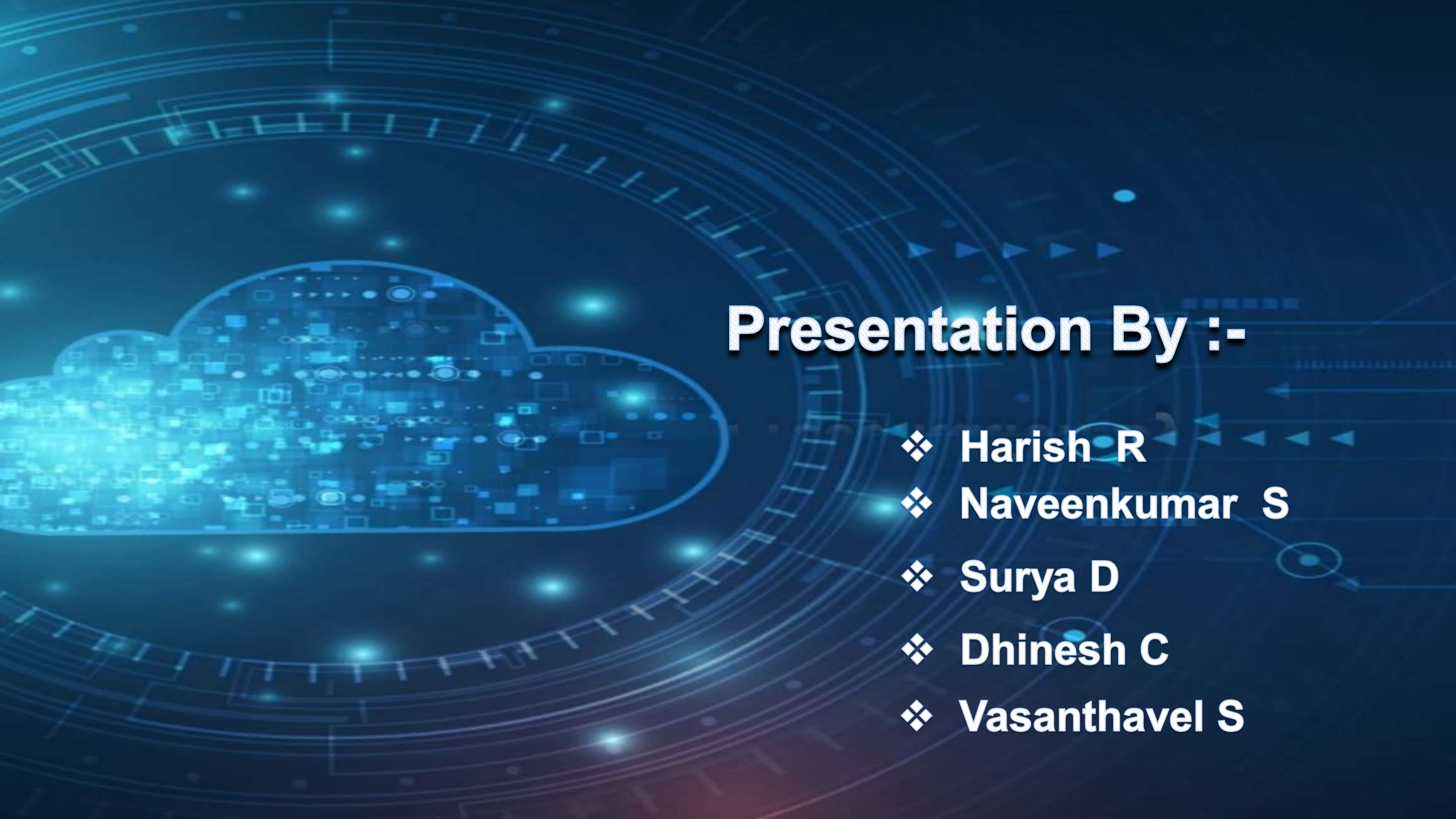
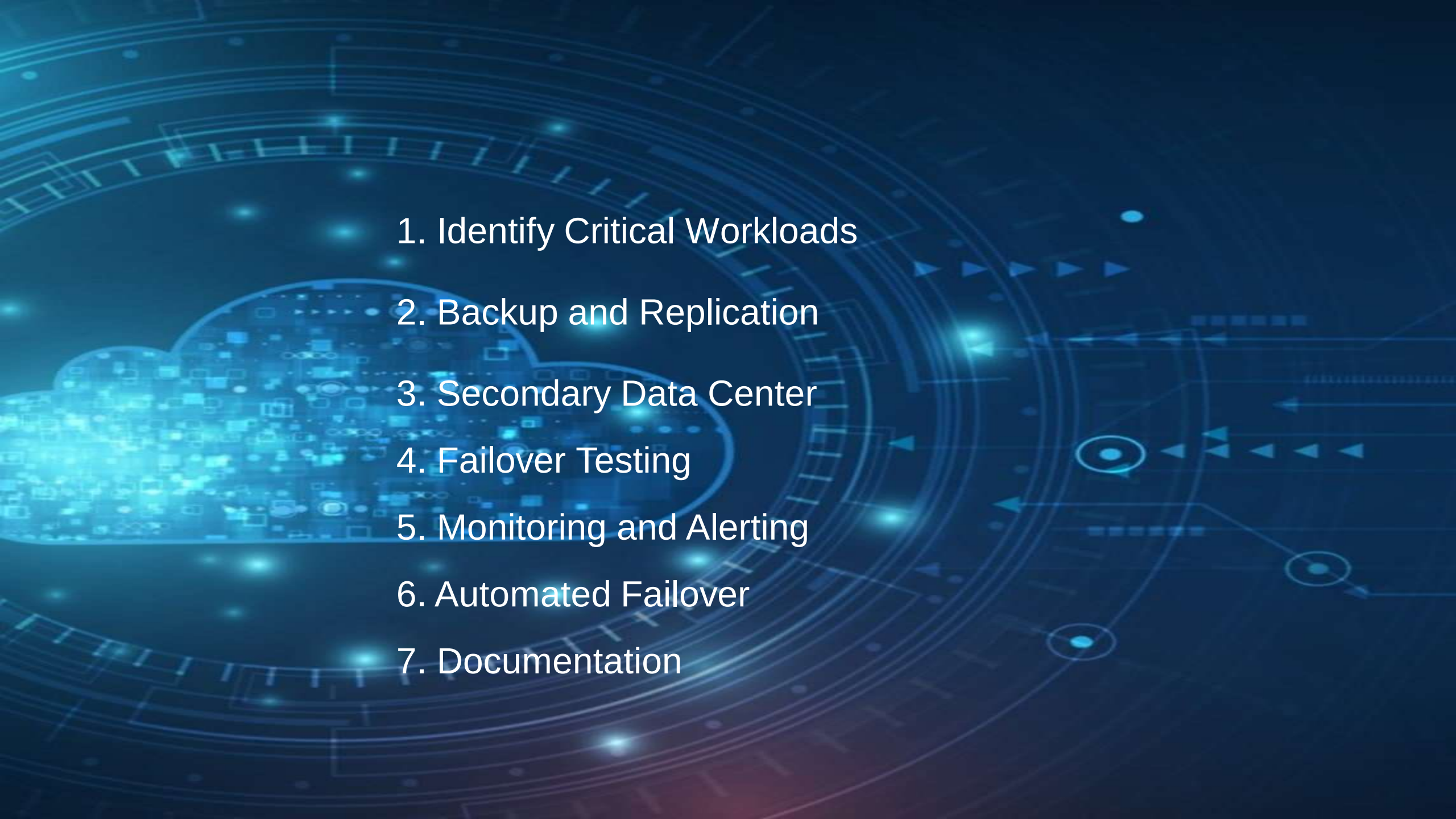
DISASTER RECOVERY WITH IBM CLOUD VIRTUAL SERVERS


