|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Risk | Threat Source | Threat Event (Characterised by TTPs) | Vulnerability | Likelihood | Impact |  |
| Access Control Risk | **Adversarial**  Individual - Insider:  Sharing of login credentials for internal systems to “save time” | -Mishandling of critical and/or sensitive information by authorised user  -Spill sensitive information  -Obtain unauthorised access  -Compromise software of organisational critical information system |  |  |  |  |
| Asset Management Risk | **Structural**  IT Equipment - Storage:  No formal inventory existing for IT Assets | -Cause deterioration/destruction of critical information system components and functions  -Lack of awareness of Assets  -Inadequate protection of records with regards to information security and sensitivity |  |  |  |  |
| Incident Management Risk | **Structural**  IT Equipment - Communications:  No clear process for reporting security incidents | -Threat of attacks going unreported  -Allow prolonged spread of infectious malware with lack of clear report systems in place |  |  |  |  |
| Physical Security Risk | **Structural**  Environmental:  Office servers are stored in an unlocked room accessible to all employees | -Exploitation of physical access of vulnerable integral areas to gain access to organisational facilities  -Compromise of critical information systems via physical access |  |  |  |  |
| Data Protection Risk | **Structural**  IT Equipment -Storage:  Customer data stored unencrypted in unbacked cloud storage |  |  |  |  |  |

Risk assessment based on Nist 800 principlesA close-up of a document

AI-generated content may be incorrect.