



# COUNTY OF LOS ANGELES

## CHIEF INFORMATION OFFICE

500 West Temple Street  
493 Kenneth Hahn Hall of Administration  
Los Angeles, CA 90012

**JON W. FULLINWIDER**  
CHIEF INFORMATION OFFICER

Telephone: (213) 974-2008  
Facsimile: (213) 633-4733

August 19, 2004

To: Supervisor Don Knabe, Chairman  
Supervisor Gloria Molina, Chair Pro Tem  
Supervisor Yvonne B. Burke  
Supervisor Zev Yaroslavsky  
Supervisor Michael D. Antonovich

From: Jon W. Fullinwider *Jon W. Fullinwider* (HB)  
Chief Information Officer

Subject: **EXECUTIVE OFFICE INFORMATION TECHNOLOGY (I/T)  
OPTIMIZATION STUDY**

On April 20, 2004, the Los Angeles County Board of Supervisors instructed the Chief Information Officer to evaluate the Executive Office's Information Resource Management (IRM) organization for the purpose of assessing their ability to support and sustain Board operations. This memo transmits the results of that assessment. The Executive Summary and report provide findings and recommendations for each phase of the review process. The team performed a "health check" of the server environment, an assessment of IRM operations and management, an assessment of the technical environment and a brief security review.

The study identifies the opportunity to leverage the recommended organizational changes and upgrades to the server infrastructure as the foundation to launch a strategy of premise-based local area networks (premise-based LANs) and support. In both the private sector and in many levels of government there is a recognition of the mission critical nature of the I/T environment, and the high costs and difficulty in maintaining redundant infrastructures and skilled staff to support distributed server farms and data centers. The conclusion of this report briefly speaks to the opportunity and the need to implement a strategy of premise-based LANs and server consolidation.

Each Supervisor  
August 19, 2004  
Page 2

My office will be scheduling a briefing with your respective I/T Deputies to review and answer questions about the study and to discuss next steps. If you have questions prior the scheduled briefing, please feel free to call me, or in my absence, Jonathan Williams, Chief Deputy, at 213.974.2008.

JWF:JW:ygd

#### Attachments

c: Executive Officer, Board of Supervisors  
County Counsel  
Chair, ISC  
Interim Director, Internal Services Department  
Mark Gascoigne, Internal Services Department

# COUNTY OF LOS ANGELES



**August 2004**

## **EXECUTIVE SUMMARY**

### **EXECUTIVE OFFICE I/T OPTIMIZATION STUDY**

**Executive Office Information Resource Management  
Assessment**

# EXECUTIVE OFFICE I/T OPTIMIZATION STUDY

## Executive Summary

The purpose of this report is to make recommendations for ensuring the operational integrity and sustaining viability of the Board's technology-based resources.

On April 20, 2004, the Los Angeles County Board of Supervisors instructed the Chief Information Officer (CIO) to evaluate the Executive Office's Information Resource Management (IRM) organization for the purpose of assessing their ability to support and sustain Board operations as a direct result of recent events that impacted the Board's ability to communicate and perform basic business functions. In responding to this request, the CIO with assistance from the Internal Services Department (ISD) and several other organizations performed an assessment of the Executive Office's IRM technology infrastructure, its organization and management and the documented procedures in place of delineating processes required to ensure the sustaining viability of services provided to the Board, as well as Commissions and other County departments. On May 4, 2004, a report of preliminary findings was submitted to your Board. The attached report examines in greater depth the technical, management and procedural issues surrounding the Board's I/T environment today, and presents recommendations for correcting and improving the general delivery of technology-based services in a highly reliable and redundant environment. Additionally, the report presents a recommendation proposing a fundamental reassignment of responsibility of server operation and management. This will allow the Executive Office to focus on its core competency, providing direct Board support, and ISD to focus on providing sustained management and operation of IRM's server environment. Based on our review of the Executive Office's fiscal year 2004-05 Business Automation Plan (BAP), the findings of this report align with some of the weaknesses documented by IRM Management, as part of their self-assessment.

### System Outage

Prior to the April 7, 2004 system disruption, a chain of events displaced knowledgeable IRM staff from the day-to-day operations of the central server environment that supports the Board of Supervisors and other organizations. The April 16, 2004 letter from the Executive Officer articulates the circumstances that led to the disruption, and the remedial actions taken by IRM immediately following the incident. However, even considering these extenuating circumstances, the April 7, 2004 disruption highlights the vulnerability of the technology environment serving the Board and other organizations. The loss of key staff members from the Network/Hardware Support Unit (server operations) and incomplete backup processes for their directory services (Microsoft's Active Directory), affected their disaster recovery capability and contributed to the widespread problem experienced in accessing e-mail, calendaring and shared files.

On the afternoon of April 7, 2004, 89% (43) of the respondents to a survey of Board of Supervisors' staff were experiencing difficulties with Microsoft Outlook (e-mail, calendar, contacts) and GoldMine. In addition, users could not access data or documents on shared disk drives. When combined with information provided in the interviews of the staff within the Board offices, this percentage is consistent with the verbal reports of the scope of the problems. The research also revealed that the Board and departmental users were the first to identify and report the problem. It was determined that the Board's directory services had been unintentionally compromised requiring the directory to be recovered. Without directory services, both user profiles and network resources could not be accessed. Since the latest directory backup was approximately three (3) months old, IRM decided to rebuild the directory rather than work with the backup. Within the directory, each person is represented by a unique user security identifier (SID), which is used by the network servers to authorize use of shared resources. If a user's account is deleted and then rebuilt (rather than recovered from a backup), even with the same user name, the user SID is different, and hence appears as a different user to the servers. Consequently, these new user accounts with new user SIDs must be reassigned network privileges. This is the Microsoft Windows server security model since Windows NT 3.1 was released in 1993. Additionally, user profiles must be recreated. As a result, IRM had to visit each user's desktop computer to make the necessary remedial changes. The alternative solution would have been to recover the directory from the latest backup, and then make the appropriate changes that had occurred during the previous three (3) months, such as new or removed users. In this case, only those new users would have been required to endure the process of the recreation of their user accounts, network privileges, and user profiles.

An assessment of the impact of the outage was attempted by issuing two (2) electronic surveys to Board staff in the Hall of Administration and field offices which revealed the average time required to restore a user's computer was 48 hours. The majority of respondents indicated that they were unaware of their dependency and need for basic office services provided by IRM. The percentage of employees affected (89%) by the outage, based on the survey and interview responses, suggests that productivity within the Board offices may have been reduced by 50 percent. In some instances the length of the impact on their operations extended for up to 32 business hours. The financial impact of this incident is estimated at approximately \$300,000 and does not include the cost associated with the impact to the Commissions and other supported departments impacted by the loss of directory services.

## **Assessment Process**

To provide a thorough evaluation of the Executive Office's IRM capability to support and sustain Board operations, a review team was established with representatives from the Chief Information Office (CIO), Internal Services Department (ISD), Department of Public Works (DPW), and the Chief Administrative Office (CAO). Additional resources from the private sector (i.e., SBC Communications, Cisco Systems, Network Associates [NAI], Dell, and Microsoft) were included to provide an outside assessment and make recommendations based on "best practices" applied within their respective organizations. The cooperation of the IRM staff was also vital to obtaining available information, which made the assessment possible.

Three groups were formed and worked in parallel, each focusing on specific areas: Management/Operations (CIO Lead), Technical (Microsoft Lead), and Security (CISO/CIO Lead). See Figure 1.

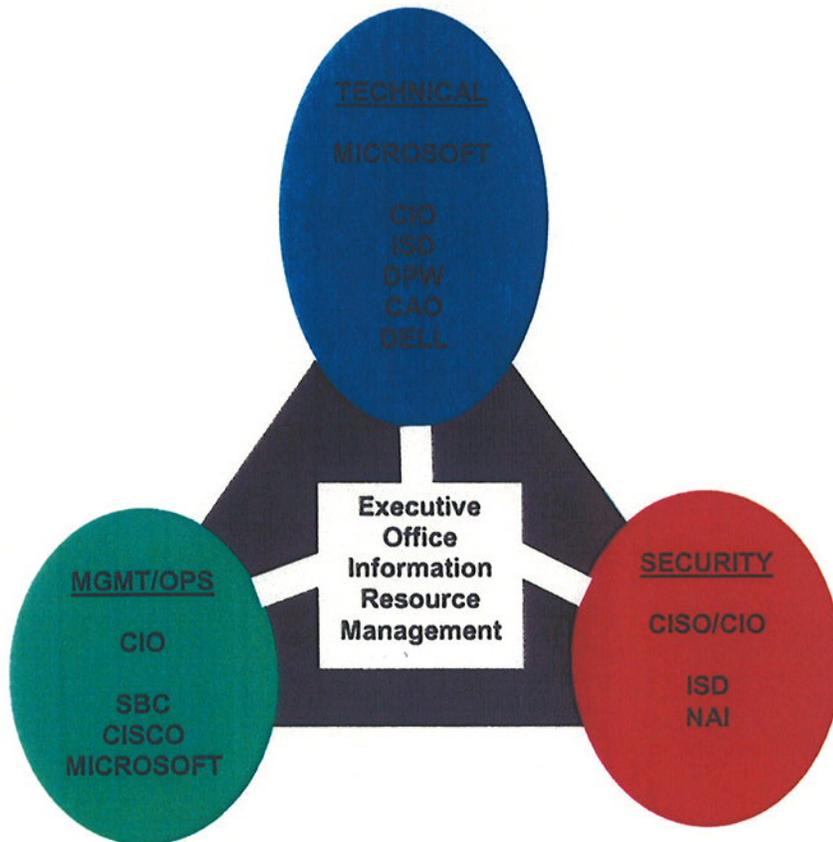


Figure 1

### Summary of Findings and Recommendations

The first activity in the review effort was to assess the stability of the existing server environment to ensure that it was operating reliably with no apparent problems that would cause further interruptions. The result of the review found that the environment was stable with no errors or critical issues that threatened the sustaining operation of the servers. The review also confirmed that the basic technical architecture (i.e., the hardware and software), implemented by the IRM staff was a viable foundation on which to construct a highly reliable and recoverable (future state) server environment.

This is not to suggest that all the issues have been resolved and that the Board's exposure to additional extended outages have been mitigated. The environment was simply assessed to ensure it was operationally stable.

The assessment also included a review of existing documentation (Executive Office Business Automation Plan [BAP], Help Desk logs, operating procedures and other material provided by IRM).

The review of the technical environment, management and operations and security resulted in the formulation of the following findings and resultant recommendations:

**1 Finding:           Management and Operations**

A thorough review of the requirements of the Board offices and other users supported by IRM clearly identified that two very distinct skill sets or competencies are required of the support organization: 1) end-user support and 2) back-office server support. The end-user support requirements include Help Desk support, training, identifying operational needs that can be addressed through use of existing tools or new technologies, remote/home/field office support, and application development and support, with a desire to have an assigned individual responsible for coordinating the delivery of services in a timely and satisfactory manner.

The staff of the Board offices, in interviews and electronic surveys during the assessment, acknowledged that IRM is hard working but they also delineated a number of examples where the level of performance fell short of their expectations and requirements. The specific area most consistently identified was poor communication on the status of reported problems and a desire for a higher level of VIP support (an assigned support liaison that monitors satisfactory and timely resolution of problems and identifies changing technology needs).

The identified requirements for the server support functions focused on the need for highly available computing resources. Each of the offices emphasized that the maximum duration for an unplanned system outage was under four (4) hours. They also emphasized their concerns about the security and integrity of their data. Through the interview process they also identified that the precision with which changes to the environment are carried out frequently falls short of expectations, and these planned events result in extended periods when members of the Board's staff do not have full use of required resources. The subsequent communication about the status of a problem between server support staff and the Help Desk and then to the affected users is a major area of concern.

The IRM staff is best positioned to provide the customer service (end-user support) functions and there is strategic and operational value to the Executive Office in acquiring server and infrastructure support services from an organization that can provide these services as a core competency. Acquiring resources that specialize in the technical area of server and infrastructure support would allow the Executive Office to reassign existing resources that are knowledgeable about Executive Office and Board operations to strategic end-user support and application develop roles, thereby leveraging organizational strengths.

**Recommendation:**

Acquire server support and other infrastructure services maintained by IRM, from ISD, the organization that provides central computing services to County departments. The

existing IRM staff can be used to augment the end-user support activities provided by the Executive Office. See Exhibit 1, Leveraging Organizational Strengths, for an illustration of the recommended division of responsibilities. The Executive Office, the Board and supported organizations will benefit from using the additional capabilities and services that can be provided by ISD.

To minimize expenditure of County resources, ISD and CIO must work with IRM to develop a plan for the assumption of server support for the Executive Office, the Board of Supervisors and other supported organizations. A final proposal and plan that provides project assumptions, approach, timing, organizational responsibilities and cost must be developed and submitted to the Executive Officer of the Board.

**2 Finding:        Technical**

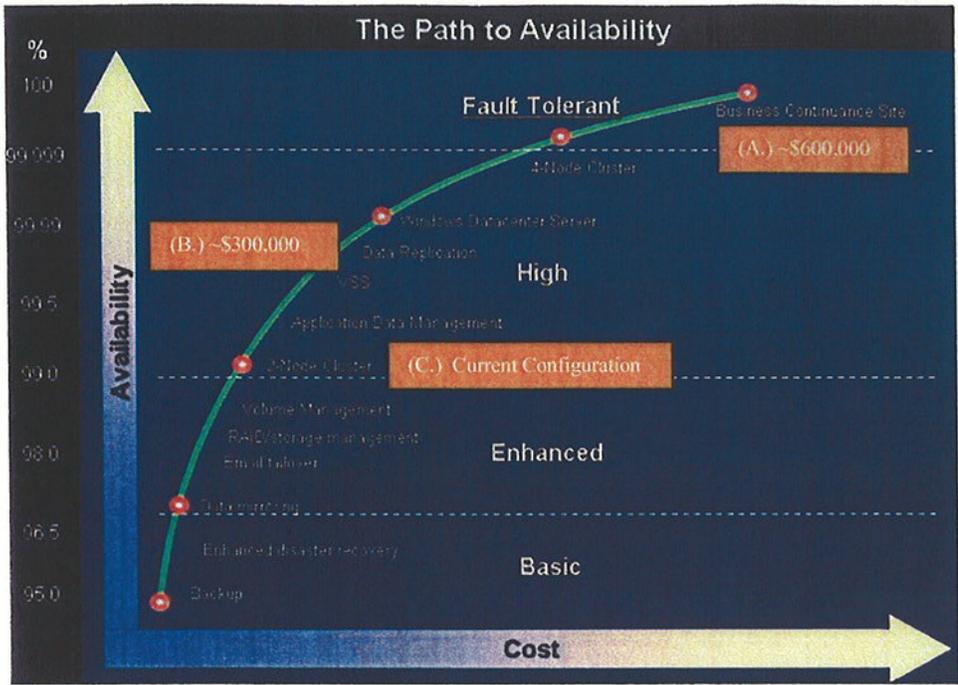
The current server environment supporting the Board, the Executive Office and other supported departments is not sufficient to provide the level of reliability required by its users. Survey responses and direct management and staff interviews confirmed that a high availability infrastructure is essential in allowing the Board offices and other affected departments to operate with a high degree of confidence in their computing environment. The basic infrastructure services must be consistently available, and in the event of a failure, recoverable in a timely manner with an assurance that the integrity of the data and the functionality of the systems is intact. The information provided by the Board offices indicated that a recovery time of less than four (4) hours is essential.

Recommendation:

Upgrade the existing server environment to provide improved redundancy and higher availability. The full report contains a proposed hardware and software upgrade and configuration changes to automate recovery from system failures and provide replication of data for disaster recovery purposes.

Beyond the benefits of providing a highly redundant and reliable server environment managed by ISD, there is an additional opportunity to leverage components of the environment into a cost saving strategy of server consolidation and the ability to deliver premise-based LAN services within the Hall of Administration and Hall of Records.

Server consolidation and premise LANs are common practices being implemented in the private sector and has resulted in significant cost savings with no negative operational impact to the affected organizations. The strategic opportunities associated with server consolidation, premise LAN service delivery and data center consolidation will be highlighted as a key opportunity for I/T optimization, based on the findings of the Board-directed I/T Optimization Study.



**Figure 2 High Availability Architectures**

Figure 2 graphically represents the relationship between cost and percentage of days per year of availability. At point (A) on the graph is a hardware and software configuration that is geographically remote, with fully configured and redundant equipment and real-time data updates that can automatically assume processing without interruption to the application. Configuration (A) estimates unscheduled downtime to average less than one hour per year. Point (B) on the graph identifies the recommended locally positioned configuration providing hardware and software redundancy and real-time local replication of the data. Configuration (B) estimates unscheduled downtime to average less than nine hours per year. Configuration (C), the current configuration, estimates unscheduled downtime to average less than four days per year. The estimated cost shown in this figure is hardware and software acquisition costs only and does not include recurring maintenance, additional staffing or costs associated with the implementation of a full disaster recovery solution.

A more detailed discussion of the estimated reliability and risks associated with high availability and fault tolerant hardware and software configurations is depicted in Exhibit I of the full report.

ISD must immediately be involved with the architectural planning and upgrades to achieve improvements to the IRM server environment. ISD and the CIO will work with the Executive Office and Chief Administrative Office to develop a "takeover plan" and to perfect the estimated one-time cost of \$300,000 for equipment, software and services and an annual estimated maintenance cost of \$400,000, required to provide a high availability server infrastructure, and identify funds to support the proposed changes. The proposed environment will support system recovery of a major hardware or software failure within an estimated two (2) hour interval. The planning and evaluation process will

also need to carefully examine the network infrastructure within the Hall of Administration to ensure that it also supports the high availability model we propose to establish. An examination of the network is not included in this review.

