Carnegie Mellon University
Software Engineering Institute

A Prototype Set of Cloud Adoption Risk Factors

Christopher J. Alberts

April 2021

CERT Division

http://www.sei.cmu.edu

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM21-0383

Table of Contents

List of Figures

List of Tables

1 Introduction

The adoption of cloud services as a virtual replacement for on-premises information technology (IT) assets requires a cultural shift within an organization. A key aspect of a cloud environment is the use of third-party cloud service providers (CSPs) that are responsible for managing part or all of the organization's technology environment. The move to a cloud environment provides significant benefits. For example, cloud resources can be scaled quickly, updated frequently, and widely accessed without geographic limitations. However, realizing these benefits requires organizations to adapt their risk management processes to a new operational reality.

Cloud adoption affects many business units across an organization and might change how those business units operate. Senior leaders must balance a variety of stakeholders' interests, opportunities, risks, and issues. Technology developers might want immediate access to new technologies or services. At the same time, finance managers might favor initiatives that reduce costs and provide a high return on investment. If left unchecked, these competing goals can prevent an organization from optimizing its investment in cloud computing.

In some organizations, managers of business units have the authority to charter cloud initiatives based on the needs of their particular units. Here, a cloud initiative might align with a business unit's parochial goals. If these local benefits do not align with the organization's business strategy and goals, the overall organization might not achieve the benefits that senior management desires. This misalignment of organization and business-unit goals, and the lack of a coordinated governance, can put cloud adoption at risk.

A variety of organizational and technical factors can adversely affect an organization's cloud initiative. Organizational factors include an insufficient organizational cloud strategy, ill-defined organizational roles and responsibilities, insufficient technical skill set, and poor change management practices. Technical factors include inadequate architecture and design; poor integration of on-premises and cloud technologies; and cloud service that lack needed agility, availability, and security properties.

1.1 Report Scope

The Software Engineering Institute (SEI) recently chartered a study to identify risk factors that can adversely affect an organization's adoption of cloud technologies. For this study, we decided to develop a prototype set of risk factors consistent with the structure and format required by the SEI Mission Risk Diagnostic (MRD) method. The product of this development is a set of 24 risk factors for cloud initiatives. These risk factors cover a broad range of potential problems that can affect a cloud initiative, including business strategy and processes, technology management and implementation, and organizational culture. This report presents the initial results of the SEI study into cloud adoption risks.

1.2 Audience

The primary audience for this report includes managers or senior staff members who oversee the implementation of a cloud initiative and who have a familiarity with risk management. Also, anyone who has experience with or is interested in the following topics may also find this report useful:

- cloud computing
- technology adoption
- methods for assessing and managing risk

This report assumes familiarity with the basic concepts of cloud computing concepts. Those with a general interest in risk management should also find the content of this report to be useful.

1.3 Caveats and Limitations

The risk factors presented in this report are a protype set. They were developed using (1) published information on cloud adoption frameworks and (2) input from SEI technical staff who have experience with both cloud computing and technology adoption initiatives. To date, the risk factors have not been piloted in the field. Those who intend to apply the risk factors in this report should be mindful that the factors have not been vetted in the field by SEI developers. However, the risk factors do incorporate information from reliable sources, including Amazon [AWS 2017], Microsoft [Microsoft 2020], and Google [Google 2020].

The next section presents an overview of the SEI MRD method. This basic description of the MRD method provides context for how to develop, structure, and apply a set of risk factors.

2 MRD Method

Since the early 1990s, the SEI has conducted research and development in the area of risk management and has applied risk management methods, tools, and techniques across the software lifecycle (including acquisition, development, and operations) and supply chain. In addition, past SEI research examined various types of risk, including software development risk [Dorofee 1996, Williams 1999, Alberts 2009], system acquisition risk [Gallagher 1999], operational risk [Gallagher 2005], mission risk [Alberts 2009], cybersecurity engineering risk [Alberts 2016, Alberts 2020], incident management risk [Alberts 2014a], and information security risk [Alberts 2002]. A key result of our research into the practice of risk management was the development of the MRD method, a mission-oriented approach for assessing risk in mission threads, business processes, and organizational initiatives.

The overarching goal of the MRD method is to determine the extent to which a mission thread, business process, or organizational initiative is positioned to achieve its mission objective(s) [Alberts 2012]. As shown in Figure 1, the MRD method can be applied in a variety of contexts. To date, we have piloted the MRD in software acquisition and development, cybersecurity incident management, software security, software supply-chain, and business portfolio management, among others.

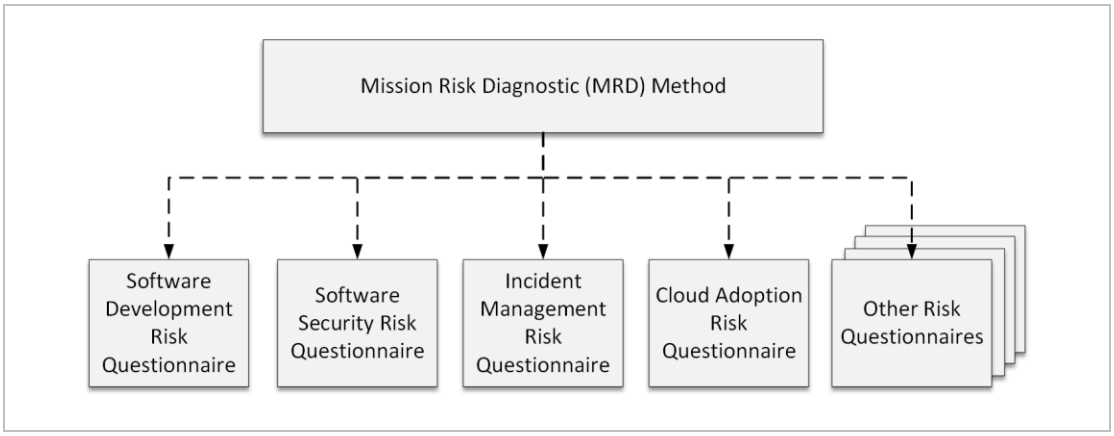

Figure 1: Single Platform, Multiple Assessments

When we tailor the MRD method to a given context, we first develop and document a unique set of risk factors for that context. An MRD risk factor is a systemic condition that has a strong influence on the eventual outcome or result (i.e., whether or not mission objectives will be achieved). After we define a set of risk factors, we integrate those risk factors with the MRD method to produce a unique assessment. In this way, the MRD method provides a common platform for a family of related assessments. The MRD method for cloud adoption is a new assessment in the MRD family.