Presentation By :-
Harish R
Naveenkumar S
Surya D
Dhinesh C
Vasanthavel S

Disaster Recovery with IBM Cloud Virtual Servers

Introduction:-

Disaster recovery with IBM Cloud Virtual Servers involves setting up a plan to ensure the availability and resilience of your virtual server infrastructure in the event of a disaster. Here are some steps you can take:

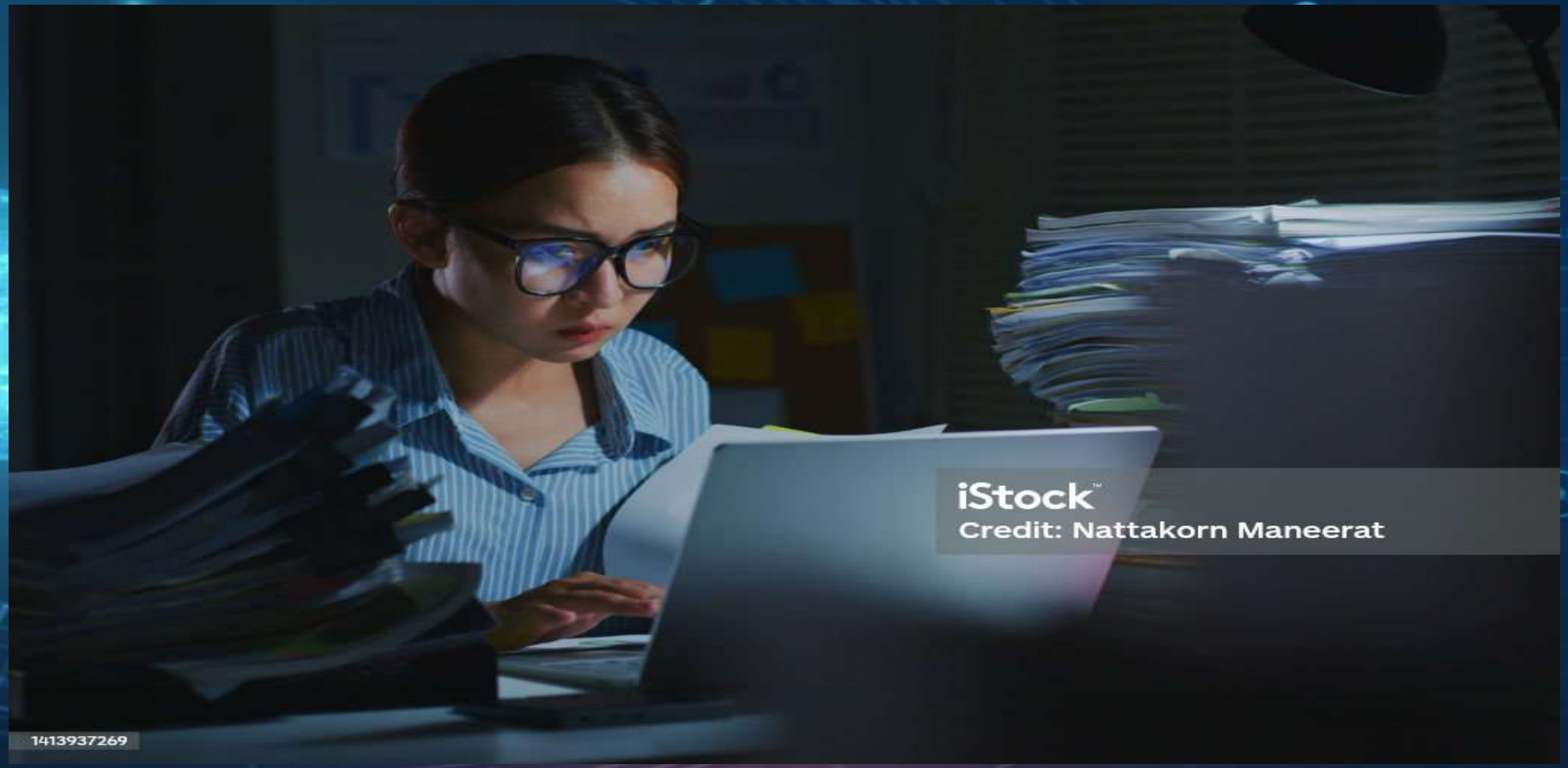

1. Identify Critical Workloads
2. Backup and Replication
3. Secondary Data Center
4. Failover Testing
5. Monitoring and Alerting
6. Automated Failover
7. Documentation

1. Identify Critical Workloads:-

Critical workloads are specific tasks or processes within an organization that are of utmost importance and have