Risk Management on Enterprise Architecture and System Integration

Eric Tse

Abstract

This paper highlights and consolidates interesting risk management topics for enterprise information systems from enterprise architect and system integration perspectives.

We first highlight concepts of

- Advanced risk modelling
- Enterprise architecture

and how these two disciplines are related. Afterwards, we will consolidate all the common risk factors people have identified for enterprise architecture and system integration.

Finally, we get a case study of how people use one of the models, HHM, National Institute of Standards and Technology, and Project Management Body of Knowledge (PMBOK) to manage their enterprise architecture in modern times.

Implementing and deriving a quantitative model for information systems is out of scope, but hopefully we will provide bits and pieces to people who want to develop something handy from this paper.

Introduction

During the last two decades, enterprises utilize information technology for their business. There are many system integration projects involved and after the projects there are lots of operation and ongoing support work.

As the whole enterprise involves a lot of different technologies, different people, different infrastructure and many other factors, managing it becoming very complex. Risk management on our enterprise architecture is one of the big topics enterprise architectures and executive should care about.

There have been pragmatic guidelines for helping IT professional manage risks to their systems, but there are not many formal quantitative methodologies of how people should manage their risk. Also this is the highest bird eye view of risk management of technology. It consists of a lot of human and social factors from the whole enterprise and IT professional may not see them in a black and white way.

This paper will try to collect bits and pieces of different components, such as:

- Complex models for risk management
- Enterprise architecture principles and highlights
- Identify common risks for enterprise and system integration projects
- Existing frameworks on what people are doing in the industry

We hope people can utilize the paper as a starting point to develop further sophisticated quantitative models, or even software for enterprise architecture risk management.

Advanced Methodology of Risk Modelling

We will first layout the principles and models for risk management. The purpose here is that enterprise architecture risk management is complex and we need some building blocks to give us foundations.

Second, instead of just giving some pragmatic guidelines, we want to provide some theoretical depth to the discussion, for the sake of people who want to develop models from our bit and pieces of information.

Why risk modelling is complex?

Three fundamental reasons for the complexity of risk modeling [4].

- One is that decision making under uncertainty literally encompasses every facet, dimension and aspect of our lives. It affects us at the personal, corporate and government levels. It also affects us during the planning, development, design, operation, and management phases.
- The second reason risk based decision making is complex is that it is cross disciplinary. The subject has been further complicated by the development of diverse approaches of varying reliability. Some methods, which on occasion produce fallacious results and conclusions, have become entrenched and will be hard to eradicate.
- The third reason is grounded on the need to make trade-offs among all relevant and important cost, benefits, and risks in a multi-object framework, without assignment weights with which to commensurate risks costs and benefits.

We will discuss why enterprise architecture modelling needs this complex concepts later - after we discuss what enterprise architecture is.

Different modelling tools and concepts

We are going to introduce some advanced concepts of risk modelling. We are not going to derive our enterprise architecture risk management models from them in this paper but hopefully it would provide some useful information for people who are interested. We would introduce some example how people are using it in information system in later chapters

- Haimes [1981] [10] introduced **hierarchical holographic modelling (HHM)** to clarify, understand , model and document not only multiple components, objects, and constraints of a system, but also its welter of social aspects (functional, temporal, geographical, economic, political, legal, environmental, sector, institutional, etc.)
- Zigler [1984][5] introduced **Multifaceted Modelling and Discrete Event Simulation.** The term multifaceted to denote an approach to modelling which recognizes the existence of multiplicities of objects and models as a fact of life.
- Systems Engineering [Sage 1992][6]. (Identify several phases of the systems engineering life cycle and embedded in such analyses are the multiple

perspectives (structural definition , the functional definition and the purposeful definition)

1.2 SYSTEM ENGINEERING
1. Define and generalize the needs
2. Determine objectives, goals, performance criteria and purpose
3. Consider the total problem environment
4. Study the interactions in the environment
5. Incorporate multiple models and synthesize
6. Solve models
7. evaluate various feasible solutions
8. Evaluate solutions in the short and long term
9. Communicate the solution to the client
10. Evaluates the impact of current decisions on future options.

- Warfield [1976][8] societal systems and complexity
- Singh [1987][7] multiple volumes of the systems and control encyclopaedia: theory technology applications on modelling large scale and complex systems. Multifaceted modelling, meta systems, hierarchical holographic modelling and other contributions in the field of large scale systems.

