# RISK ASSESSMENT WIZARD

## ASSESSMENT DETAILS

### ESCALATION CONTACT:

| Team Lead: | | Contact No.: | |
|---|---|---|---|
| Affected Parties: | | | |

## ACTIVITY OR SERVICE DETAILS

| Purpose: | Date: |
|---|---|
| | |

**Benefit:** Enhances trust and credibility with stakeholders. | Ensures adherence to legal and regulatory standards. | Improves operational efficiency through streamlined compliance processes. | Mitigates risks of penalties and legal disputes. | Promotes ethical practices and corporate governance. | Reduces reputational risks through proactive management.

## HAZARDS

| HAZARD | RISK | RISK BENEFIT | MEASURE | RISK TO | RISK LEVEL |
|---|---|---|---|---|---|
| Failure to comply with environmental regulations | Legal penalties, environmental damage, reputational harm | Enhances corporate social responsibility profile, attracting environmentally conscious investors and customers. | Conduct environmental impact assessments, implement sustainable practices, and ensure compliance with environmental laws. Provide training on environmental responsibilities. **(ALL)** | Environment, community, organization | Before Measure: **High** After Measure: **Med** |
| Failure to comply with financial reporting standards | Regulatory fines, inaccurate financial statements, loss of investor trust | Allows for transparent financial disclosures, attracting investors and stakeholders by demonstrating financial integrity. | Develop a comprehensive financial reporting framework that aligns with applicable standards (e.g., IFRS or GAAP). Implement internal controls over financial reporting, conduct regular audits, and provide ongoing training to accounting personnel on current standards. **(ALL)** | Accounting team, investors, organization | Before Measure: **High** After Measure: **Med** |

| HAZARD | RISK | RISK BENEFIT | MEASURE | RISK TO | RISK LEVEL |
|---|---|---|---|---|---|
| Failure to comply with tax regulations | Tax penalties, legal action, financial losses | Avoids legal penalties and interest, ensuring financial stability and credibility with tax authorities. | Maintain accurate financial records, stay informed about tax law changes, and conduct regular tax compliance audits. Engage tax professionals to ensure proper tax planning and reporting. **(ALL)** | Finance team, organization | Before Measure: **High** After Measure: **Med** |
| Failure to detect insider trading | Market manipulation, regulatory fines, loss of reputation | Maintains market integrity and investor confidence, essential for a reputable financial institution. | Deploy surveillance systems to monitor trading activities, establish clear policies on insider trading, and provide regular training to employees. Implement whistleblower programs and conduct periodic reviews of trading patterns. **(ALL)** | Employees, traders, organization | Before Measure: **High** After Measure: **Med** |
| Failure to monitor employee communications | Data leaks, policy violations, internal fraud | Balances the need for transparency and privacy, fostering a compliant yet collaborative work environment. | Use automated monitoring systems with AI-driven analytics to review communications for compliance breaches. Ensure employee awareness and establish clear policies governing acceptable use. Provide regular ethical behavior training. **(ALL)** | Employees, organization | Before Measure: **High** After Measure: **Med** |
| Inadequate business continuity planning | Operational downtime, loss of revenue, diminished stakeholder confidence | Ensures operational resilience, allowing the institution to withstand and recover from unforeseen events. | Develop and test business continuity plans, ensure critical functions can operate during disruptions, and communicate plans to all stakeholders. Incorporate disaster recovery strategies and conduct regular drills. **(ALL)** | All employees, management, organization | Before Measure: **High** After Measure: **Med** |
| Inadequate customer due diligence (CDD) | Onboarding high-risk customers, financial crime, regulatory breaches | Enables the onboarding of a diverse customer base, fostering business growth while managing financial crime risks. | Establish a risk-based CDD program that includes identity verification, beneficial ownership identification, and ongoing monitoring of customer transactions. Utilize technology solutions for efficient data collection and analysis, and ensure compliance with AML regulations. **(ALL)** | Compliance officers, financial team, customers | Before Measure: **High** After Measure: **Med** |

