ISACA®
Trust in, and value from, information systems

SAMPLE AUDIT AND ASSURANCE PROGRAM IN 5 STEPS—VIRTUAL PRIVATE NETWORK

ISACA® has developed a five-step process for creating audit and assurance programs. Using this methodology, we have created this sample program for a virtual private network, illustrating how these five steps work in practice. Use this sample document to create a specific audit and assurance program tailored to your unique needs.

Step 1: Determine the audit subject. Virtual private network (VPN)

Step 2: Define the audit objective. The objective of the review is to provide management with an independent assessment of the VPN implementation and ongoing monitoring/maintenance of the effectiveness of the supporting technology.

Step 3: Set the audit scope. The review will focus on VPN standards, guidelines and procedures as well as the implementation and governance of these activities. The review will rely on several sources:
- Other operational audits of the incident management process, configuration management, and security of networks and servers
- Security management and awareness
- Business continuity management
- Information security management
- Governance and management practices of IT and business units
- Relationships with third parties

Step 4a: Identify locations or facilities to be audited. One data center located in the United States

Step 4b: Identify sources of information for test or review (including policies, standards and procedures). Possible sources include:
- The latest network security risk analysis, including any information on system, data and service classifications
- Security policy
- Security strategy or strategies
- Security procedures and standards
- Network architecture documentation
- Network inventory or schematic of physical network components
- Network problem tracking, resolution and escalation procedures
- VPN-related documentation and vendor contracts
- Copies of signed user security and awareness documents
- New employee training materials relating to security
- Relevant legal and regulatory information related to security and information access
- VPN supplier contracts, SLAs
- Supplier due diligence selection criteria, process
- Business impact analysis (BIA), business continuity plans (BCPs), disaster recovery plans (DRPs) and all plans relating to continuity of operations
- HR onboarding/offboarding procedures and standards
- Information security remote access policies, procedures and standards
- Information security mobile computing policies, procedures and standards
- Information security wireless networking standards
- Information security acceptable use policies, procedures and standards
- Encryption policies, procedures and standards
- Incident response policies, procedures and standards
- Monitoring and audit policies, procedures and standards

Excerpted from ISACA White Paper: *Information Systems Auditing: Tools and Techniques—Creating Audit Programs* (*www.isaca.org/creating-audit-programs*).

Step 5a: Define and record the audit approach that will be used for the specific audit or assurance engagement. The risk-based approach for this audit or assurance engagement consists of the following steps:
- Understand the enterprise's internal and external environment.
- Review documentation.
- Understand the internal control environment.
  - Regulatory statutes
  - Control environment
  - Control risk assessment
  - Control procedures
  - Equation of total risk
- Identify key internal controls to be tested in the following areas:
  - VPN governance
  - VPN policy
  - VPN configuration
  - VPN maintenance and monitoring
- Test controls, document results and conclusions, and gather supporting evidence.
- Conduct a closing meeting to brief management on the preliminary findings of the engagement.
- Draft the report and recommendations.
- Prepare the report and provide it to stakeholders for review and comment.
- Issue the final report.

Step 5b: Identify sources of information to expand the understanding of the audit area/subject.
Possible sources include:
- Interview the senior security officer and the IT security administrator regarding VPN implementation.
- Interview the technical support team leader or equivalent responsible for VPN architecture, design, implementation, and maintenance processes and procedures.
- Perform a high-level walk-through of the network architecture using VPN-technology.
- Review the VPN logs.

Step 5c: Identify a list of individuals to interview. Possible approaches include:
- Obtain and review the current organization chart for the system and network administration areas.
- Identify the key network administration staff, the security manager and the key network user stakeholders.

