|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **SN** | **Risk Description** | **Severity** | **Likelihood** | **Risk Mitigation Plan** |
| **1** | Fail to detect disaster as soon as it occurs | **Critical** | **High** | 1. Leverage on current monitoring tools such as Nagios, htop, Cloudtopus, AWS Cloudwatch, VisualPing, FreshPing and AWS Alarms 2. Train team on how to use these monitoring tools |
| **2** | Fail to recover from disaster as per business requirement | **Critical** | **Medium** | 1. Plan for possible disasters on Disaster Recovery Plan 2. Team to conduct Disaster recovery plan exercise to familiarize team on what to do in the event of a disaster |
| **3** | Possibility of recurring attack from same hackers as loophole has not been detected and patched yet | **Critical** | **Medium** | 1. Leverage on current monitoring tools such as Nagios, htop, Cloudtopus, AWS Cloudwatch, VisualPing, FreshPing and AWS Alarms to detect threats early 2. Train team on how to use these monitoring tools |
| **4** | Miscommunication during disaster | **Critical** | **Medium** | 1. Ensure that team is familiar with Disaster Recovery Plan 2. Team to conduct Disaster recovery plan exercise to familiarize team on what to do in the event of a disaster |
| **5** | Team did not follow disaster recovery plan | **Critical** | **Low** | 1. Brief team about processes based on Disaster Recovery Plan 2. Team to conduct Disaster recovery plan exercise to familiarize team on what to do in the event of a disaster |
| **6** | Losing backed-up AMI image | **Critical** | **Low** | 1. Ensure backup instance has images backed up regularly as well 2. Conduct regular tests to ensure images are properly backed up |