

BCDR Plan and Activities



Dr. Lyron H. Andrews

Cybersecurity Advisor - CISSP/CCSP/SSCP/CRISC/CISM/CCSK

<https://www.linkedin.com/in/drlyronhandrews/>



Overview



Understand the role of business continuity management in organization resiliency

Define the stages of business continuity planning

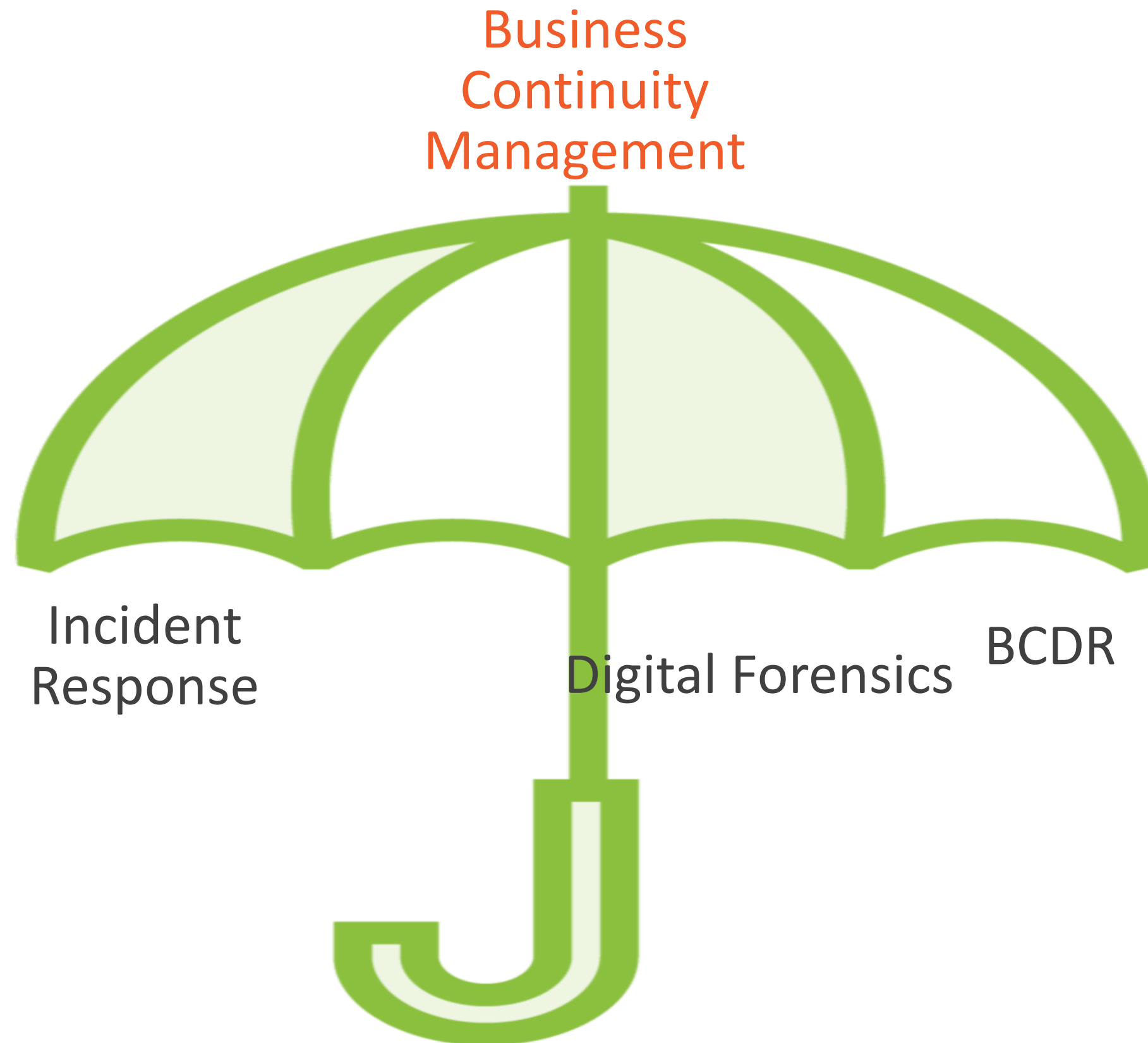
Review the technologies and strategies associated with disaster recovery



