Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Government Financial Architecture: A Focus on Centralized Security and Continuity of Operations

To reverse trends of weak security in government technology systems, Congress now requires Federal agencies to better manage internal IT security. Financial operations are of specific interest, and this effort involved looking at the technical architecture supporting the financial activities of a large Federal agency undergoing the implementation of a new financial system. The information contained in this document was provided to the Chief Financial Officer (CFO) in response to concerns of compliance. The primary focu...

Copyright SANS Institute
Author Retains Full Rights

AD

Government Financial Architecture

A Focus on Centralized Security and Continuity of Operations

Matthew Mickelson
GIAC Security Essentials Certification (GSEC)
December 4, 2003
Practical Assignment Version 1.4b, Option 2

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

ABSTRACT **3**

BACKGROUND **3**

BEFORE SNAPSHOT **4**

DEFINING THE BOUNDARY 4
ESTABLISHING A BASELINE PICTURE 5
RISK ASSESSMENT 7

DURING SNAPSHOT **8**

ANALYSIS OF ASSESSMENT RESULTS 8
IDENTIFICATION OF CHANGE DRIVERS 11
SOLUTION OPTIONS 11

AFTER SNAPSHOT **12**

RECOMMENDATION 13
NEXT STEPS 14
CONCLUSIONS 15
LESSONS LEARNED 15

APPENDIX A – VIRTUAL MACHINES **17**

REFERENCES **20**

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Abstract

To reverse trends of weak security in government technology systems, Congress now requires Federal agencies to better manage internal IT security. Financial operations are of specific interest, and this effort involved looking at the technical architecture supporting the financial activities of a large Federal agency undergoing the implementation of a new financial system. The information contained in this document was provided to the Chief Financial Officer (CFO) in response to concerns of compliance.

The primary focus of this effort was to address security issues laid out by the CFO; specifically the following key areas for improvement:

- De-Centralized Architecture
- Disaster Recovery
- Continuity of Operations
- Network and Server Availability

With these goals in mind, information was collected, a risk assessment was performed, and four basic solutions were developed. Benefits and challenges associated with each solution were compared, and a final recommendation was presented as the "best fit" solution given the business need, available resources, security issues, and overall political consensus.

Specifically, this work resulted in a concrete diagram of the financial network, the identification of critical gaps in contingency planning, and set the stage for completion of a full disaster recovery plan. The consolidation plan recommended during this process was the key step allowing the CFO to centralize control of the network and bring the costs of disaster recovery testing within budgetary limitations.

Moreover, this document seeks to provide the reader with a solid understanding of the architecture analysis and recommendation process, the order in which steps should be completed, results of this effort, and lessons learned from the experience. The data was used by the CFO, Federal policy officials, internal IT staff, and key decision-makers as a comprehensive picture of the financial environment and strategic options for developing a more secure architecture.

Background

During the summer of 2000, the US General Accounting Office (GAO) called for information security audits of Federal agencies. The resulting report summarized security weaknesses identified in audit reports from the past year. The report highlighted that "evaluations of computer security … continue to show that Federal computer security is fraught with weaknesses and that, as a result, critical operations and assets continue to be at risk." [1]

[1] General Accounting Office – http://www.gao.gov/new.items/ai00295.pdf

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Subsequently, the President signed the Government Information Security Reform Act (GISRA), P.L. 106-398, Title X, Subtitle G, as part of the Defense Authorization Act of 2001. [2] GISRA requires agencies to better manage internal information security and requires an independent review by the Inspector General (IG).[3]
Although GISRA expired November 29, 2002, the Federal Information Security Management Act (FISMA) was enacted as part of the Homeland Security Bill and permanently extends the IT security requirements of GISRA.

FISMA was created to ensure security of resources supporting Federal operations and assets. It covers both unclassified systems and those pertaining to national security. The scope of the effort outlined in this document was for the protection of unclassified systems.

Before Snapshot

Implementation of a new web-based financial application will transition manually intensive financial management processes to highly automated processes throughout the organization. This will also transfer larger volumes of data onto the network systems. The data load (storage only) is expected to grow from about 10 Gigabytes of data on the production database to over 90 Gigabytes (spread over eight database instances).

