Risk number	Risk rating	Risk owner	Description	Project objectives impacted	Risk probability	Risk impact	Potential triggers	Potential mitigation	Potential responses	Root causes
1	8.0 High	Linux and Solaris Administrators	**Security Vulnerability** Personnel within the Unix (Linux/Solaris) environments with administrative privileges are logging with 'root' username both from the console physically connected to the computer and from the network.	Scope	0.2	6.9	The security policy for this project does not address CSC Control 5: Controlled Use of Administrative Privileges	*Warning: Before you block access to root account, create an administrative account.* **Linux :** 1. To disable the 'root' username from being used, go to the **/etc/password** file and change **/bin/bash** to **sbin/nologin** 2. To disable SSH root login, first, go to the /etc/ssh/sshd_config file and set PermitRootLogin to "no", then restart sshd service to apply changes 3. To prevent the 'root' user from logging in at the console attached to the machine, remove the contents in the '/etc/securtty' file by entering 'echo > /etc/securetty' at the command line.	Mitigate by following the Potential Mitigation steps to reduce the probability of occurrence or the impact of the risk.	Unix-like operating systems come with the default 'root' username having administrative permissions and being able to log in from the console and the network.
								Warning: Before you block access to root account, create an administrative account. **Solaris:** Note: Solaris makes the root account a role. This implies that you can't login directly as root but have to login as an authorized user first and assume the root role. The sulogin program will authenticate a specific user and ask for username and password of that user. 1. The following commands takes root from being a normal root account and granting the user 'debbie' the ability to assume the root role and enter single user mode: - usermod -K type=role root - usermod -R +root -A +solaris.system.maintenance debbie - rolemod -D roleauth=user root - passwd -N root 2. To prevent the 'root' user from logging for both remotely configure the CONSOLE variable with 'CONSOLE=/dev/null' in the '/etc/default/login' file		
2	8	Windows Administrators	Personnel within the Windows environments with administrative priveleges are logging with 'Administrator' username both from the console physically connected to the computer and from the network.	Scope	0.2	6.9	The security policy for this project does not address CSC Control 5: Controlled Use of Administrative Privileges	**Windows :** *Note: Microsoft does not recommend disabling the 'Administrator' account anymore. This was removed since the forest recovery white paper makes use of this account.* It is recommeded that the following settings for the built-in administator accounts be configured in each domain in the forest: 1. enable the 'account is sensitive and cannot be delegated' flag on the account 2. enable the 'smart card is required for interactive logon' flag on the account 3. configure GPOs (Group Policy Objects) to restrict administrator accounts at the domain level with the following settings at 'User Rights Assignments' : - deny access to this computer from the network - deny log on as a batch job - deny log on as a service - deny log on through Remote Desktop Services	Mitigate by following the Potential Mitigation steps to reduce the probability of occurrence or the impact of the risk.	Windows operating systems come with the default 'Administrator' username having administrative permissions and being able to log in from the console and the network.
3	6.4	Systems, Database, and ALM Administrators	**Security Vulnerability** There is no strong passowrd policy in place for all users logging in the operating environments.	Scope	0.2	6.1	The security policy for this project does not address CSC Control 16: Account Monitoring and Control	**Linux:** 1. **Best practices** for the password policy include to use a **complex password** (digits, letters and special characters), **minimum character length** of 8 ,**account lockout** after six invalid login attempts and **secure password expiration** and **password reuse** time intervals. This is configured in the **/etc/login.defs, /etc/system-auth**, and **/etc/pam.d/password-auth** files. 2. In addition, **Google's PAM can be installed and configured for Mulit-factor authentication (MFA)**. Pluggable authentication modules (PAM) is an authentication infrastructure used on Linux and Unix systems.	Mitigate by following the Potential Mitigation steps to reduce the probability of occurrence or the impact of the risk.	Operating Systems, Database, and Applications default password policy after installation is not strong.
								Solaris: 1. Use the **/etc/default/password** file to configure the password policy in best practices stated above such as password length and password complexity. 2. Solaris also uses PAM for MFA .		
