Risk Management and Methodologies

A Survey of PMI, FARES, and FRAAP

Andrew Bruce, CISSP, FITSP, PMP
CTO, RiVidium Corporation (http://www.rividium.com/)
andy.bruce@rividium.com
21 February 2011

Topic Summary:

- Relate risk management to business objectives and information security
- Identify components of risk management and how they support management decision makers
- Contrast selected risk assessment methodologies

Table of Contents

Illustration Index

About the Author

Andrew Bruce is Chief Technical Officer for RiVidium Incorporated, a Service Disabled Veteran Owned Small Business in the suburban Washington, DC area. RiVidium provides professional services to the Federal Government and the Department of Defense, specializing in customizing and developing architecture and governance models that leverage our proprietary technologies. Mr. Bruce's job responsibilities include: working directly with customers and partners for new business development, supporting proposal efforts, overseeing RiVidium's network infrastructure, working with project managers to ensure project completion, managing software development efforts throughout the entire system life-cycle, and leading new technology research and proofs-of-concept. After a career spanning decades in shrink-wrap, commercial, and corporate software development, Mr. Bruce is focusing on Information Assurance to achieve his goal of building and managing large data centers providing cloud computing utility services for commercial and Government customers.

1.0 Introduction

Companies thrive based on the results of their business decisions: from headliners (*invest in cloud computing or upgrade servers?*); to managerial (*add resources to an executing project?*); to operational (*is it time to replace disk drives within our servers?*). Correct and secure information assets provide the foundation for all of these decisions, and senior management must be able to demonstrate their fiduciary responsibility in protecting these assets. This white paper analyzes three Risk Management (RM) methodologies that can be used to:

- Identify and classify information assets and their vulnerabilities;
- Prioritize threats to those assets; and,
- Apply cost-effective controls to reduce risks to those assets to acceptable levels.

By providing a firm information foundation upon which decision-makers at every level in the company can depend, RM helps to ensure that each business decision is made using the best data possible.

2.0 Risk Management Principles

Defining the term “risk” turns out to be somewhat problematic, as these different definitions show:

- *Dictionary* – “possibility of loss or injury.”[1]
- *Project Management Institute (PMI)* - “an uncertain event or condition that, if it occurs, has an effect [***positive or negative***][2] on at least one…objective” (PMI 2008).
- *National Institute of Standards and Technology (NIST)* – “a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that

[1] Source: Merriam-Webster online dictionary (http://www.merriam-webster.com/dictionary/risk).

[2] Addition by the author.

would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence" (NIST 2010).

For the purposes of this white paper, risk is interpreted as the probability of a positive or negative event or condition occurring and the impact that such an occurrence would have on an organization. However, all three of the above definitions agree on the common themes of *uncertainty* and *harm*. All decisions involve some element of risk. Most individual everyday decisions involve relatively small risk that can easily be accepted (for example, driving to work versus taking the bus). Managing organizational risk requires a more formal approach even where an organization has a very high *utility function*, or its willingness to accept risk (Moneim).[3] This section provides a brief introduction to the components of and the support provided by an RM program.

2.1 Components

NIST (2010) defines Risk Management as a having four basic components:

- *Framing*: The way an entity views threats, vulnerabilities, and consequences.
- *Assessment*: How an entity identifies and prioritizes threats, vulnerabilities, and their impact.
- *Response*: How best to handle identified risks; this typically includes acceptance, transference, or mitigation.
- *Monitoring*: Detecting that a risk has materialized and activating the correct response.

Specific RM strategies differ in their approaches but always address these core components.

2.2 Support for the Enterprise

Decision makers use RM to satisfy two primary needs: providing information security and enabling business objectives to be met cost-effectively. Information security is a fundamental business requirement today to comply both with Government laws and regulations as well as with industry-specific standards. As an example, the recent Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH) adds significant information processing requirements to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), including *downstream liability*. Downstream liability means that organizations which process Electronic Personal Health Information (ePHI) are liable not only for their own data and system management processes, but also for that of any organizations with which they share or provide ePHI.

