**Security Assessment**

Executive Summary:

1. *Layout and format.* The layout and format for the mini project are defined in the *Risk Register* document template.
2. Perform a risk assessment on this system.

* There are a number of issues with the computing and software infrastructure in this project that need to be fixed. The main risks are having too many people with administrative access to Windows and Unix systems, having improperly configured passwords for each operating system, and unauthorised code changes. Other important concerns include suspicious backup tapes, unreliable alternate power supplies, incorrect database access, outdated policies and processes, and remote access being performed over RDP from the Internet.
* The situation for this project would be to implement appropriate access controls, establish and enforce password policies, monitor code changes, test backup tapes and backup power sources on a regular basis, restrict authorised personnel from accessing databases, update policies and procedures, and provide secure remote access.

* To archive this, it is advised to enforce strong password policies, implement code change monitoring and auditing tools, test backup tapes and backup power sources regularly, restrict database access to authorised personnel, update policies and procedures on a regular basis, and establish secure remote access protocols in order to achieve this ideal state.

3. ***Risk Register*** Use the Risk Register template to define the risks for this project. Copy and paste the table in the template in order to have a risk register entry for each identified risk. The items in the risk register entry include:  
 ○ Risk *number.* A unique number assigned to each risk register entry. Use any suitable numeric or alphanumeric format.  
 ○ Observation*.* A brief description of the issue.  
 ○ Risk*.* The impact value of the risk. Estimates are ok here.  
 ○ Severity. The options are Low, medium, High, and Critical.  
 ○ Recommendations*.* List any ways that the likelihood of the risk can be reduced or its impact on the project reduced.



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk Number** | **Observation** | **Risk** | **Severity** | **Recommendations** |
| 1 | Too many people with administrative access to Windows and Unix systems. | High | Critical | Implement appropriate access controls |
| 2 | Improperly configured passwords for each operating system | High | Critical | Establish and enforce password policies. |
| 3 | Unauthorised code change | High | Critical | Implement code change monitoring and auditing tools. |
| 4 | Suspicious backup tapes | High | Major | Test backup tapes regularly to ensure recovery in case of data loss. |
| 5 | Unreliable alternate power supplies | High | Major | Test alternate power sources on a regular basis |
| 6 | Incorrect database access | High | Critical | Restrict database access to authorised personnel |
| 7 | Outdated policies and processes | High | Low | Update policies and procedures on a regular basis |
| 8 | Remote access being performed over RDP from the Internet. | High | Critical | Establish secure remote access protocols in order to achieve this ideal state. |

3. ***How many risks should you identify?*** At least eight major risks across all environments

* 8 risks