The "before snapshot" of this effort was comprised of the following steps:

- Defining the boundary – the scope of the study
- Establishing a baseline picture of the financial architecture
- Risk assessment

Defining the Boundary

The first step in assessing any system is defining it by determining its boundaries and interfaces with other systems. This includes technical boundaries as well as organizational ones. The system studied during this effort was defined by financially related processes, applications, communications, and storage. As a general rule, these systems have one or more of the following characteristics:

- Under direct management control of the office of the CFO
- Have financial or accounting business functions or objectives
- Have essentially the same security needs

All components of a system do not need to be physically connected. For example, a system may consist of a group of stand-alone PC's in an office, or multiple

[2] General Services Association – http://www.gsa.gov/attachments/GSA_PUBLICATIONS/extpub/legupdate4.doc
[3] Federal Computer Week - http://www.fcw.com/fcw/articles/2001/1210/web-gisra-12-13-01.asp

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

configurations installed in locations with the same environmental and physical safeguards. Both scenarios describe very different, but valid systems.[4]

Establishing a Baseline Picture

Before any analysis can be performed, an accurate baseline picture of the network must be established. To accomplish this, the necessary information was gathered and compiled in an easy to read format. All system owners were interviewed, and key statistics were compiled for each component of the financial architecture within the boundaries established earlier. A sample entry from the resulting information gathering process is pictured below:

Web Server X	
Location	Bldg ABC; Room 123
Manufacturer	IBM
Machine Type	J30 RS-6000
Age	5 years
Operating System	AIX
Supported Applications and Processes	Oracle Development Database, Financial Applications, Oracle Name Server
Processor(s)	4 x 112MHz
RAM	768MB
Hard Disk Space	30GB 80% used
Average CPU Utilization	25%
Backup Method(s)	TSM – Daily; Off-site 8mm – Weekly
Encrypted Sessions	PowerTerm 128 bit
Maintenance	$725/month hardware
General Comments	$50,000 depr over 3 yrs

Snapshot of the Network

The current architecture reflected a combination of different systems purchased to support financial processing over the past five years. The machines were then grouped by function into the following categories:

- Database
  - Production database(s)
  - Test/Development database(s)
  - Configuration management repositories
  - Other Oracle Services
- Mainframe
  - An older system in use since 1988
  - CPU recently replaced
  - Financial data repository

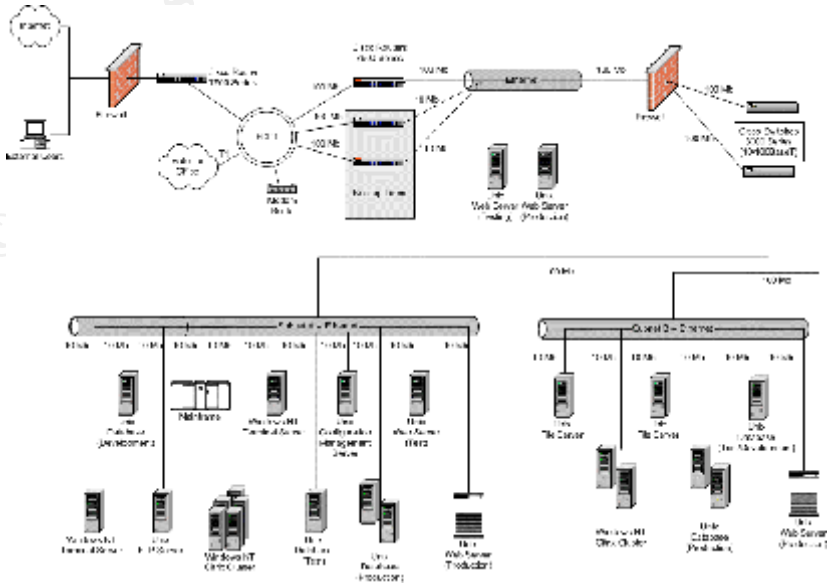
[4] Dept. Health & Human Services - http://www.cms.hhs.gov/it/security/docs/ssp_meth.pdf

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

    - Canned financial reports used throughout the organization
- Web Support – External Use
    - Production Web Application Services
    - Test/Development Web Application Services
- Web Support – Internal Use
    - Citrix clusters supporting financial applications
    - Citrix clusters connecting users to other secure systems
    - Oracle Web services
- File Support
    - Batch file transfers (slave FTP services)
    - File repositories
- Backbone
    - Routers (Cisco 7500 series)
    - Switches (Cisco 3000 series – 10/100BaseT Ethernet)
    - Firewalls
    - Ethernet

All machines were attached to uninterruptible power supplies (UPS) and were backed up on-site nightly. Additionally, taped back-ups of critical systems were created weekly and were stored off-site at a local satellite office. All systems featured 128 bit encryption (SSL) for all sessions with two exceptions: the mainframe offered 168 bit encryption and a slave-only FTP server offered no encryption (used only for automated internal batch file transfers).

