| Security Risk Ass | | | |
|---|---|---|---|
| Risk # | Risk | Risk Family | Control |
| 1 | VPC3 File storage supports only AES-128 Encryption | Data at Rest | VPC3 File storage only supports AES-128 Encryption |
| 2 | Databases in production are unencrypted | Data at Rest | Databases in production are unencrypted |
| 2b | Databases in production are unencrypted | Data at Rest | Databases in production are unencrypted |
| 3 | Internal network users require a 7-character password | User Access | Internal network users require a 7-character password |
| 4 | Passwords never expire | User Access | Passwords never expire |
| 5 | VPN Access does not require MFA | User Access | VPN Access does not require MFA |
| 6 | TLS V1.1 is used between the cloud production environment and SwiftTech's physical location | Data in Transit | TLS V1.1 is used between the cloud production environment and SwiftTech's physical location |
| 7 | Application development Tiers are not logically segmented from Business Application servers | Network Security | Application development Tiers are not logically segmented from Business Application servers |

| | | | |
|---|---|---|---|
| 7b | Application development Tiers are not logically segmented from Business Application servers | Network Security | Application development Tiers are not logically segmented from Business Application servers |
| 8 | Development Tier servers are unpatched and contain multiple vulnerabilities | Vulnerability Management | Development Tier servers are unpatched and contain multiple vulnerabilities |
| 9 | Application code is not scanned for vulnerabilities before being published into production environment | Secure Code | Application code is not scanned for vulnerabilities before being published into production environment |

**Notes:**
Risk - descriptions should be some reasonable approximation of what is written above but does not need to be e
risk Family -
Data at Rest
,Data in Transit,
User Access
,Secure Code,
Network
Security,
Vulnerability
Management

Likelihood - Low,
Medium, High
Impact - Low,
Medium, High

Reasoning - The reasoning should approximately match to the user's assessment of the liklihood and impact of a
reasoning should reflect why 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 liklihood x impact. For instance, if L

**essment**

| Liklihood | Impact | Reasoning | Mitigating Controls | Total Risk Score |
|---|---|---|---|---|
| Medium | Medium | AES-128 encryption is considered weak for sensitive data. | Placeholder<br>Assume none | Medium |
| Medium | High | Unencrypted databases increase the risk of data breaches. | Placeholder<br>Assume none | High |
| Medium | High | Unencrypted databases increase the risk of data breaches. | Placeholder<br>Assume none | High |
| Low | Medium | Longer passwords provide better security against brute force attacks. | Placeholder<br>Assume none | Low |
| Low | Medium | Expired passwords pose a security risk due to potential unauthorized access. | Placeholder<br>Assume none | Low |
| Low | High | Lack of MFA increases the risk of unauthorized access. | Placeholder<br>Assume none | Low |
| Low | Medium | TLS v1.1 is an outdated protocol with known vulnerabilities. | Placeholder<br>Assume none | Low |
| Medium | High | Lack of logical segmentation increases the risk of lateral movement and unauthorized access. | Placeholder<br>Assume none | High |

| | | | | |
|---|---|---|---|---|
| Medium | High | Lack of logical segmentation increases the risk of lateral movement and unauthorized access. | Placeholder<br>Assume none | High |
| High | High | Unpatched servers with known vulnerabilities increase the risk of exploitation. | Placeholder<br>Assume none | High |
| High | High | Lack of vulnerability scanning increases the risk of deploying vulnerable code. | Placeholder<br>Assume none | High |

exact

potential risk.  If, for instance the liklihood and impact are marked high, the

=High and I=High (and no mitigating control exists) then Risk cannot equal Low