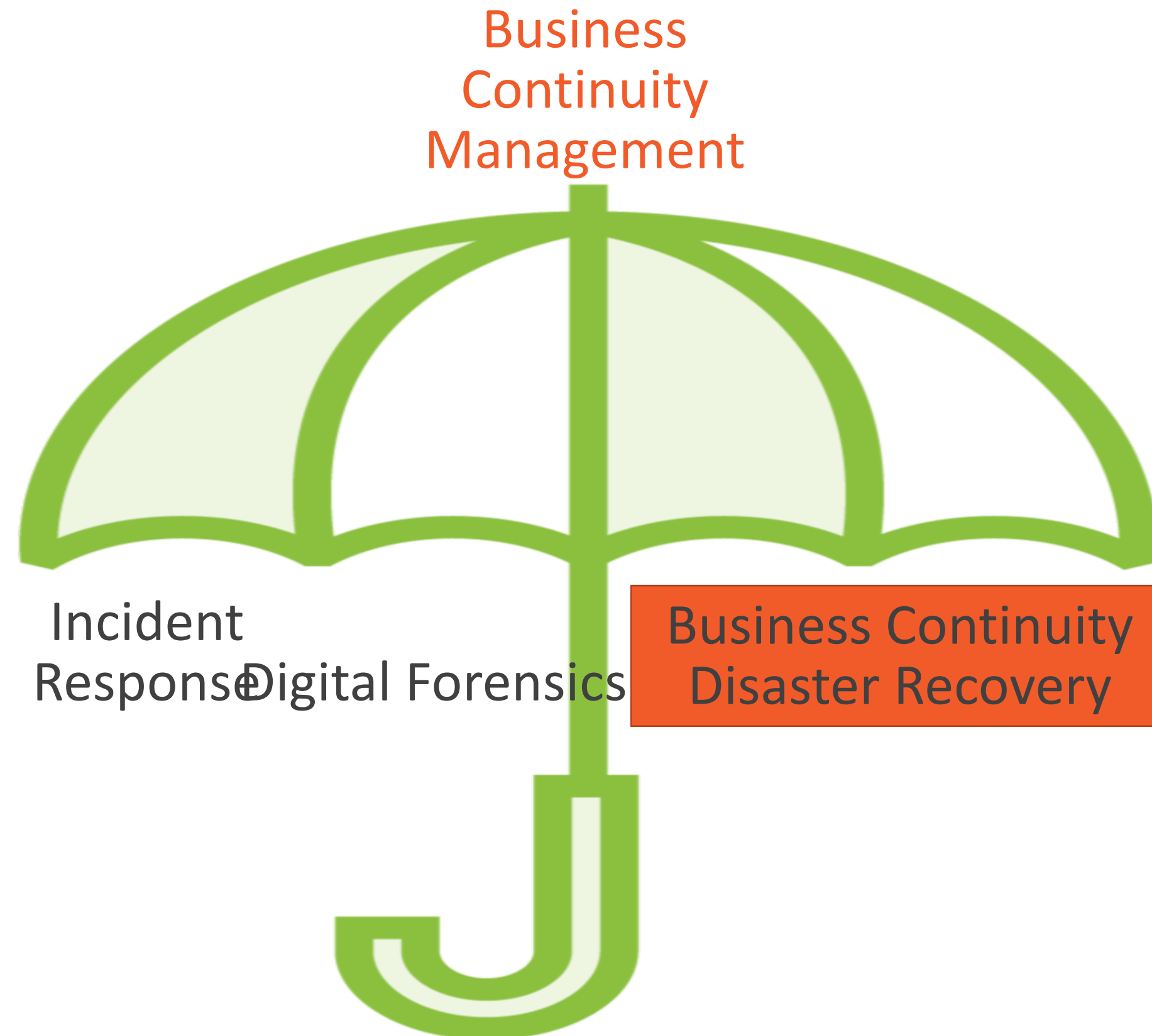
Business Continuity and Disaster Recovery



BCM as Parent of Various Activities



BCM as Parent of Various Activities



“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 describing business continuity.

