Defining a Risk-based Approach to the Design and Technology Usage of Systems to Attain IT Availability and Recoverability Requirements

Michael Azzopardi VP, Arvin Levine Ph.D., VP
Infrastructure Architecture
Credit Suisse
New York, NY, USA
michael.azzopardi@credit-suisse.com
arvin.levine@credit-suisse.com

John Lamb, Ph. D., Senior Technical Staff Member
IBM Global Services
IBM
Somers, NY, USA
jlamb@us.ibm.com

***Abstract*— This paper explains the rationale and overall concept for defining a risk-based approach to the design and technology usage of systems to achieve a set of differentiated business availability and recoverability classes. It provides an overview of the various dimensions being taken into consideration and also elaborates on the aspects that drive the differentiation of best practices or technical capabilities used to achieve the different classes.**

The paper elaborates on the generic process aspect of assessment of existing systems. It explains how we would utilize this foundation to establish guidelines for applications, the underlying technology and infrastructure, as well as the operational set-up.

The principal motivations for the availability and recoverability classification are i) to improve the ability to fulfill the required levels of availability and recoverability and ii) to optimize the investment and operational cost. Businesses will classify their availability according to the distinctions defined here which will limit the extent of high cost critical applications. Additionally, applications will architect their designs for lower cost methods of achieving the desired level of availability.

There is no cookie-cutter formula to accomplish these goals. Only if all pieces and building blocks of the architecture are designed from the beginning to fit to each other, will the entire system achieve optimized service availability levels.

Keywords-component; availability; recoverability; enterprise architecture

I. INTRODUCTION

Availability and recoverability of a single application can be approached in a measured manner to achieve a desired class of service. Design, technology and process aspects can be comprehended and implemented. To achieve the same result across an enterprise which might comprise hundreds or thousands of applications is a far different exercise. No longer is this a matter of ensuring that something is 'up'. Rather, the infrastructure, operations and application development areas have to be aligned along the axis of availability and reliability. Furthermore, accomplishing this in a cost-effective manner is highly non-trivial.

Our concern here is enterprise-wide: how to manage potentially thousands of applications in an global production environment. An approach which works for a single solution in isolation may not be applicable with this goal.

We propose an approach based on a framework with an architectural mapping of best practices and technical capabilities. An alternative approach might construct a catalog of rules for enforcement which we most typically find in the security realm.

II. FRAMEWORK FOR ANALYSIS

A. Desiderata

Availability and recoverability can be assessed from different perspectives:

- Dependencies to surrounding systems
- Dependencies on the underlying technology stack
- Resilience to failures of components, subsystems or surrounding systems
- Ability to recover from failure situations

Moreover, the extent of a global application landscape and hosting infrastructure implies technical and operational dependencies that are not necessarily visible or controllable by any single party within the Information Technology organization.

The desired outcome of the proposed method is to provide and enterprise-wide abstraction to this complexity that allows the organization to steer the construction of individual systems, the provisioning of technology and transformation of operational processes.

978-1-4577-1591-4/11/$26.00 ©2011 IEEE

B. Structure

It is necessary to take a holistic approach: only if all pieces and building blocks of the architecture are designed from the beginning to fit to each other, will an entire system achieve optimized levels of availability and recoverability. As an alternative to looking at the design and implementation of a single system, we look at the practices and processes within the enterprise that influence the availability and recoverability across the application landscape as a whole. Fig. 1 indicates the enterprise IT-wide availability and recoverability structure. We describe the corresponding artifacts in the following section.

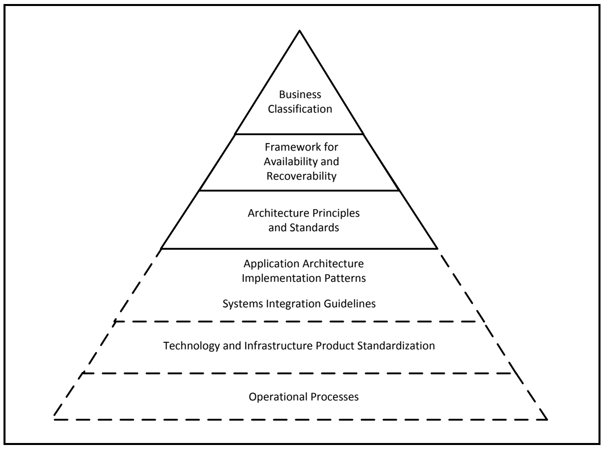

Business Classification
Framework for Availability and Recoverability
Architecture Principles and Standards
Application Architecture Implementation Patterns
Systems Integration Guidelines
Technology and Infrastructure Product Standardization
Operational Processes

