RISK IDENTIFICATION OVERVIEW

IT Service Providers are frequently exposed to significant threats to their continued, safe and regular operation and provision of these services for their customers. These threats come in a wide variety of forms, and when combined with vulnerabilities in the systems, processes and people of the IT provider can result in major disruptions. Risk management seeks to address these potential risks to the organization by establishing a formal process of identifying these risks, assessing their potential impact and devising strategies to respond to them.

This report presents the risks identified by the Office of Information Technology (OIT) throughout the year of 2009. Identified risks are reported to the OIT Organizational Resilience Services (ORS) unit who documents the risks and coordinates recommendations for mitigation. The risks contained within this report were identified via a variety of activities, including the following:

- **Incident Reports**
  Occasionally throughout the year, significant events or incidents occur that cause major disruptions to OIT-provided services or systems. After each of these events, an official Incident Report is produced that includes an analysis of what caused the incident, how OIT responded to the incident, and identifies any outstanding vulnerabilities to the OIT’s overall resiliency that the incident and its corresponding response may have highlighted.

- **Business Continuity Planning**
  Organizational Resiliency Services is responsible for coordinating the OIT-internal Business Continuity planning as well as working with the University’s Business Continuity and Disaster Recovery Department in their consultations with critical business units relating to IT resilience and recovery efforts. During these discussions, undocumented risks are sometimes discovered and captured.

- **Business Continuity Testing**
  Throughout the year planned tests of the central IT environment, specific services and internal unit business continuity plans occur. Results of these tests sometimes reveal risks and/or vulnerabilities that are identified and documented.

- **Business Process Documentation and Improvement**
  OIT often develops and refines internal business processes. Sometimes this process reveals risks that had not previously been quantified or documented, which are then captured at that point.

- **Service Assessments**
  Service owners frequently assess their services for effectiveness and efficiency. When risks are identified during these assessments, they are captured and identified.

The risks in this report have been organized by their criticality factor, a measure of how serious a threat the risk is to the regular operation of OIT’s services. In addition to listing the risks by criticality, the report also includes what measures were recommended in order to mitigate the risks.
RISK SUMMARY

Below is a summary of the risks that were identified during 2009. A detailed description of the identified risk and what was done to remediate the risk is contained in the following pages. Note that some of these risks are specific incidents and have been fixed. Others are indicators of a more systemic issue and are being addressed to reduce the larger impact.

Criticality: High
1. The Checkpoint Firewall service contract was allowed to lapse.
2. The implementation of the Checkpoint firewall is inefficient and leads to decreased incident response times and reduced resiliency capabilities.
3. Inadequate cross-team communication regarding the GroupWise backup implementation, leading to loss of backup data.
4. Data Center 1 (DC1) is currently at full capacity for power and cooling. Data Center 2 (DC2) cooling is not sized to power capacity. The uninterruptible power supplies (UPS) located in DC2 are not properly load balanced.
5. The current infrastructure of WolfWise Post Offices is inefficient and may lead to issues with customers’ mailboxes.

Criticality: Medium
6. The lack of established centralized communication processes may hinder the coordination of regular assessment and recovery activities.
7. Communication tools utilized during major incidents are not optimal.
8. Inability to easily map which services rely upon the Checkpoint Firewall greatly reduces the ability to adequately respond to outages of the firewall.
9. The Checkpoint firewall was running as a single node.
10. Insufficient procedures and technology in place to ensure Novell servers have adequate virus protection, leading to increased vulnerability during virus outbreaks.
11. Insufficient procedures and technology in place to ensure administrative Novell client machines have sufficient virus protection, leading to increased overall impact of virus outbreaks.
12. Technical procedures for IMAP migrations insufficiently established and documented.
13. Inconsistent entry of vital technical assets in asset management system may adversely affect strategic planning, asset maintenance, insurance and service contracts, and the security of assets.
14. Insufficient Data Center management procedures established and documented regarding cooling equipment maintenance.
15. Limited resiliency in the current NetBackup architecture. The virtual tape library is located in DC2 with no redundancy in DC1. The tape library in MCNC does not have a media server attached to it.
16. No formal password escrow system exists which result in system administrator IDs with shared passwords and administrator accounts with a limited knowledge of the password.

