Spring 2011

Risk Considerations When Determining Network in Infrastructure Upgrade Methodology

Gene Brandt
Regis University

Regis University
College for Professional Studies Graduate Programs
Final Project/Thesis

Disclaimer

Abstract

Risk considerations when determining network infrastructure upgrade methodology have been interesting in areas of cost, time, and path. This paper evolved from a concrete look at upgrading a specific network to a more abstract investigation of the dangers inherent to upgrading large scale networks based on the form the upgrade took. Personal experience had suggested a remove and replace strategy might be most cost effective but planning, scope creep and other factors combined to show risk mitigation is best practiced on a small scale implementation when possible to reduce the consequences of even partial failure. A study of the cost of risk aversion in specific industries seems almost mandated to see if theory in this area is close to practical reality.

Acknowledgements

I would like to acknowledge the individuals who have helped me create opportunities for continued excellence. First and foremost, I would extend thanks to my lovely wife, for her strength and determination and dedication to the journey of us. Secondly, to Robert Krause, who taught me to question every single test result. Lastly, to my children, who teach me more than they know.

Table of Contents

List of Figures

List of Tables

Chapter 1 – Introduction

Tying the upgrade of network infrastructure to the business bottom line is one of the continuing tasks of the consummate IT professional. Dedrick, Gurbaxani and Kraemer (2003) made the case based on 50+ collections of economic indicator data that empirical evidence showed a strong link to IT investment and a company's portfolio prosperity. Unfortunately, making a real world case for the pieces and parts that connect the visible, touchable and obvious signs of customer input can be difficult. Seel (2007) discussed upgrades and such in terms of transformation. His book discussing next generation networks said that program managers and engineers had to "Realize that IT transformation is simply an enabling mechanism for business transformation to a new, more efficient and lower-cost business. First commit to the business transformation program, then commit to the IT modernization program as a key enabler." (A Correct Strategy for IT Transformation, para 2). Rosenberg (2004) noted the measurement of return on investment might tend to ignore or marginalize other contributing factors. His comments are very applicable to the case where the benefit of a working network is one of those marginalized support mechanisms.

The overall goal of this thesis is an exercise in risk management (RM) principle utilization. The research of a least cost method in RM terms as a means for providing guidance and intelligence to discussing network infrastructure plant upgrades. Specifically, in reference to costs incurred during upgrade such as are dependent on the methodology of upgrade utilized. While it can and should be noted that the transport mechanism is a behind the scenes support medium that supplies services to and for the business and its consumers, the technical support requirement of technology as a business supporting mechanism was mentioned by Kallinikos (2006) where it was noted there did not appear to be a direct logical link between IT and business

ends supported, but Dedrick et al. indicated that their collection of data and studies provided the missing link of logical supposition. The two methods of upgrade examined here are incremental or spiral upgrade methods vs. the total removal and then replacement of a current infrastructure. Costing methods and discussion of training for personnel will also be given grounding in real world application, but only at the basic technician or support administration level. The need for upgrade itself should be tied into a business case analysis which dictates the use of new technology or upgrade services to increase the reach of the business, expand the scope of the customer base or more simply put, increase revenue more than the cost of the new equipment and services. Specific to the equipment being replaced are the layers 1-4 (Open Systems Interconnect model) items utilized for network transport but do not include the physical plant such as cabling (network and power), requirements for heating, ventilation and air conditioning, and even space and rack requirements. This does not include the servers, workstations, printers and other end-user or end-point support mechanisms which are direct touch items. These excluded items are only represented in port count requirements which determine transport mechanism sizing.

When to pull the trigger on a network upgrade, and the ramifications in risk to cost are main points in the thrust of this investigation. Is it cheaper and more operationally sound to migrate slowly and methodically or maintain a network plant until absolute replacement is called for? Change for the sake of change in this arena is possibly worse than almost any status quo, in that interoperable equipment may not always follow the released standard for that interoperability. The windows of opportunity for successes in these systems are mostly in the careful planning and quick execution once the resources are gathered. If the cost of upgrading the network is less than the cost to the company for maintenance and repair of the current

infrastructure, or when opportunity might be lost because the tools to take advantage of said chance at greater success are hampered by inadequate resources or availability of resources that can be shown to directly correlate with network interconnections, then the apparent case is easy. The converse is not always the case in that waiting until the last possible moment to begin an upgrade can lead to equipment failure that requires the purchase of resources that were not budgeted.

Baseline

An established network baseline includes the System Interface Document, the System Communications Description and other items and inventories needed to describe the starting point for upgrade related discussions. This starting point was vendor homogenous to simplify the core documentation. This allowed for simpler description of upgrade paths and risk assessments. It is also a necessary starting point for any upgrade process examination.

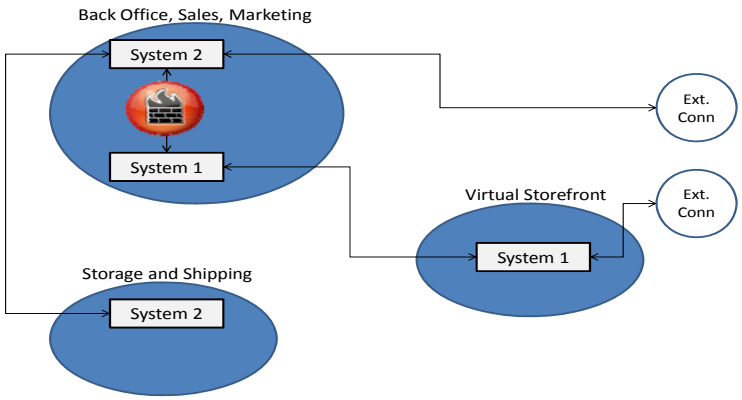

Figure 1. This artifact is a System Interface Document which lays out a generic set of systems which utilize firewall mechanisms to prevent unauthorized traffic from contaminating the offset LAN.

The Systems Interface Document is a very high level overview that should not be expected to change in other than an evolutionary basis. The basis for such change should be technology or assumptions in the marketplace that drive the baseline into other formats. Examples of this change in the past have been the thin-cable (10Base2), thick-cable (10Base5), and Token Ring architectures which have been mostly overtaken by the 'T' or twisted pair based Ethernet series of network constructs. For the purposes of discussion relevant to this endeavor, the baseline will remain static.