								Oracle: 1. Modify the default password policy for every database user account by modifying the 'DEFAULT' profiles' attributes in Oracle Enterprise Manager Database Express. Configure the policy to address password complexity, failed login attempts and password expiration. 2. Oracle database can be configured to use MFA by implementing directory services such as RADIUS protocol. Use the SQLNET.ORA file on oracle server to configure RADIUS and MFA.		
								MircoFocus ALM : 1. The SaaS administration tool replaces ALM site administration to configure a password policy. On 'Welcome Page' go to 'Administration' and then go to 'User Management' tab to create a user. 2. In 'User Management' there is a 'locked' column that it indicates if a user is locked due to too many failed login attempts. 3. In the 'Authentication' tab, you can set password complexity, user lockout options, and password expiration. 4. ALM supports external authentication where a reverse proxy positioned in front of the ALM is configured to support an external authentication system such as smart card. ALM uses smart card certificates in place of the standard model of each user manually entering a username and password.		
								Windows Domain: 1. In Active Directory you can use the Computer Group Policy Object (GPO) to configure the default domain password policy. Best practices as mentioned above should include password length, password complexity, and password age. 2. In order to enable MFA, you should select at least on additional authentication method. By default, in ADFS in Windows Server, you can select smart card-based authentication which uses certificates as an additional authentication method.		
								Microsft SQL Server: 1. Microsoft Windows Authentication mode in SQL Server Management Studio (SSMS) allows a user to connect to the SQL server database through a windows user account in active directory.		
4	5.3	ALM administrators	The developers have performed unauthorized code changes using Micro Focus ALM with a compatible IDE for coding.	Scope	0.5	5.9	Change request is not in place for the project and "CSC Control 18: Application Software Security" is not addressed.	**Micro Focus Fortify Static Code Analyzer:** 1. Use MF Fority for Static Application Security Testing (SAST) to identify security vulnerabilites during the beginning stages of development when it is less costly. It provides immediate feedback to developers on issues introduced into code. 2. Fortify SCA works like a compiler to read source code and convert them in a structure for security analysis. 3. Additionally, Users can manually or automatically push issues into defect tracking systems. 4. Fortify SCA detects 815 unique categories of vulnerabilites across 27 programming languages. Accuracy is at a true positive rate of 100% in the OWASP Benchmark.	Mitigate by following the Potential Mitigation steps to reduce the probability of occurrence or the impact of the risk.	The programmers/developers are not practicing secure coding habits.

5	6.1	ALM administrators	The production and development environments are not separated in the ALM. The developers have access to the production environment.	Scope	0.5	6.9	The security policy for this project does not address CSC Control 14: Controlled Access Based on the Need to Know	**MicroFocus ALM:** 1. Access the SaaS Adminstration Tool (replaces Site Administrator) which you access from the Administration link on the ALM Welcome screen. Go to the Role Management tab on right. This section defines the user's role in the admin tool. The Customer Admin built-in role is similar to 'root' in unix and can create and delete projects and domains. The User Admin built-in role allows the user to change their password and personal information. A user with the User Admin role can be assigned additional permissions by beloning in a group. You can also create a customized role. 2. In User Management tab create a user. 3. in Projects tab, you can create a project and domain. You can assign one or mulitple users to one or many projects. You can also assign groups to users all in one operation. The default groups which you cannot change permissions to are TDAdmin, QATester, Project Manager, Developer and Viewer. You can create customer user groups using the default group as a template.	Mitigate by following the Potential Mitigation steps to reduce the probability of occurrence or the impact of the risk.	Projects created by the developers might have undocumented and unknown permissions with no security policy in place.
