The highest severity vulnerabilities give potential attackers the opportunity to <TODO BAD ACTIONS THAT COULD OCCUR HERE - FULL PARAGRAPH WITH HIGH-LEVEL DETAIL>. In order to ensure data confidentiality, integrity, and availability, security remediations should be implemented as described in the security assessment findings.

Note that this assessment may not disclose all vulnerabilities that are present on the systems within the scope. Any changes made to the environment during the period of testing may affect the results of the assessment.

## <TODO Optional - Big Issue> Recommendation

This is an optional paragraph that discusses a very critical series of business failures (e.g. failure to adhere to applicable legal regulations) that isn’t a technical vulnerability but still should be brought to the attention of the executive team.

# HIGH LEVEL ASSESSMENT OVERVIEW

## Observed Security Strengths

US New-England Team 1 identified the following strengths in Robert A. Kalka Metropolitan Skyport’s network which greatly increases the security of the network. RAKMS should continue to monitor these controls to ensure they remain effective.

Access Controls

* Multiple active CVEs were remediated due to strong access controls, preventing attackers to access sensitive directories on company web servers.

<TODO Strength Category>

* <TODO Individual Strength>

## Areas for Improvement

US New-England Team 1 recommends Robert A. Kalka Metropolitan Skyport takes the following actions to improve the security of the network. Implementing these recommendations will reduce the likelihood that an attacker will be able to successfully attack RAKMS’s information systems and/or reduce the impact of a successful attack.

### **Short Term Recommendations**

US New-England Team 1 recommends Robert A. Kalka Metropolitan Skyport take the following actions as soon as possible to minimize business risk.

Password Policies

* Update RAKMS’s corporate password policy to enforce robust password standards.
* Update all domain users’ passwords to prevent further compromise and abuse of domain accounts.

Update Out-of-Date Software

* Multiple hosts use out-of-date software which either present current vulnerabilities or make the host susceptible to future exploits.

<TODO Recommendation Category>

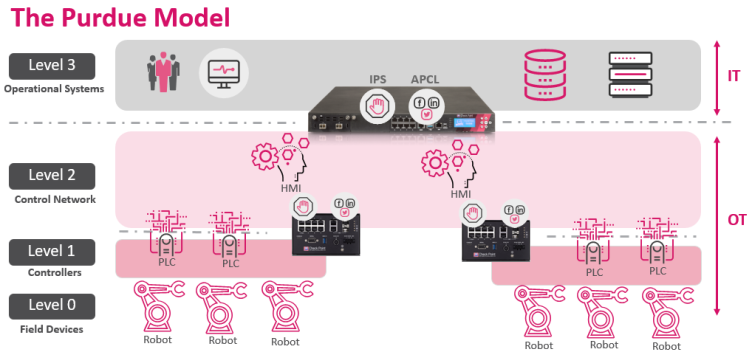
* <TODO Individual Recommendation>

### **Long Term Recommendations**

Robert A. Kalka Metropolitan Skyport recommends the following actions be taken over the coming months to fix hard-to-remediate issues that do not pose an urgent risk to the business.

Implement Additional Controls to Protect Operation Technology

* US New-England Team 1 suggests that RAKMS segments their Train network into several subnets according to the Purdue Model as seen in Figure TODO.
  + This framework for structuring operational technology networks will provide RAKMS with a guide on proper network segmentation.
  + This will reduce RAKMS’s attack surface and improve their security posture.



* US New-England Team 1 suggests that RAKMS further segment the Train network so that people mover technology can only be accessed from human management interfaces, HMIs, on a restricted subnet.
  + HMIs should only be accessable from TODO
  + Due to their sensitivity, it’s imperative to restrict access to the OT environment as much as possible.

TSA compliance

* <TODO Individual Recommendation>

Perform Regular Compliance Auditing

* Performing regular compliance auditing ensures RAKMS’s security posture is in accordance with modern standards, preventing the likelihood of future attacks.

Network Security

* Set firewall rules to deny unnecessary traffic between networks
* Consider using an IPS/IDS to monitor communications between networks

Active Directory Policy

* Reduce amount of domain administrators.
* Follow the principle of least privilege to ensure users only have the permissions needed for their jobs.