# Network Perimeter Security Audit/Assurance Program


ISACA®
Serving IT Governance Professionals

# Network Perimeter Security Audit/Assurance Program

**ISACA®**
With more than 86,000 constituents in more than 160 countries, ISACA (*www.isaca.org*) is a recognized worldwide leader in IT governance, control, security and assurance. Founded in 1969, ISACA sponsors international conferences, publishes the *ISACA Journal®*, and develops international information systems auditing and control standards. It also administers the globally respected Certified Information Systems Auditor™ (CISA®) designation, earned by more than 60,000 professionals since 1978; the Certified Information Security Manager® (CISM®) designation, earned by more than 10,000 professionals since 2002; and the new Certified in the Governance of Enterprise IT™ (CGEIT™) designation.

**Disclaimer**
ISACA has designed and created *Network Perimeter Security 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/assurance professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or IT environment.



**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 978-1-60420-080-5
*Network Perimeter Security Audit/Assurance Program*
Printed in the United States of America

## ISACA wishes to recognize:

**Author**
Norm Kelson, CISA, CGEIT, CPA, The Kelson Group, USA

**Expert Reviewers**
Michael Castro, CISA, CISSP, Suncor Energy Inc., Canada
Hugo Köncke, CISM, CISSP, GCIH, INAC, Uruguay
Sanjay Vaid, CISA, Fujitsu Siemens Computers, Belgium
Reinhard E. Voglmaier, GlaxoSmithKline—Medical Department, Italy



 

# Network Perimeter Security Audit/Assurance Program

## 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 roadmap for the completion of a specific assurance process. The ISACA Assurance Committee has commissioned audit/assurance programs to be developed for use by IT audit and assurance practitioners. This audit/assurance program is intended to be utilized 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 IT Governance Institute® (ITGI™) *Control Objectives for Information and related Technology* (COBIT®)—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. They 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 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 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 pre-fieldwork preparation. Because the pre-fieldwork 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 the use of the program, the audit/assurance program describes the audit/assurance objective—the reason for performing the steps in the topic area. The specific controls follow and are shown in **blue** type. 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 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, since 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. 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 the professional reviews each control, he/she 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 has 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 enterprises 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. |

 

| 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 timeframe 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 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. 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 organization, so 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.

The *IT Assurance Guide Using COBIT*, Appendix VII—Maturity Model for Internal Control, in **figure 2**, provides a generic maturity model showing 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. |
| 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 level 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 progression in the enhancement of controls. However, it must be noted that 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 the 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. The graphic presentation describing the achievement or gaps between the actual and targeted maturity goals has been removed from this presentation since only one COBIT subsection is within the scope of this review. It is suggested that the maturity assessment for this review be included in the IT information security review, which would focus on the Deliver and Support (DS) domain, IT process DS5 *Ensure systems security*.

## IV. Assurance and Control Framework

### ISACA IT Assurance Framework and Standards

The following sections in ITAF are relevant to network perimeter security:

- 3410—IT Governance
- 3425—IT Information Strategy
- 3490—IT Support of Regulatory Compliance
- 3630.7—Information Security Management
- 3630.11—Network Management and Controls
- 3630.16—Enterprise Portals
- 3630.17—Identification and Authentication

ISACA has long recognized the specialized nature of IT assurance and strives to advance globally applicable standards. Guidelines and procedures provide detailed guidance on how to follow those standards. IS Auditing Standard S15 IT Controls, IS Auditing Guideline G38 Access Controls, and IS Auditing Procedures P3 Intrusion Detection and P6 Firewalls are relevant to this audit/assurance program.

### ISACA Controls Framework

COBIT is an IT governance framework 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 on which IT audit/assurance activities are based aligns IT audit/assurance with good practices as developed by the enterprise.

The COBIT control objective DS5.10 *Network security*, in the DS domain, addresses good practices for ensuring 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.*

 

Refer to the IT Governance Institute'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.

## V. Executive Summary of Audit/Assurance Focus

### Network Perimeter Security

Network perimeter security is a proactive process to ensure the protection of the enterprise's data, assets and information that are stored on computer equipment residing on a network, and the information flowing through the network.

