Cyber Security

Capstone Project Problem Statement

Capstone Project: Comprehensive Business Continuity

Background of the problem statement:

ZZIIPPEE Bank is one of the fastest growing banks in India with more than 1200 branches across the country and manages $200 billion in assets. Handling millions of dollars of banking transactions per day, its customers depend upon the integrity and availability of their banking data.

The Bank has to comply with a new cybersecurity regulation that requires financial institutions to have DRPs and BCPs to prevent massive losses during a disaster or data breach.

The Bank realizes that it has to move its IT operations to a less risk-prone area. Furthermore, it has to separate its production and disaster-recovery facilities by a large distance to be immune to a widespread disaster. But it has to do this in such a way that it would lose no data in the event of a production data-center disaster.
The Bank plans to consolidate its multiple data centers into a single production data center with remote protection. It plans to have their disaster-recovery site in another state with an equipment configuration that is an exact mirror of the production facility.

The Bank plans to keep the backup data-center's databases in synchronism with the production data center via asynchronous replication.

However, the Bank estimates that it might lose up to 30 seconds of data following a production-site outage because of the asynchronous-replication solution. To solve this problem, the Bank can use a third minimal disk-only "bunker" site closer to the production site to act as a second up-to-date data repository.

The Bunker is a secure ex-military compound, purpose-built to protect data from every potential threat including nuclear attack. All infrastructure is kept 30 meters below ground, behind concrete walls three meters thick only accessible through two-ton steel doors and guarded 24/7. It is flood proof, bomb proof, and immune to EMP and digital-eavesdropping.

Therefore, should the production site fail, the nearby data bunker would contain all transactions that were executed up to the time of the outage. No data would be lost. This data bunker is designed to survive the effects of a disaster that could take down the production site. The data bunker would be linked to both the production site and the backup site. In the event of a production-site outage, the backup site would quickly bring its database up-to-date by establishing a session with the data bunker and downloading

only the data changes that it had missed. Once this is accomplished, the backup site would be put into production with zero data loss.

Implementing a 3-Data-Center (3DC) architecture using a mix of asynchronous and synchronous replication ensures that no common disaster will prevent the Bank from offering its services to its customers and partners while at the same time ensures zero data loss and fast recovery times.

You are required to complete the following tasks to assist the Bank to implement a comprehensive business-continuity, backup, recovery, and archiving solution.

Task 1

Identify minimum three threats per category that could disrupt the bank's operations.

Categories	**Threats**
System Events	Network problems, hardware or software failures, corrupted data, bugs, glitches, viruses
Internal Events	Fire, plumbing leaks, human error, electrical spikes, construction defects, angry employee
External Events	Utility interruptions, sabotage or terrorism, hacking, accidents
Acts of Nature	Hurricane or typhoon, tornados, earthquakes , floods

Task 2

A new vulnerability was identified in the bank mobile app during a vulnerability assessment. The vulnerability allows a remote unauthorized user to easily upload and execute a simple script to cause a major denial-of-service (DoS) attack on the web server.

Use the CVSS 3.1 calculator to calculate the base score and identify the vulnerability as critical, high, medium, or low.

Copy and paste the URL that includes the selected parameters.

https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Score (6.5) Medium

Task 3

Complete the following Risk Register:

THREAT	RISK DESCRIPTION	IMPACT LEVEL	LIKELIHOOD LEVEL	PRIORITY LEVEL	MITIGATION NOTES
	Brief summary of the risk	Rate 1 (Low) 5 (High)	Rate 1 (Low) 5 (High)	(IMPACT x PROBABILITY) Address highest first	What can be done to minimize the risk?
Ransomware attack	Unable to access critical System/Info (data encryption) , loss due to paying the ransom , lost productivity .	5	3	15	Awareness , anti-ransomware , backups , SIEM , regular offsite
Tornado	Damaged building, , loss of life , loss of critical systems	4	4	16	DRP , BCP
SQL injection attack on the customer portal	Data loss, corruption, or disclosure to unauthorized parties, loss of accountability, or denial of access.	4	1	4	Input validation, parametrized, stored procedures, queries, WAF
Data breach by third-party service provider	Reputation loss, compliance risk, financial loss	5	5	25	Contracts, SLA, independent audits

- Use the following Risk Matrix to calculate the priority level:

IMPACT

LIKELIHOOD	Negligible (1)	Minor (2)	Moderate (3)	Significant (4)	Severe (5)
Very Likely (5)	5	10	15	20	25
Likely (4)	4	8	12	16	20
Possible (3)	3	6	9	12	15
Unlikely (2)	2	4	6	8	10
Very Unlikely (1)	1	2	3	4	5

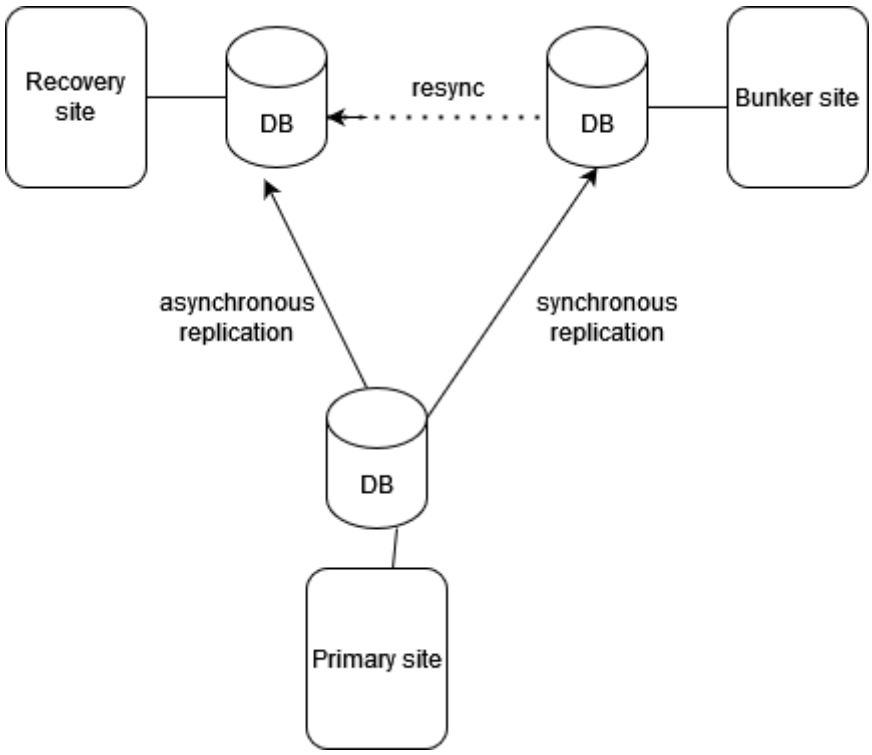
Task 4

- If the primary database is corrupted by an incident, the bank might lose 30 seconds of data at the recovery site.
- The transaction throughput at the recovery site will be 75%.
- The bank will be able to use the database from recovery site, but customer experience will be negatively affected after 24 hours.
- The access to the primary database will be restored within eight hours.
- Based on the given scenario, identify the values for the following parameters:

Parameter	Value
Recovery time objective (RTO)	8hours
Maximum tolerable outage (MTO)	24hours
Service delivery objective (SDO)	Transection throughput at 75% capacity
Recovery point objective (RPO)	30s

Task 5

Draw the 3-data-center architecture diagram described in the above scenario.


Recovery site
DB
resync
DB
Bunker site
asynchronous replication
synchronous replication
DB
Primary site