Figure 1. Enterprise structure for IT-wide availability and recoverability

C. Artifacts

Each level of the enterprise structure is documented with an appropriate artifact.

- **Business Classification**: definition of availability and recoverability classes for classification of business services [1] (business level definition, executive approval)
- **Framework for IT Availability and Recoverability**: description of the problem statement, concept and structure for addressing enterprise wide availability and recoverability (IT architecture ratification)
- **Architecture Principles and Standards**: elaboration of verifiable and enforceable practices to govern the approach of how individual systems achieve that stated level of service (IT architecture approval)
- **Application Architecture Implementation Patters**: definition of architecture patterns for addressing availability and recoverability across different types of applications (IT architecture approval)
- **Systems Integration Guidelines**: guidelines for systems integrators to apply valid configurations of technology aligned to application technical requirements and business requirements of availability and recoverability (IT integration approval)
- **Technology and Infrastructure Product Standardization**: differentiation technology offering (in the form of a Product Catalogue) covering technical capabilities that contribute to the availability and recoverability of individual technical components and the system as a whole (IT engineering approval)
- **Operational Processes**: description of procedures to operate an application and its underlying infrastructure (IT operations approval)

D. Defining the scope of differentiation

To address the required classes of availability and recoverability across the three lowest layers of the structure the best practices, technology and operations set-up need to be adequately aligned. We align the framework (See Fig. 2) to the respective IT stakeholders, competencies and organizational responsibilities.

1. **Application Suitability**: what are the best practices across the various stages of the lifecycle of the application that contribute towards achieving a certain level of availability?
2. **Technical Capability Utilization**: what are the capabilities of the underlying technology stack that contribute to the ability of a system to achieve a certain level of availability and recoverability?
3. **Operational Readiness**: what are the organizational requirements necessary such that the system is operated in such a way that the defined service levels can be met?

When elaborating the aspects to be assessed retrospectively for a system, we explicitly differentiate the relevant scope elements:

- aspects that could provide an insight in the quality of a system implementation as a basis for generalizing potential fit for purpose
- aspects that could identify gaps that could realistically be remediated
- aspects that could provide tangible cost optimization opportunities

It should be noted that production applications should be differentiated from pre-production (e.g., development and test) applications in the analysis.

[1] By business service we refer to the usage of systems to realize specific business processes or functions. Business users are consumers of applications.

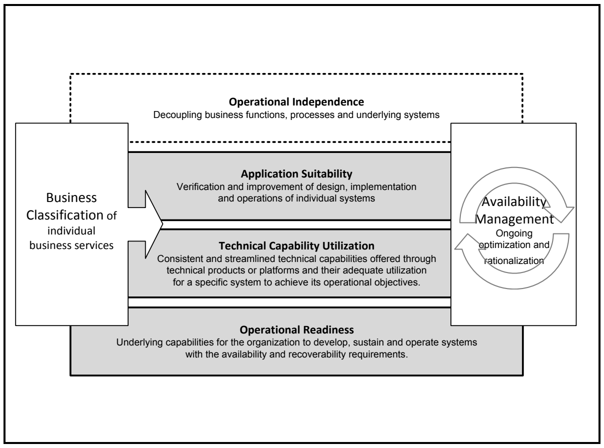
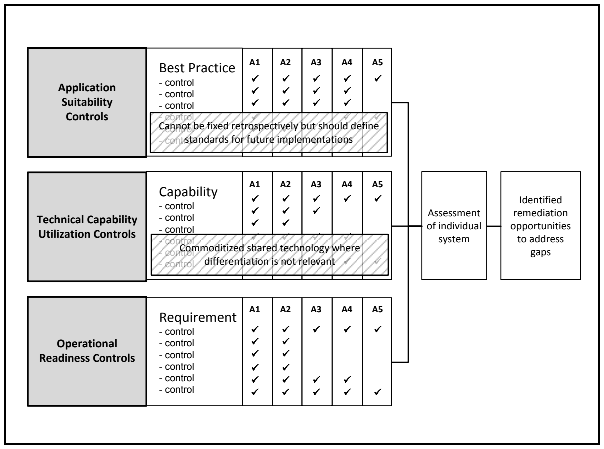

