Firehawk Consulting

The following report was prepared on behalf of SwiftTech.

Thank you for giving Firehawk Consulting the opportunity to review your security posture in anticipation of performing a SOC II security assessment.

We hope you find the notes below as you begin your journey. Please do not hesitate to contact us if you have further questions.

For

SwiftTech

Firehawk Consulting

After review, Firehawk has noted the following areas of concern. You may wish to consider updating policy and security controls based on your current business goals, risk management posture, and compliance considerations.

Controls

Data Storage

- VPC3 File storage supports only AES-128 encryption
- Databases in production environment are unencrypted

End User Management

- Internal Network users require a 7-character password
- Passwords never expire
- VPN access does not require MFA

Network Controls

- TLS v1.1 is used between the cloud production environment and SwiftTech’s physical location
- Application development Tiers are not logically segmented from Business Application servers

Patching and Vulnerability Management

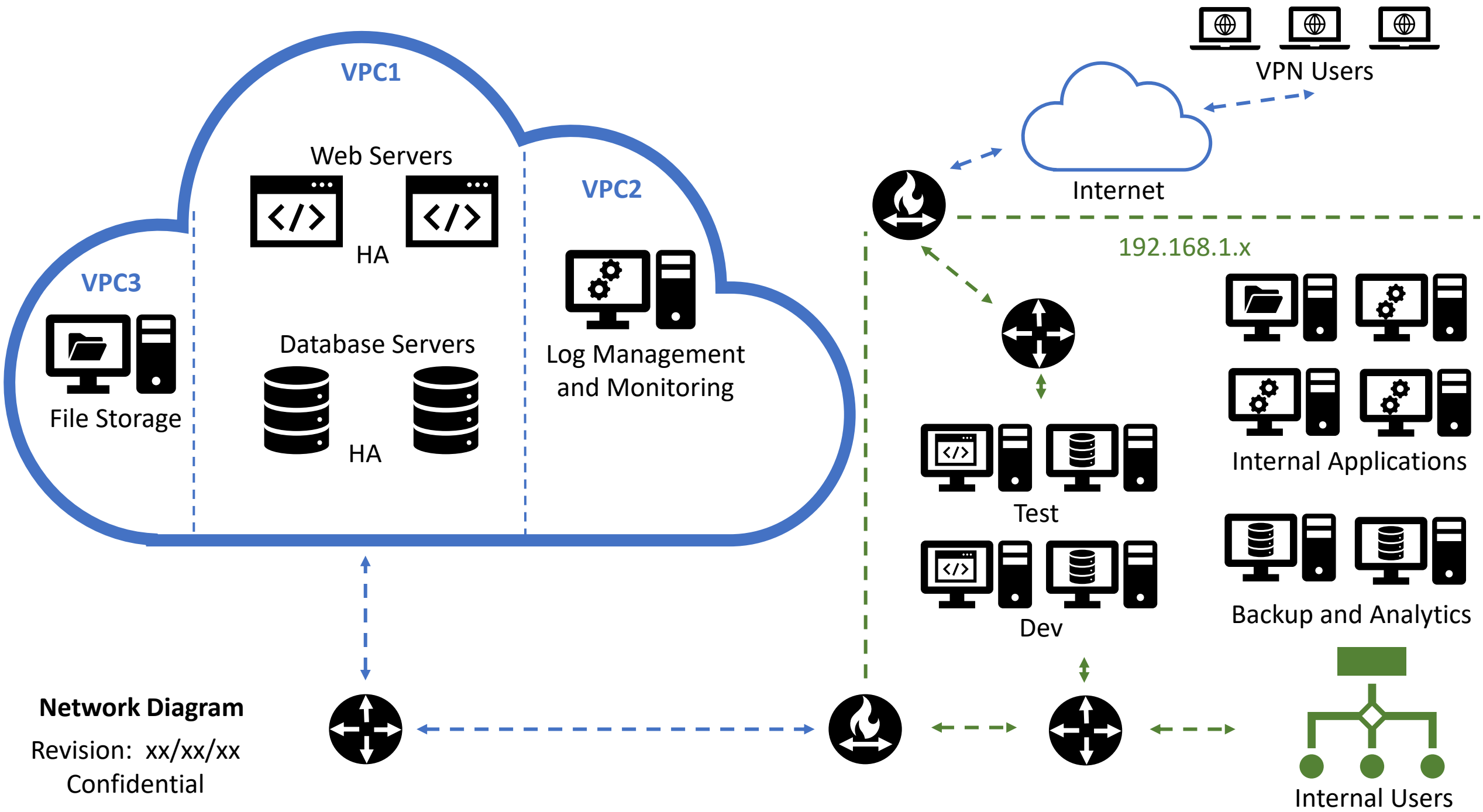
- Development Tier servers are unpatched and contain multiple vulnerabilities