a significant impact on the business's operation, revenue, or reputation. Identifying critical workloads is essential for prioritizing resources and ensuring their smooth functioning. These workloads often include:

- ✓ Manufacturing Control Systems
- ✓ Emergency Services
- ✓ Communication Infrastructure
- ✓ Supply Chain Management
- ✓ Energy and Utilities
- ✓ National Security and Defense
- ✓ Data Centers
- ✓ Disaster Recovery

Identify Critical Workloads



2. Backup and Replication :-

Backup and replication are two essential data management strategies used to ensure the availability, integrity, and recoverability of data in various IT environments:

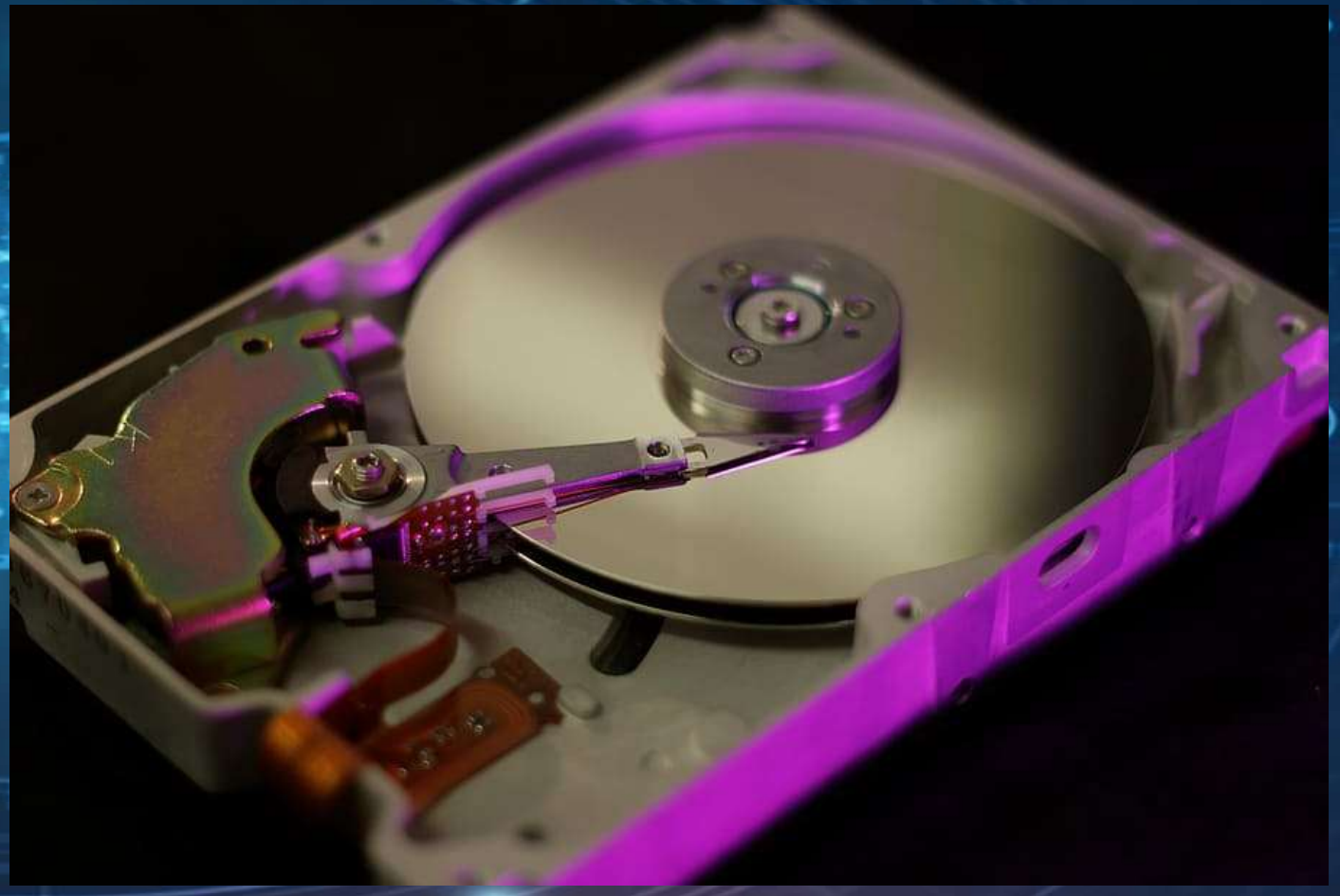
✓ Backup :

