Risk Number	Control Objective	Risk Rating	Risk Owner	Risk Description	Project Objective Impact	Potential Mitigation	Potential Response	Risk Probability
R1	Root Privileges are limited to proper people and locked down	9	IT Department	Unauthorized people with root access can cause damage or change rules in the system which needs to be locked down	Any and everything could be damaged if unauthorized users gain root access	By locking down root from unauthorized users and harden the config prevents user escalation that has not been approved	Lockdown Root account with strong passwords and authentication methods.	0.32
R2	Admin to Windows and Unix systems are given to proper personel and locked down	7.2	IT Department	Only People with authorization should have admin privileges to prevent an insider attack	Sensitive data could be breached due to unauthorized users having access to the system and would be difficult to log	audit accounts to make sure only pre approved users have the role	Remove privileges from accounts that do not require admin rights.	0.3
R3	Proper Password configurations set in systems	8.8	IT Department	Users need to use stronger password so attackers have a harder time to crack passwords	attackers could easily crack passwords due to weak passwords	Establishing strong password policies and ensuring all user adhere to it.	Utilize group policies to push for stronger password policies and standards.	0.2
R4	Proper user authentication with passwords and enable MFA were capable	8.8	IT Department	Password policies need to be implemented properly so nobody is able to bypass authentication which would allow better logs to know who is accessing the account	By not having MFA nobody would know if the users was the real user due to only knowing the name of the account	ensure all users authenticate upon logging into their workstations to ensure proper logs are maintained.	Utilize group policies to push for proper authentication and prevent any auto login systems.	0.2
R5	Account management	7.8	Info Sec	Audit accounts and delete accounts that aren't active in the organization.	By leaving old accounts in the system anyone knowing the login to the account could gain access to the system	Audit accounts to deleted old and unused account.	check account logs and implement least privilege policies.	0.8
R6	Network Segmentation between production, and Testing, and Development Environments	6.6	IT Networking Department	isolated all environments from each other so that no one has access to another environment	Not separating production, testing and development environments can cause unexpected problems across our system and makes it easier for threat actors to access out systems.	Properly separating our network from production, development and testing to prevent any problems.	all environments were seperated which allows more security	0.25
R7	Unauthorized code changes and implementation	6.1	Dev Team	code needs to be changed so that we can maintain logs	Makes it difficult to track changes	setting a standard guide for code changes, so it may be tested first to prevent any problems in our production side.	implement and support a standard for implementing code changes.	0.6
R8	Backups need to be tested	6.5	IT department	Ensure that back ups are maintained properly so that in worst case they are secure and are up to date	We would not be able to restore systems if data were to be lost	Set up periodic standard to test our backups.	test and maintain backups.	0.2
R9	alternative power sources for disaster response	6.5	Operations	we need to ensure we can provide back up power incase of emergency	the system could go down if we dont have alternate data in emergency	Set up periodic standard to test our backup power source.	Perform maintenance and routine inspect backup power sources.	0.2
R10	Improper database access (RBAC)	5.5	IT department	Ensure that roles only have the required access given to them	Unauthorized users could expose sensitive data and compromised accounts can lead to a leak of said data.	Audit accounts to limit authorized users to be approved first.	audit and remove privileges from users that do not require it.	0.6