TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Luca Mizzi

201843IVSB

An ISO/IEC 27001 Compliance Assessment of an OpenVPN with Dual LDAP for Distributed Workforce Authentication

Bachelor's thesis

Supervisor: Valdo Praust
Lecturer, Programme Director (Cyber Security Engineering)

Co-Supervisor: Mohammad Tariq Meeran
Senior Lecturer, PhD

Tallinn 2024

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Luca Mizzi

201843IVSB

LDAPi ja OpenVPNi põhise hajutatud töövooga autentimisskeemi ISO/IEC 27001 vastavushindamine

Bakalaureusetöö

Juhendaja: Valdo Praust

Lektor,
Programmijuht
(Küberturbe
Tehnoloogiad)

Kaasjuhendaja: Mohammad Tariq
Meeran
Vanemlektor, PhD

Tallinn 2024

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Luca Mizzi

04.01.2024

Abstract

Organizations operating in a distributed workforce environment face the challenge of securing remote access while adhering to stringent information security standards, such as ISO/IEC 27001. This thesis explores the strategic implementation of an OpenVPN with dual LDAP authentication as a robust and compliant solution.

By leveraging Google LDAP for internal employees and OpenLDAP for external stakeholders, the proposed dual LDAP VPN provides a differentiated access control mechanism, ensuring that access privileges are tailored to individual user groups. A real-world case study is analyzed to demonstrate the practical implementation of the system and its effectiveness in meeting ISO/IEC 27001 requirements, balancing security with operational efficiency.

A key outcome of this study is a practical guideline presented in checklist format, derived from the insights gained. This checklist serves as a valuable resource for organizations aiming to integrate their own VPN solutions while ensuring adherence to ISO/IEC 27001 requirements.

This thesis is written in English and is 33 pages long, including 6 chapters, 3 figures and 4 tables.

Annotatsioon

LDAPi ja OpenVPNi põhise hajutatud töövooga autentimisskeemi ISO/IEC 27001 vastavushindamine

Hajutatud tööjõukeskkonnas tegutsevad organisatsioonid seisavad silmitsi väljakutsega tagada kaugjuurdepääs, järgides samal ajal rangeid infoturbestandardeid, nagu ISO/IEC 27001. See lõputöö uurib topelt-LDAP autentimise strateegilist rakendamist OpenVPN-iga kui tugeva ja nõuetele vastava lahendusega.

Kasutades Google'i LDAP-i sisemiste töötajate jaoks ja OpenLDAP-i väliste sidusrühmade jaoks, pakub kavandatud topelt-LDAP VPN diferentseeritud juurdepääsukontrolli mehhanismi, tagades juurdepääsuõiguste kohandamise üksikutele kasutajarühmadele. Analüüsitakse reaalset juhtumiuuringut, et demonstreerida süsteemi praktilist rakendamist ja selle tõhusust ISO/IEC 27001 nõuete täitmisel, tasakaalustades turvalisust töö efektiivsusega.

Selle uuringu põhitulemuseks on praktilised juhised, mis on esitatud kontrollnimekirja vormingus ja mis on tuletatud uuringu tulemustest. See kontrollnimekiri on väärtuslik ressurss organisatsioonidele, kes soovivad integreerida oma VPN-lahendusi, tagades samas vastavuse ISO/IEC 27001 nõuetele.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 33 leheküljel, 6 peatükki, 3 joonist, 4 tabelit.

List of abbreviations and terms

2FA	Two-Factor Authentication
ACL	Access Control List
BCP	Business Continuity Plan
CIA Triad	Confidentiality Integrity and Availability
CISO	Chief Information Security Officer
CSP	Cloud Service Provider
CTO	Chief Technology Officer
DIT	Directory Information Tree
DNS	Domain Name System
DRP	Disaster Recovery Plan
GCP	Google Cloud Platform
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
IaaS	Infrastructure as a Service
IaC	Infrastructure as Code
IAM	Identity and Access Management
IdP	Identity Provider
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IETF RFC 4301	IETF Request for Comments
IP	Internet Protocol
IPsec	Internet Protocol Security
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IS	Information Security
ISMS	Information Security Management System
ISO	International Organization for Standardization
LDAP	Lightweight Directory Access Protocol
MFA	Multi-Factor Authentication

NIST	National Institute of Standards and Technology
NIST SP	NIST Special Publication
OpenVPN	Open Source Virtual Private Network
PCI DSS	Payment Card Industry Data Security Standard
PII	Personal Identifiable Information
RAS	Remote Access Server
RBAC	Role-Based Access Control
SSL	Secure Sockets Layer
SSO	Single Sign-On
UI	User Interface
VAPT	Vulnerability Assessment and Penetration Testing
VPC	Virtual Private Cloud
VPN	Virtual Private Network

Table of Contents

List of Figures

List of Tables

1 Introduction

In an era marked by the rapid evolution of technology and the increasingly commonplace use of virtual private networks (VPN), the intersection of information security and distributed workforce authentication has become a focal point for organizations striving to maintain robust data protection standards. As businesses adapt to dynamic operational landscapes, the need for comprehensive solutions that align with internationally recognized standards, such as ISO/IEC 27001, has never been more critical.

This thesis explores the strategic integration of OpenVPN with dual LDAP authentication as a means to enhance ISO/IEC 27001 compliance for organizations with distributed workforces. By analyzing this technological implementation, this thesis seeks to uncover practical insights that not only fortify information security measures but also pave the way for a resilient and compliant operational framework.

In the presented case study, internal employees utilize Google LDAP for authentication, while external stakeholders rely on OpenLDAP for streamlined access to organizational resources. This segregated approach ensures that access privileges are meticulously tailored to individual user groups, thereby enhancing data protection and enhancing overall security posture. It is crucial to acknowledge that the suitability of this solution depends on the diverse needs of the business, which must be balanced with information security requirements.

The forthcoming chapters will unveil the theoretical framework and the methodology employed in the creation of this paper. In Chapter 4, we will delve into the ISO/IEC 27001 guidance for VPN implementation, shaped by a thorough study of the standard. Subsequently, Chapter 5 will outline the design and implementation of the VPN solution in the case study, offering insights into the rationale behind choosing the dual LDAP VPN approach. The concluding summary will encapsulate succinct results, paving the way for the final discussion.

1.1 Problem Statement

In the current remote work scenario, securing data and ensuring compliance with ISO/IEC 27001 standards pose significant challenges. One notable gap is the lack of exploration on how implementing OpenVPN with dual LDAP authentication could help to address these challenges. This study aims to fill this gap by investigating how the use of OpenVPN with dual LDAP can enhance both information security and ISO/IEC 27001 compliance. The focus is on providing practical insights into how organizations can strengthen security and meet regulatory standards, particularly in the context of a small company with a distributed workforce.

1.2 Research Questions

How does the strategic implementation of OpenVPN with dual LDAP authentication contribute to the enhancement of ISO/IEC 27001 compliance for organizations operating with distributed workforces?

What practical guidelines can be derived from this implementation to aid similar organizations in fortifying their information security posture?

1.3 Objectives of the Study

The primary objective of this study is to comprehensively examine how the strategic deployment of OpenVPN with dual LDAP authentication serves to elevate ISO/IEC 27001 compliance for organizations with distributed workforces. This involves a detailed analysis of the positive impacts, addressing how the implemented solution enhances the organization's adherence to international information security standards.

In addition to its overarching objective, the study includes specific goals. One of these goals is to contextualize the effectiveness of the solution by considering the varied business needs and requirements, emphasizing the importance of a balanced approach that aligns with organizational objectives.

Another goal is to critically examine any challenges or potential drawbacks associated with the implementation of an OpenVPN with dual LDAP. Recognizing that an in-depth understanding of both successes and challenges is crucial for a holistic evaluation, this

aspect of the study involves an examination of any potential drawbacks linked to the strategic deployment of OpenVPN with dual LDAP authentication. In particular, the enhanced or reduced level of compliance with the relevant controls from Annex A of ISO/IEC 27001 is going to be assessed.

The last objective of this study is to craft practical guidelines, presented in the form of a checklist, Appendix 3 – ISO/IEC 27001 VPN Implementation Guideline, derived from the implemented solution. These guidelines are meticulously designed to steer analogous organizations in fortifying their information security posture by designing and implementing their own VPN solution following the guidance of the ISO/IEC 27001 standard. The process involves distilling valuable insights from the strategic integration and transforming them into tangible and actionable recommendations that can be readily applied by the broader community.

2 Theoretical Framework

The theoretical framework of this thesis is anchored in a review of literature about the relevant topics and a meticulous examination of the applicable standards to conduct a thorough compliance assessment of the proposed solution. Additionally, knowledge and technical comprehension of the case study VPN implementation have been acquired by a thorough analysis of relevant documentation.