Operational Independence
Decoupling business functions, processes and underlying systems
Business Classification of individual business services
Application Suitability
Verification and improvement of design, implementation and operations of individual systems
Technical Capability Utilization
Consistent and streamlined technical capabilities offered through technical products or platforms and their adequate utilization for a specific system to achieve its operational objectives.
Availability Management
Ongoing optimization and rationalization
Operational Readiness
Underlying capabilities for the organization to develop, sustain and operate systems with the availability and recoverability requirements.

Figure 2. Framework for IT Availability and Recoverability

E. *Alternative to this approach*

A controls catalogue could be constructed which would provide a checklist for project or application evaluation. The catalogue scope is indicated in Fig. 3. The catalogue is used to:

- Retrospectively assess whether a system is suitable to meet the availability and recoverability requirements established through the BCS Rating Process
- Frame the standards, guidelines, best practices and technical capabilities to improve the alignment and cost efficiency for realizing availability and recoverability requirements.


Application Suitability Controls
Technical Capability Utilization Controls
Operational Readiness Controls
Assessment of individual system
Identified remediation opportunities to address gaps

Best Practice	A1	A2	A3	A4	A5
- control	✓	✓	✓	✓	✓
- control	✓	✓	✓	✓	
- control	✓	✓	✓	✓	

Cannot be fixed retrospectively but should define standards for future implementations

Capability	A1	A2	A3	A4	A5
- control	✓	✓	✓	✓	✓
- control	✓	✓	✓		
- control	✓	✓			

Commoditized shared technology where differentiation is not relevant

Requirement	A1	A2	A3	A4	A5
- control	✓	✓	✓	✓	✓
- control	✓	✓			
- control	✓	✓			
- control	✓	✓			
- control	✓	✓	✓	✓	
- control	✓	✓	✓	✓	✓

Figure 3. Control catalog for assessing system implementations

Our reservations to this approach lie in the complexity factor of an enterprise environment. An application can choose from alternative architectures to achieve its goals. We would need a checklist for each architectural approach, which would make the use of the catalogue impractical. In fact, the catalogue is similar to the "Technology and Infrastructure Product Standardization" implementation artifact described above.

III. Defining Availability, Recoverability, and Max Data Loss

Reliability, Availability and Serviceability (RAS) is a set of related attributes that must be considered when designing, implementing, deploying and operating a computer system or components composed of hardware or software.

A. *Availability*

Availability is the ratio of time a system or component is functional to the total time it is required or expected to function. The availability we are concerned with is "end user availability". Components of end user availability include service availability and system availability.

Availability can be expressed as a percentage of expected uptime. It can also be expressed in terms of average downtime per week, month or year or as total downtime for a given week, month or year. Sometimes availability is expressed in qualitative terms, indicating the extent to which a system can continue to work when a significant component or set of components goes down.

To increase a system's availability, one needs to decrease the duration of outages, decrease the frequency of outages, or both. Technical capabilities for availability can be separated into those needed to configure and operate the system during normal operation and those that are used to detect and handle faults.

Different availability techniques may result in maintaining the same quality of service of the system or make a compromise by ensuring a minimal level of service. For example, a dual-trail system that at normal operation is able to handle 100% load, would reduce its capacity to 50% if one of the trails fail. Fig. 4 depicts availability with resulting 100% or 50% capacity. Reduced capacity could be a significant cross dependency to integrity requirements in the larger scope of business criticality. There are various considerations to be taken when deciding that a system is recovered only at a reduced quality of service. The business would have to accept the risk of reduced capacity and quality of service or employ risk mitigations to deal with the impact.

