Risk register

Operational environment:

The bank is located in a coastal area with low crime rates. Many people and systems handle the bank's data—100 on-premise employees and 20 remote employees. The customer base of the bank includes 2,000 individual accounts and 200 commercial accounts. The bank's services are marketed by a professional sports team and ten local businesses in the community. There are strict financial regulations that require the bank to secure their data and funds, like having enough cash available each day to meet Federal Reserve requirements.

Asset	Risk(s)	Description	Likelihood	Severity	Priority
Funds	Business email compromise	*An employee is tricked into sharing confidential information.*	2	3	6
	Compromised user database	*Customer data is poorly encrypted.*	1	3	3
	Financial records leak	*A database server of backed up data is publicly accessible.*	1**	3	3
	Theft	*The bank's safe is left unlocked.*	1	2	2
	Supply chain disruption	*Delivery delays due to natural disasters.*	1	1	1
Notes	*How are security events possible considering the risks the asset faces in its operating environment?*				

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**

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

1) Employee sharing confidential information, it is possible via social engineering and phishing, so it is more likely to happen but not certain. Depending on who leaks their information, their level of access will determine the severity, but I would place it at either 2 or 3
2) The bank has strict policies and regulations requiring the bank to secure their funds and data, so it is unlikely that the user database would be compromised; however in the event that it was compromised, it would be level 3 severity bc the database contains SPII of all clients and could cause hefty damage in the wrong hands *** **because of backup leak possibility, likelihood should be a 2**
3) Because of strict policies, it is very unlikely that there would be a data leak from a database server of backed up data to be publicly leaked, but severe if it were to happen *** **Should actually be certain because of the marketing and remote employees, so likelihood of backup server to be with one of the employees or elsewhere is high.**
4) Bank's safe unlocked; people are careless sometimes so this is more likely, but the severity is moderate because while losing cash is bad, the area of the bank has low crime rates and the bank gets its cash reserves replenished every day
5) Delivery delays due to natural disasters, likelihood is low and severity is also low. Severity is low because the bank generally doesn't use all its cash reserves within a given day, plus with debit and credit cards, cash is becoming less and less popular.