### 3 Finding: End-User Support

The end-user surveys and interviews with the Chief Deputy and Office Manager for each Board office identified that there was a consistent recognition and appreciation for the hard work and dedication of the IRM staff that supported their respective offices. However, they also identified an urgent need for improved communication and improvement in the timely and effective resolution of support issues. As referenced in Finding No. 1, each of the Board offices identified examples in which problems reported to the Help Desk were either closed without a follow-up call to the user to confirm that the problem was corrected or neglected status to the user to reassure them that the problem was still open and being addressed. This lack of communication and the lack of an established standard or target period for problem resolution left the users with no way of knowing when a follow-up call was required or expected. The lack of communication from the Help Desk and the lack of service standards prevent the staff of Board offices from managing the tasks they need to perform and activities for the day. If problems are going to require an extended period to resolve, the user may need to take action to assess required data and other equipment to ensure that deadlines are met.

#### Recommendation:

Adopt within IRM, industry standards and best practices to improve communication to end-users, establish mutually acceptable service levels standards and accountability in managing end-user support. This action aligns with the recommendation for Finding No. 1, which proposes using existing and knowledgeable IRM resources to focus on end-user support to improve overall end-user satisfaction.

The CIO and ISD will work with IRM to identify industry and County standards and best practices as a reference to develop policies, procedures, service level metrics, and staffing levels and training that respond to the needs of IRM's end-users.

### 4 Finding: Security

The assessment confirmed that IRM is in varying stages of implementing security tools that have been identified and recommended through the County's Information Security Program. As members of the team performed the assessment, they provided input and technical recommendations to IRM staff to assist them in implementing security tools or to improve the effectiveness of the tools they had in place. IRM promptly implemented the recommendation on configuring and refining their use of the Network Associates, Inc. (NAI) anti-virus products. The review found that IRM had also acquired and implemented a software product (Altrius) to manage distribution for software and software updates (patches). However, they encountered a hardware problem and the Altirus application was out of service for several weeks pending receipt of new hardware. The hardware problems impacted their ability to schedule assistance from the CAO in properly configuring the product.

IRM also has the complex task of implementing effective information security tools and practices that do not excessively or appropriately limit the functionality in use by their users. The requirements for remote access and the implementation of appropriate and effective security within the private residences of Board members also create potential vulnerabilities that must be identified, understood and mitigated.

Recommendation:

In parallel with the efforts to enhance the stability of the server environment, conduct a security assessment which includes an assessment of network, servers, remote access vulnerabilities and security of the respective offices' documents and e-mail to ensure that the issues and security level required by the Board are met.

The Chief Information Security Officer (CISO) will work with IRM to finalize the scope and requirements of a security assessment for the Executive Office's computing environment. The assessment must 1) identify vulnerabilities, 2) weigh the risks against user requirements and 3) recommend strategies to mitigate the risks, vulnerabilities and exposures of Board and Executive Office information, while preserving important functionality for IRM users.

**Cost**

The following table summarizes our preliminary estimate of one-time costs for recommendations presented in this report. The recommendations without estimated cost figures are anticipated to be completed by existing IRM and/or ISD staff.

<u>Recommendation</u>	<u>Estimated 1<sup>st</sup>-Year Cost</u>
<b>1. MANAGEMENT AND OPERATIONS</b> ISD manage server and infrastructure	\$400,000
1.1 Identify and implement server monitoring tools	\$0
1.2 Document policies, procedures and technical documentation.	\$0
<b>2. TECHNICAL</b> Server upgrade for high availability	\$300,000
<b>3. END-USER SUPPORT</b> Establish standards and metrics for End-User Support – Training (additional staffing not included)	\$25,000
3.1 Improve Help Desk policies, procedures and operations	\$10,000
<b>4. SECURITY</b> Conduct security vulnerability assessment	\$25,000
4.1 Server hardening	\$10,000
<b>TOTAL</b>	<b>\$770,000</b>

## Strategic Opportunities

The assessment performed during this review and the self-assessment in the 2004-05 Executive Office BAP confirm that the IRM organization has a heavy workload and staff that work hard, but largely in a reactive mode. IRM lacks sufficient staff with the breadth and depth of expertise to deliver the required reliability and quality of service to promote efficient and effective use of technology within the organizations they support.

The recommendations highlighted in this report are those deemed most important in effecting a material change in the reliability and quality of services provided to the users supported by the Executive Office.

The recommendations to upgrade the server environment and have ISD assume responsibility for operating the IRM server infrastructure provides improved redundancy, reliability and management improvements by relying on an organization that specializes in the support and management of the server resources. It also provides an opportunity to establish a business continuity plan for the Board, Executive Office and other departments by leveraging the larger ISD plan that is being developed. The ISD Disaster Recovery Plan includes geographically remote recovery facilities. The recommendation to redirect the existing IRM resources to functions that provide end-user support leverages the existing staff's knowledge of Board and Executive Office operations. It also allows improved support for the infrastructure by relying on an organization that specializes in using best practices to support and manage server resources. It also provides an opportunity to improve the business continuity planning by leveraging the larger ISD plan.

The Board members and their staff were left without the tools (word processing, calendaring, e-mail, internet access, etc.) that they have come to rely on in managing the County of Los Angeles. Being accessible to and responsive to their constituents is a vital component of their functions. The estimated cost of the approximately four (4) full work days is estimated at a minimum of \$300,000, and potentially greater cost when considering the intangible impact on public relations. Based on information collected during the study, we have attempted to develop recommended upgrades to the hardware and software infrastructure to improve overall reliability to a more acceptable range (99.9% or not more than nine (9) hours per year of unscheduled downtime). The current configuration, though considered high availability, is estimated to average four (4) days of downtime per year.

The consensus of the overall team is that the IRM organization has staff that works hard, but largely in a reactive mode. There are vacancies within IRM, which if filled with individuals with the appropriate expertise, would improve IRM's ability to deliver the reliability, quality, and effective support required by their users. However, the assessment also identified that additional focus on effectively leveraging existing tools and improving the consistency in which policies, procedures and technical documentation are developed would significantly improve the management and support of the I/T environment(s) of the Board, the Executive Office and other departments.

The recommended organizational changes, improved documentation of policies and procedures, and increased focus on communication, will make a dramatic improvement in the level of satisfaction of the users.

## **Server and Data Center Consolidation Benefits**

The recommended organizational structure will provide the opportunity for server and data center consolidations, the benefits of which are magnified as more departments participate in this model, creating a Hall of Administration or Civic Center "premise network". This strategy and architecture can subsequently be replicated at other major County facilities.

Owning and maintaining a distributed infrastructure is very expensive. Each separate data center/server room must maintain hardware, software, floor space, HVAC (heating, ventilation, and air conditioning), power, data communications, a minimum required head count, and a disaster recovery capability. Further, each data center is sized for the peak workload it encounters, which means for the most part that there is unused capacity during the non-peak times. Overall, the total consumption of resources is considerably greater than if the infrastructure was consolidated and shared.

As the number of servers and disparity of hardware/software configurations decrease through consolidation, the reduction in complexity makes change control, planning, operations, and troubleshooting much easier. Disaster recovery planning also becomes easier as the number of unique platforms and data files is reduced. A more centralized approach can also lead to more consistent backups of data. Moreover, centralized servers are easier to secure physically and logically than distributed servers. The economies of scale and simplified risk profile of a central location enable a higher level of security to be attained. Expensive security tools and support staff can be shared across a larger pool of servers, in contrast the cost of replicated protection can be prohibitive in a distributed environment.

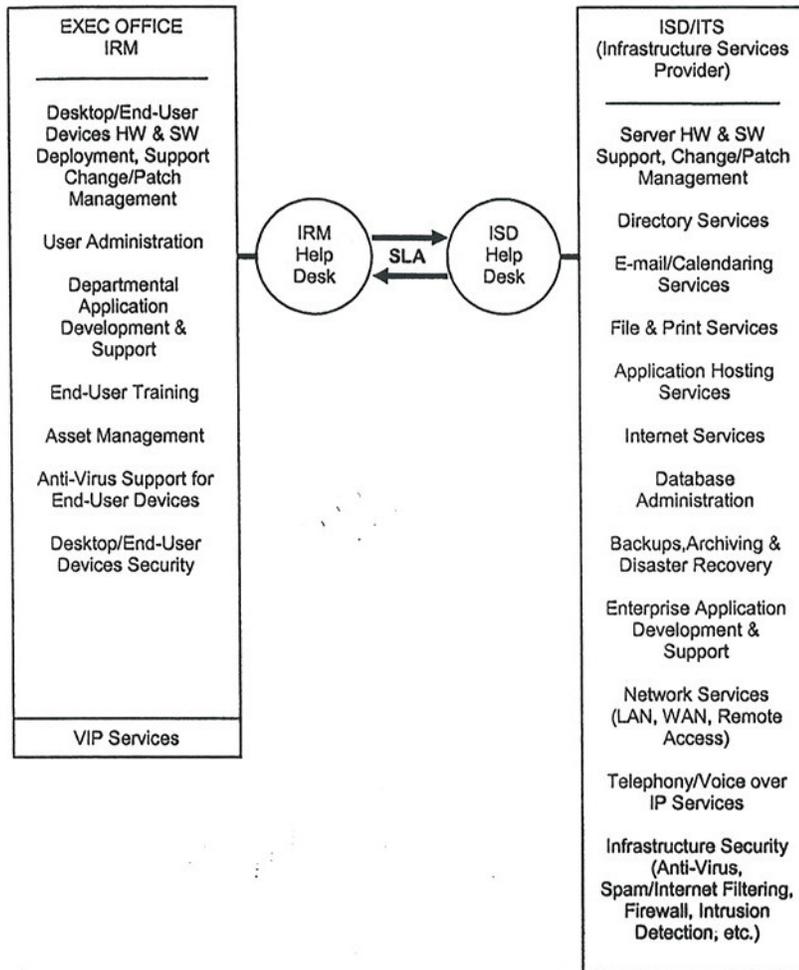
The County is updating its strategic plan to include a strategy that recognizes data as a strategic County asset and the need to leverage its value through sharing. We strongly suggest a plan that includes sharing the data and information technology assets. Directly supportive of that strategy is examining and implementing approaches that improve the cost-effective management of information resources.

## **Acknowledgements**

Exhibit 2 acknowledges the individuals and organizations that invested time in participating in the development of the assessment, findings and recommendations documented in this report. On behalf of the County of Los Angeles, we extend them our sincere appreciation.

# EXHIBIT 1

## LEVERAGING ORGANIZATIONAL STRENGTHS



**ACKNOWLEDGEMENTS**

We would like to extend our sincerest appreciation for assistance provided by the following individuals and their respective organizations:

Los Angeles County, Board of Supervisors

- Barbara Nack, Office Manager, 1<sup>st</sup> District
- Louisa Ollague, I/T Deputy, 1<sup>st</sup> District
- Sandra Fierro, 1<sup>st</sup> District
- John Hill, Chief of Staff, 2<sup>nd</sup> District
- Miriam Simmons, I/T Deputy, 2<sup>nd</sup> District
- Alisa Belinkoff Katz, Chief of Staff, 3<sup>rd</sup> District
- Joel Bellman, Deputy, 3<sup>rd</sup> District
- Brence Culp, I/T Deputy, 3<sup>rd</sup> District
- Gail LeGros, Office Manager, 4<sup>th</sup> District
- Mike Gin, I/T Deputy, 4<sup>th</sup> District
- Kathryn Barger-Leibrich, Chief of Staff, 5<sup>th</sup> District
- Angela Mazzie, I/T Deputy, 5<sup>th</sup> District
- And, all who shared their experiences in our electronic surveys.

Los Angeles County, Executive Office

- Violet Varona-Lukens, Executive Officer
- Charlene Abe, Chief Deputy
- Gary Sysock, I/T Manager
- Martha Campos, Senior Information Resource Specialist
- Andy Xu, Information Resource Specialist

Los Angeles County, Department of Public Works

- Ted Chu, Senior Telecommunications Systems Engineer
- Jeff Orlin, Information Systems Analyst II

Los Angeles County, Chief Administrative Office

- Edwin Ro, Network Administrator

Los Angeles County, Internal Services Department

- Dave Chittenden, Midrange Computing Division Manager
- Jeff Luna, Messaging and Directory Specialist
- Nhan Le, Network Security Specialist

Los Angeles County, Chief Information Office

- Jonathan Williams, Chief Deputy
- Al Brusewitz, Chief Information Security Officer
- Robert Pittman, Assistant Chief Information Security Officer

- John McIntire, Associate CIO
- David Hamamoto, Associate CIO

#### Microsoft Corporation

- Brian Karasawa, Senior Microsoft Services Consultant
- Javier Rodriguez, Senior Technology Specialist
- Don Born, Government Account Executive
- Jim Heflin, Technical Account Manager
- Richard Kwon, Active Directory ROSS Engineer
- Raphael Song, Exchange ROSS Engineer

#### Cisco Systems Incorporated

- Anne Barrett, Executive Advisor
- James Hersey, Account Manager

#### Dell Incorporated

- Dave Otto, Major Account Manager
- Mike Lookingbill, Enterprise Storage Specialist

#### SBC Communications Incorporated

- Steve Itano, Senior Systems Manager of I/T Operations
- Ray Schneider, Technical Sales Executive
- Sandy Chu, Senior Account Manager

#### Network Associates Incorporated

- Dennis London, Senior Systems Engineer
- Bret Brasso, Territory Manager

#### Gartner Incorporated

- Jeff Heath, Senior Account Executive

# COUNTY OF LOS ANGELES



**August 2004**

## **EXECUTIVE OFFICE I/T OPTIMIZATION STUDY**

**Executive Office Information Resource Management  
Assessment**

# EXECUTIVE OFFICE I/T OPTIMIZATION STUDY

## FINAL REPORT

The purpose of this report is to make recommendations for ensuring the operational integrity and sustaining viability of the Board's technology-based resources.

On April 20, 2004, the Los Angeles County Board of Supervisors instructed the Chief Information Officer (CIO) to evaluate the Executive Office's Information Resource Management (IRM) organization for the purpose of assessing their ability to support and sustain Board operations as a direct result of recent events that impacted the Board's ability to communicate and perform basic business functions. In responding to this request, the CIO with assistance from the Internal Services Department (ISD) and several other organizations performed an assessment of the Executive Office's IRM technology infrastructure, its organization and management and the documented procedures in place delineating processes required to ensure the sustaining viability of services provided to the Board, as well as Commissions and other County departments. On May 4, 2004, a report of preliminary findings was submitted to your Board. The attached report examines in greater depth the technical, management and procedural issues surrounding the Board's I/T environment today, and presents recommendations for correcting and improving the general delivery of technology-based services in a highly reliable and redundant environment. Additionally, the report presents a recommendation proposing a fundamental reassignment of responsibility for server operation and management. This action will allow the Executive Office to focus on its core competency, providing direct Board support, and ISD to focus on providing sustained management and operation of IRM's server environment. Based on our review of the Executive Office's fiscal year 2004-05 Business Automation Plan (BAP), the findings of this report align with some of the weaknesses documented by IRM Management, as part of their self-assessment.

### **System Outage**

Prior to the April 7, 2004 system disruption, a chain of events displaced knowledgeable IRM staff from the day-to-day operations of the central server environment that supports the Board of Supervisors and other organizations. The April 16, 2004 letter from the Executive Officer articulates the circumstances that led to the disruption, and the remedial actions taken by IRM immediately following the incident. However, even considering these extenuating circumstances, the April 7, 2004 disruption highlights the vulnerability of the technology environment serving the Board and other organizations. The loss of key staff members from the Network/Hardware Support Unit (server operations) and incomplete backup processes for their directory services (Microsoft's Active Directory), affected their disaster recovery capability and contributed to the widespread problem of accessing e-mail, calendaring and shared files.

On the afternoon of April 7, 2004, 89% (43) of the respondents to a survey of Board of Supervisors' staff were experiencing difficulties with Microsoft Outlook (e-mail, calendar, contacts) and GoldMine. In addition, users could not access data or documents on shared disk drives. When combined with information provided in the interviews of the staff within the Board offices, this percentage is consistent with the verbal reports of the scope of the

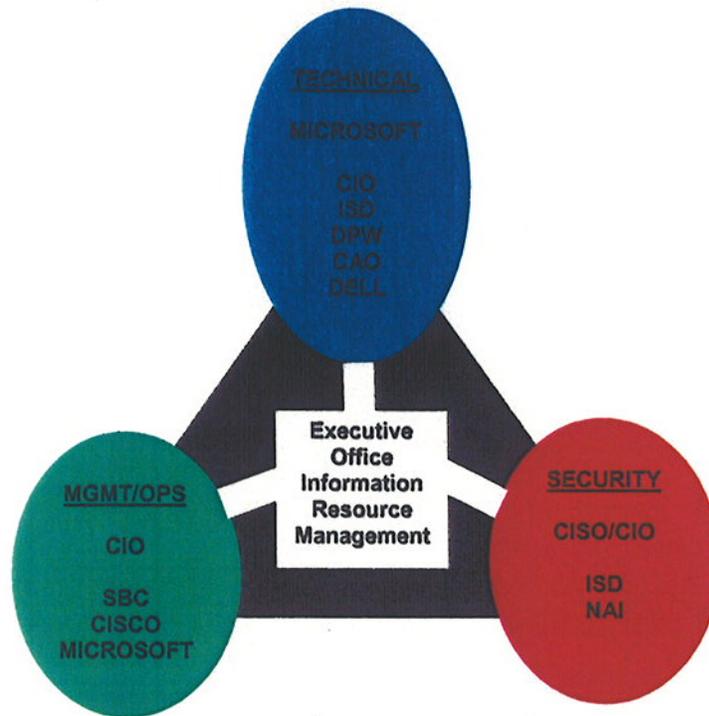
problems. The research also revealed that the Board and departmental users were the first to identify and report the problem. It was determined that the Board's directory services had been unintentionally compromised requiring the directory to be recovered. Without directory services, both user profiles and network resources could not be accessed. Since the latest directory backup was approximately three (3) months old, IRM decided to rebuild the directory rather than work with the backup. Within the directory, each person is represented by a unique user security identifier (SID), which is used by the network servers to authorize use of shared resources. If a user's account is deleted and then recreated (rather than recovered from a backup), even with the same user name, the user SID is different, and hence appears as a different user to the servers. Consequently, these new user accounts with new user SIDs must be reassigned network privileges. This is the Microsoft Windows server security model since Windows NT 3.1 was released in 1993. Additionally user profiles must be recreated. As a result, IRM had to visit each user's desktop computer to make the necessary remedial changes. The alternative solution would have been to recover the directory from the latest backup, and then make the appropriate changes that had occurred during the previous three (3) months, such as new or removed users. In this case, only those new users would have been required to endure the process of the recreation of their user accounts, network privileges, and user profiles.