Criticality: Low
17. Crisis response work area in the data centers is needed.
18. If the halon fire suppression in DC1 were to be triggered, refill of the system will take approximately 3-4 business days. This would leave the affected area in DC1 unprotected for that length of time.
DETAILED RISK INFORMATION

The below detailed information is summarized as much as possible. Further details can be found in the actual source of information (e.g., incident reports, test results, assessments, reviews, etc.) which can be found in the OIT Risk Management system (via QuickBase).

CRITICALITY: HIGH

1. **RISK:** The Checkpoint Firewall contract was allowed to lapse.

   **AFFECTED OPERATIONAL GOAL AND STRATEGY:**
   Proactive Customer Service and Solutions -
   - Provide resources and opportunities to enable OIT staff to streamline customer service.
   - Be a technology leader and innovator, remaining current with software (versions and patches), hardware and best practices as appropriate.

   **RECOMMENDATION:**
   a. Renew the Checkpoint support contract as soon as possible. Move management of this contract to the Software License Management team.

   **ACTION TAKEN:**
   a. An additional year of support has been purchased. Management of the contract has been moved to the S&C Software License Management team.

2. **RISK:** The implementation of the Checkpoint Firewall is inefficient and leads to decreased incident response times and decreased organizational resiliency.

   **AFFECTED OPERATIONAL GOAL AND STRATEGY:**
   Reliable Systems and Security:
   - Use a sustainable funding model including lifecycle funding as part of the design of all services and new projects offered.
   - Consider training, security, compliance and resiliency in the design and implementation of projects.
   - Design systems that have redundant operations and appropriate service levels to meet customer requirements.

   **Innovation, Agility and Alignment:**
   - Identify, collect and share relevant data to measure the value, success and return on investment for OIT services.
   - Prioritize the use of resources (funding and personnel) to meet strategic goals and prioritized projects.
   - Research technology alternatives, including those in development, open source, purchasing and outsourcing options, to select appropriate models that provide high returns on investments and meet education and business goals.
   - Review existing solutions to leverage them, instead of duplicating technologies or services.
   - Clearly define services, have Service Level Agreements (SLAs) for all services and share cost information for all services.
RECOMMENDATIONS:

a. Raise priority for firewall re-architect / transition projects.
b. Transition the monitoring and management of the legacy administrative switches into the existing Communication Technologies framework.
c. Reconfigure the management server (Governator) and other critical nodes to remove network dependencies.
d. Acquire servers to act as new cluster nodes.
e. Configure legacy network devices to additionally log to the syslog server currently being implemented by Communication Technologies.
f. Move all network devices and data center hosts into a unified monitoring system.
g. Complete the migration of essential core resources onto up-to-date remotely manageable KVM.
h. Move DR off of desktop PC's onto more highly available virtual machines along with migrating the VPN from the deprecated checkpoint with local accounts to the campus ComTech managed VPN which uses campus authentication.
i. Relocate the secondary firewall (Franz) to DC2 or bring a third firewall (Arnold) online. Note: This recommendation may be redundant once the Firewall architecture is redesigned and implemented.

ACTIONS TAKEN:

a. The firewall transition/re-architecture project is on OIT’s priority project roadmap.
b. ComTech and ISO Provisioning (ISO Prov) have directed network logging to the ComTech log server for the legacy network hardware. About half of the legacy network terminal server equipment has been transitioned to the new ComTech ILO networks.
c. ISO Prov has reconfigured the management server (Governator) and other critical nodes to remove network dependencies. The new management station has been installed with minimal dependencies.
d. A new version of the Checkpoint firewall has been deployed with higher network bandwidth capacity and tested active failover.
e. A log management solution, Splunk, has been purchased. System logs, legacy switching, and other pertinent logs are currently being moved into Splunk.
f. Legacy data center switches are being included in the monitoring of servers and services as time permits.
g. An additional KVM has been purchased. Some existing servers will be virtualized; freeing up capacity while adding easier manageability.
h. Two suggestions are proposed to mitigate this risk:
   1) Train EAS staff who depend on the Checkpoint firewall to use the new Comtech ASA based VPN. The 192.168.15.x subnet would need to be added as a drop off point and DNS would need to be pointed to ns60,61.
   2) Reduce dependency on desktop pc’s which are attached to edge closet switches and UPS’s by making sure all technical staff have virtual machines running under data center standards that have any tools needed for remote maintenance and validation. This is currently being provided to staff on a limited basis.