2.1 Establishing Risk Factors

MRD risk factors are used to analyze performance in relation to the objective(s) of a mission thread, business process, or organizational initiative. Once the set of risk factors is established, analysts can then evaluate each risk factor in the set to gain insight into the likelihood of achieving those objective(s). To evaluate performance effectively, analysts must ensure that the set of risk factors conveys sufficient information about the objective(s) being assessed.

An MRD risk factor has a strong influence on the eventual outcome or result (i.e., whether or not objectives will be achieved). Deriving a set of risk factors requires gathering information and lessons learned from people who have experience and expertise relevant to the specified objectives. This information can come from (1) analyzing documented information (e.g., reports, articles) and (2) by interviewing people with the required experience and expertise. For example, identifying a set of risk factors for software development objectives requires analyzing data related to successful and unsuccessful development projects. Similarly, analysts seeking to identify a set of risk factors for cloud adoption would review lessons learned from best-practice reports on cloud adoption and interviews with people who have expertise in implementing cloud initiatives within organizations.

When reviewing documents and interview notes, analysts try to answer the following questions:

- What circumstances, conditions, and activities prevent the mission thread, business process, or organizational initiative from achieving its objective(s)?
- What circumstances, conditions, and activities enable the mission thread, business process, or organizational initiative to achieve its objective(s)?

Analysts look for a broad range of factors that can drive a mission thread, business process, or organizational initiative toward or away from its objective(s), including factors related to people, processes, work environment, and technology. After documenting a list of candidate risk factors, analysts categorize these factors into approximately 15–25 groups that share a central idea or theme. We used this approach for identifying drivers in a variety of areas, including software acquisition and development programs, cybersecurity processes, and business portfolio management.

2.2 Conducting an MRD Assessment

An MRD assessment can be expert-led or self-applied. This report is written from the perspective of using an external expert to conduct the MRD assessment. Expert-led assessments are facilitated by a small team, called the *assessment team*, which is responsible for conducting the assessment and reporting its findings to stakeholders. The assessment team generally comprises three to five people who have a collective understanding of the technical and management aspects of the mission and the ability to conduct an MRD assessment. During an expert-led assessment, the assessment team completes the following basic tasks:

- The assessment team identifies groups of organizational peers (called participants) and assigns them to interview sessions. As a group, participants must have first-hand knowledge of the mission thread, business process, or organizational initiative that is being evaluated.

- The assessment team facilitates an interview session with each group. Participants in each session answer the driver questions individually (usually by completing a survey). The assessment team then facilitates a discussion of participants' answers. The assessment team documents the rationale for each answer as well as any supporting evidence that is cited by the participants.
- After all interview sessions are complete, the assessment team reviews the responses from each interview group. The team then answers each driver question based on its review of the individual responses. Team members discuss the answer to each driver question among themselves. This discussion can take time. Once consensus is reached, the team documents its answer, rationale, and supporting evidence for each risk question.
- The assessment team documents the results of the assessment and communicates the results to the MRD assessment's stakeholders.

A completed MRD assessment provides stakeholders with a high-level diagnosis (i.e., a "health check") of conditions that enable and impede the successful completion of a mission thread, business process, or organizational initiative. Mission stakeholders can then improve current conditions when warranted and conduct follow-on, deep-dive assessments to gather additional information when needed.

2.3 Evaluating an MRD Risk Factor

An MRD assessment typically requires an assessment team to evaluate 15-25 risk factors for a given set of objectives. A question for each risk factor is documented in a format prescribed by the MRD method [Alberts 2012]. Each risk question is a yes/no question that is phrased from the success perspective. Figure 2 depicts a question with a range of responses for a risk factor titled *Plan*.

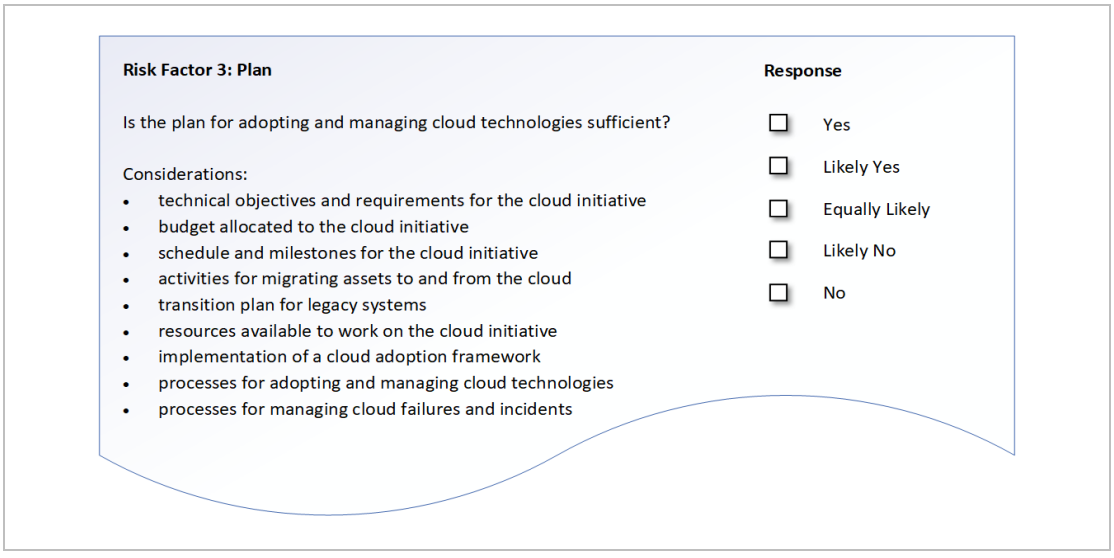

Figure 2: Risk Question and Responses

An assessment team chooses one of the following responses for each risk question: *yes*, *likely yes*, *equally likely*, *likely no*, and *no*. Because the question in Figure 2 is phrased from the success perspective, a *yes* answer indicates minimal risk to the mission. In contrast, a *no* answer indicates maximum mission risk. A range of answers is used to determine probabilities (*likely yes*, *equally likely*, *likely no*) when the answer is not a definitive *yes* or *no*. In addition, key items to consider when answering each question, called *considerations*, are provided for each risk question. Assessment team members use a set of *risk evaluation criteria*, such as those shown in Figure 3, to define each response. The criteria also translate each response into values of mission risk and mission assurance.