An assessment of the impact of the outage was attempted by issuing two (2) electronic surveys to Board staff in the Hall of Administration and field offices which revealed the average time required to restore a user's computer was 48 hours. The majority of respondents indicated that they were unaware of their dependency and need for basic office services provided by IRM. The percentage of employees affected (89%) by the outage, based on the survey and interview responses, suggests that productivity within the Board offices may have been reduced by 50 percent. In some instances the length of the impact on their operations extended for up to 32 business hours. The financial impact of this incident is estimated at approximately \$300,000 and does not include the cost associated with the impact to the Commissions and other supported departments impacted by the loss of directory services.

### **Assessment Process**

To provide a thorough evaluation of the Executive Office's IRM capability to support and sustain Board operations, a review team was established with representatives from the Chief Information Office (CIO), Internal Services Department (ISD), Department of Public Works (DPW), and the Chief Administrative Office (CAO). Additional resources from the private sector (i.e., SBC Communications, Cisco Systems, Network Associates [NAI], Dell, and Microsoft) were included to provide an outside assessment and make recommendations based on "best practices" applied within their respective organizations. The cooperation of the IRM staff was also vital to obtaining available information, which made the assessment possible.

Three groups were formed and worked in parallel, each focusing on specific areas: Management/Operations (CIO Lead), Technical (Microsoft Lead), and Security (CISO/CIO Lead).



### Summary of Findings and Recommendations

The first activity in the review effort was to assess the stability of the existing server environment to ensure that it was operating reliably with no apparent problems that would cause further interruptions. The result of the review found that the environment was stable with no errors or critical issues that threatened the sustaining operation of the servers. The review also confirmed that the basic technical architecture (i.e., the hardware and software), implemented by the IRM staff was a viable foundation on which to construct a highly reliable and recoverable (future state) server environment.

This is not to suggest that all the issues have been resolved and that the Board's exposure to additional extended outages have been mitigated. The environment was simply assessed to ensure it was operationally stable.

The assessment also included a review of existing documentation (Executive Office Business Automation Plan [BAP], Help Desk logs, operating procedures and other material provided by IRM).

The review of the technical environment, management and operations and security resulted in the formulation of the following findings and resultant recommendations:

**1 Finding: Management and Operations**

A thorough review of the requirements of the Board offices and other users supported by IRM clearly identified two very distinct skill sets or competencies that are required of the support organization: 1) end-user support and 2) back-office server support. The end-user support requirements include Help Desk support, training, identifying operational needs that can be addressed through use of existing tools or new technologies, remote/home/field office support, and application development and support, with a desire to have an assigned individual responsible for coordinating the delivery of services in a timely and satisfactory manner.

The staff of the Board offices, in interviews and electronic surveys during the assessment, acknowledged that IRM is hard working but they also delineated a number of examples where the level of performance fell short of their expectations and requirements. The specific area most consistently identified was poor communication on the status of reported problems and a desire for a higher level of VIP support (an assigned support liaison that monitors satisfactory and timely resolution of problems and identifies changing technology needs).

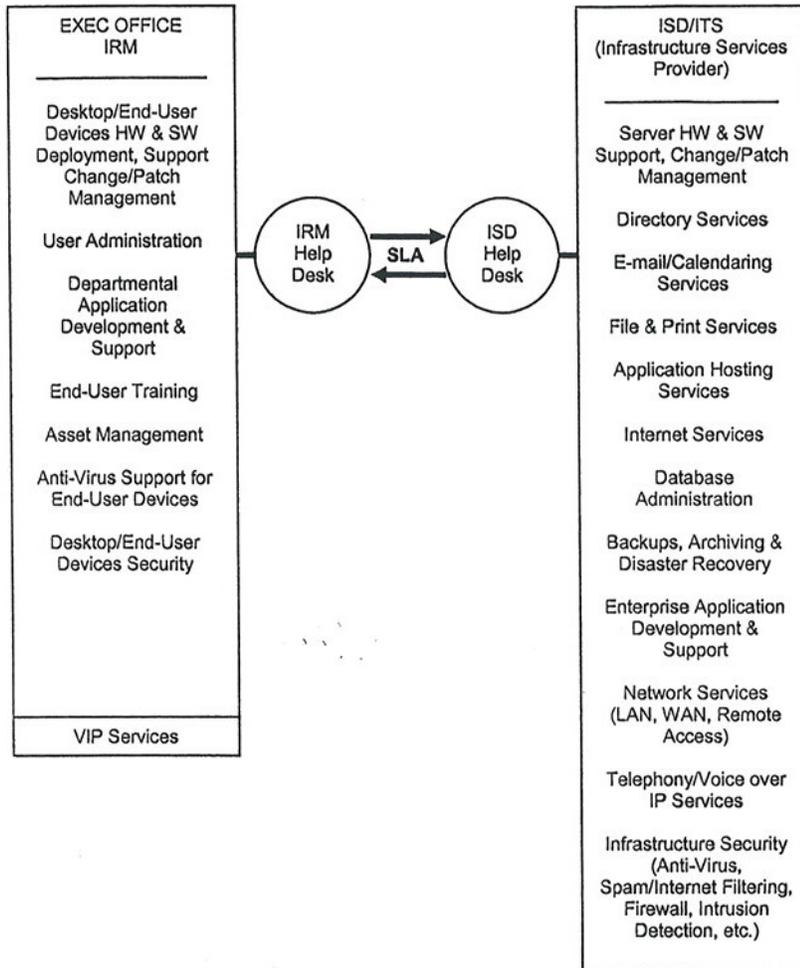
The identified requirements for the server support functions focused on the need for highly available computing resources. Each of the offices emphasized that the maximum duration for an unplanned system outage was under four (4) hours. They also emphasized their concerns about the security and integrity of their data. Through the interview process they also identified that the precision with which changes to the environment are carried out frequently falls short of expectations, and these planned events result in extended periods when members of the Board's staff do not have full use of required resources. The subsequent communication about the status of a problem between server support staff and the Help Desk and then to the affected users is a major area of concern.

The IRM staff are best positioned to provide the customer service (end-user support) functions and there is strategic and operational value to the Executive Office in acquiring server and infrastructure support services from an organization that can provide these services as a core competency. Acquiring resources that specialize in the technical area of server and infrastructure support would allow the Executive Office to reassign existing resources that are knowledgeable about Executive Office and Board operations to strategic end-user support and application develop roles, thereby leveraging organizational strengths.

**Recommendation:**

Acquire server support and other infrastructure services maintained by IRM from ISD, the organization that provides central computing services to County departments. The existing IRM staff can be used to augment the end-user support activities provided by

the Executive Office. See Figure 1, Leveraging Organizational Strengths, for an illustration of the recommended division of responsibilities. The Executive Office, the Board and supported organizations will benefit from using the additional capabilities and services that can be provided by ISD.



**Figure 1** Leveraging Organizational Strengths

To minimize expenditure of County resources, ISD and CIO must work with IRM to develop a plan for the assumption of server support for the Executive Office, the Board of Supervisors and other supported organizations. A final proposal and plan that provides project assumptions, approach, timing, organizational responsibilities and cost must be developed and submitted to the Executive Officer of the Board.

**1.1 Finding:**

The lack of system/network monitors and operational policies and procedures requiring staff to monitor the systems means there is no early warning of failures or alerts that can

trigger ad-hoc diagnostic efforts to determine and accurately isolate the cause of the problem(s). This increases the elapsed time before beginning efforts to correct problems and/or restore the system. Lack of procedures, documentation on system configurations and the absence of system monitors contributes to the vulnerability of the IRM server infrastructure. Use of available system monitors and alerts are standard practices for organizations providing server and infrastructure support as a main mission.

Recommendation:

Implement policies and tools to monitor mission-critical systems that will allow the establishment of a baseline of expected system/network performance. Use of these policies and tools will assist in identifying a system outage during work or off-hours thereby promoting early intervention and an earlier start to system restoration. This recommendation focuses on reducing downtime during normal work hours that impacts productivity and performance against established service levels.

ISD will work with IRM to identify systems and tools available to promptly begin monitoring critical systems to provide early alerts, pending action on our recommendation for the transition of server and infrastructure support to ISD.

**1.2 Finding:**

IRM does not consistently have documented technology-related policies, procedures and technical documentation to guide the management of their operations. Some of the critical facts about their server environment are not documented and are held in the memory of key members of their staff. An informal information technology (I/T) policy environment that does not consistently mandate written policy, procedures and technical documentation limits the ability of temporary or new staff to reliably provide support for the environment. The policies, procedures and technical documentation are essential components of a viable and stable operating environment as well as establishing an effective business continuity capability.

Recommendation:

Establish as a priority, the routine practice of developing written policies, procedures and technical documentation for the server support, end-user support and application development functions. The policies, procedures and documentation will be required to achieve a successful transition of server support to ISD and the reassignment of existing staff to new responsibilities.

IRM must immediately begin the development of technical documentation for the server environment and development of the supporting policies and procedures, which must include performance standards that align with the business needs of the organizations they support. Additionally, immediate action is required to establish policies, procedures and documentation for the end-user support and application development functions to which existing staff may be reassigned.

## 2 Finding: Technical

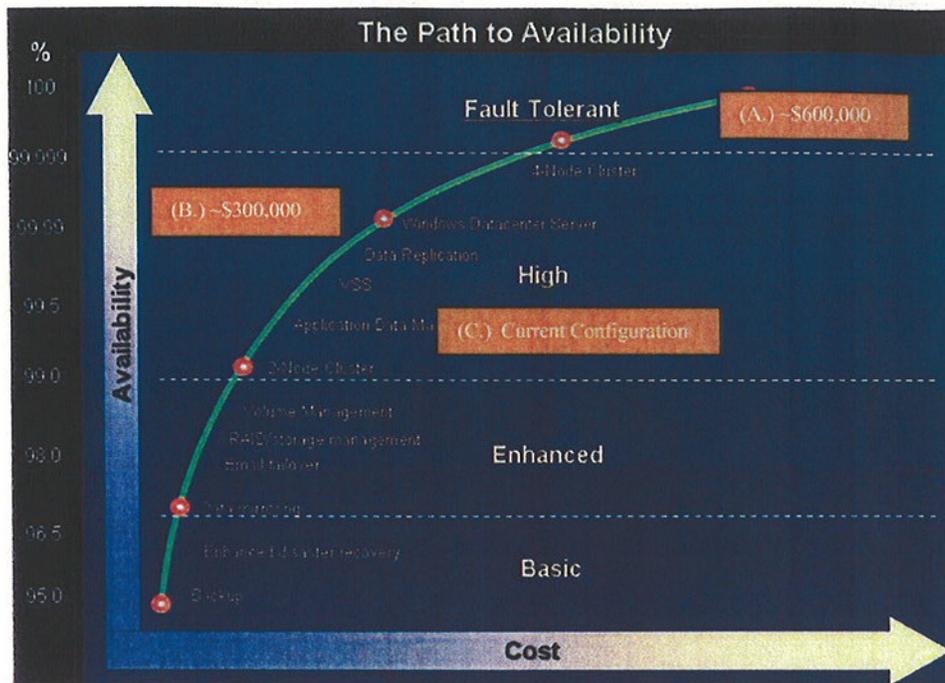
The current server environment supporting the Board, the Executive Office and other supported departments is not sufficient to provide the level of reliability required by its users. Survey responses and direct management and staff interviews confirmed that a high availability infrastructure is essential in allowing the Board offices and other affected departments to operate with a high degree of confidence in their computing environment. The basic infrastructure services must be consistently available, and in the event of a failure, recoverable in a timely manner with an assurance that the integrity of the data and the functionality of the systems is intact. The information provided by the Board offices indicated that a recovery time of less than four (4) hours is essential.

### Recommendation:

Upgrade the existing server environment to provide improved redundancy and higher availability. The proposed upgrade will require additional local hardware, configuration changes and new software to automate recovery of system failures and ensure the rapid data exchange with the County's Downey Data Center, which is operated by ISD.

Beyond the benefits of providing a highly redundant and reliable server environment managed by ISD, there is an additional opportunity to leverage components of the environment into a cost saving strategy of server consolidation and the ability to deliver premise-based LAN services within the Hall of Administration and Hall of Records.

Server consolidation and premise LANs are common practices implemented in the private sector and has resulted in significant cost savings with no negative operational impact to the affected organizations. The strategic opportunities associated with server consolidation, premise LAN service delivery and data center consolidation will be highlighted as a key opportunity for I/T optimization, based on the findings of the Board - directed I/T Optimization Study.



**Fig. 2 High Availability Architectures**

Figure 2 graphically represents the relationship between cost and percentage of days per year of availability. At point (A) on the graph is a hardware and software configuration that is geographically remote, with fully configured and redundant equipment and real-time data updates that can automatically assume processing without interruption to the application. Configuration (A) estimates unscheduled downtime to an average of less than one hour per year. Point (B) on the graph identifies the recommended locally positioned configuration providing hardware and software redundancy and real-time local replication of the data. Configuration (B) estimates unscheduled downtime to average less than nine hours per year. Configuration (C), the current configuration estimates unscheduled downtime to average less than four days per year. The estimated cost shown in this figure is hardware and software acquisition costs only and does not include recurring maintenance, additional staffing or costs associated with the implementation of a full disaster recovery solution.

A more detailed discussion of the estimated reliability and risks associated with high availability and fault tolerant hardware and software configurations is illustrated in Exhibit I.

ISD must immediately be involved with the architectural planning and upgrades to achieve improvements to the IRM server environment. ISD and the CIO will work with the Executive Office and CAO to develop a "takeover plan" and to perfect the estimated one-time cost of \$300,000 for equipment, software and services and an annual estimated maintenance cost of \$400,000, required to provide a high availability server infrastructure, and identify funds to support the proposed changes. The proposed environment will support system recovery of a major hardware or software failure within an estimated two (2) hour interval. The planning and evaluation will also need to carefully examine the network infrastructure within the Hall of Administration to ensure

that it also supports the high availability model we propose to establish. An examination of the network is not included in this review.

**BENEFITS/RISKS SUMMARY OF HARDWARE CONFIGURATION OPTIONS.**

<b>Configuration</b>	<b>Benefits</b>	<b>Risks</b>	<b>Cost Increase</b>
<p><b><u>Current Environment</u></b></p> <p><b>(C)</b></p> <p><b>Local Cluster</b></p> <p>Redundant hardware and software components</p>	<ul style="list-style-type: none"> <li>- 4 day average downtime/year</li> <li>- minimal impact on users when applying patches, etc.</li> </ul>	<ul style="list-style-type: none"> <li>- no protection from failures caused by corrupted Exchange data structures</li> <li>-limited protection from software failures</li> <li>- no protection from building infrastructure problems</li> <li>-no protection from internal network failures</li> <li>-no protection from external network problems</li> </ul>	\$ 0
<p><b><u>Option #1</u></b></p> <p><b>(B)</b></p> <p><b>Mirrored Cluster/Remote Data Replication</b></p> <p>Fully redundant systems with synchronized remote data back-up</p>	<ul style="list-style-type: none"> <li>-9 hours average downtime/year</li> <li>- protection from failures caused by corrupted Exchange data structures</li> <li>-protection from software problems</li> </ul>	<ul style="list-style-type: none"> <li>-moderate cost</li> <li>- no protection from building infrastructure problems</li> <li>-no protection from internal network failures</li> <li>-no protection of external network problems</li> </ul>	~ \$ 300K
<p><b><u>Option #2</u></b></p> <p><b>(A)</b></p> <p><b>Geo-Cluster</b></p> <p>Two identical and synchronized systems residing in different geographic areas</p>	<ul style="list-style-type: none"> <li>-1 hour average downtime/year</li> <li>-protection from failures caused by corrupted Exchange data structures</li> <li>-protection from software problems</li> <li>-protection from building infrastructure problems</li> <li>-limited protection from internal network problems</li> <li>-limited protection from external problems</li> </ul>	<ul style="list-style-type: none"> <li>- higher cost</li> <li>-complexity</li> </ul>	~ \$600K

**Figure 3 Benefits/Risks Summary Of Hardware Configuration Options**

**3 Finding: End-User Support**

The end-user surveys and interviews with the Chief Deputy and Office Manager for each Board office identified that there was a consistent recognition and appreciation for the hard work and dedication of the IRM staff that supported their respective offices. However, they also identified an urgent need for improved communication and improvement in the timely and effective resolution of support issues. As referenced in Finding No. 1, each of the Board offices identified examples in which problems reported to the Help Desk were either closed without a follow-up call to the user to confirm that the

problem was corrected or neglected to advise users of status to reassure them that the problem was still open and being addressed. This lack of communication and the lack of an established standard or target period for problem resolution left the users with no way of knowing when a follow-up call was required or expected. The lack of communication from the Help Desk and the lack of service standards prevent the staff of Board offices from managing the tasks they need to perform and activities for the day. If problems are going to require an extended period to resolve, the user may need to take action to assess required data and other equipment to ensure that deadlines are met.

Recommendation:

Adopt within IRM, industry standards and best practices to improve communication to end-users, establish mutually acceptable service levels standards and accountability in managing end-user support. This aligns with the recommendation for Finding No.1, which proposes using existing and knowledgeable IRM resources to focus on end-user support to improve overall end-user satisfaction.

The CIO and ISD will work with IRM to identify industry and County standards and best practices as a reference to develop policies, procedures, service level metrics, and staffing levels and training that respond to the needs of IRM's end-users.

