

**Citrixexperience.com**

**1Y0-613 Citrix Access Suite 4.0: Analysis**

**Study Guide**

**Version 1.0**

(November 14, 2006)

## Citrix® Access Suite 4.0: Analysis Study Guide

---

This study guide has been created by Citrixexperience.com. The materials used for creation of this study guide, besides personal field experience, are the 1Y0-613 Exam Enablement Guide and Citrix® courseware CTX-6113AI Citrix® Access Suite 4.0: Analysis, both of which are copyrights of Citrix® Systems.

Along with the items listed above, this study guide is meant to be used in preparation for the 1Y0-613 Citrix® Access Suite 4.0: Analysis exam. Also suggested for preparation are the Citrixexperience.com 1Y0-613 online and offline practice exam simulations, and the offline printable PDF practice exam found at [www.Citrixexperience.com](http://www.Citrixexperience.com), other books that relate to the subjects, and above all, personal experience with the products.

The license for this study guide is for one user only. It is a copyright of Citrixexperience.com and may not be reprinted, copied, reproduced, distributed, republished, downloaded, displayed, posted or transmitted in any form or by any means, including but not limited to electronic, mechanical, photocopying, recording, or other means, in full or in part, without the prior express written permission of Citrixexperience.com.

Citrix, the Citrix logo, Citrix ICA, Citrix MetaFrame, Citrix MetaFrame XP, Citrix Nfuse, Citrix Extranet, Citrix Program Neighborhood, Citrix WinFrame, and other Citrix product names referenced herein are registered trademarks or trademarks of Citrix Systems, Inc. in the United States and other jurisdictions. All other product names, company names, marks, logos, and symbols are trademarks of their respective owners.

Citrix® Systems, Inc. is not affiliated with Citrixexperience.com in any way.

## Table of Contents

---

<b><u>Subject</u></b>	<b><u>Page</u></b>
Pre-Engagement Activities	1
Business, Technical and End-User Analysis	5
Access and Personalization	6
Presentation Services and Application Deployment	11
Security and Identity Management	20
Collaboration and IT Infrastructure	26
Operational Procedures	32

## **Pre-Engagement Activities**

---

### **Citrix Consulting Methodology phases**

The Citrix Consulting Methodology consists of:

- ❖ *Analysis*
- ❖ *Design*
- ❖ *Build and Test*
- ❖ *Rollout*

### **Analysis phase**

During the analysis phase of the Citrix Consulting Methodology, the architect evaluates an organization's goals and how the current IT environment supports these goals. This review allows the architect to gauge the readiness of the organization by identifying and categorizing strengths and risk factors in the environment.

The objectives of the analysis phase of the Citrix Consulting Methodology consist of: Understanding the current environment, assessing the readiness of an environment, providing recommendations and providing information resources.

### **Documents provided to the organization during the analysis phase**

The following documents are deliverables that can be provided to the organization during the analysis phase of the Citrix Consulting Methodology:

- ❖ *Access Strategy Executive Summary*
  - ◆ Targeted at stakeholders and project sponsors.
  - ◆ It defines the key findings and identifies opportunities for improvement.
  - ◆ It includes the following sections:
    - Project Overview, which includes information about the project focus and deliverables.
    - Project Conclusions, which includes key requirements and key findings.
    - Assessment Grid, which lists each of the access infrastructure components that are reviewed as part of the process of developing an Access Strategy.
    - Contacts and Resources, which identifies the project stakeholders and project team members.
- ❖ *Access Strategy Assessment Document*
  - ◆ States the project requirements, risks and recommendations resulting from an assessment.
  - ◆ Provides a component overview and requirements, identified strengths and risks, impacted user community and associated recommendations.

❖ *Access Strategy Assessment Plan*

- ◆ A detailed project plan that identifies the tasks and milestones required to implement an access strategy for the organization.
- ◆ Includes all phases of the Citrix Consulting Methodology.

**Analysis phase time frame**

The suggested analysis phase time frame for an Access Strategy Assessment for Citrix Access Suite is 160 work hours.

The suggested analysis phase time frame for an Access Strategy Assessment for Citrix Presentation Server only is 80 work hours.

The suggested analysis phase time frame for an Access Strategy Plan is 80 work hours.

- ❖ Very large or complex environments might require additional time.

**Analysis phase checkpoints**

The Citrix Consulting Methodology places logical checkpoints between each of the various phases. Checkpoints are designed to allow the team to confirm that the project is on track and to present detailed plans for the next phase of the project. During scheduled project checkpoints, the team should confirm current project objectives, confirm project timelines, review current project issues and reset expectations if necessary.

Consider the following guidelines when performing a checkpoint at the end of each phase:

- ❖ Conduct an overview or presentation at the end of each phase and include the executive sponsor and related project stakeholders.
- ❖ Verify that all risks can be addressed.
- ❖ Verify that all requirements are met prior to moving to the next phase, including resources and staff.
- ❖ Ensure buy-in regarding accomplished activities and completed tasks.

**Documents for the project team during the analysis phase**

❖ *Statement of Work (SOW)*

- ◆ Documents the assumption and success criteria for the engagement.
- ◆ Sets clear expectations for the work to be performed along with the components that are within the scope for the proposed project.
- ◆ Once agreed upon and signed by the organization, the SOW becomes the basis for all project negotiations thereafter.
- ◆ The SOW should include the following sections:
  - Project Overview, which contains a company brief, goal, vision and objective and states what the project team will accomplish working with the organization

as a trusted advisor.

- Project Scope and Approach, which defines the key segments of the Citrix Consulting Methodology and identifies which segments are in scope.
  - Project Deliverables, which contains detailed information related to the work that the project team will perform during the engagement.
  - Billing Estimates and Expenses, which contains added assumptions required to clearly establish and control project scope.
    - This is critical for the Access Strategy Assessment.
  - Customer Billing Information, which provides organizational billing information.
  - Other Considerations, which provides considerations such as copyright and liability statements.
  - Engagement Agreement, which contains organization and project team signatures.
- ❖ Access Strategy Assessment
- ◆ Contains the following sections (in order):
    - Project Overview
    - Architecture Overview
    - Business Process and Procedures
    - User Communities
    - Access and Personalization
    - Presentation Services and Application Deployment
    - Security and Identity Management
    - Collaboration
    - IT Infrastructure
    - Operational Procedures
- ❖ Status report
- ◆ Includes useful information, such as overview of accomplishments, status of all project deliverables, critical issues, list of significant tasks completed, steps and actions to concentrate on and totals by task of budgeted time versus actual time and the variance of engagements that are longer than two weeks.
  - ◆ Deliver status reports on a weekly basis.
- ❖ Risk memo
- ◆ Identifies any potential risks or issues that can jeopardize the project plan or the project as a whole.