Response	Definition	Measures	
		Risk	Assurance
Yes	The answer is almost certainly "yes." Almost no uncertainty exists. There is little or no probability that the answer could be "no." (~ > 95% probability of yes)	Maximum	Minimum
Likely yes	The answer is most likely "yes." There is some chance that the answer could be "no." (~ 75% probability of yes)	High	Low
Equally likely	The answer is just as likely to be "yes" or "no." (~ 50% probability of yes)	Medium	Medium
Likely no	The answer is most likely "no." There is some chance that the answer could be "yes." (~ 25% probability of yes)	Low	High
No	The answer is almost certainly "no." Almost no uncertainty exists. There is little or no probability that the answer could be "yes." (~ < 5% probability of yes)	Minimum	Maximum

Figure 3: Risk Evaluation Criteria

The criteria for analyzing a driver can be tailored for each application of the MRD. For example, the criteria in Figure 3 are based on a five-point scale, which allows decision makers to incorporate different levels of probability in their answers. A different number of answers (i.e., more or less than five) can be incorporated into the analysis when appropriate. In addition, some people prefer to include a *don't know* response to highlight those instances where more information or investigation is needed before a driver can be analyzed appropriately.

Figure 4 shows an example of an evaluated risk factor. The answer to the driver question is *likely no*, which indicates high risk to the mission. As a result, the organization's plan for adopting cloud technologies is inadequate, and as a result, cloud adoption will likely not be successful.[1]

[1] By definition, a *risk factor* describes a condition that is critical to achieving a mission. As a result, that condition has a direct influence on the achievement of the mission objectives. If the answer to a risk question is *likely no*, then the objective will likely not be achieved.

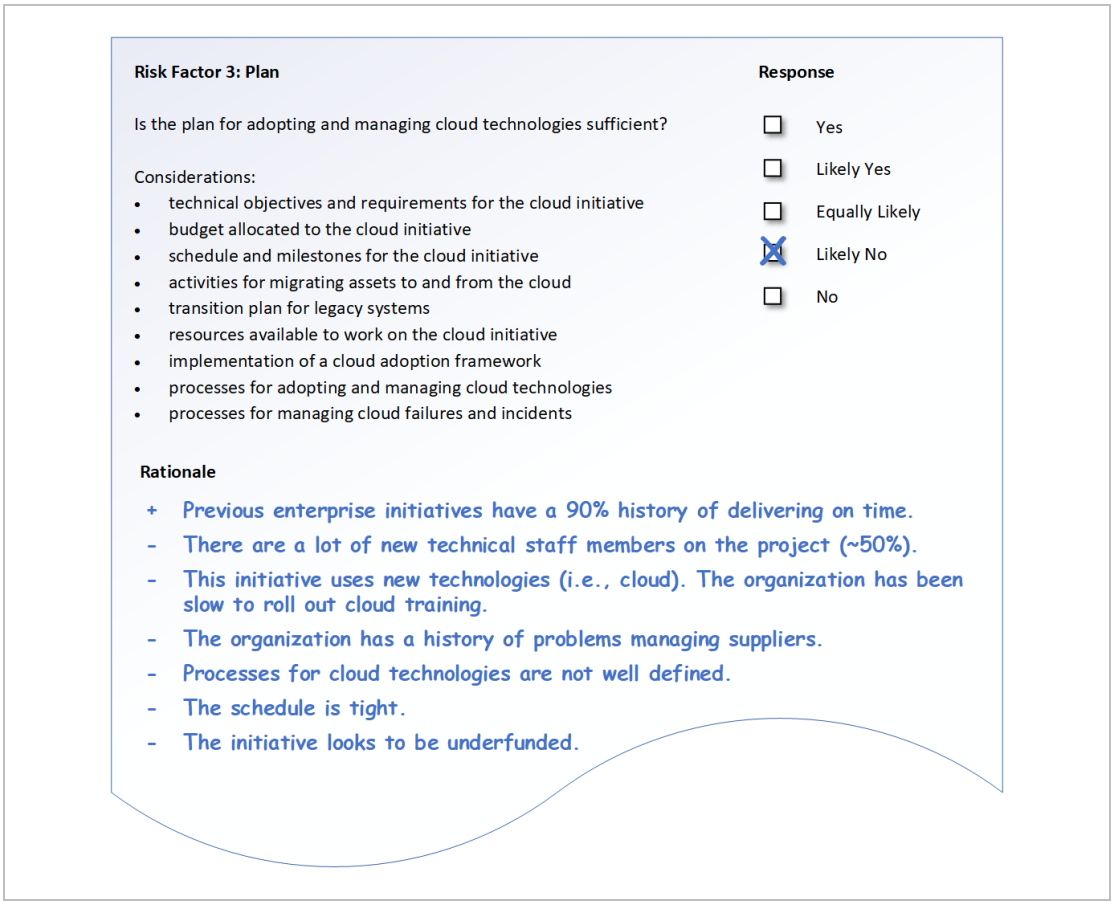

Figure 4: Evaluated Risk Factor

The rationale for the response to each driver question must also be documented because it captures the reasons why analysts selected the response. Any evidence supporting the rationale, such as the results of interviews with system stakeholders and information cited from system documentation must be cited as well. (Figure 4 only shows the rationale.) Recording the rationale and evidence is important for validating the data and associated information products, for historical purposes, and for developing lessons learned.

The MRD principles and concepts presented in this section provide the context for how we develop a unique set of risk factors for mission objectives. The next section presents an overview of the problem space for cloud adoption. We used the characteristics of this problem space to develop a prototype set of risk factors that can be used to assess a cloud initiative.

3 Problem Space

The adoption of cloud computing fundamentally changes how an organization obtains, uses, and manages information technology (IT). At the same time, it can change an organization's business processes (e.g., how it budgets and pays for IT). Cloud adoption requires key stakeholders across an organization to understand the benefits and costs associated with cloud computing. An organization's staff must carefully plan and manage the adoption of cloud technologies to be successful. This includes updating the knowledge, skills, and abilities of business and technical staff; updating existing business and IT processes; and introducing new processes to leverage the many benefits of cloud computing.