   Login is via vpn.ncsu.edu. Some resources will need to be accessed via Administrative VMs or Virtual Machines for better security. DNS transition of Campus VPN is in discussion with Comtech. New, secure internal desktop VLAN still needs to be implemented to deal with multiple legacy VLANs and problems that exist implementing between legacy and new firewalls.
i. Spanned VLANS will not be removed for legacy firewalls. We will need to keep spanned VLANs until more modern network techniques can be deployed.
3. **RISK:** Inadequate cross-team communication regarding the GroupWise backup implementation, leading to loss of backup data.

**AFFECTED OPERATIONAL GOAL AND STRATEGY:**

**Reliable Systems and Security:**
- Consider training, security, compliance and resiliency in the design and implementation of projects
- Design systems that have redundant operations and appropriate service levels to meet customer requirements

**RECOMMENDATIONS:**
- Re-architect backup systems for PO01-10. Includes replacement of server ETSSGW9.
- Improve notifications and conduct backup/restoration “health” meetings
- Conduct backup/restoration exercises
- Implement backup server redundancy
- Document responsibilities and procedures

**ACTIONS TAKEN:**
- Replacement blade has been ordered for server ETSSGW9 as well as a redundant blade.
- Informal back-up health meetings have taken place.
- Backup/restoration tests/exercises will occur on a quarterly basis.
- Backups for much of this environment will be moving to NAS for more reliable backups.
- Responsibilities and procedures are being documented.

4. **RISK:** Data Center 1 (DC1) is currently at full capacity for power and cooling. Data Center 2 (DC2) cooling is not sized to power capacity. The uninterruptible power supplies (UPS) located in DC2 are not properly load balanced.

**AFFECTED OPERATIONAL GOAL AND STRATEGY:**

**Reliable Systems and Security:**
- Use a sustainable funding model including lifecycle funding as part of the design of all services and new projects offered
- Design systems that have redundant operations and appropriate service levels to meet customer requirements

**Innovation, Agility and Alignment:**
- Identify, collect and share relevant data to measure the value, success and return on investment for OIT services
- Prioritize the use of resources (funding and personnel) to meet strategic goals and prioritized projects

**RECOMMENDATION:**
- Complete retirement of legacy SAN and NAS devices to re-coup large power sources. Accelerate virtualization projects to include larger frame machines currently in production.

**ACTION TAKEN:**
a. Island of Improvement project in DC1 will yield uplifted space to consolidate and implement further virtualization and ‘tune’ infrastructure footprint under current capacity constraints. Retirement of Mainframe will free up additional power and cooling in DC1. Planned investment in a point cooling solution (cool blue doors) will raise cooling constraint in DC2.

5. **RISK:** The current infrastructure of WolfWise Post Offices is inefficient and may lead to issues with customers’ mailboxes.

**AFFECTED OPERATIONAL GOAL AND STRATEGY:**

**Reliable Systems and Security:**
- Use a sustainable funding model including lifecycle funding as part of the design of all services and new projects offered
- Consider training, security, compliance and resiliency in the design and implementation of projects
- Design systems that have redundant operations and appropriate service levels to meet customer requirements

**Innovation, Agility and Alignment:**
- Identify, collect and share relevant data to measure the value, success and return on investment for OIT services
- Prioritize the use of resources (funding and personnel) to meet strategic goals and prioritized projects
- Research technology alternatives, including those in development, open source, purchasing and outsourcing options, to select appropriate models that provide high returns on investments and meet education and business goals
- Review existing solutions to leverage them, instead of duplicating technologies or services
- Clearly define services, have Service Level Agreements (SLAs) for all services and share cost information for all services

**RECOMMENDATIONS:**

a. Migrate the current GroupWise post offices (1-10) to the new WolfWise infrastructure as soon as possible for more storage, easier maintenance and more efficiency.

b. Migrate the WolfWise post offices to GroupWise version 8 to be on Novell’s current release. This includes the upgrade of the new WolfWise servers to OES SP2 to stabilize connectivity with the storage infrastructure.