In this environment, executive management must have a sound RM program to demonstrate fiduciary responsibility In the author's own organization, the RM program must show that risks have been identified (including indirect risks like downstream liability) and that appropriate mitigating controls have been implemented.[4]

[3] Dr. Moneim quantifies the *utility function* as a mathematical construct based on rate of change relative to money (the independent variable).

[4] Source: Personal interview, Chief Operations Officer, February 3, 2011.

3.0 Risk Management Techniques

This white paper surveys three RM techniques:

- PMI's Project Risk Management
- FARES - Forensic Analysis of Risks in Enterprise Systems
- FRAAP - Facilitated Risk Analysis and Assessment Process

3.1 PMI's Project Risk Management

3.1.1 Overview

As a leader in effective project management, PMI[5] recognizes the importance that RM plays in delivering quality results. PMI encourages its members and practitioners to understand and to apply RM as defined within the Project Management Body of Knowledge (PMBOK®). As with all PMI disciplines, effective planning ensures a successful RM program; fully five of the six PMI RM processes deal exclusively with planning.

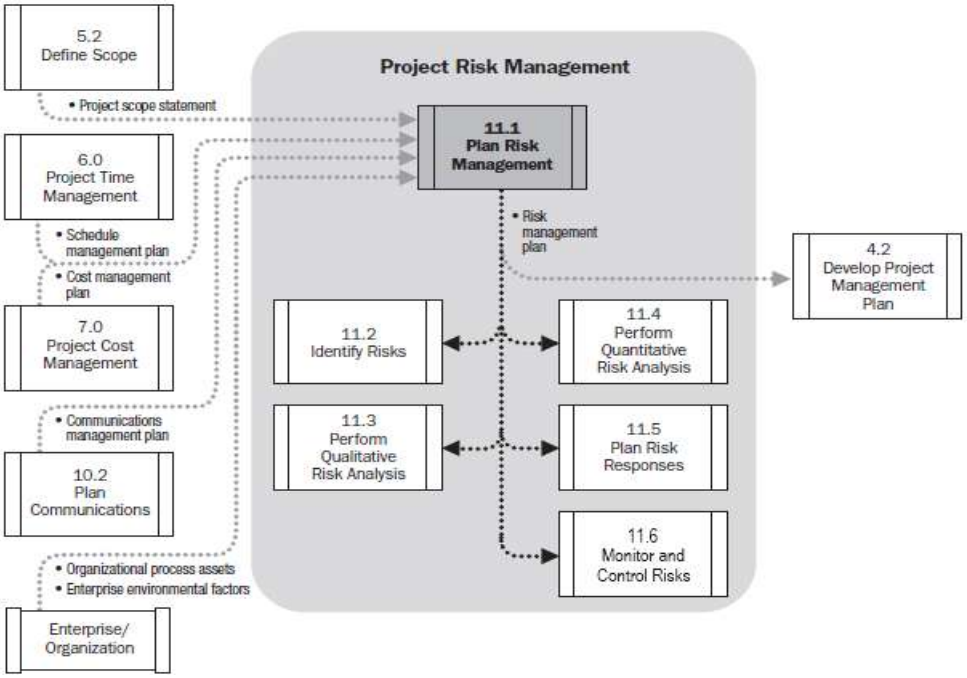

Figure 1: PMI Risk Management[6]

The PMI model differs from others in that risks can be positive ("opportunities"). All risks must be managed using the approaches outlined in the sections below.

[5] The reader may refer to http://www.pmi.org/ for more information regarding the PMI.

[6] NIST 2010, p 277 (slightly modified by the author for this paper).

3.1.2 Approach

PMI's RM approach uses an artifact-focused set of processes:

1. *Plan Risk Management*. The organization must establish its risk tolerance and establish risk assessment boundaries by using the "iron triangle" of scope, time, and cost. Communication is a critical success factor for any project: all stakeholders need to understand the risks and must be kept properly informed when a risk materializes. This results in an RM plan that specifies overall risk categories and permits risks to be added or removed from the project via integrated change control processes.
2. *Identify Risks*. This iterative process occurs at the beginning of any project and continues throughout the project lifecycle. Risk managers use a variety of tools and techniques to identify risks: reviewing and monitoring project documentation, performing interviews, researching historical information, and so on. Identified risks are then stored within a "risk register," which serves as the primary RM resource.
3. *Perform Qualitative and Quantitative Analyses*. Qualitative analysis assigns priority ratings to identified risks, while quantitative analysis assigns estimated monetary values (generally an expensive effort). Practitioners must be aware that results from these analyses can be used only as guides and must be reevaluated as a project progresses.
4. *Plan Risk Responses*. PMI defines eight possible risk responses based on the type of risk (positive or negative). Negative risks might include computer failures or physical break-ins and responses include:
    - *Acceptance.* Taking no action to prevent or mitigate the risk.
    - *Transference*. Assigning risk responsibility to a third-party.
    - *Mitigation*. Implementing a control to reduce the risk level.
    - *Avoidance.* Pursuing an alternative solution.

    Positive risks might include a project finishing earlier than expected or falling costs of commodities and responses include:

    - *Exploitation.* Taking action to ensure that the opportunity occurs.
    - *Sharing.* Including a third-party to help exploit the opportunity.
    - *Enhancement*. Taking action to improve the chances for the opportunity to occur.
    - *Acceptance.* Acknowledging the opportunity but not taking direct action to enhance or to exploit it.
5. *Monitor and Control Risks*. This ongoing process uses the risk register to detect and to respond to materialized risks ("issues" is the PMI term). This process also works continuously to identify new or changed risks and to update the risk register accordingly.

3.1.3 Summary

The PMI approach emphasizes up-front planning and documentation-based risk assessment to identify and to manage risks. Risk is best mitigated by *avoidance*, and the assumption is always that a meaningful monetary value can be applied to a particular risk if a qualitative analysis warrants that added effort. Organizations rely on contingency funds to address accepted risks and on "management reserve" funds to address unknown risks as

they materialize. The author's own organization uses this approach for its risk assessment and reserve funding.[7]

This approach works quite well for risks that can reliably be forecasted (such as natural disasters or certain types of system risks). As other RM approaches demonstrate, however, responding to malicious risks using the PMI model can be more problematic.

3.2 FARES

3.2.1 Overview

Dr. Peter Stephenson developed the idea for FARES in 2004 as a reaction to two significant problems he observed within traditional RM. First, qualitative and quantitative analyses are inherently subjective and produce unreliable results; such as, the infamously inaccurate "annual loss expectancy" values from Federal Information Processing Standard (FIPS) Publication 65. Second, most risk assessments can identify only known vulnerabilities. As an alternative, Stephenson posited that the same techniques used in forensic analysis to identify and to correct problems after they have occurred could also be used as an effective RM technique.

Stephenson defines risk thusly: "vulnerabilities, the credible threats that could exploit them in a particular environment, the impacts caused by such a successful exploitation, and the countermeasures used to mitigate the impact" (Stephenson 2009, p 570). By explicitly identifying both vulnerabilities and countermeasures as risk components, he lays the groundwork for his objection to current RM as well as his alternative approach.

3.2.2 Approach

FARES identifies three types of threats: natural, malicious, and system. Natural threats are handled by using governmental publications for a geographic area to identify the threats (storms, flooding, and so on) and then taking appropriate action (purchasing insurance, building to code, and so on). System threats are handled similarly by using specifications and trade studies to establish the mean time between equipment failure and then ensuring that an appropriate repair / replace plan is implemented (along with training and procedures to prevent human errors). In both cases, the PMI dollar-based RM approach works well to mitigate risk.

Where FARES distinguishes itself is in regard to the second type of threat: malicious events. Stephenson identifies six types of "threat factors" that relate to a malicious threat agent:

- *capability* (knowledge and means to perform the attack);
- *motivation* (desire to perform the attack);
- *access* (logical or physical proximity to initiate the attack);
- *catalyst* (event that sparks an attack);
- *inhibitors* (controls that prevent or mitigate an attack); and,
- *amplifiers* (vulnerabilities that enable or expand an attack).

The first four threat factors apply primarily to *threat agents*; defenders must discover these agents to implement proactive defenses. The last two threat factors, however, are under direct control of the defending entity and define an organization's "hardness" in the face of an attack.

[7] Source: Personal interview, Chief Operations Officer, February 3, 2011.

