|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Description** | **Evaluation** | **Likelihood** | **Impact** | **Responsibility** | **Response** | **Control measures** |
| Unauthorised SSH access over the internet to theservices’ instances | Someone unauthorised would have access to the services’ instances - with use of sudo | Low | High | Developers responsibility | Stop the instance on AWS and reconfigure another instance with stronger security to prevent this happening in the future | Use a bastion EC2 with a security group that only allows access from developer’s IPs.  Only allow SSH access on services instances from within the Virtual Private Cloud |
| Unauthorised acquisition of passwords and access keys  DEPLOYMENT  PROJECT | Someone would be able to access passwords or access keys | Low | Medium | Developers responsibility | Change passwords and/or access keys immediately | Ensure only strong passwords are used.  Ensure that anything uploaded to VCS (GitHub) is sanitised of raw passwords/access keys.  Ensure that different strong passwords are being used for different access points for services used  Ensure that no private access keys are stored on EC2 instances |
| Cloud provider failing  DEPLOYMENT  LIVE ENV  PROJECT | Resources would shut down and would be no longer accessible | Low | Very high | AWS | Recreate the AWS infrastructure in a different region | Ensure all deployment and code for resources are as automated as possible to allow for a quick recovery. |
| Reintroduction of legacy bugs | Broke jenkins deployment | Happened | High | Developers | Cross reference an earlier build to remove the bug | Ensuring accurate use of main and development feature branch model in VCS (Git).  Ensures any legacy bugs are temporary |