The hardware components supporting the financial processes are currently grouped into several subnets. However, two subnets comprise a majority of the support network. Subnet A is the collection of servers supporting internal accounting activities. Subnet B is the primary support for all other financial activities. The resulting baseline network diagram (cleaned of sensitive information for the purposes of this document) of the financial system is displayed below.



© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Risk Assessment

The next step of the effort involved a focused risk assessment of the financial architecture. Following the guidelines set forth by the CFO, the environment defined in the previous steps was analyzed with particular emphasis on the following areas:

- De-Centralized Architecture
- Disaster Recovery
- Continuity of Operations
- Network and Server Availability

Risk assessments are an extremely important tool for evaluating the state of a given system. Assessments can be large or small in scope. Regardless of how complex a risk assessment is, each is just a combination of a few simple concepts. Before moving on, we introduce some of the basic concepts.

A ***threat*** is anything with the potential to adversely affect a system (e.g. destruction of data, disclosure of data, modification of data, or denial of service). Threats can be man-made (either accidental or intentional behavior) or environmental (e.g. tornado, flood, utility failure). For example, a malicious hacker intending to compromise an organization's critical server is a threat. Similarly, a broken water pipe above a room containing an organization's network infrastructure is also a threat.

A ***vulnerability*** is a potential weakness. Vulnerabilities can apply to policies, procedures, systems, or controls. For example, a server having a null password and not protected by a firewall is a vulnerability (possibly exploited by a hacker). Similarly, servers located under leaky pipes also a vulnerability (to the threat of water damage).

A ***risk*** is the likelihood a given threat will take advantage of a given vulnerability.

A ***risk assessment*** is tool to determine the resulting impact of risks to an organization. Assessment of each risk includes determining the impact it would cause to each underlying asset of an organization. It is important to remember assets include the technology, information, and people supporting an organization. These assets are usually grouped by type. In our financial architecture effort, we grouped assets by function (e.g. database services, web services, network backbone).

The risk assessment involved the following actions (and questions):

- Identification of valuable assets (What should I protect?)
- Measurement of threats (What should I protect against?)
- Measurement of corresponding risks (What is the likelihood this threat will happen?)
- Measurement of vulnerabilities (Where should I focus protection?)
- Determination of appropriate countermeasures (How can I mitigate a particular risk?)
- Determination costs versus benefits (What is the cost of protection in terms of time and money? Is the risk worth the cost?)

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

General risk assessments are used to highlight potential compromises to any of the following:

- Confidentiality (e.g. information restricted to a specific group of people)
- Integrity (e.g. the fact that data in the database is correct)
- Availability (e.g. the fact that the database is functional and accessible)

However, our focused risk assessment explored issues primarily related to availability.

During Snapshot

Although this assessment was narrowly focused on the availability issues of the financial systems, the amount of information available beforehand was scarce. As a result, much work was required to complete the tasks previously outlined in the "Before Snapshot" section. For the purposes of this document, we have chosen to begin the "During Snapshot" effort once all the critical information (e.g. a completed network diagram, server statistics, a completed risk assessment matrix) was collected. With the information collected in the previous steps now available, the task of interpreting the results and providing a solution was begun.

Analysis of Assessment Results

A brief summary of the assessment results confirmed the need for the organization to centralize its computing resources. The key security issues coming out of the analysis were the following:

- Aging Hardware/Software
- Disaster Recovery (DR)
- Continuity of Operations (COOP)
- High Availability
- Back-Up/Restore
- Capacity Planning

Aging Hardware/Software

There were nine servers over five years old and quickly becoming underpowered – several supporting production activities. The rest were approaching three years old. Consolidation (and subsequent retirement) of as many of these machines as possible was deemed a key business driver for any proposed solution. Additionally, the production databases were run using Oracle 7 – now unsupported by the vendor. Furthermore, several critical security vulnerabilities affecting these installations were now outside the support agreement.

Disaster Recovery

The next major outcome of the assessment was the need for a solid disaster recovery plan; the resources to test it annually, and the resources to execute it successfully as

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

needed. Disaster recovery tools and procedures form a roadmap to recover a portion of the system (or the whole system) in the event of a significant failure. Disaster recovery plans deal with events ranging from an unplanned server or power outage to a full-scale loss of infrastructure. For a power or server outage, this typically includes the proper shutdown of affected components along with instructions for bringing the component live again and restoring cached data. For full-scale infrastructure disasters, details for bringing off-site components and applications on-line should be outlined.