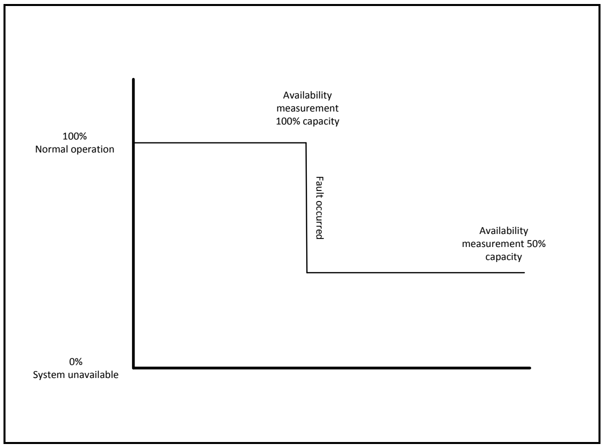


Figure 4. Availability with resulting 100% or 50% capacity

Availability strategies: The following strategies can increase availability of individual application systems:

- Resilience allows a component to continue at full or partial function after faults occur. Thus, resilient components provide a higher availability level than comparable non-resilient components.
- Redundancy, achieved by duplicating components in the architecture, increases overall systems availability since the probability of failure is divided across two or more components. This strategy is adopted at lower level hardware design of enterprise class servers up to the overall system in multi-trail systems architecture. Reliable communication needs to be ensured by also having multiple communication paths to and from the redundant components.

B. Recoverability

In this context we define recoverability as the response to a fault that caused the system not to be available (i.e. 0%).

Disaster Recovery (DR) mechanisms are typically invoked at the point of failure to make an alternative system available. Recovery may also result in a reduced quality of service until the normal production environment is restored. The recovery time objective (RTO) is the acceptable duration of recovering a system after a failure occurs. Fig. 5 shows a disaster recovery with resulting 50% capacity.

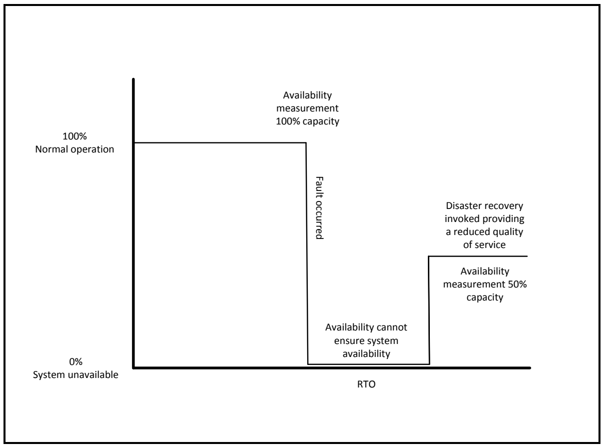


Figure 5. Invoking disaster recovery with resulting 50% capacity

The key dimensions to be considered in the design and implementation of recoverability are:

- The Recovery Time Objective (RTO) which defines the maximum time it takes to switch over to the disaster recovery instance of the application
- The Recovery Point Objective (RPO) defining how much data loss can be incurred in case of a disaster

Three questions to be answered are:

- How to decide to go to DR (time, situation -- cause of failure, number of systems, etc.)
- How long will it take for DR to be ready?
- What is the difference in terms of data between the active DR environment and the production environment at the point of failure?

Recoverability strategies: The main approach to recoverability is having a secondary set-up of the systems that are completely isolated up to the level that it is physically located in a distant data center.

Apart from time to recover and the state at recovery, the key challenges to consider for recoverability are:

- The time required for resuming normal availability and recoverability
- The Quality of Service (QoS) at point of recovery
  - o Limitations on business functionality
  - o Transaction throughput
  - o Number of users / Scalability
  - o Performance
  - o Historic data available
- Prioritization of systems to recover

C. Maximum Data Loss

Another requirement that influences the impact of a failure of a system to the end-users is Maximum Data Loss. When failures occur, data may be lost if it has not been made persistent or did not reach its target system.

D. Business Classification for Availability, Recoverability and Maximum Data Loss

The business classification is intended to provide a simplified way of classifying requirements to the application. In order to minimize the number of parameter combinations, we combine availability and recoverability under one class even though the way to address them from a technical and operational standpoint is not necessarily the same.