Step 5d: Identify and document risk and existing internal controls. Areas of risk and internal control include:

Risk
- Identify the business risk associated with the failure to implement VPN technologies and the failure to implement VPN technologies securely.
  - Public relations issues with the customers or the public (reputational risk)
  - Inability to comply with regulatory processing requirements (regulatory and financial risk)
  - Inability to perform critical business functions (operational and financial risk)
  - Inability to maintain payroll and employee privacy (regulatory and reputational risk)
  - Loss of physical or informational assets (reputational and financial risk)
  - Inability to meet contractual SLAs with third parties or customers (contractual risk)
- Identify the technology risk associated with the failure to implement VPN technologies and the failure to implement VPN technologies securely.
  - Metadata[1] may be available to attackers in cleartext.
- Determine if a VPN architecture threat assessment and modeling processing process has been established and implemented.

[1] Metadata is one of the current "hot topics" in VPN security. Metadata, which is the blueprint of the data being transferred over the VPN, can exist at entry points in cleartext despite the communication being sent encrypted. These residual data residing at the entry points are called crumbs.

Internal Controls
• Perform a high-level walk-through of the network architecture using VPN technology.
• Use an ICQ to request information about existing internal controls.

Step 5e: Develop audit tools and methodology to test and evaluate internal controls. Develop testing procedures for the following areas:
• VPN governance
• VPN policy
• VPN configuration
• VPN maintenance and monitoring

Note: For each test step, ensure that **what**, **why**, **how** and by **whom** are answered. For example, the following statements address those topics: "New users are added by a security administrator using the security console to ensure that access is replicated to systems that support single-sign-on (SSO) automatically. This reduces the probability of errors in the user information."

VPN Governance Audit and Assurance Program

VPN Governance					
Area	**Control Objective**	**Control**	**Test Steps**	**Cross-reference**	**Comments**
Executive Responsibility and Accountability of VPN-related Processes	The VPN implementation and maintenance is assigned to an executive sponsor, who is responsible for its effective implementation and operations.	A senior executive within the IT organization is responsible for the VPN implementation, maintenance and oversight.	1. Identify the senior executive responsible for the VPN program. 2. Obtain the position description of the executive responsible for the VPN program. 3. Determine if the position has cross-reporting to the business units and IT management (security, administration, etc.). 4. Obtain meeting minutes and other documentation to support the responsibilities and accountability of the executive sponsor.		
Senior Management Involvement in VPN Programs	Senior management participates in key decisions related to VPN programs.	Senior management provides oversight of the VPN programs, including review and approval of policies affecting their respective operations.	1. Determine if business units affected by VPN implementation participate in the review of policies affecting their business units. 2. Determine if support functions (e.g., HR, corporate communications, compliance, information security) affected by VPN implementation participate in the review of VPN policies.		
End of VPN Governance					

VPN Policy Audit and Assurance Program

VPN Policy					
Area	**Control Objective**	**Control**	**Test Steps**	**Cross-reference**	**Comments**
HR Policies	VPN policies align with and are integrated into HR policies.	HR policies include VPN disclosures, usage requirements as part of the initial "onboarding" process and the annual employee acknowledgement of use policies.	1. Obtain a selection of HR policies relating to VPN usage. 2. Determine if VPN usage policies are incorporated in the HR policies.		
Corporate Policies	VPN policies align with corporate compliance policies.	Corporate compliance (financial reporting, regulatory and statutory) functions review VPN policies prior to implementation to assure adherence to appropriate requirements.	1. Obtain the corporate compliance policies relating to data security and privacy. 2. Determine if VPN requirements are a component of the policies. 3. Obtain a selection of VPN policy proposals or modifications. 4. Determine if corporate compliance representatives have reviewed and provided documented approval of VPN policies.		
Compliance With Legal and Regulatory Policies and Requirements	VPN policies align with legal and regulatory policies and requirements.	VPN technologies are defined to satisfy legal and regulatory requirements within the enterprise's industry.	1. Obtain a selection of VPN policy proposals or modifications. 2. Determine if the enterprise's legal representatives have reviewed and provided documented approval of VPN policies.		
VPN Policies Align With Information Security	VPN policies are in compliance with information security policies.	The information security function assures compliance with information security policy by reviewing information security-related VPN policies prior to their adoption and implementation.	1. Obtain a selection of VPN policy proposals or modifications. 2. Determine if information security representatives have reviewed and provided documented approval of VPN policies.		
VPN Policy Integrated With Enterprise's Data Classification Policy	The Data Classification Policy includes VPN usage and configuration requirements.	The data classification policy identifies VPN requirements and configuration for each data classification.	1. Obtain the data classification policy. 2. Determine if the data classification policy includes VPN configuration and usage requirements. 3. Determine if the VPN configuration and usage policy includes specific applications or data elements requiring VPN usage. 4. Determine if VPN configuration and usage policy identifies functions that must be executed using a VPN, and functions that must be excluded from execution, with or without a VPN.		
End of VPN Policy					