6	6.1	LInux/Solaris, Windows and Database administrators	The backup tapes are not reliable and there is no schedule in place for the testing of the backups.	Quality	0.8	7	The security policy for this project does not address CSC Control 10: Recovery Capability	**EMC Networker and Splunk:** 1. Implement a reliable plan for removing all traces of a security attack. 2. Use EMC Networker to automatically back up all files required to restore each system. Install EMC Networker and Splunk on the file server to backup these files. 3. Backup all systems at least weekly and sensitive data more often and regularly test the restoration process quarterly. 4. Use Splunk software to monitor the backup log file output from Networker and utilize the information in searches and dashboards to confirm critical systems are being backed up. 5. Splunk can also send alerts if back up activity is not seen.	Hire a vendor to backup the IT infrastructure and test the backups.	There are not enough Backup administrators to implement reliable backup procedures and testing.
7	4.6	System Administrators	A reliable alternate power supply in case of a power outage is lacking for the data center and there is no scheduled testing for it.	Cost	0.5	6.4	There can be natural disasters or overuse of electricity that can cause a power outage.	**UPS and Generators:** 1. Use a common power backup source such as an Uninterruptible Power Supply (UPS) which connects the main power supply to the IT system. If the main power supply fails, the battery in the UPS takes over the power supply for the system. 2. Since UPS is costly, it is usually a temporary battery backup that triggers a warning to users in case of a poweer outage. 3. Generators are also a reliable power supply in case of a power outage. 4. Generators can work with UPS systems, so that the UPS can handle a transmission from the main power source to the generator power. 5. It is recommended to have one or more backup generators available in case the primary generator fails. 6. Schedule regular maintenance of generators and test them annually in a lab to ensure they operate effectively.	Hire an electrician to install and test the UPS and/or generator.	There is not enough money in the budget for a UPS and/or generator.
8	6.4	Linux and Solaris Administrators	NFS is not secure. Proper user permissions and protocols are not in place making it susceptible to attacks.	Scope	0.2	7.4	The security policy for this project does not address CSC Control 13: Data Protection	**NFS:** 1. Use NFS as a distributed file system solution since the LAN consists mostly of unix-like operating systems. NFS is a low-cost easy central management file system which enables multiple users to share the same file thus preventing the clients from needing to buy storage space on their local machine. 3. NFS version 3 is widely used however version 4 has strong authentication and is more compatible with Windows. 4. To secure NFS, establish secure channels using VPN and give appropriate access rights to the client. 5. Use Kerberos authentication on versions 3 and 4 of NFS.	Accept the risk that you need a centralized file system for developers to share files. Data going across the network however is not secure and the risk of an attacker stealing the data increases.	The developers need a distributed file system to share files while coding.
9	5.1	System Administrators	The Linux/Solaris administrators need the ability to startup/shutdown the Oracle databases but they should not be able to perform CRUD (create, read, update, delete) operations. They currently have administrative permissions for the Oracle databases.	Scope	0.6	6.5	The security policy for this project does not address CSC Control 5: Controlled Use of Administrative Privileges.	**Oracle Database and RMAN:** 1. Use Recovery Manager (RMAN) in Oracle Database 12c provides for separation of database administration (DBA) duties for the Oracle Database by introducing task-specific and least-privilege administrative privileges that do not require the SYSDBA administrative privilege. 2. The new privilege to connect and execute commands in RMAN is the SYSBACKUP privilege. System Administrators can use RMAN to execute startup and shutdown scripts.	Mitigate by following the Potential Mitigation steps to reduce the probability of occurrence or the impact of the risk.	There is an inappropriate level of trust from management that system administrators are knowledgeable enough to have administrative permissions on the databases.
10	5.9	System administrators	There is no reliable logging and monitoring procedure in place in case of a security attack.	Quality	0.6	7.1	The project budget does not include the purchase of a logging and monitoring tool.	**Splunk:** 1. Use Splunk to generate standardized logs for each hardware device and the software installed on it, including date, time stamp, source addresses, destination addresses and other information about the packets and transactions. 2. If management approves the cost of purchasing servers, store logs on dedicated servers and run biweekly reports to identify and document abnormalites.	Mitigate by following the Potential Mitigation steps to reduce the probability of occurrence or the impact of the risk.	A logging and monitoring tool has not been purchased due to budget constraints.