- ◆ When preparing a risk memo, the project team member should assess and categorize the issue as a risk and document it by providing the following information:
  - Overview, which states the potential risk or issue at a high level.
  - Risk assessment, which describes the potential risk or issue in detail.
  - Impact analysis, which includes how the potential risk or issue will impact the organization.
  - Recommendation, which suggests possible work-arounds or decision points.

### **Risk Memo**

A risk memo should be created when a significant obstacle prevents moving to the next phase of the Citrix Consulting Methodology.

The risk memo can be distributed to the sponsor, stakeholder and related functional groups as required to inform them of the risk and related consequences, and enact some plan to resolve them.

### **Project team members**

It is important that the project team staffed for the project be technically astute in the required areas of focus for the project.

Project team members should have the following knowledge requirements:

- ❖ Be technically astute in predefined areas of the project.
- ❖ Be perceived as an expert by the organization.
- ❖ Research background information as it relates to the planned project.
- ❖ Be aware of the Citrix Global Alliance Partners Program.

### **Project manager's initial tasks**

Prior to the first business and technical meeting, the project manager should address the following tasks as part of organizing and preparing for a successful engagement:

- ❖ Review the SOW document.
- ❖ Contact the project team and set expectations.
- ❖ Create a project plan and task list.
- ❖ Designate a central repository for documents.

## **Business, Technical and End-User Analysis**

---

### **Project kick-off meeting**

The process for the project kick-off meeting goes as such:

- ❖ Complete pre-engagement activities.
- ❖ Make the first call to the identified contact within the organization.
- ❖ Create and submit a meeting agenda.
- ❖ Review the Statement of Work.
- ❖ Conduct the kick-off meeting which includes taking meeting minutes.
- ❖ Gathering business environment information from the attendees and gathering technical information from the attendees.
- ❖ Provide the organization with meeting minutes and a finalized agenda for the project engagement.

The following business topics should be addressed in the project kick-off meeting:

- ❖ Business drivers
- ❖ Project milestones
- ❖ Political issues
- ❖ Audit guidelines
- ❖ Decision points
- ❖ Key decision owners
- ❖ Personnel and project budget

During the project kick-off meeting, the technical environment should be addressed by creating a high-level architectural diagram.

- ❖ A discussion and diagram should address the current state of the environment, current issues, goals and the desired environment.

### **End-user communities**

When gathering information and requirements for end-user communities, the following topics should be discussed:

- ❖ Current user communities
- ❖ Future user communities
- ❖ User resource requirements
- ❖ Application requirements

- ❖ Access requirements
- ❖ Primary user devices
- ❖ Collaboration requirements
- ❖ Challenges and user satisfaction

## **Access and Personalization**

---

### **Internal connectivity**

Users in the office access resources using the LAN.

LAN connections typically allow for ample bandwidth and few constraints for internal user connectivity.

When analyzing access over a wireless LAN, the architect should gather information related to security, latency and connectivity.

A VPN solution can also be used to secure a wireless connection.

### **Remote connectivity**

WAN performance directly impacts the ability of external users to access resources and perform their job in an efficient manner.

When gathering facts about the WAN, look at how it is managed to ensure that enough bandwidth is available.

VPNs are widely used to provide remote users access to internal resources through the internet.

Commonly deployed VPNs include IPSEC and SSL VPNs such as Secure Gateway and Access Gateway.

When assessing the use of VPNs, an architect should keep in mind that some external users might not be employees of the organization and require access to only specific resources. As such, access to resources should be provided only as needed.

### **Quality of Service**

*Quality of Service (QoS)* refers to a method for prioritizing network traffic.

QoS might be useful to ensure that sufficient bandwidth is available for higher priority real-time applications.

If network traffic is prioritized for one application, it might cause degradation for other applications.

QoS implementations can be quite political because of the negative network and application impact that others in the organization may experience.

### **Assessing user access to resources**

Address the following areas when assessing how users access resources:

- ❖ Accessibility
  - ◆ Clear, accessible and concise information
- ❖ Remote PC access
- ❖ Portal or consolidated presentation
  - ◆ Access from one or multiple points
- ❖ User or group access
- ❖ Resources
  - ◆ Content to present and make available
- ❖ Security

### **Assessing client devices and software**

When gathering information related to client devices, the architect should ask:

- ❖ What type of client devices have been deployed throughout the environment?
- ❖ Are non-corporate devices such as a home PC or kiosk allowed to connect to internal resources?

### **Assessing Citrix Client software**

When assessing the Citrix Client software, an administrator should gather information for:

- ❖ Client deployment
- ❖ Client type
- ❖ Updates
- ❖ Permissions
- ❖ Configurations

### **32-bit Windows client devices risks and recommendations**

Potential risks for 32-bit Windows client devices are:

- ❖ Multiple operating systems
- ❖ Installing Client software might require elevated privileges.
- ❖ Remote Desktop Client is built-in and users might try to access the server farm with it.

- ❖ Windows 9x is no longer supported by Microsoft.

Recommendations to mitigate these risks are:

- ❖ Create a standardized operating environment.
- ❖ Design a Client deployment strategy.
- ❖ Use the Java version of the Client, if available.
- ❖ Add support for the Remote Desktop Client and advise users that all features might not be available to them.
- ❖ Restrict the Remote Desktop protocol to only administrators on Presentation Server.
- ❖ Investigate a migration to a supported version of 32-bit Windows operating system.

### **Pocket PC and WinCE devices risk and recommendation**

The potential risk for Pocket PC/WinCE client devices is that these specialized devices might not be the best solution for every purpose because of their small form-factor.

Recommended to mitigate this risk is that the environment should be set up to detect these devices and deliver access to the appropriate resources.

### **Macintosh client devices risks and recommendations**

The potential risks for Macintosh client devices are:

- ❖ They are in use by only a small percentage of the population.
- ❖ The user must initiate Client installs or upgrades.

Recommendations to mitigate these risks are:

- ❖ Design a different deployment strategy.
- ❖ Ensure that the help desk can adequately support users.
- ❖ Use the Java version of the Client, if available.

### **Thin client devices risk and recommendation**

The potential risk when using thin client devices is that the firmware may be out of date.

Recommended to mitigate this risk is check the vendor web site regularly for firmware updates.

### **Unix and Linux client devices risks and recommendations**

The potential risks for Unix and Linux client devices are:

- ❖ They are in use by only a small percentage of the population.

- ❖ The user must initiate Client installs or upgrades.