Thirteen systems on the network were deemed essential. However, only the mainframe and the production database servers were included in a disaster recovery plan. Including all essential systems in the disaster recovery plan would have roughly tripled the costs of disaster recovery efforts. Server consolidation was the easiest (and most cost effective) method to counteract this trend. Fewer physical servers require fewer backups, and hence this option is less costly. On the other hand, more physical servers would require more disaster recovery tasks from more system administrators. The mainframe was also found to support significantly more load and only require a single recovery plan for all of its supported services. Placing several systems on the mainframe was estimated to cut disaster recovery costs about 80%.

Continuity of Operations (COOP)

Continuity of operations includes disaster recovery efforts, but also outlines the minimal processes and accompanying hardware necessary to maintain critical operations. For example, the core financial data was determined to be the most critical asset of this assessment. However, this data was distributed across several disparate systems. Consolidating this data onto a single machine would simplify the COOP efforts desired by the executive staff by simply focusing on the uptime of one machine.

It should be emphasized there are two clear sides to this issue. While consolidation can be viewed as leading to a more centralized point of failure, it also achieves a more central point of control. The risk assessment clearly found that the business advantages of a single point of control outweighed the risks of placing such systems in a single point of failure; given the uptime statistics of the various equipment. For example, consider placing email servers, file servers, web servers, and database servers on a single mainframe (isolated by virtual machines). In the event of a disaster, business operation can continue once the mainframe is back online. A complete COOP framework for the financial architecture was addressed during a later effort as a result of these findings.

High Availability

The next key finding of the assessment was that high availability solutions (already in place on a few machines) should be included on all mission critical components (e.g. the production databases). Two different high availability solutions were offered to ensure connectivity in the event of hardware or software failure depending on the server. The first was a fail-over solution. This involves using at least two redundant

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

(generally lower cost) machines capable of serving a client computer. If one fails, the second takes over seamlessly providing a stable connection while the first is brought back online. The second solution was to use equipment (generally higher cost) specifically engineered for high mean-time-between-failure (MTBF) rates. If the MTBF is vastly greater than the lifetime (or periods between scheduled outages) of the machine, this is usually sufficient for practical purposes. For instance, the MTBF of the current mainframe was 65 years and that of the Unix servers was several months. With over 12 (16 in fact) Unix servers in use, at least one server on average would be expected to experience an unplanned outage each month. This makes consolidation onto the mainframe the most reliable approach and offers increased application uptime for essential applications.

Back-Up/Restore

All data should be backed up and placed off-site for secure storage; especially the core financial data. Currently all servers on the network have automatic backup procedures, but no formal procedures exist to restore the systems. These must be created and tested to ensure essential data can be restored successfully in case of an emergency. A cost analysis included as part of the risk assessment put maintenance costs for the financial systems at approximately $1.7 million per year. However, funding levels provided half that amount. This disparity between the operational cost and the budget resulted in Disaster Recovery Plans that have never been tested. Consolidating processes onto the mainframe will result in a reduction in backup and restore time and costs and will allow affordable testing of the disaster recovery plan.

Capacity Planning

The assessment also underscored another key issue related to the off-site back up procedures. Outside the internal firewall, only one line is active (providing at most a 100 Mb connection). Inside this firewall, connections are routed to two lines capable of 100 MB each. In addition, nightly back up procedures require data to travel through the internal firewall to get to the off-site back-up location. If each 100 Mb line inside is transmitting at full capacity, there is a bottleneck transferring the 200 Mb of data onto the 100 Mb line on the other side of the firewall. Removing the bottleneck would decrease strain on the firewall during the nightly backups. Without upgrading the network line (i.e. to Gigabit Ethernet), the bottleneck may be mitigated through reduction in the number of servers serving connections outside the internal firewall. Consolidation of servers would help to resolve these issues.

As highly manual processes transition to more automated ones, more data capacity will be required on the network. Sufficient storage must be allocated, and sufficient processing power must be available for end users to run financial transactions and reports. Most servers were identified as over-utilized or approaching maximum capacity limits. For example, seven servers were using over 80% of their disk space. Consolidating these servers onto the mainframe would allow processing power and capacity to be allocated as needed. This would relieve the burden of maintaining

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

multiple servers and storage space can be allocated to Virtual Machines as required by the application or data size.

Identification of Change Drivers

After the results of the focused risk assessment had been analyzed, the first step toward proposing viable solutions was to identify the key components behind any recommended changes. Many of these change drivers were outlined by the CFO before the assessment (e.g. de-centralized architecture, disaster recovery). However, a few additional motivating factors came out of the study. The key factors that influenced the final recommendations are briefly outlined below.