VPN Configuration Audit and Assurance Program

VPN Configuration					
Area	**Control Objective**	**Control**	**Test Steps**	**Cross-reference**	**Comments**
VPN Architecture	Edge routers are properly terminated.	Edge routers[2] terminate at the network firewall and an effective firewall configuration applies appropriate filtering.	1. Identify edge routers within the network architecture. 2. Determine that the edge router terminates (a) at or in front of the demilitarized zone (DMZ) or (b) at an inline Intrusion Prevention System (IPS) deployed between the edge router and the firewall. 3. Select a sample of edge routers. 4. Determine if the edge routers selected terminate at the firewall or in the DMZ.		
VPN Architecture	Edge routers use appropriate encryption protocols.	Edge routers use asymmetric keys supported by a public key infrastructure or alternatively, one of the two standard symmetric key technologies, Triple Data Encryption Standard (3DES) or Advanced Encryption Standard (AES).	1. Select a sample of edge routers. 2. Identify the encryption configuration in use to protect the data. 3. Determine the effectiveness of the control of keys and digital certificates. 4. Determine if an untrusted partner would have the ability to compromise the private key structure.		
VPN Architecture	Trusted routers are properly terminated.	Trusted routers[3] terminate in a trusted DMZ or within the network, subject to appropriate firewall filtering.	1. Identify trusted router terminations within the network architecture. 2. Determine that the trusted router terminates in a designated DMZ designed with firewall filtering appropriate to the data classification of the data traversing the network segment. 3. Determine that the designated DMZ is designed with firewall filtering appropriate to the data classification of the data traversing the network segment.		
VPN Architecture	Trusted routers use appropriate encryption protocols.	Trusted routers use symmetric keys supported by appropriate key length, security of key storage and, where appropriate, contracts/agreements.	1. Select a sample of trusted router networks. 2. Identify the encryption configuration in use to protect the data. 3. Determine the effectiveness of the control of keys. 4. Determine if appropriate SLAs, contracts and other legal remedies have been executed between nonrelated parties. 5. Determine if a trusted partner would have the ability to compromise the key structure.		

[2] Edge routers are defined as untrusted site-to-site connected networks.
[3] Trusted routers are defined as site-to-site networks integrated into a wide-area local area network (LAN).

