



	Risk	Risk Family
	Stored customer and ePHI data vulnerable to unauthorized access due to weak encryption (AES-128)	
1	Unauthorized access to sensitive production data due to lack of database encryption	Data at Rest
2	Regulatory non-compliance and potential contract termination with healthcare customers	Data at Rest
2b	User accounts vulnerable to brute force and dictionary attacks due to weak password requirements	Data at Rest
3	Compromised credentials remaining valid indefinitely, enabling persistent unauthorized access	User Access
4	Remote access compromise due to single-factor authentication on VPN	User Access
5	Data in transit vulnerable to interception and man-in-the-middle attacks due to deprecated TLS version	User Access
6	Lateral movement from development to production environments, enabling data breach or system compromise	Data in Transit
7		Network Security

Accidental or unauthorized modification
of production systems by developers

7b Network Security

Exploitation of known vulnerabilities in
development servers leading to system
compromise

8 Vulnerability Management

Deployment of vulnerable application
code to production, creating exploitable
security flaws

9 Secure Code

Notes:

Risk - descriptions should be some reasonable approximation of what is written above

Reasoning - The reasoning should approximately match to the user's assessment of
it might be high

Mitigating Controls - For the purpose of this exercise we did not include mitigating controls

Total Risk Score - Should not be less than a reasonable approximation of the likelihood

Security Risk Assessment

Control	Likelihood	Impact
VPC3 File storage only supports AES-128 Encryption	Low	Medium
Databases in production are unencrypted	Medium	High
Databases in production are unencrypted	High	High
Internal network users require a 7-character password	High	High
Passwords never expire	High	High
VPN Access does not require MFA	Medium	High
TLS V1.1 is used between the cloud production environment and SwiftTech's physical location	High	High
Application development Tiers are not logically segmented from Business Application servers	Medium	Medium
	High	Medium

Application development Tiers are not logically segmented from Business Application servers

Medium Medium

Development Tier servers are unpatched and contain multiple vulnerabilities

Medium High

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

High High

ove but does not need to be exact

† the likelihood and impact of a potential risk. If, for instance the liklihood and imp

controls

od x impact. For instance, if L=High and I=High (and no mitigating control exists)

Reasoning	Mitigating Controls	Total Risk Score
AES-128 does not meet the MSA requirement for AES-256 or stronger encryption. Healthcare data is a high-value target for	None	High
Unencrypted databases expose all stored data to anyone with database access or in the event of a breach. This violates healthcare	None	High
MSA Section 14.4 explicitly requires strong encryption for all company information. Failure to comply gives the customer exclusive right to terminate the agreement after	None	High
Industry best practice (NIST SP 800-63B) recommends minimum 8-character passwords, with 12-15 characters preferred for sensitive systems. 7-character passwords can	None	High
Without password expiration, compromised credentials from phishing, breaches, or social engineering remain valid indefinitely. While modern MFA is critical for remote access security. Without it, stolen credentials (via phishing,	None	High
keyloggers, credential stuffing) provide immediate network access	None	High
TLS 1.1 has known vulnerabilities and has been deprecated by major standards bodies (PCI DSS, NIST). Industry standard requires TLS 1.2	None	High
or 1.3. Medium likelihood as Development environments typically have weaker security controls and are more likely to be compromised. Without segmentation, attackers can pivot	None	Medium

Without segmentation, developers may have excessive access to production systems. This creates risk of accidental changes, unauthorized testing in production, or insider threats.	Medium	None	Medium
Unpatched systems with known vulnerabilities are easily exploited using publicly available tools. Combined with lack of network segmentation (Risk #7), compromised dev servers become launchpad for production attacks.			
High likelihood given automated scanning by attackers, high impact MSA Section 14.5 explicitly requires code to be tested and free of medium/high security flaws before production deployment. Without scanning, vulnerabilities like SQL injection, XSS, or authentication issues are present.	None	None	High
			High

Impact are marked high, the reasoning should reflect why

then Risk cannot equal Low