ISO/IEC 27000 defines Information Security (IS) as the protection of information from unauthorized access, use, disclosure, disruption, modification, or destruction, thereby ensuring the Confidentiality, Integrity, and Availability of information (CIA Triad). [1]

ISO/IEC 27001, the international standard for Information Security Management Systems (ISMS), provides a structured framework for managing and protecting sensitive information. The application of ISO/IEC 27001 ensures a systematic and risk-based approach to safeguarding organizational assets, aligning the compliance assessment with globally recognized standards. [2]

Stallings' well-established textbook, "Network Security Essentials: Applications and Standards" provides a comprehensive overview of the fundamental principles of information security. This authoritative resource covers a wide range of topics, from cryptography and network security protocols to network access control and cloud security. Stallings' clear and concise explanations, along with numerous real-world examples, make this book a valuable resource for anyone seeking to gain a solid understanding of network security. [3]

Expanding the theoretical framework to higher abstraction levels, "Computer Security: Principles and Practice" by William Stallings and Lawrie Brown enriches the understanding of general security principles. This layer ensures that security considerations extend beyond the specific domains of VPNs and LDAP, providing a holistic approach to compliance assessment. The chapter about IT security management and risk assessment and the chapter regarding IT security controls, plans, and

procedures provide the framework and tools for the development of a robust security posture within the distributed workforce authentication context. [4]

"Security Engineering: A Guide to Building Dependable Distributed Systems" by Ross Anderson complements the theoretical framework by emphasizing security engineering principles. This resource provides insights into building secure and dependable systems, guiding the compliance assessment towards the integration of security measures at the system architecture level. [5]

Rico Brandenburg and Paul Mee on the MIT Sloan Management Review have recently highlighted how organizations have rapidly shifted to semi-remote working arrangements and thus they must be equally speedy in mitigating the cyber risks created by the expanded “attack surfaces” that have accompanied the “work anywhere” operating models. To take on the new cybersecurity challenges of this virtual working environment, organizations must understand the changes in their cybersecurity risk profile and revamp their strategies, training, and exercises to address these changes. Otherwise, the current better-than-expected outcome of the rapid shift to “work from home” may not succeed in the longer term. [6]

Understanding VPN technologies is paramount for ensuring secure communication within distributed workforce environments. "Virtual Private Networks" by Charlie Scott, Paul Wolfe and Mike Erwin provides insights into the design and implementation of VPNs. Additionally, "Cryptography and Network Security: Principles and Practice" by William Stallings contributes theoretical perspectives on cryptographic principles, vital for ensuring the confidentiality and integrity of VPN communications. This layer of the framework enables the application of industry best practices in the VPN implementation. [7] [8]

The LDAP component of the theoretical framework draws from the expertise outlined in "LDAP System Administration: Putting Directories to Work" by Gerald Carter and "Understanding and Deploying LDAP Directory Services" by Tim Howes, Mark C. Smith, and Gordon S. Good. These resources provide a deep dive into LDAP system administration, directory services, and the principles of identity management. Incorporating dual LDAP for distributed workforce authentication aligns with the theoretical underpinnings of managing user identities and access control. [9] [10]

In a study, Mohammed A. Qadeer, Mohammad Salim and M. Sana Akhtar introduce a technique for managing user profiles and authentication through the utilization of the Lightweight Directory Access Protocol (LDAP). The user profiles are stored in the LDAP Directory Information Tree (DIT), containing diverse information about users. Users can retrieve this information based on the access levels granted to them on the network. This authentication mechanism is employed by various services to permit authorized users, who provide accurate authentication details as stored in the LDAP server, to access corresponding services. LDAP is commonly utilized for authenticating users in services such as VPNs, Remote Access Servers (RAS), Web servers, and mail servers. [11]

2.1 Standards and Regulations

The primary theoretical framework for this study is rooted in the guidance of ISO/IEC 27001, a globally recognized standard for Information Security Management Systems. This framework equips organizations to establish, implement, operate, monitor, review, maintain, and continually improve their ISMS. ISO/IEC 27001 sets the requirements for effectively managing information security risks. A detailed exploration of how these requirements are met in the design and implementation of a VPN solution is provided in Chapter 5. [2]

The rationale behind selecting ISO/IEC 27001 for this study lies in its worldwide recognition, its comprehensive approach to all elements of an ISMS, and its adaptable, process-based methodology. Additionally, ISO 27001 is often a prerequisite for regulatory compliance in certain industries, such as those handling sensitive data like credit card information or healthcare records. [2]

The decision to embrace ISO/IEC 27001 for this research facilitated a comprehensive utilization of ISO/IEC 27002, which offers detailed guidance on applying each of the 93 controls outlined in ISO/IEC 27001 Annex A. It's noteworthy that, for both ISO/IEC 27001 and ISO/IEC 27002, the latest 2022 version has been embraced. In this revision, the list of controls has undergone reorganization from 114 to 93 in number, categorically distributed into four groups: organizational controls, people controls, physical controls, and technological controls. Additionally, ISO/IEC 27000 has been

employed to grasp key concepts, terminology, and relationships within the ISMS domain. [1] [2] [12]

Other standards were consulted and potentially utilized in this study, contributing to a comprehensive understanding of the regulatory landscape concerning VPN implementations. One such standard is the National Institute of Standards and Technology (NIST) Cybersecurity Framework, designed as a tool for managing cybersecurity risk. It equips organizations with the means to identify, prioritize, and address cybersecurity risks. VPNs prove instrumental in implementing several recommended practices of the NIST Cybersecurity Framework, including strong authentication and encryption of data at rest and in transit. [13]

Specifically, the NIST Special Publication (NIST SP) 800-113, Guide to SSL VPNs, makes recommendations for designing, implementing, configuring, securing, monitoring, and maintaining Secure Sockets Layer (SSL) VPN solutions. SP 800-113 provides a phased approach to SSL VPN planning and implementation that can help in achieving successful SSL VPN deployments. It also includes a comparison with other similar technologies such as Internet Protocol Security (IPsec) VPNs and other VPN solutions. [14]

Wort to consider for compliance assessment and further research is the IETF RFC 4301, Security Architecture for the Internet Protocol. The IETF RFC 4301 specifies the base architecture for IPsec-compliant systems. It describes how to provide a set of security services for traffic at the Internet Protocol (IP) layer, in both the IPv4 and IPv6 environments. The document describes the requirements for systems that implement IPsec, the fundamental elements of such systems, and how the elements fit together and fit into the IP environment. It also describes the security services offered by the IPsec protocols, and how these services can be employed in the IP environment. [15]

Compliance with ISO/IEC 27001 aids in adhering to the Health Insurance Portability and Accountability Act (HIPAA), a legislation designed to safeguard the privacy of medical information. VPNs play a crucial role in meeting HIPAA requirements by offering a secure method for healthcare providers to share medical information securely with authorized individuals. Organizations entrusted with Protected Health Information

(PHI) are mandated under the law of the United States of America to comply with HIPAA regulations. [16]

Adhering to the ISO/IEC 27001 guidance also facilitates compliance with the Payment Card Industry Data Security Standard (PCI DSS). This standard is specifically crafted to safeguard sensitive payment card data from unauthorized access, use, disclosure, disruption, modification, or destruction. VPNs are frequently employed to fulfil PCI DSS requirements by establishing a secure tunnel for transmitting payment card data. Organizations involved in storing, processing, or transmitting payment card data are obligated to adhere to PCI DSS regulations. [17]

It is worth considering the potential impact of VPN implementation on enhancing the privacy protection of Personal Identifiable Information (PII) for users and other involved stakeholders. In this context, this study references the General Data Protection Regulation (GDPR), particularly Article 32.1 (Security of processing), which stipulates: “Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: the pseudonymisation and encryption of personal data; the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.”. The GDPR applies to all 27 member countries of the European Union and to all countries in the European Economic Area. [18]

2.2 Technical Documentation

The case study's VPN implementation leverages a synergistic combination of technologies, each playing a pivotal role in delivering a secure, scalable, and manageable solution tailored to the needs of a distributed workforce. These technologies are seamlessly integrated to provide comprehensive remote access capabilities while

adhering to the stringent security requirements of ISO/IEC 27001. Throughout the implementation process, the relevant documentation for each technology was accessed and reviewed. [19] –[25]

Google Cloud Platform (GCP), is a Cloud Service Provider (CSP), it serves as the robust backbone of the VPN infrastructure, providing a scalable and secure cloud environment that supports the distributed nature of the workforce. GCP's infrastructure is resilient, fault-tolerant, and geographically dispersed, ensuring seamless access to corporate networks regardless of the employee's location. [19]

Google Workspace operates as the Identity Provider (IdP), facilitating secure user authentication and authorization. Google Workspace's comprehensive user management capabilities ensure that only authorized individuals can access sensitive corporate resources. Google Workspace's integration with GCP streamlines the user authentication process, allowing remote users to seamlessly connect to the VPN without compromising security. [20]