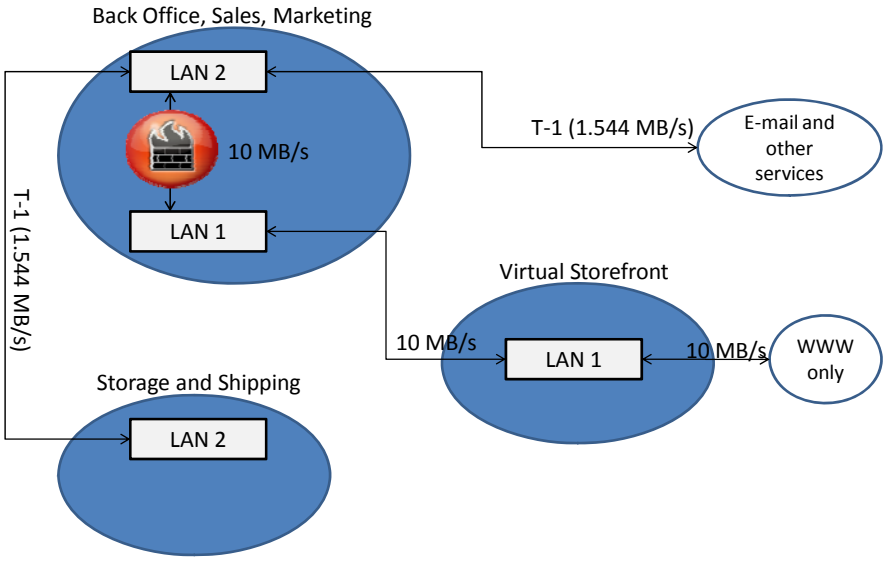

Figure 2. This artifact is the Systems Communication Description utilized in the baseline to provide an example for business requirement for growth into today's generic bandwidth needs. The rates utilized for this SA-2 would have been competitive 15 years ago and still usable between 2000 and 2006. The rates offered today to meet business requirements are larger, though 5 MB/s rates are still available as a starting business rate from companies such as Verizon.

The Systems Communication Description is concerned with the type and speed of communications from system to system. This artifact, in relation to Systems Interface Document

is much more subject to change, as the cost for such change is almost inherent in the upgrade process. The rates chosen seem artificially low in comparison to current standards of network connectivity, but this is in part to demonstrate the requirement for upgrade. Specifically, support for streaming video, voice over IP applications and other bandwidth intensive or latency dependant network services. LAN 2 as shown above would be acceptable or basic email service and file sharing. LAN 1 would be set for support of higher requirements found in virtual storefronts and other service providing entities.

Table 1. Enterprise Building and Personnel Baseline

Location	Description	Number of levels	People per level	Base dimensions
Building 1	Main Office	4	150	300 X 300
Building 2	Back Office	2	100	200 X 300
Building 3	Server Farm	2	25	100 X 200
Building 4	Warehouse 1	1	15	600 X 200
Building 5	Warehouse 2	1	15	600 X 200
Building 6	Warehouse 3 &Shipping Dept.	1	25	600 X 400

This is a high level look at buildings and people being supported by the network infrastructure. This allows for reasoned assumptions for meeting current and perceived requirements. Harler (2006) and Koffel (2001) were used to provide realism in port count determination. Table 1 is an example of part of the baseline information needed to demonstrate upfront planning risks and network sizing requirements. The port count for each building is the number for wired-only access which would be the number of levels multiplied by people per level. One port per eight people for printers/scanners and the like for a medium density of generic input/output were also added. The total thus reached was multiplied by 1.15 to add 15% for possible growth. Switch ports come in series of 2/4/8/12 for the high-speed connections from a supervisory engine and 12/24/48 for basic user and peripheral connections. For that reason,

after the calculations above, the port count should be taken to the next grouping of 12/24/48 depending on what is available and if switch stacking is used or chassis based network connections are employed. The server farm building would have an arbitrarily high port assignment due to transport requirements beyond those required to support individual people. Support in this area often consists of specialized switches and bound channels which share information loads, such as taking four 100Mb/s physical channels or connections and making them logically into a single 400Mb/s stream. Additional channels for management purposes and connections that allow for more robust architecture to prevent single points of failure should always be factored in as well. Total inventory of the network equipment baseline consisted of 34 separate items, some chassis based, all from a single equipment provider to help assure interoperability. The complete baseline inventory of equipment is displayed in Appendix A.

Spiral Planning

With any planning effort, some thought must go into operational risk management. The risks involved with incremental upgrade (and the planning of such) must be detailed in order to present an appropriate picture to decision makers. In this case, upgrading over a series of years or at least in specified increments carries the following risks. The amount of planning going into each increment will be less than that going into an entire remove and replace exercise. This does not mean that less planning will happen over all during the tenure of the network, but it should be recognized that replacing 25% of the network equipment is going to take less effort in planning and implementation at one time than the same effort for a 100% replacement. This degree of planning might be considered less of a risk overall because each upgraded item is likely going to be considered for testing against its direct connections while an entire remove and replace would have to consider each piece as part of the whole from the beginning. The small

scale of iterations makes it easier to consider items as single pieces rather than part of a whole construct, and this focus of attention makes the planning in this area a negative.

The complexity in spiral upgrades is less which is a definite positive on the risk assessment. Fewer pieces should lead to less worry with regard to effects for each of the iterations. This may seem like a flip-flop with regard to the previous risk, but as each is considered only against the upgrade in time, each should be less risky. It is the overall planning risk taken by doing small steps that can cause an avalanche effect. Incremental upgrades are actually less flexible in time, for purposes of risk assessment. This is due to the nature of the upgrade path, in that a decision must be made well prior to the calendar year (CY) implementation of what equipment should be upgraded first. This requires a first rate prognosticator, especially for the items furthest out in time. This inflexibility must be built in and is inherent to the process, otherwise upgrades to the access switches might be the 'best' decision to make multiple years and leave other items in status quo even when they still require upgrading to maintain support. Because of the nature of this method of upgrading, this is deemed a negative. Spiral updates to network systems will generate more document iterations as well. Each of the upgrades will require updates to all system diagrams, leading to a minimum of four rewrites to the baseline system documents and associated material. Version control will be especially important as decision paths are chosen. The ability to step back two or three steps to see what calls were made and hopefully why they were made will be invaluable. The ability of documentation to escape control and be lost, misplaced or otherwise be inadvertently compromised makes this a negative.

Smaller amounts of equipment to install are going to make implementation in this kind of upgrade much easier than a full scale remove and replace. The Keep It Simple Stupid principle

will apply, and the room for errors to be noticed, testing to be completed, and fixes to be coordinated will be much less complex than during a total evolution of the network environment. Stepping back during the implementation is going to be much less difficult as well, even going back to an old architecture as needed while fixes to issues that arise are worked. This is a huge positive in the risk assessment.

Cost control is another risk of any upgrade method. In the case of an incremental upgrade, the initial investment portion is likely to be less while the management over time of a network will tend toward being higher. No company willingly locks themselves into a single provider of services or support, because a failure of that company could mean a failure of the business to continue to prosper. This is never more evident than in the year by year accumulation of network transport which makes every purchase based on cost to purchase at that point in time. The bottom line of cost control in this area is that it tends to make best purchase at the lowest cost without regard for the administrative burden or technical complexity created by a mish-mash of vendors that are only interoperable at the most basic level.

Five methods suggested for spiral upgrade requirements determination are division by port, division by location, division by function, division by maintenance and sustainability and lastly, though frequently not the last picked division by cost of replacement. A mix of more than one method to support cost and requirement needs will likely be adequate for consideration.

