Cloud-based BCDR

Dr. Lyron H. Andrews
CISSP/CCSP/SSCP/CRISC/CISM/CCSK

www.linkedin.com/in/drlyronhandrews/

Overview

Understanding BCDR

Establishing BCDR related to business needs

Creating, implementing, and testing BCDR

Understanding BCDR

defines business continuity as “the capability of an organization to continue delivery of products and services within acceptable time frames at predefined capacity relating to a disruption.”

ISO/DIS 22301:2019

defines disaster recovery as the “ability of the information and communication technology (ICT) elements of an organization to support its critical business functions to an acceptable level within a predetermined period of time following a disruption.”

ISO/IEC 27031:2011

BCDR Elements

Organizational mission

Protect value

Roles and activities

Business Continuity Framework - Leadership

Policy and objectives aligned with strategy

Ensure resources for BCMS success

Ensure BCMS achieves intended outcomes

Direct and support personnel to achieve purpose

Promote continual improvement

Business Continuity Framework - BIA

Defines impact categories and criteria

Determines maximum tolerable period of disruption (MTPD)

- Recovery time objective (RTO)
- Recovery point objective (RPO)

Business Continuity Framework – Legal

Understand legal and regulatory issues

Implementable process for tracking

Document and keep updated

Business Continuity Framework – Awareness

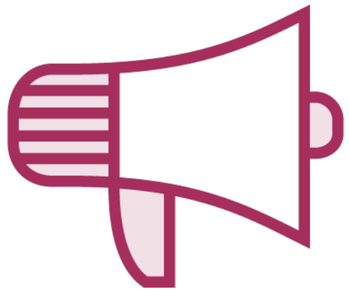
Roles and responsibilities for implementing

Following BCMS plan

Implications of not following the plan

Benefits of improved business function

Business Continuity Framework – Communication



Internal/external communication

Answer questions of what, when, how, who

Recovery site locations

Business Continuity Framework – Create/Update

Plan shared based on a need-to-know

Confidentiality of plan maintained

Storage, preservation, change control, retention

Business Continuity Framework – Resources

People

Transportation

Data

Infrastructure

Finance

Alternative location

Business Continuity Framework – Response

Assessment of disruption

Activation process

Establish prioritization

Monitor effectiveness

Creating a Business Established BCDR Strategy

Business Impact Analysis

MTPD

maximum tolerable period of disruption

RTO

Recovery time objective

RPO

Recovery point objective

Questions for BCDR Strategy

What is the required recovery point objective (RPO)?

What is the required recovery time objective (RTO)?

What kinds of “disasters” are included in the analysis?

Does that include provider failure?

