Business Continuity and Disaster Recovery (BCP/DRP)

A Comprehensive Guide to understand BCP/DRP.

Authored by: Khushi Malhotra

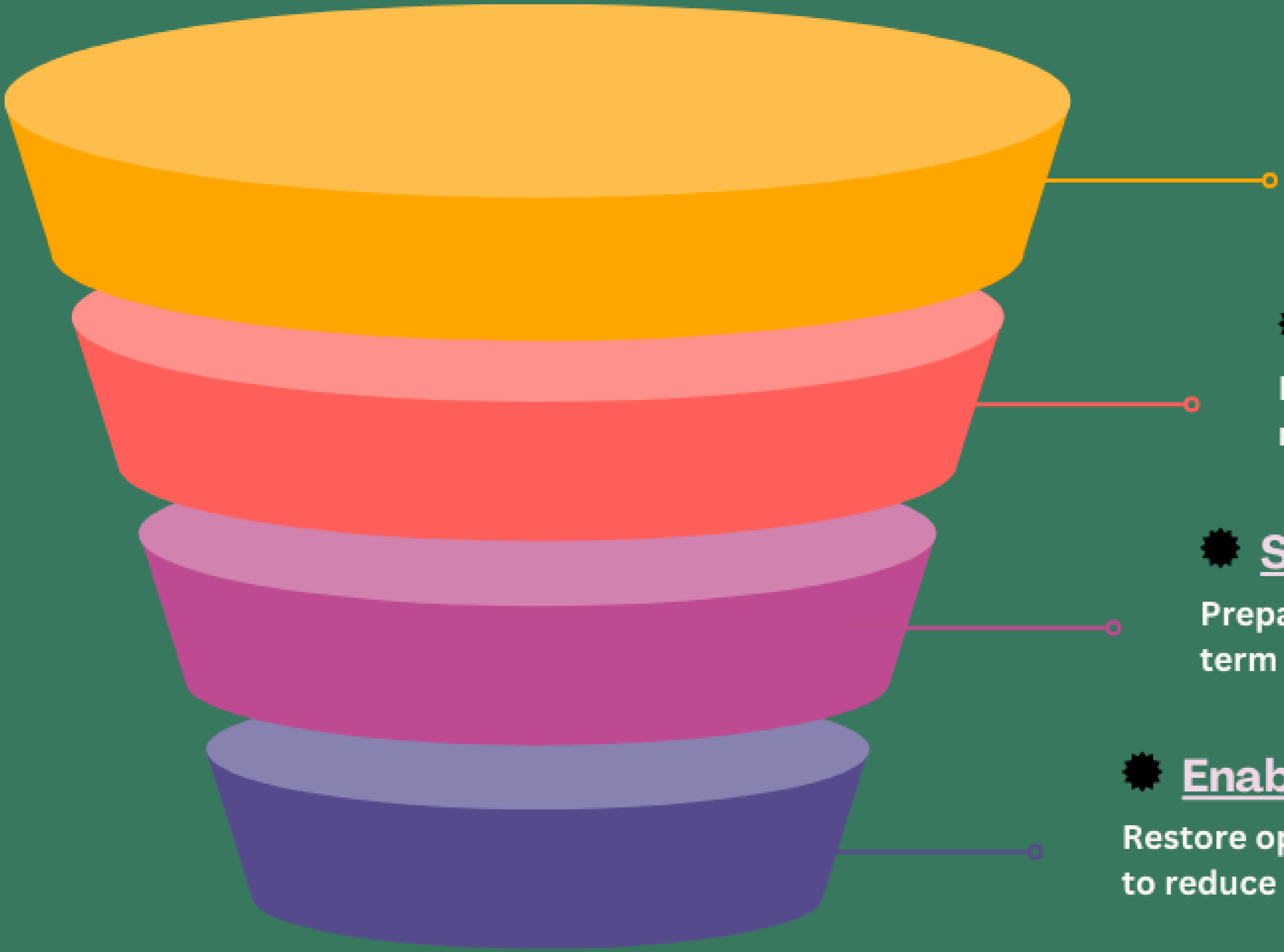
Introduction

BCP: BCP ensures that essential business operations continue during and after a disruption.

DR: DRP focuses specifically on recovering IT systems and data after a disaster or disruption.

- Ensures critical operations continue with minimal interruptions during disruptions. **01**
- Safeguards important data, systems, and resources from loss or damage. **02**
- Enables the organization to restore operations swiftly and efficiently. **03**

Objectives of BCP and DRP



- **Minimize Disruption**

  Ensure key business operations continue smoothly during disruptions.

- **Ensure Compliance**

  Meet legal and regulatory requirements to avoid penalties.

- **Strengthen Resilience**

  Prepare to adapt and recover for long-term stability.

- **Enable Rapid Recovery**

  Restore operations and systems quickly to reduce downtime.