**3.1 Finding:**

Based on the user surveys and subsequent interviews with members of the Board offices, the performance of the Help Desk was a consistent area of frustration. The concerns identified centered on communication and timely response to reported problems.

Help Desk calls are recorded in HEAT, an automated Help Desk management tool. But the current status, preliminary actions and description of the solution are not entered into the system. The staff conducting the assessment was not able to identify any analysis performed by IRM to help identify patterns in problems to allow proactive actions. The responses from users indicated they do not receive feedback or follow-up from the Help Desk. The reported dissatisfaction captured in the surveys and interviews is inconsistent with the data on user satisfaction that is entered into the HEAT System. See Exhibit II and III. No mutually acceptable service level standards have been established, so there are no user accepted criteria which allows users to measure satisfaction. Exhibit IV is a discussion of customer satisfaction and I/T performance measures, with an example of an end-user support scorecard measurement tool.

Recommendation:

Develop procedures and systems to make greater use of HEAT, the Help Desk management system. The procedures must require solutions to be documented and reviewed to build an internal knowledge base. HEAT data should be reviewed and analyzed for trends and to continuously identify opportunities to manage service requests and to improve service delivery. IRM must develop mutually acceptable service level standards which are communicated to their users.

IRM should promptly review the functionality of the HEAT system and update procedures to take full advantage of the software's ability to compile a knowledge base to speed the resolution of repetitive problems and create opportunities to take proactive actions to reduce problem calls and increase user satisfaction.

IRM should consult the ISD Customer Assistance Center (CAC), ISD's Help Desk, to see if there are policies, procedures and service level standards that might be discussed with users and refined for IRM's user population.

#### **4 Finding: Security**

The assessment confirmed that IRM is in varying stages of implementing security tools that have been identified and recommended through the County's Information Security Program. As members of the team performed the assessment, they provided input and technical recommendations to IRM staff to assist them in implementing security tools or to improve the effectiveness of the tools they had in place. IRM promptly implemented the recommendation on configuring and refining their use of the Network Associates, Inc. (NAI) anti-virus products. The review found that IRM had also acquired and implemented a software product (Altrius) to manage distribution for software and software updates (patches). However, they had encountered a hardware problem and the Altrius application was out of service for several weeks pending receipt of new hardware. The hardware problems impacted their ability to schedule assistance from the CAO in properly configuring the product.

IRM also has the complex task of implementing effective information security tools and practices that do not excessively or appropriately limit the functionality in use by their users. The requirements for remote access and the implementation of appropriate and effective security within the private residences of Board members also create potential vulnerabilities that must be identified, understood and mitigated.

#### Recommendation:

In parallel with the efforts to enhance the stability of the server environment, conduct a security assessment, which includes an assessment of network, servers, remote access vulnerabilities and security of the respective offices' documents and e-mail to ensure that the issues and security level required by the Board are met.

The Chief Information Security Officer (CISO) will work with IRM to finalize the scope and requirements of a security assessment for the Executive Office's computing environment. The assessment must 1) identify vulnerabilities, 2) weigh the risks against user requirements and 3) recommend strategies to mitigate the risks, vulnerabilities and exposures of Board and Executive Office information, while preserving important functionality for IRM users.

#### **4.1 Findings:**

The detail review of the server environment found that there were certain permissions (capabilities) assigned to the global "Everyone Group" which are a default setting following installation of the Exchange (e-mail) server. The errors or issues with the

permissions or rights for established groups on the Exchange and file servers can result in inappropriate personnel having access to data that should be private or restricted to a very limited number of users. In some instances depending on the nature of the permission, data could be exposed across Supervisory Districts or departments.

These permissions must be carefully reviewed to determine if they are appropriate or if they were default settings simply overlooked during the installation process. Failure to review and revise default settings on servers during the installation process can create serious security vulnerabilities.

Recommendation:

The services of a technical consultant should be acquired to assist with the "hardening" (strengthening security by eliminating vulnerabilities) of the Executive Office's server environment. This requires carefully reviewing the requirements of the different groups of users supported by the IRM. Server hardening also limits functionality of the Microsoft products. The appropriate balance of risk for the sake of functionality versus security must be determined.

Working with the CISO and ISD, develop an approach to acquire the necessary expertise from within ISD or from a technical consulting contractor to complete an assessment and harden the server environment.

**Cost**

The following table summarizes our preliminary estimate of one-time costs for recommendations presented in this report. Those recommendations without estimated cost figures are anticipated to be completed by existing IRM and/or ISD staff.

<u>Recommendation</u>	<u>Estimated 1<sup>st</sup> - Year Cost</u>
<b>1. MANAGEMENT AND OPERATIONS</b> ISD manage server and infrastructure	\$400,000
1.1 Identify and implement server monitoring tools	\$0
1.2 Document policies, procedures and technical documentation.	\$0
<b>2. TECHNICAL</b> Server upgrade for high availability	\$300,000
<b>3. END-USER SUPPORT</b> Establish standards and metrics for End-User Support – Training (additional staffing not included)	\$25,000
3.1 Improve Help Desk policies, procedures and operations	\$10,000
<b>4. SECURITY</b> Conduct security vulnerability assessment	\$25,000
4.1 Server hardening	\$10,000
<b>TOTAL</b>	<b>\$770,000</b>

### Strategic Opportunities

The assessment performed during this review and the self-assessment in the 2004-05 Executive Office BAP confirm that the IRM organization has a heavy workload and staff that work hard, but largely in a reactive mode. IRM lacks sufficient staff with the breadth and depth of expertise to deliver the required reliability and quality of service to promote efficient and effective use of technology within the organizations they support.

The recommendations highlighted in this report are those deemed most important in effecting a material change in the reliability and quality of services provided to the users supported by the Executive Office.

The recommendations to upgrade the server environment and have ISD assume responsibility for operating the IRM server infrastructure provides improved redundancy, reliability and management improvements by relying on an organization that specializes in the support and management of the server resources. It also provides an opportunity to establish a business continuity plan for the Board, Executive Office and other departments by leveraging the larger ISD plan that is being developed. The ISD Disaster Recovery Plan includes geographically remote recovery facilities. The recommendation to redirect the existing IRM resources to functions that provide end-user support leverages the existing staff's knowledge of Board and Executive Office operations. It also allows improved support for the infrastructure by relying on an organization that specializes in best practices to support and manage server resources. It also provides an opportunity to improve the business continuity planning by leveraging the larger ISD plan.

The Board members and their staff were left without the tools (word processing, calendaring, e-mail, internet access, etc.) that they have come to rely on in managing the County of Los Angeles. Being accessible to and responsive to their constituents is a vital component of their functions. The estimated cost of the approximately four (4) full work days is estimated at a minimum of \$300,000, and potentially greater cost when considering the intangible impact on public relations. Based on information collected during the study, we have attempted to develop recommended upgrades to the hardware and software infrastructure to improve overall reliability to a more acceptable range (99.9% or not more than nine (9) hours per year of unscheduled downtime). The current configuration, though considered high availability, is estimated to average four (4) days of downtime per year.

The consensus of the overall team is that the IRM organization has staff that works hard, but largely in a reactive mode. There are vacancies within IRM, which if filled with individuals with the appropriate expertise would improve IRM's ability to deliver the reliability, quality, and effective support required by their users. However, the assessment also identified that additional focus on effectively leveraging existing tools and improving the consistency in which policies, procedures and technical documentation are developed would significantly improve the management and support of the I/T environment(s) of the Board, the Executive Office and other departments.

The recommended organizational changes, improved documentation of policies and procedures, and increased focus on communication will make a dramatic improvement in the level of satisfaction of the users.

### **Server and Data Center Consolidation Benefits**

The recommended organizational structure will provide the opportunity for server and data center consolidations, the benefits of which are magnified as more departments participate in this model, creating a Hall of Administration or Civic Center "premise network". This strategy and architecture can subsequently be replicated at other major County facilities.

Owning and maintaining a distributed infrastructure is very expensive. Each separate data center/server room must maintain hardware, software, floor space, HVAC (heating, ventilation, and air conditioning), power, data communications, a minimum required head count, and a disaster recovery capability. Further, each data center is sized for the peak workload it encounters, which means for the most part that there is unused capacity during the non-peak times. Overall, the total consumption of resources is considerably greater than if the infrastructure was consolidated and shared.

As the number of servers and disparity of hardware/software configurations decrease through consolidation, the reduction in complexity makes change control, planning, operations, and troubleshooting much easier. Disaster recovery planning also becomes easier as the number of unique platforms and data files is reduced. A more centralized approach can also lead to more consistent backups of data. Moreover, centralized servers are easier to secure physically and logically than distributed servers. The economies of scale and simplified risk profile of a central location enable a higher level of security to be attained. Expensive security tools and support staff can be shared across a larger pool of servers; in contrast the cost of unnecessarily redundant investment in security can be prohibitive in a distributed environment.

The County is updating its strategic plan to include a strategy that recognizes data as a strategic County asset and the need to leverage its value through sharing. We strongly suggest a plan that includes sharing the data and information technology assets. Directly supportive of that strategy is examining and implementing approaches that improve the cost-effective management of information resources.

### **Acknowledgements**

Exhibit V acknowledges the individuals and organizations that invested time in participating in the development of the assessment, findings and recommendations documented in this report. On behalf of the County of Los Angeles, we extend them our sincere appreciation.

## ***Hardware Configuration Discussion***

### **1.0 IRM's Current Server Environment**

Dell | EMC CX400 Storage Array

(15) 146GB 10K FC Disks

SAN Software: Navisphere, Access Logix, PowerPath, SnapView

(2) McData Flexport FC Switches, each with 8 ports active

Dell EMC Gold Support

(6) 2650 Dell Servers, Dual 2.8Ghz, 4GB RAM, Dual 73GB SCSI Disks RAID

1, Qlogic HBA

Dell Enterprise Gold Support

Dell PowerVault 132T Tape Library – 2 SDLT Drives

Dell Enterprise Gold Support

Dell 42U Rack

(2) APC 3000 UPS'

(1) 16 Port KVM switch

Dell Gold Support provides:

- Engineer-to-Engineer Support with direct access to Dell's senior-level Gold Queue.
- Technical Account Management Team for attentive support and escalation management.
- Customer-Defined Call Priority so that you maintain control of your case.
- On-Demand Engineer Dispatch for select Severity 1 incidents to quickly receive onsite service.
- [Software Support Resolution Pack](#).
- Web-Based Remote Troubleshooting to quickly mobilize experts.
- Remote Monitoring for Dell/EMC Systems.
- 4-Hour Same Day On-Site Response Service<sup>1</sup>.

Dell Enterprise Gold Support (Servers and Tape Drives):

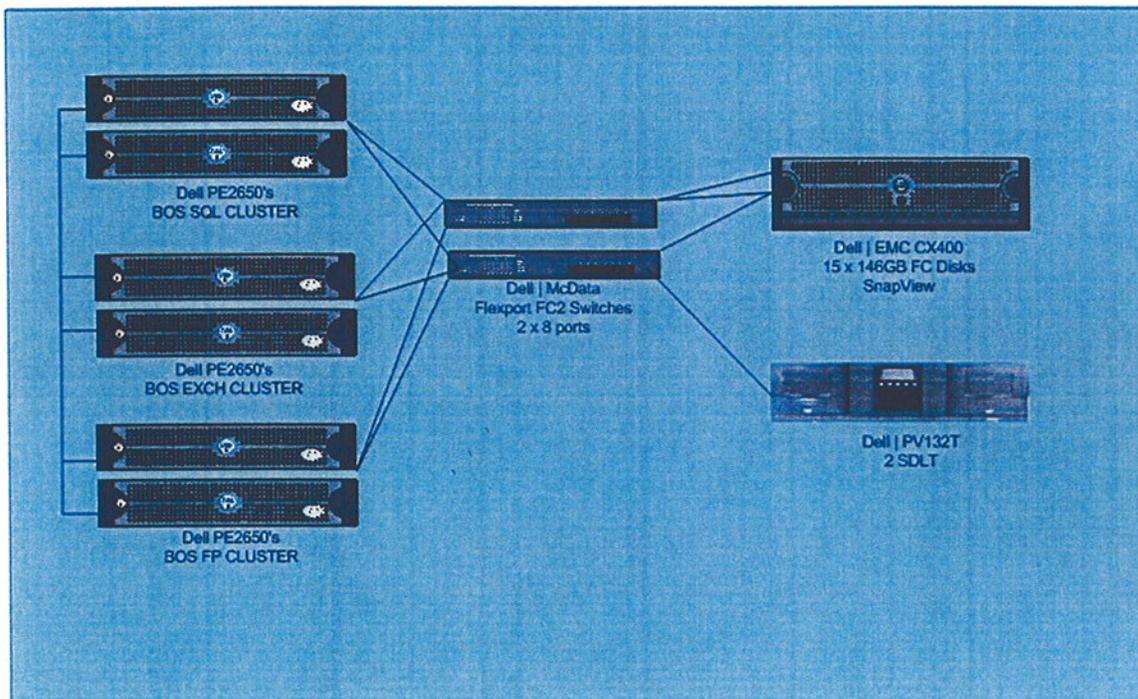
<http://www1.us.dell.com/content/topics/global.aspx/services/en/pesstiersgold?c=us&cs=RC974033&l=en&s=slq>

Dell | EMC Gold Support:

<http://www1.us.dell.com/content/topics/global.aspx/services/en/emcgoldsupport?c=us&cs=RC974033&l=en&s=slg#tn1>

## Current Environment Diagram

County of Los Angeles  
Board of Supervisors  
Existing SAN Infrastructure



## 2.0 Discussion of Options

### 2.1 Clustering (Current Environment)

As an improvement to highly internally redundant servers, clustered Exchange servers offer protection for relatively few failure scenarios such as a failure of a non-redundant component, a system board or memory. Clustered servers will fail over in the event of an operating system failure, although a single-node server will attempt to reboot from such an event.

Clustered servers offer no protection whatsoever from failures caused by corruption in Exchange databases, logs, queues or other data structures because all Exchange data is stored on disk drives that are shared by all clustered nodes.

Cluster technology adds complexity to an Exchange 2003 environment. More hardware parts are required, more complexity is included in the operating system software, and more complex application software is required. In addition, system designers and administrators must take special care to ensure that add-on products, such as virus scanners and backup software, are cluster compliant. A properly configured non-clustered Exchange 2003 Server running on high-quality, completely internally redundant hardware can operate very reliably.

Software failures may receive some limited benefit from clustered servers, such as in the case where a failed service causes the server to fail over to the working node. However, failed services can be restarted on a single-node server through the use of a server monitor. Some software failures that have their origins in disk files stored on shared volumes may cause clustered servers to fail back and forth repeatedly, which may only serve to temporarily mask the true problem without giving any added benefit to the user. Some application problems will not cause a failover at all and will require a manual failover, a scenario that is not any better than the reboot of a single-node server.

Clustered Exchange servers offer the opportunity to apply service packs, patches and hot fixes, and to install add-on software components without having to take the server down for maintenance. Maintenance is performed on the standby node, then the system is failed over and the other node is updated. Because they are scheduled events, such maintenance can be performed on single-node servers during periods of relatively low activity. If performance of maintenance is a primary driver for clustering, it places a very high cost for providing availability during off-peak hours. When service level agreements force such decisions, it may make better business sense to reevaluate the service level agreements rather than paying any cost to meet the higher level standard of performance.

Windows 2003 and Exchange 2003 clusters add substantial complexity to an Exchange environment, requiring a higher level of expertise for much of the most routine administration. The outside consultants participating in this project agree that often clusters add problems to Exchange rather than solve them because of mistakes made by inexperienced or inadequately trained administrators.

Finally, a driver to clustering can be a fear that higher management will criticize any future failure with the question, "Why didn't we cluster Exchange?" This needs to be addressed through advance communication and documentation, such as this document, and appropriate level-setting. The team must assure management that the decisions being made at this point are made in the best business interests of LA County. In summary, fear of being second-guessed by upper management should not be a primary consideration for a technology or architecture.

Clustering adds cost. For each Exchange server, one must purchase two of everything except the shared disk drives--just two additional drives per cluster are required for a mirrored pair of the quorum disk. In addition, Windows Server 2003

Enterprise is required on both nodes, where it is not necessary in a non-clustered system. Exchange 2003 Enterprise is also required for clustering.

The aforementioned arguments apply primarily to two-node clusters. Four-node clusters are available for Exchange and the value proposition is improved because the additional equipment represents only a one-third increase in cost (exclusive of disk storage), i.e., one additional node is required for three nodes, where in a two-node cluster, double the equipment is required.

It should also be noted that Exchange 2003 clusters are designed for the largest environments.

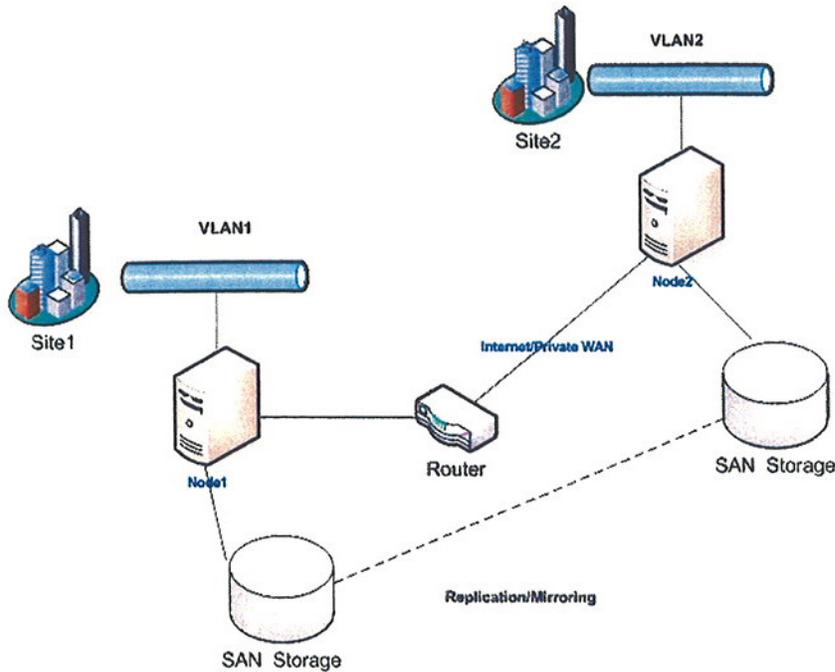
## 2.2 Geo-Clustering

A geographically dispersed cluster is a combination of hardware and software. In other words, a geographically dispersed cluster is a combination of pieces supplied by different vendors. Due to the complex nature of these configurations and the configuration restrictions that are fundamental to the Microsoft Cluster Service (MSCS) technology, geographically dispersed clusters should be deployed only in conjunction with vendors who provide qualified configurations.