Enterprise Architecture + System Integration

What is Enterprise Architecture? [2]

> *"Enterprise Architecture is about understanding all of the different elements that go to make up the enterprise and how those elements inter-relate". (From The Open Group)*
>
> *"Enterprise Architecture is a strategic information asset base, which defines the business mission, the information necessary to perform the mission, the technologies necessary to perform the mission, and the transitional processes for implementing new technologies in response to the changing mission needs. (USA Federal CIO Council)*

Some of the critical success factors for enterprise architectures are

- Reduce risk and prepare the enterprise for rapid unplanned change.
- Avoid the pitfalls of business-unit IT functions operating at odds with one another

Why Enterprise Architecture Risk Management is complex?

Enterprise architecture involves every facet, dimension and aspect of the enterprise. It affects everyone at the personal, corporate levels, and it also affects system integrations during the planning, development, design, operation, and management phases.

The second reason is that risk based decision making is complex in that it is cross disciplinary. Enterprise architecture involves thousands of solution architecture(s), software, applications, hardware, network, databases, middle-wares etc, business processes, operations, line of businesses, support, projects, departments, politics, etc.

The third reason is grounded on the need to make trade-offs among all relevant and important cost, benefits, and risks in a multi-object framework, without assignment weights with which to commensurate risks costs and benefits.

Identify Risk Factors in enterprise architecture and system integration

Mary Summer's paper [1] has identified many risk factors. When we do our architecture assessment or system integration, we have to bare those in mind. We are going to summarize it in two tables.

Summary of risk factors in IS projects

Risk factor	Issue
Organizational fit	Organizational environment (resource insufficiency and extent of changes) (Block, 1983; Borki *et al*., 1983) [13][14] Changing scope and objectives (Keil *et al*., 1998)[18]
Skill mix	Lack of technical expertise (Ewusi-Mensah, 1997)[16] Lack of application knowledge (Barki, *et al*., 1993; Ewusi-Mensah, 1997) [14] [16] Inappropriate staf. ng and personnel shortfalls (Block, 1983; Boehm, 1991; Keil *et al*., 1998) [13][15][18]
Management structure and strategy	Lack of agreement on project goals (Block, 1983; Ewusi-Mensah, 1997) [13][16] Lack of senior management involvement (Ewusi-Mensah, 1997; Keil *et al*., 1998) [16][18]
Software systems design	Misunderstanding requirements and changes in requirements (Block, 1983; Boehm, 1991; Cash *et al*., 1992; Keil *et al*., 1998) [13][15][18] Lack of an effective methodology, poor estimation and failure to perform the activities needed (Block, 1983; Keil *et al*., 1998) [13][18]
User involvement and training	Lack of user commitment and ineffective communications with users (Block, 1983; Keil *et al*., 1988) [13][18] Conflicts between user departments (Keil *et al*., 1998) [18]

Risk factor	Issue
Technology planning	Lack of adequate technology infrastructure (Ewusi-Mensah, 1997) [16] Technological newness, strained technical capabilities and failure of technology to meet speci. cations (Block, 1983; Boehm, 1991; Cash *et al*., 1992; Barki *et al*., 1993) [13][15][14] Application complexity (technical complexity) (Barki *et al*., 1993) [14]
Project management	Unrealistic schedules and budgets (Boehm, 1991) [15] People and personality failures, lack of effort, antagonistic attitudes and people clashes (Block, 1983) [13] Lack of measurement system for controlling risk and inadequate project management and tracking (Block, 1983; Ewusi-Mensah, 1997) [13][16]
Social commitment	Inability to recognize problems. a tendency to keep pouring resources into a failed project and unrealistic expectations (Ginzberg, 1981; Willcocks and Margetts, 1994; Keil and Montealegre, 2000) [17][20][19]

Risk category	Risk factor
Organizational fit	Failure to redesign business processes Failure to follow an enterprise-wide design which supports data integration
Skill mix	Insufficient training and re-skilling Insufficient internal expertise Lack of business analysts with business and technology knowledge Failure to mix internal and external expertise effectively Lack of ability to recruit and retain qualified ERP systems developers
Management structure and strategy	Lack of senior management support Lack of proper management control structure Lack of a champion Ineffective communications

Risk category	Risk factor
Software systems design	Failure to adhere to standardized specifications which the software supports Lack of integration
User involvement and training	Insufficient training of end-users Ineffective communications Lack of full-time commitment of customers to project management and project activities Lack of sensitivity to user resistance Failure to emphasize reporting
Technology planning/integration	Inability to avoid technological bottlenecks Attempting to build bridges to legacy applications

Existing Enterprise Architecture Risk Management Best Practices

This section provides some examples of how people do risk management in enterprise architecture environment. Some of them use the models we describe earlier.