**ACTIONS TAKEN:**

a. The migration and enhancement process is underway with increase storage, upgraded servers and better infrastructure.

b. The project to migrate/enhance the current GroupWise environment and upgrade to version 8 is on the priority project road map. OES SP2 upgrades are planned and scheduled.

**CRITICALITY: MEDIUM**

6. **RISK:** The lack of established centralized communication processes may hinder the coordination of regular assessment and recovery activities.
AFFECTED OPERATIONAL GOAL AND STRATEGY:
Proactive Customer Service and Solutions -
- Develop a customer focused culture within OIT
- Provide services that meet or exceed agreed upon customer expectations
- Manage customer expectations with two-way communications
- Provide resources and opportunities to enable OIT staff to streamline customer service
- Ensure that OIT services can be accessed and are accessible by all customers on their own terms

RECOMMENDATION:
- Develop an OIT Incident Communications Plan (including a flowchart) that documents expectations and responsibilities for communication during a crisis or major incident, including timeliness, content and audience. This document should also describe management escalation procedures for use when on-call staff is unresponsive.

ACTION TAKEN:
- ORS in conjunction with TSS has developed a draft version of an OIT Incident Communications Plan Flowchart that has been reviewed by the OIT Leadership Team followed by OIT management staff and the CAB. ORS is currently developing the associated OIT Incident Communications Plan document (contains details of identified flowchart processes) for review by appropriate OIT staff.

7. RISK: Communications tools utilized during major incidents are not optimal.

AFFECTED OPERATIONAL GOAL AND STRATEGY:
Proactive Customer Service and Solutions -
- Provide services that meet or exceed agreed upon customer expectations
- Provide resources and opportunities to enable OIT staff to streamline customer service
- Create simplified paths to problem resolution including assignment of resolution paths

RECOMMENDATIONS:
- Establish a crisis communication channel that is easy to maintain during an incident. The oit_maintenance Jabber chat room is already available for this purpose, but a standing email list hosted by majordomo2 may also be of benefit and should be investigated.
- A section of SysNews, like Realm Status, should be established for major service announcements.

ACTIONS TAKEN:
- ORS will work with involved OIT units/teams to create a standing email list via the most effective mechanism.
- ORS will incorporate the use of SysNews features such as Realm Status into the Communications Plan.

8. RISK: Inability to easily map which services rely upon the Checkpoint Firewall greatly reduces the ability to adequately respond to outages of the firewall.

AFFECTED OPERATIONAL GOAL AND STRATEGY:
Proactive Customer Service and Solutions -
• Provide resources and opportunities to enable OIT staff to streamline customer service
• Provide one-stop shopping for services, support and service information

Reliable Systems and Security:
• Use and share effective project management processes to ensure the promised results
• Promote consistent, authoritative data sources/services to avoid duplication, misinterpretation and confusion.

RECOMMENDATION:
a. Raise the priority of service/process mapping project planned by Organizational Resilience Services. This project is currently on hold due to resource limitations. The information that service mapping can provide is important to both crisis and risk mitigation and is a crucial component of the Service Planning project jointly sponsored by Security & Compliance and Technical Support Services.

ACTION TAKEN:
a. The project for implementing a Configuration Management Database (CMDB) is now on the OIT Project Priority Map that lists the top 35 projects that will be completed in the next two years. The Service Planning project is a component of the CMDB in which the first phase produces templates for technical and customer service catalogs. Completing the Service Catalog portion is the foundation for developing the process mapping.

