**Cyber Security**

Capstone Project Problem Statement

**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:**

**Answer:**

Minimum three threats per category that could disrupt the bank’s operations are below:

|  |  |
| --- | --- |
| **Categories** | **Threats** |
| System Events | Unencrypted data, Malware, Third party services that aren't secure |
| Internal Events | Cultural shift, Data that has wrongly been manipulated, Physical damage to hardware |
| External Events | Customers retention, Cannot attain gain, Competitors core advantage |
| Acts of Nature | Earthquakes, Flooding, Cyclones or Hurricanes |

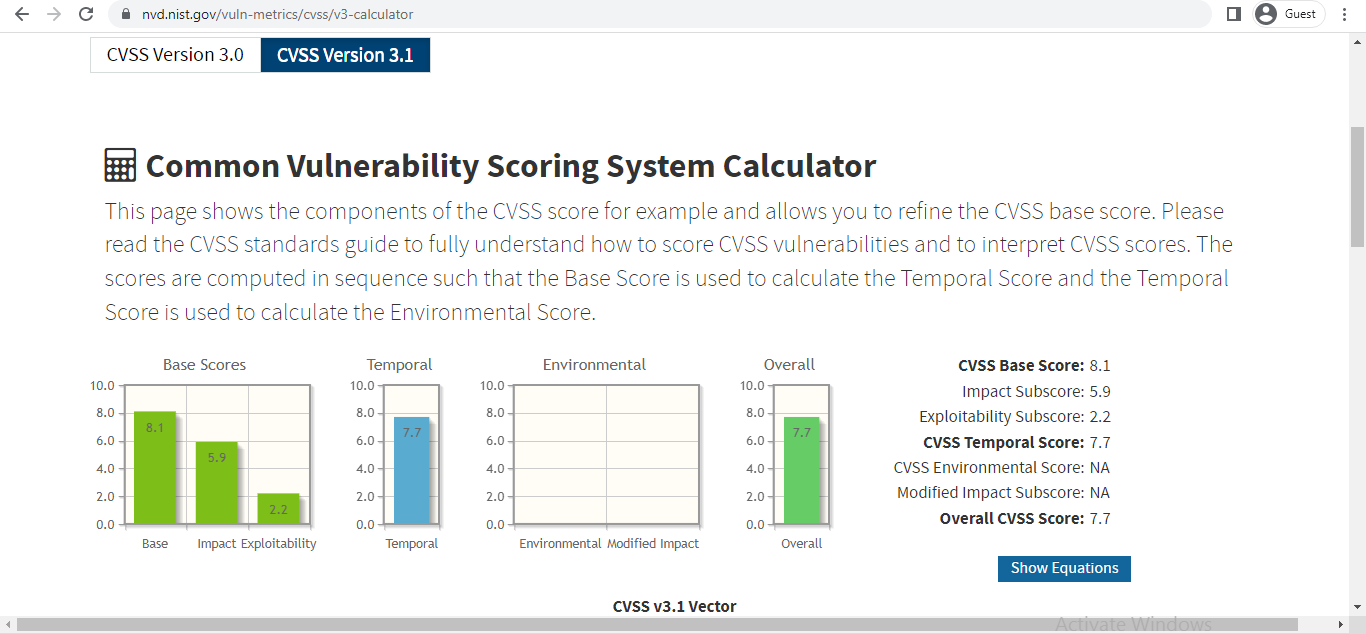
**Task 2:**

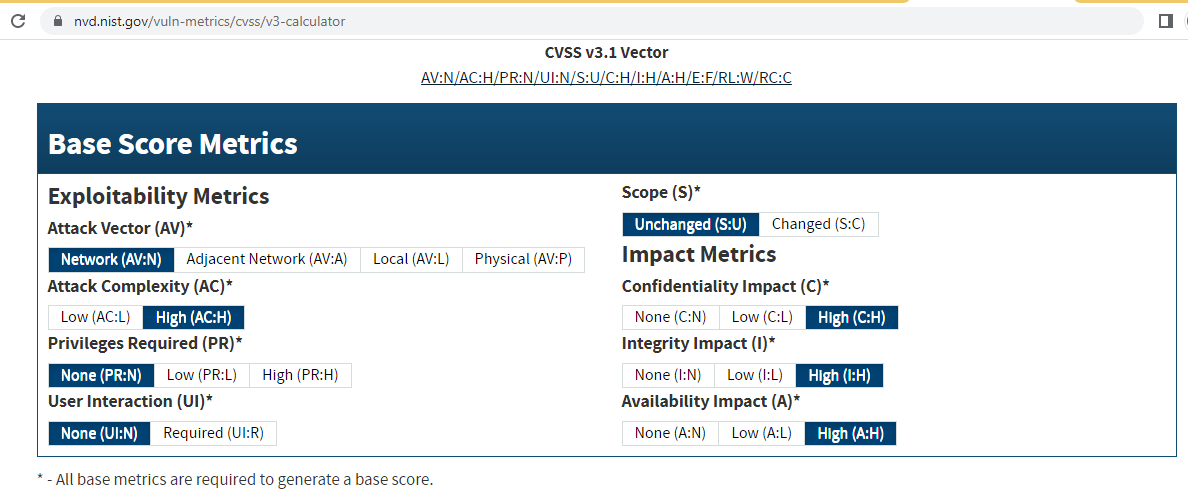
**Answer:**

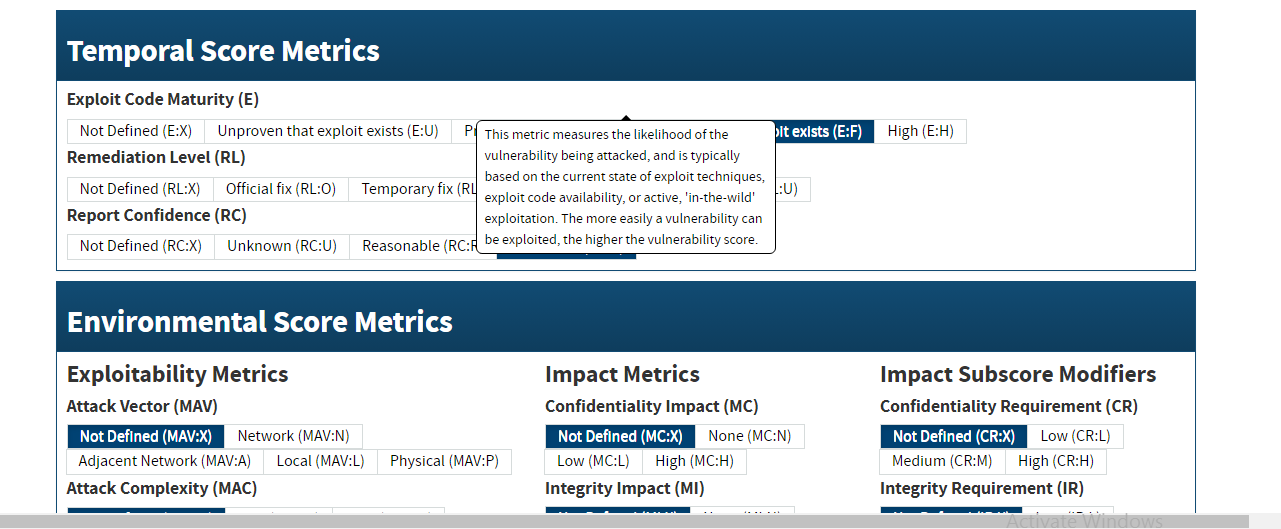
To calculate the base score for the identified vulnerability in the bank's mobile app, let's use the CVSS 3.1 calculator. The provided information indicates that the vulnerability allows a remote unauthorized user to easily upload and execute a simple script to cause a major denial-of-service (DoS) attack on the web server.

Using the CVSS 3.1 calculator, we can determine the base score and the associated severity level. Here are the selected parameters:

* **Attack Vector (AV):** Network (N)
* **Attack Complexity (AC):** Low (L)
* **Privileges Required (PR):** None (N)
* **User Interaction (UI):** None (N)
* **Scope (S):** Unchanged (U)
* **Confidentiality (C):** None (N)
* **Integrity (I):** None (N)
* **Availability (A):** High (H)

****

****1: Base Score



02: Tempoal Scoral

**URL that includes the selected parameters:**

<https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:W/RC:C&version=3.1>

**TASK:3.**

**ANSWER:**

Here is the completed Risk Register based on the information provided and the given Risk Matrix:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **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 | Unauthorized access and data encryption | Severe (5) | Very Likely (5 | 25 | Regular data backups, strong cybersecurity measures |
| Tornado | Physical damage to infrastructure | Severe (5) | Unlikely (2) | 10 | Implement disaster recovery plan, safe storage |
| SQL injection attack on the customer portal | Unauthorized data access and manipulation | Significant (4) | Possible (3) | 12 | Regular code reviews, input validation |
| Data breach by third-party service provider | Exposure of sensitive data | Significant (4) | Likely (4) | 16 | Thorough vendor assessment, contractual safeguards |