TABLE I. GENERIC RATING SCHEME FOR APPLICATION AVAILABILITY AND RECOVERABILITY

Objective	**Availability Definitions**		
	Annual Availability	***Maximum acceptable outage per incident (RTO)***	***Reasoning***
A-1	99.9%	4 hours	Proven legal or regulatory need
A-2	99.9%	24 hours	Selected applications
A-3	99.4%	24 hours	Support critical business areas
A-4	99.4%	72 hours	Default
A-5	Best effort	n/a (best effort)	Risks must be signed off

The A-n availability levels, shown in Table I, reflect the business view of decreasing relative financial impact of an outage for that rating class, where A-1 is the required rating when there is a very large financial impact from an outage and A-5 is the rating for a smaller impact of outage. The availability levels entail a scale of cost to implement and support, where A-1 would be associated with the highest costs to run, and A-5 the lowest.

The two lowest ratings, A-5 (the "best effort") and A-4 (the "default") would include, by far, the great majority of business applications. This is based on the premise that not "over classifying" the availability requirements for a system can reduce the overall IT spend while supporting the realization of the higher classes.

We also presented a simplified classification scheme for Maximum Data Loss to aid the business owners of applications in defining the amount of acceptable loss of data in the event of a failure.

TABLE II. GENERIC RATING SCHEME FOR MAXIMUM DATA LOSS

Objective	Data loss characteristic	Business Value
R-1	Momentary data loss sub-second, minutes, hours	$$$
R-2	DEFAULT 24 hours data loss	$$
R-3	Best effort	$

Table II shows recoverability levels. A contentious part of this proposal is the R-1 rating as there an increased architectural and cost implication for reducing data loss the more you approach zero. Some A-1 applications have a zero data loss requirement. For the intents and purposes of this paper, this requirement would be considered a special case of the R-1 rating with RPO very near zero (e.g., sub-second).

Recoverability cannot be designed for a single system or single component in isolation because in most enterprise environments a single system is dependent on functions, processes, interfaces and data delivered by other systems. This may lead to two distinct approaches:

- Ensure that the dependent systems have the same level of disaster recovery
- Design systems for resilience in a disaster recovery set-up to optimize the number of systems that need higher level recoverability objectives

The following questions need to be discussed with the business owner of the system to validate the required disaster recovery setup of an application:

- (A-x) Which availability and recoverability classification is required for this application?
- (R-y) How much data can the business afford to lose? That is, how current must the data be after it is recovered?
- How much degradation in performance is acceptable to the business during a disaster?
- Does this application send data to or receive data from other applications?
- Do the business processes supported by the application depend on the availability of surrounding systems?

Moreover, we have identified additional factors that may drive the complexity and cost of the recoverability design:

- The scope of functionality that is made available at the point of recovery
- The timeliness and history of data available
- The capacity, performance or throughput of the system
- The time to fully restore the production environment and return to normal operation

These questions lead to an informed decision on what recoverability implementation is adopted that appropriately addresses the availability, recoverability and maximum data loss of a system.

IV. IMPLEMENTATION STANDARDS

A. *Application Suitability*

Applications have requisite dependent application design and hosting engagement process steps that must be followed to support attainment of the specified availability goals. Infrastructure in and of itself is not sufficient to allow attainment of desired availability.

When looking at availability in the context of large organizations, one needs to consider a broader view. The typical evaluation of availability of a system is dependent on the underlying technology stack. However, in an enterprise environment one needs to take into consideration the availability of surrounding systems on which the application functions or data are dependent (operational independence[2]). Hence the capability of functions of an application to be available when other components, subsystems or dependent surrounding systems are not available is important in defining the availability strategy of a system and the supported business processes.

The project and application must align with applicable application architecture principles and undergo specific reviews. There are various best practices that need to be taken into consideration across the lifecycle of an application to ensure that availability and recoverability are not an afterthought but a core architectural quality of the system. We can use the various stages of the lifecycle (also referred to as process areas) of a system to map these best practices to the different availability and recoverability ratings. Across

[2] By operational independence, we mean the development of an architecture to reduce runtime dependencies and hence limit the effect of incidents across the IT landscape.

these process areas we identified best practices that are followed in most system implementation projects.