9. RISK: The Checkpoint firewall was running as a single node.

AFFECTED OPERATIONAL GOAL AND STRATEGY:
Reliable Systems and Security:
• Use a sustainable funding model including lifecycle funding as part of the design of all services and new projects offered
• Consider training, security, compliance and resiliency in the design and implementation of projects
• Design systems that have redundant operations and appropriate service levels to meet customer requirements

Innovation, Agility and Alignment:
• Identify, collect and share relevant data to measure the value, success and return on investment for OIT services
• Prioritize the use of resources (funding and personnel) to meet strategic goals and prioritized projects
• Research technology alternatives, including those in development, open source, purchasing and outsourcing options, to select appropriate models that provide high returns on investments and meet education and business goals
• Review existing solutions to leverage them, instead of duplicating technologies or services
• Clearly define services, have Service Level Agreements (SLAs) for all services and share cost information for all services

RECOMMENDATION:
a. Restore the Checkpoint firewall cluster.

ACTION TAKEN:
a. The Checkpoint firewall cluster was re-established to production service and the Windows
Checkpoint cluster was reconfigured to allow for dynamic failover.

10. **RISK:** Insufficient procedures and technology in place to ensure Novell servers have adequate virus
protection, leading to increased vulnerability during virus outbreaks.

**AFFECTED OPERATIONAL GOAL OR STRATEGY:**
Proactive Customer Service and Solutions –
- Be a technology leader and innovator, remaining current with software (versions and
patches), hardware and best practices as appropriate.

Reliable Systems and Security –
- Consider training, security, compliance and resiliency in the design and implementation of
projects.

**RECOMMENDATIONS:**

a. Upgrade the relevant servers to Trend OfficeScan as soon as possible.

b. Implement a monitoring system that contacts system administrators when antivirus software
falls out of revision or stops communicating with the antivirus administration server.

c. Draft an OIT standard/procedure requiring server administrators to keep security software,
including antivirus applications, up to date. When a new version should not be implemented,
require documentation justifying the decision. This documentation should be reviewed and
approved by senior OIT management.

d. The access rights of users and groups to application server volumes should be reviewed to
ensure that write permissions have not been granted to users who do not have a need for that
level of access.

e. SHS should draft a procedure requiring infected servers to be locked from client access until
determined to be cleared of infected files.

f. Server incident response procedures need to be drafted/updated to ensure that antivirus
software is immediately and thoroughly inspected when server files become infected.

g. The Security Incident Response procedure should require that any report of virus infected
server files be immediately reported to S&C.

**ACTIONS TAKEN:**

a. Servers fisapps1, fisapp2, and acsapps1 along with the remaining production and test
administrative Novell file/print servers were migrated to Trend Micro. The "ETSS Auth
Tree" production Edirectory Novell servers has been migrated to Trend Micro.

b. CNS staff have implemented several layers of testing/monitoring.

c. S&C has updated the University Anti-Virus Software Requirements Regulation
(http://www.ncsu.edu/policies/informationtechnology/REG08.00.10.php) and is facilitating
the review/approval process for the changes. The approval/publish date is dependent on the
PRR review process.

d. CNS and TSS staff will audit/review administrative Novell accounts that have "administrator-
equivalent" rights to determine if these rights are necessary and/or appropriate. S&C staff
will assist with the review. Roles should be identified and incorporated into SAR if feasible
so a periodic review of roles for OIT staff can occur.

e. S&C will investigate strategies to isolate user desktops. SHS will check the operational status
of antivirus software of a server which has been identified to hold infected user file(s).
f. S&C has reviewed the Anti-Virus Software Requirements Regulation to ensure it addresses the isolation of infected servers.
g. S&C now has a project to finalize the Security Incident Procedures which will include a review, approval and communication process. The incident investigation will attempt to determine how the infection began and how it can be remediated including use of anti-virus.

11. **RISK:** Insufficient procedures and technology in place to ensure administrative Novell client machines have sufficient virus protection, leading to increased overall impact of virus outbreaks.

**AFFECTED OPERATIONAL GOAL OR STRATEGY:**

Proactive Customer Service and Solutions –
- Be a technology leader and innovator, remaining current with software (versions and patches), hardware and best practices as appropriate.

Reliable Systems and Security –
- Consider training, security, compliance and resiliency in the design and implementation of projects.