A geographically dispersed cluster is an MSCS cluster that has the following attributes:

- Has multiple storage arrays, at least one deployed at each site. This ensures that in the event of failure of any one site, the other site(s) will have local copies of the data that they can use to continue to provide the services and applications.
- Nodes are connected to storage in such a way that in the event of a failure of a site or the communication links between sites, the nodes on a given site can access the storage on that site. In other words, in a two-site configuration, the nodes in site A are connected to the storage in site A directly, and the nodes in site B are connected to the storage in site B directly. The nodes in site A can continue without accessing the storage on site B and vice-versa.
- The storage fabric or host-based software provides a way to mirror or replicate data between the sites so that each site has a copy of the data. (Different levels of consistency are available, see the section depicted on the next page).

The figure below shows a simple two-site Active/Passive Geo-cluster configuration:



### 2.3 Data Replication

Data can be replicated using many different techniques at many different levels:

- Block level – Disk device level replication or mirroring. This is typically provided either by the storage controllers or by mirroring host software.
- File system level – Replication of file system changes. This is typically provided by host software.
- Application level – Application specific replication mechanisms such as SQL Server log shipping.

There are two replication methodologies typically implemented by different vendors, as follows:

- Synchronous replication means that if an application performs an operation on one node at one site, then that operation will not be completed until the change has been made on the other sites. Consider the case of synchronous, block level replication. If an application at site A writes a block of data to a disk mirrored to site B, then the input/output (I/O) operation will not be completed until the change has been made to the disk on site A and the disk on site B.

- Asynchronous replication means that if a change is made to the data on site A, that change will eventually make it to site B. Taking the same example as above, if an application at site A writes a block of data to a disk mirrored to site B, then the I/O operation will be completed as soon as the change is made to the disk at site A. The replication software will transfer the change to site B in the background and will eventually make that change to site B. Using asynchronous replication the data at site B may be out of date with respect to site A at any point in time. Different vendors implement asynchronous replication in different ways. Some preserve the order of operations, others do not. If a solution preserves ordering, then the disk at site B may be out of date, but it will always represent a state that existed at site A at some point in the past. In other words, site B is crash consistent; the data at site B represents the data at site A if site A had crashed at that point in time. If a solution does not preserve ordering, the I/Os may be applied at site B in an arbitrary order. In this case, the data set at site B may never have existed at site A. Many applications can recover from crash consistent states; very few (if any) can recover from out of order I/O sequences. In short, never use asynchronous replication unless the order is preserved. If order is not preserved, the data on site B may well appear corrupt to the application and may be totally unusable.

## 2.4 Application Failover

Applications in a multi-site cluster are typically setup to failover just like a single-site cluster. MSCS itself provides health monitoring and failure detection of the applications, the nodes and the communications links. There are, however, cases where the software cannot differentiate between different failures modes.

The MSCS architecture requires there to be a single quorum resource in the cluster that is used as the tie-breaker to avoid split-brain scenarios. A split-brain scenario happens when all of the network communication links between two or more cluster nodes fail. In these cases, the cluster may be split into two or more partitions that cannot communicate with each other. Each partition cannot communicate with the other partition(s) and cannot therefore differentiate the two cases:

- Communication between sites failed and the other site is still alive.
- The other site is dead and no longer available to run applications.

While this can certainly happen in a single-site cluster deployment, it is much more likely to happen in a multi-site configuration. The cluster service guarantees, that even in these cases, a resource is only brought online on one node (actually the guarantee is that it will never be brought online on more than one node). If the different partitions of the cluster each brought a given server function online, then it would violate the cluster guarantees and potentially cause data corruption. When the cluster is partitioned, the quorum resource is used as an arbiter; the partition that owns the quorum resource is allowed to continue, the other partitions of the

cluster are said to have lost quorum. The cluster service and any resources hosted on the nodes which were not part of the partition that has quorum are terminated.

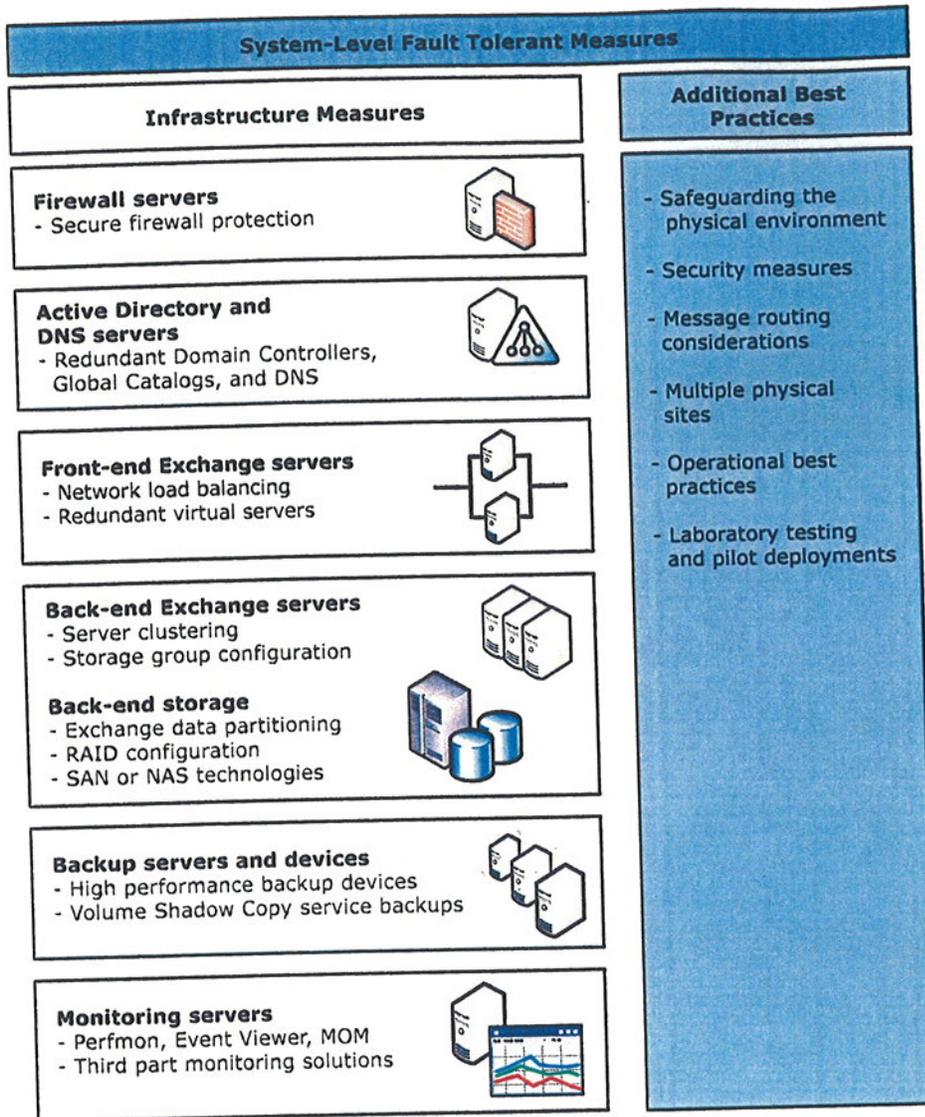
The quorum resource is a storage-class resource and, in addition to being the arbiter in a split-brain scenario, it is used to store the definitive version of the cluster configuration. To ensure that the cluster always has an up-to-date copy of the latest configuration information, the quorum resource must itself be highly available. In Windows 2000, the quorum device was typically a shared disk or physical disk resource type.

There are, however, cases where the software cannot make a decision about which site should host resources. Consider two identical sites, the same number of nodes and the same software installed. If there is a complete failure of all communication (both network and storage fabric) between the sites, neither site can decide to continue without manual intervention since neither has enough information to know whether the other site will continue or not. Different vendors solve this problem in different ways; however, they all require some form of administrator intervention to select which site should continue. The goal of any geographically dispersed configuration is to reduce the number of scenarios where manual intervention is required.

Some operational procedures require that manual intervention is always required in the event of a site loss. Typically, losing a site can mean that other procedures have to be initiated such as redirecting phones, moving personnel, etc. Getting the applications up and running is a piece of a more complex puzzle that needs to be orchestrated within the business procedures.

## 2.5 High Availability for Exchange Servers

As described above, there are many components to building a highly available messaging infrastructure. The following figure summarizes these pieces:



The following describes five Exchange 2003 topologies, including estimated availability percentages. However, actual availability levels will vary, depending on many variables.

**Tier description**

**Estimated availability level**

**First-tier messaging system.** The figure below shows a first-tier messaging system, upon which all the higher tiers are built.

99% (87.6 hours = 3.65 days downtime per year) or higher

**Second-tier messaging system.** A second-tier system meets the requirements of a first-tier system, but also includes multiple domain controllers, multiple DNS servers, a separate monitoring server, and an entry-level redundant array of independent disks (RAID) storage solution that is not on a SAN.

99.5% or higher

**Third-tier messaging system.** A third-tier messaging system meets the requirements of the second-tier system, but also includes a mid-range RAID storage solution using a SAN, and Network Load Balancing (NLB) implemented on Exchange front-end servers.

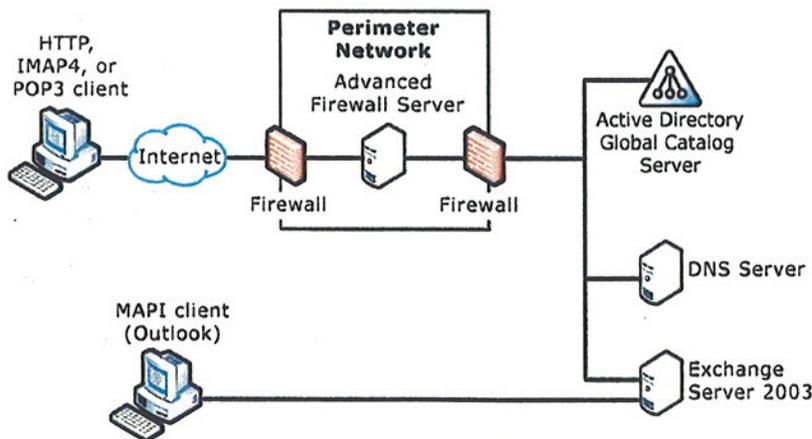
99.9% (8.76 hours downtime per year) or higher

**Fourth-tier messaging system.** A fourth-tier message system meets the requirements of the third-tier system, but also includes a high-range RAID storage solution, a high-range SAN solution, back up and restore using Volume Shadow Copy service, and active/passive Microsoft Windows® Clustering (with multiple passive nodes), for all back-end Exchange servers.

99.99% (52.56 minutes downtime per year) or higher

**Fifth-tier messaging system.** A fifth-tier messaging system meets the requirements of the fourth-tier system, but also includes complete site failover (in the event of a site failure) through the use of a multi-site design that includes a geographically dispersed clustering solution.

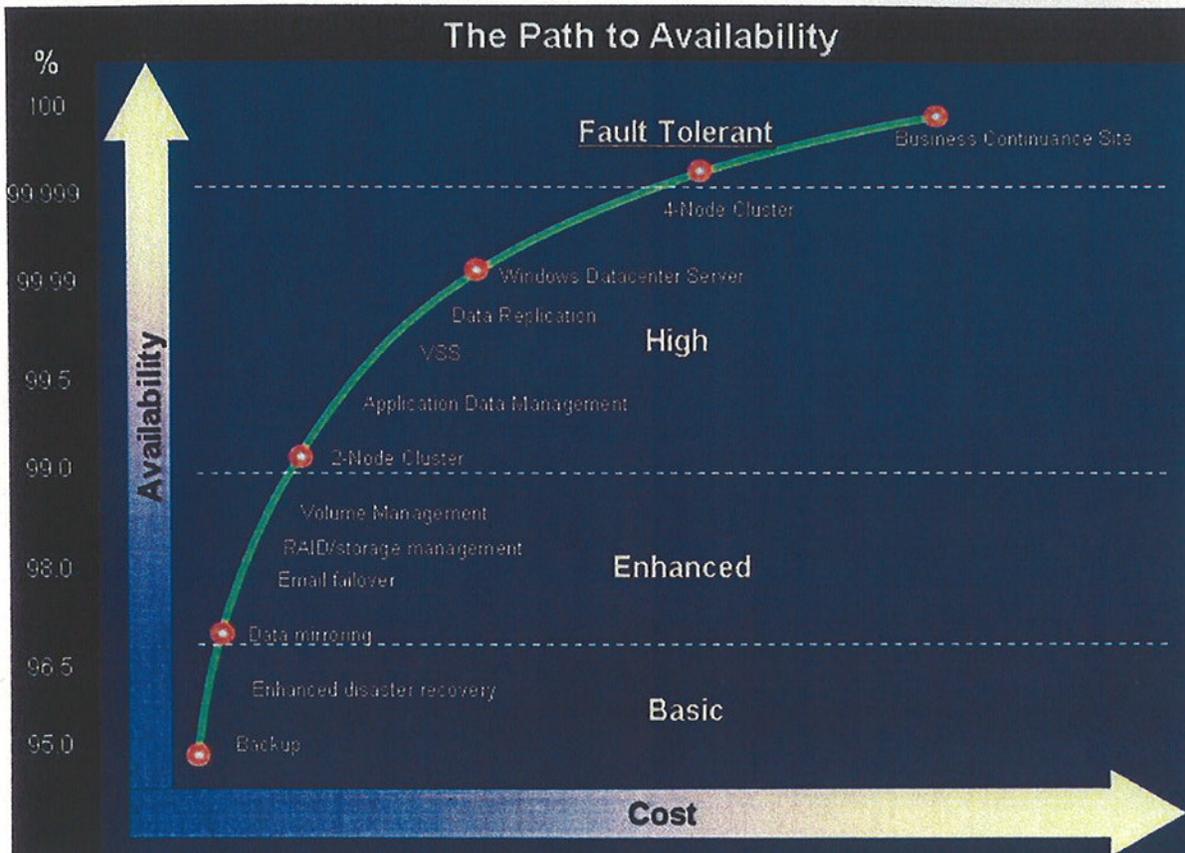
99.999% ("five nines" = 5.256 minutes downtime per year) or higher



**First-Tier Messaging System**

- Mid-level server-class hardware in all servers.
- Single-server advanced firewall solution.
- Single domain controller that is also configured as a global catalog server.
- Single server that is running Domain Name System (DNS).
- Exchange 2003 and Windows Server 2003 correctly configured.

The quest for greater availability must contend with many barriers. For example, an organization must have highly trained and skilled support staff that understand MSCS, Windows Server 2003, Exchange 2003, Server and SAN hardware architecture. Another is cost. The following figure depicts the exponential increase in cost as higher levels of availability are engineered:



#### Climbing the Availability Curve

- RAID/disk/volume management
- Clustering
- Storage technologies (e.g., fibre channel storage area networks)
- Point-in-time copies/VSS
- Geo-clustering

Clustering, however, is not adequate to protect against a site/data center failure due to natural disasters or premise failures (loss of power, air conditioning, network, etc.). This may be of particular concern if the area housing the servers is not a true data center, with the typical infrastructure redundancy. Multi-site clustering, also

known as geographically dispersed clustering, can provide business continuity during a site failure.

Engineering for high availability does not negate the need for disaster recovery and business continuity planning. Although disaster recovery encompasses issues including power, systems, geographic location, application, etc., the most important issue is data backup/restore. Without a well-defined and thoroughly tested backup/restore plan, access to data can be at risk. There are many business continuity and disaster recovery solutions for Exchange servers from Dell, EMC, HP, Hitachi, IBM, Veritas and from many other vendors. These solutions can be broadly classified into the following:

- Geographically clustering solution (Geo-Clustering hardware based).
- Multi-Site cluster.
- Majority node set clusters (Windows 2003).
- Disaster Recovery using replication/mirroring software.

#### Highly Available Directory Infrastructures

If Active Directory information becomes corrupt, users might not be able to log in and access network resources. As a best practice, deploy Active Directory servers on three volumes: the operating system volume, the Active Directory database information volume, and the Active Directory log files volume. Active Directory is backed up as part of System State, which includes the database, log files, registry, system boot files, COM+ registration database, and Sysvol. Therefore, it is critical that these volumes be backed up and restored as a set.

Active Directory information must be protected against a number of potential problems:

- **Hardware Failure** – To protect against problems that result in disk or other hardware failure, it is recommended that an organization use a combination of fault tolerant protected volumes (using either mirroring or RAID-5), and at least two domain controllers in each Active Directory domain. These domain controllers act as peers sharing the Active Directory workload; however, if the hardware fails in one server, the second server, with its replicated copy of the data, continues to provide necessary services. Note that, when there is an outage of one server in a configuration that has only two Active Directory servers, the remaining server is a single point of failure for the duration of the outage.
- **Data Corruption** – While mirroring and RAID-5 configurations provide fault tolerance for potential hardware failures, these solutions do not protect against data corruption, because the mirrored copy of data is damaged along with the original copy. Potential data loss or corruption issues traditionally require a single point-in-time backup copy of all volumes, and it is necessary

to keep this backup physically separate from the original. Using a tape archive backup solution has been the preferred method for implementing recovery procedures for these kinds of failures.

