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

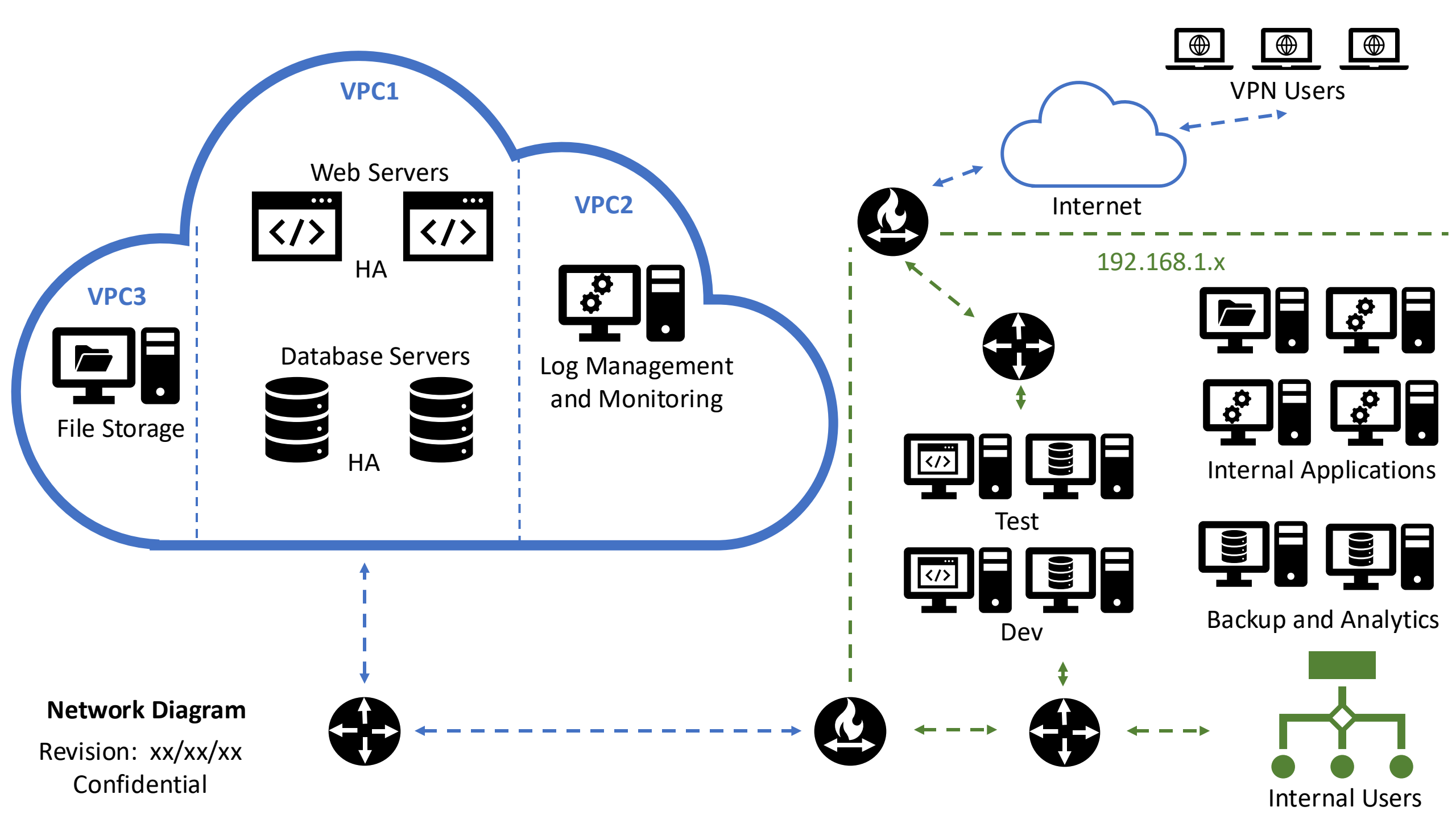
- Development Tier servers are unpatched and contain multiple vulnerabilities