Network perimeter security is built on the concept that layers of security components, when aggregated, provide the necessary protection from unauthorized access to the network. This process includes:

- Security policy built on good practices, using recognized standards
- Authorization and access controls addressed by identity management
- External perimeter control through the use of firewalls to protect the internal network from external intrusion
- Virtual private networks (VPNs) to allow authorized traffic through the firewall, using encryption techniques to prevent eavesdropping, and physical devices (tokens) of which the user must have custody to further enhance authentication
- Intrusion detection tools to identify suspect network activity and issue alerts
- Penetration testing to ensure that firewalls are securely configured
- Internal security assessments to evaluate policy and procedures
- Risk management to evaluate and identify networks and resources requiring enhanced security
- Internal network segmentation, limiting access of data in certain locations to authorized users and restricting that area from others within the enterprise

### Business Impact and Risk

The enterprise's network is the primary communications channel in that:

- Key business processes (applications) function through the network.
- Financial transactions are stored and processed.
- E-mail containing privileged information is exchanged.
- Analysis, business strategy, intellectual property, presentations, etc., are stored and exchanged.
- Personal identification information may be stored and transmitted.

The failure to provide adequate network security could result in:

- Disclosure of privileged information
- Loss of physical assets
- Loss of intellectual property
- Loss of competitive advantage
- Loss of customer confidence
- Violation of regulatory requirements
- Disruption of network traffic, resulting in the inability to perform critical business functions
- Infection of computer systems with viruses and other malware, which disrupt processing and require costly disinfection
- Use of the network as a launching pad for malicious activity against other enterprises (and the potential to be held liable for their damages)

 

# Network Perimeter Security Audit/Assurance Program

## Objective and Scope

**Objective—**The objectives of the network perimeter security audit/assurance review are to:

- Provide management with an independent assessment relating to the effectiveness of the network perimeter security and its alignment with the IT security architecture and policy
- Provide management with an evaluation of the IT function's preparedness in the event of an intrusion
- Identify issues that affect the security of the enterprise's network

**Scope—**The review will focus on the network perimeter security, including associated policies, standards and procedures as well as the effectiveness of the security implementation.

{Before providing this document to the client, the reviewer should customize the remainder of this paragraph on scope to describe which networks within the enterprise will be reviewed. In addition, the reviewer should determine if the scope also includes independent penetration and intrusion testing. Generally, this requires significant planning to avoid disrupting the business processes and other network traffic. The scope should include such statements as:

- The review will focus on the networks at the XYZ location as well as the connectivity to the Internet
- The web servers managed by third-party suppliers will be excluded from this review and assessed separately}

## Minimum Audit Skills

The IT audit and assurance professional must have an understanding of good-practice systems network security processes and requirements as well as a good grasp of networking concepts, exposures and control techniques. Professionals who have achieved CISA certification should have these skills.

 

## 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 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 and review the business continuity and IT continuity policies. | | | | | | | | | |
| 1.2.2 Obtain and review the business continuity plan (BCP) and IT continuity plan (ITCP). | | | | | | | | | |
| 1.2.3 Determine the entities addressed in the BCP and ITCP. | | | | | | | | | |
| 1.2.4 Establish initial boundaries of the audit/assurance review. | | | | | | | | | |
| 1.2.5 Identify limitations and/or constraints affecting audit of specific systems. | | | | | | | | | |
| **1.3 Define assurance.** The review requires two sources of standards. The corporate standards defined in policy and procedure documentation establish the corporate expectations. At minimum, corporate standards should be implemented. The second source, a good-practice reference, establishes industry standards. Enhancements should be proposed to address gaps between the two. | | | | | | | | | |
| 1.3.1 Review the business continuity policy and standards. | | | | | | | | | |

 