Google LDAP complements Google Workspace by centrally managing user and group information. This centralized directory service ensures consistency and accuracy of user data, enabling efficient and secure authentication across the VPN infrastructure. Google LDAP's integration with Google Workspace further enhances the overall security posture of the solution. [21]

OpenVPN stands out as the primary solution for remote access, creating secure tunnels connecting remote users to corporate networks. With its strong encryption capabilities, OpenVPN ensures the protection of sensitive data transmissions, guarding against unauthorized access and potential data breaches. The flexibility of OpenVPN allows the VPN to accommodate different client devices and operating systems, addressing the varied requirements of a distributed workforce. [22]

OpenLDAP plays a crucial role in reinforcing the VPN solution's robustness by providing a secondary authentication mechanism. This open-source directory service acts as an auxiliary backup for Google LDAP, safeguarding seamless access to corporate networks even in the event of a system outage or service interruption. The

integration of OpenLDAP with OpenVPN elevates the overall reliability and resilience of the remote access solution. [23]

Terraform, an Infrastructure-as-Code (IaC) tool, automates the provisioning and configuration of cloud resources, including the VPN infrastructure. Terraform's standardized infrastructure code ensures consistency and efficiency in deployment, minimizing the risk of human error and facilitating rapid deployment of VPN infrastructure. [24]

Ansible, an automation platform, simplifies the configuration and management of network devices, including OpenVPN gateways. Ansible's automation capabilities streamline the ongoing management of the VPN solution, reducing manual tasks and ensuring the consistent application of security policies across the VPN infrastructure. [25]

3 Methodology

The methodology employed for this thesis combines practical experience, a thorough examination of relevant ISO/IEC standards, and a comprehensive case study analysis to provide a holistic understanding of the proposed OpenVPN with dual LDAP solution within the context of real-world implementation scenarios. The case study approach, while acknowledging its limitations, offers a valuable tool for evaluating the solution's effectiveness and identifying potential areas for improvement.

The case study approach is particularly well-suited for this research as it allows for a comprehensive and in-depth examination of a real-world implementation of the proposed OpenVPN solution, facilitating an in-depth examination of instances where ISO/IEC standards have been followed, particularly ISO/IEC 27001 for Information Security Management Systems.

While other research methodologies, such as surveys or experiments, could be employed to investigate the proposed OpenVPN solution, the case study approach offers several advantages that make it a more appropriate choice for this research. Surveys rely on self-reported data, which may be inaccurate or biased, and experiments may be difficult or unethical to conduct in real-world settings. In contrast, the case study methodology provides a detailed and objective evaluation of the solution in its actual operating environment.

By focusing on a single instance, the case study method provides a detailed understanding of the intricacies of the solution and its alignment with industry best practices and compliance requirements. This approach enables a practical assessment of the solution's effectiveness and allows the identification of potential gaps and weaknesses that may still be present, which can then be addressed enhancing the organization's overall security posture.

Collaboration with industry peers and colleagues in the implementation of the presented solution is integral to this research. Discussions and interactions with professionals

well-versed in OpenVPN implementation enhance the exploration of best practices and industry benchmarks. This collaborative approach ensures that the research benefits from diverse perspectives and experiences.

3.1 Research on ISO/IEC 27001 Applicability

A significant aspect of the methodology involves a detailed study of the application of ISO/IEC standards on the studied solution, particularly ISO/IEC 27001 for the information security management system requirements, ISO/IEC 27000 for the overall framework, and ISO/IEC 27002 for information security controls guidelines. The research evaluates how the proposed solution aligns with these standards, ensuring a robust and compliant approach to information security.

By combining these elements, the methodology aims to provide a comprehensive and practical foundation for the exploration and analysis conducted in this thesis, ensuring a holistic understanding of the proposed solution within the context of ISO/IEC standards relevant to the information security field.

3.2 Research Limitations and Ethical Considerations

Preserving the confidentiality and integrity of information assets is of utmost importance. Therefore, the name of the company under investigation, as well as the complete Ansible or Terraform code, both fundamental parts of the presented solution, will not be disclosed. This measure is taken to uphold ethical standards and safeguard the proprietary information of the involved organization.

The main limitation of this research is its reliance on a single case study. Given the nature of compliance assessment and the imperative to protect the privacy of the involved company, quantitative data collection as evidence supporting the thesis was not feasible. The constraints inherent in compliance-related research, coupled with privacy considerations, restricted the ability to gather quantitative data in support of the thesis.

4 ISO/IEC 27001 Guidance for VPN Implementation

The integration of a VPN into an organization's information security framework is a critical undertaking that necessitates strict adherence to established standards for comprehensive risk management and information security controls. This section provides insight into the guidance outlined by the ISO/IEC 27001 standard, recognized as a benchmark for information security management, with a specific focus on VPN implementation. The objective is to furnish organizations with a structured approach, ensuring that the transmission of information through VPNs aligns seamlessly with international best practices, thereby safeguarding the confidentiality, integrity, and availability of information assets. Organizations embarking on VPN implementation must discern, interpret, and prioritize specific controls within ISO/IEC 27001. This ensures the harmonious integration of VPN functionalities with internationally recognized standards, taking into account business requirements and environmental conditions.

4.1 Risk Assessment and Management

A comprehensive inventory of information assets is foundational to the subsequent risk assessment. By discerning the sensitivity and criticality of these assets, organizations can tailor their VPN implementation strategies to address the unique risk profile of their information landscape.

Conducting a specialized risk assessment for VPN implementation is recommended. This process entails a systematic evaluation of potential threats, vulnerabilities, and the resulting impact on information assets. The results of this assessment should be integrated into the overarching fabric of organizational risk management.

It’s important to Develop robust mitigation strategies that emanate from the identified risks. These strategies must be meticulously aligned with the organization's overall risk

tolerance, ensuring a calibrated approach to mitigating VPN-specific vulnerabilities while maintaining congruence with broader risk management objectives.

4.2 Design and Resources Allocation

The VPN design process and the subsequent configuration demand an explicit integration of ISO/IEC 27001 controls. This encompasses the design and configuration of encryption protocols, access controls, and authentication mechanisms to ensure that the VPN infrastructure resonates with the stringent security requirements outlined in ISO/IEC 27001 also affording a robust defence against potential security breaches.

The management tasked with the design and implementation of the VPN solution, being the CTO or the CISO of the organization, also needs to ensure that a proper amount of technical and economic resources are allocated. One critical aspect of resource allocation in VPN operations is the careful consideration of bandwidth. Adequate bandwidth is fundamental to the smooth transmission of data across the VPN infrastructure. Organizations must assess their network requirements and allocate sufficient bandwidth to accommodate the volume of traffic associated with VPN usage. This proactive approach helps prevent potential bottlenecks and ensures a seamless user experience.

Resources allocation extends beyond current needs, it requires forward-thinking scalability planning. Organizations should assess the potential growth of VPN usage and allocate resources with scalability in mind. This involves ensuring that the VPN infrastructure can adapt to increased demand without compromising performance or security. Scalability planning safeguards against resource constraints as organizational requirements evolve, aligning with the dynamic nature of information technology landscapes.

In essence, effective resource allocation ensures that the VPN not only meets current demands but also possesses the flexibility to adapt to future requirements, enhancing its resilience and sustainability within the organization's operational framework and business continuity strategy.

4.3 User Authentication and Access Control

Strengthening user authentication mechanisms within the VPN solution is crucial, and the implementation of multi-factor authentication (MFA) plays a paramount role in this context. This additional layer of security enhances user access controls, aligning with the principles outlined in ISO/IEC 27001.

The implementation of MFA introduces a versatile layer of protection by requiring users to provide multiple forms of identification. Various MFA methods can be explored to cater to user preferences and organizational needs. These may include but are not limited to, one-time passcodes sent via SMS, biometric verifications like fingerprint scans, smart card authentication, or token-based authenticators. The flexibility in MFA options allows organizations to tailor authentication methods based on the sensitivity of data accessed through the VPN and user convenience, fostering a robust yet user-friendly security posture.

To further enhance user authentication efficiency within the VPN solution, organizations can consider the integration of a unified Identity and Access Management (IAM) system with Single Sign-On (SSO) capabilities. SSO enables users to access multiple applications with a single set of credentials, streamlining the authentication process. By integrating SSO with the IAM, organizations unify user access across various platforms, ensuring that a user authenticated for VPN access is seamlessly authenticated for other applications as well. This not only simplifies user experience but also aligns with ISO/IEC 27001 principles by enforcing consistent and secure access controls throughout the organization. The combination of MFA and SSO through IAM creates a harmonized approach to user authentication, elevating both security and user convenience within the VPN environment.

Is important to implement Role-Based Access Control (RBAC) to further refine user permissions within the VPN environment. This strategic alignment with ISO/IEC 27001 principles of least privilege ensures that users possess only the needed access rights. By embracing RBAC, organizations bolster their security posture within the VPN environment. Users are granted access based on a need-to-know basis, minimizing the attack surface and limiting the impact of potential security incidents.