The successful adoption of cloud technologies requires chartering an organizational initiative to manage the resulting change in business and IT practices. The purpose of the initiative is to develop and implement a systematic framework for adopting cloud services. At a minimum, this framework should address the following topics:

- aligning IT and business objectives
- defining business justification and expected outcomes of adoption
- establishing senior-level sponsorship of the cloud initiative
- developing the capabilities of organizational staff
- prioritizing and managing IT investments, programs, and projects
- managing organizational change
- defining technical requirements that provide the desired capabilities and required quality of service to the organization
- defining a roadmap and architecture for the target IT environment
- selecting and implementing security controls that meet the organization's needs
- operating, using, and recovering IT workloads based on business requirements

This report presents a prototype set of systemic risk factors for cloud adoption initiatives. We developed these risk factors in the structure and format required by the SEI MRD method. As noted in the previous section, MRD risk factors are derived from the objectives being pursued by a mission thread, business process, or organizational initiative. The problem space for the risk factors presented in this report is defined by the following characteristics:

- The basic architecture is hybrid IT. Some applications will continue to run on-premises while others will be migrated to a public cloud.
- The migration target includes infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). The organization has identified and assessed public cloud deployment options for its applications. Existing applications may leverage IaaS and PaaS deployment models. In some cases, applications might be replaced by SaaS offerings.

- For applications being migrated to the public cloud, IaaS and PaaS will be used to maximize automation and leverage cloud capabilities. Cloud-native services, rather than software in VMs, should be considered to better be able to take advantage of cloud capabilities and potential cost savings. The organization will implement selected cloud management tools in addition to some DevSecOps automation tools.

Given these characteristics, we identified the following objectives for the cloud initiative:

- By the end of the migration and deployment phase (N months),
  - the IT infrastructure will provide agreed-upon services to users
  - the organization's business processes will be updated as appropriate for a cloud environment
  - migration and deployment costs cannot exceed X percent of original estimates

The variables in the above objective statement (i.e., N and X) are defined by the organization. These objectives define a "picture of success" for the cloud initiative; they address business processes and IT services as well as cost and schedule. The remainder of this report presents a prototype set of risk factors that can be used to assess a cloud initiative against these objectives.

4 Cloud Adoption Risk Factors

Table 1 lists a prototype set of 24 risk factors for cloud adoption. A cloud adoption risk factor describes a systemic condition that has a strong influence on whether or not a cloud initiative will achieve its business objectives. As illustrated in the table, risk factors that share common organizational and management attributes are assigned to a common area. Assigning risk factors to areas can facilitate leveraging common risk mitigation activities based on shared risk characteristics.

Table 1: Cloud Adoption Risk Factors

Area	Risk Factor	
Planning and Preparation	1.	Business Case
	2.	Strategy
	3.	Plan
Governance and Management	4.	Governance
	5.	Financial Management
	6.	Change Management
	7.	Supplier Management
Organizational Capability	8.	Organizational Roles and Responsibilities
	9.	Organizational Competencies
	10.	Task Execution
	11.	Coordination
	12.	Tools and Technology
	13.	Resilience
Environment	14.	Organizational Conditions
	15.	Compliance
Engineering Lifecycle	16.	Requirements
	17.	Architecture
	18.	Implementation and Integration
	19.	Test and Evaluation
	20.	Operations
Quality of Service	21.	Performance
	22.	Agility
	23.	Availability
	24.	Security

The risk factors featured in Table 1 are a protype set that have not been piloted in the field. They were developed using published cloud-adoption frameworks and input from people with expertise in cloud adoption. Consider these risk factors to be a starter set that can be tailored to unique environments. The remainder of this report describes the risk factors for each area, beginning with *Planning and Preparation*.

4.1 Planning and Preparation

The successful adoption of cloud technologies begins with an organization's planning and preparation activities. Effective planning and preparation provide a solid foundation for a cloud initiative by ensuring that the organization has sufficient funding and resources in place to support the cloud initiative. The *Planning and Preparation* area includes the following risk factors:

1. Business Case
2. Strategy
3. Plan

Business Case (Risk Factor 1)

A business case provides justification for undertaking a cloud initiative. It evaluates the costs, benefits, and risks of alternative options and provides justification for the selected alternative. The business case for a cloud initiative is focused on ensuring that IT is aligned with the organization's business needs and that IT investments can be traced to demonstrable business results [AWS 2017].

MRD Question*: Does the organization's business case justify the decision to move to the cloud?*

Considerations

- business drivers
- scope of the cloud initiative
- stakeholder support of the business case
- strategic options
- assumptions
- costs and benefits
- business and technical risks
- opportunity costs
- desired business outcomes

Strategy (Risk Factor 2)

A strategy defines an organization's approach for achieving one or more of the its business goals. An organization's cloud strategy outlines the actions and decisions needed to leverage cloud computing as a business enabler. The strategy goes beyond technological considerations to also address the motivation for adopting cloud technologies, organizational changes that must be managed, and the governance and management structures needed to support the cloud environment.

***MRD Question**: Does the organization's cloud strategy sufficiently define the role of cloud computing in the organization?*

Considerations

- motivations behind cloud adoption
- organizational changes required for cloud adoption
- governance structure required for a cloud initiative
- benefits and risks of migrating assets, applications, and workloads to the cloud
- network evolution needed to support native, hybrid, and multi-cloud deployments
- data classification for placement in the cloud
- where and how security will be operationalized between on-premises and cloud resources
- desire to add new capabilities or new technologies

Plan (Risk Factor 3)

A plan outlines a sequence of activities, including timing and resources, needed to achieve a set of objectives. The plan for adopting cloud technologies defines the requirements, budget, schedule, milestones, and resources for the initiative.

***MRD Question**: Is the plan for adopting and managing cloud technologies sufficient?*

Considerations

- technical objectives and requirements for the cloud initiative
- budget allocated to the cloud initiative
- schedule and milestones for the cloud initiative
- analysis of changes to business processes and workflows
- activities for migrating assets to and from the cloud
- transition plan for legacy systems
- resources available to work on the cloud initiative
- compensation program to attract and retain the personnel in a cloud-based IT model
- implementation of a cloud adoption framework
- processes for adopting and managing cloud technologies
- processes for managing cloud failures and incidents

4.2 Governance and Management

Governance focuses on the alignment of the organization's IT strategy and goals with its business strategy and goals. An effective governance program is designed to maximize the business value of IT investments while minimizing the associated risks. Management is the coordination and administration of tasks to achieve business goals. An organization's management activities must be implemented in accordance with the organization's system of governance rules, practices, and processes. The *Governance and Management* area includes the following risk factors:

4. Governance
5. Financial Management
6. Change Management
7. Supplier Management

Governance (Risk Factor 4)

Governance establishes the management framework in which decisions for the cloud initiative are made, providing a system where an organization can manage its investments in cloud technologies. It defines the relationships among all groups involved in the cloud initiative and describes the flow of information among the initiative's stakeholders.

