Risk register

Operational environment:

El banco está ubicado en una zona costera con bajos índices de delincuencia. Numerosas personas y sistemas gestionan los datos del banco: 100 empleados presenciales y 20 remotos. La base de clientes del banco incluye 2000 cuentas individuales y 200 cuentas comerciales. Un equipo deportivo profesional y diez empresas locales de la comunidad comercializan sus servicios. Existen estrictas regulaciones financieras que exigen al banco proteger sus datos y fondos, como tener suficiente efectivo disponible diariamente para cumplir con los requisitos de la Reserva Federal.

Asset	Risk(s)	Description	Probabiliy	Severity	Priority
Funds	Business email compromise	*An employee is tricked into sharing confidential information.*	3	3	9
	Compromised user database	*Los datos de los clientes están mal cifrados.*	3	3	9
	Se filtran registros financieros	*Un servidor de base de datos con datos respaldados es de acceso público.*	3	3	9
	Robo	*La caja fuerte del banco se deja abierta.*	3	3	9
	Ataque de fuerza bruta	*Intentos automatizados de adivinar credenciales de empleados o clientes para acceder a información sensible.*	2	3	6
	Transferencias fraudulentas	*Un ciberdelincuente obtiene acceso a cuentas internas y realiza transferencias no autorizadas.*	1	3	3

	Interrupción de la cadena de suministro	*Retrasos en la entrega debido a desastres naturales.*	1	2	2
	Ransomware	*Un atacante cifra los sistemas del banc datos financieros.*	3	3	9
Infrastructure	Ataque DDoS	*Un ataque de denegación de servicio satura los sistemas bancarios, impidiendo transacciones legítimas.*	1	3	3
Notes	¿Cómo son posibles los eventos de seguridad considerando los riesgos que enfrenta el activo en su entorno operativo?				
	La complejidad del sistema, con un gran número de empleados y clientes, aumenta el riesgo de ataques de phishing o robo de credenciales. Aunque la zona tenga bajos índices de delincuencia, la infraestructura digital está expuesta a vulnerabilidades que pueden comprometer los fondos. El uso de servicios remotos y la dependencia de terceros incrementan los riesgos.				

Asset: The asset at risk of being harmed, damaged, or stolen.
Risk(s): A potential risk to the organization's information systems and data.
Description: A vulnerability that might lead to a security incident.
Likelihood: Score from 1-3 of the chances of a vulnerability being exploited. A 1 means there's a low likelihood, a 2 means there's a moderate likelihood, and a 3 means there's a high likelihood.

Severity: Score from 1-3 of the potential damage the threat would cause to the business. A 1 means a low severity impact, a 2 is a moderate severity impact, and a 3 is a high severity impact.
Priority: How quickly a risk should be addressed to avoid the potential incident. Use the following formula to calculate the overall score: **Likelihood x Impact Severity = Risk**

Activo: El activo en riesgo de sufrir daños, ser dañado o robado.
Riesgo(s): Un riesgo potencial para los sistemas de información y los datos de la organización.
Descripción: Una vulnerabilidad que podría provocar un incidente de seguridad.
Probabilidad: Califique del 1 al 3 las probabilidades de que una vulnerabilidad sea explotada. Un 1 significa una probabilidad baja, un 2 significa una probabilidad moderada y un 3 significa una probabilidad alta.
Gravedad: Califique del 1 al 3 el daño potencial que la amenaza causaría a la empresa. Un 1 significa un impacto de gravedad baja, un 2 significa un impacto de gravedad moderada y un 3 significa un impacto de gravedad alta.
Prioridad: La rapidez con la que se debe abordar un riesgo para evitar el posible incidente. Utilice la siguiente fórmula para calcular la puntuación general: Probabilidad x Gravedad del impacto = Riesgo

Sample risk matrix

Likelihood	Severity: Low 1	Severity: Moderate 2	Severity: Catastrophic 3
Certain 3	3	6	9
Likely 2	2	4	6
Rare 1	1	2	3