Application of HHM in enterprise information system

Thomas A. Longstaff utilizes the hierarchical holographic modelling framework we mentioned earlier, which promotes a systemic process for assessing risk to critical infrastructures. [12]

The hierarchical holographic modelling framework is used to identify the source of software risks in systems integration. Each of the seven visions addresses multiple categories of risk sources. Although not shown, there are many couplings and interdependencies among these categories and among individual risk sources.

Switching perspectives in the HHM framework. In (a), the sources of risk to software quality are the primary concern. Of secondary concern are the sources of risk in the environmental vision. In (b), the perspectives are switched. The HHM provides the flexibility to see the system from many perspectives, which lets analysts see the myriad factors that can affect risk sources in a particular perspective or category.

Recommendations of the National Institute of Standards and Technology

National Institute of Standards and Technology (NIST) provides a very comprehensive risk management guide for information technology systems. We are going to highlights some of the interesting parts. [21]

These standards didn't address a lot of the risk modelling. However it addresses many risk management aspect specific to information technology enterprise infrastructure. We can see are trying to bridge the gap between high level risk management methodology and enterprise architecture, on the other hand we are trying to bridge the gap between enterprise architecture, and risk modelling. These set of standards focus of the methodology.

As you can see the following tables mainly classify things into System Development Life Cycle and security risks. Basically we can say one is during the system is being developed. The second is after the system is developed, and is operational.

For development risk management, the (NIST) uses a phase approach or linear process approach to partition the risk management. The methodology flow chart has a strong reference to the system engineering process we talked about in the earlier chapter.

After the system is developed, NIST talk about risk management in the operational maintenance phase of the enterprise architecture. They focus the risk management on security. I think their main concern is security threat. I also think they didn't spend a lot of time describe other risks like system failure, functional, performance, integrity, compliance which are very important and many of them can get political.

Based on my experience, one of the challenges of an enterprise system after it is set up is the system has some functional defects during operation time or causing outage. Since the system is cross disciplinary, none of the experts have enough knowledge to determine where the problems are. Since the impact of IT system failure can cause millions of dollars lost, no one would like to bear responsibility. Instead of accepting the problem, people from different department point fingers at each other, saying this is the other person's problems. You can see 30 people on a phone call with several directors, just to solve one technical problem. With good operational and compliance process, we hope we can mitigate this kind of situation to a minimum.

Integration of Risk Management into the SDLC

SDLC Phases	Phase Characteristics	Support from Risk Management Activities
Phase 1 Initiation	The need for an IT system is expressed and the purpose and scope of the IT system is documented	Identified risks are used to support the development of the system requirements, including security requirements, and a security concept of operations (strategy)
Phase 2 Development or Acquisition	The IT system is designed, purchased, programmed, developed, or otherwise constructed	The risks identified during this phase can be used to support the security analyses of the IT system that may lead to architecture and design tradeoffs during system development

SDLC Phases	Phase Characteristics	Support from Risk Management Activities
Phase 3 Implementation	The system security features should be configured, enabled, tested, and verified	The risks identified during this phase can be used to support the security analyses of the IT system that may lead to architecture and design tradeoffs during system development
Phase 4 Operation or Maintenance	The system performs its functions. Typically the system is being modified on an ongoing basis through the addition of hardware and software and by changes to organizational processes, policies, and procedures	Risk management activities are performed for periodic system reauthorization (or reaccreditation) or whenever major changes are made to an IT system in its operational, production environment (e.g. new system interfaces)
Phase 5 Disposal	This phase may involve the disposition of information, hardware, and software. Activities may include moving, archiving, discarding, or destroying information and sanitizing the hardware and software	Risk management activities are performed for system components that will be disposed of or replaced to ensure that the hardware and software are properly disposed of, that residual data is appropriately handled, and that system migration is conducted in a secure and systematic manner