The simplest method, division by port, to determine order is not adequate to support upgrade. With the baseline as it is, the chassis based systems would be subdivided, and partial chassis upgrades without adequate room power, HVAC and possibly rack space would undermine the work and put unnecessary strain on the existing infrastructure. Division by location could frontload or backload the cost with the chassis based infrastructure locations being

the largest contributor to that cost. These systems will tend to be the most expensive part of the upgrade. Further subdivision at specific locations such as communications closets or smaller buildings might allow for a more granular approach. The likening of the physical plant to the logical plant is seductive, but the result will not tend toward elegance. Examples in this area utilize references such as Table A1 from Appendix A. The port count method using that information would divide the systems up irregularly and make for an implementation process with more controls required.

Division by function would break the spiral upgrade down into core and access areas, with other possible breakdowns in internal and external connectivity. During the implementation portion of the upgrade, it would be a very good idea to utilize the same methodology in order to minimize extraneous effects brought on by the use of too many variables. This allows for reasoned upgrades on like items throughout the enterprise which when combined with a burn in period would allow technicians to grasp the effects on the network without too many new input parameters clouding the issue. Table A1 is also useful here for description purposes. Grouping the equipment by function (i.e. wireless, switching, routing, external connectivity or other grouping nomenclature) presents well, but the bulk of the dollar cost would reside in the switching arena due to that being the biggest contributor in the hierarchy of network infrastructure.

Division by cost of replacement is taking the entire estimated cost of replacement, dividing it by the number of years during which upgrades will be taking place, and allocating new resources based on this estimate. Plans of this nature are fluid as the price per port is not locked and prices, like inflation, do not tend in a negative direction.

Division by maintenance and sustainability is simple and straightforward. When the items are approaching end of life with regard to sale and support it should be targeted for replacement. If multiple items are expecting a visit from the blue screen of death, then prioritization based business needs should take place. This requirement may obviate a more elegant form of approach in this area, but is one that can be quickly and easily tied into continuing business requirements. Table A2 in Appendix A is representative of a system that upgrades in this manner. Simple and straightforward should not be confused with best either, as it will driving costs based on the current available equipment which may not be flexible in terms of risk or management.

Table 2. Maintenance and Support Upgrade Path – Spiral Example

Nomenclature	Device Type	Number of devices	CY1	CY2	CY3	CY4
Cisco 2501	Router	3	X			
Cisco 2912 XL	Switch	10	X			
Cisco 5509	Switch/Router	6		X		
Cisco 5505	Switch/Router	2			X	
Cisco PIX 515E	Firewall	3			X	
Cisco Aironet 1100	Wireless Access Point	10				X

Note. The spiral upgrade path suggested here is based on the maintenance and supportability with the assistance of a manufacturers extended warranty mechanism. The first to lose support was the first to be replaced even if it did not fall under any of the other requirements determinations.

The process which fit most closely with the examples and tables provided for the spiral method network upgrade was division based on maintenance and supportability. The baseline equipment was dated and required replacement in order to maintain a manufacturer supported contract. The end of life supportability times for many of the items comprising the baseline network was already past, and this made the reason behind the upgrade method the most sensible to concentrate upon.

Remove and Replace Planning

The operational and planning risks associated with non-evolutionary upgrades of networks are complex, both in the initial stages where the entire baseline might be considered a living organism and after the implementation when the planning for the next step in IT prowess must be considered. The detailed layout of current conditions and technical path toward meeting the decision makers requirements are of large import. Specific to this method of upgrade, the following risks are noted.

The upfront planning required for a complete replacement effort is immense. While specific areas of the physical plant may be backwards compatible, with examples of 1Gbps Ethernet being dropped in as replacements for 100Mbps Ethernet, this can only be stretched so far. The starting point for a system must be examined or known to determine the requirements and a lack of documentation in this area is not uncommon. Miller (2006) pointed out multiple areas where lack of documentation created planning and implementation headaches. Thus, the physical plant must be captured and the current network structure from port security, spanning tree optimization, routing and transport concerns, this initial plan has to foresee what the company is going to require four to six years from the completion of implementation. It is a monumental task of sorts, but Moore's law does not appear to be as applicable to network traffic requirements as it is to computer processor growth. The whole scope of the upgrade should allow the pieces and parts to be chosen in a manner supporting graceful interaction, possibly even making selections that permit use of vendor network engineers if they promise a specific degree of consanguinity. The initial planning requirement complexity makes this a negative for any risk assessment.

As mentioned above in the spiral upgrade planning discussion, complexity escalates risk. The plan has to include the entire network from cable plant to the external connectivity requirements and all the bits in between. The good thing about a complete remove and replacement of a local area network transport mechanism is the ability to be flexible. Changes can be made at any part of the network prior to purchase and implementation if modeling and simulation of the new network show bottlenecks that need to be corrected. This is a plus against the spiral technique which would focus on the next piece of the upgrade when a change to existing infrastructure along with the installation might result in a better overall network. Admittedly, it is possible that such changes might be modeled for incremental changes as well and be able to make similar choice break points, that assumes the entire network is remodeled each time a new increment is proposed.

A remove and replace planning effort should generate less documentation over time than a spiral replacement strategy. Oppenheimer (2004) noted that complete documentation can facilitate implementation and approval. The network should be baseline documented a minimal number of times and after the installation, it should not need upgrading until the next significant change. As such, from a documentation point of view, there will be fewer chances for version controls to be misused or unused. Baseline plus revisions in network diagrams that are maintained in an electronic format only are actually each a new baseline. Baseline plus new baseline documentation is the same way, with some fewer iterations. The representative view of a spiral or incrementally upgraded network would sit at baseline plus the number of years the network has been in existence if the upgrade strategy indicated a yearly format to network expenditure. Thus the over time aspect could be considered a positive with risk identification in

that each new version in a spiral would garner versions linearly while the entire network upgrade format would do the same with the versions being separated by years.

Implementation risk identification of a remove and replace construct on the network entire is going to be difficult and complex. From a step back point of view, once the initial trigger is pulled and the upgrade has commenced, every minute puts the entire network about five minutes further from being able to go back to the way it was before. From a staging and burn-in perspective, it is very helpful to have a spare empty warehouse or data center to put the equipment in and lots of spare physical connectivity to make sure the pieces and parts can communicate as advertised. For these reasons, in regard to planning, the risk at implementation is a negative.

Cost control with the upgrade of an entire network at one time is going to come with an extremely high upfront loading. This same upfront cost should allow for concrete management of over-time costs for maintenance and support. Once the network is up and stable, it should require much less care and feeding than a network which is in a constant state of flux or preparation for the next upgrade.

Implementation

Implementation planning has similar concerns no matter what scale the task. This is a question of IP space configuration internal to the company. Should it be maintained in which case the entire setup must be removed and replaced during one long session? Is the equipment put in place and connected via unused copper or fiber to burn in, be tested, verified etc prior to stand-up? Is there space in the communications closets and points of access with adequate power/HVAC and other necessary elements to support this method of change? Each of these

questions raises a cost issue as well, in that answering them often results in the need to provide a least cost solution to a very solvable problem.