VPN Configuration Audit and Assurance Program *(cont.)*

VPN Configuration *(cont.)*					
Area	**Control Objective**	**Control**	**Test Steps**	**Cross-reference**	**Comments**
VPN Architecture	Secure Sockets Layer (SSL) configuration is secure.	SSL VPN is installed with a secure configuration which mitigates its inherent weaknesses.	1. Obtain the SSL VPN Configuration Policy. 2. Determine if strong user authentication has been implemented. Consider: •Two-factor authentication •Password AND hardware tokens •Digital certificates •Smart cards 3. Determine if user computer identity verification has been implemented: • User computer validated to be in compliance with enterprise security requirements and policies prior to connection. • Validation of user computer identity and configuration includes: – Personal firewall configuration – Antivirus/malware configuration and currency of pattern files – Required security patches – Limitation of split tunneling – Evaluation of registry entries 4. Determine if a secure desktop solution or “sandboxing” has been implemented for connections not satisfying or unable to validate computer identity verification. 5. Determine if the SSL VPN provides for deletion of all session data from the client’s cache, including: • Browser history • Internet temporary files • Cookies • Documents • Passwords 6. Determine if the SSL VPN provides a keystroke logger detection sweep prior to completing a connection. 7. Determine if session time-outs are implemented and what the time-out period is and determine if it complies with security policies, standards and procedures. 8. Determine if SSL verification is required prior to connection and denied if the SSL version level is at a lower level that security policy dictates.		

VPN Configuration Audit and Assurance Program *(cont.)*

VPN Configuration *(cont.)*					
Area	**Control Objective**	**Control**	**Test Steps**	**Cross-reference**	**Comments**
VPN Architecture *(cont.)*			9. Determine if server certificate support has been implemented and will only permit connection with a valid, authenticated certificate. 10. Determine if resource availability, system functionality, and application access are limited based on satisfying the configuration parameters considered above. 11. Determine if public computers (e.g., Internet cafés, kiosks, etc.) are permitted to connect to the SSL VPN. 12. Determine if client-side certificates are required, and if so, connection is contingent upon client-side certificate verification and authentication.		
VPN Architecture	SSL VPN awareness programs are in place.	User education and security awareness is provided on a regular basis and participation by all users of the enterprise's VPN facilities is required.	1. Determine that VPN awareness and security programs are routinely and regularly offered. 2. Determine if the security awareness program addresses the VPN use policy. 3. Evaluate how the follow-up process is maintained to assure user participation. 4. Determine if participation is documented in logs or sign-in sheets.		
VPN Architecture	VPN appliance configuration reflects the latest and vendor support patches, updates or upgrades.	VPN appliances are maintained with the most current configuration, and support is readily available from the vendor.	1. Verify that the most current configuration of the VPN appliance has been applied. 2. Determine that a vendor support contract or vendor support option is available.		
VPN Architecture	VPN appliances are configured following best practices.	Vendor-suggested and other best practices are applied to VPN appliance configuration.	1. Determine if the VPN appliance vendor offers best practice guidance. 2. Determine if the VPN appliance configuration is in compliance with vendor guidance. 3. Review VPN logs and determine if passwords are stored in clear text.		

VPN Configuration Audit and Assurance Program *(cont.)*

VPN Configuration *(cont.)*					
Area	**Control Objective**	**Control**	**Test Steps**	**Cross-reference**	**Comments**
VPN Architecture	VPN clients installed on specific computers are configured properly.	VPN clients are configured using vendor-suggested and other best practices in compliance with organization security policies.	1. Determine if strong user authentication has been implemented: • Two-factor authentication • Password AND hardware tokens, digital certificates or smart cards 2. Determine if user computer identity verification has been implemented: • User computer is in compliance with organization security requirements and policies. • Validation of user computer identity and configuration: – Personal firewall configuration – Antivirus/malware configuration and currency of pattern files – Required security patches – Limitation of split tunneling – Evaluation of registry entries 3. Determine if resource availability, system functionality and application access are limited to authorized individuals, based on satisfying the configuration parameters considered above.		
VPN Architecture	The VPN architecture uses security protocols to protect traffic.	VPN encryption protocol is patched regularly to address vulnerabilities that can compromise traffic.	1. Validate if VPN configuration uses VPN, Internet Protocol security (IPsec) or Point-to-point Tunneling Protocol (PPTP) as primary security protocol. 2. Verify that VPN appliances are patched regularly to address “port fail” vulnerabilities and that there is a process in place to monitor for new VPN specific vulnerabilities as they arise. **Note:** VPNs using several versions of Juniper OS are at risk of containing code that can decrypt VPN traffic if unpatched.		
VPN Architecture	VPN clients are installed based on job functional need.	VPN clients are installed on user computers based on data classification policy of applications installed on computer or on another request.	1. Determine if the data classification policy requires a VPN be installed as a condition of accessing specific sensitive data. 2. Select a sample of computers with the VPN installed and determine if the data classification policy/VPN policy is practiced.		

