Integrating Virtualization and Cloud Services into a Multi-Tier, Multi-Location Information System Business Continuity Plan

Michael D. Mattei
Bellarmine University

Eric Satterly
Bellarmine University

After surviving two significant natural disasters, and numerous man-made ones, virtualizing both of our data centers and installing a geo-clustered private cloud seemed like the perfect way to keep critical systems running during the next major disaster. While implementing our newly minted disaster recovery plan, it became apparent that our strategy was flawed and growing in complexity beyond acceptable limits. Incorporating lessons learned from traditional disaster recovery and business continuity planning, this paper outlines steps to create a plan to match virtualization and cloud tools to a multi-tier, multi-location infrastructure that maximizes the delivery of services under unforeseen events.

INTRODUCTION

In the late afternoon on a spring day in 1985, the senior vice president of administration for a large Midwest consumer products firm called together the senior members of his IT department. It was a group of three department managers, six project managers and six senior analysts and tech support specialists. The director was out of town; most present assumed that was intentional. In a surprise announcement he informed the group that an airplane had just crashed through the roof of the data center destroying the mainframe and the backup mainframe. The door to the tape vault was blocked by the wreckage of the airplane.

One of the senior analysts, who had just spent an entire year writing a disaster recovery plan, walked to the telephone and informed the VP that he would call Sungard to activate the plan but the cost would be $25,000. The VP said, “Don’t bother, they are expecting you.” In spite of a well detailed plan, the scene was quite chaotic. Within 24 hours about 10 staff, including IT audit personnel, were at the (warm, not hot) backup site in Chicago, 300 miles away. A war room was setup in the conference room at the headquarters building and staffed 24 hours a day for the duration of the test.

At the end of three days about 20 staff were at the backup site and one customer order was successfully processed. Since many of the customers turned their inventory over 200 times per year, the goal was to be able to process customer orders within 24 hours of the disaster. In other words, the surprise test was successful, but the plan was not. One of the authors of this paper drove to Chicago with the off-site backup tapes, which were two generations old.

That was the "old days" of the ten thousand square feet centralized mainframe data center, reel to reel tape drives, synchronous modems and truck size diesel backup generators. At the time it seemed quite complex but it looks like "child's play" when compared to the myriad of technology options available today. The problems of keeping it all running are more challenging now because everyone is connected and expect instant access 24 hours a day.

Our university is relatively small but the challenges of keeping the campus information services running reliably has been anything but small. The following partial list of events, many considered tail-risk ones, have seriously disrupted the delivery of IT services to the entire campus over the past 10 years and continue to validate Murphy's Law.

- Email was down for four days angering students, faculty and administrators. A consultant was finally hired to restore service, then the IT Director was dismissed.
- A wind storm, the aftermath of Hurricane Ike, cut off power to campus for two days.
- Less than six months after the wind storm, an ice storm cut off power to campus for five days. Students were sent home. The data center backup generator was not rated to run continuously for more than 100 hours (4.2 days).
- The core network switch was lost during the last afternoon of finals. The backup switch located in the same rack was not configured properly resulting in two hours of LAN downtime.
- A lightning strike fried the entire telephone switch when the telephone was still a major telecommunications service.
- Internet was for down five hours even with two paths off campus to the Internet Service Provider (ISP). The ISP said we would never lose connectivity, ha-ha.
- A cigarette tossed from the balcony of a dorm (even though smoking is prohibited on campus) ignited a small patch of mulch immediately below an 18 inch portion of fiber cable running from the building into the ground to a key campus building across a highway. The vendor responded immediately, but the repair took nearly six hours.
- A water line break on the floor above the hot data center sent water down a stairwell into the data center.

In spite of numerous backup systems and contingency plans, nature and extraordinary man-made events continued to throw curve balls resulting in major service interruptions. After a lengthy disaster recovery and business continuity planning process using a traditional approach (Wallace & Webber, 2010), a formal planning document was created and implementation was begun.