To implement RBAC effectively, organizations can adopt solutions that automate user role assignments and permissions. This not only streamlines the process but also reduces the likelihood of manual errors in access provisioning. Additionally, regular audits and reviews of user roles and permissions can identify discrepancies or changes in organizational structure, allowing for prompt adjustments to maintain the principle of least privilege.

4.4 Logging

Robust logging mechanisms within the VPN infrastructure are foundational to ISO/IEC 27001 compliance. These logs should comprehensively capture relevant information, fostering transparency and aiding in compliance reporting and audit trails.

Within the framework of a VPN solution, it is imperative to define mandatory conditions that trigger specific actions or alerts within the system logs. For instance, logs should systematically record failed login attempts, successful access, and any changes to user permissions. By meticulously analyzing these logs, organizations can identify potential security threats, such as unauthorized access attempts or unusual patterns of user behaviour. Defining and regularly reviewing these mandatory conditions ensures a proactive stance in identifying and mitigating security risks within the VPN infrastructure.

In the context of daily log monitoring, organizations should prioritize the review of critical events, such as authentication attempts, system modifications, or unusual user activities. Daily checks enable rapid response to emerging security incidents. Monthly log reviews should encompass a broader perspective, focusing on trends and patterns over an extended period. This includes evaluating the effectiveness of implemented security measures, identifying potential weaknesses, and adjusting strategies accordingly. Striking a balance between daily vigilance and monthly trend analysis ensures a comprehensive approach to log monitoring tailored to both immediate threats and long-term security assessments.

Establishing clear log retention policies is crucial for regulatory compliance and effective forensic analysis. Organizations need to define the duration for which logs should be retained based on legal requirements, industry standards, and the

organization's specific needs. While daily and frequent logs may have a shorter retention period, monthly logs may be stored for a more extended duration. Aligning log retention policies with compliance standards ensures that organizations maintain the necessary data for audits, investigations, and continuous improvement in information security practices.

To optimize log management within the VPN solution, organizations should implement a log rotation strategy. Log rotation involves periodically archiving and removing older logs to free up storage space and maintain system performance. Deciding the appropriate rotation frequency depends on factors such as the volume of log data generated daily and storage capacity. A judicious log rotation strategy prevents storage issues, ensures efficient log analysis, and facilitates compliance with data retention policies.

As the volume and complexity of logs increase, organizations can benefit from automated log management tools. These tools streamline the collection, analysis, and retention of logs, offering real-time insights and alerts. Automation enhances efficiency in daily log monitoring and facilitates the seamless execution of log rotation strategies. Additionally, automated tools contribute to the implementation of proactive measures, enabling organizations to respond promptly to security incidents and adhere to stringent log retention policies.

4.5 Audit and Review

Securing a VPN implementation demands a comprehensive strategy that integrates both internal and external evaluations. Internally, a systematic review of VPN audit trails is vital for daily and monthly analyses, aligning with ISO/IEC 27001's principle of continual improvement in information security practices. This internal vigilance ensures the timely detection and remediation of security incidents, fostering a proactive security stance.

Externally, third-party involvement in the form of Vulnerability Assessments and Penetration Testing (VAPT) is crucial. Vulnerability assessments systematically identify potential weaknesses in the VPN infrastructure, while penetration testing simulates real-world cyberattacks to assess the system's resilience. Engaging third-party

cybersecurity experts provides an unbiased and expert evaluation, offering invaluable insights into the effectiveness of security measures.

Regarding the timing of VAPTs, a quarterly or semi-annual cadence is recommended. This frequency strikes a balance between thorough evaluation and operational continuity. Conducting VAPTs more frequently might result in diminishing returns and increased operational disruption, while less frequent assessments may leave the system vulnerable to emerging threats.

The suggested timing aligns with industry standards and best practices. Quarterly assessments allow for consistent scrutiny without overwhelming operational workflows, ensuring that the VPN implementation undergoes regular and rigorous evaluation. Furthermore, this periodicity provides sufficient time to address and remediate any vulnerabilities identified during the assessments, contributing to the overall security posture.

By adopting an approach of regular internal reviews and periodic external VAPTs, organizations establish a dynamic and robust security audit framework. Internal reviews maintain day-to-day vigilance, while external assessments offer an impartial perspective, validating the effectiveness of security controls. This collaborative strategy enhances the organization's resilience against evolving cybersecurity threats, supporting a proactive and adaptive security environment.

4.6 Documentation and Reporting

Creating comprehensive documentation is not merely a procedural formality; it is a strategic imperative in maintaining information security. The documentation should intricately detail VPN policies and procedures, ensuring clarity and precision. Crucially, this documentation must align with the documentation requirements stipulated by ISO/IEC 27001. By doing so, organizations ensure that their ISMS adhere to international standards, fostering a culture of transparency, accountability, and continual improvement.

Clear and comprehensive documentation provides a reference point for all stakeholders involved in the VPN implementation and usage, ensuring that everyone is on the same

page regarding security protocols and procedures. In the event of security incidents or audits, having well-documented policies and procedures enables efficient communication and swift decision-making, contributing to an organization's overall resilience against potential threats.

Automation plays a pivotal role in expediting and enhancing the compliance process. Implementing automated reporting mechanisms within the VPN infrastructure offers a streamlined approach to generating compliance reports required for ISO/IEC 27001 assessments. This not only ensures accuracy in reporting but also accelerates the reporting process, saving valuable time and resources. Automated reports provide real-time insights into the VPN's security posture, facilitating prompt identification of potential issues and enabling proactive responses to emerging threats.

Up-to-date documentation is inherently linked to an effective Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP). In the context of a security incident or a disaster, having current and accurate documentation serves as a crucial reference for implementing BCP and DRP measures. It aids in swift decision-making, helping organizations to resume operations efficiently. Moreover, automated reporting mechanisms contribute to the proactive identification of vulnerabilities, aligning with the preventive aspects of both BCP and DRP.

4.7 Awareness and Training

The establishment of robust awareness programs assumes a critical role in fostering a heightened sense of security within the organizational culture. These programs serve as educational foundations, imparting crucial insights to employees regarding the significance of VPN usage, associated security protocols, and the broader landscape of ISO/IEC 27001 compliance. Regular updates become imperative, ensuring that the workforce remains well-informed about evolving security practices and potential threats. Beyond technology, these programs also shed light on the roles and responsibilities individuals play in maintaining a secure environment.

The implementation of targeted training initiatives, specifically focusing on VPN usage and adherence to ISO/IEC 27001 controls, becomes an essential component of a proactive security strategy. These training sessions operate as proactive measures,

arming employees with the skills required to securely navigate VPN interfaces, comprehend access implications, and effectively recognize and report security incidents.

Seamlessly integrating awareness and training initiatives into the VPN implementation process ensures that stakeholders are not only proficient in utilizing VPN technology but also comprehend their roles in upholding ISO/IEC 27001 compliance through secure VPN practices. This integrated approach positions the workforce to be not just technologically adept but knowledgeable contributors to the organization's overarching security objectives. This includes a clear understanding of individual roles and responsibilities in maintaining the security fabric of the organization, reinforcing the collective commitment to a secure VPN environment.

4.8 Relevant Controls from Annex A

The following tables list the relevant controls from Annex A of the ISO/IEC 27001 standard relevant to the integration of a VPN. As per Annex A, these controls are categorized into organizational controls, people controls, physical controls, and technological controls.

Each organization may craft its own set of controls tailored to its unique business requirements and environment. While the list in Annex A of ISO/IEC 27001 provides a foundational framework, it serves as a starting point rather than a one-size-fits-all solution.

Table 1. Organizational Controls for VPN.

5.1 Policies for information security	Ensure the VPN implementation aligns with the organization's overarching information security policy. This includes explicit mention of VPN usage, access controls, and encryption protocols.
5.2 Information security roles and responsibilities	Establish clear roles and responsibilities for individuals involved in VPN administration and operation. Define and communicate the organizational structure supporting VPN security.
5.9 Inventory of information and other associated assets	Clearly define responsibilities for managing and protecting VPN-related assets, including servers, cryptographic keys, and configuration files.
5.14 Information transfer	Develop policies and procedures governing the secure transfer of information over the VPN, addressing data integrity and confidentiality.
5.15 Access control	Develop a comprehensive access control policy that explicitly covers VPN access. This policy should specify who has access, under what circumstances, and what controls are in place.
5.16 Identity management	Implement a robust user access management process for VPN users, including user provisioning, de-provisioning, and periodic access reviews.
5.19 Information security in supplier relationships	Ensure that suppliers involved in providing VPN-related services adhere to information security requirements and standards.
5.24 Information security incident management planning and preparation	Develop and implement an incident response plan specific to VPN security incidents, emphasizing timely detection, reporting, and resolution.
5.31 Legal, statutory, regulatory and contractual requirements	Ensure that VPN operations comply with legal and contractual requirements related to information security.
5.35 Independent review of information security	Conduct periodic reviews and audits specifically focused on the information security aspects of VPN operations.
5.37 Documented operating procedures	Develop and document operational procedures specific to VPN management, encompassing routine maintenance, incident response, and change management.