The priority level for each risk is calculated by multiplying the impact level by the likelihood level:

1. Ransomware attack: Priority Level = 5 (Impact) x 5 (Likelihood) = 25
2. Tornado: Priority Level = 5 (Impact) x 2 (Likelihood) = 10
3. SQL injection attack: Priority Level = 4 (Impact) x 3 (Likelihood) = 12
4. Data breach by third-party service provider: Priority Level = 4 (Impact) x 4 (Likelihood) = 16

The priority level indicates the relative urgency of addressing each risk. It's recommended to focus on mitigating the risks with the highest priority levels first. The mitigation notes provide general strategies for minimizing each risk.

**TASK:4.**

**ANSWERS:**

Based on the provided scenario, we can identify the values for the following parameters:

* Recovery Time Objective (RTO): The maximum acceptable time it takes to recover the system after an incident.

Since access to the primary database will be restored within eight hours, the RTO would be 8 hours.

* Maximum Tolerable Outage (MTO): The maximum amount of time a system can be unavailable before it starts having significant negative impacts on the organization.

Since customer experience will be negatively affected after 24 hours, the MTO would be 24 hours.

* Service Delivery Objective (SDO): The level of service that an organization aims to provide
* during a disaster or disruption.

The scenario doesn't explicitly provide a value for the SDO, but it does mention that customer experience will be negatively affected after 24 hours. This could be considered as the SDO, indicating that the bank aims to maintain an acceptable level of customer experience for at least 24 hours.

* Recovery Point Objective (RPO): The maximum acceptable amount of data loss that an organization is willing to tolerate during a recovery.

Since the bank estimates that it might lose up to 30 seconds of data in the event of a primary database corruption, the RPO would be 30 seconds.

To summarize:

|  |  |
| --- | --- |
| **Parameter** | **Value** |
| Recovery time objective (RTO) | 8 hours |
| Maximum tolerable outage (MTO) | 24 hours |
| Service delivery objective (SDO) | 75% |
| Recovery point objective (RPO) | 30 seconds |

Based on the provided scenario, we can identify the values for the following parameters:

* Recovery Time Objective (RTO): The maximum acceptable time it takes to recover the system after an incident.

Since access to the primary database will be restored within eight hours, the RTO would be 8 hours.

* Maximum Tolerable Outage (MTO): The maximum amount of time a system can be unavailable before it starts having significant negative impacts on the organization.

Since customer experience will be negatively affected after 24 hours, the MTO would be 24 hours.

* Service Delivery Objective (SDO): The level of service that an organization aims to provide
* during a disaster or disruption.

The scenario doesn't explicitly provide a value for the SDO, but it does mention that customer experience will be negatively affected after 24 hours. This could be considered as the SDO, indicating that the bank aims to maintain an acceptable level of customer experience for at least 24 hours.

* Recovery Point Objective (RPO): The maximum acceptable amount of data loss that an organization is willing to tolerate during a recovery.

Since the bank estimates that it might lose up to 30 seconds of data in the event of a primary database corruption, the RPO would be 30 seconds.

To summarize:

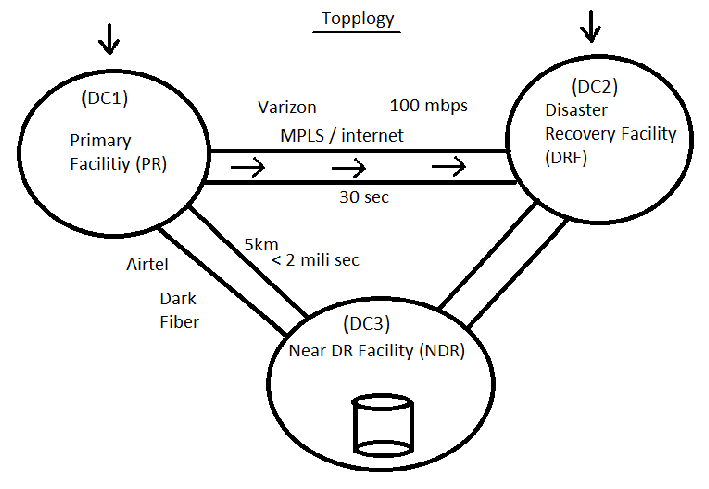
* Recovery Time Objective (RTO): 8 hours
* Maximum Tolerable Outage (MTO): 24 hours