Recommendations to mitigate these risks are:

- ❖ Design a different deployment strategy.
- ❖ Ensure that the help desk can adequately support users.
- ❖ Use the Java version of the Client, if available.

### **Web browser risks and recommendations**

The potential risks when using browsers in a Presentation Server environment are:

- ❖ Not using encryption.
- ❖ Using multiple browsers can result in inconsistent access between devices.
- ❖ Strict security settings might result in launch failure.

Recommendations to mitigate these risks are:

- ❖ Ensure that encryption standards can be met by all supported client devices.
- ❖ Standardize on a supported browser that meets the business requirements.
- ❖ Ensure browser settings do not block Java applets.

### **Peripherals attached to client devices risks and recommendations**

The potential risks related to peripherals attached to client devices in a Presentation Server environment are:

- ❖ Mapping too many print devices can cause degradation to the user experience.
- ❖ Synchronizing PDAs will have an impact on network utilization.
- ❖ Using TWAIN devices will have an impact on network utilization.
- ❖ Using microphones will have an impact on network utilization.

Recommendations to mitigate these risks are:

- ❖ Optimize the printing solution to give users only what they need.
- ❖ Use PDA synchronization, TWAIN devices and microphones only when necessary.

### **Client for Web risk and recommendation**

The potential risk for the Client for Web is that the correct Client for Web might not be installed.

- ❖ There are two varieties of Client for Web: Full Client (ICA32T.EXE) and Minimal Client (WFICAC.CAB).

It is recommended that the administrator determine the smallest Client download that is required and to understand the functionality of the two Clients for Web.

### **Program Neighborhood Agent risk and recommendation**

The potential risk for the Program Neighborhood Agent is that not all device types support it, so if users access from multiple devices, access will be inconsistent.

It is recommended that the administrator ensure that the appropriate Client is deployed to the client devices.

### **Program Neighborhood risk and recommendation**

The potential risk for Program Neighborhood is that there is administration overhead, as configuration is required on each device.

It is recommended that the administrator consider using another Client type with the ability to centrally manage.

### **Java Client risk and recommendation**

The potential risk for the Java Client is that it can be blocked by a firewall or browser.

It is recommended that the administrator ensure that Java applets are not blocked.

### **Password Manager agent risks and recommendations**

Potential risks for the Password Manager agent are:

- ❖ Users can change configurations.
- ❖ Non-published applications will not be recognized if there is no local agent installed.

It is recommended that:

- ❖ The administrator pre-configures the settings.
- ❖ The administrator verifies installation of the Password Manager agent on all local workstations.

### **Access Gateway Advanced Edition and VPN Clients risks and recommendations**

Potential risks related to Access Gateway Advanced Edition and VPN Clients are:

- ❖ Users might not know how to access the resources in the access server farm.
- ❖ Users might not have sufficient rights to download and install Clients.

It is recommended:

- ❖ The administrators provide appropriate training with clear instructions to learn how to access the resources in the access server farm.

- ❖ To be able to download and install the Clients, certain users may be granted administrative or power user rights or allow users to access resources in the server farm using browser-only access.

### **Citrix Access Client Packager risks and recommendations**

Potential risks related to the Citrix Access Client Packager are:

- ❖ Multiple client software deployments create confusion for the administrators and the users.
- ❖ Client configurations create administrative overhead.

Recommended to resolve these issues are:

- ❖ Use the Citrix Access Client Packager to simplify and streamline Client deployment.
- ❖ Use the Citrix Access Client Packager to pre-configure the Clients into a single package for deployment.

### **Web Interface risks and recommendations**

Potential risks related to Web Interface are:

- ❖ The user may not be able to customize it.
- ❖ The user may not understand the options available for customizing it.

Recommendations to alleviate these risks are:

- ❖ Assess the needs of the organization and grant personalization permissions as appropriate.
- ❖ Provide user training and reference manuals.

### **Aspects of personalization**

The two aspects of personalization are administrator and user.

- ❖ The architect must assess how the administrator personalizes and customizes the user interface.
- ❖ Users see the Web Interface site the way the administrator personalizes or configures it in Web Interface.
- ❖ Users can only take advantage of the features that the administrator grants them permissions to.

## **Presentation Services and Application Deployment**

---

### **Assessing Presentation Services**

When assessing Presentation Services, the architect should address:

The most trusted site on the web for Citrix certification preparation products, Citrixexperience.com

- ❖ Server configuration
- ❖ Core components
- ❖ Optional components
- ❖ Farm configuration
- ❖ Print management

### **Assessing server configuration**

When assessing server configuration, the architect should consider:

- ❖ Server build type
- ❖ Windows Server platform
- ❖ Directory service
- ❖ Product platform
- ❖ Service packs and hotfixes

### **Manual server build risk and recommendation**

A potential risk in the server build process is manual server builds increases the likelihood of inconsistencies in server configuration, makes testing more difficult and increases subsequent administration complexity.

The recommendation to mitigate this issue is to create an automated build process so that all deployments are consistent.

### **Inconsistent server build risk and recommendation**

A potential risk with inconsistent server builds is that it causes user experience to vary across locations, applications and user groups.

The recommendation to mitigate this issue is to standardize server builds to use the same operating system and configuration.

### **Multiple versions/platforms risk and recommendation**

A potential risk with multiple versions and/or platforms is it makes administration more complex.

The recommendation to mitigate this issue is to standardize on a version and platform.

### **Inconsistently applying service packs and hotfixes risks and recommendation**

Potential risks with inconsistently applying service packs and hotfixes is that it makes troubleshooting more complex and creates varying user experiences.

The recommendation to mitigate these issues is to standardize the rollout of service packs and hotfixes.

### **Presentation Server core components**

The core components of Presentation Server, which form the backbone common to all implementations, are:

- ❖ The data store
- ❖ Server farms
- ❖ The license server
- ❖ Zones

### **Multiple farms risks and recommendations**

With multiple farms the organization cannot take advantage of load balancing and it brings an increase in administrative complexity.

Recommendations for these issues include consolidating farms where possible and leveraging the Access Suite Console to help centralize administration of multiple farms.

### **Multiple administrators risks and recommendations**

Having too many administrators for a server farm might result in inconsistent configurations and conflicting settings, and also create a security risk.

Recommendations to mitigate these issues are to limit the number of administrators and ensure that they are adequately trained, and to curtail individual administrator rights.

### **Single data center and multiple data center risks and recommendations**

A single data center does not offer failover or business continuity in the event of an outage or disaster, while too many data centers can be difficult to administer.

Recommendations to mitigate these issues are to consolidate data centers if too many exist and to consider having more than one data center to help ensure business continuity in the event of a failover.

### **Microsoft Access or MSDE data store risk and recommendation**

A data store based on Microsoft Access or MSDE might not scale for future growth.

