**Part 3: Risk Mitigation Plan**

**Health Network Inc. New Risk Assessment Plan**

**By: Kaleb Alstott**

**Introduction**

After looking over possible risks for Health Network Inc we now move onto how to deal and resolve issues with these risk to pursue a residual risk level. To start a plan of action and to develop a strategic guide we need to understand what a possible risk mitigation plan does and what it looks like. A risk mitigation plan is “the process of developing options and actions to enhance opportunities and reduce threats to project objectives.” (mitre.org). A risk mitigation plan will also implement a process of executing risk mitigation actions as well as who would do so. The last step in the mitigation process is prevention and continuous monitoring to stop or limit possible new/old risks. In our next section we will look at a chart that will provide all this information for us.

**Risk and Mitigation Strategies**

In our past document, the risk assessment plan, we covered and went over possible risk threat vulnerability pairs, possible control techniques for these risks, and most importantly the overall risk importance, impact level, and probability of these risks taking place. Now we will take a deeper look into these risks and find mitigation strategies and techniques that will form a plan of action to eliminate as much risk as possible for Health Network Inc. In the table below we can see we will be covering the risk, mitigation type, mitigation plan, and what team or individual will take this action on. As you carefully read through the graph and mitigation techniques, please take into consideration the last document (risk assessment plan) to find the prioritization of these possible risks.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Risk** | **Mitigation Type** | | **Mitigation Plan** | | **Team/Individul** | | |
| **Loss of data due to hardware being removed** | Mitigate | | 1.Routine database backups should be done regularly  2. Before replacing any hardware there should be a checklist of how to properly store, wipe, and destroy the data on the devices  3.Lastley, backups should also be stored on a cloud (possible third-party source) | | 1. IT management /team  2.Third party course for backup information | | |
| **Loss of data due to lost or stolen devices** | Mitigate | | 1.All devices should be encrypted with a password rest on the device every 60-90 days.  2.Devices should have appropriate protocols assigned to employee.  3.Devices should also have authentication protocols in place, if possible two factor authentication. | | 1. IT Management / team  2. Possible law enforcement | | |
| **Loss of customers due to production outages** | Third Party | | 1.All data needs to be backed up properly via third party or cloud that is offsite in case of onsite problems.  2.Software should be updated and patched as frequently as possible | | 1.Third party team to backup data  2.IT intern to check for updates | | |
| **Internet threats** | Mitigate | | 1.Strong password protected/encrypted networks using routers/firewall.  2. Be aware of outsider attacks by training and lesson implementation.  3.Security on all ends of the company should be practiced protecting from internet or outsider threats | | 1.IT team  2.Security personal teachers | | |
| **Insider threats** | Mitigate | | 1.Enforcing strict password and account management  2.Regularly monitoring employees’ online actions  3.Providing the employees with the least privilege protocol needed for their job  4. Security Awareness Training should be given to all the employees.  5.Employees should have restricted access to forms of downloading unknown files. 6.Physical security measures such as video surveillance, biometric authentication to server rooms, man traps, and entry logs should be implemented. | | 1.IT management  2. Security Team Training | | |
| **Changes in regulatory landscape** | | Third Party | | 1.New landscape plans need to be dealt with one at a time and in timely manner.  2. If we are still having stability and building issues possibly think upon relocation | | 1.Contractor  2.Landscaping  3.CEO  4. Real Estate Agent if needed |

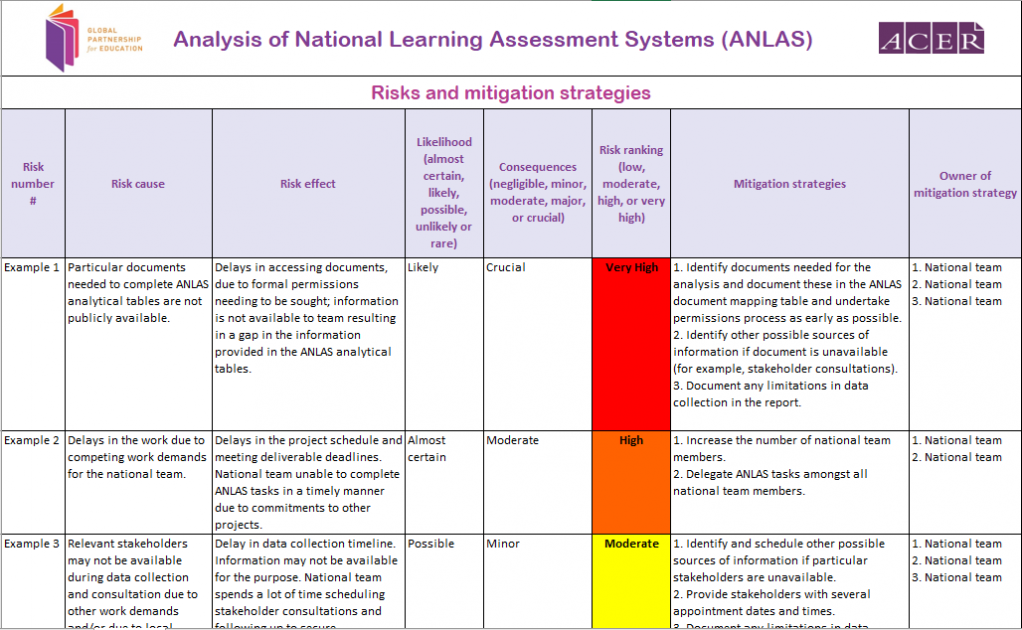
**Continuous Monitoring**

After reading through the mitigation plan, we have one more step left in this process and that is monitoring. Even once we manage all risks down to a residual risk level, we must work on preventing these risks again and keep an eye out for new ones. The only way to do this is by implementing a team or induvial to continuously monitor vulnerabilities. To stay protected and secure we need to make sure that Health Network Inc is always running tests on their systems, checking networks, up to date with security protocols, limiting access to assets, and much more. Hiring a team to continuous monitor your vulnerabilities and threats are key to having a successful security.

**References**

Risk-Mitigation-Roles.docx

## MRIS-3E-Chapter09.pptx



<https://www.globalpartnership.org/content/risks-and-mitigation-strategies-template>

<https://www.mitre.org/publications/systems-engineering-guide/acquisition-systems-engineering/risk-management/risk-mitigation-planning-implementation-and-progress-monitoring>