Traditional vulnerability analyses rely upon assessing the results of controlled attacks against targeted vulnerabilities (such as buffer overruns or malformed communication packets), thus making these analyses "vulnerability-centric." FARES takes a different approach and applies standard incident post-mortem analysis to vulnerability assessment. By the simple expedient of hypothesizing that an incident of a given "class" has occurred, a FARES assessment analyzes how the enterprise is protected against that entire class of risk (thus making FARES "risk-centric"). Organizations realize cost savings by avoiding the need to perform specific vulnerability tests for every threat falling under a given risk class. Stephenson recommends the use of the Common Criteria Profiling Knowledge Base (CC-PBK) to define the threat classes as shown below:

CC-PKB General Threats

1. Administrative errors of commission
2. Administrative errors of omission
3. Hostile administrator modi cation of user or system data
4. Administrator violates user privacy policy
5. A critical system component fails
6. Software containing security-related a ws
7. Failure of a distributed system component
8. Hacker undetected system access
9. Hacker attempts resource denial of service
10. Hacker eavesdrops on user data communications
11. Cryptanalysis for theft of information
12. Hacker masquerading as a legitimate user or as system process
13. Message content modi cation
14. Exploitation of vulnerabilities in the physical environment of the system
15. Social engineering
16. Malicious code exploitation
17. Unexpected disruption of system or component power
18. Recipient denies receiving information
19. Sender denies sending information
20. A participant denies performing a transaction
21. Legitimate system services are spoofed
22. Hostile user acts cause con dentiality breaches
23. User abuses authorization to collect data
24. User errors cause con dentiality breaches
25. User error makes data inaccessible
26. User errors cause integrity breaches
27. User errors undermine the system's security features
28. User's misuse causes denial of service
29. User abuses authorization to modify data
30. User abuses authorization to send data

Figure 2: CC-PKB General Threats[8]

By analyzing an information system's capabilities and distributing them between these risk classes, Stephenson believes that the organization both understands its risk factors better and reduces the overall cost of future risk

[8] Stephenson 2009, p 572.

assessments.

Colored Petri Net (CPNet)

No discussion of FARES would be complete without mentioning the CPNet model, as it is fundamental to FARES' forensic analysis roots. In forensic analysis, an incident is examined and its root causes are traced back to underlying vulnerabilities; in effect, threat pathways are identified. Stephenson has broad experience in this field and uses the CPNet technology to model these pathways, as shown below in a CPNet examining the SQL Slammer worm from 2003:

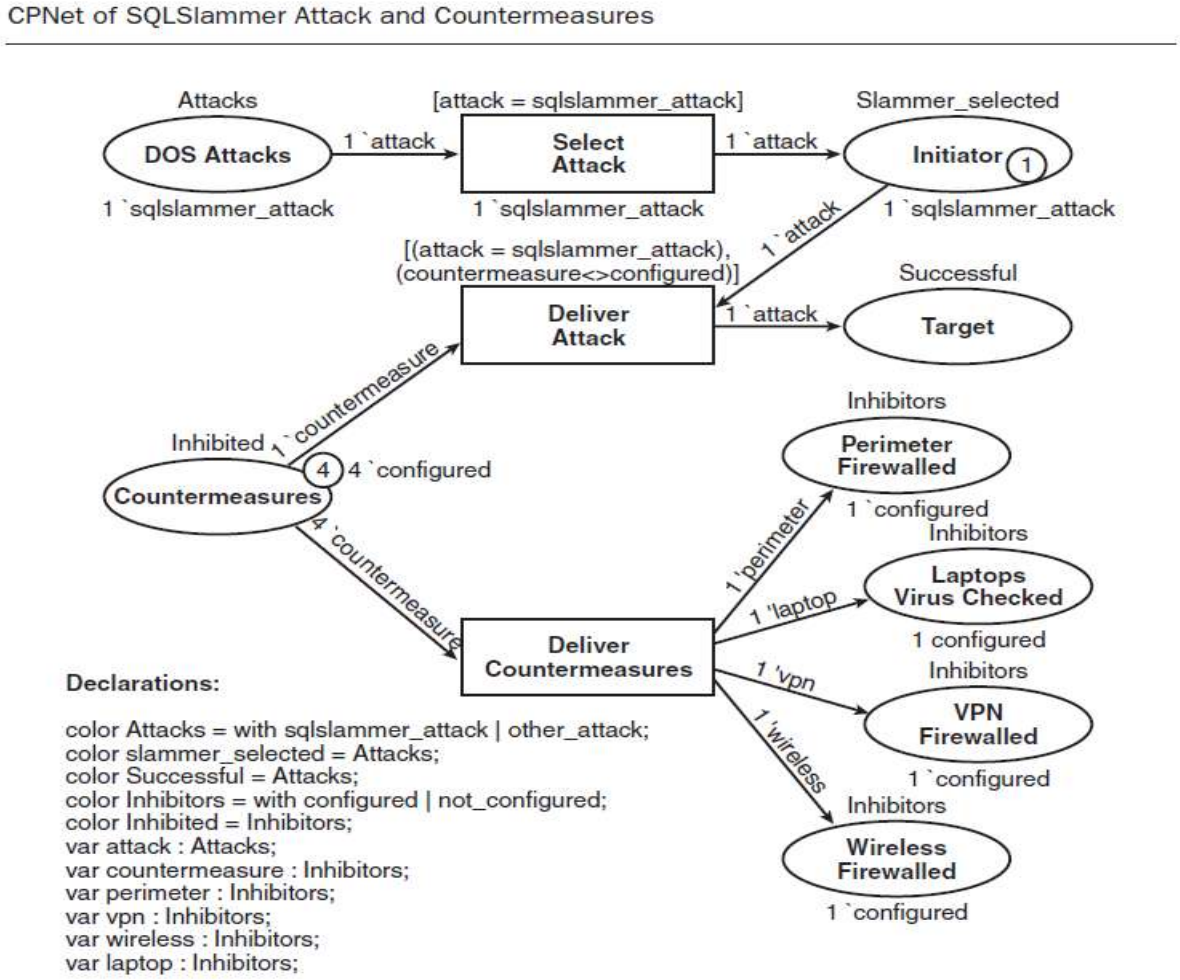

Figure 3: CPNet for SQL Slammer[9]

FARES states that by implementing inhibitor controls to close pathways to identified vulnerabilities, threat agents can be neutralized.

[9] Stephenson 2009, p 571.

3.2.3 Summary

FARES attempts to provide a next-generation RM model based on the concepts of discovering root causes of risk (basic vulnerabilities within systems) and addressing those causes by implementing inhibiting controls along a threat pathway. This provides true defense-in-depth, and cost savings can be achieved by: 1) applying only those controls necessary to prevent credible threats; and, 2) brute-force vulnerability / penetration testing no longer becomes necessary because the root vulnerabilities have already been mitigated. Stephenson bases his claims on his research into the relative failures of traditional qualitative and quantitative risk assessments. While still an experimental RM approach, FARES offers an intriguing and "risk-centric" focus that merits review from the RM practitioner.

3.3 FRAAP

3.3.1 Overview

Thomas Peltier's FRAAP is a proven and cost-aware RM methodology that recognizes the importance of using in-house subject matter experts (SMEs) led by a facilitator trained in FRAAP. (If possible, this facilitator is provided by the organization's own Project Management Office [PMO]). FRAAP also addresses the fact that risk assessments must compete for scarce time and personnel resources by emphasizing the following characteristics:

- *Focused.* Specific lines-of-business with well-defined scope boundaries are targeted.
- *Planned.* As in PMI's approach, up-front planning results in a predictable and successful outcome.
- *Phased*. Analyses are broken into pre-FRAAP, FRAAP, and post-FRAAP sessions with well-defined deliverables.
- *Optimizing.* Over time, organizations accumulate previous FRAAP results into a library to inform and improve future FRAAPs.

FRAAP works to prevent risk assessments from failing by monitoring scope creep, ensuring that SMEs are part of the process, and verifying that implemented controls always tie back to business objectives.