Key Differences Between BCP and DRP

BCP

VS

- Ensures business functions continue during disruptions.
- Covers all operations, processes, and resources.
- Activated before, during, and after a disruption.
- Activated before, during, and after a disruption.

DRP

- Restores IT systems and data after a disaster.
- Focuses on IT infrastructure and critical data.
- Implemented after a disaster or major IT failure.
- Prevents data loss and enables quick IT recovery.

Components of a BCP

MINISTRY OF MOS SECURITY

Supply Chain Disruptions

Delays or disruptions from vendors affecting operations.

Power Outages

Electrical outages disrupting IT & operations.

Regulatory Non-Compliance

Failure to meet standards, leading to penalties.

Economic Instability

Financial crises or market changes impacting operations.

Cybersecurity Breaches

Cyberattacks such as ransomware, phishing compromising systems.

Components of a DRP

Risk Assessment

Identifies potential risks and threats to IT systems.

Recovery Strategies

Defines steps to restore IT infrastructure & services.

Disaster Recovery Team

Assigns roles and responsibilities for effective recovery.

Data Backup and Recovery

Ensures regular backups and outlines data restoration steps.

Plan Maintenance

Updates the DRP to address new business or tech changes.

BCP/DRP Framework

IDENTIFY CRITICAL OPERATIONS

Pinpoint essential business processes and assets

ASSESS RISKS

Evaluate vulnerabilities and potential downtime

DEVELOP PLANS

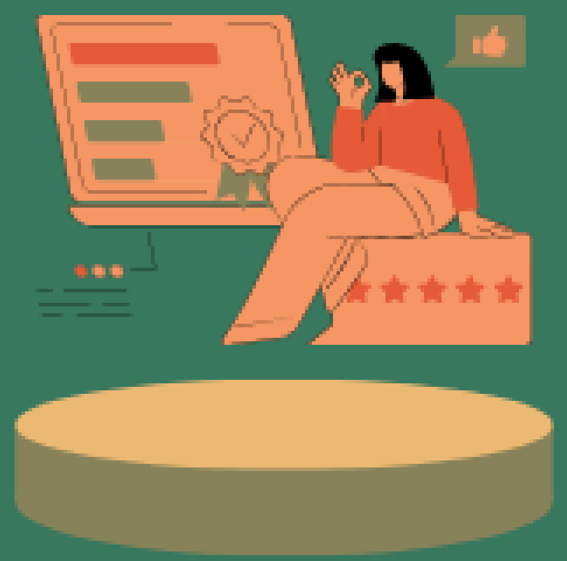
Draft recovery procedures & communication plans.

IMPLEMENT TRAINING

Train employees on their roles in the plan.

TEST AND REVISE

Conduct regular drills and adapt to new risks.



Tools and Technologies

Cloud Backup Solutions

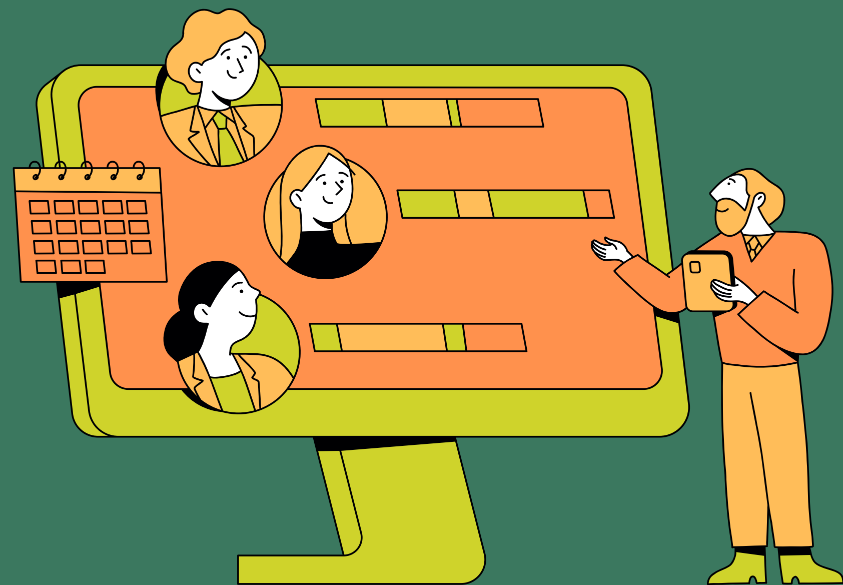
AWS, Azure Backup, Google Cloud.

Disaster Recovery as a Service

Services like Zerto, Veeam, and Acronis.

Automation Tools

PagerDuty, Splunk for incident management.



Real-Life Example of BCP/DRP

PROBLEM

In 2016, Netflix experienced a significant disruption when its AWS cloud infrastructure suffered an outage due to a technical issue in one of its data centers. This affected streaming services for millions of users globally.

BCP/DRP RESPONSE

Team quickly communicated via Slack, restored data using cloud backups, & shifted to backup data centers. It helps minimized downtime & highlighted the importance.