Cloud-based BCDR Options

On-premises, cloud as BCDR

Cloud consumer, primary provider BCDR

Cloud consumer, alternative provider BCDR

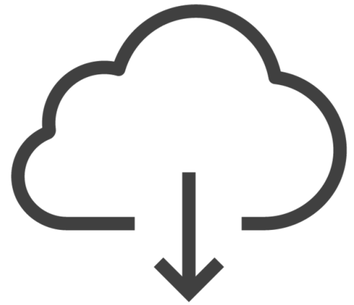
On-premises, Cloud as BCDR

Backup to cloud

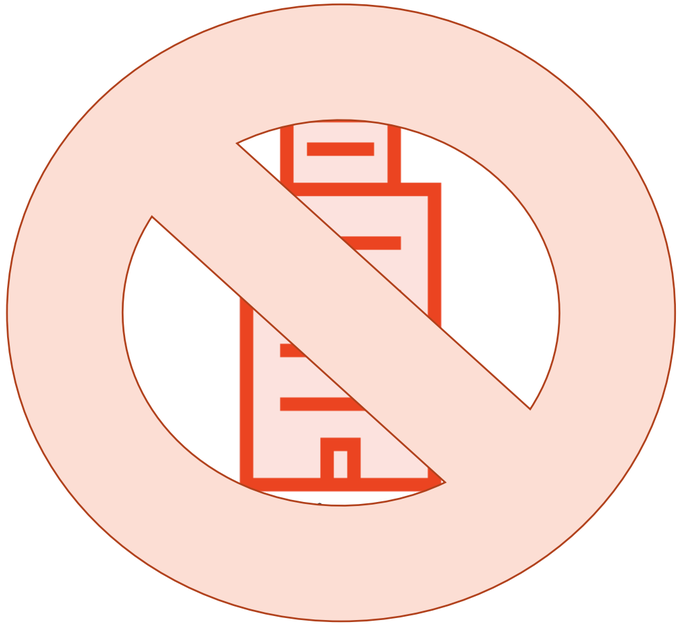
Primary site data center

On-premises, Cloud as BCDR

Backup to cloud

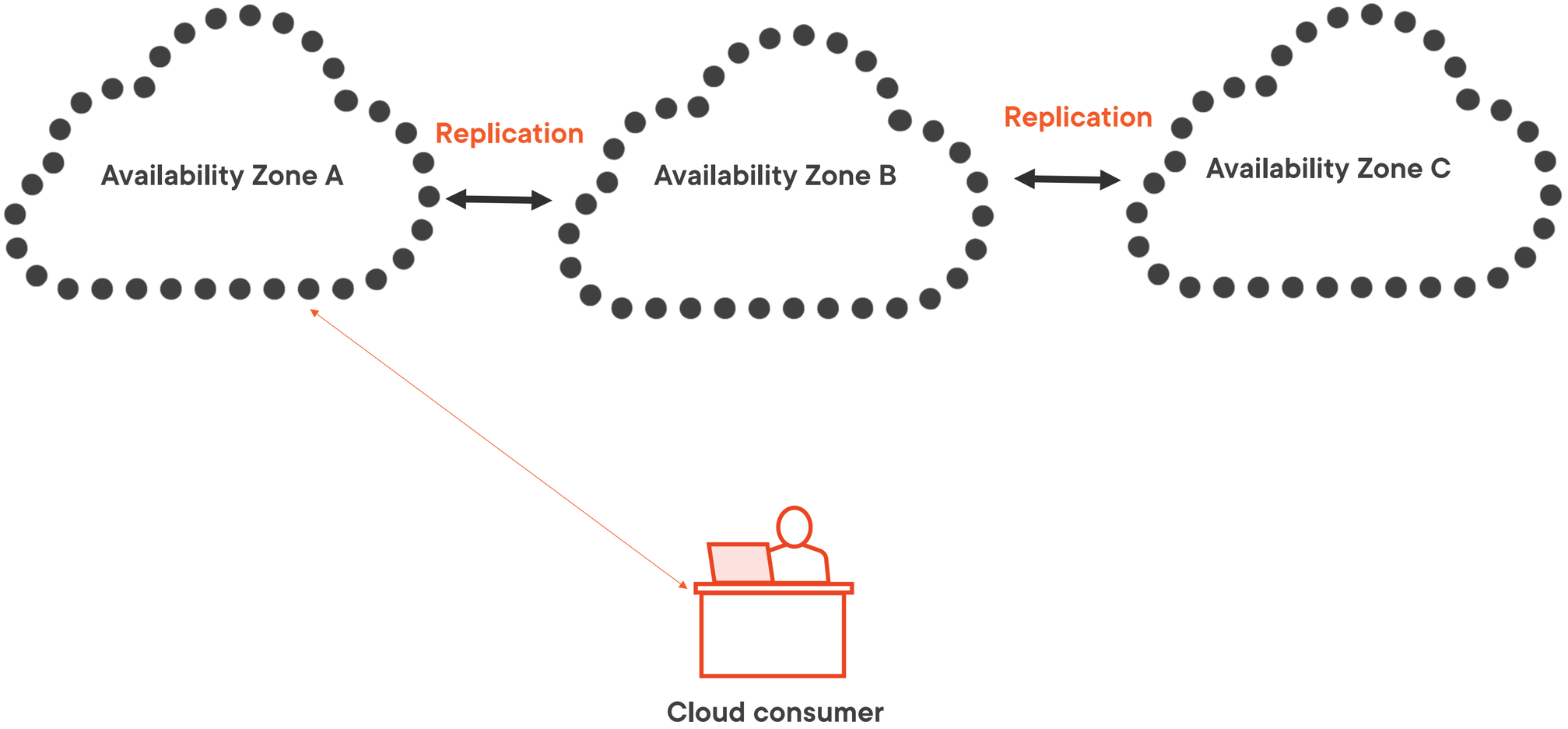


Recovery from cloud