To mitigate this problem, implement a data store using IBM DB2, Oracle or Microsoft SQL Server.

### **Organizations lacking in-house database expertise risk and recommendations**

An organization might lack the in-house expertise to implement and maintain an enterprise class database server.

Recommendations for this issue include implementing a Microsoft Access or MSDE data store for small farms if there is no existing database administrator and review the feasibility of hiring a database administrator to monitor and maintain an enterprise class database server. Doing so might allow the organization to consolidate other database functions.

### **Geographically distributed farm in multiple data centers risk and recommendation**

A geographically distributed farm with servers in multiple data centers connected through slow WAN links might experience network and server congestion.

Consider replicating the data store database to another data center to reduce the traffic over WAN links.

### **Database corruption risk and recommendations**

If the data store database becomes corrupt or lost, then the farm must be rebuilt.

To prevent this, back up the data store database on a regular schedule and prepare a plan to restore the database in the event of a failure. Also, consider the possibility of clustering the data store database server if the in-house expertise and hardware are available.

### **Multiple zones risk and recommendation**

Too many zones can negatively impact performance.

Reduce network traffic by consolidating zones.

### **Data collector failure risk and recommendations**

A failure of the data collector of a given zone might result in a situation where it is unclear which member server will assume the role of data collector.

To prevent this, plan a clear election hierarchy in each zone by designating one or more servers as Preferred and designate special servers hosting any mission-critical or resource-intensive applications as Not Preferred.

### **Data collector performance risks and recommendation**

Network congestion, server hardware, application demands, user demands or other limitations might reduce data collector performance in medium or large zones.

Consider dedicating the data collector for each zone by restricting it from serving applications.

### **User redirection risk and recommendations**

Users might be redirected to servers across WAN links unnecessarily.

To prevent this, ensure that zone preference and failover is configured to optimize user connections and ensure zones are defined geographically as appropriate.

### **License tracking risks and recommendations**

Previous product versions might have used different licensing schemes, making license tracking difficult when multiple products or product versions are involved.

To avoid this issue, implement the latest product with improved license monitoring, tracking and administration and consolidate license servers where necessary.

### **Presentation Server optional components**

Optional components of Presentation Server include Resource Manager and Network Manager. These tools allow organizations to maintain and monitor their implementation.

### **Resource Manager default metrics**

If the default metrics in Resource Manager don't meet an organization's need, they should review the metric options as customize as appropriate.

### **Resource Manager historical data**

To capture historical data in Resource Manager, configure the summary database to view archived data in reports.

### **Resource Manager reports**

To make the Resource Manager reports most effective for the organization, customize the reports to provide clear and useful data.

### **Network Manager and SNMP**

If an organization is capturing SNMP data and desires to monitor it, Network Manager or a different SNMP monitoring tool should be deployed.

### **Server farm configuration topics**

When gathering information related to server farm configuration, an architect should consider the following topics:

- ❖ Farm and server properties
- ❖ Load manager
- ❖ Presentation Server policies

- ❖ Redundancy
- ❖ Maintenance procedures

### **SpeedScreen risk and recommendation**

Not using SpeedScreen might create a negative user experience when viewing certain graphical content.

Solution: Revise SpeedScreen settings for the environment.

### **Default load evaluator risk and recommendation**

The Default load evaluator or an improperly configured load evaluator might affect application performance and underutilize server resources, resulting in unnecessary hardware purchases.

Solution: Review the load evaluators and create a custom load evaluator for the specific environment and applications, if necessary.

### **Incorrect policy priority risks and recommendation**

Incorrect policy priority might negate intended functionality or otherwise produce unintended results.

Solution: Determine effective policies, accounting for priority, and compare with intended results.

### **Redundancy risk and recommendation**

The lack of redundancy for mission-critical resources can cause serious delays should an issue arise.

Solution: Identify single points of failure in the environment and develop redundancy and failover measures.

### **Monitoring strategy risk and recommendation**

Improper or no monitoring strategy can create an environment that is reactive to problems rather than proactive to changes.

Solution: Identify gaps in maintenance and monitoring procedures and develop an appropriate strategy.

### **Unreliable network risk and recommendation**

Dropped connections from unreliable networks can cause users to lose productivity.

Solution: Implement session reliability as appropriate.

### **Print management topics**

When assessing print management, an architect should address the topics:

- ❖ Printer policies
- ❖ Network printer assignment
- ❖ Printer creation
- ❖ Printer drivers

### **Printer creation topics**

When gathering information about printer creation in the organization, the architect should discuss the following topics:

- ❖ Auto-creation settings
- ❖ Imported print servers
- ❖ Session printers

### **Printer policy topic**

When gathering information about printer policies in the organization, the architect should ask "Is a printer bandwidth policy in effect?"

### **Printer driver topics**

When gathering information about printer drivers in the organization, the architect should discuss the following topics:

- ❖ Printer driver replication method
- ❖ Driver mappings
- ❖ Auto-install of native drivers
- ❖ Universal printer driver

### **Network printer assignment topics**

When gathering information about network printer assignment in the organization, the architect should discuss the following topics:

- ❖ Active Directory
- ❖ Logon scripts
- ❖ Third party tools

### **Printer management risks and recommendations**

Potential risks and recommendations associated with printer management in a Presentation Server environment are:

- ❖ Unrestricted bandwidth might allow printing to monopolize dedicated WAN links.
  - ◆ Solution: Limit printer bandwidth using policies.
- ❖ Native drivers auto-installed (default setting) might cause too many drivers to be installed on servers.
  - ◆ Solutions: Configure a policy to disallow auto-install and implement the universal printer driver.
- ❖ The client software might not include the new universal printer driver.
  - ◆ Solution: Review client versions and upgrade if necessary.
- ❖ Users see too many printers and are confused and don't know which printer to use.
  - ◆ Solutions: Configure printing to auto-create only the default printer and reduce printers using the session printers policy.
- ❖ Users cannot access network printers.
  - ◆ Solution: Create a session printers policy.

### **Application configuration topics**

An architect should focus on application configuration topics, such as:

- ❖ Published application properties
- ❖ Helper applications
- ❖ Load-managed groups
- ❖ Application isolation

### **Application display settings risk and recommendation**

If display settings for all published applications are not identical, then session sharing cannot be used.

Solution: Align display settings to enable use of session sharing.

### **Application color depth risk and recommendation**

If color depth for published applications is not at least 16 bit, then SpeedScreen Browser Acceleration will not work.

Solution: Set color depth for all applications to 16 bit or higher.

### **Application conflicts risk and recommendation**

Some applications installed on the same server causes application confliction.

