# Executive Summary

Robert A. Kalka Metropolitan Skyport enlisted the help of <<REGIONALS/FINALS-#>>’s penetration testing services to evaluate their corporate, user, train, and guest networks. This test was an assessment for vulnerabilities present in Robert A. Kalka Metropolitan Skyport’s networks. The penetration test occurred on 10/14/2023 and encompassed a singular workday.

The purpose behind this penetration test is to help Robert A. Kalka Metropolitan Skyport better secure its critical infrastructure. This is important to both our firm and RAKMS since protecting these systems has a direct effect on a customer’s experience with the company. Throughout this engagement, our firm considered this factor when conducting tests and assessing the criticality of vulnerabilities. It is of the utmost importance that customer data is secured to maintain Robert A. Kalka Metropolitan Skyport’s commitment to its customers.

Among the findings from our assessment, a few were particularly noteworthy due to their significant risk to Robert A. Kalka Metropolitan Skyport. The first of these is <<Finding 1 and details regarding how it affects business>>. The second, of which, is <<Finding 2 and details regarding how it affects business>>. A final finding that should be addressed is <<Finding 3 and details regarding how it affects business>>. Our firm wanted to highlight these vulnerabilities specifically since they were the single most important points of failure found during the engagement. We recommend remediating these vulnerabilities immediately to mitigate risk. This will help protect the company from bad actors who seek to disrupt business operations, damage business reputations, or erode trust between the business and the consumer.

Robert A. Kalka Metropolitan Skyport falls under the TSA standards for security compliance. The three biggest standards that need re-evaluating are the <<LISTOFCOMPLIANCEAREAS>> areas of security compliance. Failure to meet these standards can result in possible legal fees and fines, reputational damage, loss of consumer trust, operational disruption, and more. We recommend analyzing the following findings and patching them along with the vulnerabilities mentioned earlier: <<FINDING1COMPLIANCE and details, etc.>>. By maintaining security compliance standards, the business will have an increased security posture that will be critical in protecting consumer data.

While this was a test to find vulnerabilities, it was also a test of the security position of Robert A. Kalka Metropolitan Skyport’s Networks. Based on our testing, we found RAKMS excelled in the areas of <<AREA1, AREA2, AREA3>>. <<Details for Area 1 explaining why they did well>>. <<Details for Area 2 explaining why they did well>>. <<Details for Area 3 explaining why they did well>>. We commend you for excelling in these areas of the business’ security posture.

Overall, we were able to find <<NUMOFFINDINGS>> during the period that we had access to <<COMPANYACRYONYM>>’s corporate, user, train, and guest networks. Our findings consisted of <<PERCENTCRIT>> Critical, <<PERCENTHIGH>> High, <<PERCENTMED>> Medium, <<PERCENTLOW>> Low, and <<PERCENTINFO>> Informational. With the proper protections in place, many of the attacks performed in the testing of the network would be impossible and thus lower the risk to customer data and service uptimes and increase the overall safety of the network.