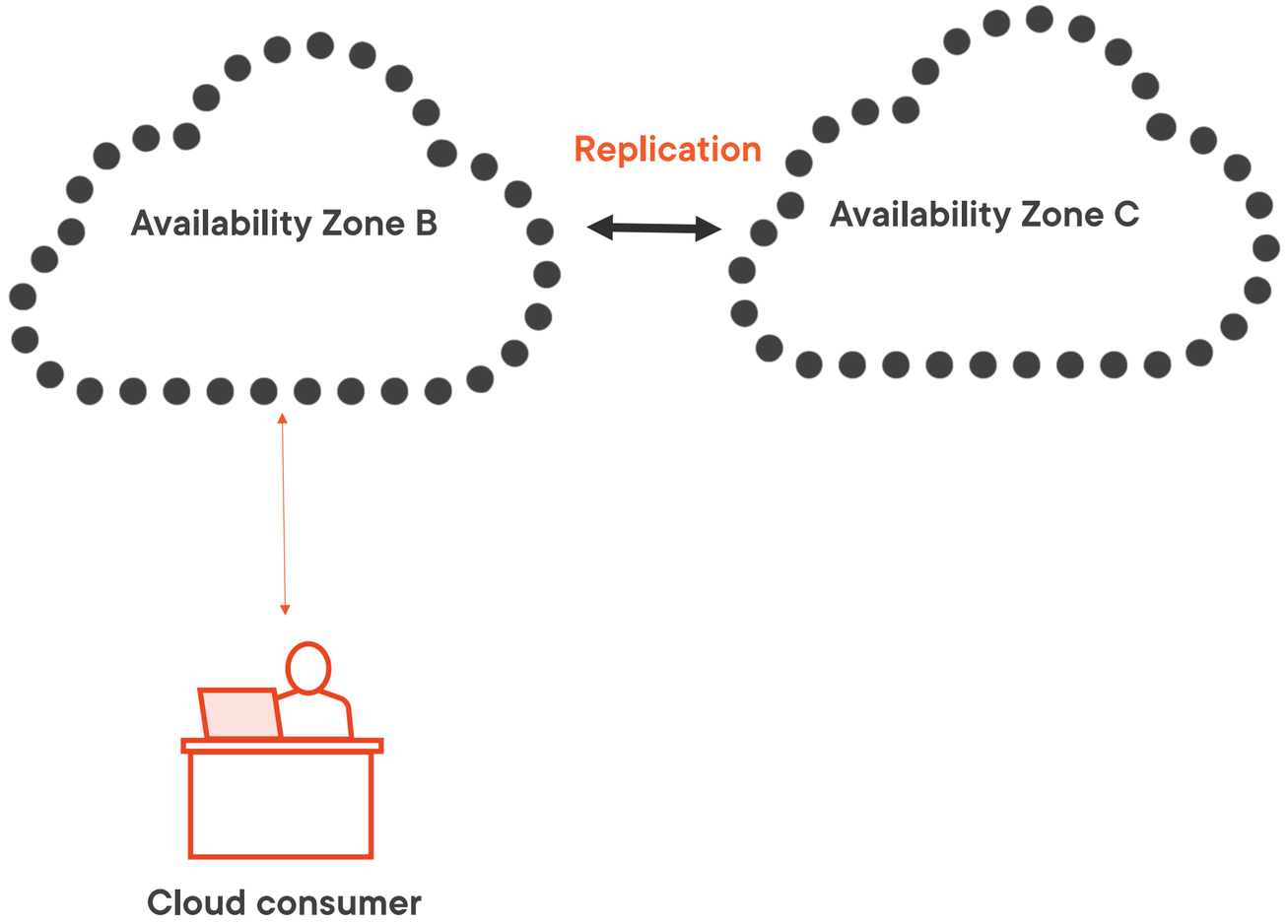


Alternate site data center

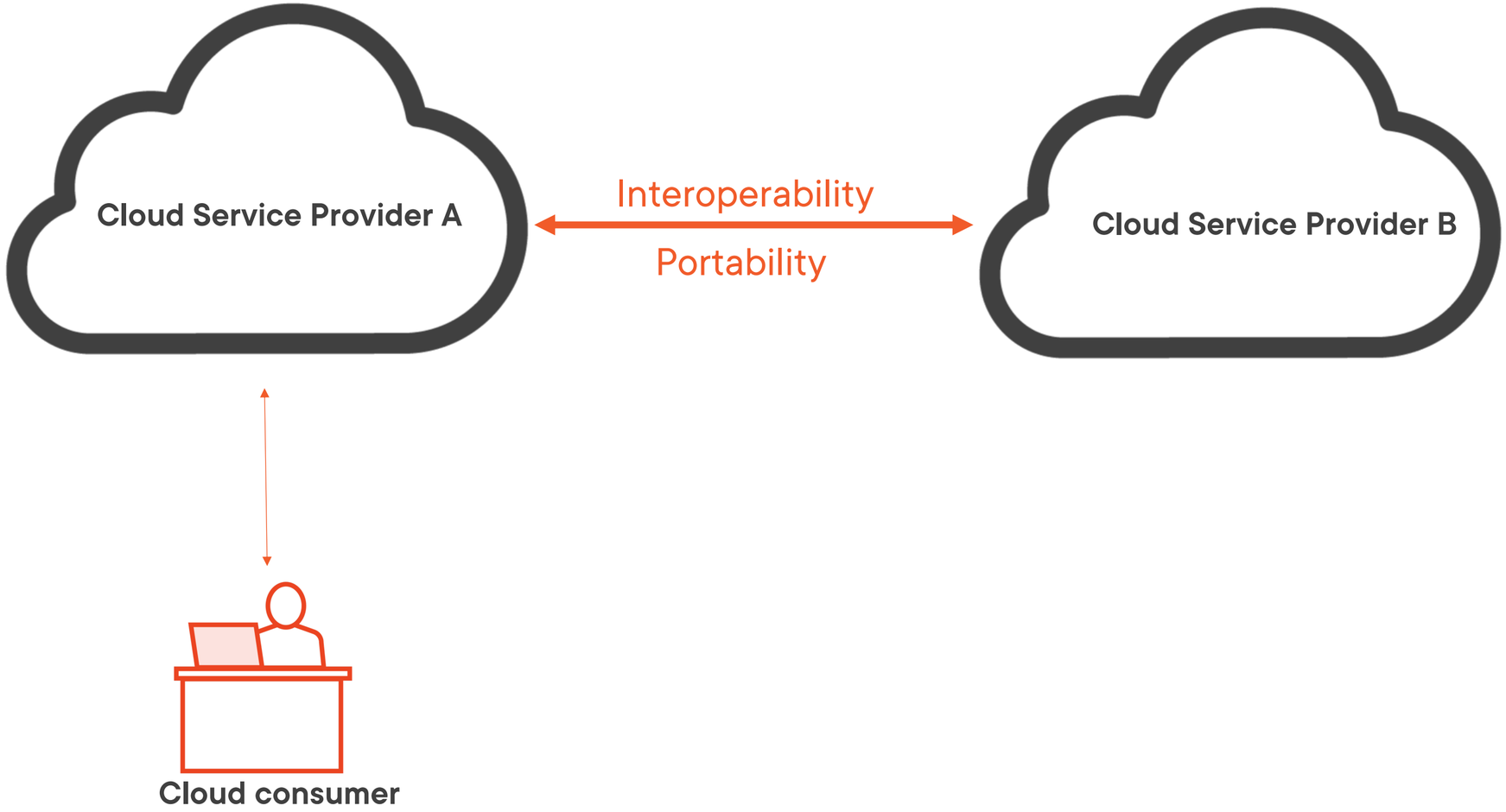
Cloud Consumer, Primary Provider BCDR



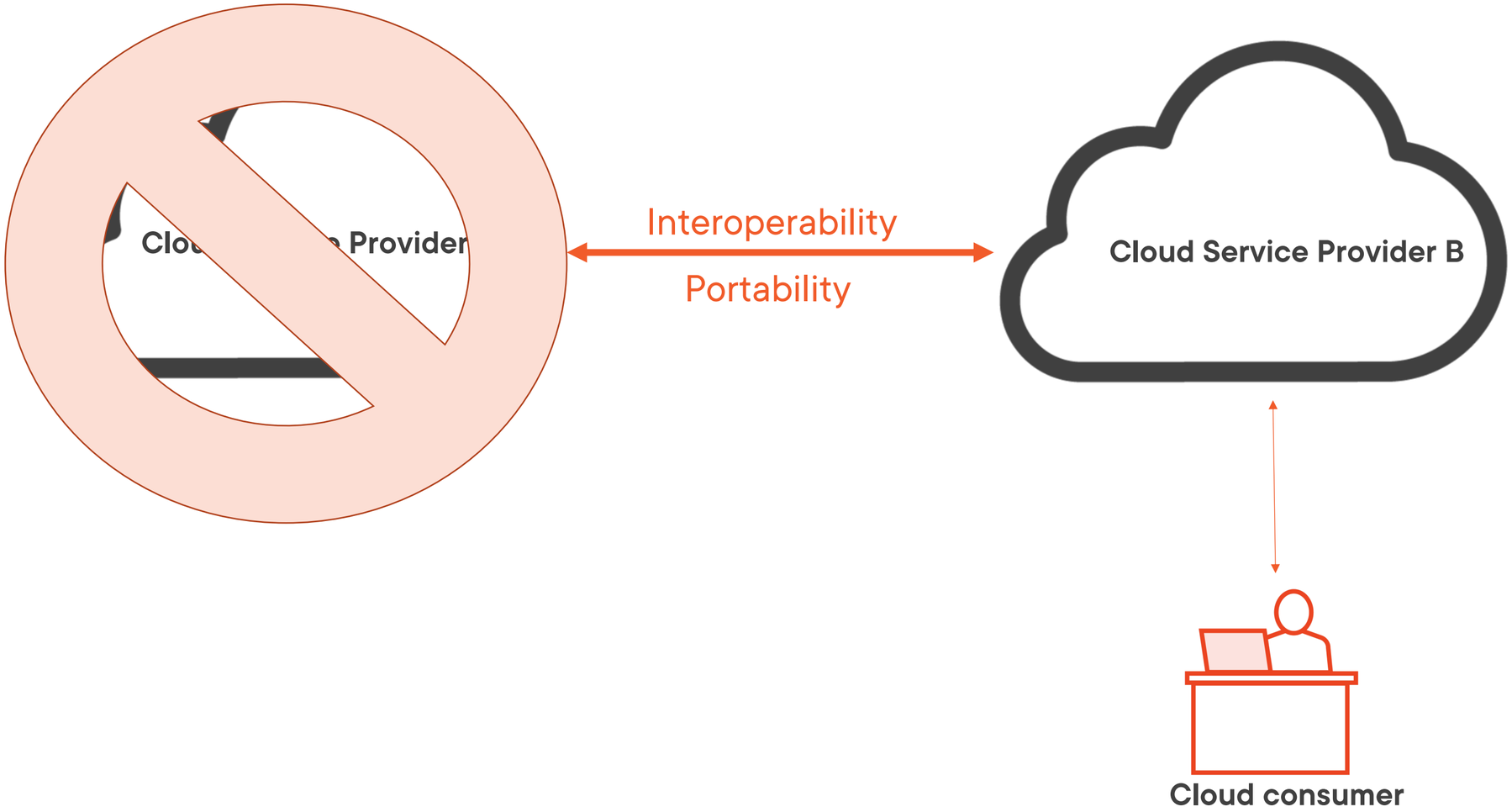
Cloud Consumer, Primary Provider BCDR



Cloud Consumer, Alternative Provider BCDR



Cloud Consumer, Alternative Provider BCDR



Primary BCDR Activities

Recovery

Restoration

Recovery Activities

Prevention

Detection

Response

Recovery