Our initial strategy was built upon two data centers located in separate buildings. The building locations were analyzed in detail. The details included the likely path of a tornado. In 1974 the city was hit by the Super Outbreak of April 3 – 4, 1974, one of the most severe convective weather episodes in the continental United States. The location analysis indicated that if a F4 tornado struck one building the other would be damaged but the data center had a high probability of remaining operational.

Numerous other disasters and significant events were considered and factored into the plan leading to the formulation of the following "broad brush" strategy. The primary goal was 99.9% uptime for the top ten applications serving the University. Five nines did not seem appropriate or necessary for our environment.

- Two data centers (production and hot) located on campus in separate buildings connected underground with redundant fiber optic cable running at 10Gb/s.
- Two core switches each in a network room in separate buildings, specifically the main distribution facilities (MDF) and a backup distribution facility.
- Virtualize all physical servers and employ multiple hosts.

- Utilize synchronous storage area network (SAN) technology, one in the production data center and the other in the hot data center.
- Mirror critical applications in the production and hot data centers so that one takes over if the other is lost.

Implementing the plan would be rather costly but doable if spread over three budget years. As we began developing the original plan, it soon became apparent that the ERP and CRM data were the most challenging to restore. As a result, the decision was made to create a private cloud and mirror all transaction using a synchronous SAN. For the SAN to work effectively, redundant 10 Gb/s fiber optic paths were installed between the two data centers. Everything was going fine until efforts to implement two core switches presented numerous insurmountable challenges. In trying to resolve the communication challenge a few more "gotchas" were identified. For instance, what if:

- There is no true disaster but the data centers lose communication with each other, which one is primary? Do we need a third data center for quorum?
- An errant process deletes a virtual machine or application data base in the production data center? Will the hot data center delete it to stay in synch?
- The VM, SAN, Application layers compete to take control?

Needless to say, while the goal still seemed appropriate, we had to reconsider the plan. The traditional methods of business continuity planning were helpful, but did not seem to address the complexity inherent in the use of virtualization, cloud storage, cloud processing, fiber networks and the Internet. Researching alternative approaches did not identify any processes that adequately addressed the integrated environments prevalent in today's IT infrastructure, so we created one that is detailed in this paper. The most unique aspect of the process is the Critical Services Grid which identifies the locations of each critical application on a Processing-Storage Grid (the "Grid"). Each cell within the Grid lists all the possible processing options on the x-axis and all the possible storage options on the y-axis.

Terminology and Definitions

What would IT be without its acronyms and inconsistent definitions? The following terms and definitions are used in this paper and are the basis for the process presented.

- Event – an occurrence that happens, especially one of importance
- Consequence – a result or effect of an action or event
- Uncertainty – future outcomes not known with confidence
- Risk – uncertainties with possible undesirable outcomes or consequences
- Tail risk event – probability of occurrence is less than 0.03%, virtually nil (beyond three standard deviations from the mean)
- RTO – recovery time objective
- Production site – an organization's active or primary production computing site
- Hot site – an active duplication of the organization's production systems
- Warm site – a site with systems and communications ready to use, just need to restore data and application software
- Cold site – a place to store data, has adequate space and infrastructure
- Mobile site – a self-contained, transportable office custom fitted with IT and communications equipment
- DR/BC – disaster recovery/business continuity

Virtualization Overview

Virtualization is the decoupling of a "system" from its native environment and transplanting it in a new ecosystem. Virtualization is not a new technology. Supercomputers have made use of virtual machines for decades – the 1960's to be exact, but by comparison it is a relatively young technology for servers, networks and clients. However, this is a rapidly maturing technology and most data center computing environments leverage virtualization. There are a number of compelling arguments for virtualization including:

- Data Center Consolidation – reduce the number of physical servers and decrease the footprint
- Outlive Obsolescence – older systems can be upgraded based on business needs rather than out of technical necessity
- Live Migration – the ability to move servers from host to host allows for maintenance to be done anytime
- Snapshots – point in time images of an entire server allows for updates to be done with little risk
- High Availability – combining server and storage virtualization allow for servers to survive a host level crash

It is getting much easier to virtualize. Software exists that allows you to convert a physical server into a virtual machine, the process is called P-to-V and it is very common. With Hardware Assisted Virtualization almost any OS can be virtualized since OS modifications are not necessary to run in that virtual environment. This means that systems can often be virtualized without being upgraded or redeployed. As with most areas of technology, there are trade-offs to consider (Collett, 2011; Kotsovinos, 2011; Lorraine, 2009), but in most cases the benefits outweigh the risks.