Tape backups are time intensive and impact server performance, and therefore tend to be done relatively infrequently (full backups are usually done only once a week). In addition to this drawback, there are a number of other limitations, including:

- A time intensive tape restore process.
- A time intensive resynchronization process. The longer the tape restore process, the greater the divergence between the shadow copies and the online Active Directory server(s) that continue to write transactions to disk.
- Decreased performance of the remaining Active Directory server(s) because it now carries an increased workload.

A highly effective alternative to traditional tape-based protection is to make point-in-time shadow copies. Use of point-in-time shadow copies with Active Directory configurations allows rapid recovery from a number of specific system problems, including:

- Bad service pack installation.
- A third-party component, such as an application agent, filter driver, or device driver that has rendered the system unusable or unstable.
- Corruption of the system registry.
- A virus that has affected a system component.

Because this mirroring (or "cloning") process is fast and non-disruptive to system performance, shadow copies can be made more frequently than tape backups. Shadow copies kept locally on a storage area network can be quickly accessed; with the appropriate hardware provider, they can be transported to a backup server, backed up to tape, and sent to offsite storage for archiving.

With the Volume Shadow Copy Service (VSS) and the Virtual Disk Service (VDS), Windows Server 2003 contains new functionality to enable fast data restores, cutting restore time from the hours it can take with tape backups to just minutes. Since the restore time is so much faster, correspondingly fewer Active Directory changes can occur. This shortens resynchronization times considerably, enabling the machine to return to production significantly faster.

The figure below compares recovery times for Active Directory with Windows Server 2000 and with the new VSS and VDS features of Windows Server 2003:

• Steps to Active Directory recovery with and without the new capabilities of Windows Server 2003			
• Server 2000	• Time	• Server 2003	• Time
1) Analyze failure to determine if server can be recovered.	30-90 minutes	N/A	N/A
2) If unable to recover server, save corrupted data using xcopy or robocopy.	Minutes to hours, depending on amount of data	1) Use LUN masking to hide corrupted data (T <sub>2</sub> ); save for later analysis.	seconds
3) Retrieve tapes from offsite vault	Minutes to hours	N/A	N/A
4) Restore volumes from backup tape.	Minutes to hours	2) Using LUN unmasking, recover shadow copy volumes backed up at T <sub>1</sub> .	seconds
5) Reboot Active Directory Server	2 minutes	3) Reboot Active Directory Server (change HBA boot LUN).	2 minutes
6) Resynchronize with redundant machine.	Time between failure and restore long; can be significant data divergence	4) Resynchronize	Time between failure and restore minimal; limited data divergence
7) Resume production.	<b>May be hours before production is resumed</b>	5) Resume production	<b>Can return to full operations within 5 minutes of failure</b>
8) No preventative action possible if corrupted data overwritten in step 3.		6) Analyze cause of failure; take preventative action	

Using Windows Server 2003 with VSS and VDS can significantly reduce the recovery time of a failed Active Directory server on a storage area network, as well as allow the system administrator to analyze root causes of failure without impacting the production environment. An organization's hardware vendor should be consulted for support of these new components.

### 3. Discussion of Recommendations

#### 3.1 Training

Although training was delivered to the original IRM staff during the installation process, additional training is recommended for any new staff involved in operations. Training on SAN and server technology and management is offered. For advanced students, Dell Certification testing is available for server and storage expertise. Dell Training & Certification offers programs which can help make more efficient use of I/T resources by maximizing their capabilities and increasing their productivity. Training classes are offered either onsite, at a regional training center, or at the Dell training center in Austin, TX.

*Estimated Training Cost: \$6,000 per student plus travel expenses.*

In addition, Dell publishes a quarterly technical journal called PowerConnect that may be helpful for IRM staff to keep up to date on enterprise technology solutions. Free subscriptions are available at:

<http://www1.us.dell.com/content/topics/global.aspx/power/en/power?c=us&cs=555&l=en&s=biz>

#### 3.2 Server and Storage Certifications

▶ Dell Certified Server Professional (DCSP)

Guarantees the knowledge and skills required to implement Dell servers into an existing I/T infrastructure. Covers Dell PowerEdge hardware, firmware, OS installation, configuration, local and remote management, and troubleshooting. I/T professionals are required to pass an exam in order to become certified.

▶ Dell Certified Storage Networking Professional (DCSNP)

Guarantees the knowledge and skills required to implement Dell storage into an existing I/T infrastructure. Includes storage fundamentals and initial setup, configuration, and management of Dell/EMC storage arrays, the advanced features of Dell/EMC SAN solutions such as SnapView and MirrorView, clustering, and performance management. I/T professionals are required to pass an exam in order to become certified.

#### 3.3 EMC | SAN Training

**UNDERSTANDING DELL STORAGE NETWORKING TECHNOLOGIES**

**Overview:** Online course designed to provide entry-level I/T professionals with the basic information required for further study of Dell Storage Networking technologies including DAS, NAS, and SAN.

### **IMPLEMENTING DELL ENTERPRISE STORAGE SOLUTIONS**

**Overview:** Two-day instructor-led, hands-on course focusing on the Dell/EMC CX series and covering SAN fundamentals, initial setup, configuration, and management of Dell storage arrays. This course prepares the administrator for the Dell Certified Storage Networking Professional exam.

### **IMPLEMENTING DATA PROTECTION ON DELL STORAGE**

**Overview:** Three-day instructor-led, hands-on course focusing on the Dell/EMC series and covering SAN features like SnapView and MirrorView, Clustering, and performance management of SAN solutions. This course is a follow-up to Implementing Dell Enterprise Storage Solutions and prepares the administrator for the Dell Certified Storage Networking Professional exam.

## **3.4 Server Training**

### **UNDERSTANDING DELL SERVERS AND SYSTEMS MANAGEMENT**

**Overview:** Online course designed to provide entry-level I/T professionals with the basic information required for further study of Dell servers and systems management tools. Assessment included.

### **DELL SERVER CONFIGURATION AND MANAGEMENT**

**Overview:** Three-day hands on course managing and configuring Dell Server technologies using Dell OpenManage tools.

### **POWEREDGE 2650 ONLINE TRAINING**

**Overview:** Four-hour on-line course covering hardware, software and firmware fundamentals.

## **3.5 OpenManage**

Dell OpenManage is a comprehensive set of tools that allow for efficient systems management across Dell systems. Integration with Microsoft MOM (Microsoft Operations Manager) is also available from Dell. Some OpenManage features have already been implemented in the current Executive Office environment, but a review of the implementation for completeness and training of the staff on its use should be considered. Most OpenManage tools are available at no charge. Dell is able to offer consulting services to provide OpenManage implementation assistance and knowledge transfer as needed.

*Estimated OpenManage Consulting Cost: \$8,000 for 3-4 days.*

## **3.6 Expand FC Switch Capacity**

The existing McData Flexport switch environment could be expanded to offer additional redundancy and performance by enabling eight (8) additional ports. This would allow the CX400 to have one (1) additional connection for added redundancy and throughput (noted as red line on the current environment diagram). The current implementation is using all 16 available ports. The cost to enable a block of eight (8) additional ports is approximately \$6,000.

*Estimated Upgrade Cost: \$6,000 for eight (8) additional ports, \$12,000 for 12 additional ports.*

### 3.7 Onsite Spares

Although the SAN already has one hot spare disk drive to support the (14) 146GB disks, an additional onsite spare drive may also want to be considered for added redundancy.

*Estimated Disk Cost: \$2,500 per 146GB FC disk.*

### 3.8 SAN Health Check Service

SAN Health Check provides periodic testing, analysis, and reporting of the health of the SAN. Results also include recommendations about capacity, bandwidth, and upgrade recommendations. At the time of a Health Check, Dell can apply the latest software updates and revisions available from EMC Powerlink. This service can be scheduled yearly or twice a year if needed.

[http://www.dell.com/downloads/global/services/ds\\_emc-maint.pdf](http://www.dell.com/downloads/global/services/ds_emc-maint.pdf)

*Estimated SAN Health Check for yearly service. Cost: \$2,500 per visit.*

### 3.9 VisualSAN Software

VisualSAN software should be considered to help simplify SAN configuration and improve management capabilities. All three (3) modules described below would be valuable to optimize the management of the SAN.

VisualSAN Network Manager (NM) provides service-level and centralized management of storage area networks (SANs). It monitors events, distinguishes urgent SAN events, and generates alerts, enabling rapid troubleshooting from a centralized web-enabled console.

VisualSAN Configuration Manager (CM) creates point-in-time comparisons for problem isolation, historic reference, change management, asset management, and replication. Activate VisualSAN CM's automated capture capability to detect unauthorized SAN changes.

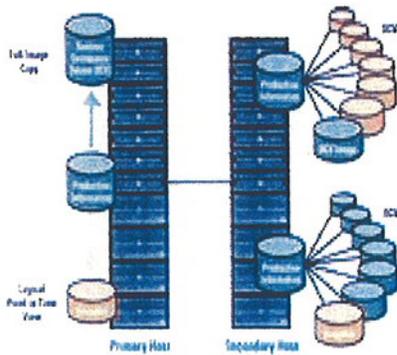
VisualSAN Performance Manager (PM) provides historical and real-time SAN performance monitoring for throughput optimization. With VisualSAN PM, downtime can be reduced by quickly discovering high-traffic areas and further decrease the need for hands-on SAN management.

<http://www.dell.com/downloads/global/products/pvaul/en/visualsannetworkmanagementsuite.pdf>

*Estimated Cost: \$6,000 - \$25,000 depending on functionality and level of implementation assistance needed.*

### 3.10 Review Backup and Recovery Design

Several options are available for implementing a robust backup and recovery solution. EMC SnapView software was included in the original SAN purchase. SnapView software cost-effectively accelerates backup and recovery through economical, disk-based "instant restore" of production data. SnapView creates point-in-time snapshots and full-copy business continuance volumes (clones) of production data for non-disruptive backup, and enables applications and data restores in seconds versus the hours often required for traditional tape-based methods. Consideration should be given to integrating SnapView into the overall backup and recovery plan. EMC also offers Exchange Replication Manager for a disk-based backup strategy to reduce the need for recovery from tape in the event of a data loss or corruption. To fully utilize these tools, additional storage and server(s) may be needed.



**EMC SnapView captures snapshots or makes clones of production data.**

*Estimated Backup and Recovery Design Consulting Cost: \$10,000 - \$50,000 depending on scope.*

### 3.11 Onsite Mirrored Data

Leveraging SnapView, Exchange Rapid Recovery Solution allows users to create hot splits of Exchange databases. A hot split is essentially a point-in-time copy of an Exchange database that allows users to recover within minutes when corruption is discovered, avoiding the need to revert back to tape copies. The Exchange Rapid Recovery Solution uses a combination of SnapView business continuance volumes (BCVs), as well as SnapView snapshots, to produce the hot splits that can be used to quickly recover Exchange databases. The Exchange Rapid Recovery Solution automates several steps needed to create a clean hot split.

## The Exchange Rapid Recovery Solution:

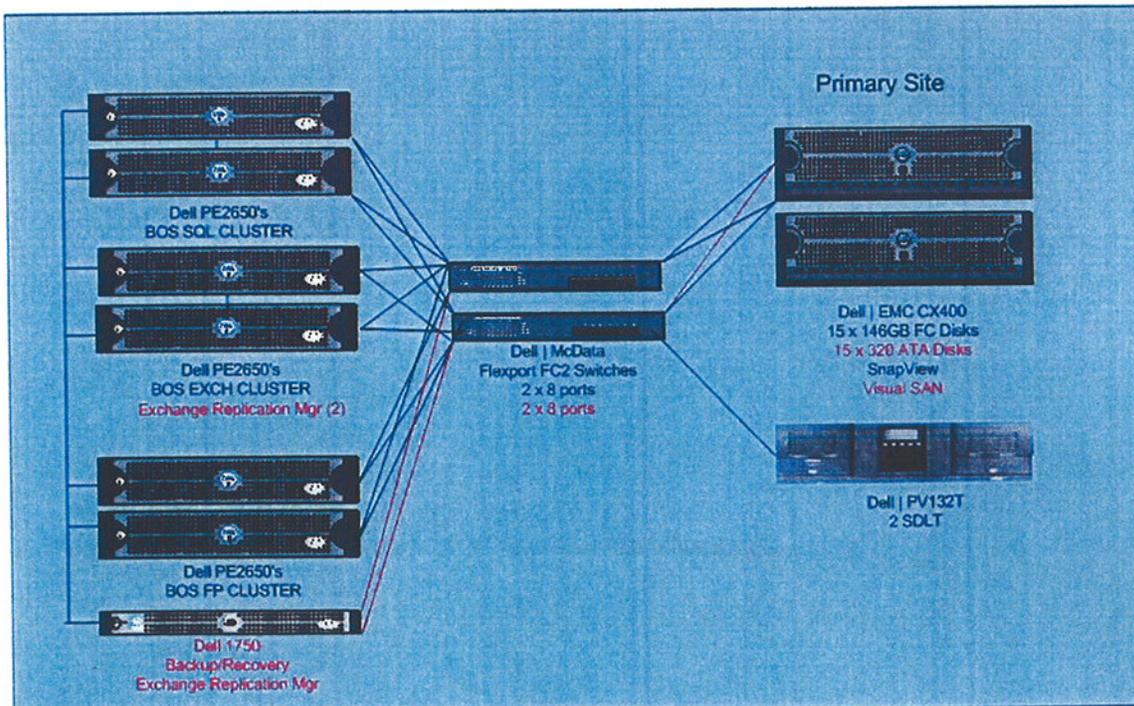
- Checks the database for preexisting corruption.
- Synchronizes the database and log file BCVs.
- Fractures the BCVs from their source logical units (LUNs).
- Mounts a Snapshot of each BCV to the recovery host.
- Checks split for data integrity using ESEutil.

The hot split gives users a point-in-time copy of the database that can be used for recovery. Typically, users would need to restore their production data from tape, which would require several hours, but with the Exchange Rapid Recovery Solution and SnapView, it is instant. Users can instantly restore their production data to a known good point in time, and then roll their production log files into the instantly restored copy, thereby allowing the database to be updated up to the last logged entry.

Finally, part of the review of the backup and recovery design should include consideration to add additional lower cost ATA disk drives to the existing SAN to allow for backup solutions that include a backup-to-disk and recover-from-disk component.

[http://www.dell.com/downloads/global/products/pvaul/en/ata\\_dae2\\_infobrief.doc](http://www.dell.com/downloads/global/products/pvaul/en/ata_dae2_infobrief.doc)

### County of Los Angeles Board of Supervisors Enhanced Single Site



*Estimated Costs:*

- *Estimated ATA Disk Enclosure with 4+TB Storage, Licensing & Installation Cost: \$40,000.*
- *Estimated Exchange Rapid Recovery (ERM) Software Cost: \$5,000 per server (2).*
- *Estimated Exchange Rapid Recovery Consulting Cost: \$10,000 – \$30,000 depending on scope.*
- *Estimated Cost of Backup and Recovery Server Hardware (SAN Connected): \$12,000.*
- *Estimated Cost of VisualSAN: \$6,000 - \$25,000 depending on functionality and level of implementation assistance needed.*

**3.12 Recommended Strategy - Remote Failover Solution with Asynchronous Mirror**

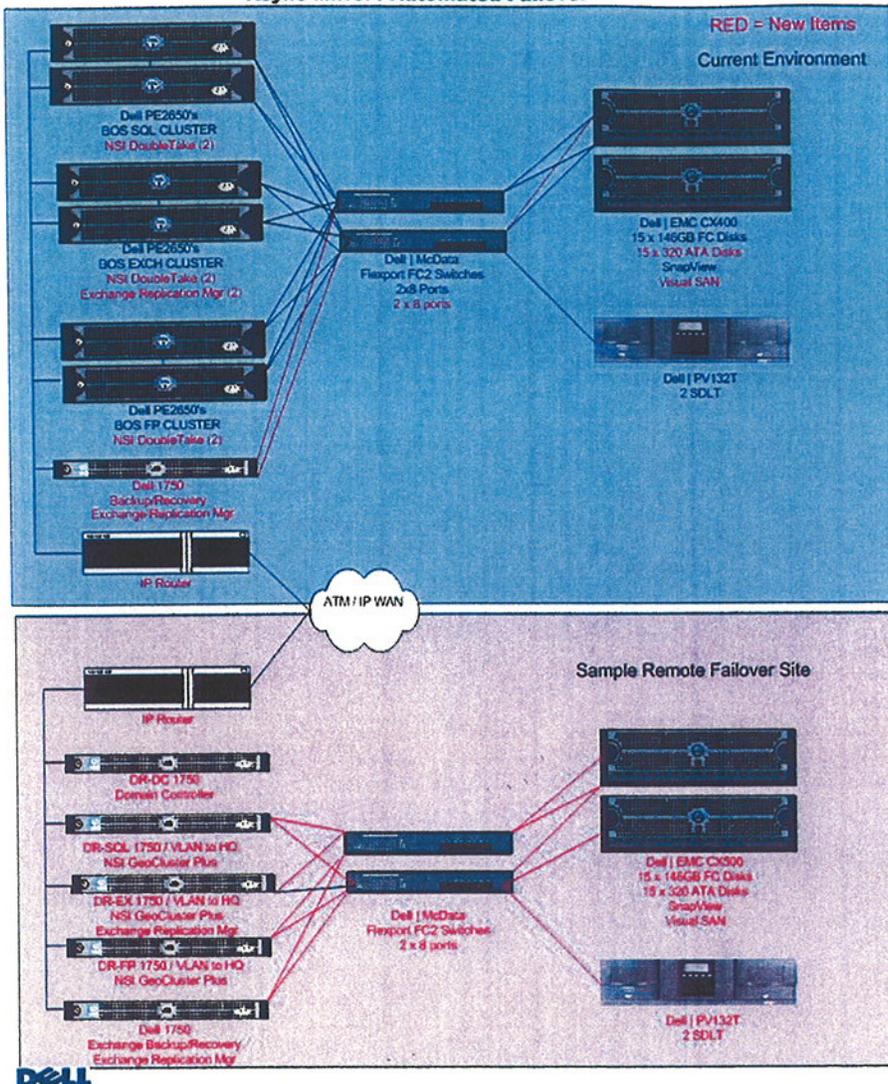
For high availability requirements, a remote site failover solution can be added to the existing server and storage environment. Tools such as NSI DoubleTake and NSI GeoCluster provide an asynchronous mirror of the data and allow for automated application failover between sites. In this case, the following would need to be added:

- NSI DoubleTake Advanced Server to each server at headquarters to be mirrored.
- At least one server with adequate storage for mirroring of data at the remote site.
- NSI GeoCluster to the remote server(s) to enable application failover.
- Connection via IP network.
- Implementation assistance and training on NSI DoubleTake and GeoCluster for staff.