Table 2. People Controls for VPN.

6.1 Screening	Implement background checks and security screenings for personnel involved in VPN administration to mitigate insider threats.
6.3 Information security awareness, education and training	Provide ongoing training and awareness programs for personnel involved in VPN operations. This ensures they are well-versed in security best practices.
6.5 Responsibilities after termination or change of employment	Develop procedures for promptly revoking VPN access for employees whose employment has been terminated or who have changed roles.

Table 3. Physical Controls for VPN.

7.1 Physical security perimeters	Ensure physical security measures are in place to protect servers and networking equipment hosting the VPN infrastructure.
7.8 Equipment siting and protection	Implement safeguards to protect VPN equipment from physical tampering or unauthorized access.

Table 4. Technological Controls for VPN.

8.3 Information access restriction	Ensure that access controls are configured and enforced not only at the user level but also at the system and application levels within the VPN infrastructure.
8.15 Logging	Establish comprehensive logging and monitoring capabilities within the VPN infrastructure to detect and respond to security events.
8.20 Networks security	Ensure that network security measures are implemented and maintained to protect the confidentiality and integrity of VPN communications.
8.24 Use of cryptography	Define and implement cryptographic controls for the VPN, including the use of strong encryption algorithms for data in transit and secure key management practices.
8.26 Application security requirements	Incorporate security requirements specific to VPNs during the acquisition, development, or maintenance of information systems.

5 Case Study Design and Implementation

The OpenVPN solution implemented in this research is based on the OpenVPN Community Edition, an open-source and widely recognized VPN server. The provisioning and configuration of the entire system are orchestrated using Terraform and Ansible, ensuring a seamless and reproducible deployment process.

The seamless integration of these technologies enables the case study organization to implement a secure, scalable, and manageable VPN solution that addresses the specific needs of its distributed workforce while adhering to the stringent security requirements of ISO/IEC 27001. The robust architecture, combined with the comprehensive automation capabilities, ensures that the VPN solution remains secure, resilient, and efficient in supporting the organization's remote work operations.

5.1 Understanding the Business Requirements

Tailoring the VPN solution with dual LDAP authentication to the specific business requirements of the company involves considerations related to the distributed workforce, cost-effectiveness, and diverse user access scenarios.

With approximately 75% of the company's 70 employees working remotely, the VPN solution recognizes the significance of catering to a distributed workforce. The dual LDAP authentication, integrating both Google LDAP for internal employees and OpenLDAP for external collaborators, ensures a seamless and secure remote access experience for all users, irrespective of their location and employment status.

Acknowledging the financial implications of software licensing, the business requirement to optimize costs is addressed through a strategic approach. While Google Workspace Enterprise licenses, including Google LDAP, are allocated to employees, the VPN solution optimizes expenses by leveraging the cost-effective OpenLDAP server. This approach ensures efficient authentication processes without compromising

on security while balancing the financial considerations associated with Google Workspace licenses.

The business requirement to facilitate VPN access for external stakeholders without Google LDAP access is a central consideration. The VPN solution accommodates this by provisioning an OpenLDAP server, enabling secure authentication dedicated to external collaborators. This inclusive approach ensures that various external entities, such as clients, partners, or contractors, can seamlessly connect to the VPN infrastructure, fostering collaboration while maintaining security standards.

Anticipating potential business growth and workforce changes, scalability becomes a fundamental business requirement. Leveraging Terraform and Ansible for provisioning and configuration, the VPN solution offers scalability of its infrastructure components. This scalability not only accommodates organizational changes but also contributes to business continuity, assuring a resilient and effective VPN infrastructure in the face of evolving demands.

5.2 Cloud Architecture Overview

The company uses Google Cloud Platform as its Infrastructure as a Service (IaaS) solution. GCP hosts three main projects: Production, Stage, and Hub-Network (the management project), as illustrated in Figure 1, Network Topology. Each project possesses its dedicated Virtual Private Cloud (VPC), and these VPCs are interconnected through VPC Peering to facilitate seamless communication.

Within the Hub-Network project, critical components, including the OpenVPN server, an OpenLDAP server for user authentication, and a Bind9 DNS server for internal DNS resolution, are installed. Each of these components resides on its dedicated Virtual Machine (VM), as depicted in Figure 2, VMs in Hub-Network. The provisioning and configuration of these elements are orchestrated using a combination of Terraform and Ansible. The associated code for these processes is securely stored within the company's Git repository, ensuring accessibility for the recovery team and integration into the comprehensive recovery plan. This approach significantly contributes to the overall consistency and reliability of the entire infrastructure, harmonizing with industry best practices in system management.

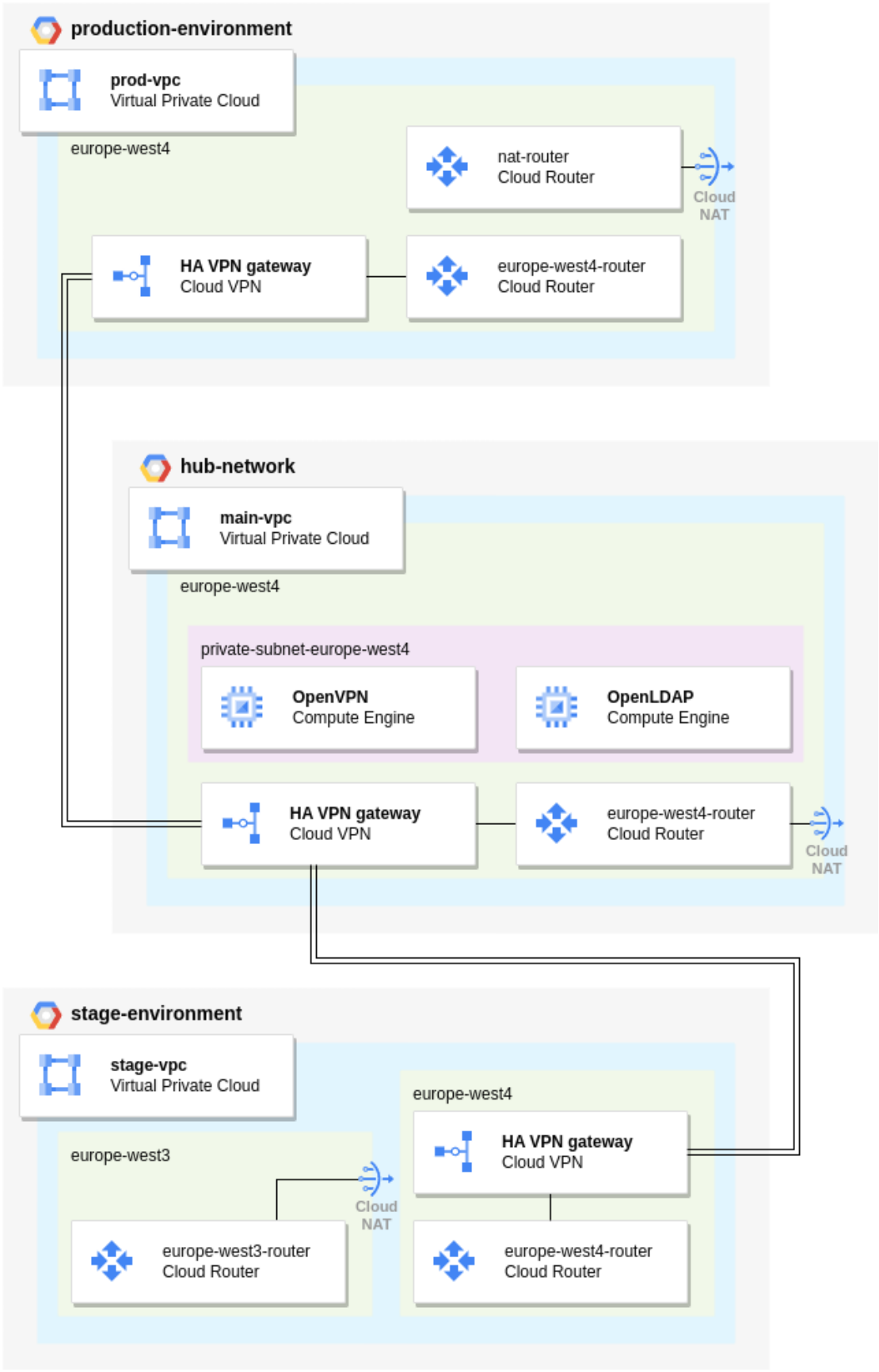

Figure 1. Network Topology.

