Microsoft® Windows File Server Audit/Assurance Program

ISACA®
With 95,000 constituents in 160 countries, ISACA (*www.isaca.org*) is a leading global provider of knowledge, certifications, community, advocacy and education on information systems (IS) assurance and security, enterprise governance and management of IT, and IT-related risk and compliance. Founded in 1969, the nonprofit, independent ISACA hosts international conferences, publishes the *ISACA® Journal*, and develops international IS auditing and control standards, which help its constituents ensure trust in, and value from, information systems. It also advances and attests IT skills and knowledge through the globally respected Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in Risk and Information Systems Control™ (CRISC™) designations. ISACA continually updates COBIT®, which helps IT professionals and enterprise leaders fulfill their IT governance and management responsibilities, particularly in the areas of assurance, security, risk and control, and deliver value to the business.

Disclaimer
ISACA has designed and created *Microsoft® Windows File Server Audit/Assurance Program* (the "Work") primarily as an informational resource for audit and assurance professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, audit and assurance professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or IT environment.

Reservation of Rights

ISACA
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
E-mail: *info@isaca.org*
Web site: *www.isaca.org*

ISBN 978-1-60420-187-1
Microsoft® Windows File Server Audit/Assurance Program

ISACA wishes to recognize:

Author
Norm Kelson, CISA, CGEIT, CPA, CPE Interactive Inc., USA

Expert Reviewers
Gbadamosi Folakemi Toyin, CGEIT, CRISC, IT Governance Consult, Nigeria
Michael Jones, CISA, CIA, CISSP, BMO Financial Group, Canada
Abdus Sami Khan, Deloitte, Pakistan
Gary Langham, CISA, CISM, CGEIT, CISSP, CPFA, Australia
Tariq Shaikh, CISA, Tim Hortons Inc., Canada
Vinoth Sivasubramanian, ABRCCI, CEH, ISO 27001 LA, ITIL V3, UAE Exchange Centre LLC, UAE
John G. Tannahill, CISM, CGEIT, CRISC, CA, J. Tannahill & Associates, Canada

Solvay Brussels School of Economics and Management
Strategic Technology Management Institute (STMI) of the National University of Singapore
University of Antwerp Management School
ASI System Integration
Hewlett-Packard
IBM
SOAProjects Inc
Symantec Corp.
TruArx Inc.

Table of Contents

I. Introduction

Overview

ISACA has developed the *IT Assurance Framework*™ (ITAF™) as a comprehensive and good-practice-setting model. ITAF provides standards that are designed to be mandatory and are the guiding principles under which the IT audit and assurance profession operates. The guidelines provide information and direction for the practice of IT audit and assurance. The tools and techniques provide methodologies, tools and templates to provide direction in the application of IT audit and assurance processes.

Purpose

The audit/assurance program is a tool and template to be used as a road map for the completion of a specific assurance process. ISACA has commissioned audit/assurance programs to be developed for use by IT audit and assurance professionals with the requisite knowledge of the subject matter under review, as described in ITAF section 2200—General Standards. The audit/assurance programs are part of ITAF section 4000—IT Assurance Tools and Techniques.

Control Framework

The audit/assurance programs have been developed in alignment with the ISACA COBIT framework—specifically COBIT 4.1—using generally applicable and accepted good practices. They reflect ITAF sections 3400—IT Management Processes, 3600—IT Audit and Assurance Processes, and 3800—IT Audit and Assurance Management.

Many organizations have embraced several frameworks at an enterprise level, including the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control Framework. The importance of the control framework has been enhanced due to regulatory requirements by the US Securities and Exchange Commission (SEC) as directed by the US Sarbanes-Oxley Act of 2002 and similar legislation in other countries. Enterprises seek to integrate control framework elements used by the general audit/assurance team into the IT audit and assurance framework. Since COSO is widely used, it has been selected for inclusion in this audit/assurance program. The reviewer may delete or rename these columns to align with the enterprise's control framework.

Governance, Risk and Control of IT

Governance, risk and control of IT are critical in the performance of any assurance management process. Governance of the process under review will be evaluated as part of the policies and management oversight controls. Risk plays an important role in evaluating what to audit and how management approaches and manages risk. Both issues will be evaluated as steps in the audit/assurance program. Controls are the primary evaluation point in the process. The audit/assurance program identifies the control objectives and the steps to determine control design and effectiveness.

Responsibilities of IT Audit and Assurance Professionals

IT audit and assurance professionals are expected to customize this document to the environment in which they are performing an assurance process. This document is to be used as a review tool and starting point. It may be modified by the IT audit and assurance professional; it *is not* intended to be a checklist or questionnaire. It is assumed that the IT audit and assurance professional has the necessary subject matter expertise required to conduct the work and is supervised by a professional with the Certified Information Systems Auditor (CISA) designation and/or necessary subject matter expertise to adequately review the work performed.

II. Using This Document

This audit/assurance program was developed to assist the audit and assurance professional in designing and executing a review. Details regarding the format and use of the document follow.

Work Program Steps

The first column of the program describes the steps to be performed. The numbering scheme used provides built-in work paper numbering for ease of cross-reference to the specific work paper for that section. The physical document was designed in Microsoft® Word. The IT audit and assurance professional is encouraged to make modifications to this document to reflect the specific environment under review.

Step 1 is part of the fact-gathering and prefieldwork preparation. Because the prefieldwork is essential to a successful and professional review, the steps have been itemized in this plan. The first level steps, e.g., 1.1, are in **bold** type and provide the reviewer with a scope or high-level explanation of the purpose for the substeps.

Beginning in step 2, the steps associated with the work program are itemized. To simplify use, the audit/assurance program describes the audit/assurance objective—the reason for performing the steps in the topic area and the specific controls follow. Each review step is listed after the control. These steps may include assessing the control design by walking through a process, interviewing, observing or otherwise verifying the process and the controls that address that process. In many cases, once the control design has been verified, specific tests need to be performed to provide assurance that the process associated with the control is being followed.

The maturity assessment, which is described in more detail later in this document, makes up the last section of the program.

The audit/assurance plan wrap-up—those processes associated with the completion and review of work papers, preparation of issues and recommendations, report writing and report clearing—has been excluded from this document because it is standard for the audit/assurance function and should be identified elsewhere in the enterprise's standards.

COBIT Cross-reference

The COBIT cross-reference provides the audit and assurance professional with the ability to refer to the specific COBIT control objective that supports the audit/assurance step. The COBIT control objective should be identified for each audit/assurance step in the section. Multiple cross-references are not uncommon. Subprocesses in the work program are too granular to be cross-referenced to COBIT. The audit/assurance program is organized in a manner to facilitate an evaluation through a structure parallel to the development process. COBIT provides in-depth control objectives and suggested control practices at each level. As professionals review each control, they should refer to COBIT 4.1 or the *IT Assurance Guide: Using COBIT* for good-practice control guidance.

COSO Components

As noted in the introduction, COSO and similar frameworks have become increasingly popular among audit and assurance professionals. This ties the assurance work to the enterprise's control framework. While the IT audit/assurance function uses COBIT as a framework, operational audit and assurance professionals use the framework established by the enterprise. Since COSO is the most prevalent internal control framework, it has been included in this document and is a bridge to align IT audit/assurance with the rest of the audit/assurance function. Many audit/assurance organizations include the COSO control components within their reports and summarize assurance activities to the audit committee of the board of directors.

For each control, the audit and assurance professional should indicate the COSO component(s) addressed. It is possible, but generally not necessary, to extend this analysis to the specific audit step level.

The original COSO internal control framework contained five components. In 2004, COSO was revised as the *Enterprise Risk Management (ERM) Integrated Framework* and extended to eight components. The primary difference between the two frameworks is the additional focus on ERM and integration into the business decision model. Large enterprises are in the process of adopting ERM. The two frameworks are compared in **figure 1**.

Figure 1—Comparison of COSO Internal Control and ERM Integrated Frameworks

Internal Control Framework	ERM Integrated Framework
Control Environment: The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values, management's operating style, delegation of authority systems, as well as the processes for managing and developing people in the organization.	**Internal Environment**: The internal environment encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an entity's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.
	Objective Setting: Objectives must exist before management can identify potential events affecting their achievement. Enterprise risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the entity's mission and are consistent with its risk appetite.

Figure 1—Comparison of COSO Internal Control and ERM Integrated Frameworks	
Internal Control Framework	**ERM Integrated Framework**
	Event Identification: Internal and external events affecting achievement of an entity's objectives must be identified, distinguishing between risks and opportunities. Opportunities are channeled back to management's strategy or objective-setting processes.
Risk Assessment: Every entity faces a variety of risks from external and internal sources that must be assessed. A precondition to risk assessment is establishment of objectives, and, thus, risk assessment is the identification and analysis of relevant risks to achievement of assigned objectives. Risk assessment is a prerequisite for determining how the risks should be managed.	**Risk Assessment**: Risks are analysed, considering the likelihood and impact, as a basis for determining how they could be managed. Risk areas are assessed on an inherent and residual basis.
	Risk Response: Management selects risk responses—avoiding, accepting, reducing or sharing risk—developing a set of actions to align risks with the entity's risk tolerances and risk appetite.
Control Activities: Control activities are the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address risks to achievement of the entity's objectives. Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties.	**Control Activities:** Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.
Information and Communication: Information systems play a key role in internal control systems as they produce reports, including operational, financial and compliance-related information that make it possible to run and control the business. In a broader sense, effective communication must ensure information flows down, across and up the organization. Effective communication should also be ensured with external parties, such as customers, suppliers, regulators and shareholders.	**Information and Communication:** Relevant information is identified, captured and communicated in a form and time frame that enable people to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across and up the entity.
Monitoring: Internal control systems need to be monitored—a process that assesses the quality of the system's performance over time. This is accomplished through ongoing monitoring activities or separate evaluations. Internal control deficiencies detected through these monitoring activities should be reported upstream and corrective actions should be taken to ensure continuous improvement of the system.	**Monitoring:** The entirety of enterprise risk management is monitored and modifications are made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations or both.

Information for **figure 1** was obtained from the COSO Web site, *www.coso.org/aboutus.htm.*

The original COSO internal control framework addresses the needs of the IT audit and assurance professional: control environment, risk assessment, control activities, information and communication, and monitoring. As such, ISACA has elected to utilize the five-component model for its audit/assurance programs. As more enterprises implement the ERM model, the additional three columns can be added, if relevant. When completing the COSO component columns, consider the definitions of the components as described in **figure 1**.

Reference/Hyperlink

Good practices require the audit and assurance professional to create a work paper that describes the work performed, issues identified and conclusions for each line item. The reference/hyperlink is to be used to cross-reference the audit/assurance step to the work paper that supports it. The numbering system of this document provides a ready numbering scheme for the work papers. If desired, a link to the work paper can be pasted into this column.

Issue Cross-reference

This column can be used to flag a finding/issue that the IT audit and assurance professional wants to further investigate or establish as a potential finding. The potential findings should be documented in a work paper that indicates the disposition of the findings (formally reported, reported as a memo or verbal finding, or waived).

Comments
The comments column can be used to indicate the waiving of a step or other notations. It is not to be used in place of a work paper that describes the work performed.

III. Controls Maturity Analysis

One of the consistent requests of stakeholders who have undergone IT audit/assurance reviews is a desire to understand how their performance compares to good practices. Audit and assurance professionals must provide an objective basis for the review conclusions. Maturity modeling for management and control over IT processes is based on a method of evaluating the enterprise, so that it can be rated from a maturity level of nonexistent (0) to optimized (5). This approach is derived from the maturity model that the Software Engineering Institute (SEI) of Carnegie Mellon University defined for the maturity of software development.

IT Assurance Guide Using COBIT Appendix VII—Maturity Model for Internal Control (**figure 2**) provides a generic maturity model that shows the status of the internal control environment and the establishment of internal controls in an enterprise. It shows how the management of internal control, and an awareness of the need to establish better internal controls, typically develops from an *ad hoc* to an optimized level. The model provides a high-level guide to help COBIT users appreciate what is required for effective internal controls in IT and to help position their enterprise on the maturity scale.

Figure 2—Maturity Model for Internal Control

Maturity Level	Status of the Internal Control Environment	Establishment of Internal Controls
0 Non-existent	There is no recognition of the need for internal control. Control is not part of the organization's culture or mission. There is a high risk of control deficiencies and incidents.	There is no intent to assess the need for internal control. Incidents are dealt with as they arise.
1 Initial/*ad hoc*	There is some recognition of the need for internal control. The approach to risk and control requirements is *ad hoc* and disorganized, without communication or monitoring. Deficiencies are not identified. Employees are not aware of their responsibilities.	There is no awareness of the need for assessment of what is needed in terms of IT controls. When performed, it is only on an *ad hoc* basis, at a high level and in reaction to significant incidents. Assessment addresses only the actual incident.
2 Repeatable but Intuitive	Controls are in place but are not documented. Their operation is dependent on the knowledge and motivation of individuals. Effectiveness is not adequately evaluated. Many control weaknesses exist and are not adequately addressed; the impact can be severe. Management actions to resolve control issues are not prioritized or consistent. Employees may not be aware of their responsibilities.	Assessment of control needs occurs only when needed for selected IT processes to determine the current level of control maturity, the target level that should be reached and the gaps that exist. An informal workshop approach, involving IT managers and the team involved in the process, is used to define an adequate approach to controls for the process and to motivate an agreed-upon action plan.
3 Defined	Controls are in place and adequately documented. Operating effectiveness is evaluated on a periodic basis and there is an average number of issues. However, the evaluation process is not documented. While management is able to deal predictably with most control issues, some control weaknesses persist and impacts could still be severe. Employees are aware of their responsibilities for control.	Critical IT processes are identified based on value and risk drivers. A detailed analysis is performed to identify control requirements and the root cause of gaps and to develop improvement opportunities. In addition to facilitated workshops, tools are used and interviews are performed to support the analysis and ensure that an IT process owner owns and drives the assessment and improvement process.
4 Managed and Measurable	There is an effective internal control and risk management environment. A formal, documented evaluation of controls occurs frequently. Many controls are automated and regularly reviewed. Management is likely to detect most control issues, but not all issues are routinely identified. There is consistent follow-up to address identified control weaknesses. A limited, tactical use of technology is applied to automate controls.	IT process criticality is regularly defined with full support and agreement from the relevant business process owners. Assessment of control requirements is based on policy and the actual maturity of these processes, following a thorough and measured analysis involving key stakeholders. Accountability for these assessments is clear and enforced. Improvement strategies are supported by business cases. Performance in achieving the desired outcomes is consistently monitored. External control reviews are organized occasionally.

Figure 2—Maturity Model for Internal Control		
Maturity Level	**Status of the Internal Control Environment**	**Establishment of Internal Controls**
5 Optimized	An enterprisewide risk and control program provides continuous and effective control and risk issues resolution. Internal control and risk management are integrated with enterprise practices, supported with automated real-time monitoring with full accountability for control monitoring, risk management and compliance enforcement. Control evaluation is continuous, based on self-assessments and gap and root cause analyses. Employees are proactively involved in control improvements.	Business changes consider the criticality of IT processes and cover any need to reassess process control capability. IT process owners regularly perform self-assessments to confirm that controls are at the right level of maturity to meet business needs and they consider maturity attributes to find ways to make controls more efficient and effective. The organization benchmarks to external best practices and seeks external advice on internal control effectiveness. For critical processes, independent reviews take place to provide assurance that the controls are at the desired level of maturity and working as planned.

The maturity model evaluation is one of the final steps in the evaluation process. The IT audit and assurance professional can address the key controls within the scope of the work program and formulate an objective assessment of the maturity levels of the control practices. The maturity assessment can be a part of the audit/assurance report and can be used as a metric from year to year to document progress in the enhancement of controls. However, the perception of the maturity level may vary between the process/IT asset owner and the auditor. Therefore, an auditor should obtain the concerned stakeholder's concurrence before submitting the final report to management.

At the conclusion of the review, once all findings and recommendations are completed, the professional assesses the current state of the COBIT control framework and assigns it a maturity level using the six-level scale. Some practitioners utilize decimals (x.25, x.5, x.75) to indicate gradations in the maturity model. As a further reference, COBIT provides a definition of the maturity designations by control objective. While this approach is not mandatory, the process is provided as a separate section at the end of the audit/assurance program for those enterprises that wish to implement it. It is suggested that a maturity assessment be made at the COBIT control level. To provide further value to the client/customer, the professional can also obtain maturity targets from the client/customer. Using the assessed and target maturity levels, the professional can create an effective graphic presentation that describes the achievement or gaps between the actual and targeted maturity goals. A graphic is provided as the last page of the document (section VIII), based on sample assessments.

IV. Assurance and Control Framework

ISACA IT Assurance Framework and Standards

ITAF section 3630.14—Operating Systems (OSs) Management and Controls—is relevant to the Microsoft Windows File Server.

ISACA Control Framework

COBIT is a framework for the governance of IT and a supporting tool set that allows managers to bridge the gap among control requirements, technical issues and business risks. COBIT enables clear policy development and good practice for IT control throughout enterprises.

Utilizing COBIT as the control framework from which IT audit/assurance activities are based aligns IT audit/assurance with good practices as developed by the enterprise.

COBIT IT process DS9 *Manage the configuration*, from the Deliver and Support (DS) domain, addresses good practices for ensuring the integrity of hardware and software configurations. This requires the establishment and maintenance of an accurate and complete configuration repository. Sections from DS5 *Ensure systems security* and AI3 *Acquire and maintain technology infrastructure* are relevant in the implementation process.

The configuration COBIT control objectives are:
- DS9.1 Configuration repository and baseline
- DS9.2 Identification and maintenance of configuration items
- DS9.3 Configuration integrity review

The security and design COBIT control objectives are:
- AI3.2 Infrastructure resource protection and availability
- AI3.3 Infrastructure maintenance
- DS5.3 Identity management
- DS5.4 User account management
- DS5.5 Security testing, surveillance and monitoring
- DS5.6 Security incident definition
- DS5.10 Network security
- DS11.6 Security Requirements for Data Management

These COBIT control objectives are provided in section VII of this publication.

Refer to ISACA publication *COBIT® Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition*, published in 2007, for the related control practice value and risk drivers.

V. Executive Summary of Audit/Assurance Focus

Windows File Servers

The file server is the most basic of system servers. As the name implies, its function is to store and manage data. Departmental and organizational folders are established to store and make available data, programs, documents, etc. In the early days of networked office systems, each file server had its individual access configuration; today, all user access rights, including identity management and user access are controlled by Microsoft Active Directory, a single sign-on system that integrates all servers into a domain. This simplifies user identity and access privilege maintenance.

File servers may perform other server duties, but this is strongly discouraged because the configuration requirements for other servers, e.g., web, application or active directory domain controllers, are quite different from those of the file server.

File servers once performed print server functions; however, this has been virtually eliminated because this function is incorporated into most network-connected printers.

Business Impact and Risk

A successful attack on or compromise of a file server would depend upon the information contained on the file server's disk, and could expose the enterprise to a variety of undesirable outcomes, including:
- Disclosure of privileged information
- Loss of intellectual property
- Corruption of the underlying data in sensitive databases
- Loss of competitive advantage
- Reputational risk and loss of confidence by stakeholders, business partners and customers due to disclosure of information or related publicity
- Breach of statutory or regulatory requirements

- Disruption of the computer infrastructure, resulting in the inability to perform critical business functions and incurring remediation costs
- Introduction of computer viruses and other malware that could cause significant hardships and remediation costs to the enterprise
- Fines and penalties due to noncompliance with relevant statutes and regulations
- Security breaches leading to lost productivity and incurring remediation costs

Objective and Scope

Objective—The File Server audit/assurance review will provide management with an independent assessment of the effectiveness of the configuration and of the security of the enterprise's file servers.

Scope—The review will focus on the configuration, management, and physical security of a cross section of the relevant and high-risk file servers in the enterprise. The selection of specific servers will be based on the risk introduced to the enterprise by these systems.

The review will focus on the configuration controls relating to:
- File server management and administration
- File server configuration settings
- Physical security of the file servers
- Secure administrative practices and logical security

The scope excludes:
- Applications operating on the file servers
- Workstation configurations
- User access and identity management (these are maintained by Active Directory)
- Domain Name Service (DNS) management
- File servers not connected to a domain using Active Directory

It is recommended that:
- Workstation configuration assessments be performed using audit/assurance programs designed for the operating system and function (desktop, laptop, special applications, etc.)
- User access and identity management be reviewed using ISACA's *Identity Management Audit/Assurance Program*
- DNS management be approached as part of a network assessment

{The remainder of this paragraph needs to be customized to describe which servers and applications within the enterprise will be reviewed.}

Minimum Audit Skills

This review is considered moderately technical. The audit and assurance professional should have the requisite knowledge of Windows file servers, their functionality, features, weaknesses and security good practices.

The audit and assurance professional should be cautioned not to attempt to conduct an audit/assurance review of Windows file servers utilizing this program as a checklist. This audit program should be conducted by individuals with good technical knowledge of Windows file servers.

It should not be assumed that an audit and assurance professional holding the CISA designation alone has the requisite skills to perform this review.

VI. Audit/Assurance Program

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
1. PLANNING AND SCOPING THE AUDIT									
1.1 Define the audit/assurance objectives. The audit/assurance objectives are high-level and describe the overall audit goals.									
1.1.1 Review the audit/assurance objectives in the introduction to this audit/assurance program.									
1.1.2 Modify the audit/assurance objectives to align with the audit/assurance universe, annual plan and charter.									
1.2 Define assignment success. The success factors need to be identified. Communication among the IT audit/assurance team, other assurance teams and the enterprise is essential.									
1.2.1 Identify the drivers for a successful review.									
1.2.2 Communicate success attributes to the process owner or stakeholder, and obtain agreement.									
1.3 Define the boundaries of the review. The review must have a defined scope. Understand the functions and application requirements for the file servers within the scope.									
1.3.1 Obtain a list and description of the departments storing files or using applications on the file servers.									
1.3.2 Determine the file servers to be within scope.									
1.4 Identify and document risks. The risk assessment is necessary to evaluate where audit resources should be focused. In most enterprises, audit resources are not available for all processes. The risk-based approach assures utilization of audit resources in the most effective manner.									
1.4.1 Identify the business risk associated with the file server applications and any specific functionality of the file server.									
1.4.2 Based on the risk assessment, evaluate the overall risk factor for performing the review.									
1.4.3 Based on the risk assessment, identify changes to the scope.									
1.4.4 Discuss the risk with IT management, and adjust the risk assessment.									
1.4.5 Based on the risk assessment, revise the scope.									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
1.5 Define the change process. The initial audit approach is based on the reviewer's understanding of the operating environment and associated risk. As further research and analysis are performed, changes to the scope and approach may result.									
1.5.1 Identify the senior IT assurance resource responsible for the review.									
1.5.2 Establish the process for suggesting and implementing changes to the audit/assurance program and the authorizations required.									
1.6 Define the audit/assurance resources required. The resources required are defined in the introduction to this audit/assurance program.									
1.6.1 Determine the audit/assurance skills necessary for the review.									
1.6.2 Estimate the total audit/assurance resources (hours) and time frame (start and end dates) required for the review.									
1.7 Define deliverables. The deliverable is not limited to the final report. Communication between the audit/assurance teams and the process owner is essential to assignment success.									
1.7.1 Determine the interim deliverables, including initial findings, status reports, draft reports, due dates for responses or meetings, and the final report.									
1.8 Communicate. The audit/assurance process must be clearly communicated to the customer/client.									
1.8.1 Conduct an opening conference to discuss: Objectives with the stakeholders Documents and information security resources required to perform the review Scope, scope limitations (audit boundaries), budgets, due dates, time lines, milestones and deliverables									
2. PREPARATORY STEPS									
2.1 Obtain and review the current organizational chart for the management and security functions responsible for the file servers.									
2.2 Obtain the job functions of IT personnel responsible for file server management.									
2.3 Determine if audits of the OS and its physical security have been performed.									
2.3.1 If these audits have been performed, obtain the work papers for the previous audits.									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
2.3.1.1 Review the security configuration, and determine if identified issues have been corrected.									
2.3.1.2 Determine if the specific servers under consideration for inclusion in the scope of this audit have been included in the review.									
2.4 Select the servers to be included in the review.									
2.4.1 Based on the prioritized list of servers developed previously, identify the servers to be included in the review. Be sure that there is a representative sample of high-risk servers. A group of servers may have similar functions and can be aggregated into a group.									
2.4.2 Determine if there is a corporate standard server configuration and related settings for each type of server.									
2.5 Obtain documentation for the servers to be reviewed.									
2.5.1 Obtain an understanding of the operating environment and management issues.									
2.5.2 Interview the senior management analyst (manager or director) responsible for the underlying OS to obtain an understanding of policies, procedures and known issues.									
3. ACCESS CONTROL									
3.1 Domain Membership Audit/Assurance Objective: All file servers are members of a domain within Active Directory.									
3.1.1 Domain Membership Control: File servers are assigned to an Active Directory domain.	AI3.2 DS5.2 DS5.3 DS5.4 DS6.3 DS9.1 DS9.2 DS11.6			X					
3.1.1.1 Determine that file servers are members of an Active Directory domain.									
3.1.2 Domain Exclusion Control: File servers excluded from Active Directory have been authorized with appropriate explanation.	AI3.2 DS6.3 DS9.2			X					
3.1.2.1 Identify file servers in the sample that are not members of a domain.									
3.1.2.2 Determine if each file server exempted from Active Directory has been appropriately authorized and approved.									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
3.1.2.3 Determine if the justification for exclusion from domain membership is reasonable based upon the server's function and data stored.									
3.2 Administrator Access Audit/Assurance Objective: Access to the built-in administrator account is limited on a need to know basis; access is monitored, and is accountable.									
3.2.1 Administrator User IDs Control: The built-in administrator user ID is restricted, the password is secure, and access is monitored.	AI3.2 DS5.2 DS5.3 DS5.4 DS9.2			X					
3.2.1.1 Determine if the built-in administrator user ID has been changed.									
3.2.1.2 Determine if the built-in administrator user ID has been disabled.									
3.2.1.3 Determine if the built-in administrator user ID (renamed) password has limited privileges.									
3.2.1.3.1 Inquire if a copy of the password is secured in a locked area.									
3.2.1.3.2 Interview several staff to determine who has knowledge of the password.									
3.2.1.3.3 Evaluate if there are too many individuals with access to the built-in user ID.									
3.2.1.4 Determine if a logging and monitoring function exists within the local audit policy to monitor use of the built-in administrator user ID.									
3.2.1.4.1 Obtain the logging policies and procedures.									
3.2.1.4.2 Determine if the logging can be disabled without notification.									
3.2.1.4.3 Determine if the logging reports are reviewed regularly and if the review process is documented.									
3.2.2 Administrator Equivalent User IDs Control: Each technician responsible for managing a specific server has a unique ID equivalent to the built-in administrator function.	AI3.2 DS5.2 DS5.3 DS5.4 DS9.2			X					
3.2.2.1 Determine if there are several user IDs assigned to the specific server.									
3.2.2.2 Determine if there are too many administrator user IDs (depending on organizational requirements, this number should be 2 or 3, but conditions could									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
warrant additional ones).									
3.2.2.3 Determine if the administrator user IDs require complex passwords.									
3.2.2.3.1 Obtain the local security policy.									
3.2.2.3.2 Verify that: • Complex passwords are in use • Passwords are required to have an expiration date									
3.2.3 Local Administrator Group Control: Domain administrator group is a member of the local administrator group and no individual users are members.	AI3.2 DS5.2 DS5.3 DS5.4 DS9.2			X					
3.2.3.1 Determine that the domain administrator group is a member of the local administrator group.									
3.2.3.2 Determine that other users who are members of the local administrator group require access.									
3.3 Non-Administrator Access Audit/Assurance Objective: Users access to file servers is only through Active Directory.									
3.3.1 Non-Administrator Access Control: No users have user IDs assigned on a local file server. It may be necessary to assign local file server IDs to specific applications or functions on an as-needed basis.	AI3.2 DS5.3 DS5.4 DS9.2 DS11.6			X					
3.3.1.1 Determine that no local user IDs other than administrator equivalent users required to maintain the server are assigned.									
3.3.1.1.1 Obtain a list of users from the local server console using the server manager: selecting -> configuration -> users and groups.									
3.3.1.1.2 Determine that no user IDs exist other than the administrator equivalents. If user IDs exist, determine if they are necessary.									
3.4 File Access Audit/Assurance Objective: File access control is managed centrally by Active Directory.									
3.4.1 File Access Denied to Local Server Control: Local file shares are not permitted on the file server.	AI3.2 DS9.1			X					

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
	DS9.2 DS11.6								
3.4.1.1 Determine if no local file shares are defined on the file server.									
3.4.1.1.1 Review the file share settings for each disk drive on the file server.									
3.4.1.1.2 Display the Share and Storage Management Console Plug-in (storagemgmt.msc).									
3.4.1.1.3 Determine there are no shares.									
3.5 Console Access Limitations Audit/Assurance Objective: Console access to file servers is limited to a need to know basis.									
3.5.1 Console Access Limitation Control: File server console access is limited.	AI3.3 DS5.10 DS9.2 DS12.2			X					
3.5.1.1 Determine the Remote Desktop application is restricted to specific IP addresses.									
3.5.1.2 Determine if the Remote Desktop port has been changed to a non-standard port number.									
3.5.1.3 Remote desktop application is restricted by the local user rights policy: LogonLocally and LogonThroughTerminalServices/.									
4. NETWORK SECURITY									
4.1 File Server Network Security Audit/Assurance Objective: File servers are protected from unauthorized network access.									
4.1.1 Port Restrictions Control: The file server utilizes a software firewall to limit access to only necessary ports.	DS5.10 DS9.2			X					
4.1.1.1 Determine the ports necessary for the file server.									
4.1.1.2 Determine that only these ports are open within the file server firewall.									
4.1.2 Virtual LAN Segmentation Control: The file server is connected to a local area network segment dedicated to processing data with similar classifications.	DS5.10 DS9.2			X					
4.1.2.1 Identify other file servers and equipment connected on the local area network segment.									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
4.1.2.2 Determine if the data that traverses this network segment pose any risk to the file server being audited.									
5. OPERATING SYSTEM SECURITY									
5.1 Separation of Virtual Machines Audit/Assurance Objective: File servers operating as virtual machines are segregated from other virtual machines.									
5.1.1 Assurance of Virtual Machine Separation Control: The audit team has confirmed the separation of virtualized environments through separate assurance reviews.	AI3.2 AI3.3 DS9.1 DS9.2			X					
5.1.1.1 Determine if an audit of the virtualized environment has been performed.									
5.1.1.2 If no virtualization audit has been performed, consider performing an audit. (ISACA's *Virtualization Audit/Assurance Program* can be used).									
5.1.1.3 If a virtualization audit has been performed, determine if the scope of that audit included the servers that were reviewed within scope of this audit.									
5.1.1.4 If the virtualization audit did not include the servers that were reviewed within scope of this audit, determine if the servers selected within the scope of the virtualization review provide relevance and assurance for the selected servers.									
5.1.1.5 Determine if a virtualization audit needs to be performed prior to continuing with this audit.									
6. SHARED IT MANAGEMENT SERVICES									
6.1 Patch Management Audit/Assurance Objective: Patch management procedures are consistently applied using installation policies and procedures.									
6.1.1 Patch Management Control: Standard installation patch management policies and procedures are implemented for the file server.	AI3.3 DS4 DS9.3			X					
6.1.1.1 Obtain the patch management policies and procedures.									
6.1.1.1.1 Determine that appropriate testing, authorization, prioritization and promotion-to-production procedures are in use for the file server-related patches and hot-fixes.									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
6.1.1.1.2 Determine that appropriate testing, authorization, prioritization and promotion-to-production policies are documented for the file server-related patch management									
6.1.1.1.3 Determine that all applicable patches were completed.									
6.1.1.1.4 Obtain explanations for any current patches that are not complete.									
6.1.1.2 Obtain recent audit/assurance work papers of patch management.									
6.1.1.2.1 Evaluate open issues, and determine their impact on the web server controls environment.									
6.2 Log Management Audit/Assurance Objective: Logs of critical server activities are available for review and analysis, and are reviewed by someone other than the administrators responsible for the actions recorded in the log.									
6.2.1 Log Management Control: Management generates appropriate security logs, reviews logs regularly and retains the logs for discovery and forensic analysis.	AI3.2 AI7 DS9.1 DS9.2			X	X	X			
6.2.1.1 Obtain the file server log management policies.									
6.2.1.2 Determine that appropriate logs are generated and retained.									
6.2.1.3 Select a sample of critical logging reports.									
6.2.1.4 Review the procedures for evidence of management review, incident escalation based on the review of logs, remediation and retention policies.									
6.2.1.5 Select a sample of issues arising from the logging reports, and determine that, in each case, the previously mentioned procedures were followed.									
6.3 Incident Management Audit/Assurance Objective: Incident management processes assure that issues affecting the file server environment are identified and researched, an action plan for remediation is established, protection actions are implemented, significant issues are escalated to appropriate management, incidents are closed and incident trends are analyzed.									
6.3.1 Incident Management Control: Enterprise incident management processes include file server activities, and the incident management processes are actively monitored.	DS5.6 DS8			X					

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
6.3.1.1 Obtain the enterprise's incident management process(es).									
6.3.1.2 Determine if file server activities are included in the incident management procedure.									
6.3.1.3 Select file server-related incidents from the incident management system. Follow the incident investigation and remediation to closure.									
6.3.1.4 Determine if significant security incidents have been escalated to the appropriate officials per the IT incident management plan.									
6.3.1.5 Determine if all steps in the procedure, including remediation and closure, have been adequately documented.									
6.4 Intrusion Monitoring and Prevention Audit/Assurance Objective: Web servers are included in the intrusion detection system (IDS)/intrusion prevention system (IPS) activities of the enterprise.									
6.4.1 Intrusion Detection/Prevention Control: Web servers are within the scope of the enterprise's firewall and intrusion detection/prevention policies.	AI3.2 AI7 DS5.5 DS5.9 DS9.1 DS9.2			X	X	X			
6.4.1.1 Obtain and review the relevant network architecture diagram to determine that the network segment containing file servers is included in the scope of the relevant firewall(s) and IDS/IPS device(s).									
6.4.1.2 Determine if an audit/assurance assessment has been performed on the intrusion monitoring and detection process associated with network perimeter audits.									
6.4.1.3 If audits have been performed, obtain the work papers and the report.									
6.4.1.4 Determine if the scope of the intrusion detection/prevention process includes the file server environment.									
6.4.1.5 If an audit has not been performed or if the file server environment has been excluded from the standard monitoring process, expand the scope of this audit or perform a separate audit of the intrusion monitoring program.									
6.5 Physical Security Audit/Assurance Objective: File servers have adequate physical security to prevent physical access by unauthorized individuals.									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
6.5.1 Physical Security Control: File servers are within the scope of the enterprise's physical security policies and procedures.	DS12			X					
6.5.1.1 Obtain and review a copy of the enterprise's current physical security policies and procedures, and determine that file servers are not excluded in any way.									
6.5.1.2 Visit the data center housing the file servers, and view physical security controls, e.g., electronic and/or biometric access controls, magnetic door locks, hardened physical structure, guards, reception desk, magnetic badges, all visitors accompanied, video surveillance cameras, 24x7 guard service, locked server racks, backup heating, ventilating and air conditioning (HVAC) and electrical power systems, etc.									
6.5.1.3 Determine if the file servers are maintained outside the data center.									
6.5.1.3.1 Obtain a list of file servers not maintained in the data center.									
6.5.1.3.2 Determine if the file servers not contained in the data center are maintained in secure locations, consider the following: • Key lock or combination lock doors • Adequate air flow and air conditioning • Entry/exit monitoring									
6.6 Secure Administrative Practices Audit/Assurance Objective: File servers are administered in a secure manner.									
6.6.1 Secure Administration Control: Procedures are in place to ensure that the administration of file servers are adequately restricted, controlled and audit trailed.	DS9 DS11.6 DS13			X					
6.6.1.1 Obtain copies of the enterprise's policies and procedures for system administration, and determine that file servers are not excluded from any procedures. Obtain explanations from IT management for any discrepancies.									
6.6.1.2 Obtain and review a list of all staff with administrative privileges over file servers, and obtain explanations for unusual conditions, e.g., non-IT staff with such privileges, excessive numbers of administrators per server, incompatible duties, etc.									
6.6.1.3 Obtain a list from human resources of current staff and ensure that all individuals with file server administrative privileges are active, i.e., not suspended or terminated.									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
6.6.1.4 Obtain a sample of audit trails over administrative access to the file servers or a sample of file servers (if more than one); review for unusual activities, e.g., excessive time spent logged on for administrative functions, unusual times of the day (late at night, weekends, office-closed holidays); and obtain explanations.									
6.6.1.5 Determine that a backup copy exists for all administrative IDs and corresponding passwords, which is kept safely by a person in IT or general management, e.g., in a locked safe with limited access.									
6.7 Change Management Audit/Assurance Objective: Changes to production file servers are properly authorized, tested and reviewed.									
6.7.1 Change Management Control: Procedures are documented and in place for all changes to file server configurations, including emergency changes.	AI6								
6.7.1.1 Determine that file servers are included in the enterprise's normal change control procedures, including (but not limited to): • Determination of the need for changes • Authorization to proceed • Tests of changes in a controlled environment (sandbox) • Approval of test results • Authorization to deploy into production • Backout procedures for unsuccessful changes • Postimplementation review									
6.7.1.2 Choose a sample of emergency changes and determine that they were: • Fully documented • Approved, after the fact, by an appropriate management level • In accordance with documented procedures for emergency changes									

VII. Maturity Assessment

The maturity assessment is an opportunity for the reviewer to assess the maturity of the processes reviewed. Based on the results of the audit/assurance review and the reviewer's observations, assign a maturity level to each of the following COBIT control objectives.

COBIT Control Objective	Assessed Maturity	Target Maturity	Reference Hyper-link	Comments
AI3.2 Infrastructure Resource Protection and Availability Implement internal control, security and auditability measures during configuration, integration and maintenance of hardware and infrastructural software to protect resources and ensure availability and integrity. Responsibilities for using sensitive infrastructure components should be clearly defined and understood by those who develop and integrate infrastructure components. Their use should be monitored and evaluated.				
AI3.3 Infrastructure Maintenance Develop a strategy and plan for infrastructure maintenance, and ensure that changes are controlled in line with the organisation's change management procedure. Include periodic reviews against business needs, patch management, upgrade strategies, risks, vulnerabilities assessment and security requirements.				
DS5.3 Identity Management Ensure that all users (internal, external and temporary) and their activity on IT systems (business application, IT environment, system operations, development and maintenance) are uniquely identifiable. Enable user identities via authentication mechanisms. Confirm that user access rights to systems and data are in line with defined and documented business needs and that job requirements are attached to user identities. Ensure that user access rights are requested by user management, approved by system owners and implemented by the security-responsible person. Maintain user identities and access rights in a central repository. Deploy cost-effective technical and procedural measures, and keep them current to establish user identification, implement authentication and enforce access rights.				
DS5.4 User Account Management Address requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges with a set of user account management procedures. Include an approval procedure outlining the data or system owner granting the access privileges. These procedures should apply for all users, including administrators (privileged users) and internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information should be contractually arranged for all types of users. Perform regular management review of all accounts and related privileges.				

COBIT Control Objective	Assessed Maturity	Target Maturity	Reference Hyper-link	Comments
DS5.5 Security Testing, Surveillance and Monitoring Test and monitor the IT security implementation in a proactive way. IT security should be reaccredited in a timely manner to ensure that the approved enterprise's information security baseline is maintained. A logging and monitoring function will enable the early prevention and/or detection and subsequent timely reporting of unusual and/or abnormal activities that may need to be addressed.				
DS5.6 Security Incident Definition Clearly define and communicate the characteristics of potential security incidents so they can be properly classified and treated by the incident and problem management process.				
DS5.10 Network Security Use security techniques and related management procedures (e.g., firewalls, security appliances, network segmentation, intrusion detection) to authorize access and control information flows from and to networks.				
DS9.1 Configuration Repository and Baseline Establish a supporting tool and a central repository to contain all relevant information on configuration items. Monitor and record all assets and changes to assets. Maintain a baseline of configuration items for every system and service as a checkpoint to which to return after changes.				
DS9.2 Identification and Maintenance of Configuration Items Establish configuration procedures to support management and logging of all changes to the configuration repository. Integrate these procedures with change management, incident management and problem management procedures.				
DS9.3 Configuration Integrity Review Periodically review the configuration data to verify and confirm the integrity of the current and historical configuration. Periodically review installed software against the policy for software usage to identify personal or unlicensed software or any software instances in excess of current license agreements. Report, act on and correct errors and deviations.				
DS11.6 Security Requirements for Data Management Define and implement policies and procedures to identify and apply security requirements applicable to the receipt, processing, storage and output of data to meet business objectives, the organisation's security policy and regulatory requirements.				

VIII. Assessment Maturity vs. Target Maturity

This spider graph is an example of the assessment results and maturity target for a specific enterprise.