With any actual implementation, the choice to hot swap the equipment or configure items for dual operation for burn-in and gradual migration is a risk assessment that is highly dependent on the size of the network and the scale of the implementation. Some parts of this are mandatory paths of action, such as when there is not enough physical space, adequate power, or HVAC in the area the equipment will be located. Environmental drivers like this can be overcome, but building 2x or 3x the real world space, power and HVAC requirement is expensive and in set structures, can be prohibitively expensive to reengineer. This decision point may be made based on musts rather than wants, but is a call that must be made for both upgrade investment strategies.

Documentation of the location and label structure of the physical plant structure is a requirement of any upgrade. McCabe (2003) suggested that lack of documentation caused by network wizards with a trick or two is unacceptable in the enterprise environment. The written portion also allows for the efforts toward upgrade to be reproducible, thus allowing good trends to continue and removing poorly performing assets from the field. Many upgrades today are able to reutilize the existing plant, which is a significant cost and risk savings. If the baseline is properly documented pre-upgrade, and proper controls on changes maintained, this will reduce risk for incremental and complete network enhancements. Failure at this task will result in unexplained preventable network failures caused by low level infrastructure problems such as un-terminated or incorrectly positioned equipment being unable to perform the normal business function.

The use-by date of the documentation is significantly more important on large scale network migrations. The implementation timeline such as that used in high-level scheduling as shown by Oppenheimer (2004) should link the version date to the start of actual installation. Part of pre-implementation capture is labeling connections prior to the move, and possibly capturing the logical information in a cut-sheet manner in order to give the technicians doing the actual change-over the ability to look into the old switch and make sure that the new square connection has been placed in the appropriate square hole. In very large networks, this use-by date becomes closer much more quickly than in small or more static networks. Engineers and technicians will want to put in a date from which no new connections can be made. In a small network such as posed in this thesis that assumption is one that might be valid, depending on network requirements. A new person or piece of equipment sufficiently high in the food chain will upset the apple cart. As such, the introduction of label as you go, or the requirement that any new connection after a specific date utilize a special color code of cable, label or connection making these single problems less of an issue is encouraged.

The logical portion of the network requires the same vigor of application, so that changes after a specific time (be it to a new VLAN, IP structure or spanning-tree root) be captured and relayed to the team responsible for the change. This is where McCabe's "Network Wizard" (2003) commentary becomes most evident. A single failure of this can lead to problems that persist for hours, and multiple applications of the same can stop work on an upgrade for a much more significant length of time. Specifics in this area to layer 2 issues caused by poor tactics are spanning tree loops, broadcast storms, and improper spanning tree roots. Specifics in the realm of IP management are routing loops, inability to connect to network resources, and the possibility

of complete network failure due to device configuration mismatches or poor planning for new equipment.

The last area of concern in the transport support mechanism upgrades is the area of external connectivity and firewall rule-sets. When new installs require IP changes, this can affect external connectivity and routes. The accepted practice of permit by exception is excellent in that it requires strong documentation to use and should therefore give the engineers and technicians responsible to performing the cutover ample direction for when end points change.

Chapter 2 – Review of Literature and Research

The literature related to gathering, measuring, defining and exploring network systems as they relate to the possible costs of the system and returns on investment of the same with regard to risk management of a network upgrade are reviewed below. With the widespread use of these disciplines, and the multiple methods taught in different schools, the review below is not encompassing, but rather representative. The methods for gathering and organizing research for a thesis were presented in books from Creswell (2003) for various suggestions on data collection and Leedy & Ormrod (2005) for research design. The books by Willis (2007) and Yin (2003) were considered but discarded mostly due to a concern of qualitative research versus quantitative results.

Systems Engineering (SE) and Enterprise Architecture (EA) are more typically utilized in large systems with complex interactions. Both SE and EA become more useful in situations where large savings may be found in placement and organization of the network space. The EA process points to this in both its name, and as referenced by Bernard (2005) discussing ROI and TCO of EA. McCabe (2003) and Oppenheimer (2004) both utilized methods other than specific frameworks of architecture such as the EA3 method of capturing the process. SE is also a discipline devoted to enterprise scale endeavors with multiple roles in tying business and network systems processes together.

Specific to EA, reviews were taken of the Zachman Framework, EA3 and the DODAF. Use of EA3 as referenced by Bernard (2005) was suited to discussing the various artifacts and entity types of EA, including network inventory displays along with the multiple flavors of system description documentation artifacts being used for a graphical display of the overall

network picture. The overall suitability of EA3 and its ease of use was the primary driver in selection over other methods of EA.

SE on the network path includes the planning, design, implementation and lifecycle maintenance of the network infrastructure. It is not usually as focused because it is a nominal tool for large and complex scale network creation. SE is entirely applicable to a specific instance such as in this case where the interrelation of the network pieces is not so difficult and the trade-offs are easier to manage. SE specific information perused during this endeavor included utilization of the U.S. Department of Defense (DoD) Defense Acquisition Guidebook, Chapter 4 (2010) and Bernard's "Introduction to Enterprise Architecture" (2005).

Lifecycle management and risk of the network is one of the considerations that an engineer must be concerned with. The cradle to grave planning process is a subtask of the general SE endeavor. The process of documenting the baseline, documenting the changes and planning for and ultimately disposing of specific items or products is integral to the smooth functioning of the network. The multiple literary references from Marcus & Stern (2003) regarding Key High Availability Guidelines, to Seel (2007) talking about Next Generation Network and IT Systems and Oppenheimer (2004) discussing technical constraints in network design indicate that poor planning in this area causes cost overruns when trying to implement changes to network baselines. The DoD Risk Management Guide (2006) in conjunction with Gido & Clements (2006) book "Successful Project Management" were especially helpful in forming the risk identification and assessment portions, both in design of matrix charts and in placing quantitative values against somewhat subjective definitions.

End-point disposal of unsupported network infrastructure can take on multiple forms. These forms range from disposal via contracted refuse support, repurposing in other areas of

concern, donations to charitable organizations or even recycling via the new vendor as part of a trade in program. One point of concern here is that network equipment may be hazardous and thus may fall under the aegis of special rules for disposal of parts. Falling prey to legal and environmental safety concerns benefits no one, thus homework in that area is required. The article that covered this topic in contemporary fashion was from Cisco (2010) discussing equipment end of life concerns.

Open Standards in network support, design and architecture allow for generic skill and tool sets to be used for management of the network. Fabbi & Curtis (2009) were quick to point out that migrating to such a network from a single vendor network could lower cost and risk if managed properly. Though some loss or lack of realization in network performance might be incurred if a proprietary algorithm for routing and/or switching provided a more robust and speedy process. The gains though, in preventing a lock based on equipment manufacturer or network system type, are not minimal from a negotiating and risk standpoint. Oppenheimer (2004) and all other cited non-vendor sponsored texts promote these same open standards or do not mention specific vendors in order to prevent bias for or against a specific company.

Business Case Analysis (BCA) and the Analysis of Alternatives (AoA) are artifacts in the sense of EA, but deserved specific mention due to their importance to this paper. From Bernard's diagrams (2005) and explanations of reasoning for such to Gido & Clements (2006) discussion of lifecycle management and requirements lock-down. The argument for upgrade is moot, so long as there is a business requirement behind that discussion. The baseline setup and maintenance support requirements enhance the need for upgrade. Tables 3 and 4 (Appendix A) are not a specific case but rather indicate a network that reached end of life in many of the items

and needed upgrade. The BCA and AoA to upgrade in this case were network failure and loss of communications that supported the business.

Chapter 3 – Methodology

The methodology used to compile this report was quantitative in nature. The initial baseline and skill set were assumed, created and quantified with regard to possible tax breaks, price incentives or economies in purchasing large quantities. These real world possibilities are not over looked, but for the purpose of examining costs over time vs. cost extremes, the initial state is expected to be operational. The original cost is then moot.

The data collected consisted of cost information with regard to network components of the baseline port count and future requirements in that area. Network obsolescence in the form of supportability from the equipment manufacturer was derived from the baseline manufacturer's website. In addition, port counts based on population density and loaded with arbitrary additional ports to cover growth, special use network peripherals such as printers and scanners we also surmised.

Variables included the possible rates of change in the network, mostly due to network obsolescence in support from the manufacturer. Unknown variables were the amount of cost discount a customer might receive when purchasing an entire suite of network equipment at one time vs. a steady yearly purchase from the same vendor. While the baseline was considered static information, the upgrade path was variable in that it tried to account for the possible cost savings by purchasing cheapest in kind that provided a slight excess to the requirement for upgrade.

Scientific prediction, as inferred from pricing agreements between Cisco & SonicWall (2001) where larger purchases bring in a higher discount than lower volume purchasing, suggested that a spiraled investment in network upgrades will tend to be more expensive than removing and replacing the entire network specific to layers 1-4 of the OSI model. This is

predicated on the possibility of discounts for bulk purchase and the spiral investment of the cost of replacement over time while holding off on that purchase until such period as to spend the entire amount as a capital equipment replacement.

Cost of training or remuneration for specific training was fluid across geographical areas and type of training to tie it specifically into the risks of network upgrades. Depending on the company hiring a specific person, and the skill set they bring, variations in tens of thousands of dollars were readily evident. For example, the Science Applications International Corp will hire a network engineer at a rate between $62-81K per year (2010, Payscale), whereas Cisco Systems Inc hires a person highly qualified in their area at $77-101K (2010, Payscale). The conclusion drawn from a position that was polled in the same geographical area with the same title and duty types indicate that a generically trained individual might be unable to make inroads where a more specifically trained individual might.

Chapter 4 – Project Analysis and Results

TCO in terms of dollars for any network will be dependent on the machinery and human support. The abstract makes it difficult to quantify as the locale, environment, socio-economic norms for the geographical location and other factors well outside the scope of this thesis are all contributors on a real network. TCO in terms of risk and its effects on ROI with regard to upgrading a network is more quantifiable as broad swaths of the process are able to be generalized.

The initial baseline was useful for identifying strategies for incremental upgrade analysis. The vendor maintenance and support issue raised its head quickly, as did the planning requirements sizing for incremental upgrades. The target network as an issue was disregarded, even though the baseline gives insight as to direction for that end point. Issues such as vendor lock, and network homogeneity vs. heterogeneity as referenced by Masuda, Murata and Shibuya 2009) were also examined against the risks identified. In terms of risks in planning an upgrade, these were determined to have a lesser impact than the issues raised below. The remove and replace upgrade format had its own set of complexities that also became apparent during risk identification and assessment.

Table 3. Risk Identification matrix

Area of Concern	Spiral Upgrade	Remove and Replace Upgrade
Upfront Planning	Less planning required	More planning required
Complexity	Less complex to plan and implement	More complex to plan and implement
Flexibility	Less flexible (path dictated)	More flexible (destination dictated)
Document Control	More document iterations	Fewer document iterations
Implementation	Easier to implement	Harder to implement
Initial Investment	Cost control – initial investment lower	Cost control – initial investment higher
Investment over time	Cost control – management over time	Cost control – management over time

Table 3's side by side representation of the identified risks organized under spiral and all-in-one network enhancements. This is a simplified version of the discussions regarding baseline analysis and spiral vs. revamp planning. Each of them had to be viewed in a risk assessment matrix which covered risks in each area, consequences for failure, chance of occurrence, impact of occurrence along with actions and responses to be taken should the success threshold not be met. The areas of risk examined were in upfront planning requirements, complexity in designing a new construct, flexibility or lack thereof in the path chosen, document control specific to versioning and iterations of baseline required, implementation strategies, and costing in initial and overtime states. Each of these items is addressed separately below.

The risk assessment matrix in Appendix B covering the risks identified in both types of network upgrade discussed each in terms of chance of occurrence and impact of occurrence as well as possible responses to each. The consequence categories related mostly to problems created in time, in cost and in flexibility to make changes. The risk categories were in initial planning, complexity, flexibility, documentation and cost control. The bottom line with planning, both with incremental and entire replacement methodologies came to cost, time and

integration concerns. The chances of occurrence ranged from low to medium, but the integration concern with both methods showed a high impact if the event came to pass. In the incremental side, this had to do with the possibility of a vendor mismatch created when two supposedly similarly open source methods are expected to work congenially. Examples of this such as Virtual LANs or spanning tree optimization between different vendors may create instances where the manufacturer's adherence to the open standard is subject to definition. On the entire network replacement methodology, the concern was with upgrades that might require more resources or space than the replaced technology. This could be seen with the Cisco 6500 series which took up more rack space and required more power than the previous Cisco 5500 series of chassis based switches. In both instances, the response was to do the appropriate pre-planning investigation to document issues and mitigate possible problems.

Complexity between the two methodologies is vastly different. The incremental side can drive perfection in requirement that might limit future expansion if honed too sharply. The only high impact problem in complexity is that the testing of the new equipment will typically end up being completed on the live network. This is because without all the pieces being connected, the portion of the network being upgraded does not have all the required pieces and parts to prove the processes are functioning in accordance with registered specifications. The live network connection can create unforeseen network activity through equipment features that are on prior to going live, because of this it was suggested that all upgrades be moved to outside business hours when feasible. The complexity of a remove and replace migration strategy is much higher in terms of number of issues that can arise. Network sizing issues, physical plant requirements, baseline lockdown and testing are all high probability concerns with high being the normal impact in case of event.

Flexibility of the networks leans toward the remove-and-replace strategy for initial effort, in that an entirely new equipment conglomeration is being considered. Flexibility issues in the spiral version are related to the lock-in based on strategy of upgrade, be it a spiral based on port count, item cost, maintenance expiration date or some other item in relation to need. The spirals prior to the current spiral play a large portion in dictating what form the spiral of investment takes if it is to take advantage of previous iterations of network enhancement. This seeming flexibility of doing small steps at one time leads the network down a road that will narrow the future choice possibilities. The incremental impact of consequence vs. that of the enterprise network replacement impact is not an apples to apples comparison at all in terms of range. Failure on the remove-and-replace strategy can cause a business to be unable to meet the requirements of tomorrow, whereas failure on the incremental strategy, at least small failures will be able to be corrected over a period of time.

Baseline document control for either strategy is a concern, with slightly higher chances of consequences on the incremental side of the equation, but with significantly increased scope for failure on the remove and replace portion. The risk increase for spiral investment is just due to the number of times the document trail has to be touched. This can be mitigated or avoided through good change management practices for both evolutions. The baseline verification is also of importance, but again, the impact of failure for many more components is such that small steps seem more cost effective.

Cost Control, both initial and over time are of large concern. The initial costs in comparison to each other are easily surmised. The maintenance and support costs over a period of time are much more dependent on market conditions.

Figure 3. Investment Risk

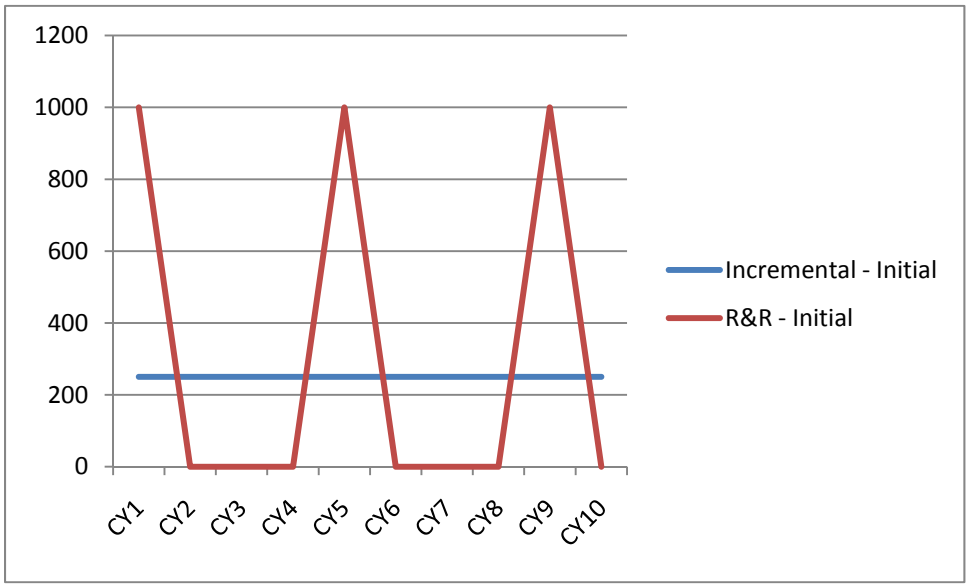

Figure 3. Assuming initial rate of investment is equal to investment overtime as measured in the dollars or buying power at any giving starting point. Utilized to demonstrate the risk inherent with extremely large upgrades. Consequence of failure in large scale investment is shown to be immediate and in proportion to the amount of resources used to invest.

Figure 3 shows similar investment dollars spent over a period of fiscal periods with the spikes in network infrastructure investment being much more severe for the all at once replacement strategy. The risks here on the impact of failure, where two failures of the incremental method of replacement being insignificant when compared to two failures of the remove and replace strategy.

Chapter 5 – Project History

This project started in 2009 with MSCC 697 at Regis University. The idea was to create a generic enterprise baseline for a large, geographically separated company and discuss TCO vs. ROI in large scale upgrades. The concept of studying this started back in early 2005 while working large scale improvement projects in network infrastructure upgrade. The decision to remove and replace an entire 750+ piece network seemed overly complex and an inefficiently realized method for upgrade in the terms above. This project was confined to network layers 1-4 to reduce scope and complexity, and then further defined on these layers to utilize open standards based networking in order to minimize and allow for discounting training requirements, other than those required to be minimally proficient with a specific vendor.

Cost of upgrade as a method of determining TCO and ROI was a seductive line of reasoning, but ultimately, the intangibles were too much to overcome. Capturing the risks inherent in either method of upgrade was more quantifiable and made for an intriguing line of inquiry. This also allowed for the scope to be more minimal as the requirement for pricing of various network component manufacturers became moot.

Focus was directed more on the process of change management than the pieces and parts because the sales figures for pieces of hardware are subject to manipulation. Depending on the starting point for any upgrade, i.e. changing the physical connections set from category 3 cabling to category 5e or higher to support higher data rates or entirely changing the area where specific network tasks are worked are less difficult to quantify and would offer more stability for long term use of the information gathered.

Chapter 6 – Conclusions

With respect to entire investment and the total cost of ownership versus return on investment for network layers 1-4, a spiral investment strategy is likely to turn out to be less expensive over a period of years than a remove and replace wholesale strategy every four to five years when risk is factored in. The remove and replace investment strategy could become more cost effective overtime if no failures in foresight by the system engineers or chief information officers were to take place. Even assuming regular probabilities of low chances of occurrences, taken together, the risks inherent to a remove and replace migration of large and extremely large networks should be avoided short of a complete technology change.

In terms of funding, market variables and vendor discounts made possible by large vs. small purchase defied academically pure description. The risk between 1 and 10 widgets being purchased is not as easily quantifiable due to the human factors involved. Equipment discounts from various manufacturers ranged from zero to 43% depending on factors that are not entirely rational. They have to do with the vendor market and cannot be assumed or hard coded at any point in time. A large scale instance of any network brand that utilizes a specific vendor or manufacturer for the purchase, maintenance and support is likely to receive the same discount for incremental purchases as the one who removes all of one set of equipment and replaces it with another. Vendor lock carries its own risks as well though.

In terms of complexity, a remove and replace strategy has a much larger scope, thus a much more significant room for error. This error and possibility of cost to incur against some labor and engineering rate should not be discounted. As pointed out previously, when changing from one piece of physical equipment to another, the connections must be labeled and some form of documentation must be supplied to the people making the changes. This requirement on a

small scale is not onerous. This same task on a large scale, with large numbers of fiddly bits to be concerned with, is daunting, complex and fraught with peril.

Future consideration in this area would be to step in to plan and document the upgrade of a significantly sized network. The academic discipline of measuring risk might show real world alternatives that were not readily apparent during the research conducted. Research regarding training required to maintain such network and its relation to stability outside environmental or malicious attack concerns might also be of benefit.

References

A Plan To Reduce Enterprise Costs And Risks By Managing End-Of-Life IT Assets Maturing End-Of-Life Management Processes. (2010). Forrester Consulting for CISCO.COM. Retrieved on September 6, 2010 from http://newsroom.cisco.com/images/2010/Cisco-Thought-Leadership-Paper.pdf

Bernard, S.A. (2005). *An Introduction to Enterprise Architecture* (2nd ed.). Bloomington, IN: Author House

Creswell, J. W. (2003). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (2nd ed.). Thousand Oaks, CA: Sage Publications.