# Network Perimeter Security 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 | | | |
| 1.3.2 Determine if COBIT and the appropriate systems development framework will be used as a good-practice reference. | | | | | | | | | |
| 1.3.3 Determine if there are gaps in the policy. | | | | | | | | | |
| **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 BCP and ITCP. | | | | | | | | | |
| 1.4.2 Review previous audits of the BCP and ITCP and other assessments. | | | | | | | | | |
| 1.4.3 Determine if issues identified previously have been remediated. | | | | | | | | | |
| 1.4.4 Evaluate the overall risk factor for performing the review. | | | | | | | | | |
| 1.4.5 Based on the risk assessment, identify changes to the scope. | | | | | | | | | |
| 1.4.6 Discuss the risks with IT, business and operational audit management, and adjust the risk assessment. | | | | | | | | | |
| 1.4.7 Based on the risk assessment, revise the scope. | | | | | | | | | |
| **1.5 Define the 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. | | | | | | | | | |
| 1.5.1 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. | | | | | | | | | |

 

# Network Perimeter Security 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 | | | |
| **1.6 Define assignment success.**<br>The success factors need to be identified. Communication among the IT audit/assurance team, other assurance teams and the enterprise is essential. | | | | | | | | | |
| 1.6.1 Identify the drivers for a successful review (this should exist in the assurance function's standards and procedures). | | | | | | | | | |
| 1.6.2 Communicate success attributes to the process owner or stakeholder, and obtain agreement. | | | | | | | | | |
| **1.7 Define audit/assurance resources required.**<br>The resources required are defined in the introduction to this audit/assurance program. | | | | | | | | | |
| 1.7.1 Determine the audit/assurance skills necessary for the review. | | | | | | | | | |
| 1.7.2 Estimate the total resources (hours) and time frame (start and end dates) required for the review. | | | | | | | | | |
| **1.8 Define deliverables.**<br>The deliverable is not limited to the final report. Communication between the audit/assurance teams and the process owner is essential to assignment success. | | | | | | | | | |
| 1.8.1 Determine the interim deliverables, including initial findings, status reports, draft reports, due dates for responses and the final report. | | | | | | | | | |
| **1.9 Communications**<br>The audit/assurance process is clearly communicated to the customer/client. | | | | | | | | | |
| 1.9.1 Conduct an opening conference to discuss the review objectives with the information security officer, the network security executive and the IT operations executive. | | | | | | | | | |

 

# Network Perimeter Security 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 | | | |
| **2 . PREPARATORY STEPS** | | | | | | | | | |
| **2.1 Obtain and review the current organization chart for the system and network administration areas.** | | | | | | | | | |
| 2.1.1 Identify the key network administration staff, the security manager and the key network user stakeholders. | | | | | | | | | |
| **2.2 Obtain a copy of the latest network security risk analysis, including any information on system, data and service classifications.** | | | | | | | | | |
| 2.2.1 Obtain and review a copy of the enterprise's:<br>• Security policy<br>• Security strategy or strategies<br>• Security procedures and standards<br>• Network inventory or schematic of physical network components<br>• Network problem-tracking, resolution and escalation procedures<br>• Security violation reports and management review procedures<br>• List of vendors and customers with access to the network<br>• Copies of contracts with service providers for data transmission<br>• Copies of signed user security and awareness documents<br>• New employee training materials relating to security<br>• Relevant legal and regulatory information related to security and information access | | | | | | | | | |
| 2.2.2 Interview the senior security officer and the IT security administrator. | | | | | | | | | |

 

# Network Perimeter Security 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 | | | |
| **3 . NETWORK SECURITY DESIGN** | | | | | | | | | |
| **3.1 Security risk analysis**<br>Audit/assurance objective: Risk analysis should be employed to determine the exposures associated with the network security design. | | | | | | | | | |
| **3.1.1 Risk analysis methodology**<br>**Control: Risk methods are utilized to determine the probability and cost associated with network exposures, and asset ownership is assigned to establish accountability for risk decisions.** | PO4.8<br>PO6.2<br>PO9.4 | | X | X | | | | | |
| 3.1.1.1 Determine that a methodical security risk analysis has been completed and documented. | | | | | | | | | |
| 3.1.1.2 Obtain and review a copy of the risk analysis and determine if it includes a detailed list of all information assets—such as servers and workstations, software and data, and services running on the platforms connected to the network—that need protection. | | | | | | | | | |
| 3.1.1.3 Determine if an owner has been identified for each information asset and verify that a value has been assigned to each asset (high, medium, low) that represents the cost to the enterprise should the asset be compromised. | | | | | | | | | |
| 3.1.1.4 Compare the risk analysis with the network inventory or schematic of the network to verify that all of the physical access points to the information assets have been identified and the analysis is complete. | | | | | | | | | |
| 3.1.1.5 Obtain and review a copy of the results of the tests focused on penetration, weak point, vulnerability, honey pots, etc., performed in the past or at regular intervals, and determine what corrective and preventive actions were taken. Determine if a change plan exists. | | | | | | | | | |