Secure Software Development

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

SwiftTech

Speed, Flexibility, Success

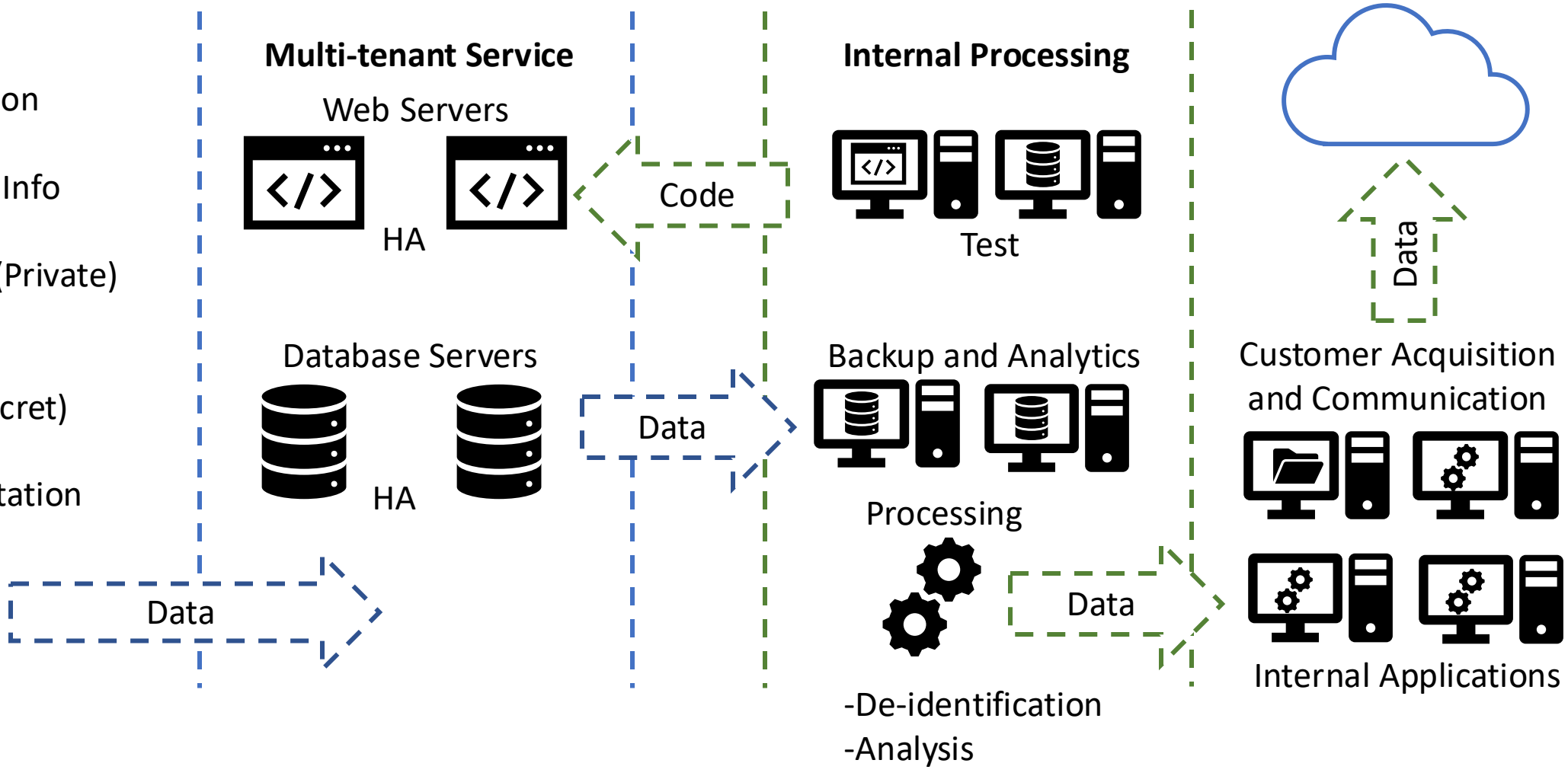

VPC1
Web Servers
HA
VPC2
Log Management
and Monitoring
VPC3
File Storage
Database Servers
HA
VPN Users
Internet
192.168.1.x
Test
Dev
Internal Applications
Backup and Analytics
Internal Users
Network Diagram
Revision: xx/xx/xx
Confidential

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 best described as **Risk Neutral**.