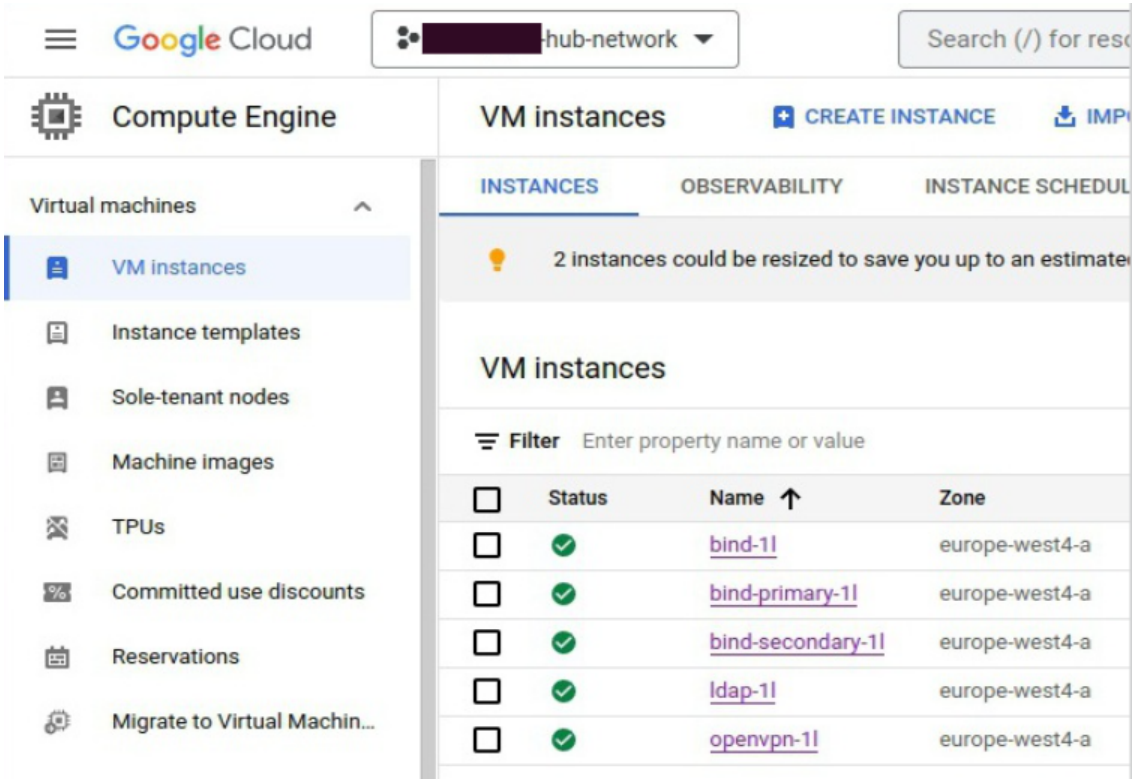

Figure 2. VMs in Hub-Network.

The scalability of the IT infrastructure is a crucial consideration for the case study organization, as it anticipates potential business growth and workforce changes. By leveraging Terraform and Ansible for provisioning and configuration, the IT infrastructure offers scalability of its components, ensuring that it can accommodate increasing numbers of users and connections without compromising on performance or security. This scalable approach not only accommodates organizational changes but also contributes to business continuity, assuring a resilient and effective infrastructure in the face of evolving demands.

5.3 OpenVPN Server Configuration

The OpenVPN server is configured to employ a split-tunneling approach, ensuring that only relevant traffic is routed through the secure VPN connection. Configuration details, encompassing encryption methods, authentication protocols, and network settings, are efficiently managed through Ansible. Stakeholders utilize the VPN to access a range of

company services, including websites in the stage and testing environments, virtual machines, management services, and various internal business tools. To adhere to the principles of RBAC, an Access Control List (ACL) is integrated, granting granular access to resources based on the user's role and operational requirements.

The performance of the VPN solution is essential for the case study organization, as it must provide a seamless and efficient experience for its distributed workforce. The use of split tunnelling ensures that only relevant traffic is routed through the VPN, minimizing latency and optimizing bandwidth usage. Additionally, the configuration of the OpenVPN server with RSA key-pair authentication and LDAP authentication provides robust authentication and authorization mechanisms, further enhancing the overall performance of the solution.

Client authentication for VPN connections is accomplished using a per-user RSA key-pair and LDAP. Employees of the company undergo authentication against Google LDAP, while external collaborators undergo verification against an OpenLDAP server. The generation of client configurations is executed through Ansible, with the detailed process documented and available to the interested parties. A snippet of the Ansible playbook used for client management can be found in Appendix 2 – Code Snippet – Client Management via Ansible.

The revocation of client profiles is conducted systematically, involving removal from designated files and the execution of Ansible commands. The management of the company can remove internal users from the usage of Google LDAP by simply excluding them from the dedicated VPN_users group via the Google Workspace Admin console, a responsibility delegated to the Security Team. Configuration settings for integrating OpenVPN with dual LDAP servers are documented in the LDAP Ansible role.

5.4 Integration of Dual LDAP Authentication

To effectively distinguish between internal employees and external collaborators, the OpenVPN server employs unique client identifiers embedded within connection requests. Upon receiving a connection request, the server extracts the client identifier and determines the user's authentication path. If the identifier signifies an internal

employee, the server directly authenticates against the Google LDAP server. Conversely, if the identifier identifies an external collaborator, the server seamlessly redirects the authentication process to the OpenLDAP server.

It's crucial to emphasize that only Google Workspace Identities, specifically those associated with licensed Google Workspace Enterprise, can leverage the benefits of Google LDAP authentication. The decision to utilize OpenLDAP for external stakeholders removes the need for sub-optimal solutions, such as providing them with dedicated Google LDAP profiles by allocating licensed Google Workspace Identities. This approach would not only be costly but also grant external users excessive access to Google's IAM system, potentially expanding the attack surface. Alternatively, granting a single or a few Google LDAP profiles for all external access, while less expensive, would compromise the principles of accountability and hinder the implementation of an ACL for granular access control.

This client-based approach empowers the OpenVPN server with the ability to effortlessly distinguish between internal and external users, ensuring that each user is authenticated against the corresponding LDAP server. This strategy bolsters the security and versatility of the dual LDAP authentication solution by enabling the server to dynamically adjust its authentication process based on the client's identity.

5.5 User Experience, Training and Awareness

The OpenVPN solution with dual LDAP authentication is designed to cater to both internal employees and external collaborators, providing a user-friendly, secure, and seamless experience. This comprehensive approach encompasses intuitive design, comprehensive guidelines, and integrated training.

To streamline the authentication process and minimize complexity, the OpenVPN solution empowers internal users to access the VPN seamlessly using their existing Google Workspace credentials. This eliminates the burden of managing multiple login credentials, enhancing overall user-friendliness and aligning with the SSO approach. Further bolstering security, the solution integrates Two-Factor Authentication (2FA), requiring users to enter an expiring code from their mobile app in addition to their

password, the same code used to access the Google Workspace account. This additional layer of protection safeguards the VPN from unauthorized access attempts.

The OpenVPN client user interface (UI) is meticulously crafted to ensure intuitive navigation and ease of use, even for users with limited technical expertise. The UI embodies a clean and modern aesthetic, accompanied by clear instructions and a user-centred approach that guides users seamlessly through the connection process. Additionally, the UI incorporates a comprehensive range of visual cues and feedback mechanisms to provide users with immediate confirmation of their actions and the real-time status of their VPN connection. For an exemplary representation of the OpenVPN solution UI design, please refer to Figure 3, OpenVPN Client User Interface.

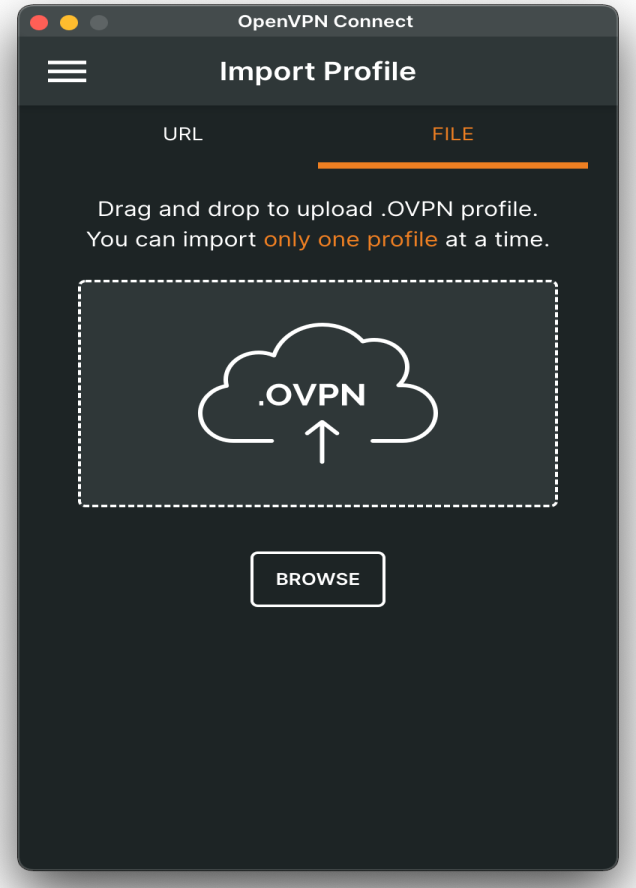

Figure 3. OpenVPN Client User Interface.