This remote failover site can be scaled to mirror a large number of business critical servers and applications by adding additional servers, storage, and network bandwidth. In the diagram that follows, a suggested set of hardware and software is shown. Depending on the actual number of servers and amount of storage being mirrored, this solution can be scaled up or down in the areas of server quantity and power, storage size and functionality, and backup library size and speed. NSI Support Services would be needed to provide the software and implementation support for this solution.

<http://www.nsisoftware.com/pdf/ExchangeWhitepaper.pdf>

County of Los Angeles  
Board of Supervisors  
Async Mirror / Automated Failover



**Estimated Costs:**

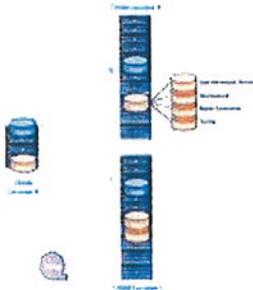
- **Server (price per server):** \$7,000 to \$40,000 depending on power and support requirements.
- **Storage (2TB):** \$20,000 to \$150,000 depending on functionality requirements (SCSI vs SAN).
- **Tape Library (2 SDLT Drives):** \$20,000.
- **NSI DoubleTake Software License and Support (per existing server):** \$6,000.
- **NSI GeoCluster Plus License and Support (per failover server):** \$9,000.
- **NSI Implementation Assistance and Knowledge Transfer:** \$6,000 - 8,000 per failover set.
- **Domain Controller Server(1):** \$5,000.
- **Estimated ATA Disk Enclosure with 4+TB Storage, Licensing & Installation Cost:** \$40,000.

- *Estimated Exchange Rapid Recovery (ERM) Software Cost: \$5,000 per server (2).*
- *Estimated Exchange Rapid Recovery Consulting Cost: \$10,000 – \$30,000 depending on scope.*
- *Estimated Cost of Backup and Recovery Server Hardware (SAN Connected): \$12,000.*
- *Estimated Cost of VisualSAN: \$6,000 - \$25,000 depending on functionality and level of implementation assistance needed.*

*Note: Additional Server Software Licensing has NOT been included other than the items above.*

### 3.13 Remote Failover Solution with Synchronous Mirror

An alternative solution for high availability, EMC MirrorView can be used to provide synchronous mirroring of SAN-based data between sites if adequate network bandwidth is available. MirrorView provides highly available data storage across a campus environment by maintaining synchronous data mirroring uni-directionally or bi-directionally between Dell/EMC arrays. Note that when using MirrorView, attention must also be paid to the server failover and DNS network redirection which is not automatic in the MirrorView solution. Typically a manual process is needed to assign replacement servers to the mirrored data and to setup the proper network redirection for users to access the servers. For these reasons, the failover process would typically be slightly slower than the automated process from NSI as described in section 7.2.9 above.

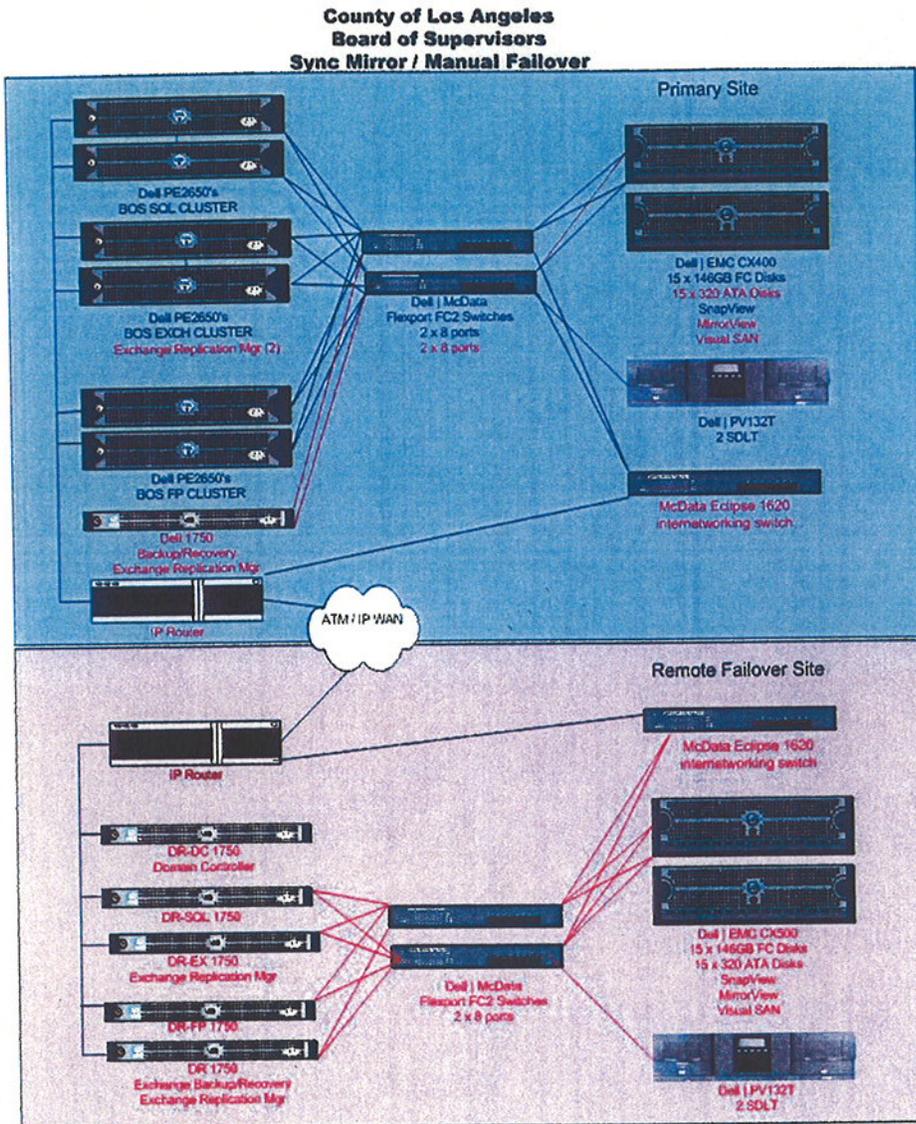


**EMC MirrorView mirrors data locally and over distance.**

This solution places a premium on up-to-date data availability and business continuity:

- Synchronous mirroring of information between Dell/EMC arrays.
- Failover to secondary sites for rapid disaster recovery.
- Maintain an exact byte-for-byte copy of your production data in a secure, remote location.
- Deploy remote mirroring solutions over dark fiber and/or IP communication links.

- Perform concurrent mirroring from one source logical unit to two different target systems.
- Deploy multiple source Dell/EMC arrays mirroring to one business continuity target system.



**Estimated Costs:**

- Servers (price per server): \$7,000 to \$40,000 depending on power and support requirements.
- Storage (2TB): \$100,000 to \$150,000 depending on functionality requirements (SAN).
- Tape Library (2 SDLT Drives): \$20,000.
- MirrorView Software (for 2 copies): \$40,000.
- MirrorView Implementation Assistance and Knowledge Transfer: \$12,000.

- *McData Eclipse 1620 Switch (for 2 switches): \$50,000.*
- *Domain Controller Server(1): \$5,000.*
- *Estimated ATA Disk Enclosure with 4+TB Storage, Licensing & Installation Cost: \$40,000.*
- *Estimated Exchange Rapid Recovery (ERM) Software Cost: \$5,000 per server (2).*
- *Estimated Exchange Rapid Recovery Consulting Cost: \$10,000 – \$30,000 depending on scope.*
- *Estimated Cost of Backup and Recovery Server Hardware (SAN Connected): \$12,000.*
- *Estimated Cost of VisualSAN: \$6,000 - \$25,000 depending on functionality and level of implementation assistance needed.*

*Note: Additional Server Software Licensing has NOT been included other than the items above.*

### 3.14 Summary of Dell Server Environment Recommendations

- Update training for operations staff on SAN and server operations and management. Consider Dell Certification programs and Dell PowerConnect Technical journal subscription (free) for staff.
- Review Dell OpenManage implementation to assure servers and storage are being monitored and are enabled for alert notification.
- Add additional redundancy and performance to the SAN environment by activating another set of eight (8) additional FC switch ports.
- Additional onsite spare components may be considered for added redundancy.
- Schedule periodic SAN Health Check onsite service to assist with periodic software upgrades and performance measurement.
- Add Dell VisualSAN management software for additional ease of configuration and performance management.
- Review backup and recovery design, consider adding S-ATA disk drives for backup-to-disk solution, and review SnapView software capabilities for possible use in backup design. Consider Exchange Rapid Restore Solution using Exchange Replication Manager and SnapView software.
- Consider adding mirrored data and failover services at a second location. Possible technologies include synchronous mirroring with manual failover, and asynchronous mirroring with automated failover.

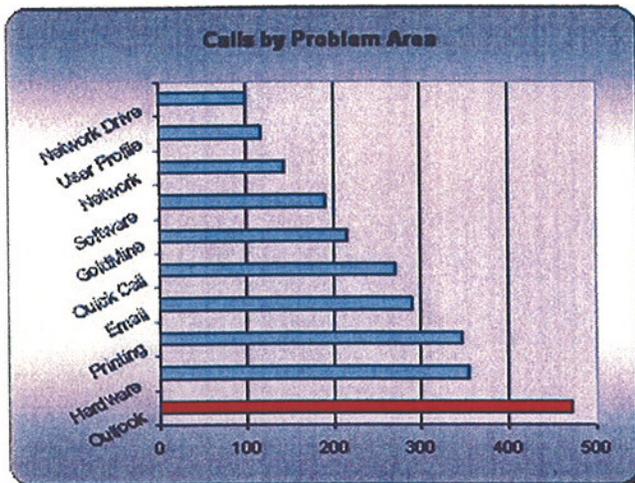
**BENEFIT/RISK SUMMARY OF HARDWARE CONFIGURATION OPTIONS:**

Configuration	Benefits	Risks	Cost Increase
<p><b><u>Current Environment</u></b></p> <p><b>Local Cluster</b></p> <p>Redundant hardware and software components</p>	<ul style="list-style-type: none"> <li>- 4 day average downtime/year</li> <li>- minimal impact on users when applying patches, etc.</li> </ul>	<ul style="list-style-type: none"> <li>- no protection from failures caused by corrupted Exchange data structures</li> <li>- limited protection from software failures</li> <li>- no protection from premise problems</li> <li>- no protection from internal network failures</li> <li>- no protection from external network problems</li> </ul>	<p><b>\$ 0</b></p>
<p><b><u>Option #1</u></b></p> <p><b>Mirrored Cluster/Remote Data Replication</b></p> <p>Fully redundant systems with synchronized remote data back-up</p>	<ul style="list-style-type: none"> <li>- 9 hours average downtime/year</li> <li>- protection from failures caused by corrupted Exchange data structures</li> <li>- protection from software problems</li> </ul>	<ul style="list-style-type: none"> <li>- moderate cost</li> <li>- no protection from internal premise problems</li> <li>- no protection from internal network problems</li> <li>- no protection of external network problems</li> </ul>	<p><b>~ \$ 300K</b></p>
<p><b><u>Option #2</u></b></p> <p><b>Geo-Cluster</b></p> <p>Two identical and synchronized systems residing in different geographic areas</p>	<ul style="list-style-type: none"> <li>- 1 hour average downtime/year</li> <li>- protection from failures caused by corrupted exchange data structures</li> <li>- protection from software problems</li> <li>- limited protection from premise problems</li> <li>- limited protection from internal network problems</li> <li>- limited protection from external problems</li> </ul>	<ul style="list-style-type: none"> <li>- high cost</li> <li>- complexity</li> </ul>	<p><b>~ \$600K</b></p>

## **IRM Help Desk Analysis**

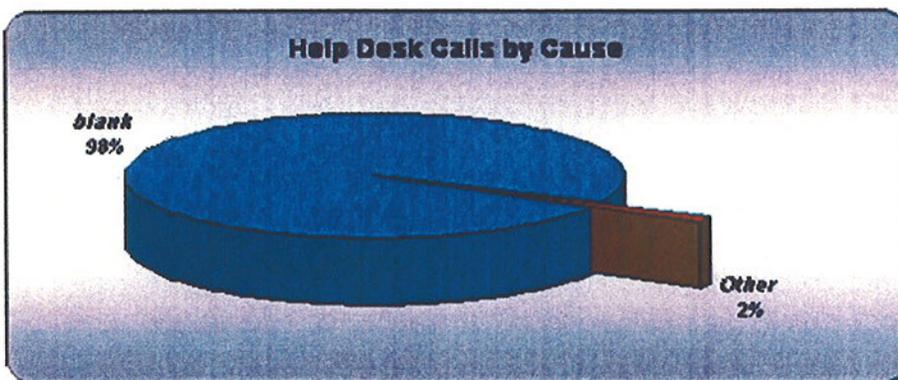
After analyzing the data from May 2003 through April 2004 within IRM's HEAT Help Desk system, the following observations and conclusions were drawn:

### Types of Helpcalls



The top three (3) problem calls were related to Outlook, general hardware problems and printing problems represent 45% of all calls for service. A proactive-focused training program or self-help capability could effectively eliminate a large number of calls to the Help Desk.

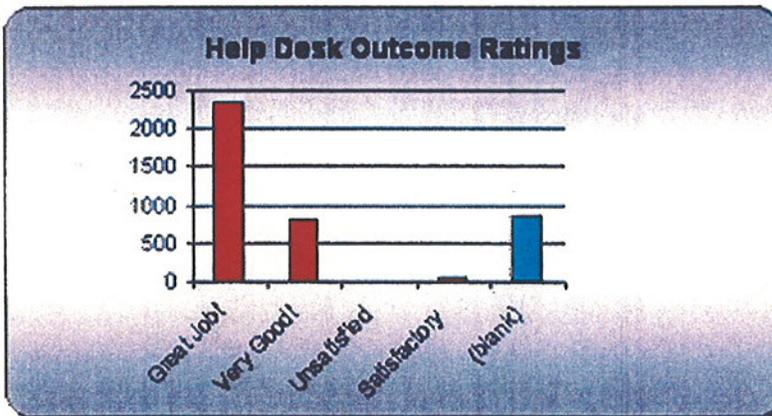
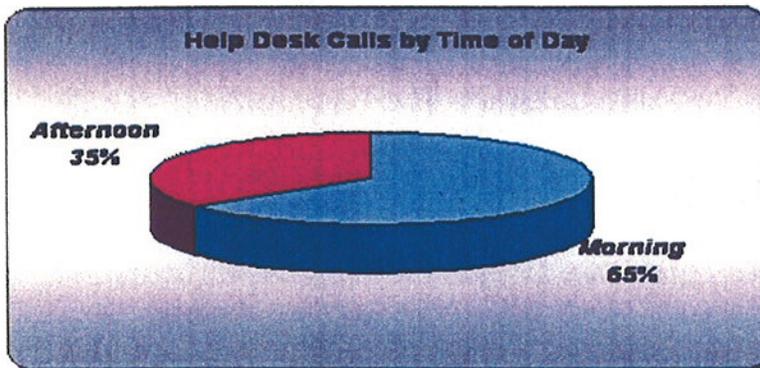
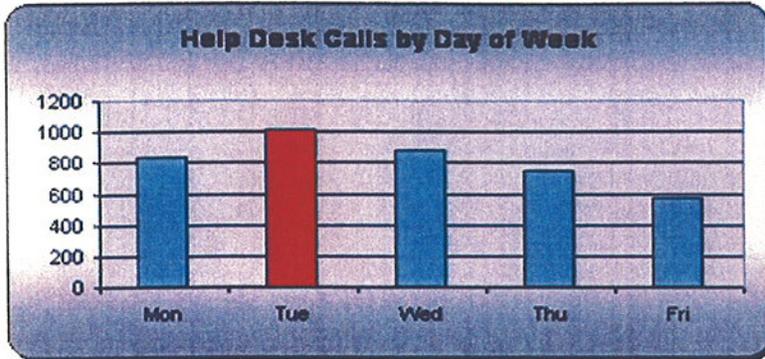
### Cause of Helpcalls



Only 2% of the calls have a "cause" identified. This information is easy to collect and record and would provide valuable information for developing proactive strategies to reduce problems and improve user support.