Risk Assessment Methodology Flowchart

Risk Assessment Activities	Input	Output
Step 1. System Characterization	• Hardware • Software • System interfaces • Data and information • People • System mission	• System Boundary • System Functions • System and Data Criticality • System and Data Sensitivity
Step 2. Vulnerability Identification	• Reports from prior risk assessments • Any audit comments • Security requirements • Security test results	List of Potential Vulnerabilities
Step 3. Threat Identification	• History of system attack • Data from intelligence agencies, NIPC, OIG, FedCIRC, mass media,	Threat Statement
Step 4. Control Analysis	• Current controls • Planned controls	List of Current and Planned Controls
Step 5. Likelihood Determination	• Threat-source motivation • Threat capacity • Nature of vulnerability • Current controls	Likelihood Rating
Step 6. Impact Analysis • Loss of Integrity • Loss of Availability • Loss of Confidentiality	• Mission impact analysis • Asset criticality assessment • Data criticality • Data sensitivity	Impact Rating

Risk Assessment Activities	Input	Output
Step 7. Risk Determination	• Likelihood of threat exploitation • Magnitude of impact • Adequacy of planned or current controls	Risks and Associated Risk Levels
Step 8. Control Recommendations		Recommended Controls
Step 9. Results Documentation		

Risk Assessment Methodology Flowchart

Threat-Source	Motivation	Threat Actions
Hacker, cracker	Challenge Ego Rebellion	• Hacking • Social engineering • System intrusion, break-ins • Unauthorized system access
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	• Computer crime (e.g., cyber stalking) • Fraudulent act (e.g., replay, impersonation, interception) • Information bribery • Spoofing • System intrusion

Threat-Source	Motivation	Threat Actions
Terrorist	Blackmail Destruction Exploitation Revenge	• Bomb/Terrorism • Information warfare • System attack (e.g., distributed denial of service) • System penetration • System tampering
Industrial espionage (companies, foreign governments, other government interests)	Competitive advantage Economic espionage	• Economic exploitation • Information theft • Intrusion on personal privacy • Social engineering • System penetration • Unauthorized system access (access to classified, proprietary, and/or technology-related information)

Threat-Source	Motivation	Threat Actions
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g., data entry error, programming error)	• Assault on an employee • Blackmail • Browsing of proprietary information • Computer abuse • Fraud and theft • Information bribery • Input of falsified, corrupted data • Interception • Malicious code (e.g., virus, logic bomb, Trojan horse) • Sale of personal information • System bugs • System intrusion • System sabotage • Unauthorized system access

Risk Mitigation Action Point

Risk Mitigation Activities	Input	Output
Step 1. Prioritize Actions	Risk levels from the risk assessment report	Actions ranking from High to Low
Step 2. Evaluate Recommended Control Options • Feasibility • Effectiveness	Risk assessment report	List of possible controls

Risk Mitigation Activities	Input	Output
Step 3. Conduct Cost-Benefit Analysis • Impact of implementing • Impact of not implementing • Associated costs		Cost-benefit analysis
Step 4. Select Controls		Selected Controls
Step 5. Assign Responsibility		List of responsible persons
Step 6. Develop Safeguard Implementation Plan • Risks and Associated Risk Levels • Prioritized Actions • Recommended Controls • Selected Planned Controls • Responsible Persons • Start Date • Target Completion Date • Maintenance Requirements		Safeguard implementation plan
Step 7. Implement Selected Controls		Residual Risks

PMBOK (Project Management Body Of Knowledge Guide)

PMBOK Project Risk Management [3] includes the processes concerned with conducting risk management planning, identification, analysis, responses, and monitoring and control on a project. The objectives of Project Risk Management are to increase the probability and impact of positive events and decrease the probability and impact of events adverse to project objectives. Project Risk Management processes include:

- **Risk Management Planning** - deciding how to approach, plan, and execute the risk management activities for a project.
- **Risk Identification** - determining which risks might affect the project and documenting their characteristics.
- **Qualitative Risk Analysis** - prioritizing risks for subsequent further analysis or action by assessing and combining their probability of occurrence and impact.
- **Quantitative Risk Analysis** - numerically analysing the effect on overall project objectives of identified risks.
- **Risk Response Planning** - developing options and actions to enhance opportunities and to reduce threats to project objectives.
- **Risk Monitoring and Control** - tracking identified risks, monitoring residual risks and identifying new risks, executing risk response plans, and evaluating their effectiveness throughout the project life cycle.