Business Drivers

- Implementation of a new organization-wide financial application will increase the user community, transaction volume, storage requirements, and overall visibility of the financial architecture.

Resource Drivers (e.g. Cost, Staffing, Equipment)

- Maintenance of a large number of servers.
- Maintenance of a disparate community of operating systems, vendors, and applications.
- Current budgetary constraints were not expected to increase significantly.
- The new IBM mainframe is currently under-utilized and is the most secure, reliable, and scalable server on the financial network.

Security Drivers

- A need for more centralized architecture
- Continuity of Operations (COOP)
- Network bottleneck limiting back up and restore activities.
- Availability of services due to older equipment.
- Disaster recovery planning and testing of all mission critical systems.
- Oracle 7 (used for the production databases) is now unsupported and contains critical security vulnerabilities that will not be patched by the vendor.

Solution Options

Four options based on the previous analysis were developed to address the overall issues outlined by the CFO and the subsequent focused risk assessment. These options varied in complexity, cost, implementation time, and overall approach to best fit a multitude of circumstances. A brief summary of each option follows:

New Server Approach – The first option included procurement of two new database servers, a new web server, and a new dedicated backup server for the databases. The database servers will replace the aging production database servers, and consolidate

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

four aging servers onto two new machines. These four servers may be retired once consolidation onto the new servers is complete.

Phased Consolidation Approach – A three-phase plan using a pilot consolidation phase, a database consolidation phase, and a network consolidation phase. First, initial upgrades to the mainframe are required to expand its functionality and allow for consolidation of the financial web servers, file servers, and periphery servers onto the mainframe. This first consolidation effort would also server as a proof-of-concept pilot to test the consolidation of physical servers onto Virtual Machines within the same mainframe. Upon successful completion, additional upgrades and licenses would be purchased for the mainframe to allow full consolidation of all database servers (if upgrades are not purchased as part of initial investment). This option would eventually retire 10 servers from the network. The final phase consists of relocating the remaining servers to the same subnet, thus further simplifying the network.

Full Consolidation Approach – This option is essentially the same as the *Phased Consolidation Approach*, just without the phased timeline. Full consolidation onto the mainframe would commence a single implementation effort.

Hybrid (Consolidated Phased/New Server) Approach – This option uses the first phase of the *Phased Consolidation Approach* consolidating non-database servers onto the mainframe, as well as the purchase (or lease) of the new servers described in the *New Server Approach* for the databases.

After Snapshot

Once the four basic solutions were developed, several meetings were held with each key stakeholder group: CFO and executive staff; system administrators; financial system experts; and financial implementation team members. These meetings were held to accomplish the following:

- present the findings in a manner geared to each audience;
- verification of the risk assessment results;
- identification of an ideal solution given the business environment; and
- to generate buy-in of the recommendation increasing its chance of success.

After the results of these meetings were incorporated with the findings from the previous sections, the benefits and challenges associated with each solution were compared with one another. The final recommendation was presented as the “best fit” solution for the business need, resources available, security issues, and overall political consensus.

Based on the results of the focused risk assessment, current change drivers, and general consensus, the recommended implementation option is the *Hybrid Approach* combining the first phase of the *Phased Consolidation Approach* and the *New Server Approach* (as outlined in the previous section). Decreasing recurring costs (e.g. hardware maintenance, disaster recovery costs) was a primary concern of

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

management. Additionally, decreasing overall maintenance of the network by using new technology (i.e. new servers) was a primary concern of the technical staff. Consolidation of activities to a central point of service clearly offered the most reward per dollar spent. However, the *Hybrid Approach* allowed for a proof-of-concept to be performed while databases could be migrated to new equipment. These were key attributes in the strategic plan of the CFO allowing added flexibility; keeping the network up to date; and setting up high-visibility milestones for measurement purposes.

Recommendation

The *Hybrid Approach* consists of two basic phases: Pilot Consolidation and Database Consolidation. This provides a middle ground between full network consolidation and purchase of new equipment. Although new database servers are purchased to resolve capacity issues, this approach still offers a net reduction of servers from the architecture in turn providing decreased recurring costs, more centralized operations, simpler more cost effective disaster recovery efforts, and a balance of political needs.

During the **pilot consolidation**, non-database servers (i.e. web servers, file servers, and periphery servers) are consolidated to the mainframe separated by virtual machines. Initial upgrades (CPU upgrade and storage capacity) to the mainframe are required to expand its functionality and allow for consolidation of the financial web servers, file servers, and periphery servers. This effort also provides a proof-of-concept to test consolidation of physical servers onto virtual machines of the mainframe.