 

# Network Perimeter Security 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 | | | |
| **3.2 Security policy**<br>Audit/assurance objective: A network security policy that recognizes the good practices of a recognized network standard and establishes a clear network security strategy should be implemented. | | | | | | | | | |
| **3.2.1 Control: A security policy has been developed and documented, based on a recognized standard.** | PO4.8<br>PO6.2<br>DS5.10 | | | X | | | | | |
| 3.2.1.1 Determine that a documented security policy has been approved and implemented. | | | | | | | | | |
| 3.2.1.2 Obtain and review a copy of the security policy and determine if it conforms to relevant standards, such as ISO 17799. | | | | | | | | | |
| 3.2.1.3 Determine if the security policy sets a clear policy direction and includes support and commitment by management for information security across the enterprise. The policy should contain:<br>• A definition of information security and its overall objectives and scope<br>• A statement of management intent, supporting the goals and principles of information security<br>• A brief explanation of the security policies, principles, standards and compliance requirements that are of particular importance to the enterprise<br>• A definition of general and specific responsibilities for information security management, including monitoring and reporting<br>• References to documentation that may support the policy, e.g., detailed security policies and procedures | | | | | | | | | |

 

# Network Perimeter Security 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 | | | |
| **3.2.2 Security strategy**<br>**Control: A security strategy that is in alignment with the security policy has been implemented.** | PO6.2<br>DS5.10 | | | X | | | | | |
| 3.2.2.1 Determine that a security strategy (or strategies) that is based on the security policy has been developed and documented. The strategy should specify the types of controls, such as demilitarized zones (DMZs), trust zones, hardened operating systems, least privilege and separation of duties, that should be implemented. | | | | | | | | | |
| 3.2.2.2 Confirm that each strategy is supported by documented detailed security procedures and standards. These procedures and standards should be specific to the application and operating system. Review the procedures and standards, and determine if they are detailed enough to enable a knowledgeable user to perform the procedure or configure the system or application. | | | | | | | | | |
| 3.2.2.3 Determine that the security strategy and its requirements are communicated to all required. | | | | | | | | | |
| **3.2.3 Third-party providers**<br>**Control: Third-party providers that are providing network services, or whose products require the enterprise's data to traverse their networks, must provide adequate assurance that the security policies required internally by the enterprise are satisfied.** | DS2.1<br>DS2.2<br>DS2.4 | | | | X | | | | |
| 3.2.3.1 Determine if sensitive data are processed on third-party networks. | | | | | | | | | |
| 3.2.3.2 If third parties are involved, determine if the contracts with those third parties require adherence to enterprise policy. | | | | | | | | | |
| 3.2.3.3 If third parties are involved, consider a relevant, scoped review of third-party network security. | | | | | | | | | |

 

# Network Perimeter Security 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 | | | |
| **3.3 Trust zones**<br>Audit/assurance objective: Trust zones should be established to establish a classification for assigning appropriate security, based upon the sensitivity of the data processed in the zones. | | | | | | | | | |
| **3.3.1 Trust zone classification**<br>**Control: A trust zone is assigned for each network node, according to the sensitivity of the data traversing the network.** | PO2.3<br>PO6.2<br>DS5.10 | | | X | | | | | |
| 3.3.1.1 Review the network inventory or schematic of the network, and verify with knowledgeable IT network personnel that all of the physical access points to the information assets have been identified. | | | | | | | | | |
| 3.3.1.2 Verify that all connections to the network have been classified as trusted, based on the level of control required by the security policy. Four potential classifications for interconnected systems are:<br>• Trusted: Systems that are under direct control of the enterprise<br>• Semitrusted: Authenticated access required to protect exposed systems not accessible by the public<br>• Untrusted: Authenticated access required to specific information resources on exposed publicly accessible systems<br>• Hostile: Restricted access to the required systems. Unauthorized access attempts are expected. | | | | | | | | | |
| 3.3.1.3 Verify that, for each of the connections documented previously, the protocols used to connect have been identified for both inward and outward services (HTTP, HTTPS, FTP, Telnet, etc.). | | | | | | | | | |
| **3.3.2 Control: The network segmentation is implemented according to the trust zone classifications.** | DS5.10 | | | X | | | | | |
| 3.3.2.1 Review the DMZ architecture in place and determine if it appears appropriate given the trust classifications and protocols associated with the connections to the network services. | | | | | | | | | |