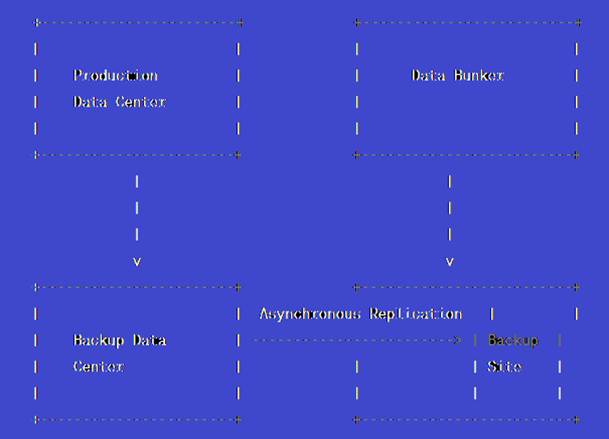
Service Delivery Objective (SDO): Maintain acceptable customer experience for at least 24 hours

Recovery Point Objective (RPO): 30 seconds

**TASK:5.**

**ANSWERS:**





**3-data-center architecture diagram**

**Assumptions:**

* Three geographically distributed data centers: DC1, DC2, and DC3.
* Each data center contains a portion of the Bank's infrastructure, including servers, databases, and networking components.

**Key Components:**

1. **Load Balancers:** Deploy load balancers in front of each data center to distribute incoming requests from clients evenly across the available resources.
2. **Database Replication:**
   * **Synchronous Replication:** Implement synchronous replication within a data center (e.g., DC1) to ensure zero data loss between primary and secondary databases. This provides strong consistency but might introduce latency due to the waiting for acknowledgments.
   * **Asynchronous Replication:** Implement asynchronous replication between data centers (e.g., DC1 to DC2, and DC1 to DC3). Asynchronous replication offers faster response times by not waiting for acknowledgments, but it might introduce some data loss in case of a disaster.
3. **Data Backup and Snapshotting:**
   * Regularly backup the data in each data center to secure storage or a cloud environment. These backups can be used for restoring data in case of catastrophic failures.
   * Utilize snapshotting techniques to create consistent copies of databases at specific intervals, allowing for faster recovery points.
4. **Disaster Recovery (DR) Sites:**
   * Each data center can serve as a Disaster Recovery (DR) site for another data center. For example, DC2 can act as the DR site for DC1, and DC3 can be the DR site for DC1.
   * In the event of a disaster in one data center, the relevant DR site can take over operations. Synchronous replication minimizes data loss between the primary and DR site.
5. **Global Traffic Management:**
   * Use global traffic management solutions to direct incoming traffic to the operational data center. In the case of a disaster affecting one data center, traffic can be redirected to the DR site.
6. **Automated Failover and Recovery:**
   * Implement automated failover mechanisms that detect when a data center becomes unavailable and automatically switch to the DR site.
   * Set up scripts or tools to automatically initiate the recovery process once the primary data center becomes operational again.
7. **Network Redundancy:**
   * Ensure redundant network paths between data centers to minimize the impact of network failures.

**Benefits:**

* **High Availability:** The architecture ensures that even if one data center experiences a disaster, the Bank's services can continue to operate from other data centers without significant disruption.
* **Data Integrity:** Synchronous replication guarantees data consistency within a data center, while periodic asynchronous replication ensures minimal data loss between data centers.
* **Fast Recovery:** Automated failover and recovery mechanisms, coupled with DR sites, enable rapid restoration of services.
* **Disaster Resilience:** Geographic distribution reduces the risk of a single disaster affecting all data centers simultaneously.

**Challenges:**

* **Latency:** Synchronous replication can introduce latency due to the need for acknowledgments between primary and secondary databases.
* **Data Conflicts:** In asynchronous replication scenarios, conflicts might arise if updates occur simultaneously in different data centers.

It's important to note that implementing such an architecture requires careful planning, thorough testing, and ongoing maintenance to ensure its effectiveness and reliability. Additionally, regulatory and compliance considerations specific to the banking industry should be taken into account when designing the architecture.

**“THE END”**