From the PMBOK, you can see they recommend quantitative models like probability distributions, sensitivity analysis, expected monetary value analysis (EMV), decision tree analysis, Monte Carlo techniques, Precedence Diagramming Method (PDM).

- **Continuous Probability Distributions** represent the uncertainty in values, such as durations of schedule activities and costs of project components. Discrete distributions can be used to represent uncertain events, such as the outcome of a test or a possible scenario in a decision tree.
- **Decision Tree Analysis.** Decision tree analysis is usually structured using a decision tree diagram (Figure 11-12) that describes a situation under consideration, and the implications of each of the available choices and possible scenarios. It incorporates the cost of each available choice, the probabilities of each possible scenario, and the rewards of each alternative logical path. Solving the decision tree provides the EMV (or other measure of interest to the organization) for each alternative, when all the rewards and subsequent decisions are quantified.
- **Modelling and Simulation:** A project simulation uses a model that translates the uncertainties specified at a detailed level of the project into their potential impact on project objectives. Simulations are typically performed using the Monte Carlo technique. In a simulation, the project model is computed many times (iterated), with the input values randomized from a probability distribution function (e.g., cost of project elements or duration of schedule activities) chosen for each iteration from the probability distributions of each variable. A probability distribution (e.g., total cost or completion date) is calculated.

For risk management that is specific for enterprise architecture, there are not many in PMBOK. But based on my previous experience in the industry, Project Managers in Information Technology infrastructure treated PMBOK as one of their best practices to manage enterprise information infrastructure. Of course there are discrepancies between PMBOK high level methodologies and actual details specific of enterprise architecture, as we can see some of the literature such as Mary Summer's paper have been trying to bridge the gap.

There are many more models mentioned in the PMBOK. We would not further elaborate since the scope of this paper is to find something beyond PMBOK. We would just want to highlight the intersection of PMBOK risk management and those topics we talked about in previous section.

Discussion and Conclusion

Enterprise architecture risk management is managing the risks of all the Information Technology and relevant business processes in an enterprise. It has the highest level perspective of managing the risks in an enterprise from technology perspective. It not only identifies security threats, but also involves functionality, multi-disciplinary, multi-faceted, human, social, and political factors. We need some complex models that can take all of them into considerations.

This paper focuses 1st on introducing some complex modelling concepts, introducing what enterprise architecture is, identify many problems that people are having in their enterprise system integration projects and then some methodologies of risk management, in enterprise architecture and system integration perspectives.

We first collected some formal quantitative models and methodology for risk management in general. We collected from different resources and references about what best practices people are using nowadays in information system industry.

We can see in some cases people are using some quantitative model such as HHM in the information industry. But many of the metrics and flow are qualitative more than quantitative. In a general decision making process, those guidelines are sufficient, but we can see it doesn't utilize a lot of quantitative methodology for evaluations.

From the National Institute of Standards, we can see many handy guidelines and processes for risk management. They really look like the traditional system engineering process. The methodology they use involves two main sections. One is for development, the other one for maintenance. The development one slices things using SDLC phases, while the operation ones focus on security risks. We would like to say functional and performance risks are also as important.

Also as common practice in the Information System security management area, people do not use a lot of quantitative analysis or software tools for risk. They use templates, and professional judgment usually. This is pragmatic enough in usual situation but also means there may be marketing opportunity to develop novel enterprise architecture risk management suites.

This paper does not do a lot of product evaluation on this kind of software. Based on the evaluation section on the enterprise architecture book, there are enterprise architecture evaluation tool that take risk assessment into account. However the criteria of risk assessment we talk about is far deeper than what are described in the white paper.

For the project management body of knowledge, there are a lot of high level best practices that are applicable in any industry. They take advantage of many mathematical models - although they are not that sophisticated, but handy. They also don't have many details specific for system development but in real life many project managers took PMBOK training before or while they manage IT infrastructure.

As a starting point, the paper provides some references and resource to initiate more quantitative ways of assessing risks management in enterprise architecture. Deriving

the quantitative models for enterprise is too much of an effort for the paper and is out of scope. We hope we can provide bits and pieces for people who are interested.