 

| 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 | | | |
| 3.3.2.2 Verify that the enterprise's internal network is on its own network segment and that services (e-mail, web, FTP, etc.) accessed from outside connections are classified into appropriate trust zones and partitioned or segmented appropriately. | | | | | | | | | |
| **3.4 Hardened systems**<br>Audit/assurance objective: The operating systems for servers and other network appliances operating on the network should be configured for maximum security (hardened). | | | | | | | | | |
| **3.4.1 Harden the server operating systems configurations.**<br>**Control: The configuration of servers' operating systems has been adequately secured (hardened) to limit exposure from well-documented exposures.[1]** | DS5.10 | | | X | | | | | |
| 3.4.1.1 Determine if the core operating system has been hardened with the following:<br>• All services/daemons/started tasks not specifically required on each server have been disabled or removed.<br>• All current, relevant patches, service packs and other updates to the operating system and applications have been applied.<br>• Unencrypted protocols have been avoided; where they have been implemented, the justification for their use is documented.<br>• External mail servers scan for malware prior to allowing e-mail files into an enterprise's network.<br>• Administrator accounts have been renamed to names that do not identify the accounts as administrators.<br>• Default passwords have been changed.<br>• Guest accounts have been disabled.<br>• Anonymous FTP has been disabled. | | | | | | | | | |

[1] If audit/assurance reviews addressing server identity management and configuration management were performed recently, with satisfactory ratings, reliance for this control may be placed on that effort.

 

| 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 | | | |
| • Access to system logs is tightly restricted.<br>• At least seven days of log files are retained.<br>• Default file, directory and other permissions are restricted on a need-to-know basis.<br>• Warning messages are routed to information security professionals when users gain access to restricted areas. | | | | | | | | | |
| 3.4.1.2 Review the access role and category schemes to determine if the access privileges granted to users are restrictive enough to limit risks from malicious users. The concept of least privilege states that each subject should be granted the most restrictive set of privileges needed for the performance of authorized tasks. | | | | | | | | | |
| **3.4.2 Separation of duties of perimeter components**<br>**Control: The perimeter security strategy and policies provide for adequate separation of duties to preclude one individual from having access and control of the enterprise's entire network.** | PO4.6<br>DS5.10 | | | X | | | | | |
| 3.4.2.1 Review the overall perimeter security strategy and policy to verify that no one individual is allowed access to all the components of an enterprise's network security structure. | | | | | | | | | |
| **4 . NETWORK SECURITY COMPONENTS** | | | | | | | | | |
| **4.1 Routers**<br>Audit/assurance objective: Routers should be configured to provide maximum security while providing appropriate access to the network segments. | | | | | | | | | |
| **4.1.1 Network segmentation**<br>**Control: Networks have been segmented by trust levels, using appropriately configured routers, and default password settings are changed from the factory defaults.** | DS5.10 | | | X | | | | | |
| 4.1.1.1 Review the network schematic, and verify that routers are installed between network segments of differing trust levels. | | | | | | | | | |

 