Backup is the process of creating a copy of data and storing it separately from the original data source. The primary purpose of backups is to ensure data can be recovered in case of data loss due to various reasons such as hardware failure, accidental deletion, or data corruption. Backups can be full (entire data), incremental (only changes since the last backup), or differential (changes since the last full backup).

✓ Replication :

Replication involves creating and maintaining duplicate copies of data in real-time or near-real-time. The primary purpose of replication is to provide high availability and fault tolerance. If one copy of the data becomes inaccessible due to hardware failure or other issues, another copy is readily available for use. Replication can occur within the same data center or across geographically distant locations for disaster recovery.

Backup and Replication



3. Secondary Data Center

A secondary data center, often referred to as a backup or disaster recovery data center, is a facility that replicates or stores data and applications from a primary data center. It serves as a redundancy measure to ensure business continuity in case the primary data center experiences downtime due to unforeseen events like natural disasters, hardware failures, or cyberattacks. In the event of a primary data center failure, the secondary data center can take over to minimize service disruptions and data loss. This redundancy is a crucial part of a company's IT infrastructure and disaster recovery planning.

Secondary Data Center

4. Failover Testing :

Failure testing, also known as fault tolerance testing or resilience testing, is a type of software testing that assesses how well a system or application

❑ **Common types of failure testing include:**

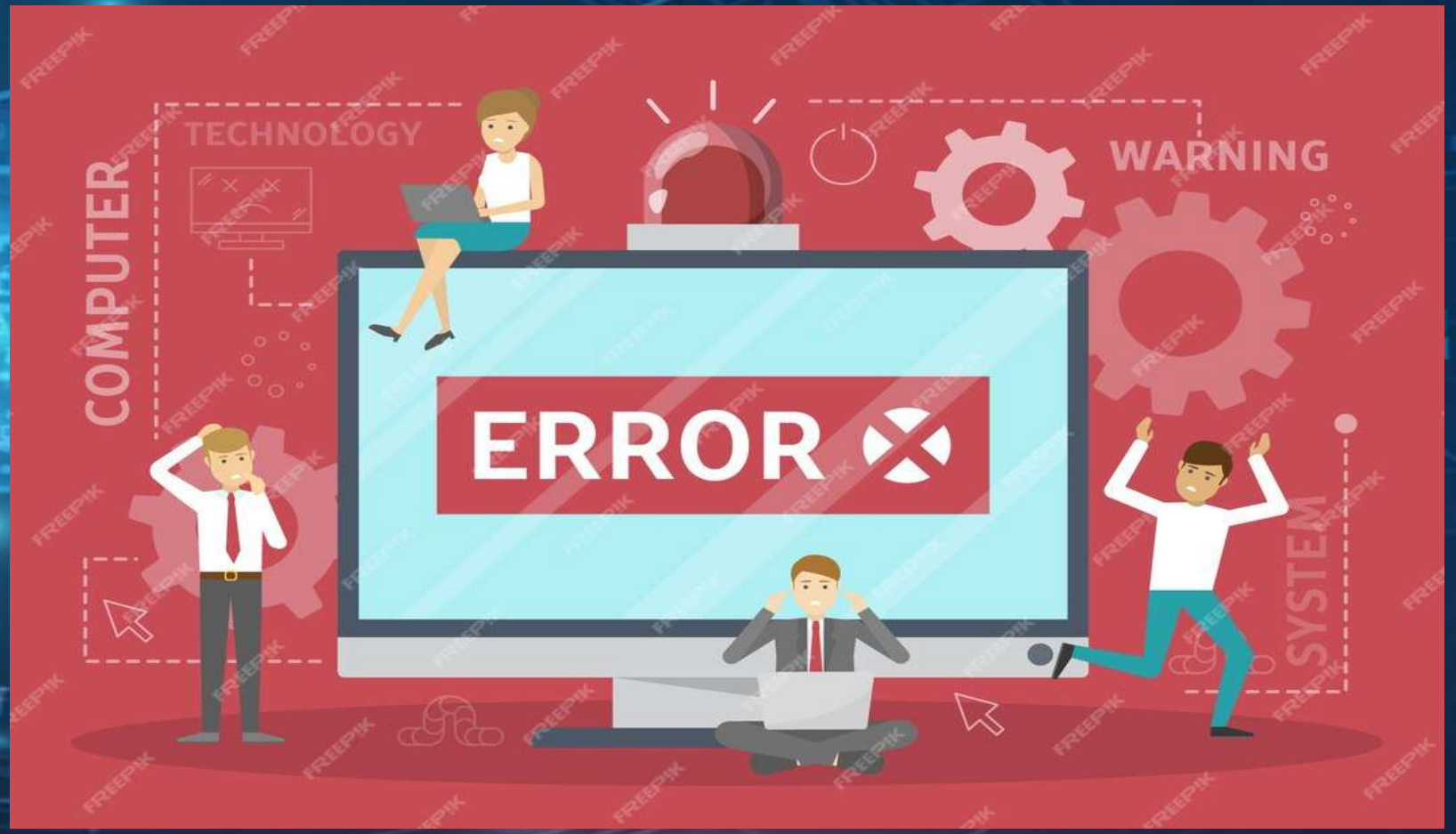
✓ Fault Injection Testing:

Deliberately introducing faults or failures into the system, such as simulating hardware failures, network outages, or software crashes, to observe how the system responds.

✓ Load Testing:

Overloading the system with an excessive volume of traffic or requests to determine how it handles increased loads and whether it can recover to normal operation afterward.

Failover Testing



5. Monitoring and Alerting

Monitoring and alerting are crucial aspects of system and network management. They involve:

✓ Monitoring:

This is the continuous observation of various metrics and parameters in a system, network, or application. It helps you understand the current state, performance, and health of these systems. Monitoring tools collect data on things like CPU usage, memory, network traffic, and more.

✓ Alerting:

Once you have monitoring in place, alerting comes into play. It involves setting up thresholds and rules based on the monitored data. When certain conditions are met or exceeded (e.g., high CPU usage or server downtime), alerts are triggered. These alerts can be notifications (emails, SMS, etc.) that notify administrators or relevant personnel of potential issues

Monitoring and Alerting

6. Automated Failover :

Automated failover is a critical component of high availability and disaster recovery planning. It refers to the automatic and seamless transition of services or resources from one system or location to another in the event of a failure. Here are some key points about automated failover:

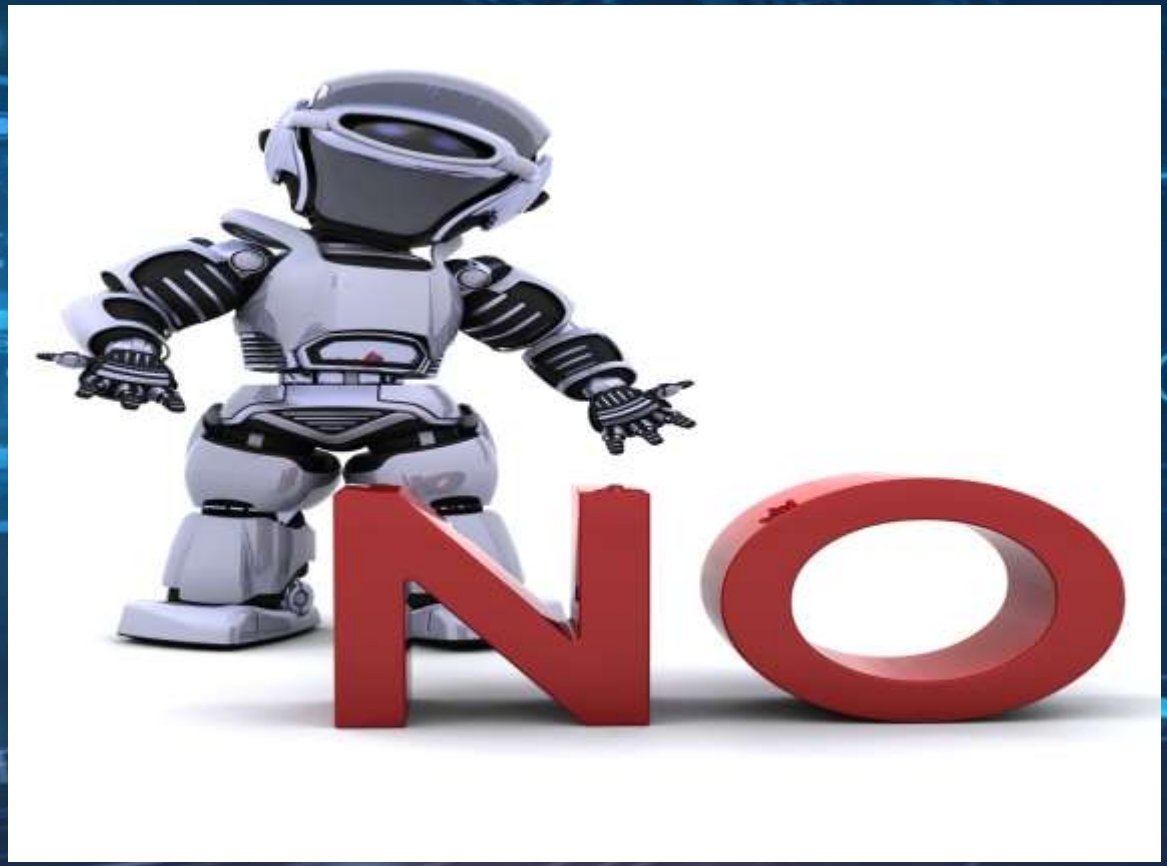
- ✓ Redundancy:

To implement automated failover, you typically have redundant systems or resources in place. This redundancy can be at the hardware, software, or network level. For example, you might have multiple servers, data centers, or cloud regions

- ✓ Monitoring:

Continuous monitoring is essential to detect when a failure occurs. Monitoring tools track the health and performance of systems and can trigger the failover process when predefined conditions (such as system downtime or excessive latency) are met.