- Business Application Requirements

Define availability and recoverability requirements of functional parts of an application. Decompose a system into logical functional parts. Identify which functionality of the system requires the highest availability levels and which functionality could be of less. This might reduce the number of sub-components or sub-systems that have higher availability requirements.

- Application Architecture & System Design

Component dependencies must be minimized through decoupling that can be achieved through managed interfaces. For example, references to components that are not necessary for the functionality must be removed.

- Technical Architecture & Deployment Design

Use system replication and component redundancy to provide higher levels of availability

- Testing & Quality Assurance

Define extreme test cases of identified failure scenarios and the expected system response. Conduct verification of extreme test cases as part of regular application testing. Extreme test case verification must be part of regular testing.

We started differentiating which practices are to be extended, improved, enforced or dismissed based on the contribution they make to the ability of the resulting system to fulfill a higher or lower A-n rating. A typical example is the requirement that, beyond normal testing and quality assurance, A-1 rated applications must undergo destructive testing (testing of concrete failure scenarios without following normal shutdown procedures, e.g., pull the plug from a server) at extreme load. On the other hand some activities that typically increase solution delivery costs and that do not contribute to the ability to deliver quality systems of the A-5 class are challenged or even discouraged.

B. *Technical Capability Utilization*

Technical Capability Utilization subcategories with requirements for each Availability Rating are shown in this section. The subcategories used for mapping for this area are:

- Technology Portfolio

Review the technology portfolio of the firm across the stack from application platforms (JEE, DWH, .Net) down to hosting infrastructure including data center, storage and network. By looking at the technical capabilities provided by each technology, we identify the contribution that technology can deliver towards different classes of application, e.g., connection pooling, dynamic lookup, clustering, fail-over and load-balancing, transaction protection, workflow.

- Alignment of Applications, Products, Platforms and Infrastructure

In a large IT landscape, technology management is critical for the optimization of resources. This includes establishing standards, providing engineered products which address common requirements and managing the lifecycle of technology usage. The management of the technology portfolio and alignment to the availability and recoverability requirements facilitates the fulfillment of these goals by individual applications.

- Commoditized Technology and Infrastructure

Much of the infrastructure at a data center is shared by all applications and there is little differentiation that can be done based on application availability requirements. For those technologies that have been commoditized or are highly shared, there is the implication of a consistent and broader provisioning of availability and recoverability. This drives additional cost. It is important to look at alternatives from a cost optimization perspective.

Based on the above structure, we identify corresponding technology that can be utilized for different classes of application. Utilizing the right technology or providing a highly redundant topology does not necessarily guarantee that the application will be able to achieve the set service levels. Application design and implementation remain fundamental characteristics of suitability. On the other hand higher capability and redundancy is discouraged for applications that do not justify their need (because they are assigned a lower A-n class). This presents an opportunity to optimize capital investment and operational costs by having the right provisioning to the right applications.

Table III is a high-level overview of recoverability strategies bringing together the identified technical capabilities identified. Establishing such patterns improves the ability to address these goals in a systematic approach across the application landscape.

TABLE III. RECOVERABILITY LEVELS WITH RESPECTIVE TECHNICAL CAPABILITIES

Availability Objective	**Recoverability Technology**		
	Recoverability	***Maximum Data Loss***	***Sample Implementations***
A-1	Instantaneous	Momentary R-1 Data Loss	Distributed cluster Multi-site availability Dedicated platforms Virtualization
A-1	Four Hours or Less	Maximum one hour R-1 Data Loss	Two-site hot standby servers Subsystem mirroring Database replication and/or network level mirroring
A-2	Four to 12 Hours	Hours R-1 Data Loss	Two active sites Software mirroring Standby server & db
A-3	12 to 24 Hours	24 hours R-2 Data Loss	Allocated hardware Backup data restore
A-4	24 to 72 Hours	72 hours R-3 Data Loss	Restore application and data from near-line backup
A-5	Weeks	Best Effort R-3 Data Loss	Rebuild system Restore from backup

V. Operational Readiness

Hosting services have requisite dependent application design and hosting engagement process steps that must be followed to support attainment of the specified availability goals. Operational measures are especially relevant for recovery time. These procedures, the supporting tools and the organization need to be evaluated in the context of servicing large numbers of applications and not simply for recovering a single application system.