This posture reflects SwiftTech's commitment to balancing its rapid innovation and time-to-market goals with the growing demands for robust cybersecurity measures.

As a company that values speed and flexibility, SwiftTech must accept a certain level of risk to maintain its competitive edge.

However, the recent steps taken, such as pursuing a SOC II attestation and hiring Firehawk Security for a readiness assessment, demonstrate a clear recognition of the importance of strong security controls.

SwiftTech's proactive approach to addressing potential vulnerabilities while continuing to innovate underscores its strategy of managing risks effectively without hindering its ability to achieve success.

Relevant Frameworks (2.)

SwiftTech

For SwiftTech's ProjectTrackPlus, the most relevant regulatory frameworks and standards to measure our existing security controls are SOC 2, HIPAA, and ISO/IEC 27001.

1. SOC 2: This framework is critical as it focuses on five trust service criteria: security, availability, processing integrity, confidentiality, and privacy. Since SwiftTech aims to serve large organizations, including healthcare providers and government agencies, achieving SOC 2 compliance will help establish a strong baseline for cybersecurity controls and provide assurance to customers that their data is handled securely.

2. HIPAA: Given that one of our potential customers is a large healthcare system in Minnesota, compliance with the Health Insurance Portability and Accountability Act (HIPAA) is essential. HIPAA sets the standard for protecting sensitive patient data, and incorporating its guidelines into our risk management framework will ensure that SwiftTech meets the stringent privacy and security requirements expected by healthcare providers.

3. ISO/IEC 27001: This international standard for information security management systems (ISMS) provides a comprehensive approach to managing information security risks. Adopting ISO/IEC 27001 will help SwiftTech align its security practices with global best practices, further reinforcing our commitment to maintaining high levels of security and risk management in our SaaS offerings.

Audit Against Frameworks (3.)

SwiftTech

1. AES-128 Encryption for File Storage (VPC3)

• **SOC 2** and **ISO/IEC 27001** both recommend using strong encryption for data at rest. While AES-128 is considered secure, current best practices favor AES-256 for stronger protection, especially for sensitive data.
• **Recommendation:** Upgrade to AES-256 encryption for file storage to align with best practices and provide stronger protection for customer data.

2. Unencrypted Databases in Production Environment

• Both **HIPAA** and **SOC 2** emphasize the need to encrypt sensitive data, particularly in environments handling personal health information (PHI) or customer data.
• **Recommendation:** Encrypt all production databases to comply with HIPAA and SOC 2 requirements and ensure that sensitive data is adequately protected.

3. End User Management - 7-Character Passwords with No Expiration

• **ISO/IEC 27001** and **SOC 2** both advocate for strong password policies, which typically recommend passwords of at least 8 characters and periodic expiration to mitigate risks associated with password compromise.
• **Recommendation:** Increase the minimum password length to 8 characters and implement a password expiration policy to enhance security and align with industry standards.

4. VPN Access Without MFA

• Multi-factor authentication (MFA) is a critical control recommended by **SOC 2** and **ISO/IEC 27001** to protect remote access points such as VPNs.
• **Recommendation:** Implement MFA for VPN access to reduce the risk of unauthorized access and strengthen compliance with security frameworks.

5. Use of TLS v1.1 Between Cloud and Physical Location

• **SOC 2** and **ISO/IEC 27001** recommend the use of the latest versions of secure protocols for data transmission. TLS v1.1 is considered outdated and may be vulnerable to security threats.
• **Recommendation:** Upgrade to TLS v1.2 or higher to ensure secure communication between the cloud environment and SwiftTech's physical location.

