|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| E.I Exam le 1: Risk Accounting | | | Form | | | | |
|  | Risk Accounting Form | | | | | | |
| Identified by. Security team | | | | | | Date:04-02-2022485 |
|  | | | | | | ID CM Tracking |
| A vulnerability in the authentication system of the online banking platform allows attackers to bypass Multi-Factor Authentication (MFA), gaining unauthorized access to user accounts. This could lead to financial fraud, compromised user data, loss of customer trust, and legal consequences. | | | | | | |
|  | Consequence. Cost Schedule Performance , Quality | | | | Risk Magnitude Rm | |
|  | Severity : Critical | |  | |  | |
|  | Probability of occurrence? High | | |  |
|  | Timeframe of risk? Near-term | | | |
| Mitigation Strategy:  Implement comprehensive security audit.  Train the employees and implement incident response plan.  Regular user activity monitoring.  Implement a plan to quickly identify the threat and a plan to mitigate it. | | | | | | |
| Contingency Action and Trigger:  In case of breach, disable access to the affected accounts.  Implement a forensic investigation.  Notify the customers so that they take the actions accordingly.  Prepare a backup plan. | | | | | | |
| Risk Grouping: risks (ty ID) thatM611 impact this risk or aro impacted by risk | | | | | | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | |  | | z  Risk Information Sheet | | | |  | Identified: Security Team | | | Priority: Critical |  | Statement of Risk:  The potential damage that can be caused to a system or asset. | | | |  | | | | Probabil |  | | High |  | | Timeframe. | | | Origin  Vulnerability in the authentication system | | Class: | Security | | Assigned TO:  Me | | Context:  A vulnerability in the authentication system of an online banking platform allows attackers to bypass multi-factor authentication (MFA), granting unauthorized access to user accounts. | | | | | |  | | | | MitigationStrategy,  Implement comprehensive security audit.  Train the employees and implement incident response plan.  Regular user activity monitoring.  Implement a plan to quickly identify the threat and a plan to mitigate it. | | | | | |  | | | | Contingency Action and Trigger:  In case of breach, disable access to the affected accounts.  Implement a forensic investigation.  Notify the customers so that they take the actions accordingly.  Prepare a backup plan. | | | | | |  | | | | Status: | | | | | | Date:  4 feb | | | | Working on the vulnerability | | | | Closing Date;  5 feb | | Closing Rationale! | | | |