VPN Configuration Audit and Assurance Program *(cont.)*

VPN Configuration *(cont.)*					
Area	**Control Objective**	**Control**	**Test Steps**	**Cross-reference**	**Comments**
VPN Architecture	VPNs installed on "Bring Your Own Device" adheres to the information security policy.	VPNs installed on nonenterprise-owned equipment subscribe to minimum security standards.	1. Determine if user computer identity verification has been implemented: • User computer is in compliance with enterprise security requirements and policies. • Validation of user computer identity and configuration: – Personal firewall configuration – Antivirus/malware configuration and currency of pattern files – Required security patches – Limitation of split tunneling – Evaluation of registry entries		
VPN Architecture	VPN access is removed upon termination or transfer.	VPN access is terminated or removed as part of the user deprovisioning process.	1. Obtain the deprovisioning procedure. 2. Determine that the VPN deactivation is part of the deprovisioning process. 3. Obtain a sample of recent user terminations and determine that the VPN privileges for the terminated users have been deactivated.		
VPN Architecture	The VPN installation list is reviewed periodically to ensure validity.	The list of installed VPNs is reviewed at least annually.	1. Determine if a list of computers or users with VPNs installed exists. 2. If the list exists, determine if the list is reviewed at least annually to ensure that only authorized users have access to and have an installed VPN.		
VPN Architecture	The VPN architecture is reviewed on a regular basis to ensure that the solution is current and addresses the risk and vulnerability issues identified in risk assessments.	VPN architecture review is conducted on a regular basis.	1. Determine if the VPN architecture review process is documented. 2. Determine the date of the most recent VPN architecture review. 3. Evaluate the effectiveness of the most recent review. 4. Determine if any vulnerabilities exist due to out-of-date technology.		
End of VPN Configuration					

VPN Maintenance and Monitoring Audit and Assurance Program

VPN Maintenance and Monitoring					
Area	**Control Objective**	**Control**	**Test Steps**	**Cross-reference**	**Comments**
Patch Management	VPN technologies are included in the routine patch management process.	Patch management of VPN technologies is included in the configuration change management processes.	1. Scan the change management system for configuration changes affecting VPN technologies. 2. Determine if the change management process implemented for VPN maintenance is in compliance with the installation change management procedure.		
Integration of VPN Technologies With the Help Desk	VPN support requests are processed routinely through the help desk.	VPN support is a help desk task with appropriate controls and procedures.	1. Obtain the help desk procedures. 2. Determine if VPN support tasks are included in the help desk procedures. 3. Determine if VPN issues are reported in the incident reporting/issue monitoring system. 4. Select VPN-related incidents in the help desk, incident reporting, and/or issue monitoring system. 5. Determine that the issues were closed on a timely basis in an effective manner.		
VPN Capacity Planning	VPN utilization and resources requirements are integrated into the installation capacity plan.	The capacity plan incorporated VPN required resources and such resources are actively monitored.	1. Obtain the installation capacity plan. 2. Determine that VPN technologies are included in the plan. 3. Evaluate capacity reports to determine that VPN resource utilization is monitored and the necessary adjustments are implemented in a timely manner.		
VPN Monitoring	Processes exist to monitor VPN usage and identify unauthorized activities and VPN usage.	VPN usage is monitored for unauthorized use.	1. Determine the process for reviewing VPN usage. 2. Select a sample of VPN usage violations. Determine how the violations were investigated and the actions taken.		
End of VPN Maintenance and Monitoring					