Cloud Service Overview

Definitions of the "cloud" vary. Generally a cloud service is one that makes use of hardware and software that is delivered across a network. It often makes use of the Internet, but it is not a requirement. There are many ways to define cloud services.

- Public such as those provided by Amazon, Microsoft, Google, Verizon, etc.
- Private are purely in house implementations for infrastructure, applications, and storage
- Community is a public cloud that is utilized by multiple organizations with similar requirements, usually used by government organizations and universities (Prince, 2015)
- Hybrid is a system that incorporates both public and private cloud elements

The reliability and availability of the network are critical when deploying cloud services. A minimum of 10 Gb/s are generally required for on-site connections and 1 Gb/s for off-site connections. Single points of failure are deadly and contingencies for the loss of a critical point are imperative. The costs of deploying cloud services seem low since many of the public services are priced quite low and are focused on an operational expense model, saving large capital expenses (Anonymous, 2015). A private cloud is not an inexpensive technology, but can provide significant disaster recovery and business continuity benefits.

The costs of a private cloud include hardware, hypervisor licensing, operating system licensing, application licensing, database licensing and of course personnel to keep it all running. It is also important to note that many public cloud services have matured to the point that there are multiple flavors of cloud computing. Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS), are all viable options for cloud-based operations.

THE CRITICAL SERVICES GRID APPROACH

Think Consequences not Events

Traditional approaches to DR/BC planning tend to begin with examining the events or weaknesses that can impact service delivery. Since many of our "disasters" were tail risk events it became apparent that trying to identify all the possible disaster scenarios was futile. Instead, we learned to focus on consequences not events. Brad Brekke, vice president of Assets Protection for Target Corporation, shared some of his organization's methods for preparing for the unpredictable (Blades, 2012). "You can't plan for everything. Instead, we plan for consequences. What happens if you lose communication, transportation, energy?"

Planning for consequences, as Brekke puts it, is one way of broadening the organization's ability to respond to unlikely events. As we focused on consequences and how we would incorporate cloud and virtualization technologies the following process evolved.

Focus on Services not Infrastructure

The first step in the approach begins with identifying the most critical services from the users' perspective and setting an uptime goal for the most critical services. Keeping in mind Pareto's Principle, specifically that 80% of users' needs are filled by 20% of the IT services. Focus on the ones that generate the most complaints if the service or application are not available to user. Think "services" not hardware and software infrastructure which is quite difficult for IT personnel to embrace. We identified 10 critical services.

Step two is to broadly define a user tolerance level (UTL) for various campus operating conditions referred to as service tiers. In our case three campus operating conditions were defined. When the campus is operating normally, everything appears normal to the users. Under these conditions there tends to be a low tolerance for service interruptions. When there is a minor but significant event on campus, maybe most offices are open and most classes are being held, but many people can see or are impacted by an event. In these circumstances the UTL tends to be moderate; users are more accepting of the interruption. In situations when a major event impacts the entire campus or a very large section, everyone can see it or is seriously impacted. For these type of events the UTL tends to be high, namely the users are very tolerant of the service interruption.

Step three is to establish a recovery time objective (RTO) for critical services for each UTL based on the campus operating condition. Higher levels of tolerance generally mean more time to recover. A table is then created similar to the one below.