# Network Perimeter Security 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 | | | |
| 4.1.1.2 Verify with the network administrator that all unnecessary services and protocols have been removed from all external routers. | | | | | | | | | |
| 4.1.1.3 Determine, where possible, if encrypted passwords have been removed from router configuration files. | | | | | | | | | |
| 4.1.1.4 Determine if all access to routers has been limited (Telnet and HTTP ports are disabled, IP addresses from which network administrators can connect to routers are limited, and modems are removed from router auxiliary ports). | | | | | | | | | |
| 4.1.1.5 Review and determine to what extent external routers are providing coarse filtering capabilities that can be applied to the entire network to reduce granular filtering by firewalls. Determine if external routers are filtering out (denying) the following:<br>• Incoming traffic with a source address that is internal to the network, within the range of invalid or private addresses or the loopback address of 127.0.0.1<br>• Incoming traffic critical to hosts, such as firewalls or firewall management console<br>• Incoming traffic with IP options set, such as source routing<br>• Incoming traffic destined for the broadcast address of a subnet<br>• All incoming and outgoing Internet Control Message Protocol (ICMP) traffic<br>• All outgoing traffic except that with a source address internal to the network | | | | | | | | | |
| 4.1.1.6 Confirm that external routers are not being used as granular filters and that stateful or dynamic filtering is being implemented by the firewall in accordance with the firewall policy. | | | | | | | | | |

 

# Network Perimeter Security 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 | | | |
| **4.2 Switches**<br>Audit/assurance objective: Switches should be placed on the network to direct traffic, provide acceptable performance, limit access to restricted network segments and provide assurance that only authorized technicians have access to the switch management facility. | | | | | | | | | |
| **4.2.1 Switch placement**<br>**Control: Switches are strategically placed on the network to maximize performance, secure the switch configuration and permit appropriate management.** | | | | | | | | | |
| 4.2.1.1 Review the placement and use of switches in the network schematic. Where there are switches that have the capability to be managed and/or monitored remotely, ensure that the network administrator has taken steps to limit access to these devices and protect passwords. | | | | | | | | | |
| **4.2.2 Switch usage**<br>**Control: Switches are utilized for network performance; routers are used when it is necessary to secure a segment of the network.** | | | | | | | | | |
| 4.2.2.1 Review the use of switches on sensitive network segments to determine if the switch provides the appropriate security or if a router solution may be more appropriate. | | | | | | | | | |
| **4.3 Firewalls**<br>Audit/assurance objective: Firewalls should be configured to provide maximum security to sensitive data, and policies and standards should be established to identify the required firewall rules. | | | | | | | | | |
| **4.3.1 Firewall rule requirements**<br>**Control: The firewall rule requirements are assessed and documented.** | DS5.10 | | | X | | | | | |
| 4.3.1.1 Determine with application, system and network administrators if there is a complete, documented understanding of network traffic that needs to pass into and out of the enterprise's network. | | | | | | | | | |

 

# Network Perimeter Security 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 | | | |
| 4.3.1.2 Discuss with the network administrator the reasoning behind the architecture and type of firewall installed, and determine if the choice was made based on an objective evaluation of the needs and requirements of the enterprise. | | | | | | | | | |
| **4.3.2 Firewall configuration**<br>**Control: The firewall configuration reflects the rule-set requirements.** | DS5.10 | | | X | | | | | |
| 4.3.2.1 Review the firewall rule set to determine if the default-deny principle by which all traffic is denied except that which is explicitly required has been appropriately implemented into the firewall rules. | | | | | | | | | |
| 4.3.2.2 Examine the firewall default implicit rule set that is shipped with a firewall to ensure that it is not circumventing the implicit firewall rules. | | | | | | | | | |
| 4.3.2.3 Review the termination of VPNs to ensure that only trusted networks and clients have VPN access. VPNs that connect any nontrusted source should not be permitted through a firewall without some form of filtering at the VPN's termination; encrypted VPN traffic precludes any inspection process by a firewall. | | | | | | | | | |
| 4.3.2.4 Verify that the firewall configuration blocks inbound remote access software (remote desktop, pcAnywhere, Virtual Network Computing [VNC], etc.) unless authorized in writing by information security management, and such use is documented and monitored. | | | | | | | | | |

 