By consolidating processes into Virtual Machines (VM) on the mainframe, the entire architecture becomes more reliable, more secure, and much easier and less expensive to maintain. Specific details regarding virtual machines on the IBM mainframe are described in the appendix.

The **database consolidation** commences upon successful completion of the pilot. This involves the purchase or lease of equipment to create a new database subnet:

- 2 new database servers (high-availability fail-over cluster)
- 1 dedicated back-up server for the database cluster (with software)
- 1 web application server for Oracle Applications dedicated to database activities
- 1 firewall to protect the new database subnet

All database activity would now occur behind a dedicated firewall. Additional upgrades and operating system licenses would be required for the mainframe to allow full consolidation of all database servers (if upgrades are not purchased as part of initial investment). Once complete, the organization ten servers could retire from the network.

Benefits

- A significant reduction in overall operating and maintenance costs.
- A significant reduction in network complexity and the overall number of servers.
- Disaster recovery efforts are simplified and less expensive to test and execute.
- Improved data security with a dedicated database firewall.
- Fewer servers streamline back up and recovery procedures and reducing costs.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

- Improved database reliability with a new fail-over database cluster.
- Tighter change control over the network.
- Essential applications are located on the most secure reliable machine.

Challenges

- Implementation of this approach is labor intensive.
- Oracle licenses for Linux (to be used on either the virtual machines of the mainframe or LPARs of the new database cluster) were not available at the time this document was presented to the CFO.
- Oracle services cannot be secured until upgrades are performed.
- While failure rates for the mainframe are extremely low (once every 65 years), there is a potential central point of failure.

Costs

- Costs of the recommended solution are broken down in the following chart. Please note all amounts were calculated in February 2002 when this document was submitted to the CFO. These figures may not be indicative of current costs.

Mainframe Costs	Costs	Database Server Costs	Costs	Total
1st CPU Upgrade for Mainframe	$42,630	Primary Server 2 x 750Mhz CPU's	$200,000	
182 GB Additional Mainframe Storage	$40,000	500 GB Storage		
2nd CPU Upgrade for Mainframe (not required unless other resources are migrated to the mainframe as well)	***	Fail-Over Server 2 x 750Mhz CPUs 500 GB Storage	$200,000	
		Back-Up Server	$100,000	
		Web Application Server	$180,000	
		Back-Up Software	$50,000	
		Maintenance ($3000/mo.)	$36,000	
		Firewall	$20,000	
	$82,630	Purchase Servers	$786,000	$868,630
		*Lease Servers	$592,200	$674,830

**Lease totals based on a 3-year $500,000 lease at 4.6% interest (standard lease w/ current promotional rate) terminated after two years and include software, firewall, and maintenance purchase.*
Mainframe upgrade costs include 12 month warranty. Afterwards, annual support fees (approx. $3,453) apply.
Application licenses ($310,000) for the new Web application server will be purchased with internal funding.

Next Steps

Based on the findings and recommendations in this document, the management was encouraged to follow these steps:

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

- Develop a transition plan from the existing production servers to the new architecture model
- Upgrade all Oracle databases immediately; the current versions cannot be adequately secured.
- Upgrade to Gigabit Ethernet outside the internal firewall.
- Explore using the link (dedicated T1 line) between the local and satellite offices for fail-over situations.
- Develop a Contingency Plan (to cover disaster recovery and continuity of operations issues)

Conclusions

The office of the CFO adopted a strategic plan of network and architecture consolidation in line with the recommendations of this effort. A full disaster recovery plan was later developed independent of this document. However, the key topics pertaining to disaster recovery were a direct outcome of this effort. A fail-over configuration was also approved for Internet-facing web servers of each office after this effort was completed. These servers were linked to provide seamless services in the event either one experienced an outage.

Lessons Learned

Start Early – Working with people in different areas of the Federal Government requires early planning of all meetings. Plan to begin all processes as early as possible. For example, interviewing system administrators and creating a network diagram from scratch involves large numbers of independent people and takes time.

Identify Peak Times and Work Around Them – Many folks are involved with several different projects with varying deadlines. Avoiding common peak times such as the end of the fiscal year will allow participants the time fully participate and minimize multiple meetings with the same individuals.