Companies and Industries for Network Engineer Jobs. (n.d.). Payscale Inc. Retrieved June 24, 2010 from http://www.payscale.com/research/US/Job=Network_Engineer/Salary

Dedrick J., Gurbaxani V., & Kraemer K.L., (2003). Information technology and economic performance: A critical review of the empirical evidence. [Electronic Version]. ACM Computing Surveys, Vol. 35, No. 1, March 2003, 1–28

Fabbi, M & Curtis, D. (2009). Introducing a Second Network Vendor Saves Money and Solidifies Operations. Gartner RAS Core Research. Retrieved March 20, 2011 from http://www.walkerfirst.com/wa_files/File/literature/Gartner%20Research%20Note-%202nd%20Network%20Vendor.pdf

Gido, J., & Clements, J., (2006). Successful Project Management (3rd ed.). Mason, OH: South-Western Cenage Learning

Harler, C. (2006). *Your Employee-To-Printer Ratio.* www.processor.com, Vol 28, Issue 47. Retrieved August 16, 2010 from http://www.processor.com/editorial/article.asp?article=articles%2Fp2847%2F33p47%2F

33p47.asp

Kallinikos, J. (2006). *The Consequences of Information: Institutional Implications of Technological Change*. Edward Elgar Publishing. Books24x7. Retrieved May 20, 2010 from http://common.books24x7.com.dml.regis.edu/book/id_22383/book.asp

Koffel, W.E. (2001). Calculating occupant loads. *NFPA Journal*. Retrieved August 6, 2010 from http://findarticles.com/p/articles/mi_qa3737/is_200107/ai_n8955440/.

Leedy, P. D., & Ormrod, J. E. (2005). *Practical Research: Planning and Design* (8th ed.). Upper Saddle River, NJ: Pearson Education.

Masuda, H., Murata, K., & Shibuya, Y., (2009). Low TCO and high-speed network infrastructure with virtual technology. *Proceedings of the ACM SIGUCCS fall conference on User services conference*. New York, NY. 321-324

Marcus, E. & Stern, H. (2003). Blueprints for High Availability (2nd ed.). Indianapolis, IN: Wiley Publishing, Inc.

McCabe, J.D. (2003). Network analysis, architecture & design, second edition. [Books24x7 version] Retrieved January 30, 2011 from http://common.books24x7.com.dml.regis.edu/book/id_7059/book.asp

Miller, D.W. (2006). *Why Network Documentation Is So Important*. Network Documentation. Retrieved Jan 23, 2011 from http://www.networkdocumentation.com/index.php?option=com_content&task=view&id=18&Itemid=2

OEM Hardware (with Software) License and Purchase Agreement - Cisco Systems Inc. and SonicWALL Inc. (May 29, 2001). Retrieved October 14, 2010 from http://contracts.corporate.findlaw.com/operations/ip/3724.html

Oppenheimer, P. (2004). Top-down network design. (2nd ed.). [Books24x7 version] Retrieved January 30, 2011 from http://common.books24x7.com.dml.regis.edu/book/id_35337/book.asp

Seel, N. (2007). *Business Strategies for the Next-Generation Network.* Auerbach Publications. Books24x7. Retrieved May 20, 2010 from http://common.books24x7.com.dml.regis.edu/book/id_16424/book.asp

U.S. Department of Defense. (2010). Defense Acquisition Guidebook. Retrieved on October 1, 2010 from https://dag.dau.mil/Pages/Default.aspx

U.S. Department of Defense. (2006). Risk Management Guide for DOD Acquisition. (6th ed.) Retrieved on October 1, 2010 from http://www.acq.osd.mil/se/docs/2006-RM-Guide-4Aug06-final-version.pdf

Willis, J. W. (2007). *Foundations of Qualitative Research: Interpretive and Critical Approaches.* Thousand Oaks, CA: Sage Publications.

Yin, R. K. (2003). *Case Study Research: Design and Methods* (3rd ed.). Thousand Oaks, CA: Sage Publications.

Appendix A

Table A1. NI-3

Description	Barcode	Location	Vendor	Model #
288 Port w/4 100M uplinks	BLDG1	1st Floor Comm room	Cisco	5509
288 Port w/4 100M uplinks	BLDG1	2nd Floor Comm room	Cisco	5509
288 Port w/4 100M uplinks	BLDG1	3rd Floor Comm room	Cisco	5509
288 Port w/4 100M uplinks	BLDG1	4th Floor Comm room	Cisco	5509
144 Port w/4 100M uplinks	BLDG2	1st Floor Comm room	Cisco	5505
144 Port w/4 100M uplinks	BLDG2	2nd Floor Comm room	Cisco	5505
144 Port w/4 100M uplinks	BLDG3	1st Floor Comm room	Cisco	5509
144 Port w/4 100M uplinks	BLDG3	2nd Floor Comm room	Cisco	5509
Firewall	BLDG3	1st Floor Comm room	Cisco	PIX 515E
Firewall	BLDG3	1st Floor Comm room	Cisco	PIX 515E
Firewall	BLDG3	1st Floor Comm room	Cisco	PIX 515E
1 Port Serial, 1 Port 10bT	BLDG4	Middle Comm Closet	Cisco	2501
12 Port w/2 100M uplinks	BLDG4	Left Comm Closet	Cisco	2912 XL
12 Port w/2 100M uplinks	BLDG4	Middle Comm Closet	Cisco	2912 XL
12 Port w/2 100M uplinks	BLDG4	Right Comm Closet	Cisco	2912 XL
Wireless	BLDG4	Left Comm Closet	Cisco	Aironet 1100
Wireless	BLDG4	Middle Comm Closet	Cisco	Aironet 1100
Wireless	BLDG4	Right Comm Closet	Cisco	Aironet 1100
1 Port Serial, 1 Port 10bT	BLDG5	Middle Comm Closet	Cisco	2501
12 Port w/2 100M uplinks	BLDG5	Left Comm Closet	Cisco	2912 XL
12 Port w/2 100M uplinks	BLDG5	Middle Comm Closet	Cisco	2912 XL
12 Port w/2 100M uplinks	BLDG5	Right Comm Closet	Cisco	2912 XL
Wireless	BLDG5	Left Comm Closet	Cisco	Aironet 1100
Wireless	BLDG5	Middle Comm Closet	Cisco	Aironet 1100
Wireless	BLDG5	Right Comm Closet	Cisco	Aironet 1100
1 Port Serial, 1 Port 10bT	BLDG6	Left Middle Comm Closet	Cisco	2501
12 Port w/2 100M uplinks	BLDG6	Left Comm Closet	Cisco	2912 XL
12 Port w/2 100M uplinks	BLDG6	Left Middle Comm Closet	Cisco	2912 XL
12 Port w/2 100M uplinks	BLDG6	Right Middle Comm Closet	Cisco	2912 XL
12 Port w/2 100M uplinks	BLDG6	Right Comm Closet	Cisco	2912 XL
Wireless	BLDG6	Left Comm Closet	Cisco	Aironet 1100
Wireless	BLDG6	Left Middle Comm Closet	Cisco	Aironet

Wireless	BLDG6	Right Middle Comm Closet	Cisco	1100 Aironet 1100
Wireless	BLDG6	Right Comm Closet	Cisco	1100 Aironet 1100

Note. This is the entire baseline inventory non-inclusive of network items outside the realm of this thesis. It would normally include items such as PCs, Servers, and other network attached items in addition to those represented.