## Breakdown of Helpcalls

CallType	Cause	#	%	Duration (hours)
Outlook	(blank)	471	18.8%	3:57
Outlook Total		471	18.8%	
Hardware	(blank)	323	12.9%	5:26
	Accident	14	0.6%	5:01
	Defective	5	0.2%	3:11
	Incompatible	5	0.2%	1:01
	Equip Failure	4	0.2%	1:26
	Defective	2	0.1%	0:36
	Mouse	1	0.0%	3:46
Hardware Total		354	14.1%	
Printing	(blank)	326	13.0%	6:34
	Printer Error	5	0.2%	2:09
	Paper Jam	4	0.2%	3:14
	Low Toner	3	0.1%	1:18
	Driver	2	0.1%	12:02
	Not Printing	2	0.1%	1:50
	Software	2	0.1%	1:49
	Servicing	1	0.0%	1:05
	Wrong Printer	1	0.0%	1:20
	Wrong Settings	1	0.0%	2:31
	Printing Total		347	13.9%
E-mail	(blank)	283	11.3%	4:17
	Hard Drive Full	7	0.3%	4:27
E-mail Total		290	11.6%	
Quick Call	(blank)	260	10.4%	8:03
	Duplicate Call	11	0.4%	2:41
Quick Call Total		271	10.8%	
GoldMine	(blank)	216	8.6%	3:02
GoldMine Total		216	8.6%	
Software	(blank)	190	7.6%	3:06
	Installation	1	0.0%	8:03
	Untrained	1	0.0%	1:54
Software Total		192	7.7%	
Network	(blank)	141	5.6%	2:56
	Network Down	1	0.0%	4:36
	Security	1	0.0%	0:33
Network Total		143	5.7%	
User Profile	(blank)	117	4.7%	3:31
User Profile Total		117	4.7%	
Network Drive	(blank)	101	4.0%	3:29
Network Drive Total		101	4.0%	
Grand Total		2502	100.0%	



## **Conclusions from Help Desk Analysis**

On the average, the Help Desk receives 15 calls per day. The average call resolution time, as recorded in the system, is an unacceptable five hours twenty-seven minutes. This may be due to the resolution time not being entered as a priority into the system. Without accurate call resolution times being collected, it is problematic in determining, staffing, proactive strategies and accountability.

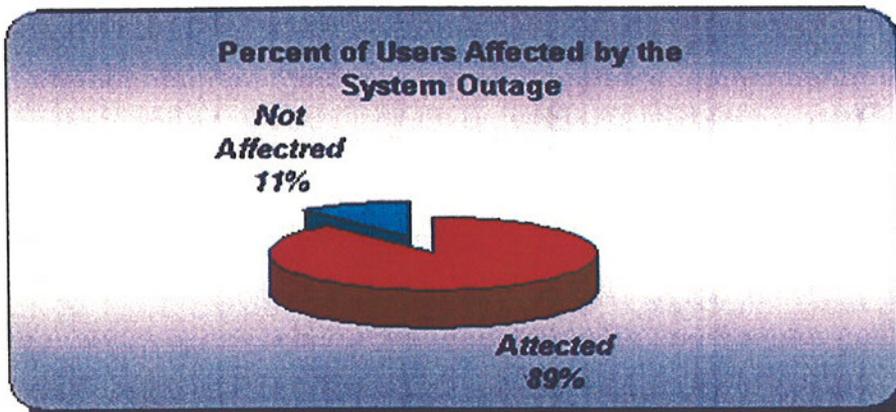
The most calls were received on Tuesdays, consistent with the business patterns of the Board. Two-thirds of the calls for service occur in the morning as compared to the afternoon. This could possibly result from problems that occur after the Help Desk closes on the previous day and may indicate a need for the Help Desk to extend hours and revise staffing patterns.

Over 77% of the Help Desk call outcomes were rated as "very good" or "great job". While these numbers are not consistent with the survey and interview data, they do reflect the informal and family attitudes prevalent at IRM and the Board Offices. Documented policies, procedures and service levels would provide the end user with an objective expectation that would better indicate whether these service levels are being met.

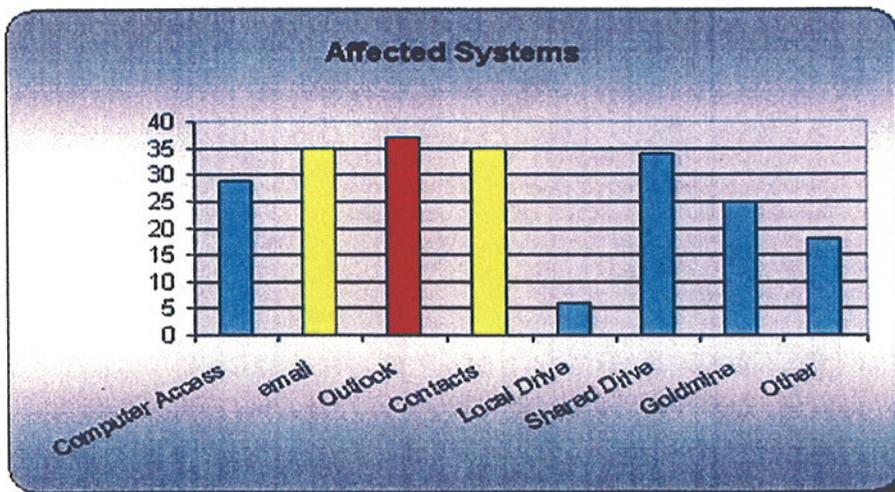
## Analysis of CIO Electronic Surveys

The CIO conducted two electronic surveys to identify the quantitative and qualitative impact of the April 7, 2004 system outage on the Board of Supervisors' business operations. Each Board Office was asked to send the e-mail surveys to their staff in the Hall of Administration and District Offices. Forty-eight individuals responded to the objective survey and 46 responded to the open-ended follow-up survey.

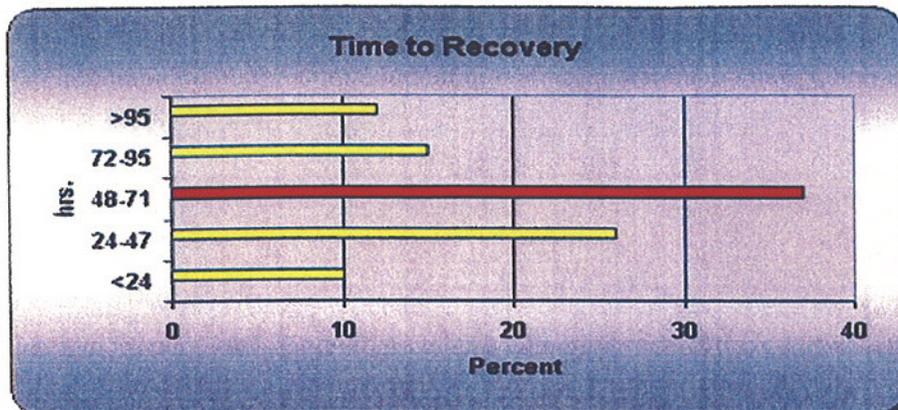
The following figures summarize the findings from these surveys:



Eighty-nine percent of the respondents indicated that they were significantly affected by the computer outage. This is consistent with the information obtained by interviews with the Office Manager and Chief Deputy from each District. Assuming a conservative productivity loss of 50 percent, the productivity loss resulting from the system outage is estimated to be approximately \$200,000.



The majority of respondents indicated that MS Office tools, including Outlook for e-mail and calendar, were the most affected services resulting from the system outage. This is consistent with the loss of the Active Directory and user profiles.



The survey indicated that the average time for full recovery was 48 hrs. When asked how long the system could be down before an outage impacted critical business operations, the Office Managers and Chief Deputies interviewed indicated four (4) hours.

A follow-up, open-ended, objective survey was conducted approximately one (1) week after the outage to obtain additional feedback into the impact of the incident and comments on the recovery process.

Interruption of Service. Consistent with the objective survey, the majority of respondents to the qualitative survey indicated that office systems, specifically Outlook e-mail and calendar, were the services most impacted. Representative comments included:

“For almost 4 days I was unable to log on at either downtown or in my field office thus rendering me useless as a field deputy. No contacts, no calendar, no Word documents, etc.”

“Denied all access to Outlook which controls flow of e-mails, contacts and calendar entries. These functions play an important role in daily activities.”

“We were non-operational for approx. 4-5 days. I was unable to access my Calendar -- a disaster and embarrassing. Fortunately, Outlook Contacts are printed every 3 months and placed in a binder. We're now printing my Calendar for a 2 week period.”

“It was very slow, but understandably so. I know Karen worked very hard. She even slept overnight on the 8th Fl.”

Impact on Business. The majority of respondents indicated that they were unaware of their dependency and need for basic office services. Representative comments include:

"Prior to the 'incident' I never fully realized the extent to which I depended on Microsoft Outlook. Not having access to my boss' calendar and being unable to obtain, retrieve and send e-mails was HUGE. Constituent information which is tracked through GoldMine probably is the most critical aspect of my position. It is invaluable and one day without it is a major set back."

"Without my computer, I'm not able to communicate with other County departments. The telephone is not always desirable."

"No email was the worst – that is how I do 90% of my communicating with co-workers and constituents."

"Hampered from responding to constituent concerns in a more timely way. Could not access their contact information to advise them of status. Not able to follow up or respond on some action items due to no email access."

"Not being able to access my H: drive affected my ability to conduct business most (since I save most of my documents on my H: drive, and was working on several projects that needed to be finalized during that time)."

Process Used to Restore System. The majority of respondents indicated dissatisfaction and frustration with the time required to restore systems and the lack of communication on the status and priorities for recovery. However, many users were understanding of the difficulties and supportive of IRM staff. Representative comments:

- "Horrible. I don't feel the issue was treated with the severity it needed to be, I thought the BOS offices were disrespected and I hope someone suffers severe consequences for it happening."
- "Everyone worked very hard to get the system back up and install everything we lost."
- "It took considerably longer than I expected."
- "Little communication as to what happened, when it would be fixed, seemed slow to restore."
- "There was a lack of coordination. I'm sure that Executive Office felt the pressures of BOS offices... in the end it worked out."
- "As far as I know, about 3 days after the outage my office computer was re-configured." However, I was not informed that my at-home laptop needed to be reconfigured as well, so it took additional days for that to come back into service.

IRM needs to maintain a list of people who work from home and be PROACTIVE in ensuring that the home systems are operational when these events occur.”

- “I know they tried their best to help in the restoration process, considering the limited staff. One problem is that there is only ONE person available (or assigned) to assist us & if that person is not in, then we sometimes have to wait for their return. Present staff is very knowledgeable; the bottom line is that they really need more staff.”
- “Eventually it came back up but made me realize how dependent we are on the system. I knew they were working as quickly as possible to restore.”
- “My only concern with the process was that, being in a district office, it was automatically determined that our work was not priority and could wait until the problems of everyone at the downtown offices were taken care of.”

Quality of Services Provided by IRM, over Past Three (3) Years. Consistent with the Chief Deputy and Office Manager interviews, respondents were pleased with the IRM staff, but indicated that policies and procedures could be improved – e.g., implementing Help Desk procedures and resources so that a majority of calls could be resolved while the caller is on the phone, stated service levels so callers have an expectation on when their problem will be resolved, etc. Representative comments include:

- “Overall I have been pleased with the service provided by the support staff in the IRM group.”
- “Not very good. Great when they finally get around to you but always slow to respond and get back to you.”
- “Karin Moran, Brenda Curtis, and Debra Connessero have done an outstanding job. They are very attentive to our needs and often stay late to get the job done. Oftentimes, their hard work goes unnoticed and they are often blamed for system errors/problems.”
- “I would say the ‘Help Desk’ line has not been very helpful. For the most part, we do not get instant help with any minor problems or questions, i.e. how to number pages in Word, how to add a column in Excel...etc. And when we email the Help Desk, we just get an email back stating that someone will contact us very soon (which does not happen often) & a Ticket #. I think that someone with basic computer skills should answer the Help Desk line; I am sure that some of the problems can be instantly resolved if it's just a simple computer question.”

## ***Measuring Performance***

In order to measure the efficiency and effectiveness of the aforementioned recommendations, and to guide adjustments where necessary, a standardized method for reporting and analyzing I/T performance data needs to be established. An I/T scorecard should be instituted to measure I/T health and to provide a high-level snapshot report of metrics and target goals. An I/T performance scorecard is an industry-standard method of maintaining consistency between I/T initiatives and corporate strategy. It balances traditional supply-side operational metrics with demand-side (consumer) measures of customer satisfaction and key indicators of strategic goal achievement.

For example, Microsoft uses an I/T performance scorecard internally. The Microsoft I/T scorecard is an internal, multi-user, monthly reporting tool used by the CIO, general managers, directors, I/T account managers, and service managers to track metrics across the Microsoft I/T organization in a centralized repository. The Microsoft I/T scorecard helps drive operational excellence. By measuring and reporting productivity, efficiency, and quality, it helps Microsoft I/T understand and manage operations, and optimize group performance. The I/T scorecard identifies the key drivers and process variables that have the greatest impact on groups and businesses. The granularity and trending approaches help Microsoft I/T understand the root causes of problems and apply corrective actions. Service performance is evaluated objectively, and trend analysis helps anticipate future performance and resource needs. Also, the I/T scorecard provides trend and comparative data to detect and correct problems early.

### **Sample Microsoft monthly scorecard report.**

Microsoft Office Excel 2003 - DEMO-IT SCORECARD (2).xls

File Edit View Insert Format Tools Data Window Help

Type a question for help

Times New Roman 36

A1 IT Scorecard Demo

IT Scorecard Demo				Target				Trend		
				Americas	Asia Pacific & Japan	EMEA	Worldwide	Two Cycles Ago	Previous Cycle	Current
<b>FY2003 Metrics</b>								Worldwide	Worldwide	Worldwide
<b>ENTERPRISE INFRASTRUCTURE SERVICES</b>										
Enterprise Infrastructure Services	# of Computer System SR's	N/A	N/A	N/A	N/A	#	#	#		
	% of Computer System SR's within SLA	0%	0%	0%	0%	0%	0%	0%		
	Average Round Trip Delay	#	#	#	#	#	#	#		
	Backup Success Rate	0%	0%	0%	0%	0%	0%	0%		
	Data Center Availability	0%	0%	0%	0%	0%	0%	0%		
	Domain Controller Availability	0%	0%	0%	0%	0%	0%	0%		
	Network Availability - Backbone	0%	0%	0%	0%	0%	0%	0%		
	Network Availability - Tailsite	0%	0%	0%	0%	0%	0%	0%		
	Proactive vs Reactive SR's	0%	0%	0%	0%	0%	0%	0%		
	Real Time Management Systems Availability	0%	0%	0%	0%	0%	0%	0%		
Restore Success Rate	0%	0%	0%	0%	0%	0%	0%			

Ready NUM

Green and red color codes are based on evaluation against a target metric. Metrics that are coded green on the report indicate that the metric is falling within an acceptable target range. If coded red, it indicates that the metric is not meeting its target goal. By design, no yellow coding appears on the report. The goal is to view data that is to be acted upon. A red metric provides an opportunity for a service manager to explain what issues are contributing to the level of service performance, and what is planned to improve it. If a metric is green for more than six months, the target is either increased or removed from the report. Because the focus is on consistent improvement in service performance, the targets are always changing and moving up incrementally.

The I/T scorecard is used during quarterly business reviews and the annual Microsoft I/T budgeting process. It assists in decisions to allocate long-term resources. I/T scorecard metrics are used to help assess the impact of additional, or fewer, resources on a service's performance level. For example, if a service group requests additional operational headcount, metrics that relate to that service can be tracked to measure a difference in service performance levels. In other words, a metric may move from red to green, proving the impact of the additional headcount and justifying the additional resource. Conversely, if a metric remains consistently green from month to month, this status may assist in justifying the reallocation of some of the resources dedicated to that service. Service performance levels are tracked if a resource is reallocated or if a function is outsourced. If the metric remains green, this status can validate the reallocation decision. In this way, I/T scorecard metrics are used as a long-term planning mechanism for strategic resourcing decisions.

## ***Acknowledgements***

We would like to extend our sincerest appreciation for input and assistance provided by the following individuals, and their respective organizations:

### Los Angeles County, Board of Supervisors

- Barbara Nack, Office Manager, 1<sup>st</sup> District
- Louisa Ollague, I/T Deputy, 1<sup>st</sup> District
- Sandra Fierro, 1<sup>st</sup> District
- John Hill, Chief of Staff, 2<sup>nd</sup> District
- Miriam Simmons, I/T Deputy, 2<sup>nd</sup> District
- Alisa Belinkoff Katz, Chief of Staff, 3<sup>rd</sup> District
- Joel Bellman, Deputy, 3<sup>rd</sup> District
- Brence Culp, I/T Deputy, 3<sup>rd</sup> District
- Gail LeGros, Office Manager, 4<sup>th</sup> District
- Mike Gin, I/T Deputy, 4<sup>th</sup> District
- Kathryn Barger-Leibrich, Chief of Staff, 5<sup>th</sup> District
- Angela Mazzie, I/T Deputy, 5<sup>th</sup> District
- And, all who shared their experiences in our electronic surveys.

### Los Angeles County, Executive Office

- Violet Varona-Lukens, Executive Officer
- Charlene Abe, Chief Deputy
- Gary Syssock, I/T Manager
- Martha Campos, Senior Information Resource Specialist
- Andy Xu, Information Resource Specialist

### Los Angeles County, Department of Public Works

- Ted Chu, Senior Telecommunications Systems Engineer
- Jeff Orlin, Information Systems Analyst II

### Los Angeles County, Chief Administrative Office

- Edwin Ro, Network Administrator

### Los Angeles County, Internal Services Department

- Dave Chittenden, Midrange Computing Division Manager
- Jeff Luna, Messaging and Directory Specialist
- Nhan Le, Network Security Specialist

### Los Angeles County, Chief Information Office

- Jonathan Williams, Chief Deputy
- Al Brusewitz, Chief Information Security Officer

- Robert Pittman, Assistant Chief Information Security Officer
- John McIntire, Associate CIO
- David Hamamoto, Associate CIO

#### Microsoft Corporation

- Brian Karasawa, Senior Microsoft Services Consultant
- Javier Rodriguez, Senior Technology Specialist
- Don Born, Government Account Executive
- Jim Heflin, Technical Account Manager
- Richard Kwon, Active Directory ROSS Engineer
- Raphael Song, Exchange ROSS Engineer

#### Cisco Systems Incorporated

- Anne Barrett, Executive Advisor
- James Hersey, Account Manager

#### Dell Incorporated

- Dave Otto, Major Account Manager
- Mike Lookingbill, Enterprise Storage Specialist

#### SBC Communications Incorporated

- Steve Itano, Senior Systems Manager of I/T Operations
- Ray Schneider, Technical Sales Executive
- Sandy Chu, Senior Account Manager

#### Network Associates Incorporated

- Dennis London, Senior Systems Engineer
- Bret Brasso, Territory Manager

#### Gartner Incorporated

- Jeff Heath, Senior Account Executive