3.3.2 Planning and Pre-FRAAP

FRAAP lays emphasis on protecting information, which in turn leads to differentiating between the data Owner, the data Custodian, and the data User. Owners classify data and define / monitor safeguards; they are ultimately responsible for the confidentiality, integrity, and availability of the data. Custodians implement the defined safeguards on behalf of the Owner; the owner retains *accountability* while the Custodian assumes *responsibility* for the data. Users are the authorized entities which access the data; they must abide by the classification and access controls defined by the Owner and enforced by the Custodian. This tripartite relationship reinforces the need for thorough planning and for well-defined data management policies and standards.

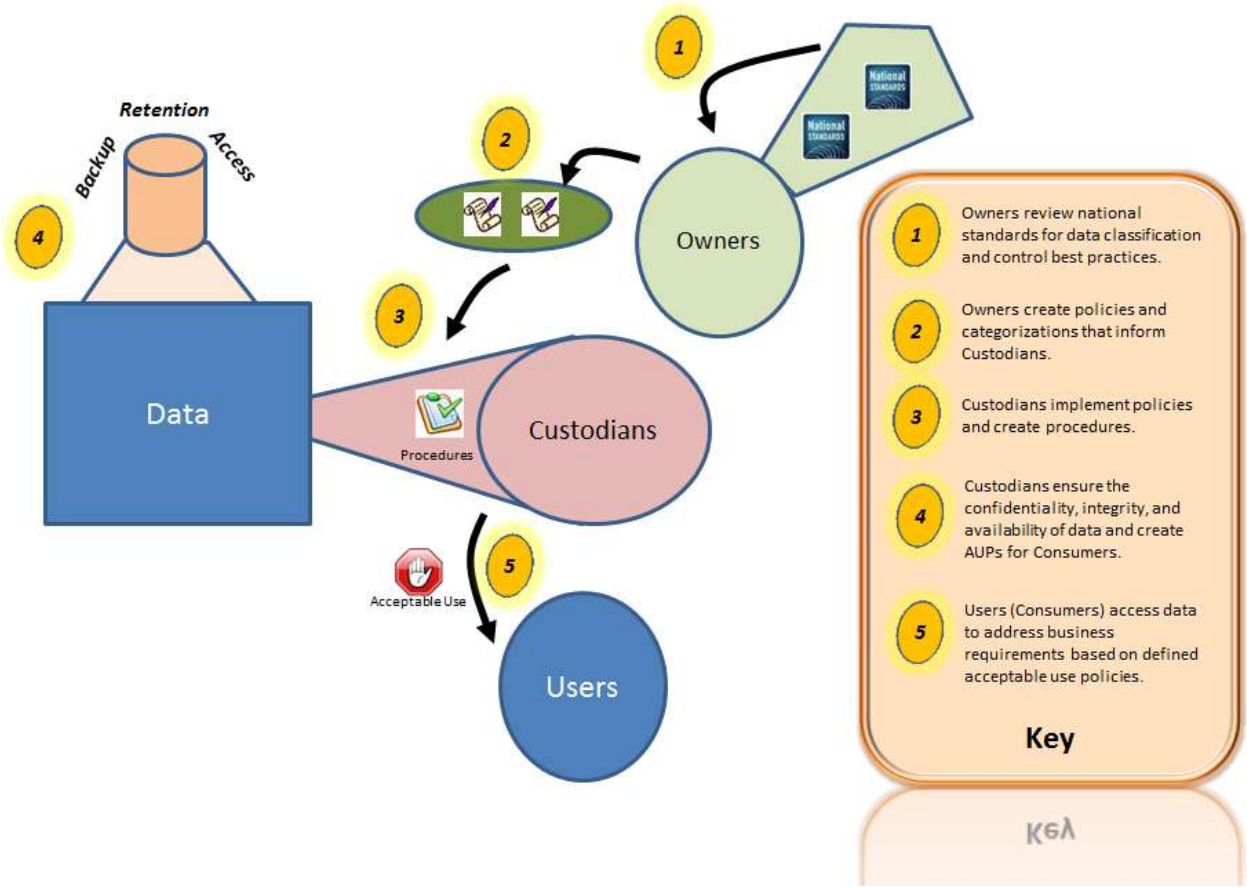

Figure 4: Tripartite relationship of Owners, Custodians, and Users[10]

The pre-FRAAP session concentrates on the facilitator working directly with the data Owner to determine the following outputs for the area or project to be assessed: overall organizational business goals; the scope of the risk assessment; time and budget constraints; and, administrative and documentation requirements. Most importantly, the pre-FRAAP session identifies the participants for the main FRAAP session. These participants must have sufficient expertise to identify and to understand relevant threats, and to provide the feedback necessary for the risk assessment to be complete.