On the other hand, I don't see a lot of regulations and guidelines in the enterprise architecture area that have human factors involved. This is always important. People who are working in this area are aware of them, but they are not extensively written on paper in risk evaluation models. In the first section, the models we have could cover some of the social, human aspect of risk management that is also possible to get integrated into existing methodology. Enterprise architecture risk is not only focused on security, although this is a very important factor.

There are many pieces of enterprise architecture evaluation software(s) in the industry. I am not sure how sophisticated the risk management portion of them can be, and how much utilization of the models is happening.

Nevertheless different methodologies also fail to address some of the principles, for example the system engineering processes.

One thing I would like to highlight is that we did not talk about cost management in this paper. This would also influence risk management decision critically. It can be treated as a separate topic but there are a lot of interdependencies between risk management and cost management for decision makers.

On the whole, there is a lot of good stuff scattering around. We just need people to consolidate and derive better things from there.

Reference

[1] Mary summer, 2000, Risk factors in enterprise-wide/ERP projects, Mary Sumner. Journal of Information Technology. London: Dec 2000. Vol. 15, Iss. 4; p. 317

[2] jaap schekkerman, 2006, how to survive in the jungle of enterprise architecture frameworks (Enterprise Architecture tools selection chapter 29)

[3]PMI, 2004, A Guide to the Project Management Body of knowledge, 3rd edition (PMBOK)

[4] Yacov Y. Haimes, 2005, **Risk Modeling, Assessment, and Management**

[5] Zigler, B. P, 1984, Multifaceted Modeling and Discrete Simulation, Academic Press, New York

[6] Sage, A.P. 1992, System Engineering, Wiley, New York

[7] Singh, M, G, 1987, Systems and Control Encyclopedia: Theory, Technology, Applications, Pergamon Press, New York.

[8] warfield J.N. 1976, Social Systems – Planning and Complexity, John wiley & Sons, New York

[9] Stanley Kaplan, B. John Garrick, 1980, On The Quantitative Definition of Risk

[10] YY Haimes, 1981, Hierarchical holographic modeling, IEEE Transactions on Systems, Man, and Cybernetics,

[11] John Steven, Gunnar Peterson, Introduction Management to Identity Management Risk Metrics

[12] TA Longstaff, C Chittister, R Pethia, YY Haimes, 2000, Are we forgetting the risks of information technology?

[13] Block, R. (1983) *The Politics of Projects* (Yourdon Press, Prentice-Hall, Englewood Cliff, NJ).

[14] Barki, H., Rivard, S. and Talbot, J. (1993) Toward an assessment of software development risk *Journal of Management Information Systems*, **10**(2), 203–25.

[15] Boehm, B.W. (1991) Software risk management: principles and practices. *IEEE Software*, **8**(1) 3241

[16] Ewusi-Mensah, K. (1997) Critical issues in abandoned information systems development projects. *Communications of the ACM*, **40**(9), 74–80.

[17] Ginzberg, M. I. (1981) Early diagnosis of MIS implementation failure: promising results and unanswered questions. *Management Science* **27**(4), 459–78.

[18] Keil, M., Cule, P.E., Lyytinen, K. and Schmidt, R.C. (1998) A framework for identifying software project risks. *Communications of the ACM*, **41**(11), 76–83.

[19] Keil, M. and Montealegre, R. (2000) Cutting your losses: extricating your organization when a big project goesawry. *Sloan Management Review*, **41**(3), 55–68

[20] Willcocks, L. and Margetts, H. (1994) Risk assessment and information systems. *European Journal of Information Systems*, **3**(2), 127–38.

[21] Stonebumer, Goguen and Alexis Feringa, 2004, Risk Management Guide for Information Teechnology Systems, National Institue of Standards and Technology.

The Author

Eric Tse is an international recognized expert/consultant in Enterprise Access and Identity Management Architecture Design and Implementation. He has been working with international renowned experts in information technology in many prestigious companies. He also pursues research interests in project management, financial models, application/enterprise/solution architectures, compilation technology and philosophy of science.

About Project Perfect

Project Perfect is a project management software consulting and training organisation based in Sydney Australia. Their focus is to provide organisations with the project infrastructure they need to successfully manage projects.

Project Perfect sell "Project Administrator" software, which is a tool to assist organisations better manage project risks, issues, budgets, scope, documentation planning and scheduling. They also created a technique for gathering requirements called "Method H"™, and sell software to support the technique. For more information on Project tools or Project Management visit www.projectperfect.com.au