Solution: Use application isolation environments.

### **Application seamless windows risk and recommendation**

Some settings prevent the use of seamless windows.

Solution: Confirm and align Web Interface or Program Neighborhood settings to enable seamless windows.

### **Permissions risk and recommendation**

Permissions may restrict access to needed applications.

Solution: Relax NTFS permissions.

### **Application deployment method topics**

When gathering information related to application deployment methods, an architect should focus on:

- ❖ Application packaging and deployment tools
- ❖ Test environment
- ❖ Deployment process
- ❖ Application teams

### **Application deployment method risk and recommendation**

The lack of a standardized application deployment method creates dissimilar server and application configurations.

Use Installation Manager to standardize application rollout.

### **Application packaging tool risk and recommendation**

The lack of an application packaging tool might result in problems deploying applications.

Use Installation Manager to standardize application packaging.

### **Untested applications risk and recommendations**

Untested applications can introduce problems to the production environment.

Ensure that applications are tested before deploying them into the production environment and ensure that the test environment mirrors the production environment.

### **Application deployment process risk and recommendation**

Not following a proven application deployment process might result in inconsistencies and unanticipated difficulties.

Document and enforce a uniform application deployment process.

## **Security and Identity Management**

---

### **Authentication topics**

When gathering information related to authentication, an architect should consider:

- ❖ Type of directory service
  - ◆ Active Directory
  - ◆ Novell
  - ◆ Other
- ❖ Password policies
  - ◆ Password length
  - ◆ Varying characters
  - ◆ Password expiration intervals
  - ◆ Other
- ❖ Additional authentication products
  - ◆ Secure token
    - RSA SecurID
    - Secure Computing SafeWord
  - ◆ Biometric devices
    - Fingerprint
  - ◆ Smart cards
  - ◆ Other
- ❖ Anonymous accounts
  - ◆ If not being used, they are removed
- ❖ Authenticate multiple times
  - ◆ Local workstation
  - ◆ Web Interface

- ◆ Other applications

### **Authentication types**

*Single sign-on* allows the user to automatically authenticate to multiple applications that have different credentials.

With *pass-through authentication*, user authentication is automatically repeated to other applications that require the same credentials.

*Multi-factor authentication* provides additional security by using third-party authentication checks in addition to directory service credentials.

- ❖ For example, an administrator can configure the Web Interface to use RSA SecurID or Secure Computing SafeWord in addition to directory service credentials.

*Smart cards* are inserted into a reader that is attached to the client device to allow authentication.

- ❖ Smart cards can be used for authentication to applications as well as to the network.

*Biometrics* refers to authentication security techniques that rely on unique physical characteristics that can be automatically checked.

- ❖ For example, the analysis of an individual fingerprint can serve as a means of authentication.
  - ◆ The system analyzes the fingerprint to determine who the user is and, based on identity, authorize different levels of access.

### **Multiple passwords risks and recommendations**

If users are required to maintain multiple application passwords:

- ❖ Users may forget their passwords, thus increasing the support costs due to password resets.
- ❖ It also creates the potential for a security risk as users may write down their passwords.

Consider using Password Manager as a single sign-on solution to increase environment security and reduce administrative costs.

### **Weak password risk and recommendation**

Users may select weak passwords for application level authentication, which does not provide a high level of security.

Consider using Password Manager as a single sign-on solution to enforce policy-based controls on application-level authentication.

### **Password complexity requirements risk and recommendation**

Some applications have no password complexity requirements.

Consider using Password Manager as a single sign-on solution to ensure users employ sufficiently complex passwords for applications.

### **Generic accounts risk and recommendation**

Using generic accounts can result in the lack of audit trails for user actions.

Discontinue the use of generic accounts and investigate using Password Manager as identity management software to facilitate user specific accounts and authentication.

### **Single-factor authentication risk and recommendation**

Single-factor authentication might not provide sufficient security for external access points.

Implement two-factor authentication to provide a greater level of security from remote locations.

### **Static password risk and recommendation**

Static passwords might be compromised over time.

Force users to change passwords at regular intervals to increase security.

### **Enterprise security topics**

When an architect is gathering information related to enterprise security including a Presentation Server environment, information should be gathered for:

- ❖ Security personnel
- ❖ Certificates
- ❖ Security configuration of Presentation Servers
- ❖ Security monitoring
- ❖ Server and user restrictions
- ❖ Administrative access
- ❖ Operating system permissions
- ❖ Anti-virus
- ❖ Physical security

### **Published desktops risk and recommendations**

Published desktops are not inherently secure; therefore, there is a risk that the user can gain access to operating system functionality.

Consider published applications instead of published desktops where appropriate and use policies to restrict the desktop to prevent user access to restricted parts of the operating system.

### **Lack of virus protection risk and recommendations**

Lack of virus protection can introduce viruses to the environment.

Implement virus protection and update regularly to minimize intrusion.

### **Insufficiently restricted server resources recommendations**

If server resources are not sufficiently restricted, use policies, security templates, permissions and third-party products to restrict access to resources.

### **Data center access recommendations**

If non-authorized personnel have access to servers in the data center, place the servers behind locked doors and limit access.

### **Remote desktop recommendations**

If users can access Presentation Server using a remote desktop connection, restrict the RDP protocol for administrative use only.

### **Insufficiently restricted servers recommendations**

To keep unauthorized users from modifying servers, restrict servers so only administrators can make changes.

### **Lack of personnel resources risk and recommendations**

Security can be compromised when there is lack of sufficient personnel resources.

Take steps to ensure there are adequate resources (team members, tools, experience and information) available to effectively manage Citrix-related servers.

### **Domain administrators risk and recommendation**

Domain administrators might have unwarranted access to Citrix servers by default.

Remove the domain administrators from the local administrators group for Citrix servers and create a global Citrix administrators group.

### **Network security topics**

When an architect is gathering information related to network security including a Presentation Server environment, information should be gathered for:

- ❖ Placement of Citrix components

- ❖ Remote access
- ❖ VPN access
- ❖ Citrix traffic flow
- ❖ Proxy server
- ❖ Remote offices
- ❖ Internal resources
- ❖ Redundancy

### **Remote access risk and recommendation**

The process used for internal access might differ from the process used for remote access and cause complexity for the user.

Use Access Gateway to allow remote users access to all necessary system resources. This single VPN solution simplifies the user experience while providing all required user access.

### **Multiple VPNs risks and recommendation**

Users might connect to different VPN devices to gain access to their applications and data. This solution requires additional maintenance and more user training.

Use Access Gateway to provide simplified remote access to allow remote users to perform any configured activities securely.

### **Firewall risks and recommendations**

Unauthorized users might gain access to internal resources if they are not secured using a firewall.

Use SSL/TLS encryption to secure all traffic.

### **Remote security risk and recommendation**

When user connections are not secured, communications can be compromised.

Use a VPN solution such as Secure Gateway or Access Gateway to ensure secure remote connections.

### **Internal resources risk and recommendations**

Users may be able to access all internal resources through the VPN instead of only the resources they require.

Use logon points and policies to restrict access using Access Gateway Advanced Edition.

### **Double-hop firewall with Access Gateway configuration**

In a double-hop firewall configuration, with an Access Gateway server deployed in the DMZ:

- ❖ Access Gateway should be placed in the DMZ so that external users can access internal resources.
- ❖ Web Interface should be installed on the internal network.

### **Double-hop firewall with Secure Gateway**

In a double-hop firewall configuration, with a Secure Gateway server deployed in the DMZ:

- ❖ Secure Gateway should be placed in the DMZ so that external users can access internal resources.
- ❖ Web Interface should be installed in the internal network for a more secure deployment.
  - ◆ Web Interface can be installed in the DMZ and can be placed on the same server as Secure Gateway.

### **Identity management solution features**

The most important features of an identity management solution are:

- ❖ Password policies
- ❖ Multi-factor authentication
- ❖ Password sharing groups
- ❖ Identity verification questions
- ❖ Single sign-on password reset

Citrix Password Manager addresses all of these features.

### **Identity management topics**

When gathering information related to identity management, an architect should gather information about:

- ❖ Multiple user passwords
- ❖ Password resets
- ❖ Disablement of user accounts
- ❖ Enforcement of application password change policies

### **Ex-employee user account risk and recommendation**

If an employee leaves the organization, the administrator might not have a mechanism to ensure that the user application accounts are disabled in all locations.

Use password manager to centralize user credentials for applications.

### **Password reset risk and recommendation**

Frequent password reset requests can increase help desk costs.

Use the Self-Service Password Reset feature in Password Manager to allow users to reset their primary password from their desktops.

### **Password change policy risk and recommendations**

Many applications have no inherent password change policy.

Configure Password Manager to enforce password policies for applications with no inherent password change policies.

### **Multiple passwords risk and recommendation**

Users might write down passwords because there are too many to remember.

Use Password Manager to eliminate the need for users to remember multiple passwords.

## **Collaboration and IT Infrastructure**

---

### **User collaboration topics**

When gathering information related to user collaboration, an architect should gather information about:

- ❖ Online presentations
- ❖ Online collaboration
- ❖ Help desk

### **Meetings and collaboration risk and recommendation**

Users might not have a mechanism to collaborate with on-screen documents. In this case, an avenue of production and innovation might be lost.

Consider a collaboration solution, such as GoToMeeting.

### **Help desk risk and recommendation**

Users might be losing time waiting for help desk personnel to physically address their issues.

Consider a remote support solution, such as GoToAssist.

### **IT infrastructure topics**

When assessing the IT infrastructure, focus on completing a thorough evaluation of:

- ❖ Server hardware
- ❖ Network architecture
- ❖ Directory services
- ❖ Client environment
- ❖ Applications
- ❖ Print configuration

### **Server hardware topics**

When gathering information related to server hardware, an architect should focus on:

- ❖ Server specifications
- ❖ Server component redundancy
- ❖ Server configuration

### **Multiple hardware platforms risk and recommendations**

Using different hardware platforms and models might require a separate build process for each configuration, increasing administrative complexity.

Standardize on a single hardware platform where possible and ensure that drivers are compatible across hardware models.

### **Hardware specifications risk and recommendations**

Insufficient processing power, memory or other server resources might not meet needs, reducing the potential number of users per server.

To mitigate this, upgrade servers as necessary or assume fewer users per server.

### **Cost efficiency risk and recommendation**

Cost efficiency of servers is not optimized by using over- or under-powered hardware.

To find out where the servers are cost-inefficient, perform a total cost of ownership analysis.

### **Server components risk and recommendation**

Server components might not meet application needs, requiring additional purchases.

Perform scalability tests to determine the exact requirements prior to making purchasing decisions.

### **Server component redundancy risk and recommendation**

Where there is no redundancy, a single point of failure in a server might cause unnecessary loss of productivity.

An IT department should purchase servers with redundant features when possible.

### **Virtual IP addressing**

*Virtual IP addressing* assigns an IP address to a session to address some of the issues associated with applications that identify the client connection to Presentation Server by an IP address.

- ❖ All virtual IP addresses must be valid and in the same subnet as the server running Presentation Server.
- ❖ If a server is configured to use virtual IP addresses, then each session will be assigned a virtual IP address.
- ❖ Only processes that are configured for virtual IP addressing will make use of this feature, but there must be enough IP addresses for all ICA connections.
- ❖ Virtual IP addressing does not support the remote desktop protocol.
- ❖ Only applications and processes that use Windows Sockets can use virtual IP addressing.
- ❖ For more information about virtual IP addressing in Presentation Server, see Citrix Knowledge Base article CTX107737.

### **Network architecture topics**

When gathering information related to network architecture, an architect should focus on:

- ❖ Work sites
- ❖ Network protocols
- ❖ Network hardware
- ❖ Subnets

### **IP addressing risk and recommendation**

Lack of a planned IP addressing scheme can cause conflicts and confusion.

Assign all servers static IP addresses or use DHCP reservations.

### **Back-end resources risk and recommendation**

The location of backend systems for client-server applications in an environment containing Presentation Server can impact application performance.

For client-server applications, keep the backend systems close to the servers running Presentation Server, if possible.

### **Wireless WAN and satellite risk and recommendation**

High latency, dropped packets and network interruptions can occur with wireless WAN and satellite connections.

Ensure that *session reliability* has been implemented to assist users with these problems.

- ❖ Session reliability is a feature that enables users to continue to view their published applications while the connection to the server is temporarily interrupted. After connectivity is regained, users can resume interaction with their published applications without launching them again.

### **Server farms spanning subnets risk and recommendation**

Server farms that span subnets increase router hops and might introduce performance problems.

Keep server farms within a single subnet when possible.

### **Virtual IP risks and recommendation**

Insufficient IP addresses allocated or incorrect configuration of virtual IP addresses might cause users to receive an error message stating that a virtual IP address could not be assigned.

Review the virtual IP address configuration.

### **Switch ports risks and recommendations**

If switch ports and network interface cards are not configured for the same speed and duplex setting, frames will be dropped resulting in poor network connections.

Configure switch ports and network interface cards for full duplex and the maximum common speed supported by all devices.

### **Multi-homed server risks and recommendations**

Multi-homed servers might introduce security holes in the network. Incorrectly multi-homed servers might cause incorrectly routed network traffic.

An IT department should evaluate the need for multi-homed servers and eliminate them if possible. If required, ensure that multi-homed servers are configured properly, with only one adapter having a default gateway. If additional adapters require access to other subnets, configure a static route.

### **Directory services topics**

When gathering information about directory services, an architect should gather information on:

- ❖ The directory service that is being used
- ❖ Terminal Server profile management
- ❖ Terminal Server group policy objects

### **Active Directory organization risk and recommendation**

If servers are not grouped and secured properly in Active Directory, administrative complexity and security risks are increased.

Place all servers running Presentation Server in organizational units and secure using group policy objects.

### **Client environment topics**

When gathering information related to the client environment, an architect should cover:

- ❖ Client devices
- ❖ Users

### **Multiple client types risks and recommendations**

Too many different client types and operating systems increase administrative complexity and provide an inconsistent user experience.

Standardize clients where possible. Consider the continuum between the cost savings of using existing equipment and the cost savings of reducing administrative complexity. Consider if the total cost of ownership model is built on using existing client devices.

### **Client build process risks and recommendations**

Having no formal client build process can increase support complexity and provides an inconsistent user experience.

Document and enforce a formal client build process.

### **Applications topics**

When gathering information related to applications, an architect should focus on:

- ❖ Application details
- ❖ Application usage
- ❖ Application characteristics

- ❖ Installation packages
- ❖ Current integration issues

### **Multiple applications risk and recommendations**

A vast number of applications might limit the ability to test the environment in later stages of the project.

Categorize similar applications according to form and function and select applications that represent each category to test. Architects should always plan to test mission-critical applications.

### **Concurrent users risk and recommendations**

Applications with a large number of concurrent users might require special design considerations.

Make note of special application cases, application dependencies and integration issues and how they might affect the project.

### **Application dependencies risk and recommendations**

Applications with significant dependencies might require special design considerations.

Make note of special application cases, application dependencies and integration issues and how they might affect the project.

### **Application integration issues risk and recommendations**

Applications with unique behaviors and integration issues or efforts might require special design considerations.

Make note of special application cases, application dependencies and integration issues and how they might affect the project.

### **Print configuration topics**

When gathering information related to printer configuration, an architect should focus on:

- ❖ Printer inventory
- ❖ Driver management
- ❖ Print volume
- ❖ Configuration strategy

### **Print device risk and recommendation**

Individual users or a department acquiring their own print devices vastly increases the number of different devices that need supporting.

Control the introduction of print devices into the organization through centralized purchasing and attempt to standardize on certain models of print devices for standard operations.

### **Local printers risk and recommendation**

Too many instances of printers defined on the client can increase the complexity of the configuration.

Consolidate print devices into network printers where possible.

### **Specialized print devices risk and recommendation**

Print devices with unique features might require special consideration.

Make note of special print devices, citing the specific features and user groups that should be considered.

### **Third-party management risk and recommendation**

Third-party tools used to manage printing might affect the design solution.

Make note of print management tools and their use.

### **Printing across WAN risk and recommendations**

Printing across a WAN link might increase network traffic to an unacceptable level.

To alleviate this, redirect printing through the client device or create printer bandwidth policies to control the flow of network traffic.

## **Operational Procedures**

---

### **System management topics**

When gathering information related to system management, an architect should gather information about:

- ❖ Hardware and server monitoring tools
- ❖ Resource Manager
- ❖ SNMP monitoring tools
  - ◆ IBM Tivoli
  - ◆ CA Unicenter
  - ◆ HP Openview
  - ◆ Network Manager
- ❖ Network monitoring tools

- ❖ Other monitoring tools
- ❖ Reporting and analysis
- ❖ Event management and correlation

### **Lack of a systems management tools risk and recommendations**

An organization might not have a method to monitor systems, resulting in unnecessary downtime in the event of a failure.

Use Resource Manager or the management pack for Microsoft Operations Manager to monitor the systems.

### **Lack of archived data risk and recommendation**

Lack of archived data prevents administrators from performing comprehensive trend analysis.

Gather baseline data in order to set Resource Manager metrics and thresholds appropriately.

### **Hardware and server monitoring risk and recommendation**

Failures might be responded to in a reactive manner.

Implement proactive monitoring to minimize failures and issues.

### **Third-party monitoring tools risk and recommendation**

When using third-party tools to monitor the servers, alerts related to Presentation Server may not be clearly identified.

Use Resource Manager to capture data on Presentation Servers.

### **Test environments**

- ❖ Most organizations do not have a test environment.
- ❖ When test environments exist, they are usually inadequate.
  - ◆ An adequate test environment:
    - Allows the administrator to fully test an application, patch, service pack or hotfix
    - Does not impact the production environment
    - Provides assurance of a successful deployment
    - Provides the administrator the opportunity to develop the necessary expertise in a lab environment prior to deployment into the production environment
    - Facilitates change control including rollback procedure
    - Saves money by avoiding mistakes in production

- ❖ In many cases, evaluation software can be used in a test environment without violating the user license agreement.
  - ◆ Make sure that the evaluation software is fully functional before using it.
- ❖ A segregated farm should always be used for testing.
  - ◆ The segregated farm can use the same license server as the one used in the production environment.
- ❖ The test environment should be as close to a fresh server build as possible to avoid inadvertently skewing the results because many factors in an environment can impact the test results.
- ❖ Do not use a zone in the production environment for testing.
  - ◆ Using a production zone can have a negative impact on production.
    - The introduction of an additional zone can cause additional inter-zone communications and also affects any software or configuration that directly impacts the farm.

### **Test environment topics**

When gathering information related to the test environment, an architect should gather information about:

- ❖ The physical test laboratory
- ❖ Test laboratory configuration
- ❖ Test process
- ❖ Server build
- ❖ Pilot process
- ❖ Evaluation
- ❖ Documentation

### **Untested implementations recommendation**

If changes are being implemented into a production environment without testing, an adequate test environment should be created to test the changes before implementing them into the live environment.

### **Additional zones risk and recommendation**

Additional zones for testing can impact production.

Designate a segregated farm.

### **Test plan documentation risk and recommendation**

Sometimes test processes are not repeatable.

It is always best to document and archive test plans.

### **Test cases risk and recommendation**

Test cases that are not based on actual scenarios can create unrealistic results.

Develop test cases based on actual scenarios including input from users.

### **Licensing and software risk and recommendation**

When using an evaluation version of software full functionality might not be available.

Ensure that evaluation software provides full functionality for a limited time by checking the software or the software manufacturer.