**RECOMMENDATIONS:**

a. Update the OIT managed workstation procedures to ensure that client software is updated in a timely and effective manner.
b. Upgrade the OIT managed workstation client base to Trend OfficeScan as soon as possible.
c. Aggressively promote the adoption of Trend OfficeScan among the general university community.
d. Implement a quarantine VLAN into which infected machines can be placed while being cleared of virus infections.

**ACTIONS TAKEN:**

a. TSS will evaluate existing tools for assessing currency of workstation antivirus software and signatures and will update the OIT-managed desktop procedures to ensure currency of antivirus software and signatures to the extent possible with those tools. TSS will also work to develop a broader set of guidelines for OIT workstations that defines the use of managed vs. unmanaged workstations and the systems maintenance expectations for staff using unmanaged workstations.
b. The development of new desktop environments by OIT will consider user roles and the need for administrative access to the workstation. In cases where there is a need for full administrative workstation access, expectations for system administration and maintenance will be communicated to the workstation user. Workstation management tools being evaluated for future use should include the capability for maintenance and reporting of antivirus software and signatures.
c. As project manager of the Trend OfficeScan implementation, S&C staff worked with TSS and the campus community to ensure the product was implemented (with automatic updates as a default) by the established deadline. The Anti-Virus Software Requirements regulation will be updated to reflect the need for automatic updates of anti-virus software and signature files.
d. A specific quarantine Vlan has not yet been configured as an MPLS implementation would be required to make this action realistic. Currently, bad machines have their port turned off by S&C.
12. **RISK:** Technical procedures for IMAP migrations insufficiently established and documented.

**AFFECTED OPERATIONAL GOAL AND STRATEGY:**

**Pervasive Transparency**—
- Expand and enhance communication efforts to keep customers, staff and other stakeholders informed

**Proactive Customer Service and Solutions**—
- Provide services that meet or exceed agreed upon customer expectations
- Create simplified paths to problem resolution including assignment of resolution paths.

**Reliable Systems and Security**—
- Use and share effective project management processes to ensure the promised results
- Consider training, security, compliance and resiliency in the design and implementation of projects
- Design systems that have redundant operations and appropriate service levels to meet customer requirements.

**RECOMMENDATIONS:**

a. Cyrus IMAP email service administration should be performed by the ISO Systems and Hosted Services team.

b. The Email Advisory Board should be formally chartered to ensure that its role as a vetting body is clear to all participants.

c. Communication Technology should become a full participant in the OIT Change Management program.

d. Establish OIT Standards for acceptable data loss due to IMAP mail migrations.

e. A Cyrus server migration document should be created that lists the steps, both technical and non-technical, which must be followed to ensure successful completion of server migration projects. Establish OIT Technical procedures and sufficiently document.

**ACTIONS TAKEN:**

a. The responsibility for administration of the Cyrus IMAP email service has been reassigned to the ISO Systems and Hosted Services team.

b. A governance structure for Email services has been implemented.

c. ComTech has merged their independent Change Management process into the OIT Change Management program.

d. The time frame in which the pre-migration of data to the full account migration will be reduced and communicated to the user.

e. For future moves, a checklist has been created to ensure all configuration files are transferred and nothing overlooked.

13. **RISK:** Inconsistent entry of vital technical assets may adversely affect strategic planning, asset maintenance, insurance and service contracts, and the security of assets.

**AFFECTED OPERATIONAL GOAL AND STRATEGY:**

**Proactive Customer Service and Solutions:**
- Provide resources and opportunities to enable OIT staff to streamline customer service.
• Be a technology leader and innovator, remaining current with software (versions and patches), hardware and best practices as appropriate.

**Reliable Systems and Security:**
• Promote consistent, authoritative data sources/services to avoid duplication, misinterpretation and confusion.

**RECOMMENDATIONS:**
a. Management should include asset management training in the orientation of new technical staff. Staff should be required to utilize the asset management system.
b. An assessment of the various OIT asset management databases should be performed to see if consolidation can increase efficiency and integration to other system components.