Identify Politically Charged Issues – Assessments should be as unbiased as possible otherwise, all the results derived from it will be tainted (or perceived as such). Politically charged issues can easily introduce bias to focused discussions or precipitate hidden agendas. Hot topics exist between groups of most organizations. It's best to identify any politically charged issues early and develop a strategy to address items that may trigger biased responses or uncooperative participants. One political manifestation within an organization using many systems is that employees responsible for each different type will promote the growth of their own area of expertise; such as mainframes, Unix servers, or Windows servers (it is even sometimes prevalent within the previous vendor groups; such as the existence of an AIX or Solaris contingent within the Unix group). Issues like these were mitigated by talking to each group separately and asking each the same relevant questions.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Explain the Process Clearly – Most people are more willing to help if they know the reasoning behind what you are doing – especially those who are analytically-minded. Explaining the purpose of what you are doing helps everyone provide the proper information and also establishes a mandate to those cynical of your motives. The overall benefit of this effort went beyond the CFO's requirement of filling gaps within the financial network. This work produced basic documentation (e.g. network diagrams, formally documented server statistics, business process flow diagrams) the organization did not have or had not updated in years. Once most people understood this, they were more than happy to provide this valuable information. It also increased the security knowledge of everyone involved by providing the opportunity for a focused risk assessment. The visibility of the assessment also revealed the impacts of threats, impacts, and vulnerabilities to some areas of the organization for the very first time.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Appendix A – Virtual Machines

This section explains why consolidation onto the mainframe is so recommended. It focuses on the advantages of using virtual machines on the mainframe, and the role of Linux as the operating system of choice to run them. In short, the strength of virtual machines is to efficiently consolidate several systems onto one server.

The mainframe on the financial network is an IBM MP3000 that is less than a year old (at the time this document was written – February 2002). The VM (Virtual Machine) application embodied in it is VM/ESA (Virtual Machine/Enterprise Systems Architecture), and is a widely-installed operating system for mainframes from IBM having the ability to host other operating systems so each VM seems to have its own complete system of software and hardware resources (e.g. data storage, telecommunications, processor). VM is popular in many large corporations as a system able to manage large number of interactive users communicating, developing, and running applications at the same time.

The strength of VM/ESA is its ability to run other operating systems as their own private virtual machine. The scope of this appendix is to outline the strengths and weaknesses of VM/ESA. As such, much of this discussion focuses on running Linux-based virtual machines (as Linux has proven to be the most efficient and streamlined operating system for such purposes).

Advantages of VM/ESA

Benefits to consolidating servers onto the Mainframe:

- The mainframe offers the highest level of security available on the current network.
- The mainframe is the most scalable server in the architecture.
- The mainframe has the longest mean time between failures (65 years) of any server in the architecture.
- Storage memory and RAM remain inexpensive (at the time this document was written).
- Consolidation of operations to a mainframe will lower overall operating costs.
- Processing power is not the main issue related to the current financial processes.
- The VM/ESA operating system offers the highest level of security available on any server in the architecture.
- The mainframe is the most scalable server in the architecture.

There are also advantages to running VM/ESA over standard logical partitions (LPARs) of a machine: performance monitors are available for VM/ESA; additional high-speed internal communication options exist; and adding new instances is easier and faster than running in LPARs. For example, a new Linux virtual machine can be added at no cost in about ten minutes from request to first use. Acquiring a new platform can take

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

months and cost hundreds of thousands of dollars. Additionally, the main storage device can be shared between VM guests, while it must be dedicated under LPARs.

The most unique characteristic of VM/ESA is each virtual machine appears (from its own point of view) to be running in its own separate environment. As a result, any (currently known) security issues or disasters in one particular virtual machine remain contained to that virtual machine. VM/ESA is considered by many to be one of the most secure operating systems currently available. Furthermore, in a recent intrusion test conducted during a financial audit, an experienced Linux hacker was granted complete access to a virtual machine and was unable to disrupt other virtual machines or gain access to unauthorized resources.

There are many other advantages to using the VM application related to server consolidation. The most obvious is the reduction in the amount of hardware. If several current physical machines are transferred to virtual machines, then those machines are free for other uses or can be removed to reduce maintenance costs. In addition, there are many advantages in terms of scalability and expandability. The mainframe is new and viable for many upgrades being purchases as the base model. If an upgrade is installed, every virtual machine residing on it reaps the benefits of the upgrade.

Given the number of virtual machines residing on one particular system, major concerns of consolidation projects are strategies for back-ups and disaster recovery. In fact, it is easier, more cost effective, and less time consuming to revive a single machine. All virtual machines residing on the system are backed up each time the mainframe is. The costs for back-up and disaster recovery would be the same for the mainframe if it housed one virtual machine or a thousand of them. It is estimated that running virtual machines on the mainframe could reduce disaster recovery costs by 80%.

