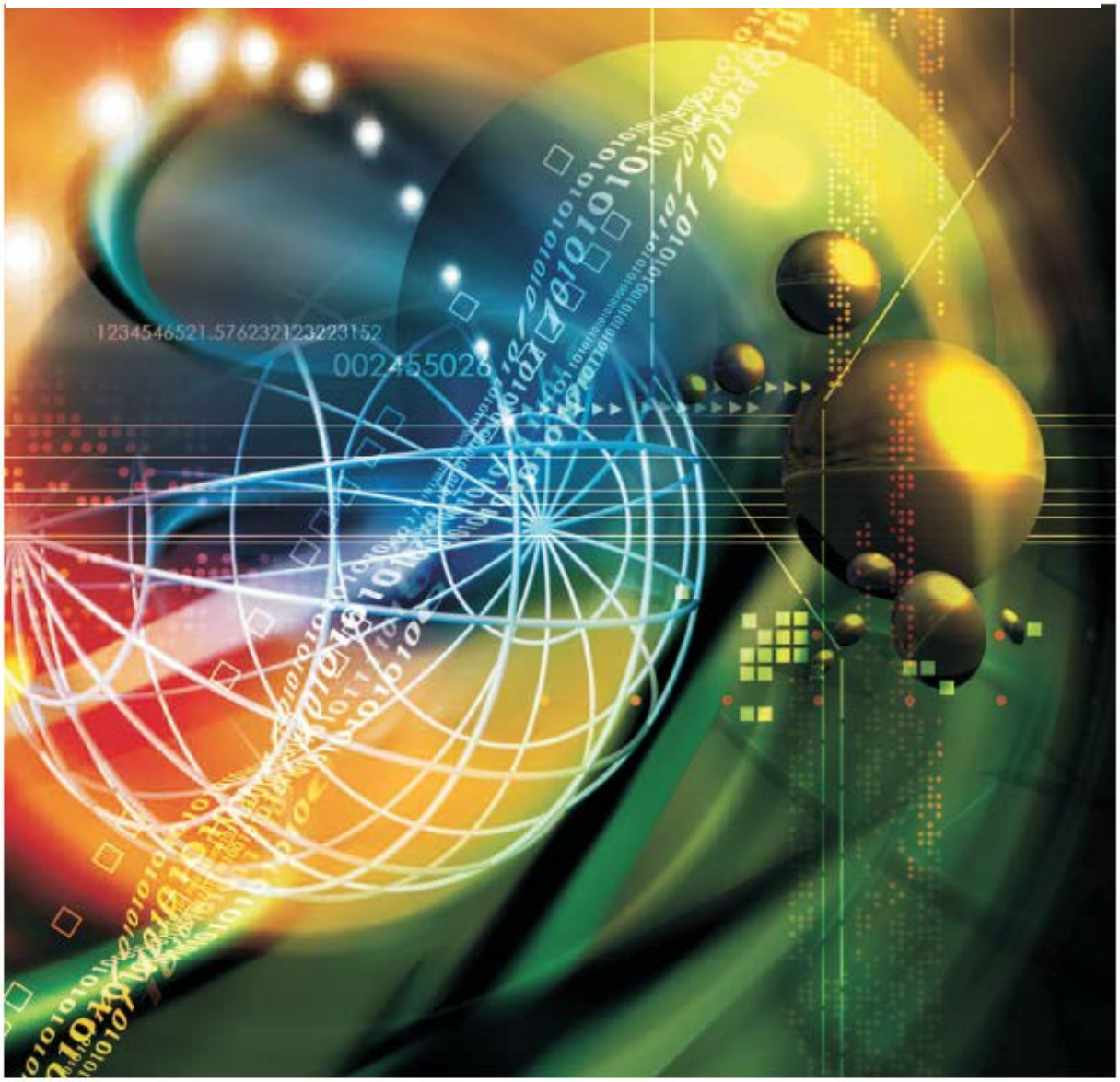
Windows® Active Directory® Audit/Assurance Program



ISACA®

Trust in, and value from, information systems

ISACA®
With more than 86,000 constituents in more than 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 of IT, and IT-related risk and compliance. Founded in 1969, ISACA sponsors international conferences, publishes the *ISACA® Journal*, and develops international IS auditing and control standards. It also administers 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 offers the Business Model for Information Security™ (BMIS™) and the IT Assurance Framework™ (ITAF™). It also developed and maintains the COBIT®, Val IT™ and Risk IT frameworks, which help IT professionals and enterprise leaders fulfill their IT governance responsibilities and deliver value to the business.

Disclaimer
ISACA has designed and created *Windows® Active Directory® 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 information technology environment.

Reservation of Rights
© 2010 ISACA. All rights reserved. No part of this publication may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise) without the prior written authorization of ISACA. Reproduction and use of all or portions of this publication are permitted solely for academic, internal and noncommercial use and for consulting/advisory engagements, and must include full attribution of the material's source. No other right or permission is granted with respect to this work.

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 978-1-60420-155-0
Windows® Active Directory® Audit/Assurance Program
Printed in the United States of America

CRISC is a trademark/service mark of ISACA. The mark has been applied for or registered in countries throughout the world.

Windows® Active Directory® Audit/Assurance Program is an independent publication and is not affiliated with, nor has it been authorized, sponsored or otherwise approved by Microsoft Corporation."

ISACA wishes to recognize:

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

Expert Reviewers
Anjay Agarwal, CISA, CGEIT, AAA Technologies Pvt. Ltd., India
Yves M. Dorleans, CISA, Charles River Laboratories, USA
Curt Hartinger, CISA, CISM, CPA, GSNA, MSIA, Oregon State Treasury, USA
Abdus Sami Khan, CIA, Sami Associates, Pakistan
William C. Lisse, Jr., CISA, CGEIT, CISSP, G7799, PMP, OCLC Inc., USA
Jack M. Redfield, CISM, Constellation Brands Inc., USA
Philippe Rivest, TransForce, Canada
Vinoth Sivasubramanian, ABRCCIP, CEH, ISO 27001 LA, UAE Exchange Center LLC, UAE
John G. Tannahill, CISM, CGEIT, CA, J. Tannahill & Associates, Canada
B.M. van Lodensteijn, CISA, CGEIT, Ordina Consultancy B.V., The Netherlands

ISACA Board of Directors
Emil D'Angelo, CISA, CISM, Bank of Tokyo-Mitsubishi UFJ Ltd., USA, International President
Hitoshi Ota, CISA, CISM, CGEIT, CIA, Mizuho Corporate Bank Ltd., Japan, Vice President
Jose Angel Pena Ibarra, CGEIT, Alintec S.A., Mexico, Vice President
Christos K. Dimitriadis, Ph.D., CISA, CISM, INTRALOT S.A., Greece, Vice President
Rolf M. von Roessing, CISA, CISM, CGEIT, KPMG Germany, Germany, Vice President
Robert E. Stroud, CGEIT, CA Technologies, USA, Vice President
Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA, Vice President
Ria Lucas, CISA, CGEIT, Telstra Corp. Ltd., Australia, Vice President
Everett C. Johnson Jr., CPA, Deloitte & Touche LLP (retired), USA, Past International President
Lynn C. Lawton, CISA, FBCS CITP, FCA, FIIA, KPMG Ltd., Russian Federation, Past International President
Gregory T. Grocholski, CISA, The Dow Chemical Co., USA, Director
Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Director
Howard Nicholson, CISA, CGEIT, CRISC, City of Salisbury, Australia, Director
Jeff Spivey, CPP, PSP, Security Risk Management, USA, ITGI Trustee

Knowledge Board
Gregory T. Grocholski, CISA, The Dow Chemical Co., USA, Chair
Michael Berardi Jr., CISA, CGEIT, Nestle USA, USA
John Ho Chi, CISA, CISM, CBCP, CFE, Ernst & Young LLP, Singapore
Jose Angel Pena Ibarra, CGEIT, Alintec S.A., Mexico
Jo Stewart-Rattray, CISA, CISM, CGEIT, CSEPS, RSM Bird Cameron, Australia
Jon Singleton, CISA, FCA, Auditor General of Manitoba (retired), Canada
Patrick Stachtchenko, CISA, CGEIT, CA, Stachtchenko & Associates SAS, France
Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA

Guidance and Practices Committee
Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA, Chair
Kamal Dave, CISA, CISM, CGEIT, Hewlett-Packard, USA
Urs Fischer, CISA, CRISC, CIA, CPA (Swiss), Switzerland
Ramses Gallego, CISM, CGEIT, CISSP, Entel IT Consulting, Spain
Phillip J. Lageschulte, CGEIT, CPA, KPMG LLP, USA
Ravi Muthukrishnan, CISA, CISM, FCA, ISCA, Capco IT Service India Pvt. Ltd., India
Anthony P. Noble, CISA, CCP, Viacom Inc., USA
Salomon Rico, CISA, CISM, CGEIT, Deloitte, Mexico
Frank Van Der Zwaag, CISA, CISSP, Westpac New Zealand, New Zealand

ISACA and IT Governance Institute Affiliates and Sponsors
American Institute of Certified Public Accountants
ASIS International
The Center for Internet Security
Commonwealth Association for Corporate Governance Inc.
FIDA Inform
Information Security Forum
Information Systems Security Association
Institut de la Gouvernance des Systèmes d'Information
Institute of Management Accountants Inc.
ISACA chapters
ITGI Japan
Norwich University
Solvay Brussels School of Economics and Management
University of Antwerp Management School
Analytix Holdings Pty. Ltd.
BWise B.V.
Hewlett-Packard
IBM
Project Rx Inc.
SOAProjects Inc.
Symantec Corp.
TruArx Inc.

© 2010 ISACA. All rights reserved.

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.

IT Governance, Risk and Control

IT governance, risk and control 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

© 2010 ISACA. All rights reserved.

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 will identify 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 holds the Certified Information Systems Auditor (CISA) designation, or has the necessary subject matter expertise required to conduct the work and is supervised by a professional with the 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 shown 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 the use of the program, the audit/assurance objective—the reason for performing the steps in the topic area—is described. The specific controls follow. Each review step is listed below 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 ISACA audit/assurance programs have adopted a maturity assessment process as documented in the *IT Assurance Guide: Using COBIT*. This audit/assurance program is technical in scope and does not lend itself to the maturity assessment. Accordingly, the maturity assessment will not appear in this document.

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 since it is standard for the audit/assurance function and should be identified elsewhere in the enterprise's standards.

© 2010 ISACA. All rights reserved.

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. Processes at lower levels 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 report 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. ERM is in the process of being adopted by large enterprises. 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.
	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 analyzed, 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.

© 2010 ISACA. All rights reserved.

Figure 1—Comparison of COSO Internal Control and ERM Integrated Frameworks	
Internal Control Framework	**ERM Integrated Framework**
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 these 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 for each line item, which describes the work performed, issues identified and conclusions. 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 describing the work performed.

III. Assurance and Control Framework

ISACA IT Assurance Framework and Standards

The ITAF section relevant to Windows Active Directory is 3630.14—Operating System (OS) Management and Controls.

© 2010 ISACA. All rights reserved.

ISACA Controls Framework

COBIT is a framework for the governance of IT and 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 secure and appropriate configuration management. Windows Active Directory is a component of most Windows implementations. Because this audit/assurance program only addresses the Active Directory design and maintenance, the following COBIT sections are only partially applicable:

- 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.

Refer to ISACA's *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.

IV. Executive Summary of Audit/Assurance Focus

Windows Active Directory

Windows Active Directory is the underlying technology within the Microsoft Windows operating system that provides for an integrated and single sign-on system that addresses security, access and identity management. The typical Windows environment is comprised of servers dedicated to specific tasks. Each device in an active directory domain trusts the Active Directory server and allows it to authenticate and approve the action that each user is trying to perform, either on the network or locally. Since the Windows architecture is decentralized, each server and workstation operates independently. Active Directory provides a central repository that contains user IDs, user permissions and audit processing. Active Directory allows for a centralized management of users and their security. Active Directory is implemented on Domain Controllers, which control the various users and computers within the controller's scope. The key issue to a secure Active Directory is the configuration settings established during its implementation, and the maintenance of this configuration during the life cycle of the Active Directory.

Business Impact and Risk

Active Directory has a pervasive effect on the business. Most enterprise users require access to a computer system, whether it is their desktop computer, mobile laptop computer or a workstation connected to a corporate resource. The single sign-on, access controls and security are controlled from Active Directory. Active Directory allows for a centralized management of users and their security.

© 2010 ISACA. All rights reserved.

Failure to design and manage effective Active Directory controls could result in:
- Disruption of computing services
- Destruction of enterprise data
- Disclosure of sensitive information, including identities, intellectual property, etc.
- Reputational risk and loss of confidence by stakeholders, business partners and customers due to disclosure of information or related publicity
- Fines and penalties
- Lost productivity due to inefficient security administration
- Security breaches

Objective and Scope

Objective—The Active Directory audit/assurance review will:
- Provide management with an evaluation of the Active Directory implementation and management security design effectiveness
- Provide management with an independent assessment of the operating effectiveness of the security controls

Scope—Windows server implementations operate with various functions and software. This review evaluates the necessary secure Active Directory infrastructure to support the servers and workstations within the enterprise. The review will focus on the configuration controls relating to:
- Active Directory management
- Secure Active Directory boundaries
- Secure domain controllers
- Physical security of the domain controllers
- Secure domain and domain controller configuration settings
- Secure administrative practices

The scope excludes:
- Windows server configurations
- Workstation configurations
- User access and identity management
- Domain Name Service (DNS) management

It is recommended that:
- Windows server configuration assessments be performed using an audit/assurance program specifically designed for the server's function (web, e-mail, file/print, etc.)
- 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 use the ISACA *Identity Management Audit/Assurance Program*
- DNS management be approached as part of a network assessment

Minimum Audit Skills

Active Directory is a technical topic requiring a thorough understanding of the underlying technologies and functionality of Active Directory. The audit and assurance professional should have the requisite knowledge of Active Directory, its 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 Active Directory, utilizing this program as a checklist.

© 2010 ISACA. All rights reserved.

V. 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 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 boundaries of review.** The review must have a defined scope. The reviewer should understand the operating environment and prepare a proposed scope, subject to a later risk assessment.									
1.2.1 Obtain Active Directory Design documentation.									
1.2.2 Obtain and review the Active Directory Topology.									
1.2.3 Determine if the entire forest will be included within the scope of the audit.									
1.2.4 Obtain enterprise, process and information architecture, and align this as reference to the Active Directory topology.									
1.2.5 Determine if separation of any forests would create or ignore key risks.									
1.2.6 Obtain and review security policies and previous audit reports with remediation plans.									
1.2.7 Obtain and review any previous audit reports with remediation plans. Identify open issues, and assess updates of documents with respect to these issues.									
1.2.8 Identify limitations and/or constraints affecting the audit of specific systems.									
1.3 **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.									
1.3.1 Determine if the applications operating within the Active Directory are assessed at the highest risk rating.									
1.3.2 Document relevant Active Directory criteria as required by regulatory requirements (i.e., Payment Card Industry-Data Security Standard [PCI-DSS], US Sarbanes-Oxley Act, US Health Insurance Portability and Accountability Act [HIPAA]) or governmental organizations.									

© 2010 ISACA. All rights reserved.

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			
1.3.3 Review previous audits of Active Directory.									
1.3.4 Determine if issues identified previously have been remediated.									
1.3.5 Evaluate the overall risk factor for performing the review.									
1.3.6 Based on the risk assessment, identify changes to the scope.									
1.3.7 Discuss the risks with IT management, and adjust the risk assessment.									
1.3.8 Based on the risk assessment, revise the scope.									
1.4 **Define the audit change process.** The initial audit approach is based on the reviewer's understanding of the operating environment and associated risks. As further research and analysis are performed, changes to the scope and approach will result.									
1.4.1 Identify the senior IT assurance resource responsible for the review.									
1.4.2 Establish the process for suggesting and implementing changes to the audit/assurance program and the authorizations required.									
1.5 **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.									
1.5.1 Identify the drivers for a successful review (this should exist in the assurance function's standards and procedures).									
1.5.2 Communicate success attributes to the process owner or stakeholder, and obtain agreement.									
1.6 **Define 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 resources (hours) and time frame (start and end dates) required for the review.									
1.6.3 Determine the Active Directory reporting and analysis tools available to the auditor.									
1.6.4 Determine that the appropriate permissions have been granted to allow the auditors to execute the auditing tools and that appropriate security controls have been implemented to prevent the auditor from making any changes to the configuration.									
1.7 **Define deliverables.** The deliverable is not limited to the final report. Communication between the audit/assurance teams									

© 2010 ISACA. All rights reserved.

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			
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 **Communications** The audit/assurance process must be clearly communicated to the customer/client.									
1.8.1 Conduct an opening conference to discuss the review objectives, timeline, scope, etc., with the Active Directory assessment.									
2. ACTIVE DIRECTORY MANAGEMENT									
2.1 **Active Directory Management Organization** Audit/Assurance Objective: The organization responsible for Active Directory reports to appropriate management responsible for technical and security services.									
2.1.1 **Active Directory Administrative Management** Control: Active Directory organization reports to a technical support management group that has technical competency of the process.	PO4.11 PO7.5 PO7.6	x			x				
2.1.1.1 Obtain an organization chart describing the Active Directory job descriptions, reporting relationships and incumbent personnel assigned to each position.									
2.1.1.2 Identify the individuals responsible for: • Establishing Active Directory policy • Monitoring adherence to Active Directory policy • Domain controllers • Service administration • Data administration • Root domains • Enterprise administrators • Schema administrators • Domain administrators • Information/application architecture • Forest owners • Backup operators • Outlook e-mail systems									

© 2010 ISACA. All rights reserved.

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			
2.1.1.3 Evaluate the separation of duties of these job responsibilities and, by lack of this, additional compensating controls.									
2.1.1.4 Determine if the key administration personnel are bonded and have been subject to background verification.									
2.1.1.4.1 Obtain and inspect bonding and background reports.									
2.1.2 **Information Security Function Oversight** Control: The information security function participates and monitors Active Directory activities involving the information security architecture and function.		x		x		x			
2.1.2.1 Determine if the information security function is actively involved in the establishment and enforcement of Active Directory information policy and standards.									
2.1.2.1.1 Obtain policy documents, and verify information security function review and approval.									
2.1.2.1.2 Obtain minutes of meetings to verify involvement.									
2.1.2.2 Determine if the information security function receives appropriate reports, dashboards, etc., to ensure security enforcement.									
2.1.2.3 Obtain reports and dashboards distributed to the information security function. Determine if there is evidence of review and that evidence of security issues addressed are followed up in a timely manner.									
2.2 **Active Directory Risk Management** Audit/Assurance Objective: Risk management is an integral part of Active Directory management activities.									
2.2.1 **Risk Management** Control: Active Directory management participates in an active risk management program.	PO9	x	x		x	x			
2.2.1.1 Determine if the Active Directory risk programs align with the overall IT risk management process.									
2.2.1.2 Determine that Active Directory management performs annual risk assessments of the effect Active Directory has on the control environment.									
2.2.1.2.1 Obtain and inspect annual risk assessment documentation.									

© 2010 ISACA. All rights reserved.

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			
2.2.1.3 Determine that Active Directory management prepares a residual risk profile identifying significant risks, and review the documents to determine management follow-up.									
2.2.1.3.1 Obtain and inspect risk issue monitoring documentation.									
2.2.1.4 Determine that the Information Security function participates in the risk management function.									
2.2.1.4.1 Obtain risk management meeting minutes and other documentation to determine information security involvement.									
2.3 **Active Directory Management Reporting** Audit/Assurance Objective: The Active Directory management function routinely reports activities (including problems, changes, incidents, performance and identified risks) to IT management.									
2.3.1 **Management Reporting** Control: Active Directory Management provides IT management with performance reports and incident reports on a regular basis.				x	x	x			
2.3.1.1 Obtain management reports, minutes of meetings, etc., that document Active Directory management communications and status reports.									
2.3.1.2 Determine that the information security function receives and acts upon security issues by reviewing management reports and information security incident reports/logs.									
3. SECURE ACTIVE DIRECTORY BOUNDARIES									
3.1 **Active Directory Secure Design** Audit/Assurance Objective: The design of the Active Directory supports security objectives and good practices.									
3.1.1 **Active Directory Boundaries** Control: Active Directory boundaries are documented and provide the structure of organizational requirements.		x		x					
3.1.1.1 Obtain a hierarchal representation of the Active Directory structure, beginning with the forest(s).									
3.1.1.2 Determine if the organization requires a centralized, decentralized or hybrid									

© 2010 ISACA. All rights reserved.

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			
administration structure.									
3.1.1.3 Determine the directory structure; consider: • Single domain • Single forest with multiple domains • Separate forests • Information/application architecture • Forest owners									
3.1.2 **Active Directory Design** Control: Active Directory design balances the need for autonomy and isolation in its design.	PO4.11	x	x						
3.1.2.1 Determine if the forest structure provides for a separation between service administrators (responsible for Active Directory design and highest level of administration) and data administrators (responsible for user credentials, access rights, etc.).									
3.1.2.1.1 Obtain a list of all forest owners.									
3.1.2.1.2 Determine that all forest owners are trusted and that appropriate background verification has been completed for each owner.									
3.1.2.1.3 Determine that the responsibility of the forest owners does not preclude trust between the forests for which they are responsible.									
3.1.2.1.4 Determine if possible conflictive independencies exist between the domains (functional, technical, operational and independencies between business processes, i.e., accounts payable vs. accounts receivable or payments and securities, etc.).									
3.1.2.1.5 If all domains in a forest are not under the same owner, identify controls to prevent enterprise administrators in the forest root from administering domains with different owners.									
3.1.2.2 Determine if an extranet is utilized in the Active Directory implementation and if it is isolated from the rest of the forest.									
3.1.2.3 Determine that service administrators responsible for intranet and extranet forests have separate, isolated user IDs for each internal and external forest.									
3.1.3 **Active Directory Features** Control: The Active Directory features are implemented for the most secure version.				x					

© 2010 ISACA. All rights reserved.

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			
3.1.3.1 Identify the inventory of Windows Server versions (2000, 2003 and 2008).									
3.1.3.2 Determine if Active Directory has been implemented for the appropriate mix of servers and that the version is the lowest common version.									
3.1.3.3 Obtain a list of the most actual security patches/service packs, and determine if these are implemented on all servers.									
3.1.4 **Forest Trust** Control: The forest trust is configured for maximum security.	PO4.11	x		x					
3.1.4.1 Determine if a forest trust has been established between forests.									
3.1.4.2 Determine that external trusts are permitted with prior authorization.									
3.1.4.3 Determine that appropriate administrative controls exist to prevent unauthorized granting of trusts between forests. (All requests for trust relationships should be included in a service request, the service request should be approved by an individual responsible for the trust relationships, the audit logs should indicate when the relationship was assigned and by whom, and the log should be verified to the service request).									
3.1.4.4 Determine that users from other forests are not members of the groups that: ▪ Are responsible for service management or manage membership of service administrator groups. ▪ They have administrative control over computers that store protected data. ▪ They have access to protected data or responsible for management of user or group objects having access to protected data. Special considerations should be made for the IT department that spans the globe, with individuals responsible for forests not in their geographic locations.									
4. SECURE DOMAIN CONTROLLERS									
4.1 **Secure Domain Controller Build Practices** Audit/Assurance Objective: Domain controllers are built to standard configuration specifications that have been approved, are documented and subscribe to good security practices.									
4.1.1 **Physical Security of Domain Controller Build** Control: Domain controllers are built in a controlled environment.	DS12			x					

© 2010 ISACA. All rights reserved.

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			
4.1.1.1 Determine if domain controllers are built in a datacenter or in a secure physical facility.									
4.1.1.2 Determine if completed domain controllers are transported to a final destination in a controlled manner, not subject to unauthorized access. If shipment is required, determine that a delivery signature is required and that procedures require inspection for tampering with the shipping container.									
4.1.2 **Domain Controller Build** Control: Domain controllers are built using a standard installation procedure that is repeatable, using only approved configuration options.	DS9			x					
4.1.2.1 Determine if a domain controller build procedure is documented, and obtain the procedure.									
4.1.2.2 Obtain the change log to determine that changes to the build procedure and configuration are approved and documented.									
4.1.2.3 Determine if the System Preparation Tool (SYSPREP) is used to clone preconfigured operating system configurations.									
4.1.2.4 If answer-file-based installation is used to build systems, determine whether the controls over the answer file are adequate to prevent unauthorized configurations from being introduced into the build process.									
4.2 **Domain Controller Configuration** Audit/Assurance Objective: Domain controllers are built with appropriate security configuration and virus/malware safeguards.									
4.2.1 **Antivirus Software on Domain Controllers** Control: Domain controllers have antivirus software with routine execution of virus scans.	DS5 DS9			x					
4.2.1.1 Determine if antivirus software has been installed on the domain controllers and if the virus signature files are updated regularly.									
4.2.1.2 Determine if critical operating system files have been excluded from the virus scans, according to the specifications of Microsoft and the virus vendor.									
4.2.2 **Scripts** Control: Domain controllers and administrative workstations can execute only signed				x					

© 2010 ISACA. All rights reserved.

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			
scripts.									
4.2.2.1 Determine if the group policy for domain controllers restricts script execution to only signed scripts. (This requires establishing an internal certification authority.)									
4.2.2.2 Determine if a group policy exists to prevent administrative workstations (those that manage the domain controllers) from executing unsigned scripts.									
4.2.2.3 Determine if antivirus software can be disabled or removed.									
4.2.2.4 Determine if the antivirus alerts have been investigated and acted upon according to the antivirus policy.									
4.2.3 **Domain Controller Deployment** Control: Domain controller deployment practices require secure configurations.									
4.2.3.1 Determine that the following settings are included in the build of the domain controllers: • All drives are formatted with New Technology File System (NTFS). • The only communication transport protocol is Transmission Control Protocol (TCP)/Internet protocol (IP). • Simple Mail Transport Protocol (SMTP) is disabled unless mail-based intersite Active Directory is required. • Domain name server (DNS) is selected in the networking category.									
4.2.3.2 Determine that administrative procedures are in effect to require passwords with the following characteristics: • Password length is at least nine characters. • Passwords are not easily identified with the enterprise or staff, and are not in a dictionary. • Passwords are unique and do not follow a pattern when passwords are changed. • Passwords contain symbols, numbers and one alpha letter in upper case.									
4.2.3.3 Determine that only the essential services are installed on the domain controllers. All services should have the default service type, except for the following: • Application Management can be set to Disabled to prevent the use of Add or Remove Programs, and can be started when needed. • Distributed Link Tracking Client: set to Disabled									

© 2010 ISACA. All rights reserved.

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			
• Fax: Disabled • Internet Information Services (IIS) Admin Service: Disabled • Indexing Service: Disabled • Portable Media Serial Number Service: Disabled • Shell Hardware Detection: Disabled • SMTP: Disabled • Special Administrator Console Helper: Disabled (Enable if Emergency Management Services [EMS] is used for access to console.) • Upload Manager: Disabled • Utility Manager: Disabled • Windows Audio: Disabled									
4.2.3.4 Determine if a reserve file has been created to enable recovery from disk-space attacks. If a large file that takes up considerable space is established on the domain controller, in the event of a disk-space attack, the file can be deleted to allow the Active Directory file to expand to maintain normal operations while the AD is examined for unauthorized AD entries.									
5. PHYSICAL SECURITY									
5.1 **Physical Access to Domain Controllers** Audit/Assurance Objective: Domain controllers are secured with appropriate physical access controls to prevent unauthorized access or interference with domain controller functions.									
5.1.1 **Domain Controller Access** Control: Domain controllers are stored in locked rooms with limited access.	DS11 DS12			x					
5.1.1.1 Determine, by observation and inspection, that domain controller computers are stored in locked rooms.									
5.1.1.2 Determine the types of locks used and if the access codes can be changed frequently.									
5.1.1.2.1 Verify that the lock codes had been changed routinely via inspection of the logs.									
5.1.1.3 Determine the responsibilities of each individual having access to the domain controller room.									
5.1.1.3.1 Obtain a listing of the individuals having access to the domain controller room.									

© 2010 ISACA. All rights reserved.

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			
5.1.1.3.2 Based on their job descriptions, determine if they require access to the domain controller room.									
5.1.1.4 Scan the access logs for unusual access activity, including individuals not on the access list, frequent access by anyone on the list, etc.									
5.1.1.5 Determine if rack locks are required to safeguard the domain controllers.									
5.1.2 **Domain Controller Access Monitoring** Control: Physical access to domain controllers are logged and monitored.				x		x			
5.1.2.1 Determine if there are logging devices to record access to the domain controller rooms.									
5.1.2.2 Determine if there are access logs to record access to the domain controllers.									
5.1.2.3 Determine if incident reports are required when a domain controller is modified or rebooted.									
5.1.2.4 Scan the access logs for unusual activities.									
5.1.2.5 Obtain the event log for the domain controller, and compare any reboots or other administrative activities to incident logs.									
5.1.3 **Domain Controller Availability** Control: Domain controllers remain available during a power failure and have an appropriate graceful shutdown for extended power failures.				x					
5.1.3.1 Determine if uninterrupted power supply (UPS) equipment is installed for domain controllers.									
5.1.3.2 Determine if UPS equipment has been tested.									
5.1.3.3 Determine if adequate air conditioning is available.									
5.1.4 **Domain Controller Reboot** Control: Domain controllers reboot automatically after a power failure.									
5.1.4.1 Determine that the domain controller will automatically boot upon return of power without operator intervention.									
5.1.4.2 Physically verify if the domain controllers have been fitted with dual-power supplies.									

© 2010 ISACA. All rights reserved.

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			
5.1.5 **Domain Controllers Booting Alternate OS** Control: Prevent the domain controllers from booting using an unauthorized operating system.				x					
5.1.5.1 Assess the vulnerability of the domain controller to being booted from an unauthorized operating system.									
5.1.5.2 Consider the physical security of the server room, locks on the rack cabinet and the accountability of those authorized to enter the server room.									
5.1.5.3 Determine whether additional security controls are required, including: • Use SYSKEY (prevents booting without a password or physical key device). • Disable boot from all devices except boot disk (CD-ROM, floppy drive, Universal Serial Bus [USB] drive, Bootstrap Protocol [BOOTP] network, etc.). • Set the (timeout) parameter in the Boot.ini file to 0.									
5.1.6 **Securing Backup Media Against Physical Access** Control: Domain controllers are routinely backed up, the backup data are secured against unauthorized access, and only authorized backup data are used for restores.				x					
5.1.6.1 Determine the frequency and process for backing up the domain controllers.									
5.1.6.2 Determine where the backups are stored, the security of the storage and the intermediate transport mechanism (physical and network).									
5.1.6.3 Review the procedures for restoring a domain controller.									
5.1.6.4 Evaluate the manual controls to ensure that only an authorized data file can be used in the restoration process.									
5.1.6.5 Determine if logs are maintained to document restoration processes.									
5.1.6.6 Determine if data transport procedures require signatures to evidence receipt of data.									
5.1.6.7 Determine if the restore process is documented. Review the restore process for design effectiveness.									
5.1.6.8 Determine if the restore process has been tested on a test domain controller.									
5.1.6.9 Evaluate the test process and results, and determine if they are aligned to the actual									

© 2010 ISACA. All rights reserved.

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			
disaster recovery requirements.									
5.2 **Security of Network Infrastructure** Audit/Assurance Objective: The network infrastructure has been configured to provide a secure operating environment.									
5.2.1 **Securing Cabling Rooms** Control: Cabling rooms are locked with limited access, and access to cabling rooms is logged and managed.	DS5 DS9			x		x			
5.2.1.1 Determine that cabling rooms are locked.									
5.2.1.2 Determine the types of locks used and if the access codes can be changed frequently.									
5.2.1.3 Determine the business or technical need of each individual having access to the cabling room.									
5.2.1.4 Scan the access logs for unusual access activity.									
5.2.2 **Secure Network Segments** Control: Domain controllers are protected from Internet/extranet traffic.	DS5 DS9	x		x					
5.2.2.1 Obtain a network schematic.									
5.2.2.2 Determine if all domain controllers are secured with a dedicated firewall and network controls (such as a virtual local area network [VLAN]). Ensure that the domain controllers cannot be directly reached by the Internet.									
5.2.2.3 Determine that any domain controllers located outside the corporate intranet connect to replicate to the corporate domain controllers through virtual private networks (VPNs). Verify VPN policies concerning this matter.									
5.2.3 **Domain Controller out of Band Management** Control: Domain controllers are connected to an out-of-band management network.				x					
5.2.3.1 Determine if domain controllers are connected to a dedicated management network port on the domain controller (typically a separate Ethernet connection).									
5.2.3.2 If a management network is in use, determine that: • It is segmented from other networks. • Service administration workstations are the only workstations that can connect to									

© 2010 ISACA. All rights reserved.

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			
the out-of-band network. • Highly secure identity management and access controls are in effect.									
5.2.4 **Securing Remote Restart of Domain Controllers** Control: Remote reboot of domain controllers is secured to prevent unauthorized access during reboot and while providing for remote administration and rebooting of the domain controller.				x					
5.2.4.1 Determine that datacenter-based domain controllers are installed with a remote access hardware device to allow connectivity through a separate serial or Ethernet connection.									
5.2.4.2 Determine that the remote restart network is segmented from other networks.									
5.2.4.3 Determine that remote-based domain controllers are installed with a dedicated modem and telephone line that includes a password and dial-back feature to a specific telephone number.									
5.2.5 **Firewall Configuration** Control: Firewall configuration and security adheres to best practices (such as the US National Institute of Standards and Technology [NIST]).				x					
5.2.5.1 Perform a perimeter security audit of the firewalls protecting the domain controllers. If possible, rely upon a separate audit of perimeter security.									
5.3 **Domain and Domain Controller Policy Settings** Audit/Assurance Objective: Domain and domain controller policy settings are secure.									
5.3.1 **Domain Security Policy Settings** Control: Domain security policy settings provide appropriate security for the domain.	DS5			x					
5.3.1.1 Obtain domain security policy settings. Determine if the settings adhere to good practices.									
5.3.1.2 Determine that the domain policy settings only address account policies.									
5.3.1.3 Determine that the password policy settings follow the domain policy settings. The values given below are minimums and are a guideline only: • Enforce password history: default, 24 passwords remembered • Maximum password age: default, 42 days. Change to local option; 42 days is recommended, but can be overridden for individual users.									

© 2010 ISACA. All rights reserved.

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			
• Minimum password age: default, 1 day. Prevent cycling passwords. • Minimum password length: default, nine characters • Password must meet complexity requirements: default, enabled • Store password using reversible encryption: default, disabled									
5.3.1.4 Determine that domain account lockout policies follow enterprise policy and are adequate, using the following guidelines: • Account lockout duration: 0 (requires administrator to re-enable account after lockout) • Account lockout threshold: three to five (number of attempts before account is locked and administrator intervention is required) • Reset account lockout counter after: set this number in minutes—consider that the account will be re-enabled after the number of minutes entered here									
5.3.1.5 Determine that domain Kerberos policy settings are set to default: • Enforce user logon restrictions: Enabled • Maximum lifetime for service ticket: 600 minutes • Maximum lifetime for user ticket: 10 hours • Maximum lifetime for user ticket renewal: 7 days • Maximum tolerance for computer clock synchronization: 5 minutes									
5.3.2 **Domain Controller Audit Policy Settings** Control: Domain controller audit policy settings are set to record appropriate events.				x					
5.3.2.1 Determine that domain controller audit policy settings are set to default: • Audit account logon events: Success • Audit account management: Success • Audit directory service access: Success • Audit logon events: Success • Audit object access: No auditing (N/A) • Audit policy change: Success • Audit privilege use: No auditing (N/A) • Audit process tracking: No auditing (N/A) • Audit systems events: Success									
5.3.3 **Domain Controller User Rights Policy Setting**				x					

© 2010 ISACA. All rights reserved.

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			
Control: Domain controller user rights policy settings are set to allow administration of domain without compromising security of the domain controller.									
5.3.3.1 Determine that the domain controller user rights assignment policy settings are as follows: • Policy: Allow logon locally; Setting: Administrators, Backup Operators, Server Operators • Policy: Shut down the system; Setting: Administrators, Backup Operators, Server Operators									
5.3.4 **Domain Controller Security Options Policy Setting** Control: Domain controller security options policy settings provide security over the domain controller.				x					
5.3.4.1 Determine that the domain controller security policies are defined to a separate group policy object (GPO) and that the GPO is linked to the domain controller organizational unit (OU) above the level of the default domain controller GPO.									
5.3.4.2 Determine that the domain controller security policy options are set as follows: • Audit the access of global system objects: Disabled • Audit: Audit the use of Backup and Restore privileges: Disabled • Audit: Shut down system immediately if unable to log security audits: Disabled • Devices: Allow undock without having to logon: Disabled • Devices: Allowed to format and eject removable media: Administrators • Devices: Prevent users from installing printer drivers: Enabled • Devices: Restrict CD-ROM access to locally logged-on user only: Enabled • Devices: Restrict floppy access to locally logged-on user only: Enabled • Devices: Unsigned driver installation behavior: Do not allow installation • Domain controller: Allow server operators to schedule tasks: Disabled • Domain controller: Refuse machine account password changes: Disabled • Domain member: Digitally encrypt or sign secure channel data (always): Enabled • Domain member: Disable machine account password changes: Disabled • Domain member: Maximum machine account password age: 30 days • Domain member: Require strong (Windows 2000 or later) session key: Enabled • Interactive logon: Do not display last user name: Enabled									

© 2010 ISACA. All rights reserved.

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			
• Interactive logon: Do not require CTRL+ALT+DEL • Interactive logon: Number of previous logons to cache (in case the domain controller is not available): 0 logons • Interactive logon: Prompt user to change password before expiration: 14 days • Interactive logon: Require domain controller authentication to unlock workstation: Enabled • Interactive logon: Require smart card: preferred setting is enabled for domain controllers and administrative workstations, and disabled if not in use • Interactive logon: Smart card removal behavior: Force logoff (if smart card is removed during session) • Network access: Do not allow storage of credentials or Windows Live ID for network: Enabled • Network access: Restrict anonymous access to Named Pipes and Shares: Enabled • Network security: Lightweight Directory Access Protocol (LDAP) client signing requirements: Require signing (Windows 2003 Server); Negotiate signing (Windows 2008 Server) • Recovery console: Allow floppy copy and access to all drives and folders: Disabled • Shutdown: Allow system to be shut down without having to logon: Disabled • Shutdown: Clear virtual memory pagefile: Enabled • System objects: Strength default permissions of internal system objects: Enabled • System settings: Optional subsystems: Blank if Posix is not required, otherwise Posix • System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies: not defined unless public key infrastructure (PKI) is set up—consult internal documentation									
5.3.4.3 Determine that LAN manager authentication has been disabled.									
5.3.5 **Domain Controller Event Log Policy** Control: Domain controller event log policy settings provide maximum documentation of activities.		x		x	x	x			
5.3.5.1 Determine that the domain controller event log policy settings are as follows: • Maximum application log size: Not defined									

© 2010 ISACA. All rights reserved.

<table>
<tr><th rowspan="2">Audit/Assurance Program Step</th><th rowspan="2">COBIT Cross-reference</th><th colspan="5">COSO</th><th rowspan="2">Reference Hyper-link</th><th rowspan="2">Issue Cross-reference</th><th rowspan="2">Comments</th></tr>
<tr><th>Control Environment</th><th>Risk Assessment</th><th>Control Activities</th><th>Information and Communication</th><th>Monitoring</th></tr>
<tr><td>• Maximum security log: 131,072 kb
• Maximum system log size: Not defined
• Prevent local guests group from accessing application log: Enabled
• Prevent local guests group from accessing security log: Enabled
• Retain application log: Not defined
• Retain system log: Not defined
• Retain system log: Not defined
• Retention method for application log: Not defined
• Retention method for security log: Overwrite events as needed
• Retention method for system log: Overwrite events as needed</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>5.3.5.2 Determine that a formal risk assessment took place between process owners and IT staff concerning identification of other than previously mentioned events.</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>5.3.6 Important Active Directory Objects
Control: Important Active Directory objects are properly secured.</td><td>DS5</td><td></td><td></td><td>x</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>5.3.6.1 Determine that the default audit settings for the Schema Directory Partition (CN=Schema, CN=Configuration, DC=ForestRootDomain), which report any schema container object additions, deletions or modifications, are implemented.
Note: Common name is CN, and domain component is DC.
<table>
<tr><th>Type</th><th>Name</th><th>Access</th><th>Apply To</th></tr>
<tr><td rowspan="6">Success</td><td>Everyone</td><td>Modify Permissions
Modify Owner
Create All Child Objects
Delete
Delete All Child Objects
Delete Subtree</td><td>This object only</td></tr>
<tr><td>Everyone</td><td>Write All Properties</td><td>This object and all child objects</td></tr>
<tr><td>Everyone</td><td>Change Schema Master</td><td>This object only</td></tr>
<tr><td>Everyone</td><td>Reanimate Tombstones</td><td>This object only</td></tr>
<tr><td>Administrators</td><td>All Extended Rights</td><td>This object only</td></tr>
<tr><td>Domain Users</td><td>All Extended Rights</td><td>This object only</td></tr>
</table></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>5.3.6.2 Determine that the default audit settings for the Configuration Container</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

© 2010 ISACA. All rights reserved.

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			
(CN=Configuration, DC=ForestRootDomain), which report any modifications to the permissions and the WellKnownObjects attribute on the configuration directory partition, are implemented:									

Type	Name	Access	Apply To
Success	Everyone	Modify Permissions Modify Owner Create All Child Objects Write All Properties	This object only
	Everyone	Reanimate Tombstones	This object only
	Administrators	All Extended Rights	This object only
	Domain Users	All Extended Rights	This object only

5.3.6.3 Determine that the default audit settings in the Configuration Directory Partition for CN=Sites, CN=Configuration, DC=ForestRootDomain include the following:

- Addition and removal of domain controllers in the forest
- Addition and removal of the Group Policy Setting that are applied to a site
- Association and disassociation of the subnet with a site
- Execution of the Do Garbage Collection, Recalculate Hierarchy, Recalculate Security Inheritance, and Check Stale Phantoms on a domain controller
- Addition, removal and modification of site links
- Addition, removal and modification of connections

Type	Name	Access	Apply To
Success	Everyone	Create All Child Objects Delete Delete All Child Objects Delete Subtree	This object only and all child objects
	Everyone	All Extended Rights	Domain Controller Settings objects
	Everyone	Write gPLink (property) Write gPOptions (property)	Site objects
	Domain Users	All Extended Rights	This object only

5.3.6.4 Determine that the default audit settings in the Configuration Directory Partition for CN=Partitions, CN=Configuration, DC=ForestRootDomain include the following:

- Addition and removal of domains (or external directory knowledge references) in

© 2010 ISACA. All rights reserved.

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			
the forest • Modifications to valid user principal name (UPN) suffixes for the forest • Transfer of the domain naming operations master role Type: Success; Name: Everyone; Access: Modify Permissions, Modify Owner, Write All Properties, Create All Child Objects, Delete, Delete All Child Objects, Delete Subtree, All Extended Rights; Apply To: This object only and all child objects									
5.3.6.5 Determine that the default audit settings that control changes to the dSHeuristics attributes (controls certain forestwide behavior of the directory service) in the Configuration Directory Partition for CN=DirectoryService, CN=Windows, CN=Services, CN=Configuration, DC=ForestRootDomain include the following: Type: Success; Name: Everyone; Access: Write dSHeuristics (property); Apply To: This object only									
5.3.6.6 Determine that the default audit settings for changes to forestwide parameters that govern the behavior of LDAP-based queries and operations for CN=Default Query Policy, CN=Query-Policies, CN=DirectoryServices, CN=Windows NT, CN=Services, CN=Configuration, DC=ForestRootDomain include the following: Type: Success; Name: Everyone; Access: Write IDAPAdminLimits (property); Apply To: This object only									
5.3.6.7 Determine that the default audit settings in the Domain Directory Partition for CN=domain DC=ForestRootDomain include the following: • Addition and removal of group policy settings that are applied to the domain • Modifications to valid DNS suffixes for the domain • Modifications to the permissions and the WellKnownObjects attribute on the domain directory partition • Migration of the security identifier (SID) history (user account object attribute that facilitates the authorization process when migrating Windows domains)									

© 2010 ISACA. All rights reserved.