3.3.3 The FRAAP Session

The FRAAP session involves the facilitator working with the identified FRAAP participants in a relatively short session (generally no more than four hours total, although this time may be lengthened based on the client's requirements). The session agenda is created ahead of time and identifies the area to be assessed. All FRAAP participants are involved in the session, and all ideas are recorded. In contrast to the FARES process, FRAAP actively encourages the use of qualitative risk assessments. While functional managers and SMEs may incorrectly estimate a risk's organizational impact (Stephenson's complaint against the approach), they remain the organization's best judges of this impact.

[10] Drawing by the author.

The FRAAP session is broken into two stages: the first stage (which includes all participants) performs the actual risk assessment based on the agenda, while the second stage uses a subset of the participants to summarize the results. During the first stage, appropriate controls are selected based on qualitative assessments made for each identified threat. Peltier (2009) advocates the use of a probability / impact matrix to perform this assessment as shown below:

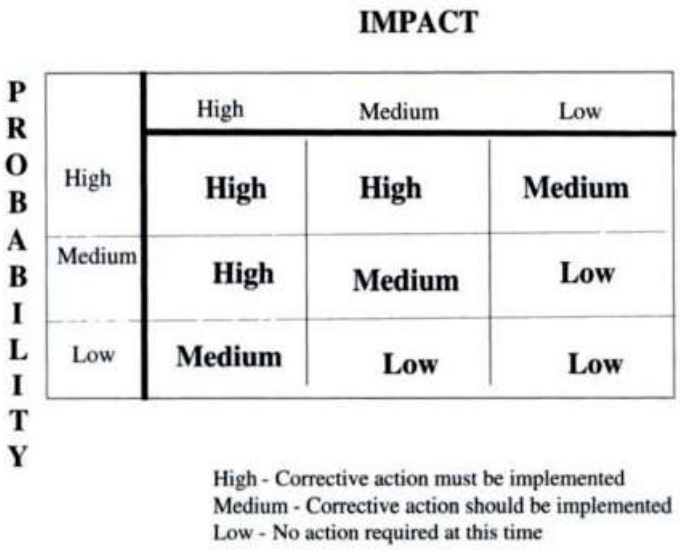

Figure 5: FRAAP Risk Level Matrix[11]

Controls identified during the FRAAP session are also numbered and stored for cross-reference to the FRAAP Worksheet that captures all of the analysis performed during the FRAAP session.

[11] Stephenson 2009, p 534 (updated by the author based on Peltier's later models).

3.3.4 Post-FRAAP and Execution

FRAAP sessions generate an Action Plan that identifies each threat, the controls that can mitigate the threat, the qualitative risk level of the threat, the control selection approach, a time frame, and a responsible party as shown below:

FRAAP Action Plan Example 1 (Management Accepts Risks)

Threat Number	*Risk Level*	*Owner Selected Action*	*Responsible Group*	*Due Date*	*Additional Comments*
1	B	ACF2 has been implemented and access controls list will be reviewed to identify authorized users.	Owner and IP	Accept risk	Management has determined that accepting the risk is in the best interest of the organization.

FRAAP Action Plan Example 2 (Control Requires Vulnerability Assessments)

Threat Number	*Risk Level*	*Owner Selected Action*	*Responsible Group*	*Due Date*	*Additional Comments*
2	B	Change management procedures already in place.	Operations	Complete	Change management process needs to be reviewed to determine if it is meeting the needs of the organization. A vulnerability assessment is suggested.

Figure 6: FRAAP Action Plan[12]

The Action Plan enables management to execute upon the risk assessment findings. To aid in this goal, a Management Summary Report provides: a list of FRAAP participants; the bounding assessment scope; the completed Action Plan; and, a summary report. One additional high-value deliverable is the Cross-reference Report that groups related threats by risk level; for cost-benefit analysis, these are the controls that provide the best overall value to the organization. This completed Management Summary Report can be stored for future reference.