Secure Software Development

- Application code is not scanned for vulnerabilities before being published into production environment

SwiftTech

Speed, Flexibility, Success



Network Diagram

Revision: xx/xx/xx

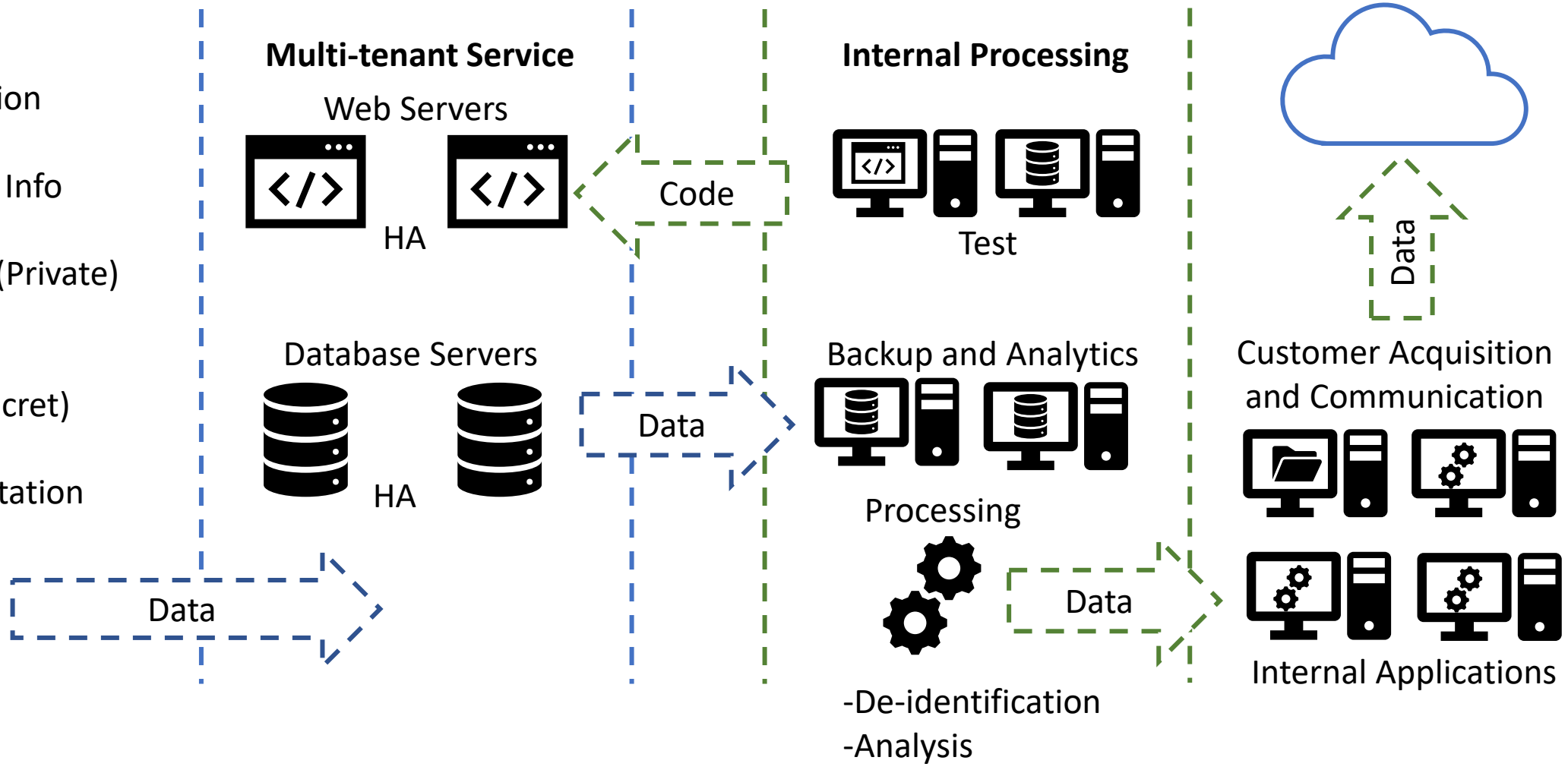
Confidential

Inputs

Company Registration
- Company Name
- Company Contact Info

User Registration
- User Information (Private)
- Role Assignment

Data Input
- Project Details (Secret)
- Project Timelines
- Related Documentation



Data Flow Diagram

Revision: xx/xx/xx

Confidential

Security Posture (1.)