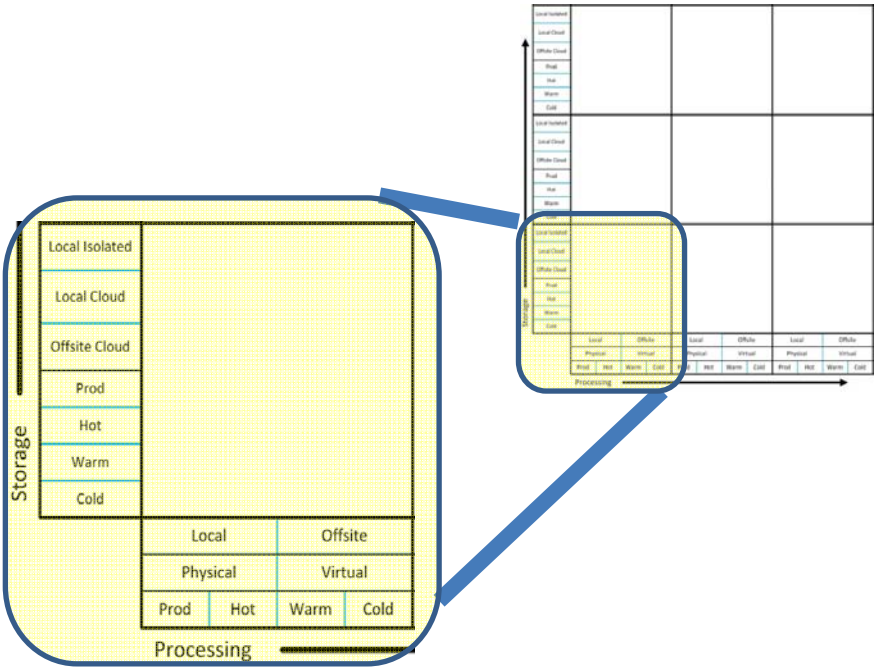
TABLE 1
SERVICE TIER RECOVERY TIME OBJECTIVES

Campus Operating Conditions and Corresponding Service Tiers		
Campus Operating Normally	Minor Disruption to Normal Campus Operation	Major Disruption to Normal Campus Operation
UTL: Low	UTL: Medium	UTL: High
Service Tier 1: RTO < 30 minutes	Service Tier 2: RTO < 4 hours	Service Tier 3: RTO < 2 days

The "Grid"

Step four requires that all unique processing locations be identified and placed on a Processing-Storage Grid (the "Grid"), which defines the various characteristics for each location. Figure 1 shows the Grid template with the storage-processing parameters for a specific cell. Most of the terms are defined above except for Local Isolated. Local isolated storage is basically a local storage device that cannot be seen beyond the physical processor to which it is attached. For each processing location or data center, the parameters of the storage technology and processing technology are identified and circled. The completed location Grid for our operating environment without critical services mapped is shown in Figure 2.