| HAZARD | RISK | RISK BENEFIT | MEASURE | RISK TO | RISK LEVEL |
|---|---|---|---|---|---|
| Inadequate data security controls | Data breaches, unauthorized access, data loss | Accepting this risk allows leveraging technology to enhance service efficiency while fostering trust through strong but flexible security practices. | Develop a layered security framework, including robust encryption for data at rest and in transit, multi-factor authentication, access control policies, and continuous monitoring. Conduct regular third-party security audits and implement incident response plans for breaches. **(ALL)** | Customers, employees, organization | Before Measure: **High** <br> After Measure: **Med** |
| Inadequate employee training on compliance | Non-compliance, legal penalties, reputational damage | Accepting this risk supports dynamic workforce development, ensuring adaptability in changing regulatory environments. | Develop mandatory, role-specific training programs covering legal frameworks, emerging risks, and internal compliance protocols. Incorporate real-world scenarios and assessments to reinforce learning. Track and report completion rates. **(ALL)** | Employees, compliance team, organization | Before Measure: **High** <br> After Measure: **Med** |
| Inadequate fraud detection mechanisms | Financial losses, reputational damage, regulatory fines | Protects assets and reduces financial losses, contributing to overall financial health. | Implement fraud detection software, establish clear reporting channels for suspected fraud, and conduct regular audits. Train employees to recognize and report fraudulent activities. **(ALL)** | Employees, financial team, organization | Before Measure: **High** <br> After Measure: **Med** |
| Inadequate handling of customer complaints | Customer dissatisfaction, loss of business, negative reviews | Improves customer satisfaction and retention, leading to sustained business growth. | Establish a robust customer complaint management system, train staff on effective complaint resolution, and analyze complaint data to identify trends and areas for improvement. **(ALL)** | Customers, customer service team, organization | Before Measure: **High** <br> After Measure: **Med** |
| Inadequate incident response planning | Extended downtime, increased damage from incidents, loss of data | Strengthens resilience, allowing rapid recovery and minimized operational downtime when risks materialize. | Develop detailed incident response playbooks for various scenarios, including cyberattacks, fraud, and service outages. Test plans through bi-annual drills, ensure roles are clearly defined, and involve external experts for evaluation. **(ALL)** | IT staff, management, organization | Before Measure: **High** <br> After Measure: **Med** |

**RISK ASSESSMENT WIZARD**

| HAZARD | RISK | RISK BENEFIT | MEASURE | RISK TO | RISK LEVEL |
|---|---|---|---|---|---|
| Inadequate monitoring of employee conduct | Policy violations, unethical behavior, legal issues | Promotes a positive organizational culture, reducing the risk of misconduct and its associated repercussions. | Implement ethics training programs, establish clear codes of conduct, and utilize monitoring tools to detect policy violations. Encourage a culture of transparency and accountability. **(ALL)** | Employees, management, organization | Before Measure: **High** After Measure: **Med** |
| Inadequate oversight of remote work environments | Security breaches, data loss, unauthorized access | Facilitates flexible work arrangements, enhancing employee satisfaction and productivity, while maintaining control over security and compliance. | Implement secure remote access solutions, such as Virtual Private Networks (VPNs) with strong encryption, and enforce endpoint security protocols on all devices. Conduct regular security awareness training focused on remote work risks and establish clear remote work policies. **(ALL)** | Remote employees, IT staff, organization | Before Measure: **High** After Measure: **Med** |
| Inadequate protection of customer funds | Loss of customer funds, legal liabilities, loss of trust | Builds customer confidence and trust, essential for business sustainability and growth. | Implement segregation of customer funds from operational funds, conduct regular reconciliations, and ensure compliance with safeguarding regulations. Utilize insured accounts and establish clear policies for fund protection. **(ALL)** | Customers, financial team, organization | Before Measure: **High** After Measure: **Med** |
| Inadequate succession planning | Leadership gaps, operational disruptions, loss of institutional knowledge | Ensures business continuity during leadership transitions, minimizing operational disruptions and maintaining stakeholder confidence. | Develop a succession planning framework that identifies key roles, potential successors, and skill gaps. Provide leadership development programs and ensure regular reviews to update the plan as organizational needs evolve. **(ALL)** | Management, employees, organization | Before Measure: **High** After Measure: **Med** |
| Inadequate third-party risk management | Vendor breaches, service disruptions, compliance failures | Allows for strategic partnerships while managing associated risks, facilitating business expansion. | Develop a third-party risk management program that includes due diligence, contract management, and ongoing monitoring. Assess third parties for compliance with legal and regulatory requirements. **(ALL)** | Third-party vendors, organization | Before Measure: **High** After Measure: **Med** |

| HAZARD | RISK | RISK BENEFIT | MEASURE | RISK TO | RISK LEVEL |
|---|---|---|---|---|---|
| Insufficient due diligence on third parties | Third-party breaches, data leaks, service disruptions | Allows the organization to harness third-party expertise and innovation while maintaining manageable risks. | Establish a vendor risk management framework with comprehensive screening, annual audits, and performance evaluations. Use contract clauses to ensure compliance and maintain accountability. Include termination clauses for breaches. **(ALL)** | Third-party vendors, organization | Before Measure: **High** <br> After Measure: **Med** |
| Limited malware protection | Malware infections, data corruption, system outages | Accepting this risk allows for broader use of technology tools while managing potential interruptions effectively. | Implement endpoint protection systems, sandboxing technologies, and advanced threat detection mechanisms. Schedule regular updates of anti-malware tools and train staff to recognize and respond to phishing attempts effectively. **(ALL)** | Employees, IT infrastructure, organization | Before Measure: **High** <br> After Measure: **Med** |
| Non-compliance with anti-money laundering (AML) regulations | Regulatory fines, legal action, reputational harm | Enables broader market access and client onboarding capabilities by managing AML risks responsibly. | Deploy advanced transaction monitoring systems, require enhanced due diligence for high-risk customers, and train staff to identify suspicious activities. Conduct mock regulatory audits to ensure readiness for inspections. **(ALL)** | Compliance officers, financial team, organization | Before Measure: **High** <br> After Measure: **Med** |
| Non-compliance with consumer protection laws | Legal penalties, customer dissatisfaction, loss of business | Enhances customer satisfaction and loyalty, contributing to long-term business success. | Establish comprehensive policies that adhere to consumer protection laws, provide regular training to employees, and implement monitoring systems to ensure compliance. Address consumer complaints promptly and effectively. **(ALL)** | Customers, employees, organization | Before Measure: **High** <br> After Measure: **Med** |
| Non-compliance with data privacy regulations | Legal penalties, loss of customer trust, data breaches | Enhances consumer confidence by demonstrating a strong commitment to data protection. | Develop a comprehensive data privacy framework aligned with global standards, appoint a Data Protection Officer, and use privacy-by-design principles in all processes. Perform regular privacy impact assessments and audits. **(ALL)** | Customers, data subjects, organization | Before Measure: **High** <br> After Measure: **Med** |