SwiftTech

SwiftTech's overall cybersecurity risk posture can be described as Risk Accepting. The organization demonstrates a willingness to accept certain levels of risk in their current security controls and practices. This posture is evident from several key facts about SwiftTech's approach to security. Firstly, the use of unencrypted databases in the production environment indicates a tolerance for the risk of data exposure or unauthorized access. Additionally, the lack of encryption beyond AES-128 for file storage suggests a willingness to compromise on data protection. Furthermore, the absence of multi-factor authentication (MFA) for VPN access indicates a lower priority given to securing remote connections. Lastly, the presence of unpatched and vulnerable servers in the development tier demonstrates a level of acceptance of the associated risks. Collectively, these factors suggest that SwiftTech is more inclined to accept certain risks rather than invest in more robust security measures, potentially due to considerations such as cost, convenience, or a perception that the current level of risk is within acceptable limits for the organization.

Relevant Frameworks (2.)

SwiftTech

Health Insurance Portability and Accountability Act (HIPAA): HIPAA is a crucial framework for healthcare organizations that handle protected health information (PHI). Since the MSA excerpt is from a healthcare provider, compliance with HIPAA is essential. By incorporating HIPAA's security and privacy requirements, such as the Security Rule and Privacy Rule, ProjectTrackPlus can align its security controls and risk management practices with industry standards specific to healthcare data protection.

National Institute of Standards and Technology (NIST) Cybersecurity Framework: The NIST Cybersecurity Framework provides a comprehensive set of guidelines, standards, and best practices for managing cybersecurity risks. It encompasses five core functions: Identify, Protect, Detect, Respond, and Recover. Adopting the NIST framework will help ProjectTrackPlus assess its existing security controls against industry-recognized standards and identify areas for improvement. It provides a flexible and scalable approach that can be applied across various industries, including healthcare, making it well-suited for the diverse customer base.

These frameworks were chosen because they are widely recognized and widely adopted in the healthcare industry. Compliance with HIPAA is not only necessary to legally handle PHI but also essential for building trust with healthcare customers. By aligning with the NIST Cybersecurity Framework, ProjectTrackPlus can ensure a holistic and systematic approach to risk management, covering all aspects of cybersecurity. Together, these frameworks will enable ProjectTrackPlus to assess its security controls, identify gaps, and establish a robust risk management framework that meets regulatory requirements and instills confidence in potential healthcare customers.

Audit Against Frameworks (3.)

SwiftTech

The concern raised is regarding the use of AES-128 encryption for VPC3 File storage.

Based on my research, it suggests to upgrade the encryption for file storage to a stronger level, such as AES-256, for enhanced data security.

Implement a secure code review process that includes scanning application code for vulnerabilities before it is published into the production environment. This helps identify and remediate security flaws early in the development lifecycle

Governance Mechanisms for End-User Management Controls (6.)

SwiftTech

1.Access Controls a. Password Security:

1. All users must create and maintain strong, unique passwords.
2. Password are managed using a Password Management tool (provided and maintained by the organization ex: Okta)
3. A Password policy rule will be created and requested to all users, based on the following criteria: minimum 16 characters long, have Lowercase and Uppercase and 2 special characters / renew every 90 days.

2. Multi-Factor Authentication (MFA):

1. Use at least two of the following factors: (Password and PIN / Password and fingerprint / password and facial scan / password and SMS / PIN and fingerprint, PIN/ facial scanner)
2. User Account Management:
3. User accounts will be managed by the principle of least privilege.
4. Every trimester the user accounts will be reviewed.

3.Encryption and Data Protection a. Data Encryption:

1. All sensitive data at rest must be encrypted using strong encryption algorithms, such as AES-256.

4.Patch Management a. System Patching:

1. Regular patch management processes
2. Critical patches must be applied within 24h (no more than 1 working day)
3. Patch Management tool will force an updates to all computers in order to meet the requirement.