Mapping for the Operational Measures category is broken down into following subcategories. ITIL standards [1] identify best practices:

- IT Operations and Processes

The processes that need to be addressed in the Operations concept of a system include Service Provider Type, Service Provisioning Model, Help Desk Support, Application Capacity Planning and Performance Management. Implementation of these processes must align the availability requirements with operational readiness and efficiency.

- IT Operations and People / Support Services

Organizational design must align to the service level requirements and scale to deal with a multi-system failure situation where applications of higher classes are given priority to those with more relaxed requirements.

- IT Operations and Tools

These are general capabilities and practices across the IT Operations landscape but should characterize higher degrees of resilience and automation for systems in the A-1, A-2 and A-3 categories. Capabilities include: Infrastructure Level Monitoring, Application Level Monitoring, and Automation of failover processes, Configuration database, Dependency Management, Security, Patch, Risk Management, Problem / Change Management, Software License Management and Automated software deployment.

VI. Organizational considerations

Availability and recoverability is a complex topic, as it not only spans the technology capabilities on which the applications run but the way that applications are designed and operated in the context of surrounding systems and operational setup of the organization. An implementation of the framework requires organizational transformation. Prescriptive controls to address the maturity gap that the overall organization may have may not be realizable in a complex application and infrastructure landscape.

The fundamental consideration managers need to take into account is how to achieve verifiable controls. In the IT industry we observed attempts to achieve this through regulation (very prescriptive rules to comply to) or standardization (by having overarching qualifying rules but elaborating the specific how through defined and implemented standards).

In the context of availability and recoverability, the framework made evident the span of areas touched and the interdependencies between them. Being over-prescriptive presents challenges:

a) *Principles and standards defined need to be interpreted for specific technology and processes*

b) *Ownership of the processes spans organizational responsibilities*

c) *If too prescriptive, you are outdated as new technology and practices are introduced*

d) *Maintaining the rules will be a lot of additional effort – one would rather maintain the architecture, technology and operational standards*

For these reasons we propose that:

i. Regulation should provide qualifying statements of the goal of differentiation and where possible identify higher level principles on how to achieve it (e.g., shared vs dedicated infrastructure)

ii. Standardization should be linked across the functions identified. For example Backup Policy, Backup Architecture Standard and Backup Requirements for Operations

iii. Standardization should be facilitated through the process definitions and technology product offerings

iv. Processes are to include specific deliverable requirements to ensure oversight and quality assurance

Setting the rules does not imply that the organization is better off. An implementation strategy is required for an enterprise-wide improvement that addresses the depth and breadth of this transformation.

VII. Conclusions

This paper has described the overall concept and rationale for defining a risk-based approach to the design and technology usage of systems with respect to availability and recoverability. We have provided an overview of the various dimensions being taken into consideration and have elaborated on the aspects of IT systems that drive the differentiation of best practices or technical capabilities used to achieve the different availability and recoverability classes. The paper gives details on the generic process used for assessment of existing systems. We have explained how we plan to utilize this foundation to establish guidelines for applications and platforms.

This foundation framework provides an enterprise strategy for developing architecture practices, supporting methods, technology and tools. A large, global enterprise requires an enterprise view of availability and recoverability in order to provide a homogenous solution, rather than an set of individual point solutions, devised as business requirements are raised.

In addition, a principal motivation for our availability and recoverability classification is to save cost. Businesses need to classify their IT availability requirements based on distinctions such as those defined in this paper since this will limit the extent of high cost high availability and recoverability architecture required for critical applications. Another aspect of the approach defined in this paper is to drive the design and architecture of applications to lower cost methods of achieving the required levels of availability and recoverability.

References

[1] http://www.best-management-practice.com/gempdf/itSMF_An_Introductory_Overview_of_ITIL_V3.pdf

[2] B. Holenstein, B. Highleyman, and P. J. Holenstein, Breaking the Availability Barrier (Vols 1-3). Bloomington, IN: AuthorHouse, 2007