The organization has taken a proactive approach to security awareness by embedding information about VPN usage and its importance into its existing information security training programs, guidance on the usage of the VPN is also made accessible through the organization's monthly cybersecurity newsletter and the dedicated “Information Security Hub” web portal on the company intranet. This integrated multi-channel approach ensures that all employees receive consistent and comprehensive information about VPN usage, fostering a culture of security awareness and responsible VPN usage practices.

While standard guidelines and policies on secure VPN usage are provided to all users, the organization also invests in comprehensive training for select members of the IT Team and the Security Team. This targeted approach ensures that a knowledgeable and capable group of individuals is readily available to handle any technical issues related to the OpenVPN Server, including creating new VPN profiles, deleting outdated ones, monitoring its usage, and addressing any potential security concerns.

By investing in specialized training for the IT Team and Security Team, the organization not only strengthens the overall security of its VPN infrastructure but also ensures timely resolution of technical issues. This proactive approach safeguards the VPN's operational efficiency and minimizes downtime while fostering a culture of expertise within the organization, enabling it to effectively manage and optimize the VPN infrastructure as security needs evolve.

The organization's training strategy aims to strike a balance between providing universal guidelines for all users and equipping a select group of individuals with advanced knowledge for handling technical tasks related to OpenVPN Server management. This approach ensures that the VPN infrastructure remains secure, efficient, and aligned with the organization's security goals.

The combined efforts of user-friendly design, comprehensive guidelines, and integrated training have resulted in a positive user experience for the OpenVPN solution with dual LDAP authentication. Users have reported that the solution is easy to use, secure, and reliable. This has contributed to increased adoption of the VPN and improved overall user satisfaction.

5.6 Enhancing Compliance with ISO/IEC 27001

A thorough evaluation of the proposed dual LDAP authentication solution has revealed its significant impact on bolstering compliance levels for the VPN implementation under examination. Notably, the solution aligns with control 5.15 “Access Control” from Annex A of ISO/IEC 27001 by enabling a robust Role-Based Access Control approach. Internal users seamlessly integrate with Google LDAP, leveraging the comprehensive security, monitoring, and integration capabilities associated with Google Workspace Enterprise identities. Conversely, external users benefit from the unwavering reliability of an OpenVPN server without compromising the integrity of the corporate identity management system. This arrangement effectively minimizes the attack surface and optimizes resource utilization.

The implemented solution meticulously adheres to “Access Control” (5.15) and “Identity Management" (5.16) controls, enabling the full-fledged implementation of RBAC and ACL for both internal and external stakeholders. Internal users continue to enjoy the advantages of utilizing Google LDAP (SSO and 2FA), while external users gain access to the VPN environment through a separate OpenVPN server. This approach safeguards sensitive corporate data while providing seamless access for authorized external users.

While the dual LDAP authentication solution offers substantial compliance benefits, it also generates the need for additional efforts in terms of policy formulation (5.1), documentation creation (5.37), incident planning (5.24), training and awareness (6.3), and logging (8.15). Adherence to these controls is crucial for ensuring the successful implementation and ongoing maintenance of the solution.

In conclusion, the dual LDAP authentication solution proves to be a valuable tool for enhancing compliance with the ISO/IEC 27001 controls and requirements. Its ability to simultaneously support internal users with Google LDAP and external users with OpenVPN server access makes it a versatile and effective solution for organizations seeking to strengthen their VPN security posture while maintaining flexibility and cost-efficiency.

6 Summary

This thesis has explored the implementation of a VPN solution with dual LDAP authentication for a case study organization, addressing the challenges of providing secure and scalable remote access for its distributed workforce. The solution leverages OpenVPN Community Edition, Google Workspace's LDAP integration, and OpenLDAP to provide a robust and user-friendly VPN infrastructure that meets the organization’s business requirements. An extensive review of the ISO/IEC 27001 standard has been conducted to ensure the proposed solution fully aligns with the organization's security and compliance objectives.

By contextualizing the solution's effectiveness within the organization's unique business context, the thesis has provided a compelling case for its adoption. Has been demonstrated that the dual-factor LDAP authentication VPN solution not only meets the technical requirements of a secure and scalable VPN infrastructure but also aligns seamlessly with the organization's specific business objectives.

The implemented VPN solution has demonstrated a good level of compliance with the ISO/IEC 27001 standard for information security. The dual LDAP authentication approach effectively enforces role-based access control for both internal and external collaborators, aligning with control 5.15 and 5.16 of ISO/IEC 27001 Annex A, “Access control” and “Identity Management" respectively.

Furthermore, the user-friendly VPN client, comprehensive documentation, and integrated training have contributed to a positive user experience and improved adoption rates, fostering a compliant user environment. These aspects align with the requirements of control 6.3 of ISO/IEC 27001 Annex A, which emphasizes user training and awareness.

Despite these positive aspects, there are areas where the VPN solution could be further enhanced to improve its compliance with ISO/IEC 27001. The incorporation of more granular logging and auditing mechanisms could provide greater visibility into user

activities and access patterns, better aligning with control 8.5 of ISO/IEC 27001. Additionally, the implementation of regular vulnerability assessments and penetration testing could identify and address potential security weaknesses, further strengthening the overall compliance posture.

To further strengthen the security and compliance posture of the VPN solution, future research work could focus on the following areas:

- Exploration of advanced authentication mechanisms: Investigate the use of more advanced authentication mechanisms, such as FIDO2 and multi-factor authentication, to provide stronger authentication for VPN users.
- Integration with machine learning and artificial intelligence (AI): Explore the integration of machine learning and AI into the VPN solution to detect and prevent potential security threats and anomalies. This could provide an additional layer of protection and enhance the overall security posture.
- Compliance with additional security standards: Assess the VPN solution against additional security standards, such as HIPAA, PCI DSS, and GDPR, to ensure compliance with industry-specific requirements and strengthen the overall security posture.

By pursuing these research avenues, organizations can further enhance the compliance, security, and efficiency of their VPN solutions, ensuring a robust and compliant remote access infrastructure for their distributed workforce.

References

[1] *ISO/IEC 27000:2018, Information technology — Security techniques —Information security management systems — Overview and vocabulary*, ISO/IEC, Genève, May, 2018, standard. Accessed: Dec 10, 2023. Available: https://www.iso.org/standard/73906.html

[2] *ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection — Information security management systems — Requirements*, ISO/IEC, Genève, Oct, 2022, standard. Accessed: Dec 10, 2023. Available: https://www.iso.org/standard/27001

[3] W. Stallings, *Network Security Essentials: Applications and Standards*, 6th ed. Pearson Education Inc., Jul 13, 2021.

[4] W. Stallings and L. Brown, *Computer Security: Principles and Practice*, 5th ed. Pearson Education Inc., Jul 28, 2023.

[5] R. J. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 3rd ed. Wiley, Dec 22, 2020.

[6] R. Brandenburg and P. Mee, *Cybersecurity for a Remote Workforce*, MIT Sloan Management Review, Massachusetts Institute of Technology, Jul 23, 2020, article. Accessed Dec 10, 2023. Available: https://sloanreview.mit.edu/article/cybersecurity-for-a-remote-workforce/

[7] C. Scott, P. Wolfe and M. Erwin, *Virtual Private Networks*, 2nd ed. Cambridge, MA: O'Reilly Media, Inc., 1999.

[8] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed. Pearson Education Inc., Jan 1, 2017.

[9] G. Carter, *LDAP System Administration: Putting Directories to Work*, O'Reilly Media, Inc., Apr 29, 2003.

[10] T. Howes, M. Smith and G. S. Good, *Understanding and Deploying LDAP Directory Services*. 2nd ed. Addison-Wesley Professional, May 15, 2003.

[11] M. A. Qadeer, M. Salim and M. S. Akhtar, *Profile Management and Authentication Using LDAP*, 2009 International Conference on Computer Engineering and Technology, Singapore, 2009, pp. 247-251, doi: 10.1109/ICCET.2009.126.