FIGURE 1
CELL PARAMETERS IN THE OVERALL GRID

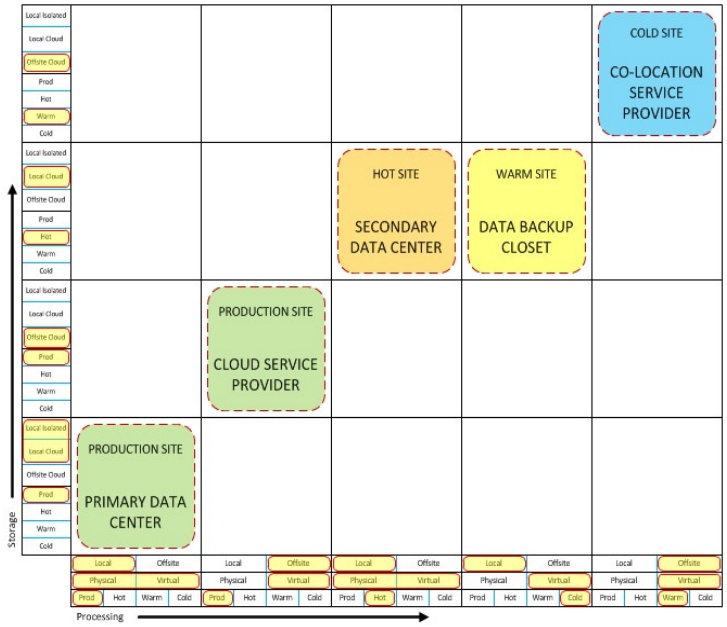


DEVELOP RECOVERY PLAN FOR THE OPERATING NORMALLY, TIER 1

Step five begins the recovery design process. Assume an event occurs that is not obvious to anyone except IT staff, probably an equipment failure, misconfiguration, or logic error. Users will have little patience given a lack of visual evidence that there is a problem. Losing the entire cell is a worst case scenario, but planning for it is the recommended approach since it will include RTOs for each application. The recovery plan will be applicable for the loss of less than a full location.

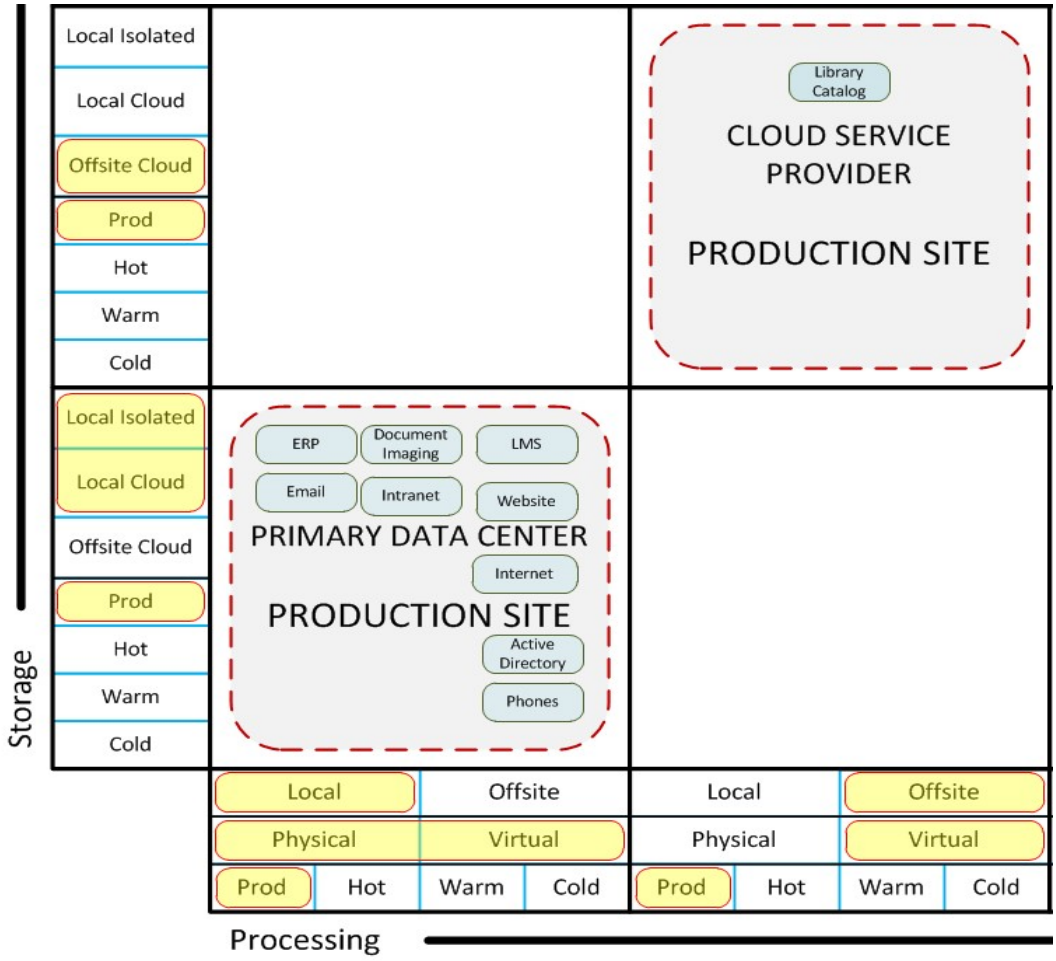
Begin by drawing a big "X" through the box on the Grid that corresponds to the production site. Next, draw a line for each application to a cell where the application can be recovered. Label the line with the amount of time it will take to get the application running to user satisfaction. When estimating time, consider the number of applications that must be recovered and the order of recovery. Did you meet the RTO set in step three? If not, adjust the data center or processing/storage parameters until the RTO can be achieved for all critical services.