Improvement

Restoration Activities

Original location

New normal

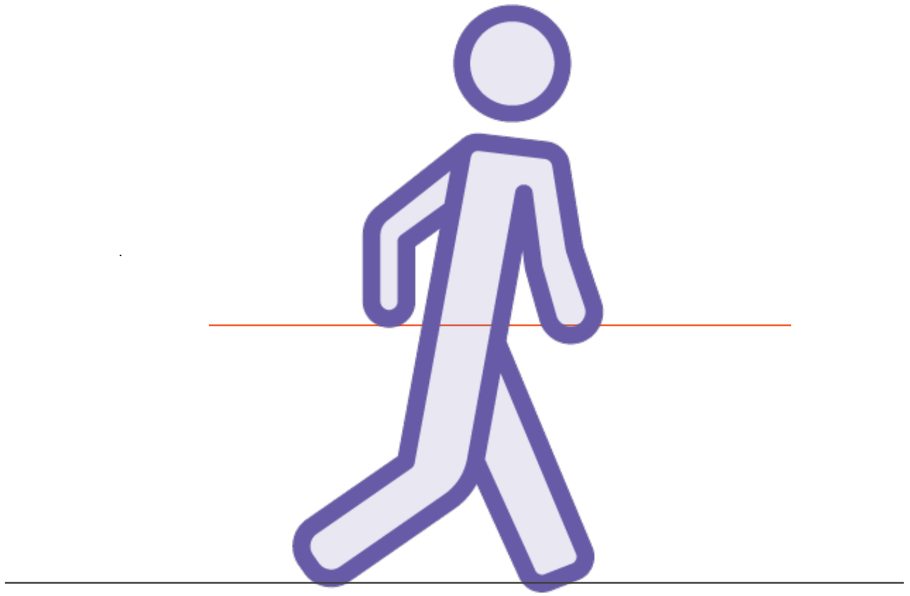
Reverse order

In concert with recovery

Contain costs/risks

Creating, Implementing, and Testing BCDR

BCDR Plan Participation



Implementers should assist in developing plan

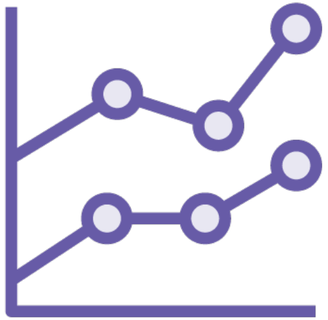
Project planning and risk management should be applied

Plan has little value without testing

