PHISHING ATTEMPT	

				RISK ASSESSMENT						POST-MITIGATION			JUDGEMENT	
TOPIC	RISK	CONTROL ENVIRONMENT	CONTROL ACTIVITIES	RISK SEVERITY	RISK LIKELIHOOD	RISK LEVEL	MITIGATIONS / WARNINGS / REMEDIES	INFORMATION AND COMMUNICATIONS	CONTROLS PRESENT?	RISK SEVERITY	RISK LIKELIHOOD	RISK LEVEL	ACCEPTABLE TO PROCEED?	COMMENTS AND NOTES
Phishing email sent to employees in the finance department in an attempt to to access financial data within the company	PHISHING ATTEMPT	Finance Team	Employee awareness and training- creating training that can inform internal employees on the risk of of clicking links in an email	INTOLERABLE	POSSIBLE	EXTREME	Isolate affected systems to prevent spread, and send out communications to all employees, advising care when clicking on links. Assess data for integrity, audit network logs to ensure no data has been exfiltrated & to observe any unexpected movements by attackers using employee credentials. Change compromised credentials and implement employee	In the event of a data breach, affected customers should be informed within the timeframe stipulated by regulatory frameworks. The legal team must be made aware in case of any legal ramifications. Stakeholders should be kept informed with regular updates, and public relations should manage the public release of information.	YES	TOLERABLE	POSSIBLE		YES	The risk level of the event has changed because there is a control in place to help mitigate this risk level down to medium.
	Email Filtering	IT DEPT	Email security solutions. Having alerts set up to inform and block any phishing attempts	UNDESIRABLE	POSSIBLE	MEDIUM	High alert - Deploying advanced email filtering tools and encrypting sensitive emails would prevent the spread of an attack in addition to having employees trained on recognizing phishing and social engineering attemps when clicking on links	Clear and concise communication and information sharing is critical to stakeholders and those affected to lunderstand its importance, functionality, and impact.	YES	TOLERABLE	POSSIBLE	LOW	YES	The risk level of the event has changed because there is a control in place to help mitigate this risk level down to low.
	Response Protocols	IT DEPT	Incident response plan. IT team having plan in place for phishing attempts on employees when suspected phishing attemps are occuring and addressing in timely fashion.	TOLERABLE	PROBABLE	MEDIUM	High alert - This critical because affected systems need to be isolated and compromised credentials need to be changed. MFA needs to be enabled. Warnings need to be issued to employees to avoid suspicious links and report phising attempts	Post incident, share lessons and and reinforce traing to prevent future attacks.	YES	UNDESIRABLE	POSSIBLE	MEDIUM	YES	The risk level of the event has changed because there is a control in place to help mitigate this risk level down to medium.
	Access Controls	Finance Team	Access control enhancements. Updating controls for internal employees only	INTOLERABLE	PROBABLE	MEDIUM	High alert - Revoke all compromised credentials and issue password resets with MFA. Monitor affected system for any backdoors or potential backdoors left by attackers. Document findings and report to regulatory body.	For compromised access controls, the affected users, IT, and legal need to be notified. The scope of compromise needs to be communicated and MFA needs to be enforced. Clear guidance needs to be provided for monitoring and reporting for suspicious activities. Transparency is key	YES	UNDESIRABLE	POSSIBLE	MEDIUM	YES	The risk level of the event has changed because there is a control in place to help mitigate this risk level down to medium.
	Past Incidents	Finance Team	Regular security audits. Having audits done randomly to assess security measures in place and mitigate any vulnerabilities	INTOLERABLE	POSSIBLE	LOW	High alert - Mitigations include root causes strengthing access controls and patching vulnerabilities. Employees need to be reminded of reporting procedures and phising risks. Conducting phishing simulations and provide ongoing cybersecurity training to prevent	For past incidents, include what happend, what data was affected, and how it was resolved. Guidance for employees/stakeholders need to be provided for protecting themselves.	YES	TOLERABLE	POSSIBLE		YES	The risk level of the event has changed because there is a control in place to help mitigate this risk level down to medium.
	IT Infrastructure Vulnerabilities	Finance Team	Phishing simulations. Testing employees to see of they pass or fail certain attacks. Also having employees recognize when phishing attempts are occuring.	UNDESIRABLE	POSSIBLE		High alert - Regular vulnerability scans and network segmentation should be done to limit exposure. Security patch updates, harden systems, and pentration tests address weaknesses.	Notifications should be sent to the appropiate teams based on the affected systems and severity. Communication channels should be established for discovering vulnerabilities and effected systems	YES	UNDESIRABLE	POSSIBLE	MEDIUM	YES	The risk level of the event has changed because there is a control in place to help mitigate this risk level down to medium.
				TOLERABLE	PROBABLE				YES					
				INTOLERABLE	PROBABLE				YES					
									YES					
									YES					
									YES					
									YES					
									YES					
									YES					
									YES					
									YES					
									YES					

RISK RATING KEY

	LOW	MEDIUM	HIGH	EXTREME
	ACCEPTABLE	ALARP (as low as reasonably practicable)	GENERALLY UNACCEPTABLE	INTOLERABLE
	OK TO PROCEED	TAKE MITIGATION EFFORTS	SEEK SUPPORT	PLACE ON HOLD

LIKELIHOOD \ SEVERITY	ACCEPTABLE LITTLE TO NO EFFECT	TOLERABLE EFFECTS ARE FELT, BUT NOT CRITICAL TO OUTCOME	UNDESIRABLE SERIOUS IMPACT TO THE COURSE OF ACTION AND OUTCOME	INTOLERABLE COULD RESULT IN DISASTER
IMPROBABLE RISK IS UNLIKELY TO OCCUR	LOW	MEDIUM	MEDIUM	HIGH
POSSIBLE RISK WILL LIKELY OCCUR	LOW	MEDIUM	HIGH	EXTREME
PROBABLE RISK WILL OCCUR	MEDIUM	HIGH	HIGH	EXTREME