### **Server build risk and recommendation**

A test environment might be inconsistent or dissimilar to the production environment.

Use the same or a similar server build that is used in the production environment.

### **Hardware risk and recommendation**

The test hardware should not be of lesser quality than the hardware used in production.

Use servers that mirror the production hardware.

### **Change control process topics**

When gathering information related to the change control process, an architect should gather information about

- ❖ Documentation
- ❖ Processes
- ❖ User communication
- ❖ Administrative coordination

### **Unapproved changes risk and recommendation**

Changes might be made without following a change control process and unapproved changes might cause problems to the environment.

The IT department should implement a stringent change control process.

### **Emergency change control process recommendation**

To be prepared for emergency changes to help alleviate undesired results that they may produce, develop an emergency change control process.

### **Rollback recommendation**

Have a pre-tested rollback procedure implemented just in case systems are not functional after rollout even after extensive testing in a testing environment.

### **Administrative communication risk and recommendation**

Information might not be circulated among various administrators, which can cause duplication of changes.

Put processes and procedures in place for management approval and information dissemination.

### **Documentation recommendation**

To help administrators reference changes that have occurred prior to the current date, implement a documentation system.

### **Support topics**

When gathering information related to support, an architect should gather information about:

- ❖ Service Level Agreements
- ❖ Technical Support Agreement
- ❖ Support tiers
- ❖ Support tools
- ❖ Metrics
- ❖ User satisfaction
- ❖ Help desk password resets

### **Service level risk and recommendation**

Sometimes there are no expectations set to ensure that administrators and users understand the turnaround time and commitments of the support organization.

Implement a Service Level Agreement or service commitment process in order to set expectations for time to address, time to resolve issues, uptime and other factors.

### **Technical support risk and recommendation**

Sometimes support staff is unable to address complex issues.

Recommend a Citrix Technical Support Agreement.

### **Support readiness risk and recommendations**

Sometimes the support staff does not have sufficient knowledge of Citrix technologies.

Training and knowledge base material should be provided.

### **Call scripts risks and recommendation**

Sometimes call scripts do not contain enough detailed questions and support calls may get routed to the incorrect team which results in support staff and user frustrations.

Implement appropriate and precise call scripts.

### **User satisfaction risk and recommendation**

Sometimes surveys are not being used to receive feedback from users. In this case, it is difficult to identify inefficiencies and improve processes.

Implement a tool that allows users to provide feedback.

### **Metrics risk and recommendation**

Sometimes metrics are not tracked, making it difficult to identify inefficiencies and improve processes.

Configure metrics to track improvements.

### **Support tiers risk and recommendation**

Lack of multi-tier support can be the cause of inefficiencies in the support process.

Implement a multi-tier support approach. This allows for efficiency in building knowledge for specific user groups and allows the support group to operate at various levels of efficiency.

### **Issue tracking risk and recommendation**

Sometimes issues are not being tracked and it leaves the organization unaware of recurring problems.

Consider the use of a tracking tool that uses a single repository for both change control and help desk tickets. This provides administrators the ability to establish a timeline and determine what change created an issue.

### **Knowledge base risk and recommendation**

Without a knowledge base, common issues are not easily resolved.

Create a knowledge base to allow the support group to reference a common set of scripts.

### **Password risks and recommendations**

Lack of a password management solution can cause a high volume of calls to the help desk by users related to password resets.

Consider the use of Password Manager to reduce help desk costs.

### **Backup architecture and restoration topics**

When gathering information related to backup architecture and restoration, an architect should gather information about:

- ❖ Data
- ❖ Backup procedures
- ❖ Data storage
- ❖ Restore process
- ❖ Documentation
- ❖ Server restoration

### **Documentation risks and recommendation**

Sometimes backup and restore procedures are not documented and administrators are not familiar with the steps.

An organization should create a fully documented backup and restore procedure to mitigate any backup and restore familiarity problems.

### **Infrequent backups risk and recommendation**

With infrequent backups, user or environmental data can be lost.

Implement a process that includes some type of daily backups.

### **Restoration risk and recommendation**

Lack of a tested restoration process causes failure at a time of emergency.

Fully test the restoration process and backup the files.

### **Disaster recovery topics**

When gathering information related to disaster recovery, an architect should gather information about:

- ❖ Redundancy
- ❖ Hardware failure

- ❖ Recovery plan
- ❖ Data replication
- ❖ Servers and components
- ❖ Zone preference and failover
- ❖ Disaster mitigation equipment

### **Access infrastructure risk and recommendation**

Single points of failure can prevent users from accessing the access server farm.

Deploy at least two access-related components.

### **Recovery risk and recommendation**

If the recovery plan has never been tested, a disaster recovery could fail.

Test the recovery plan as often as business requirements demand, but at least once a year.

### **Data center risk and recommendation**

A single data center could become incapacitated for many reasons.

To make sure that the organization is not brought to a stand-still if the data center goes down, establish a secondary data center.

### **Network risk and recommendation**

Failures occur due to having a single network supplier.

Create redundancy for internet and communications access by implementing a secondary network provider.

### **Training topics**

When gathering information related to training, an architect should gather information about:

- ❖ The user training plan
- ❖ User training
- ❖ Effectiveness of user training
- ❖ Resources for users
- ❖ Administrator and support staff training

### **User training environment risk and recommendation**

Sometimes users are not adequately trained to work in the production environment.

The organization should provide users training using the production environment.

### **User credentials risk and recommendations**

If unique accounts are used for training, the user experience in training does not always match that in production.

Implement production credentials or training specific credentials and ensure that the users know the difference.

### **Citrix support staff training risk and recommendation**

Sometimes Citrix administrators and support staff are not adequately trained.

Provide the organization with a list of local Authorized Learning Centers and information on Citrix certification tracks and consider eLearning opportunities.

### **Administrator training risk and recommendation**

A lack of time or budget for training can cause administrators to make costly mistakes in production.

Identify and implement necessary training to avoid costly mistakes in the future.

### **Project communication topics**

When gathering information related to project communication, an architect should gather information about:

- ❖ Communication of the project plan
- ❖ Tools
- ❖ Project management
- ❖ User notification process
- ❖ Timelines
- ❖ Resources
- ❖ Management buy-in

### **User notification risk and recommendations**

Users often ignore important information from the IT department.

Limit the amount of communications, send communications to the appropriate audience only and use the appropriate communication medium.

### **Timeline and resources risks and recommendation**

Aggressive timelines can create unrealistic expectations and lead to project failure, which in turn can lead to high turnover of employees.

Always create realistic project plans.

### **User communication methods risk and recommendations**

Many times users are not informed of changes to the environment.

To keep them informed, issue FAQs and executive communiqués.