MRD Question: Are the organization's governance practices sufficient for managing cloud services?

Considerations

- procedural controls that communicate acceptable behavior to organizational staff
- degree of business unit control over IT investment priorities and deployments
- organization and management of cloud resources (to ensure a structured, consistent, and controlled environment)
- organizational decision-making authority for implementing cloud services
- balance between service agility and data protection
- risk management policies and procedures for the cloud initiative

Financial Management (Risk Factor 5)

Financial management is a key function responsible for planning and directing the use of an organization's financial resources. Traditional IT initiatives required the purchase of computing equipment as well as licenses for software and applications. These assets would be purchased once and remain in service for several years. Cloud computing has changed the traditional purchasing paradigm. Developers can provision cloud computing assets at any time, which creates a financial obligation for their organization. The traditional one-time purchase of IT assets no longer applies. Financial management in a cloud environment requires understanding the CSP's billing model and pricing structure and the ability to track IT expenditures in real time.

***MRD Question**: Are the organization's financial processes sufficient for managing cloud services?*

Considerations

- understanding of the CSP's billing model and pricing structure
- comparison of on-premises application costs in relation to cloud equivalents
- incorporating cost considerations in the enterprise computing architecture
- real-time financial management processes for cloud services (e.g., dashboards, alerts)
- ability to track cloud computing costs (e.g., using cost center tagging, proactive consumption monitoring, and billing/spending alerts)

Change Management (Risk Factor 6)

Change management is a practice for dealing with the transition or transformation of organizational goals, processes, and technologies. For a cloud initiative, changes affect IT and business processes, staff competencies, and organizational structures and roles. Management and staff must be prepared to manage these organizational changes. They must also be prepared to manage changes to the organization's technologies. For example, infrastructure as code is an IT practice for managing and provisioning computing resources through machine-readable definition files rather than physical hardware configuration. An organization's infrastructure-as-code practices must be integrated into its policies and procedures for change management, which helps to prevent inconsistent configurations across the organization's computing infrastructure.

***MRD Question**: Has the organization implemented an organizational change management plan for the cloud initiative?*

Considerations

- IT and business processes updated for the cloud environment
- staff training program for cloud-based competencies
- changes in organizational structures and roles
- management of business, structural, and cultural change introduced by the cloud initiative
- processes for communicating changes to staff
- changes in CSP services or infrastructure

Supplier Management (Risk Factor 7)

Supplier management is a practice for assessing a supplier's capabilities, contracting with a supplier for products or services, and managing interactions with the supplier throughout the contracted engagement. For a cloud initiative, supplier management includes assessing the viability of a CSP, evaluating the CSP's processes and practices, contracting with a CSP for cloud services, and managing the services provided by the CSP over time.

***MRD Question**: Does the organization have a systematic process for evaluating, selecting, and managing cloud service providers (CSPs)?*

Considerations

- processes for assessing CSP viability
- understanding of CSP's processes and practices
  - pricing and support structure
  - change management (e.g., CSP processes for evolving services or infrastructure)
  - security practices (e.g., for software development and vulnerability testing)
- content of the service level agreement (SLA) with each CSP
  - cloud responsibilities for the organization and CSP
  - applications and services covered under the agreement
  - service requirements
  - guarantees and warranties provided by the CSP
- organizational processes for acquiring services from third parties
- organizational processes for managing supplier performance

4.3 Organizational Capability

Organizational capability is the unique combination of people, processes, and technologies that differentiates an organization and enables it to execute its strategy. An organization's capabilities enable it to perform a coordinated set of tasks, utilizing organizational resources, for the purpose of achieving a specific set of business objectives. For cloud adoption, the capabilities of interest enable the development and implementation of a systematic framework for adopting cloud services. The *Organizational Capability* area includes the following risk factors:

8. Organizational Roles and Responsibilities
9. Organizational Competencies
10. Task Execution
11. Coordination
12. Tools and Technology
13. Resilience

Organizational Roles and Responsibilities (Risk Factor 8)

Roles refer to people's positions on a team, while responsibilities define the tasks and duties of a particular role or job description. A cloud initiative requires multiple roles, such as a cloud architect, cloud engineers, software developers, and business and financial stakeholders. A cloud initiative must ensure that it builds the capability of its organizational staff and is able to manage the organizational change introduced by the adoption of cloud technologies.

***MRD Question**: Has the organization staffed a core team for adopting cloud technologies?*

Considerations

- cloud architect
- cloud center of excellence (CCOE)
- cloud engineers
- cloud software developers
- information technology (IT) and security operations staff
- third-party subject matter experts (SMEs)
- business and financial stakeholders in the organization

Organizational Competencies (Risk Factor 9)

Competencies are observable and measurable patterns of knowledge, skills, abilities, behaviors, and other characteristics that an individual needs to perform work roles or occupational functions successfully [Alberts 2014b]. Competencies can be decomposed into two types: technical and core competencies. Technical competencies apply specifically to a role or position; they directly affect a person's ability to perform a job task. For a cloud engineer, knowledge of cloud services is an important technical competency. Core competencies (e.g., communication, teamwork) are cross-cutting and applicable to all occupations and roles within an organization. Core competencies are relevant and important to all individuals, regardless of their technical specialty. Communication is an example of a core competency for both financial managers and cloud engineers.

***MRD Question**: Do people working on the cloud adoption initiative have the knowledge, skills, and abilities they need to do their jobs?*

Considerations

- knowledge, skills, and abilities of cloud stakeholders:
  - cloud architect
  - participants in a CCOE
  - cloud engineers
  - cloud software developers
  - IT and security operations staff
  - third-party SMEs
  - business and financial stakeholders in the organization
- experience and expertise of technical staff

- organizational training program for cloud services and technologies
- ongoing opportunities for technical staff to attend cloud training courses
- experience and expertise in cloud adoption

Task Execution (Risk Factor 10)

A task is an activity that is scheduled to be to be accomplished within a defined period of time and is designed to help achieve an initiative's goals. Task execution is the process of carrying out planned tasks and producing expected results. Tasks are performed by an individual or a group in accordance with preset requirements and expectations. Effective and efficient task execution requires experienced managers and enough technical staff members with the requisite experience and expertise. Whereas *Organizational Competencies* examine the potential of a cloud initiative's staff to complete its work, *Task Execution* assesses the realization of that potential.