Automatic Fail Over



7. Documentation

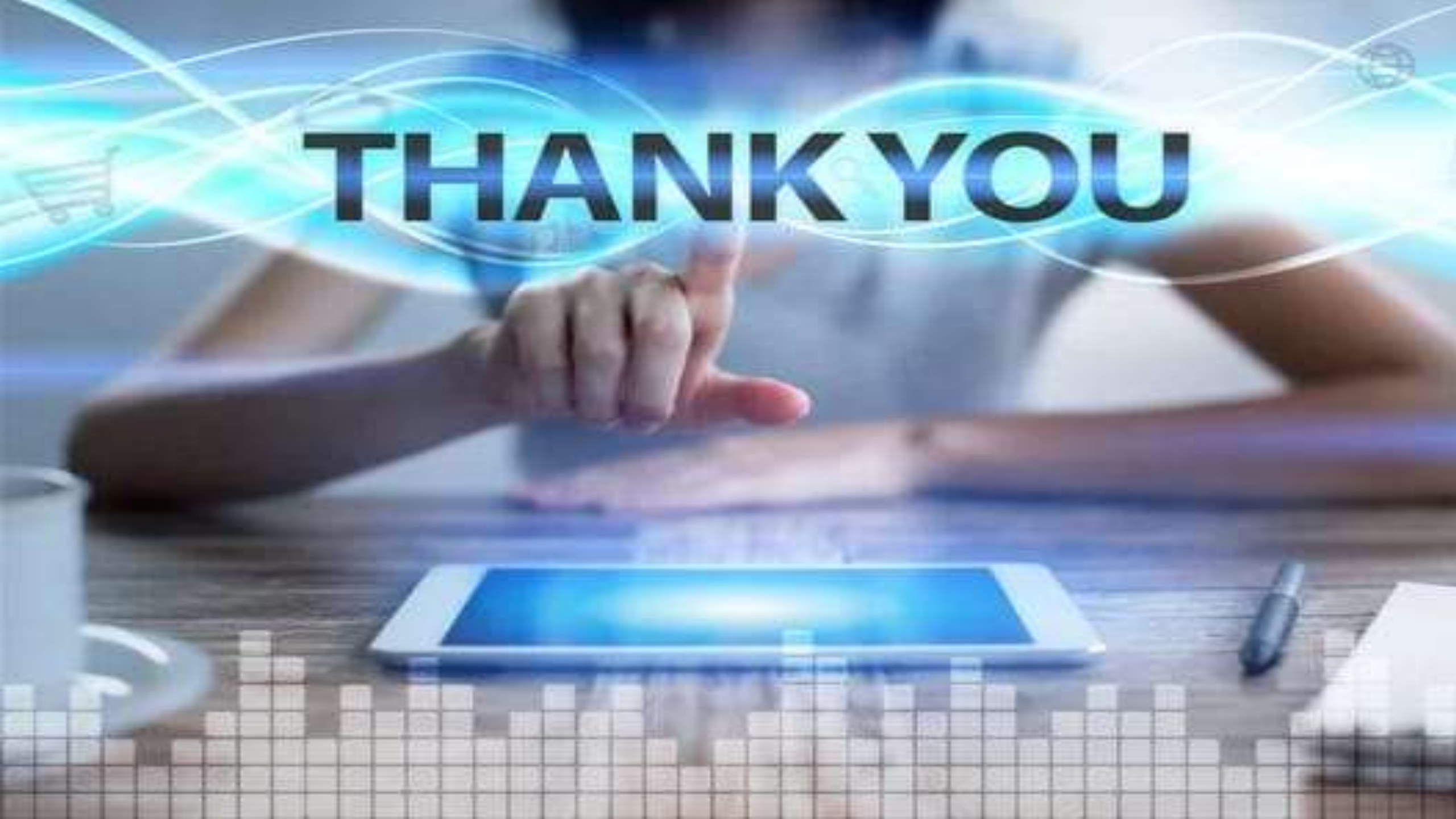
Documentation is essential in various aspects of life, from software development and project management to business operations and personal endeavors. Here are some key points about documentation

❑ Types of Documentation:

- ✓ Technical Documentation
- ✓ Project Documentation
- ✓ Business Documentation
- ✓ Personal Documentation

❑ Benefits of Documentation:

- ✓ Knowledge Transfer
- ✓ Troubleshooting
- ✓ Training
- ✓ Compliance
- ✓ Communication


THANK YOU