# Network Perimeter Security 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 | | | |
| **4.4 Remote access—VPNs**<br>Audit/assurance objective: VPNs should be used to provide secure remote access from outside the enterprise's internal network. The VPN should encrypt network traffic between the external source and the internal firewall, and provide authentication security. | | | | | | | | | |
| **4.4.1 VPN utilization**<br>**Control: VPNs are required to access sensitive enterprise information.** | DS5.10 | | | X | | | | | |
| 4.4.1.1 Determine if the remote access policy establishes classification of data requiring VPN utilization. | | | | | | | | | |
| **4.4.2 VPN configuration**<br>**Control: The VPN configuration provides communication security through encryption and ensures authentication.** | DS5.10 | | | X | | | | | |
| 4.4.2.1 Evaluate whether encryption is being utilized to minimize the exposure of unauthorized access to confidential files stored on clients connected to an enterprise's network via a VPN. | | | | | | | | | |
| 4.4.2.2 Determine if client workstation standards require the workstation utilizing a client-based VPN had unnecessary services removed that could be a source of exploitation. | | | | | | | | | |
| 4.4.2.3 Determine if the inbound ports that are sensitive (i.e., e-mail, file access/sharing, internal web sites, etc.) are unavailable without a VPN connection. | | | | | | | | | |
| 4.4.2.4 Disable split tunneling. | | | | | | | | | |

 

# Network Perimeter Security 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 | | | |
| **4.5 Remote access—Dial-up**<br>Audit/assurance objective: Dial-up remote access use should be minimized to situations where other access is not feasible and appropriate controls to positively identify the user and user location are employed. | | | | | | | | | |
| **4.5.1 Control: Remote dial-up access is secured through configuration controls, use is limited to necessary functions, encryption is utilized where possible, and workstations available for remote dial-up access are restricted.** | DS5.10 | | | X | | | | | |
| 4.5.1.1 Review and determine if servers connected to dial-up remote access capabilities are utilizing strong authentication controls. These controls should include requirements for minimum-length passwords with mixed characters and frequent change. | | | | | | | | | |
| 4.5.1.2 Review and confirm that end users are restricted from connecting modems to their desktop machines unless specifically authorized to do so. | | | | | | | | | |
| 4.5.1.3 Review and determine whether the following dial-up countermeasures have been implemented to reduce the risk of unauthorized access to network resources:<br>• Granting access to only specific users<br>• Using dial-up server features to restrict users to specific devices and applications<br>• Utilizing call-back modems<br>• Restricting remote access times, when possible<br>• Using separate dial-up usernames and passwords from those used for accessing the network<br>• Regularly monitoring all remote access traffic<br>• Utilizing tokens, smart cards, and biometric or digital certificates, when practical, to strengthen authentication<br>• Using encrypted authentication methods, such as password authentication protocol (PAP), challenge handshake | | | | | | | | | |

 

| 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 | | | |
| authentication protocol (CHAP) or Shiva password authentication protocol (SPAP) | | | | | | | | | |
| **4.6 Wireless networking**<br>Audit/assurance objective: Wireless networking should be secured with encryption features, authentication and, if possible, tokens. | | | | | | | | | |
| **4.6.1 Control: Encryption and user authentication is required for wireless networks. Use of tokens is strongly recommended.** | DS5.10 | | | X | | | | | |
| 4.6.1.1 Verify that WiFi Protected Access (WPA) is enabled. | | | | | | | | | |
| 4.6.1.2 Confirm that factory defaults for administrator user ID, password, WPA key and Service Set Identifier (SSID) have been changed. | | | | | | | | | |
| 4.6.1.3 Confirm that the wireless network has not been placed on the internal side or trusted side of an enterprise's perimeter firewall. | | | | | | | | | |
| 4.6.1.4 Confirm that perimeter firewalls allow traffic only from a wireless network that uses Internet protocol security (IPSec)—i.e., a network over which an IPSec VPN runs for confidentiality purposes. | | | | | | | | | |
| 4.6.1.5 Determine if separate keys have been assigned to each wireless device and are changed frequently. | | | | | | | | | |
| 4.6.1.6 Determine if tokens are required. | | | | | | | | | |

 