MRD Question*: Are the cloud adoption initiative's tasks being performed effectively and efficiently?*

Considerations

- experience and expertise of technical staff
- experience and expertise of the cloud initiative's management
- staffing levels
- experience with the cloud technologies and tools
- cloud initiative strategy, plan, and processes
- measurement and monitoring data for the cloud adoption initiative

Coordination (Risk Factor 11)

Coordination is the process of organizing people or groups so that they work together properly and are able to achieve a common set of objectives. Many diverse groups must work together to achieve the business goals of a cloud initiative, including the IT department, security operations, business units, and support groups (e.g., financial management, change management).

MRD Question*: Are cloud adoption and implementation activities within each team and across teams coordinated appropriately?*

Considerations

- IT
- infrastructure and operations (I&O) teams
- security operations
- business units
- cloud architect and engineers
- CCOE
- compliance staff
- organizational stakeholders (business and IT)

Tools and Technology (Risk Factor 12)

Cloud team members need to become familiar with and be able to use the tools and technologies provided by each CSP. Cloud team members use cloud native tools to perform management activities. These tools include the graphical user interface (GUI) console; application program interfaces (API); the command line interface (CLI); and tools for monitoring, notification, change management, security management, and cost management.

***MRD Question**: Are cloud team members familiar with and able to use each CSP's native tools?*

Considerations

- management tools (e.g., GUI console)
- application program interfaces (API) and command line interface (CLI)
- monitoring tools
- notification tools
- security tools
- cost management tools
- configuration management tools
- security information and event management (SIEM) tools to monitor, analyze, and manage logs
- security monitoring tools
- third-party tools that can be leveraged across multiple clouds
- cross-platform tools

Resilience (Risk Factor 13)

From a cloud initiative's perspective, resilience is the ability to anticipate, prepare for, and respond to incremental changes and sudden disruptions to achieve business objectives. The initiative must have sufficient capacity and capability to manage unexpected events and changing circumstances that can affect the adoption of cloud technologies.

***MRD Question**:* Does the cloud initiative have sufficient capacity and capability to manage unexpected events and changing circumstances?

Considerations

- flexible plans and processes
- schedule flexibility
- funding reserve
- staffing reserve (e.g., reach-back capability)
- contingency plans
- changes in CSP services or infrastructure
- need to move services between CSPs

4.4 Environment

An organization's environment comprises internal and external conditions that influence an organization's performance, operations, and resources. Internal conditions include the organization's structure, culture, and politics, as well as its communication infrastructure. External conditions include any constraints that a program inherits from its parent organization(s) or from the broader business environment. Constraints can include restrictions imposed by laws and regulations as well as limitations with services provided by third parties. The *Environment* area consist of the following risk factors:

14. Organizational Conditions
15. Compliance

Organizational Conditions (Risk Factor 14)

Organizational conditions focus primarily on internal conditions that affect a cloud initiative's ability to achieve its business objectives. Organizational culture and politics, communication enablers and barriers, and the effects of organizational bureaucracy are examples of organizational conditions that influence a cloud initiative's performance, operations, and resources.

MRD Question: Are enterprise, organizational, and political conditions facilitating execution of the cloud initiative?

Considerations

- relationship between the cloud adoption team and the business units
- management stakeholder sponsorship of the cloud adoption initiative
- designated authority of the CCOE
- organizational culture and politics
- communication enablers and barriers
- effects of organizational bureaucracy
- effects of contracts and agreements (e.g., service level agreements, nondisclosure agreements)

Compliance (Risk Factor 15)

Compliance is the act of adhering to a rule, such as a policy, standard, specification, or law. Compliance includes efforts to abide by both industry regulations and government legislation. Cloud initiatives may be subject to a variety of compliance activities, including mandated data privacy and security requirements. An effective compliance program requires an organization to understand and take the steps required to act in accordance with applicable policies, standards, specifications, and laws.

***MRD Question**: Do cloud services comply with applicable laws, regulations, and mandates?*

Considerations

- legal requirements mandated by regulators or through a contract
- data residency and security requirements
- requirements or restrictions on how data may be used in the public cloud
- risk assessment and control requirements
- requirements for specific data types:
  - personally identifiable information (PII)
  - protected health information (PHI)
  - sensitive data subject to International Traffic in Arms Regulations (ITAR)

4.5 Engineering Lifecycle

Risk factors for a cloud initiative need to address both organizational and technical issues that can affect the initiative's potential for success. To this point in the report, we focused on organizational risk factors related to preparation and planning, governance and management, organization capability, and environment. We now turn our attention toward the technical issues, beginning with the engineering lifecycle risk factors. The engineering lifecycle addresses the phases of a system's development, including concept development, requirements, architecture, implementation, test and evaluation, deployment, operations, and disposal. Technical issues related to the lifecycle include missing or incomplete requirements, inadequate architecture, poor integration of on-premises and cloud technologies, and inadequate operational support for cloud technologies. The *Engineering Lifecycle* area includes the following risk factors:

16. Requirements
17. Architecture
18. Implementation and Integration
19. Test and Evaluation
20. Operations

Requirements (Risk Factor 16)

A requirement is a statement that documents a necessary attribute, capability, characteristic, or quality of a system that provides utility to stakeholders. Requirements analysis should determine which needs or capabilities cloud services should provide. For cloud initiatives, the following types of requirements must be addressed: business, user, CSP (as documented in the SLA), technical and architectural, and quality of service (performance, availability, and security).

***MRD Question**: Are requirements for the cloud environment well understood?*

Considerations

- requirements documented in the SLA
- processing and memory requirements
- networking requirements
- resource optimization requirements
- data storage requirements
- identity and access management
- compliance requirements
- availability requirements, including
  - minimum level of service
  - levels of reliability, availability, and responsiveness to systems and applications
  - response time for reporting or addressing system failures
- security requirements, including
  - data protection requirements
  - CSP penetration testing and vulnerability analysis of processes, services, and APIs
  - security controls provided by the CSP
- management requirements, including
  - account management
  - cost management

Architecture (Risk Factor 17)

An architecture describes the functionality, organization, and implementation of computer systems in an organization. For a cloud adoption initiative, the architecture depicts the target state of the cloud environment in detail. With cloud services, many of the traditional architectural aspects of on-premises systems will change. Architects must develop new skills to codify architectures in templates and create new processes for workload optimization [AWS 2020]. When developing a cloud architecture, it is essential to address any risks inherent in using services in a public cloud. Architectural considerations include assessing tradeoffs between using CSP services and using self-managed services; selection of appropriate computing and storage options; planning for the integration of on-premises and cloud operations; and meeting the resilience and continuity requirements of systems and networks.

