|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Rank this week** | **Rank last week** | **Weeks on List** | **Risk Description** | **Severity** | **Likelihood** | **Risk Mitigation Plan** |
| **1** | **-** | **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** | **-** | **1** | Fail to recover from disaster as per business requirement | **Critical** | **High** | 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** | **-** | **1** | Possibility of recurring attack from same hackers as loophole has not been detected and patched yet | **Critical** | **High** | 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 |
| **3** | **1** | **3** | Failure to resolve incident and restore business operations so as to minimize impact to business and application. | **Critical** | **High** | 1. Ensure proper standard of procedures are addressed in Incident Management and Problem Management Plans 2. Familiarize entire team on the procedures in the above mentioned plans to facilitate disaster recovery |
| **-** | **2** | **3** | Lack of constant monitoring to detect incident | **Critical** | **Medium** | 1. Configure the ticketing system to send an alert to Tier 1 upon receiving a new ticket from a user 2. Schedule rotation shifts to reduce the chances of incidents going undetected |
| **-** | **-** | **2** | Incorrect classification of ticket as a change request, incident or disaster | **Critical** | **Low** | 1. Familiarize Tier 1 with how to identify and classify tickets 2. In the case whereby the event is directly detected by Tier 2/3, familiarize Tier 2 and 3 with ticket classification as well |
| **-** | **-** | **2** | Missing record of incidents in the Incident Log | **Critical** | **Low** | 1. Sequential numbering of incident reports is implemented to ensure proper incident logging |
| **-** | **1** | **4** | Fail to respond and resolve change request within expected timeframe. | **Critical** | **High** | 1. Set up ticketing system notification service 2. Brief team members on what to do when there’s a change request |
| **-** | **2** | **6** | Peak traffic flow may exceed server load capacity, resulting in longer response times/unsuccessful responses | **Critical** | **Medium** | 1. Load balancing using multiple app servers on a single ec2 instance by using ports. 2. Monitor traffic flow using Cloudtopus and AWS Cloudwatch, team will create more ports if there is a high consistent network packets incoming over a period of time. |
| **-** | **3** | **6** | Production server crashes during business hours and stops working. | **Critical** | **Low** | 1. Schedule for testing and maintenance on every Sunday. 2. Keeping daily backup of the website’s files (ec2 instance’s snapshot). If the site crashes, having a recent backup will ensure the site content will remain current. |
| **-** | **-** | **5** | Fail to obtain the required service levels set by the business: 99.9% per week | **Critical** | **Medium** | 1. Load balancing using multiple app servers on a single ec2 instance by serving the application on multiple ports. |
| **-** | **-** | **3** | Miscommunication during daily operations or maintenance | **Critical** | **Medium** | 1. Ensure instructions are clarified before proceeding with any important task like updating OS or configuration. 2. Ensure permission is granted by COO and IT operations manager for critical systems 3. Use layman english together with clear and concise writing during communications to avoid multiple interpretations |
| **-** | **-** | **3** | Quality not up to minimum standards during deployment / after change request / after disaster recovering | **Critical** | **Medium** | 1. IT Operations manager , support manager as well as QA must constantly communicate to ensure the entire system is running smooth. 2. Ensure systems are above minimum standards to cater for performance variance. |
| **-** | **-** | **3** | Team did not follow process | **Critical** | **Low** | 1. Brief team about processes based on documentations 2. Ensure team follows processes based on documentations |
| **-** | **-** | **3** | Some documents might not be examined during document review. | **Critical** | **Low** | 1. Develop a document checklist for document review 2. Have both QA & IT Operations sign after reviewing each document |
| **-** | **-** | **3** | Fail to respond and resolve change request within expected timeframe. | **Critical** | **High** | 1. Set up ticketing system notification service 2. Brief team members on what to do when there’s a change request |
| **-** | **-** | **3** | Failure to make changes | **Critical** | **Medium** | 1. Ensure that Tier 3 - Dev and Infrastructure & Security knows how to make the changes before proceeding 2. Ensure that ready-to-go checklist is updated for new changes |
| **-** | **-** | **3** | Changes are made without approval | **Critical** | **Low** | 1. Brief team about Change Management Process 2. Ensure team follows Change Management Process |
| **-** | **-** | **3** | Increase of incidents due to change | **Critical** | **Medium** | 1. Ensure that the live environment are being tested based on the Quality Management’s test requirements and new changes’ requirement |
| **-** | **-** | **1** | 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 |
| **-** | **-** | **1** | 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 |
| **-** | **-** | **1** | 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 |