|  |  |
| --- | --- |
| Prepared by: | Mohammad Alsowaini |
| Date: | 4/10/2022 |

|  |
| --- |
| Physical Control Recommendations |
| Based on my analysis I see that there are no any kind of physical control, so at least we can apply a detection physical control such as alarm systems or a prevention physical control such as protective barriers or antitheft devices, and the most important one fire suppression. |
| Logical Control Recommendations |
| Logical control is not less important than physical control, because we may loose the data or the services when we need it, so we can apply one detection logical control such as IDS which will allow us to monitor the traffic and have logs. Or a Security Incident and Events Management (SIEM) - a system or service that provides real-time analysis of security alerts generated by applications, computer systems, and/or hardware.  And we can apply a prevention logical control such as a Multi-factor Authentication which granting access to a resource after two or more authentication factors. Or Network Segmentation which will limit the lateral movement if an attack happened or there was a compromised machine. |
| Administrative Control Recommendations |
| *(include the names of the attached policy documents)*  ***router\_and\_switch\_security\_policy***  ***server\_security\_policy*** |