Table A2. Maintenance and Support End of Life times

Nomenclature	Device Type	Number of devices	CY Support Lost
Cisco 2501	Router	3	30-Apr-2004
Cisco 2912 XL	Switch	10	1-Nov-2006
Cisco 5505	Switch/Router	2	30-Jun-2008
Cisco 5509	Switch/Router	6	30-Jun-2008
Cisco PIX 515E	Firewall	3	27-Jul-2013
Cisco Aironet 1100	Wireless Access Point	10	18-Jun-2014

Note. This information retrieved from www.cisco.com while investigating specific equipment to see when manufacturer support would discontinue.

Appendix B

Table B1. Risk Assessment

Category	Risk	Consequence	Support	CoO*	I*	Response	Avoid/ Mitigate/ Accept
Incremental Planning							
	Focus on what must be upgraded this CY?	- Cost - Time	- immediate requirement over future need - Shiny tech vs. solid requirement	M	M	- Utilize a Systems Enginneri ng plan approved yearly by CIO/CEO as backside cover for appropriat e actions	Mitig ate
	Integration - Other parts of the network, from computers and servers to protocol stacks in various peripherals to unenhanced routers and switches	- Integration - Future support - Training	- Vendor mismatch - Open standard less optimized than many vendor specific options - Stack mismatch	L	H	- Test Plan with vendor coordinati on	Mitig ate
R&R Planning							

	Forest for trees problem	- Time - Macro and micro problems	- Extreme number of details can overwhelm planners - 100% solution is usually impossible	M	M	- Utilize a Program Manager or Systems Engineer with PM experience to manage taskings and validate completion	Accept
	Integration - concern in this are is with physical plant, and devices that use the network (PC's, servers, NAS, etc)	- Integration - Future support - Training	- Completely unusable network if computers/servers are using TCP and the switch/router is running Banyan Vines only	L	H	- Test Plan with vendor coordination	Mitigate
Incremental Complexity							
	Fewer items can drive perfection in sizing	- Cost - Support	- May limit future expansion	L	L	- Follow SEP and business plan. Future growth + 10%	Avoid
	Physical plant upgrade requirement	- Time - Cost	- Cost overruns if it has to be corrected on the fly	L	M	- Verify baseline plant against upgrades to ensure compatibility	Avoid

	Lockdown window effect	- Flexibility in current support	- No changes during network upgrades to limit causal effects	L	L	- Work with technicians to verify lockdown of baseline - Ensure coordination of techs and install team prior to implementation - Define VIP requirements that override lock down	Accept
	Testing of new items	- Network Crash/slowdown/problems - Business process effects unknown	- No spare network means all testing will be done on the live network to prove the install	H	L to H	- Move all testing that is possible to be moved to after hours - Coordinate with users and customers where possible to notify of possible downtime	Mitigate
R&R Complexity							

		- Depending on size of upgrade this can over or undersize a network by hundreds or thousands of ports			- Verify each building/comm node independently - do it at least 2 times, if there is more than a 5% gap between results,	
More items can drive over/under estimating sizing req	- Cost - Time	- Cost Overruns to fix - Cost savings not realized	H	L to M	investigate	Avoid
Entire physical plant requirement	- Cost - Time - Space	- Failure here will drive up cost, increase time and might also drive changes to building structure	L	H	- Need to compare power, HVAC and space requirements for the new equipment to the old infrastructure to see if it will be supportable	Mitigate
Lockdown window effect	- Time - Flexibility	- Decrease in old network support close to install - No new requirements during later stages of implementation - Last longer than the incremental effect with	H	L to M	- Work with technicians to verify lockdown of baseline - Ensure coordination of techs and install team prior to	Accept

			the same name, just based on number of pieces being worked at a given time			implementation - Define VIP requirements that override lock down	
	Testing of new items	- Space - Cost	- Test and burn-in may require large area/power to accommodate - Reuse of test plant and power is problematic	H	H	- Define test plan and location - Include this cost in the upgrade report	Mitigate or Avoid
Incremental Flexibility							
	Road narrows	- Flexibility	- Previous iterations will drive upgrade path, locking the network resources and capabilities - Completely new technologies may at one point require a completely new start	L	L	- SEP should define migration path way ahead - Update technical baseline to avoid stagnation	Mitigate
R&R Flexibility							

						- Integrate business plan with network strategy - Do not overstate capabilities, if anything, understate them - Avoid the cutting edge of network technology, but also avoid the 10-year model	
	Clean slate	- Flexibility	- Failure to correctly forcast future needs and requirements and unforeseen technical changes in outside technolgies may make a fairly new network obsolete	M	M to H		Mitigate
Incremental Document Control							
						- Utilize lockdown controls and checkout capabilities in work place storage of these vital documents - Update changes and ensure change process includes documentation	
	Baseline Flux	- Time - Flexibility	- Following the wrong plans leads to incorrect assumptions - Can create plans for issues that do not exist or fail to plan for existing issues - Version control/accuracy	M	L to M		Mitigate

						control - Do not close out the job until the doc's are complete	
	Footprint change	- Time	- Updates - Network version control	L	M	- Devote resources required to present an accurate picture of the network	Avoid
R&R Document Control							
	Baseline verification	- Time - Cost	- Bad/Wrong version can lead to purchase over/under size	L	H	- Measure twice, purchase once - Utilize independent or separate teams to verify	Avoid
	Footprint change	- Time	- Changes to the baseline that are not recorded can create problems as other technicians try to use resources or dedicate	L	H	- Lock the network prior to final verification - Create a process whereby VIP support is	Mitigate

			resources that are no longer available			recorded even during the lockdown	
Incremental Cost Control							
	Lower upfront cost	- Cost	- Expectation for future - Cost over time	H	L	- Expectation mitigation with process control - Maintain the infrastructure on same basis as upgrade where feasible	Mitigate
	Variable cost per CY	- Cost	- Flexibility in maintenance - Vendor lock or vendor neutral issues	H	M	- Combine efforts where economic	Mitigate
	Maintenance/support overtime	- Cost	- Flexibility in maintenance - Vendor lock or vendor neutral issues - Training	L to M	M	- Planning in this area needs to include forecasted upgrades where possible	Mitigate
R&R Cost Control							
	Large upfront cost	- Cost	- Expectation for future - Cost over time	H	H	- Show savings over time if possible - Plan and	Accept

						plan again	
	Maintenance/support overtime	- Cost	- Vendor support for non homogenous networks varies	L	M	- Coordinate support and do not purchase equipment from different manufacturers for the same purpose	Mitigate

Note. CoA is Chance of Occurrence measured in Low, Medium and/or High. I is the impact should the problem occur, and is measured in the same format.