**ACTIONS TAKEN:**
a. ISO Datacenter staff is taking the lead with periodic audits of datacenter resources to ensure asset management source is up to date. The audits are ongoing in perpetuity. The implementation of a new process for datacenter operations adding assets as they arrive is ongoing. There is an ongoing effort for ISO PROV to work with Datacenter Operations to establish a surplus (asset removal) standard.
b. ComTech has hired a consultant to assess their asset/inventory requirements with a cursory look at other asset databases being used within OIT. The recommendation for ComTech should be assessed to see if it can meet the consolidated OIT asset management needs.

14. **RISK:** Insufficient Data Center management procedures established and documented regarding cooling equipment maintenance.

**AFFECCTED OPERATIONAL GOAL AND STRATEGY:**
Proactive Customer Service and Solutions —
• Be a technology leader and innovator, remaining current with software (versions and patches), hardware and best practices as appropriate.

Reliable Systems and Security—
• Promote consistent, authoritative data sources/services to avoid duplication, misinterpretation and confusion.

**RECOMMENDATION:**
a. Create/modify data center management procedures to ensure that air conditioning units are not disabled without appropriate heat mitigation strategies in place.

**ACTION TAKEN:**
a. Data center management procedures have been modified as recommended.

15. **RISK:** Limited resiliency in the current NetBackup architecture. The tape library in MCNC does not have a media server attached to it currently; if it became necessary to restore data from this tape library (for instance in the event that the VTL became unavailable in DC2 due to a disaster), additional time and effort would be required to implement this capability (estimated to be 1 week).
AFFECTED OPERATIONAL GOAL AND STRATEGY:
Proactive Customer Service and Solutions —
   ● Be a technology leader and innovator, remaining current with software (versions and patches), hardware and best practices as appropriate.
Reliable Systems and Security —
   ● Promote consistent, authoritative data sources/services to avoid duplication, misinterpretation and confusion.

RECOMMENDATIONS:
   a. Investigate possible solutions that would result in a reduction of the delay in restore capability if DC2 became unavailable due to a disaster.

ACTIONS TAKEN:
   a. ISO-PROV is considering the option of placing a media server at MCNC.

16. RISK: No formal password escrow system exists which result in system administrator IDs with shared passwords and administrator accounts with a limited knowledge of the password.

AFFECTED OPERATIONAL GOAL AND STRATEGY:
Reliable Systems and Security —
   ● Promote consistent, authoritative data sources/services to avoid duplication, misinterpretation and confusion.

RECOMMENDATION:
   a. Investigate and implement a privileged account management system to facilitate the use of shared passwords and have needed passwords available for emergency situations.

ACTION TAKEN:
   a. A project to implement a privileged account management system has been added to the OIT project list. Due to other priorities this project is not yet on the OIT priority project roadmap.

CRITICALITY: LOW

17. RISK: Crisis response work area in the data centers is needed.

AFFECTED OPERATIONAL GOAL AND STRATEGY:
Proactive Customer Service and Solutions —
   ● Provide resources and opportunities to enable OIT staff to streamline customer service.

RECOMMENDATION:
   a. Provide tables and chairs in or near each data center for use during incident response situations.

ACTION TAKEN:
   a. Tables and chairs will be provided as needed during incident response situations.
18. **RISK:** Due to a U.S. manufacturing ban of Halon 1341, the Halon in the Halon fire suppression system in DC1 may not be able to be replaced. Over a period of time, the removal of the current Halon system and the installation of a new fire suppression system may be required.

**AFFECTED OPERATIONAL GOAL AND STRATEGY:**

**Reliable Systems and Security:**
- Use a sustainable funding model including lifecycle funding as part of the design of all services and new projects offered.
- Design systems that have redundant operations and appropriate service levels to meet customer requirements.

**RECOMMENDATION:**
- Accept the risk due to the cost of installing a new fire suppression system and the likelihood of a halon dump occurrence. Investigate a replacement for the fire suppression system when DC1 renovation options become available.

**ACTION TAKEN:**
- The risk is accepted. Due to a fire alarm and suppression system activation in March 2010, we have become aware that our existing Halon systems can be recharged. It takes 5 – 7 business days to recharge which causes the affected area to be unprotected during that time. This risk is also accepted due to the likelihood of an occurrence that will activate the Halon suppression system during that time and the cost of a replacement system.