3.3.5 Prescreening and Optimization

The outputs from previous FRAAP sessions aid an organization in optimizing future risk assessments. Over time, common sets of baseline controls emerge that can be applied unchanged if new or changed projects share characteristics with assessments that have already been performed. By building a set of questionnaires that data owners can answer before the pre-FRAAP meeting, an organization can identify whether a full FRAAP is necessary; this can help organizations control costs.

3.3.6 Summary

As a goal-oriented and quantifiable RM methodology, FRAAP concentrates on leveraging the assets and expertise that an organization already has in place. With its straightforward approach concentrating on allocating scarce resources for the best return on investment, FRAAP presents a compelling model both for RM practitioners and for business executives. Its documentation-oriented approach addresses the fact that "risk analysis and risk assessment processes will generally be used twice. The first time will be when decisions are made…[t]he other time…will be…when a problem arises and the organization must show the process it used to reach the decisions that it did" (Peltier 2009, p 59). FRAAP provides a solid foundation for both occasions.

[12] Stephenson 2009, p 551 (slightly modified by the author for this paper).

4.0 Summary and Recommendations

This paper provided a high-level view of three major RM approaches. Of the three, FARES is the more experimental while FRAAP and PMI have been implemented extensively. The PMI approach appears best suited for managing risks that lend themselves to qualitative *and* quantitative analysis (natural and certain systemic risks), while FRAAP emphasizes that RM must occur in a cost-conscious business environment with significant constraints on time and personnel resources.

Of the three approaches, FRAAP lends itself best to the author's own organization based on three factors:

1. *In-house.* FRAAP's emphasis on using in-house SMEs ensures that as new projects arise, the organization does not need to invest in expensive consultants.
2. *Cost-effective.* FRAAP assists in defining standard baseline controls can be applied to new projects as long as a simple questionnaire establishes that the technology meets existing analyzed criteria.
3. *Time-conscious.* Projects inevitably expand to fill all the time allotted to them and risk assessments are no exception. FRAAP's structured schedule and quantifiable deliverables help to create executable results quickly and reliably.

Regardless of the approach used, an organization's selected RM methodology provides the foundation for successful decision-making. Without an effective RM program, an organization simply cannot demonstrate true due diligence when problems arise and investigations are imminent.

5.0 Acronyms and Abbreviations

CC-PKB	Common Criteria Profiling Knowledge Base
CPNet	Colored Petri Net
ePHI	Electronic Personal Health Information
FARES	Forensic Analysis of Risks in Enterprise Systems
FIPS	Federal Information Processing Standards
FRAAP	Facilitated Risk Analysis and Assessment Process
HIPAA	Health Insurance Portability and Accountability Act of 1996
HITECH	Health Information Technology for Economic and Clinical Health Act of 2009
NIST	National Institute of Standards and Technology
PMI	Project Management Institute
PMBOK®	Project Management Body of Knowledge
PMO	Project Management Office
RM	Risk Management
SME	Subject Matter Expert

Reference List

Moneim, AFA. [date unknown]. A Mathematical Model for the Utility Function in Problems of Decision Analysis [Internet]. [place unknown]; [cited January 21, 2011]. Available from http://ahmedfarouk.net/images/UtilityFn.pdf.

NIST. 2010. Special Publication 800-39: Integrated Enterprise-Wide Risk Management [Internet]. Gaithersburg (MD) [cited January 31, 2011]. Available from http://csrc.nist.gov/publications/drafts/800-39/draft-SP800-39-FPD.pdf. 86 p.

Peltier, TR. 2009. How to Complete a Risk Assessment in 5 Days or Less. Boca Raton (FL): Auerbach Publications. p 57–66.

PMI. 2008. A Guide to the Project Management Body of Knowledge (PMBOK® Fourth Edition). Newtown Square, PA. 497 p.

Stephenson, PR, editor. 2009. Information Security Essentials: Section 3. Auerbach Publishing, ISBN 978-1-4398-0030-0. 684 p.