Audit/Assurance Program Step	COBIT Cross-reference	COSO: Control Environment	COSO: Risk Assessment	COSO: Control Activities	COSO: Information and Communication	COSO: Monitoring	Reference Hyper-link	Issue Cross-reference	Comments
<table><tr><th>Type</th><th>Name</th><th>Access</th><th>Apply To</th></tr><tr><td rowspan="4">Success</td><td>Everyone</td><td>Modify Permissions Modify Owner Write All Properties</td><td>This object only</td></tr><tr><td>Administrators</td><td>All Extended Rights</td><td>This object only</td></tr><tr><td>Domain Users</td><td>All Extended Rights</td><td>This object only</td></tr><tr><td>Everyone</td><td>Write gPLink Write gPOptions</td><td>Organizational Unit objects</td></tr></table>									
5.3.6.8 Determine that the default audit settings in the Domain Directory Partition for OU=Domain Controllers, DC=domain, DC=…ForestRootDomain include the following: • Addition and removal of domain controllers from the domain • Modification to any properties of domain controller computer accounts <table><tr><th>Type</th><th>Name</th><th>Access</th><th>Apply To</th></tr><tr><td rowspan="3">Success</td><td>Everyone</td><td>Modify Permissions Modify Owner Create All Child Objects Delete Delete All Child Objects Delete Subtree</td><td>This object only</td></tr><tr><td>Everyone</td><td>Write All Properties</td><td>This object only and all child objects</td></tr><tr><td>Everyone</td><td>All Extended Rights Write All Properties</td><td>This object only</td></tr></table>									
5.3.6.9 Determine that the default audit settings for modifications to the special security descriptor that protects all service administrator accounts for CN=AdminSDHolder, CN=System, DC=domain, DC=...ForestRootDomain are: <table><tr><th>Type</th><th>Name</th><th>Access</th><th>Apply To</th></tr><tr><td>Success</td><td>Everyone</td><td>Modify Permissions Modify Owner Write All Properties</td><td>This object only</td></tr></table>									
5.3.6.10 Determine that the default audit settings for transfer of the relative ID (RID)									

© 2010 ISACA. All rights reserved.

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			
operations master role CN=RIDManager$, CN=System, DC=domain, DC=ForestRootDomain are: Type: Everyone; Name: Everyone; Access: All Extended Rights, Write All Properties; Apply To: This object only									
6. SECURE ADMINISTRATIVE PRACTICES									
6.1 **Service Administration** Audit/Assurance Objective: Administrative practices involving the service administrator accounts and service administration workstations are designed to prevent unauthorized activities from affecting Active Directory operations.				x					
6.1.1 **Service Administrator Account Limitations** Control: Limit the number of service administrator accounts.	DS5								
6.1.1.1 Obtain a list of service administrator accounts.									
6.1.1.2 Determine that the listed service administrators are the only users having service administrator access.									
6.1.1.3 Assess whether the number of service administrator accounts is excessive.									
6.1.1.4 Determine if all service administrators are bonded and/or have been vetted for appropriate security and background verification.									
6.1.2 **Administrative Accounts Dedicated to Administrative Functions** Control: Administrative accounts are used for administrative functions only.	DS5			x					
6.1.2.1 Determine that all administrative users are also assigned regular user accounts for nonadministrative duties and that the administrative users use the administrative accounts for administrative processes only.									
6.1.2.2 Select a sample of service administrators, verify logon/logoff times and determine from event logs the processes performed.									
6.1.2.3 Determine that the pre-assigned administrator user name within each domain has been renamed to a nondescript name.									
6.1.2.4 Determine that after the built-in administrator name has been changed, a new administrator user has been established in each domain with no access.									

© 2010 ISACA. All rights reserved.

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			
6.1.2.5 Determine if smart cards are required for administrative access.									
6.1.3 **Service Administration Segregation** Control: Segregate the service administrators in a separate controlled OU.	PO4.11			x					
6.1.3.1 Determine that the service administrators are contained in a service administration OU.									
6.1.3.2 Determine that this OU has blocked inheritance permissions from higher up in the domain tree.									
6.1.3.3 Determine that the service administrator OU has the following access settings: • Enterprise Admins: Full control of this object and all child objects • Domain Admins: Full control of this object and all child objects • Administrators: Full control of this object and all child objects • Enterprise Domain Controllers: List contents, read all properties and read permissions to this object only • Enterprise Domain Controllers: Read all properties to user, group and computer objects									
6.1.3.4 Determine that all administrative workstations are added to the service administrator OU.									
6.1.4 **Service Administrator Auditing** Control: Establish audit processes for the service administrator OU.	ME3			x					
6.1.4.1 Verify that all activities within the OU are audited, with the following settings for all audit properties for the group EVERYONE, and applied to this and all child objects: • Write All Properties • Delete • Delete Subtree • Modify Permissions • Modify Owner • All Validated Writes • All Extended Rights • Create All Child Objects • Delete All Child Objects									

© 2010 ISACA. All rights reserved.

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			
6.1.5 **Use of AdminSDHolder to Protect Service Administrator Accounts** Control: Protect the Service Administrator Accounts by controlling access to the AdminSDHolder object.	DS5			x					
6.1.5.1 Determine that the AdminSDHolder object is protected by applying the access permissions to the AdminSDHolder object.									

Type	Name	Access	Apply To
Allow	Administrators	List Contents Read All Properties Write All Properties Delete Read Permissions Modify Permissions Modify Owner All Validated Writes All Extended Rights Create All Child Objects Delete All Child Objects	This object only
Allow	Authenticated Users	List Contents Read All Properties Read Permissions	This object only
Allow	Domain Admins	List Contents Read All Properties Write All Properties Read Permissions Modify Permissions Modify Owner All Validated Writes All Extended Rights Create All Child Objects Delete All Child Objects	This object only
Allow	Enterprise Admins	List Contents Read All Properties Write All Properties Read Permissions Modify Permissions Modify Owner All Validated Writes All Extended Rights Create All Child Objects Delete All Child Objects	This object only

© 2010 ISACA. All rights reserved.

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			
<table><tr><td>Allow</td><td>Everyone</td><td>Change Password</td><td>This object only</td></tr><tr><td>Allow</td><td>Pre–Windows 2000 Compatible Access</td><td>List Contents Read All Properties Read Permissions</td><td>User and InetOrgPerson objects</td></tr><tr><td>Allow</td><td>SYSTEM</td><td>Full Control</td><td>This object only</td></tr><tr><td>Allow</td><td>SELF</td><td>Change Password</td><td>This object only</td></tr><tr><td>Allow</td><td>Cert Publishers</td><td>Read userCert Write userCert</td><td>This object only</td></tr><tr><td>Allow</td><td>Windows Authorization Access Group</td><td>Read tokenGroupsGlobalAndUniversal</td><td>This object only</td></tr><tr><td>Allow</td><td>Terminal Server License Servers</td><td>Read terminalServer Write terminalServer</td><td>This object only</td></tr></table>									
6.1.6 **Schema Access** Control: Limit schema access, establishing access only when schema changes are required.	DS5								
6.1.6.1 Determine that no members are included in the schema administrators group.									
6.1.7 **Directory Partition Root Ownership** Control: Ownership of the directory partition root objects is assigned to the administrative group, and the schema directory partition is owned by the schema administrators group.	PC2			x					
6.1.7.1 Verify that the partition root objects have not been reassigned to another group or individual and that the schema directory partition is owned by the schema administrator.									

© 2010 ISACA. All rights reserved.