ISACA®

VPN Security Audit Program

CONTENTS

ABSTRACT

Virtual private networks (VPNs) were developed to address two challenges:

- **Security**—Enterprises require remote workers to access corporate networks securely.
- **Affordability**—Leased lines (e.g., to branch offices) represent significantly high cost.

One primary benefit of VPNs is secure data transmission. Recent increases in the number of remote workers (both full time and part time) have heightened not only enterprise security concerns, but also awareness and implementation of VPNs.

The *VPN Security Audit Program* helps auditors evaluate the risk of VPNs, and outlines guidance and testing of safeguards implemented to mitigate the risk.

VPN Security Audit Program

In preparation for audits conducted using ISACA's *VPN Security Audit Program*, auditors should familiarize themselves with the:

- Technology and terminology of VPNs
- Implementation landscape of the VPN environment being audited

In a pre-audit planning section, the *VPN Security Audit Program* outlines recommendations to help auditors become familiar with VPNs. The planning section includes documentation that the auditor should obtain for the audit. It also provides guidance on scoping for the audit.

The *VPN Security Audit Program* does not aim to provide assurance over all possible VPN implementations; however, it does provide guidance and testing that can minimize risk associated with VPNs.

Audit Subject

Some enterprises needed to establish or expand use of VPNs rapidly in the context of COVID-19. Therefore, ISACA® addresses the following areas in the *VPN Security Audit Program*:

- User education and security awareness of risk associated with using VPNs
- Documentation of VPN elements to assist in assessing risk and performing audits—these elements include, but are not limited to, VPN type (gateway-to-gateway or client-to-gateway), tunneling protocols and vendor software used to implement the VPN
- VPN inventory management that addresses concerns including actual vs. rogue VPN connections and high availability (which can mitigate single points of failure)

Audit Objectives

The primary purpose of this audit program is to assist the audit function in providing assurance around effectiveness of implemented VPN controls. Accordingly, this audit program considers assurance around:

- **Pre-audit planning**—terminology/technology, personnel, scope, documentation
- **Governance and oversight**—oversight, policies, security awareness
- **Implementation and configuration**—VPN architecture, configuration, client configuration, endpoint configuration
- **Operations**—policy implementation, data classification, VPN inventory, IT assets, VPN authentication, VPN access, vendor VPN access
- **Maintenance and monitoring**—VPN activity logging and monitoring, patch management, VPN capacity planning, integration of VPN technologies with the service desk

Considering these elements, the audit results will provide management with an evaluation of enterprise VPN configuration, operations and maintenance relative to the control environment that was established. The audit's outcome will indicate whether the control environment is operating as designed, and will also highlight any governance challenges.

Audit Scope

The scope of the *VPN Security Audit Program* includes all VPNs implemented across the enterprise under review. Accordingly, its scope includes VPNs that may connect to cloud services.

Business Impact and Risk

VPNs can help enterprises accommodate remote work.

Whether remote work offers savings over brick-and-mortar expenses, health benefits in light of COVID-19, better work/life balance for employees—or all of the above—VPNs provide an adequate platform. Their benefits can positively impact businesses and workers alike—but VPN use is not without risk:

- In some enterprises, VPNs may have been intended originally to accommodate small numbers of end users for short periods of time. Increasing numbers of end users, combined with

extended periods of use, may challenge original infrastructure, exceed original design specs, and/or adversely affect performance.
- Failure to detect unauthorized VPN activity may cause denial of service due to excessive traffic or connection attempts.
- Failure to align data classification requirements with VPN requirements and configuration may impair compliance initiatives that rely on data classification.

Minimum Audit Skills

The audit program assumes that auditors exercise due professional care and possess professional competencies culminating in the proficiency to conduct an audit. ITAF Standard 1005 and ITAF Guideline 2005 (Due Professional Care) require the auditor to exercise professional skepticism and maintain effective communication throughout the course of an audit. ITAF Standard 1006 and ITAF Guideline 2006 (Proficiency) require the auditor to have technical skill, knowledge and/or experience in the areas under assessment. This expectation is particularly relevant to auditors who do not hold CISA (or other appropriate) certification.

The IT audit and assurance professional must understand data protection and records management processes in the context of holistic business systems. It is therefore important that the auditor has sufficient functional and business knowledge to assess alignment with business compliance needs. Professionals performing this audit should ensure that they have performed the necessary research to understand VPNs.