Requirements Gathering and Context

Critical business functions

Threats to resources



Business driven

Plan Risk Assessment

- Cloud provider elasticity
- New providers address existing concerns
- Provider bandwidth to handle replication
- Provider bandwidth to BCDR location
- Legal issues to prevent or delay recovery

Plan Design, Creation, and Implementation

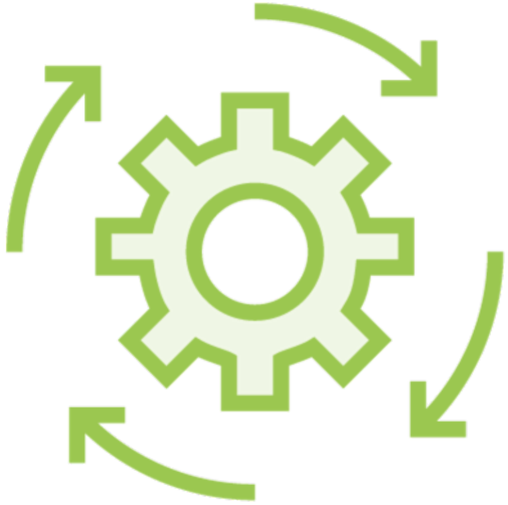
Evaluate candidate architecture

Implementation affects primary and backup locations

Ongoing updates to DR platform necessary

DR Plan Tests

Desktop review



Recovery simulation

Operational

The Ultimate Test: Chaos Engineering

Impose VM failure

Impose availability zone failure

Data portability and interoperability

Summary

Create, review, refine BCDR

Need to meet MTPD, RTO, and RPO

Make tests as realistic as possible