# Network Perimeter Security 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 | | | |
| **4.7 Intrusion detection**<br>Audit/assurance objective: Intrusion detection tools should be employed to monitor for intrusions. | | | | | | | | | |
| **4.7.1 Intrusion detection program**<br>**Control: Intrusion detection software is installed and monitored, and intrusion alerts are researched.** | DS5.10 | | | X | | | | | |
| 4.7.1.1 Confirm that host-based and network-based intrusion detection schemes are in place. | | | | | | | | | |
| 4.7.1.2 Ensure that network-based intrusion detection schemes address the following conceptual elements:<br>• Event module (the sensor)<br>• Analysis module (the traffic analyzer)<br>• Response module (generates the configured response to a detected attack)<br>• Database module (records traffic history) | | | | | | | | | |
| 4.7.1.3 Obtain and review the documented incident response procedures to determine if a knowledgeable individual will be able to investigate, understand and perform root cause analysis, and implement the appropriate response. | | | | | | | | | |
| 4.7.1.4 Determine if an incident triggers a response from the Computing Incident Response Team (CIRT).[2] | | | | | | | | | |

[2] Refer to *Incident Management Audit/Assurance Program.*

 

# Network Perimeter Security 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 | | | |
| **4.8 Network security assessments**<br>Audit/assurance objective: Network security assessments, including external penetration tests, internal security assessments, and reviews of policies and procedures, should be performed regularly, and the results of these assessments should be provided to the IT executive and risk management executive. | | | | | | | | | |
| **4.8.1 Penetration tests**<br>**Control: Penetration tests are performed on a regular schedule (monthly to quarterly, depending on the sensitivity).** | DS5.10 | | | X | X | X | | | |
| 4.8.1.1 Determine that a systematic approach has been developed and documented for conducting penetration tests. | | | | | | | | | |
| 4.8.1.2 Confirm that specific requirements have been developed and documented for the penetration tests that are conducted. | | | | | | | | | |
| 4.8.1.3 Confirm that test metrics have been developed so the results of penetration tests can be quantified and measured. | | | | | | | | | |
| 4.8.1.4 Determine if penetration tests are limited to the externally facing network, or if they also include sensitive internal networks that are protected by internal firewalls. | | | | | | | | | |
| 4.8.1.5 Ensure that the results of penetration tests are communicated adequately to the technical staff and management. | | | | | | | | | |
| 4.8.1.6 Ensure that the results of penetration tests are considered adequately in the change plan. | | | | | | | | | |
| **4.8.2 Internal network assessments**<br>**Control: Internal network assessments that review the configurations, policies and utilization of network appliances are performed at least annually.** | DS5.10 | | | X | X | X | | | |
| 4.8.2.1 Determine if information security management performs an internal | | | | | | | | | |

 

| 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 | | | |
| network self-assessment, and evaluate the frequency and effectiveness of the program. | | | | | | | | | |
| 4.8.2.2 Determine if professional reviews of the network security policy and implementation are performed periodically. | | | | | | | | | |

 

## 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 audit/assurance review, and the reviewer's observations, assign a maturity level to the following COBIT control practice.

| COBIT Control Practice | Assessed Maturity | Target Maturity | Reference Hyper-link | Comments |
|---|---|---|---|---|
| **DS5.10 Network Security**<br>1. Establish, maintain, communicate and enforce a network security policy (e.g., provided services, allowed traffic, types of connections permitted) that is reviewed and updated on a regular basis (at least annually).<br>2. Establish and regularly update the standards and procedures for administering all networking components (e.g., core routers, DMZ, VPN switches, wireless).<br>3. Properly secure network devices with special mechanisms and tools (e.g., authentication for device management, secure communications, strong authentication mechanisms). Implement active monitoring and pattern recognition to protect devices from attack.<br>4. Configure operating systems with minimal features enabled (e.g., features that are necessary for functionality and are hardened for security applications). Remove all unnecessary services, functionalities and interfaces (e.g., graphical user interface [GUI]). Apply all relevant security patches and major updates to the system in a timely manner.<br>5. Plan the network security architecture (e.g., DMZ architectures, internal and external network, IDS placement and wireless) to address processing and security requirements. Ensure that documentation contains information on how traffic is exchanged through systems and how the structure of the organization's internal network is hidden from the outside world.<br>6. Subject devices to reviews by experts who are independent of the implementation or maintenance of the devices. | | | | |

 