[12] *ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection — Information security controls*, ISO/IEC, Genève, Mar, 2022, standard. Accessed: Dec 10, 2023. Available: https://www.iso.org/standard/75652.html

[13] *Cybersecurity Framework*, National Institute of Standards and Technology, Apr, 2019, standard, [Online]. Accessed: Dec 10, 2023. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[14] S. Frankel, P. Hoffman, A. Oreabaugh and R. Park, *Guide to SSL VPNs*, NIST Special Publication 800-113, National Institute of Standards and Technology, Jul,

2008, [Online]. Accessed: Dec 10, 2023. Available: https://csrc.nist.gov/pubs/sp/800/113/final

[15] *IETF RFC 4301 (Ipsec) — Security Architecture for the Internet Protocol*, Request for Comments (RFC) 4301, Internet Engineering Task Force (IETF), Dec, 2005. Accessed: Dec 10, 2023. Available: https://datatracker.ietf.org/doc/html/rfc4301

[16] *Health Insurance Portability and Accountability Act (HIPAA)*, U.S. Department of Health and Human Services, 1996. Accessed: Dec 10, 2023. Available: https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996

[17] *Payment Card Industry Data Security Standard (PCI DSS)*, Payment Card Industry Security Standards Council, 2022, standard. [Online]. Accessed: Dec 10, 2023. Available: https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf

[18] *General Data Protection Regulation (GDPR)*, Official Journal of the European Union (2016/679), Apr, 2016. [Online]. Accessed: Dec 10, 2023. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

[19] *Google Cloud Documentation*, Google, 2023. Accessed: Dec 10, 2023. Available: https://cloud.google.com/docs

[20] *Overview of Google identity management*, Google, 2023. Accessed: Dec 10, 2023. Available: https://cloud.google.com/architecture/identity/overview-google-authentication

[21] *About the Secure LDAP service*, Google, 2023. Accessed: Dec 10, 2023. Available: https://support.google.com/a/answer/9048516?hl=en

[22] *OpenVPN Access Server Admin Manual*, OpenVPN Inc., 2023. Accessed: Dec 10, 2023. Available: https://openvpn.net/access-server-manual/introduction/

[23] *OpenLDAP Software 2.6 Administrator's Guide*, OpenLDAP Foundation, 2023. Accessed: Dec 10, 2023. Available: https://www.openldap.org/doc/admin26/

[24] *Terraform About the Docs*, HashiCorp, 2023. Accessed: Dec 10, 2023. Available: https://developer.hashicorp.com/terraform/docs

[25] *Product Documentation for Red Hat Ansible Automation Platform 2.3*, Red Hat, 2023. Accessed: Dec 10, 2023. Available: https://access.redhat.com/documentation/en-us/red_hat_ansible_automation_platform/2.3

Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I Luca Mizzi

1 Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis “An ISO/IEC 27001 Compliance Assessment of an OpenVPN with Dual LDAP for Distributed Workforce Authentication”, supervised by Valdo Praust.

1.1 to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;

1.2 to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.

2 I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.

3 I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

04.01.2024

1 The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.

Appendix 2 – Code Snippet – Client Management via Ansible

The provided YAML code snippet is an Ansible playbook that automates the creation of client profiles for the OpenVPN server, as well as revokes outdated client certificates.

The Playbook consists of six tasks: Add generate-client script, Add directory for clients, Create client profiles, Find existing clients, Revoke outdated client certificates, and Notify restart of OpenVPN.

```
---
- name: OpenVPN | Add generate-client script
  ansible.builtin.template:
    dest: /usr/local/bin/generate-client
    mode: 0755
    src: generate-client.j2

- name: OpenVPN | Add directory for clients
  ansible.builtin.file:
    path: /etc/openvpn/{{ item }}/client
    state: directory
  loop: "{{ openvpn_profiles.keys() | list }}"

- name: OpenVPN | Create client profile
  ansible.builtin.shell:
    cmd: /usr/local/bin/generate-client {{ item.0.key }} {{ item.1 }}
    creates: /etc/openvpn/{{ item.0.key }}/client/{{ item.1 }}.ovpn
  with_subelements:
    - "{{ openvpn_profiles | dict2items }}"
    - value.clients
  loop_control:
    label: "{{ item.0.key }}/{{ item.1 }}"
```

Figure 2. ansible/roles/openvpn/tasks/clients.yaml (1).

```
- name: OpenVPN | Find existing clients
  ansible.builtin.find:
    paths: /etc/openvpn/{{ item }}/client
    patterns: "*.ovpn"
  loop: "{{ openvpn_profiles.keys() | list }}"
  register: clients

- name: OpenVPN | Revoke client
  ansible.builtin.shell:
    chdir: /etc/openvpn/{{ profile }}/easy-rsa
    cmd: |
      yes yes | ./easyrsa revoke {{ user }}
      ./easyrsa gen-crl
      rm -rf /etc/openvpn/{{ profile }}/client/{{ user }}.ovpn
  when: user not in openvpn_profiles[profile].clients
  with_subelements:
    - "{{ clients.results }}"
    - files
  notify: restart openvpn {{ profile }}
  vars:
    user: "{{ item.1.path | basename | regex_replace('(.*)\\.ovpn', '\\1') }}"
    profile: "{{ item.1.path.split('/')[-3] }}"
  loop_control:
    label: "{{ profile }}/{{ user }}"
```

Figure 2. ansible/roles/openvpn/tasks/clients.yaml (2).

Appendix 3 – ISO/IEC 27001 VPN Implementation Guideline

This comprehensive guideline, presented in a checklist format, serves as a valuable resource for organizations seeking to integrate a VPN solution while ensuring strict adherence to ISO/IEC 27001 requirements.

Intended Audience

The primary audience for this document includes individuals responsible for the IT infrastructure of an organization, such as Chief Technology Officers (CTO) or those overseeing the Information Security Management System (ISMS) as Chief Information Security Officers (CISO). Additionally, this guideline can prove to be a useful reference for DevOps professionals or System Administrators tasked with the deployment and maintenance of VPN servers.

Methodology

The checklist is derived from an in-depth study of the ISO/IEC 27001 standard and its Annex A. To enhance clarity and understanding, the ISO/IEC 27002 standard has also been utilized, providing additional guidance and insights into the list of relevant controls.

ISO/IEC 27001 VPN Implementation Check List

Risk Assessment and Management:

- ✔ Identify and document all **information assets** within the organization. Evaluate the relevance and importance of each information asset concerning the VPN implementation.
- ✔ Based on the information assets identified, perform a comprehensive **risk assessment** specifically tailored to the VPN implementation. Ensure that risks associated with the VPN implementation are integrated into the broader organizational risk assessment and information asset management.
- ✔ Develop robust **mitigation strategies** derived from the identified risks.

Organizational Controls:

- ✔ Ensure the VPN implementation aligns with the organization's overarching **information security policy**. This includes explicit mention of VPN usage, access controls, and encryption protocols.
- ✔ Establish clear roles and responsibilities for individuals involved in VPN administration and operation. Define and communicate the **organizational structure** supporting VPN security.
- ✔ Clearly **define responsibilities** for managing and protecting VPN-related assets, including servers, cryptographic keys, and configuration files.
- ✔ Develop policies and procedures governing the **secure transfer of information** over the VPN, addressing data integrity and confidentiality.

- ✔ Develop a comprehensive **access control** policy that explicitly covers VPN access. This policy should specify who has access, under what circumstances, and what controls are in place.

- ✔ Implement a robust user **access management process** for VPN users, including user provisioning, de-provisioning, and periodic access reviews.

- ✔ Ensure that **suppliers** involved in providing VPN-related services adhere to information security requirements and standards.

- ✔ Develop and implement an **incident response plan** specific to VPN security incidents, emphasizing timely detection, reporting, and resolution.

- ✔ Ensure that VPN operations comply with **legal and contractual requirements** related to information security.

- ✔ Conduct **periodic reviews and audits** specifically focused on the information security aspects of VPN operations.

- ✔ Develop and **document operational procedures** specific to VPN management, encompassing routine maintenance, incident response, and change management.

People Controls:

- ✔ Implement **background checks** and security screenings for personnel involved in VPN administration to mitigate insider threats.

- ✔ Provide ongoing **training and awareness** programs for personnel involved in VPN operations. This ensures they are well-versed in security best practices.

- ✔ Develop **procedures for promptly revoking VPN access** for employees whose employment has been terminated or who have changed roles.

Physical Controls:

- ✔ Ensure **physical security** measures are in place to protect servers and networking equipment hosting the VPN infrastructure.
- ✔ Implement **safeguards to protect VPN equipment** from physical tampering or unauthorized access.

Technological Controls:

- ✔ Enhance user authentication mechanisms by implementing **multi-factor authentication** (MFA).
- ✔ Refrain from utilizing **split tunnelling** solutions when possible.
- ✔ Ensure that **access controls are configured** and enforced not only at the user level but also at the system and application levels within the VPN infrastructure.
- ✔ Establish **comprehensive logging and monitoring capabilities** within the VPN infrastructure to detect and respond to security events.
- ✔ Ensure that **network security** measures are implemented and maintained to protect the confidentiality and integrity of VPN communications.
- ✔ Define and implement cryptographic controls for the VPN, including the use of **strong encryption algorithms** for data in transit and secure key management practices.