OUTCOME

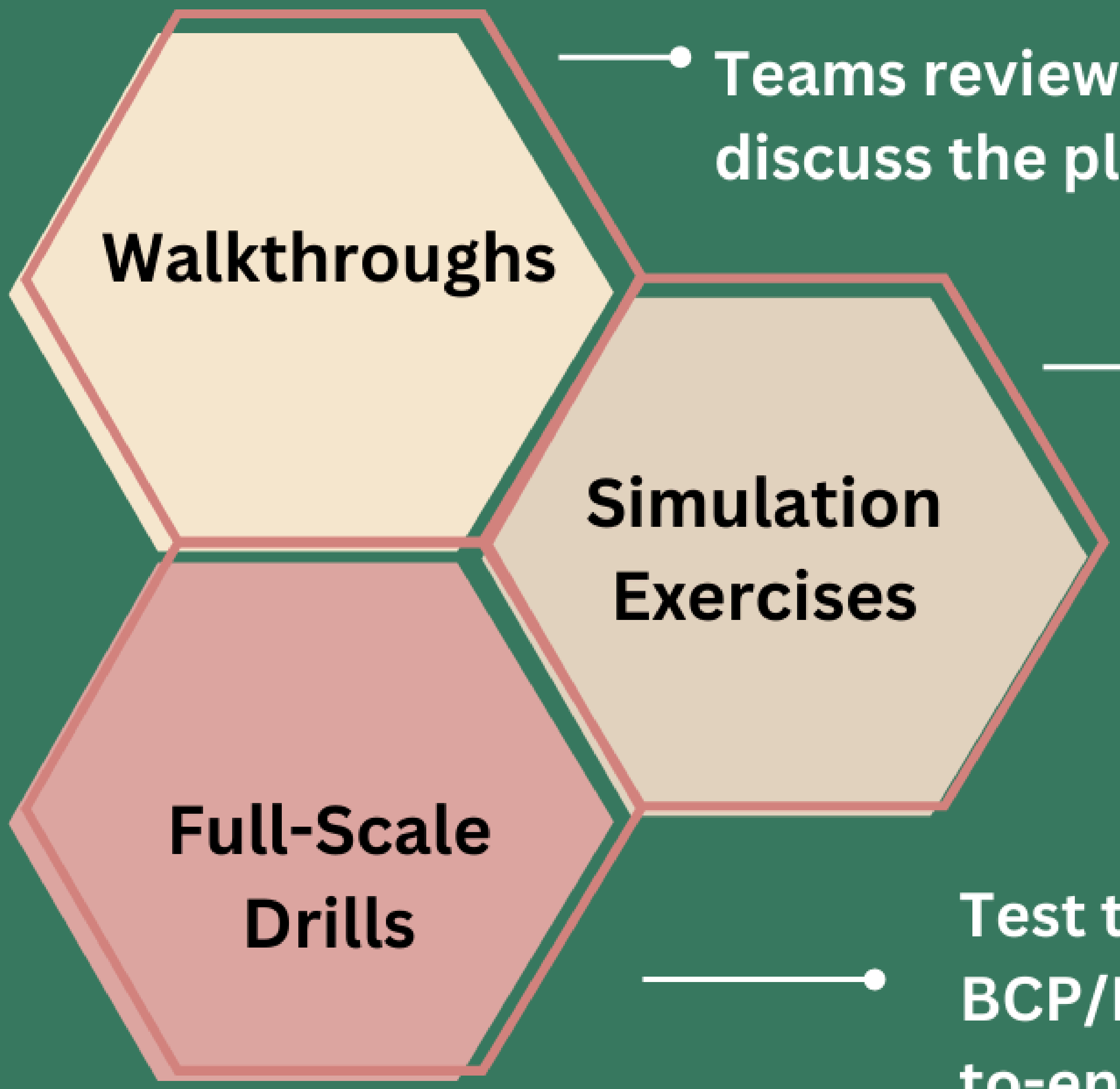
Quick recovery minimized downtime and ensured service continuity, reinforcing the importance of BCP/DRP.

Testing and Maintenance

Why Test?

To identify gaps, ensure the plan’s effectiveness, and confirm team readiness.

TYPES OF TESTS



Walkthroughs — Teams review and discuss the plan.

Simulation Exercises — Specific disaster scenarios are simulated for testing.ings.

Full-Scale Drills — Test the entire BCP/DRP process end-to-end.

Benefits of BCP/DRP

Financial Protection

Reduces losses from downtime.

Customer Trust

Maintains service continuity and confidence.

Regulatory Compliance

Meets industry standards and legal requirements.

Conclusion

Ongoing Commitment

Regular updates and improvements are necessary.

Next Steps

Implement and review your plan to stay prepared.

Importance

BCP/DRP minimizes disruption and ensures quick recovery.

Key Takeaways

Strong planning, testing, and communication are crucial.

Thank You

Guard Your Data with Encryption – Safeguard, Strengthen, and Secure.

Authored by: Khushi Malhotra