***MRD Question**: Does the enterprise architecture sufficiently mitigate risks of the public cloud?*

Considerations

- tradeoffs between using CSP services and using self-managed services
- selection of appropriate computing and storage options
- integration of on-premises and cloud operations (using a hybrid cloud architecture)
- distribution of workloads among multiple CSPs
- redundancy between CSPs
- resilience and continuity of systems and networks
- ability to scale up and quickly provision new resources
- ability to orchestrate processes with the help of automation
- implementation of network segmentation

Implementation and Integration (Risk Factor 18)

Implementation is the process of putting a decision or plan into effect, while integration is the process of effectively combining two or more things. In this report, an architecture defines the blueprint for how on-premises and cloud services will be aligned; implementation and integration focus on realizing that architecture in practice. During implementation and integration, engineers link on-premises systems with cloud services in accordance with the specified architecture.

***MRD Question**: Is each CSP's platform well integrated with critical core infrastructure services that reside on-premises?*

Considerations

- network connectivity to the cloud, including
  - virtual private network (VPN)
  - dedicated private links
  - Multiprotocol Label Switching (MPLS) implementations
  - software-defined wide area network (SDWAN)
- integrated on-premises and cloud-name-resolution services
- identity and access management (IAM) strategy
- integrated data and storage services for on-premises and cloud environments

Test and Evaluation (Risk Factor 19)

Test-and-evaluation (T&E) activities are performed to (1) verify system requirements and (2) assess the effectiveness, operational suitability, and survivability of a system under realistic operational conditions. For a cloud initiative, the transition to a commercial cloud limits an organization's direct access to IT resources that no longer run in an on-premises data center. For IT resources that have been migrated to the cloud, T&E personnel have limited observability of those resources (e.g., access to system internal communications and state) and limited ability to directly control T&E activities for those resources (e.g., the ability to inject internal faults). These limitations necessitate early T&E involvement in the definition of system requirements and architecture to ensure that sufficient observability and controllability are built into systems. T&E groups must develop close relationships with CSPs to collect the data and evidence that are needed to evaluate cloud-deployed resources. Because interaction with the cloud occurs through software APIs, T&E personnel need the ability to develop API scripts and tailor available test tools.

***MRD Question**: Are test-and-evaluation (T&E) processes, methods, and tools for the cloud environment sufficient?*

Considerations

- test-and-evaluation stakeholder participation across the engineering lifecycle
- specification of test-and-evaluation requirements in SLAs
- knowledge, skills, and abilities of test-and-evaluation staff
- mechanisms and procedures to ensure CSPs are meeting requirements
- identification of triggers and recertification criteria for follow-up testing
- implementation of ongoing monitoring activities for key systems
- degree of automation in testing and monitoring activities
- access to CSP testing, evaluation, and monitoring reports

Operations (Risk Factor 20)

During the operations-and-support phase of the lifecycle, a system is deployed, used, and maintained in the field. The primary focus of this phase is the execution of a support system that sustains the system in the most cost-effective manner possible. Key activities performed include managing, planning, and scheduling changes to the IT environment; managing changes to CSP services or infrastructure; recovering from failures; identifying and resolving safety, performance, and cybersecurity issues; and reporting on performance and costs.

***MRD Question**: Are processes for operating and maintaining the cloud environment sufficient?*

Considerations

- managing, planning, and scheduling changes to the IT environment
- managing changes to CSP services or infrastructure
- reporting on performance and costs
- analyzing and reporting performance against key performance indicators (KPIs)

- recovering from failures within the time parameters defined by the organization
- monitoring practices for cloud-based applications and services
- ability to
  - track and remediate inefficiencies when possible
  - optimize cloud spending and reduce waste when possible
  - optimize resource allocation
- ability to structure data collection methods, store monitoring data, and perform analyses across multiple types of system telemetry

4.6 Quality of Service

Quality of service describes or measures how well cloud services are expected to meet the needs and requirements of users during operations. This area examines risks that are inherent in the technical solution provided by a project or initiative. The quality-of-service risk factors focus on the correctness and completeness of the implemented technical solution. For a cloud initiative, quality of service addresses the performance and functionality provided by a cloud environment as well as quality attributes, such as availability and security. The *Quality of Service* area includes the following risk factors:

21. Performance
22. Agility
23. Availability
24. Security

Performance (Risk Factor 21)

Performance focuses on how well a technical solution addresses functional requirements and the extent to which the solution meets the needs of users and stakeholders. Performance indicators are used to assess technical performance and ensure that cloud services support business outcomes as defined in SLAs. For cloud services, performance indicators can include qualities like network latency, capacity, throughput, and response time.

MRD Question*: Will cloud services meet the organization's performance requirements?*

Considerations

- network latency
- capacity
- packet loss
- jitter
- throughput
- response time

Agility (Risk Factor 22)

In cloud computing, agility refers to the rapid provisioning of computer resources. A cloud environment provides a computing platform that can be scaled quickly, maintained at the highest level of technology refresh, and accessed without geographic limitations; these are key characteristics of an agile computing infrastructure. Cloud computing also provides the ability to rapidly develop, test, and launch software applications as well as quickly enhance or update a system.

***MRD Question**: Will cloud services be sufficiently agile to meet the organization's business requirements?*

Considerations

- automatic provisioning or de-provisioning of infrastructure, computing resources, and on-demand storage to match user demand
- ability to rapidly develop, test, and launch software applications
- deployment of new applications, solutions, and products more rapidly
- ability to quickly enhance or update a system
- automated deployment of system changes through continuous integration and continuous deployment (CI/CD) practices

Availability (Risk Factor 23)

In cloud computing, availability is the percentage of time a system or a service is accessible. When designing for availability, cloud architects and engineers need to leverage the characteristics and capabilities of the CSP's global infrastructure. Key considerations include availability requirements in the SLA, native storage replication solutions provided by the CSP, and the physical placement of workloads in the CSP's infrastructure.