**RISK ASSESSMENT WIZARD**

| HAZARD | RISK | RISK BENEFIT | MEASURE | RISK TO | RISK LEVEL |
|---|---|---|---|---|---|
| Non-compliance with employment laws | Legal penalties, employee dissatisfaction, high turnover | Fosters a fair and equitable workplace, enhancing employee morale and reducing legal risks. | Develop comprehensive HR policies that comply with employment laws, provide regular training to HR personnel, and establish grievance mechanisms. Conduct periodic reviews of employment practices. **(ALL)** | Employees, HR department, organization | Before Measure: **High** After Measure: **Med** |
| Non-compliance with ethical standards | Reputational damage, loss of trust, legal issues | Promotes a positive reputation, fostering trust among stakeholders and creating a competitive advantage in the market. | Establish a comprehensive code of ethics, supported by regular training and anonymous reporting channels. Conduct periodic ethical audits and engage third-party ethics consultants to ensure adherence to high standards. **(ALL)** | Employees, management, organization | Before Measure: **High** After Measure: **Med** |
| Non-compliance with intellectual property laws | Legal disputes, financial penalties, loss of innovation | Avoids legal disputes and fosters innovation by respecting intellectual property rights. | Implement policies to respect intellectual property rights, conduct regular audits to ensure compliance, and provide training on intellectual property laws. **(ALL)** | Employees, organization | Before Measure: **High** After Measure: **Med** |
| Non-compliance with sanctions regulations | Legal penalties, restricted transactions, reputational damage | Facilitates international operations by ensuring adherence to global sanctions regimes, minimizing legal and reputational risks. | Maintain updated lists of sanctioned entities and individuals, and integrate automated screening tools into transaction processing systems. Develop procedures for handling potential matches and provide staff training on sanctions compliance. **(ALL)** | Compliance officers, financial team, organization | Before Measure: **High** After Measure: **Med** |
| Outdated cybersecurity policies | Non-compliance, increased vulnerability to attacks, regulatory penalties | Empowers the organization to innovate confidently while adapting to an evolving regulatory and threat landscape. | Establish a policy review committee to evaluate cybersecurity policies annually, consult with industry experts on emerging trends, and ensure employees are trained on updated policies through interactive workshops and simulated threat exercises. **(ALL)** | Employees, compliance officers, organization | Before Measure: **High** After Measure: **Med** |

| HAZARD | RISK | RISK BENEFIT | MEASURE | RISK TO | RISK LEVEL |
|---|---|---|---|---|---|
| Poor management of access controls | Unauthorized access, data manipulation, insider threats | Supports operational flexibility by enabling seamless access for authorized personnel, balancing security with productivity. | Deploy role-based access control (RBAC) systems, enforce multi-factor authentication, and establish robust identity governance frameworks. Schedule quarterly access reviews and automate logging to track unauthorized access attempts. **(ALL)** | Employees, organization | Before Measure: **High** <br> After Measure: **Med** |
| Unaddressed network vulnerabilities | Network breaches, system downtime, data interception | Enables innovation through interconnected systems while maintaining the agility to quickly address emerging threats. | Perform comprehensive penetration testing bi-annually, maintain a patch management program to address known vulnerabilities, deploy advanced firewalls, and integrate real-time intrusion detection systems (IDS). Train staff on recognizing cyber threats. **(ALL)** | IT staff, organization, customers | Before Measure: **High** <br> After Measure: **Med** |
| Weaknesses in transaction monitoring systems | Undetected fraudulent transactions, regulatory breaches, financial losses | Supports growth by enabling high transaction volumes while identifying risks efficiently. | Implement AI-driven analytics to enhance transaction monitoring and use risk-based thresholds to reduce false positives. Regularly review system configurations and align them with evolving compliance requirements. **(ALL)** | Financial team, compliance officers, organization | Before Measure: **High** <br> After Measure: **Med** |
| Unforseen hazard | Illness, injury, death | | Ongoing dynamic risk assessment conducted by all relevant personnel. Any identified potential risks should be immediately reported to the appropriate supervisor or risk manager, and corrective action should be taken as necessary. **(ALL)** | All | **N/A** |

## NOTES

**Extra notes & evaluation:**

_____
**Completed by**

_____
**Reviewed/Approved by**

_____
**Risk Assessment Date**

_____
**Review Required Date**