FIGURE 2
DATA CENTERS MAPPED ON THE GRID



Step four places the critical applications as they currently exist on the Grid assuming everything is operating normally. The lower left corner of our Grid with the 10 critical applications overlaid becomes the one shown in Figure 3.

FIGURE 3
APPLICATIONS LOCATED ON THE GRID UNDER NORMAL OPERATING CONDITIONS



Strategy statement: Manually initiated recovery to the Hot Site which is a passive data center with a replicated SAN. SAN technology allows for near real-time replication that provides the ability to restore services to a very recent recovery point.

DEVELOP RECOVERY PLAN FOR THE MINOR DISRUPTION, TIER 2

Step six is to develop a recovery plan for a minor disruption. This type of disaster will be obvious to many in the community, e.g. there will be emergency personnel, potential evacuations, etc. Probably a fire, flood, or threat; likely not technically initiated. Users will have some patience as they will likely be focused on gathering information about the event instead of completing their work. Assume the production and hot sites are not operating and not accessible. Decide where to locate the critical services that will meet the RTO set in step three.
Strategy Statement: Maintain a Warm Site that will provide a recovery location. Assume that some parts of one of the campus data centers can be gathered and taken to the Warm Site.

FIGURE 4
RECOVERY PLAN FOR CAMPUS OPERATING NORMALLY

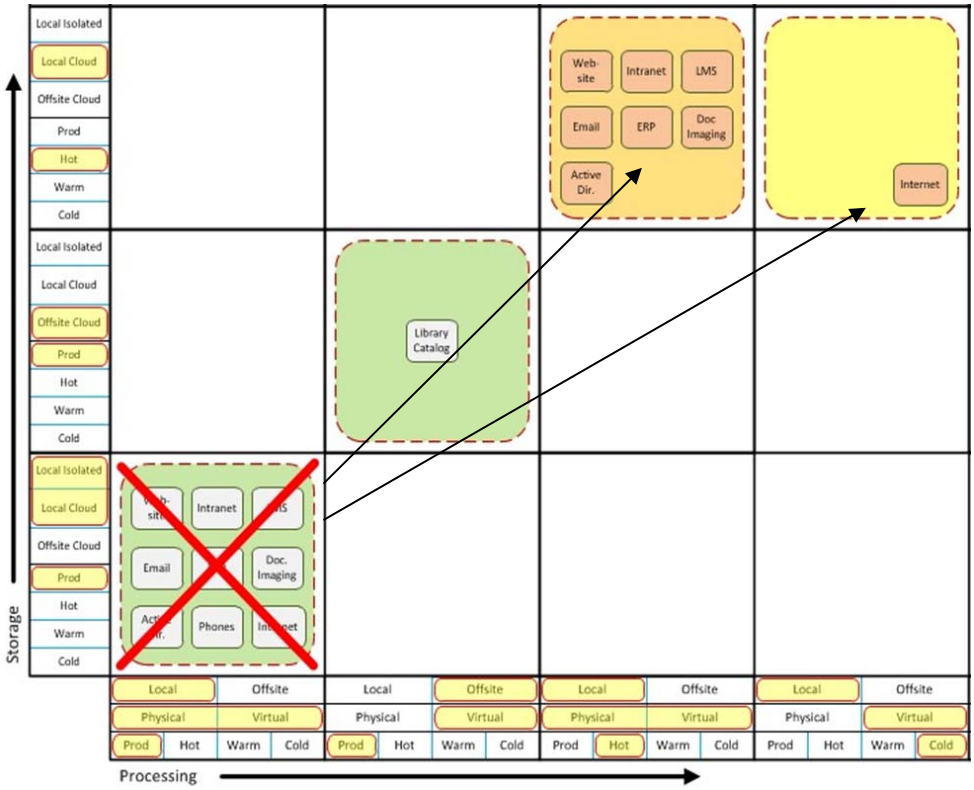
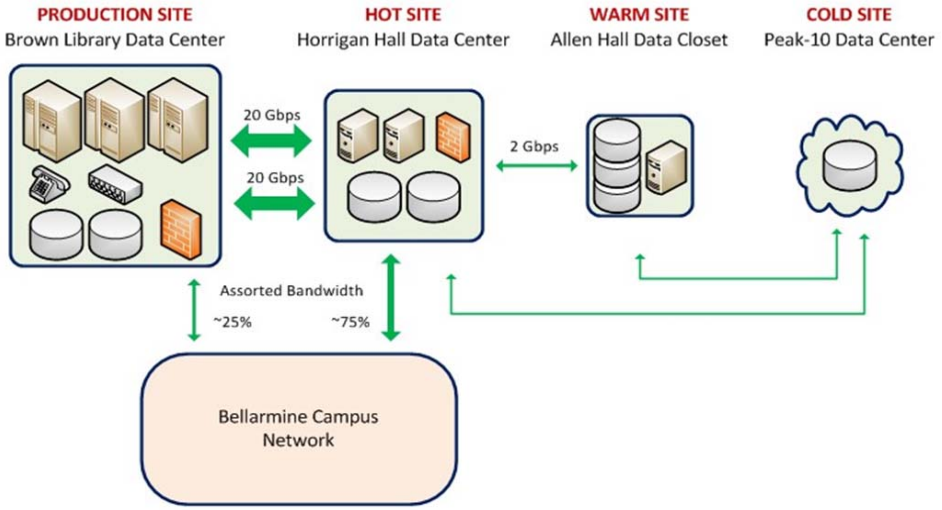


FIGURE 6
IT RESOURCES MAP AFTER STEP SIX



DEVELOP RECOVERY PLAN FOR THE MAJOR DISRUPTION, TIER 3

Step seven is to develop a recovery plan for a major disruption. This type of disaster will be blatantly obvious to the campus and surrounding community. Probably a wide scale "Act of God" type of disaster with large amounts of the university rendered inoperable. All operations are impaired and campus data centers are likely not accessible. Users will have a great deal of patience and will mainly be focused on wanting information. Assume the production, hot sites and warm site are not operating and not accessible. Decide where to locate the critical services that will meet the RTO set in step three.

Strategy Statement: Maintain critical data with a Cloud provider. Processing to be implemented at a Cold site or a Mobile site (a van fitted with recently decommissioned hardware and located in a garage, in our case at the President's house five miles from campus). An alternative would be to rebuild infrastructure processing with the Cloud provider where the data are located.