***MRD Question**: Will cloud services meet the organization's availability requirements?*

Considerations

- levels of reliability, availability, and responsiveness to systems and applications
- ability to measure and report on service-level delivery
- ability to leverage the characteristics and capabilities of the CSP's global infrastructure by understanding
  - availability requirements in providers' service level agreements (SLAs)
  - providers' native storage replication solutions
  - physical placement of workloads (e.g., within availability zones)
  - requirements for reconstituting systems from stored backups
- incident management capability to handle unplanned service degradations
- business continuity strategy designed to meet availability requirements
  - address service disruption and system failures
  - prevent unrecoverable data loss
  - prevent vendor lock-in
- public cloud exit strategy for critical applications

Security (Risk Factor 24)

Cloud security includes the technologies, policies, controls, and services that protect cloud data, applications, and infrastructure against both external and internal cyber threats. Cybersecurity activities for cloud-based systems are a shared responsibility between an organization and its CSP. The level of oversight that an organization must perform to confirm the CSP's security controls depends on the contracting provisions in place for information sharing.

***MRD Question**: Will the cloud environment be acceptably secure?*

Considerations

- encryption
- data protection
- logging and monitoring
- identity and access management (IAM) solutions
- authentication (e.g., multi-factor authentication)
- role-based access control (RBAC)
- shared responsibility for security (between organization and CSP)
- security of CSP technologies and tools
- access to results of CSP security evaluations

5 Summary

The SEI MRD method defines a time-efficient, mission-oriented approach for assessing risk in mission threads, business processes, and organizational initiatives. The overarching goal of the MRD method is to determine the extent to which a mission thread, business process, or organizational initiative is in position to achieve its objective(s). Over the past several years, we tailored the MRD method to a variety of contexts, including software acquisition and development, cybersecurity incident management, software security, software supply-chain, and business portfolio management.

In this report, we presented the results of a study that we conducted to identify a prototype set of risk factors for the adoption of cloud technologies. These risk factors cover a broad range of potential problems that can affect a cloud initiative, including business strategy and processes, technology management and implementation, and organizational culture.

We view the publication of this report as an initial step in the development of cloud adoption risk factors rather than the culmination of our work in this area. We identified a range of potential future development and transition tasks related to the MRD for cloud adoption, including the following:

- Pilot the current version of the MRD for cloud adoption with organizations that plan to adopt cloud services.
- Refine the current version of the cloud adoption risk factors based on pilot results.
- Develop and document detailed guidance for applying the MRD for cloud adoption (for expert-led assessments and self-assessments).
- Develop training for MRD for cloud adoption (for expert-led assessments and self-assessments).
- Extend and align the MRD for cloud adoption to be consistent with new or updated community standards, practices, methods, frameworks, and tools for adopting cloud computing.

Future development and transition activities will ultimately be determined by the feedback that we receive from people throughout the community. No matter which path is followed, we believe that the content presented in this report will help organizations to manage their risks more effectively as they plan and manage the adoption of cloud technologies.

References

[Alberts 2002]
Alberts, Christopher & Dorofee, Audrey. *Managing Information Security Risks: The OCTAVE^{SM} Approach*. Addison-Wesley. 2002. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=30678

[Alberts 2009]
Alberts, Christopher & Dorofee, Audrey. *A Framework for Categorizing Key Drivers of Risk*. CMU/SEI-2009-TR-007. Software Engineering Institute, Carnegie Mellon University. 2009. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=9093

[Alberts 2012]
Alberts, Christopher & Dorofee, Audrey. *Mission Risk Diagnostic (MRD) Method Description*. CMU/SEI-2012-TN-005. Software Engineering Institute, Carnegie Mellon University. 2012. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=10075

[Alberts 2014a]
Alberts, Christopher; Dorofee, Audrey; Ruefle, Robin; & Zajicek, Mark. *An Introduction to the Mission Risk Diagnostic for Incident Management Capabilities (MRD-IMC)*. CMU/SEI-2014-TN-005. Software Engineering Institute, Carnegie Mellon University. 2014. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=91452

[Alberts 2014b]
Alberts, Christopher & McIntire, David. *A Systematic Approach for Assessing Workforce Readiness*. CMU/SEI-2014-TR-009. Software Engineering Institute, Carnegie Mellon University. 2014. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=301653

[Alberts 2016]
Alberts, Christopher; Dorofee, Audrey; & Woody, Carol. *Wireless Emergency Alerts Commercial Mobile Service Provider (CMSP) Cybersecurity Guidelines*. CMU/SEI-2016-SR-009. Software Engineering Institute, Carnegie Mellon University. 2016. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=463988

[Alberts 2020]
Alberts, Christopher & Woody, Carol. *Security Engineering Risk Analysis (SERA) Threat Archetypes*. Software Engineering Institute, Carnegie Mellon University. 2020. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=650999

[AWS 2017]
Amazon.com, Inc. *An Overview of the AWS Cloud Adoption Framework, Version 2*. Seattle, WA. 2017. https://docs.aws.amazon.com/whitepapers/latest/aws-migration-whitepaper/the-aws-cloud-adoption-framework-aws-caf.html

[Dorofee 1996]
Dorofee, A.; Walker, J.; Alberts, C.; Higuera, R.; Murphy, R.; & Williams, R. *Continuous Risk Management Guidebook*. Software Engineering Institute, Carnegie Mellon University. 1996. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=30856

[Gallagher 1999]
Gallagher, Brian. *Software Acquisition Risk Management Key Process Area (KPA) – A Guidebook Version 1.02*. CMU/SEI-99-HB-001. Software Engineering Institute, Carnegie Mellon University. 1999. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=13165

[Gallagher 2005]
Gallagher, B.; Case, P.; Creel, R.; Kushner, S.; & Williams, R. *A Taxonomy of Operational Risks*. CMU/SEI-2005-TN-036. Software Engineering Institute, Carnegie Mellon University. 2005. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=7525

[Google 2020]
Google LLC. *The Google Cloud Adoption Framework*. Mountain View, CA. 2020. https://services.google.com/fh/files/misc/google_cloud_adoption_framework_whitepaper.pdf

[Microsoft 2020]
Microsoft Corporation. *Microsoft Cloud Adoption Framework for Azure*. Redmond, WA. 2020. https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/

[Williams 1999]
Williams, R.; Pandelios, G.; & Behrens, S. *Software Risk Evaluation (SRE) Method Description (Version 2.0)*, CMU/SEI-99-TR-029. Software Engineering Institute, Carnegie Mellon University. 1999. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=1355