The IT audit professional must have an understanding of security, controls and technology processes. The auditor should also possess adequate functional and business knowledge to determine alignment with business strategy. Individuals performing this audit should verify that they have performed the required research to comprehend the nature of VPN technology and its associated risk.

Testing Steps

In combination with the audit program, practitioners may conduct interviews with key stakeholders in business and technology groups to assess the use, deployment and management of VPNs.

Refer to the accompanying spreadsheet file.

Acknowledgments

ISACA would like to recognize:

Lead Developer

Ian J. Cooke
CISA, CGEIT, CRISC, CDPSE, COBIT 5 Assessor and Implementer, CFE, CIPM, CIPP/E, CIPT, CPTE, DipFM, FIP, ITIL Foundation, Six Sigma Green Belt
Ireland

Expert Reviewers

Adham Etoom
CISM, CRISC, FAIR, GCIH, PMP
Government of Jordan, Jordan

Krishna Das Manghat
CISA, CCIE, CISSP
KPMG, Australia

Padma Paluri
CISA, CRISC
NC Department of Information Technology, USA

Prithvi Mandava
CISA, CISM, CRISC, CISSP
Fortinet, Canada

Fadi Sodah
CISA, CISM, CISSP
Amman Stock Exchange, Jordan

Adetokunbo Salau
CISA, CRISC, CDPSE, CISSP, CRMA
RiskAide Consulting Inc., Canada

Board of Directors

Gregory Touhill, Chair
CISM, CISSP
Director, CERT Division of Carnegie Mellon University's Software Engineering Institute, USA

Pamela Nigro, Vice-Chair
CISA, CGEIT, CRISC, CDPSE, CRMA
Vice President–Information Technology, Security Officer, Home Access Health, USA

John De Santis
Former Chairman and Chief Executive Officer, HyTrust, Inc., USA

Niel Harper
CISA, CRISC, CDPSE
Chief Information Security Officer, UNOPS, Denmark

Gabriela Hernandez-Cardoso
Independent Board Member, Mexico

Maureen O'Connell
Board Chair, Acacia Research (NASDAQ), Former Chief Financial Officer and Chief Administration Officer, Scholastic, Inc., USA

Veronica Rose
CISA, CDPSE
Founder, Encrypt Africa, Kenya

David Samuelson
Chief Executive Officer, ISACA, USA

Gerrard Schmid
President and Chief Executive Officer, Diebold Nixdorf, USA

Asaf Weisberg
CISA, CISM, CGEIT, CRISC
Chief Executive Officer, introSight Ltd., Israel

Tracey Dedrick
ISACA Board Chair, 2020-2021
Former Chief Risk Officer, Hudson City Bancorp, USA

Brennan P. Baybeck
CISA, CISM, CRISC, CISSP
ISACA Board Chair, 2019-2020
Vice President and Chief Information Security Officer for Customer Services, Oracle Corporation, USA

Rob Clyde
CISM
ISACA Board Chair, 2018-2019
Independent Director, Titus, and Executive Chair, White Cloud Security, USA

About ISACA

For more than 50 years, ISACA® (www.isaca.org) has advanced the best talent, expertise and learning in technology. ISACA equips individuals with knowledge, credentials, education and community to progress their careers and transform their organizations, and enables enterprises to train and build quality teams that effectively drive IT audit, risk management and security priorities forward. ISACA is a global professional association and learning organization that leverages the expertise of more than 150,000 members who work in information security, governance, assurance, risk and privacy to drive innovation through technology. It has a presence in 188 countries, including more than 220 chapters worldwide. In 2020, ISACA launched One In Tech, a philanthropic foundation that supports IT education and career pathways for under-resourced, under-represented populations.

DISCLAIMER

ISACA has designed and created the *VPN Security Audit Program* (the "Work") primarily as an educational resource for IT audit 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, IT audit professionals should apply their own professional judgments to the specific circumstances presented by the systems or information technology environment.

Reservation of Rights

ISACA

1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA

Phone: +1.847.660.5505

Fax: +1.847.253.1755

Support: support.isaca.org

Website: www.isaca.org

Provide Feedback: www.isaca.org/VPN-security

Participate in the ISACA Online Forums:
https://engage.isaca.org/onlineforums

Twitter:
www.twitter.com/ISACANews

LinkedIn:
www.linkedin.com/company/isaca

Facebook:
www.facebook.com/ISACAGlobal

Instagram:
www.instagram.com/isacanews/

VPN Security Audit Program
ISBN 978-1-60420-910-5