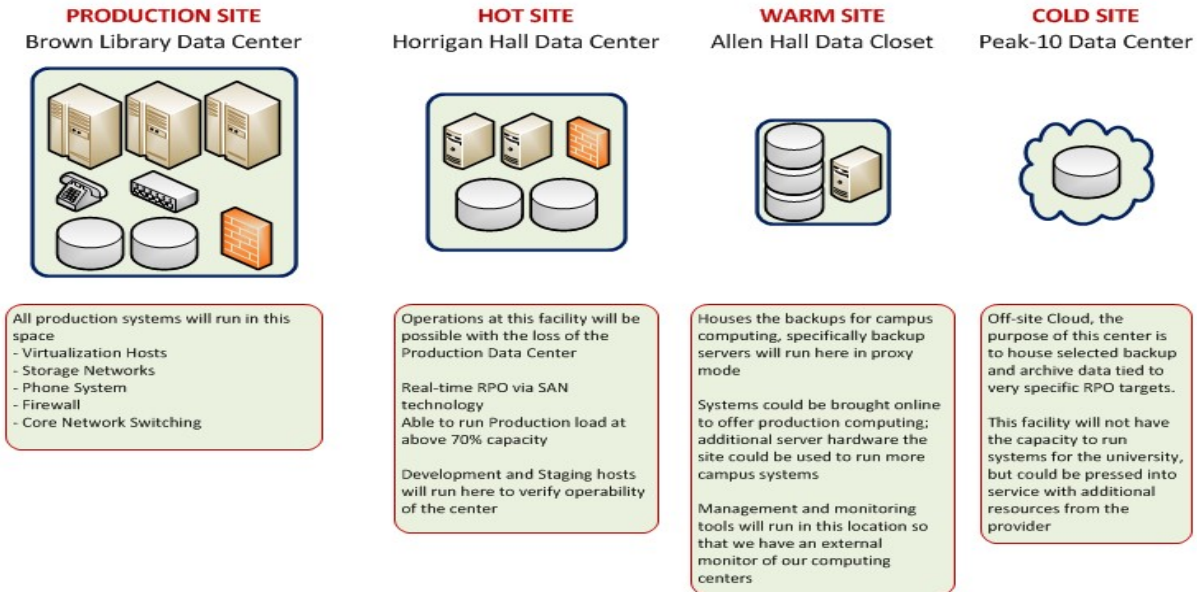
CONCLUSIONS

Virtual and cloud environments have provided numerous benefits to the operation of the data center but these benefits have costs far beyond the financial investment. As the number of applications and data that reside in virtual and cloud environments grows, so does the complexity of managing, controlling and protecting the IT assets.

There are no "right" answers. Rapid changes in technology create many recovery options. When developing your strategy, think consequences and not events or the probabilities of events. Consider user perceptions and tolerances then set appropriate RTOs. There will always be new tools and technologies, so is imperative to implement a process that allows for testing, evaluation and adaptation. Walk before you run; start with one location-tier combination and evolve to meet the needs of your organization.

The process described was condensed and generalized from two years of lessons learned. It can form the foundation for a quick start in applying cloud and virtualization tools to a wide range of organizations. A summary of our multi-location strategy is depicted in Figure 7 below.

FIGURE 7
SUMMARY OF OUR IT RESOURCES CONFIGURATION



REFERENCES

Anonymous. (2015). The Top Trends Driving Cloud Use. *Information Management*, 49(4), 14.

Blades, M. (2012). When the Unpredictable Occurs. *Security*, 49(6), 26.

Collett, S. (2011). Virtual Vexations. *Computerworld,* 45.18:16, 20, 22, 24.

Editor. (2012). Disaster Recovery: 10 Lessons from Hurricane Sandy, *Deloite CIO Journal,* Retrieved October 14, 2015, from http://deloitte.wsj.com/cio/2012/11/29/disaster-recovery-planning-10-lessons-learned-from-hurricane-sandy/.

Khnaser, E. (2010). Faster, Cheaper Recovery. *InformationWeek,* 1262:37-9.

Kotsovinos, E. (2011). Virtualization: Blessing Or Curse? *Communications of the ACM,* 54.1:61.

Lorraine, S. L. & Sawyer, R. (2009). The New Age of Virtualization. *The Internal Auditor,* 66.6:25.

Prince, K. (2015). 5 Benefits of Community Clouds. *Credit Union Magazine, 81*(2), 32-35.

Rice, J. F. (2009). Exploring Disaster Recovery Options. Computerworld, 43.4:26.

Wallace, M. & Webber, L. (2010). *The Disaster Recovery Handbook*. AMACOM, 2nd Edition.

Yarberry, W. A., Jr. (2012). Effective Disaster Recovery Programs are All Alike. *EDPACS* 45.6:1-4.