**SAMPLE RISK ASSESSMENT FORM**A picture containing drawing

Description automatically generated

|  |  |  |
| --- | --- | --- |
| REF ID NO. | SUBMITTED BY | DATE SUBMITTED |
| 002 | Edlira Taipi | 08/07/2025 |

RISK TYPE *select one*

|  |  |  |
| --- | --- | --- |
|  | Financial | |
|  | Legal / Contractual | |
|  | Reputation / Customer Relations | |
|  | Resources | |
| X | Operational | |
| X | Other: | Compliance,Cybersecurity |

RISK DESCRIPTION

|  |
| --- |
| Remote employees received emails impersonating internal IT communications, requesting them to update login credentials via a fraudulent link. The emails closely mimicked the company’s email formatting and branding, aiming to harvest usernames and passwords for unauthorised access. |

SOURCE OF RISK

|  |
| --- |
| Increased dependence on email for hybrid communication.  Lack of employee training in recognising phishing tactics.  Absence of multi-factor authentication (MFA) on internal systems.  Inadequate email threat detection tools. |

PERSON(S) IMPACTED *check all that apply*

|  |  |  |
| --- | --- | --- |
| X | Customers / Clients | |
| X | Employees | |
| X | Contractors | |
|  | Public | |
|  | Other: |  |
|  | Other: |  |
|  | Other: |  |

RISK IMPACT *select one*

|  |  |  |
| --- | --- | --- |
|  | **Impact Level** | **Description** |
|  | **NOT SIGNIFICANT** | Minimal operational disruption or negligible data risk. No injury or loss of service. |
|  | **MINOR** | Slight impact such as brief downtime or minor data exposure. Recovery is quick. |
|  | **MODERATE** | Noticeable disruption or temporary loss of system access requiring IT intervention. |
| **X** | **MAJOR** | Serious incident leading to extended downtime, significant data compromise, or legal risk. |
|  | **SEVERE** | Critical failure with severe consequences—major breach, regulatory action, or shutdown. |

RISK PROBABILITY *select one*

|  | Probability Level | **Description** |
| --- | --- | --- |
|  | HIGHLY UNLIKELY | Extremely rare occurrence. Only possible under exceptional conditions. |
|  | UNLIKELY | Could happen, but not expected under current practices or setup. |
|  | POSSIBLE | A known risk that may occur without changes to controls or behaviour. |
| X | LIKELY | The event is expected to happen under existing conditions or has occurred recently. |
|  | HIGHLY LIKELY | Frequently occurs or almost certain without immediate intervention. |

RISK SEVERITY MATRIX *based on Impact and Probability Levels*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **IMPACT x PROBABILITY** | **NOT SIGNIFICANT** | **MINOR** | **MODERATE** | **MAJOR** | **SEVERE** |
| **HIGHLY UNLIKELY** | LOW | LOW | LOW / MED | MEDIUM | MEDIUM |
| **UNLIKELY** | LOW | LOW / MED | LOW / MED | MEDIUM | MED / HIGH |
| **POSSIBLE** | LOW | LOW / MED | MEDIUM | MED / HIGH | MED / HIGH |
| **LIKELY** | LOW | LOW / MED | MEDIUM | MED / HIGH | HIGH |
| **HIGHLY LIKELY** | LOW / MED | MEDIUM | MED / HIGH | HIGH | HIGH |

RISK SEVERITY LEVEL *select corresponding Severity Level from matrix above based upon Impact and Probability Levels*

|  |  |
| --- | --- |
|  | SEVERITY LEVEL |
|  | LOW |
|  | LOW / MED |
|  | MEDIUM |
|  | MED / HIGH |
| X | HIGH |

CURRENT CONTROL MEASURES

|  |
| --- |
| The company has basic protections in place, such as email spam filtering, antivirus software, and a password policy. A “Report Phishing” button is available in the email system, but it is rarely used and not promoted. Multi-factor authentication is not yet enforced, and staff have not received formal cybersecurity training. These limited measures offer minimal defence against advanced phishing attacks. |

FURTHER ACTION NEEDED? *select one*

|  |  |
| --- | --- |
| X | YES |
|  | NO |

ACTIONS TO IMPLEMENT *if applicable*

|  |  |  |  |
| --- | --- | --- | --- |
| **ACTION** | **ASSIGNED TO** | **DUE DATE** | **STATUS** |
| Implement mandatory cybersecurity training for all employees | |  | | --- | | IT & HR Department | | |  | | --- | |  |  |  | | --- | | 15/07/2025 | | Not started |
| Enable multi-factor authentication (MFA) for all remote logins | |  | | --- | | IT Security Team | | 12/07/2025 | In progress |
| Schedule regular phishing simulations (quarterly) | Cybersecurity Lead | 01/08/2025 | |  | | --- | | Planned | |
| Update internal policy: minimum requirements for remote device security | Policy & Compliance Team | 20/07/2025 | |  | | --- | | Not started | |
| Test and update incident response plan for phishing scenarios | Compliance Officer | |  | | --- | | 25/07/2025 | | Not started |
|  |  |  |  |
|  |  |  |  |

|  |  |  |
| --- | --- | --- |
| DATE REVIEWED | APPROVING OFFICIAL NAME & TITLE | SIGNATURE |
| 08/07/2025 | Edlira Taipi - Risk Manager | **Edlira Taipi** |

REMARKS

|  |
| --- |
| Phishing remains one of the most common and effective attack methods against hybrid businesses. The incident described is not isolated it highlights a **systemic vulnerability** that requires an urgent, multi-layered response combining **technical measures**, **employee education**, and **policy updates**. A well-trained workforce, backed by secure infrastructure, is the best defence against phishing-based breaches. |