The amount of electricity a system requires to operate is another recurring hidden cost to consider when comparing servers. Staffing and space are other hidden costs. Up-front costs of a mainframe can appear high, but if energy and space costs are factored in, the VM system becomes more competitive than any rival system (at the time this document was presented to management – February 2002). In fact, hardware costs are typically 20% to 25% of running a server. Facilities, including electricity, make up on average 40%, and personnel charges are about 30%.[5]

The following is an overview of the relative strengths of running Linux under a VM system:

- Resources can be shared by multiple Linux images running on the same VM system. These resources include: CPU cycles, memory, storage devices, and network adapters.

[5] TechTarget News – http://search390.techtarget.com/originalContent/0,,sid10_gci533953,00.html

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

- Server hardware consolidation – the ability to run tens, hundreds, or thousands of Linux systems on a single machine offers savings in space and personnel required to manage physical hardware.
- Virtualization – the virtual machine environment is highly flexible and adaptable. New Linux instances can be added to a VM system quickly and easily without requiring dedicated resources. In particular, this is useful for replicating servers, and providing users a highly flexible testing environment. The initial reason IBM developed VM was to test its own systems.
- Running Linux on VM means all Linux guests transparently take advantage of VM's support for hardware architecture. That is, one support agreement covers all Linux virtual machines.
- VM/ESA provides high-performance communication among virtual machines running Linux (and other operating systems) on the same processor. Specifically, the underlying technologies enabling high-speed TCP/IP connections are: virtual channel-to-channel (CTC) adapter support and VM IUCV (Inter-User Communication Vehicle).
- Data-in-memory performance boosts.
- Control and automation – VM provides support for scheduling, automation, performance monitoring, and performance reporting. Additionally, virtual machine management is available for Linux virtual machines as well.
- Horizontal growth – an effective way to grow your Linux workload capacity by adding more Linux guests to a VM system.

Disadvantages of VM/ESA

VM is expensive and must be administered. The difficulty in finding qualified personnel to run the VM system is another common argument against moving to the platform. Yet finding skills for running high-end Sun or HP servers is a similar burden. A growing number of technicians are coming along with good Linux skills, and they are able to pick up the hardware operating skills easily. For comparison, this is similar to an approximate 50% reduction in overall administrative costs due to reduction in servers.

One of the primary disadvantages of any consolidation effort is also its primary advantage – the centralization of computing. The main disadvantage of centralization is it provides more local points of failure. However, the vendor specifics of the mainframe state the mean time between failures (MTBF) is 65 years for hardware related issues (compared with an MTBF rating of several months for most Unix systems). Running Linux under VM/ESA essentially eliminates operating system failure, and is not affected by the number of Linux instances running.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

References

1. General Accounting Office. "INFORMATION SECURITY Serious and Widespread Weaknesses Persist at Federal Agencies." Report to the Chairman, Subcommittee on Government Management, Information and Technology, Committee on Government Reform, House of Representatives. 6 Sept. 2000. URL: http://www.gao.gov/new.items/ai00295.pdf (30 Nov. 2003).

2. General Services Association. "Protecting America's Critical Infrastructure: How Secure are Government Computer Systems?" House Committee on Energy and Commerce Hearing. 5 April 2001. URL: http://www.gsa.gov/attachments/GSA_PUBLICATIONS/extpub/legupdate4.doc (30 Nov. 2003).

3. Hasson, Judi. "Davis aims to solidify GISRA". Federal Computer Week. 13 Dec. 2001. URL: http://www.fcw.com/fcw/articles/2001/1210/web-gisra-12-13-01.asp (30 Nov. 2003).

4. Dept of Health and Human Services. "System Security Plans (SSP) Methodology." Centers for Medicare & Medicaid Services. 6 Nov. 2002. URL: http://www.cms.hhs.gov/it/security/docs/ssp_meth.pdf (30 Nov. 2003).

5. Hurley, Edward. "Save A Buck Or Two – Use A Mainframe." TechTarget News. 22 Mar. 2001. URL: http://search390.techtarget.com/originalContent/0,,sid10_gci533953,00.html (30 Nov. 2003).

6. International Business Machines Corporation. "Virtual Machine / Enterprise Systems Architecture: General Information." 4th Ed. May 1999. URL: http://www.vm.ibm.com/pubs/pdf/HCSF8A10.PDF (30 Nov. 2003).

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Last Updated: May 21st, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced