation, and grievance and redress.				

or redactions. Please be careful to not include confidential business or personal ected information, or any information you do not wish to be posted.

Submit comments by August 19, 2021:

Response/Comment (Include rationale)	Suggested change

Suggestion for structuring the framework based on individual's novel risk management framework while supporting the Army, then NASA, and subsequently the DoD at large. Risk framework was topic of publication in DoD's Acquisition Research Journal, topic of invited presentation at the Defense Manufacturing Conference, and oft-reviewed and cited article at ResearchGate.net.	Recommend a cursory review of subject research for application to AI. It is provided as an email attachment with this template. Includes minor updates to the original 2010 publication. **Figure 4, in particular, is the subject of the paper and should summarize the topic.**

