Security Risk Assessment

Risk #	Risk	Risk Family	Control	Likilhood	Impact	Reasoning	Mitigating Controls	Total Risk Score
	File strong can be at risk for brute force attack.	Data at Rest	VPC3 File storage only supports AES-128 Encryption	Medium	Medium	AES-128 has 10 rounds but AES 256 has 14 rounds. The more rounds means that the more complex and difficult for brute-force attacks to guess.		Medium
1	Give attackers access to sensitive information.	Data at Rest	Databases in production are unencrypted	High	High	Encrypted as well as authenication of Databases in Production is necessary to protect particulary personally identifiable information (PII) from being accessed from attackers. Encryption and authenication will reduce the risk of the data/information from being used by attackers from transferring the information to the attacker's system or perform other actions that jeopardize the confidentaility of the data/information.	Placeholder Assume none Placeholder Assume none	High
2	Attackers can affect the integrity of the information	Data at Rest	Databases in production are unencrypted	High	High	Encryption will protect the data/information from being modified or destructed.	Placeholder Assume none	High
2b	7-character password or less increases the risk for brute force attacks as well as dictionary attacks	User Access	Internal network users require a 7-character password	High	High	The character length of a password can be affected by an offline attacks when one or more hashed passwords is given by the attacker through a data breach.		High
3	Increase admin as well as user accounts from being compromised	User Access	Passwords never expire	Medium	Medium	There are no NIST and SANS standards that explicity require no passwords expiration. There has been a movement to get rid of password expiration due to: outdated threat model, behavorial cost, and increasing risk. Need to encourage the use of long passphases, ensure evey account has a unique password, use Multi-Factor Authenication, and only change employees passwords if it has been compromised.	Placeholder Assume none Placeholder Assume none	Medium
4	Increase risk of attackers from accessing users accounts	User Access	VPN Access does not require MFA	High	High	MFA will provide a higher level of identity assurance/authenication of a user attempting to access a network via VPN.	Placeholder Assume none	High
5	Increase the risk for downgraded attacks	Data in Transit	TLS V1.1 is used between the cloud production environment and SwiftTech's physical location	High	High	TLS V1.1 use SHA-1 hash, which is cryptographically broken, for the integrity of exchanged messages. This makes it easier for an attacker to impersonate a server for Man In the Middle attacks.	Placeholder Assume none	High
6	Application development not logically separated from Business Application servers will increase risk for attack surfaces and an attackers' lateral movement and access escalation into other areas of the network.	Network Security	Application development Tiers are not logically segmented from Business Application servers	High	High	Using network segmentation and access controls to separate from each other within each non production environment will reduce the risk of attacks in this area as well as other areas.	Placeholder Assume none	High
7	Application development not logically separated from Business Application servers will increase risk for unauthorized access for each environment.	Network Security	Application development Tiers are not logically segmented from Business Application servers	High	High	Without tight restrict connections and authentication, can increase the probability of internal and/or external attack	Placeholder Assume none	High
7b	Increase the risk for Cross-Site Scripting and SQL Injection	Vulnerability Management	Development Tier servers are unpatched and contain multiple vulnerabilities	High	High	Within the Software Development Lifecycle, there are 3 tiers/levels. At each level/tier, there are security controls that should be in implemented especially if sensitive information is involved. For instance,automated patch mangement and/or automated security tools.	Placeholder Assume none	High
8	Servers that are upatched will increase risk for vulnerabilities and attacks.	Vulnerability Management	Application code is not scanned for vulnerabilities before being published into production environment	High	High	Without using any code analysis tools, developers will not be able to detect any security bugs. In addition, automated security testing tools should be incorporated in the development lifecysle.	Placeholder Assume none	High
9								

Notes:

Risk - descriptions should be some reasonable approximation of what is written above but does not need to be exact

Reasoning - The reasoning should approximately match to the user's assessment of the liklihood and impact of a potential risk. If, for instance the liklihood and impact are marked high, the 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=High and I=High (and no mitigating control exists) then Risk cannot equal Low