6. Lack of Logical Segmentation Between Application Development Tiers and Business Application Servers

• **HIPAA** and **SOC 2** both emphasize the importance of network segmentation to limit access to sensitive data and reduce the impact of potential breaches.
• **Recommendation:** Implement logical segmentation between development and production environments to prevent unauthorized access and reduce risk.

7. Unpatched Development Tier Servers with Vulnerabilities

• Regular patching and vulnerability management are critical aspects of **ISO/IEC 27001** and **SOC 2** frameworks. Unpatched systems are a common attack vector for cyber threats.
• **Recommendation:** Establish a regular patch management process to ensure that all servers, particularly those in development, are kept up to date with the latest security patches.

8. Lack of Code Vulnerability Scanning Before Production Deployment

• **SOC 2** and **ISO/IEC 27001** advocate for secure software development practices, including regular code reviews and vulnerability scanning.
• **Recommendation:** Implement automated code scanning tools as part of the software development lifecycle (SDLC) to detect and remediate vulnerabilities before code is deployed to production.

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

SwiftTech

1. Password Policy Enforcement and Compliance Auditing

• **Policy Enforcement**: Implement an automated policy enforcement tool that ensures all user accounts adhere to the minimum password length, complexity, and expiration requirements as defined in the updated Information Security Policy. This tool will enforce:
• A minimum password length of 12 characters.
• The inclusion of at least one uppercase letter, one lowercase letter, one number, and one special character.
• Password expiration every 90 days.
• **Compliance Auditing**: Set up regular automated audits that generate reports on password compliance. The audit reports should flag any accounts that do not meet the policy requirements, and corrective actions should be taken immediately. Non-compliant accounts should be required to update their passwords upon their next login.

2. Multi-Factor Authentication (MFA) Enforcement and Monitoring

• **MFA Implementation**: Ensure that MFA is enabled and enforced for all users accessing the VPN and any other remote access solutions. This can be managed using an Identity and Access Management (IAM) system that integrates with SwiftTech's existing infrastructure.
• **Continuous Monitoring**: Implement a monitoring system that logs all MFA-related activities. Any attempts to bypass or disable MFA should trigger an alert to the security team. Regular reviews of these logs should be conducted to ensure that MFA is consistently applied across all users.

3. Access Control Reviews and User Role Audits

• **Access Control**: Regularly review user roles and access levels to ensure that they are appropriate for each user's current responsibilities. This should include:
• An initial baseline review of all user accounts and roles.
• Periodic audits (e.g., quarterly) to ensure that access controls remain appropriate as users' roles change.
• Immediate reviews following any significant organizational changes, such as department restructures or mergers.
• **Audit Trails**: Maintain detailed audit trails for all changes to user roles and permissions. This includes who made the change, when it was made, and why. Regularly review these logs to ensure that no unauthorized changes have been made.

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

SwiftTech

4. Incident Response for Non-Compliance

• **Automated Incident Response**: Set up an automated incident response mechanism that triggers when non-compliance is detected. For example, if an audit finds a user account that does not comply with the password policy or if MFA is not enabled, the system should automatically:
• Lock the account.
• Notify the user and the IT security team.
• Provide instructions for the user to regain access in compliance with the policy.
• **Documentation and Reporting**: Document all incidents of non-compliance and the actions taken to resolve them. This documentation should be reviewed during governance meetings to assess the effectiveness of current controls and make adjustments as necessary.

5. Continuous Training and Awareness Programs

• **User Training**: Implement regular training programs for all employees that cover the importance of password security, MFA, and general cybersecurity best practices. These should be mandatory and include assessments to ensure understanding.
• **Awareness Campaigns**: Conduct periodic awareness campaigns to reinforce the importance of adhering to security policies. This could include emails, posters, and workshops focused on new threats and how the company's policies help mitigate them.

Thank you for the attention!