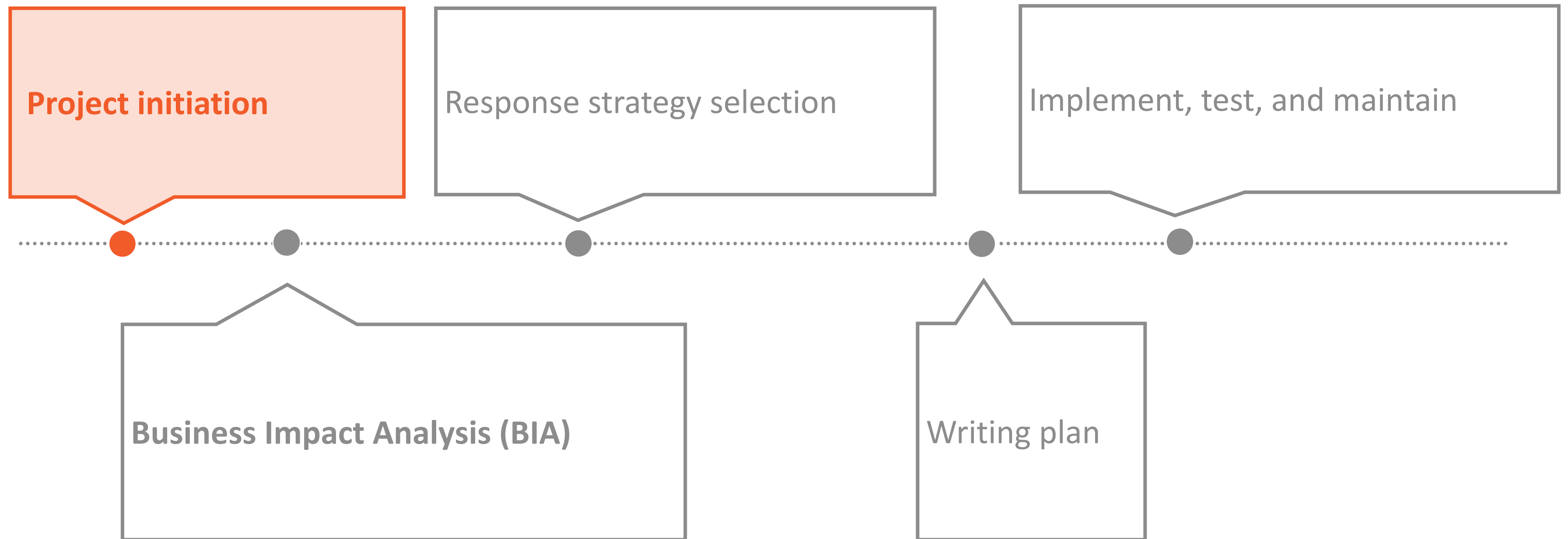


“The ability of the information and communication technology (ICT) elements of an organization to support its critical business functions to an acceptable level within a predetermined period of time following a disruption.”

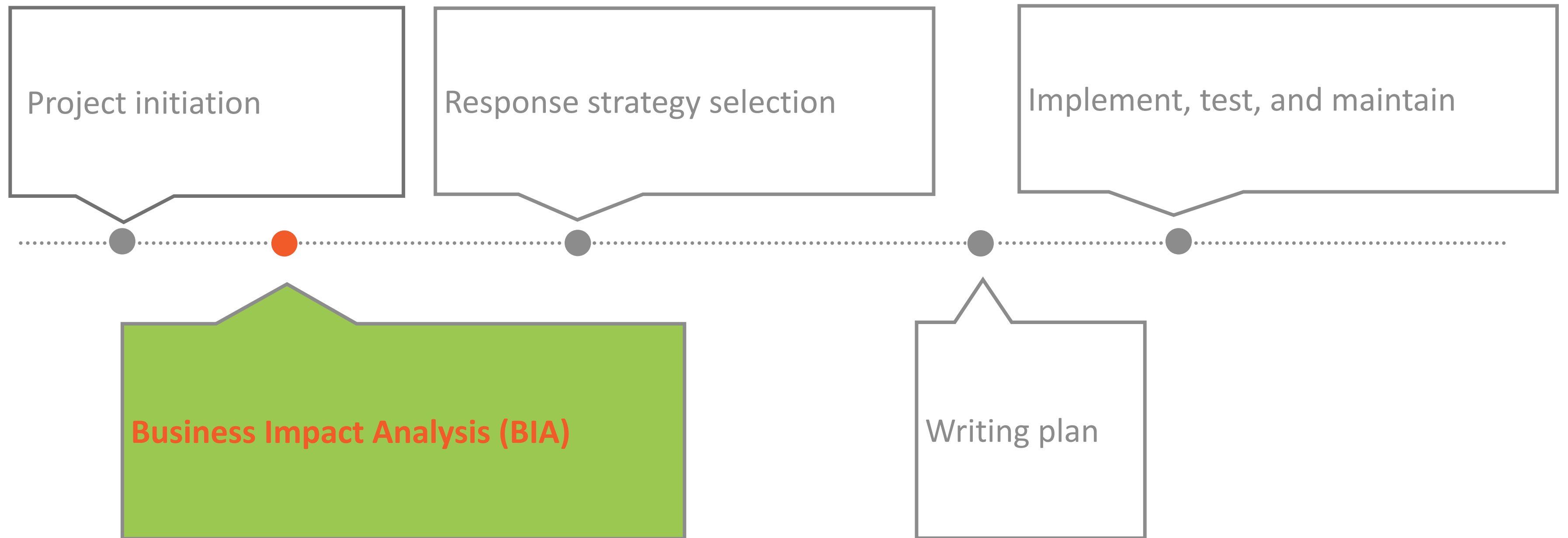
ISO/IEC 27031:2011 describing disaster recovery.



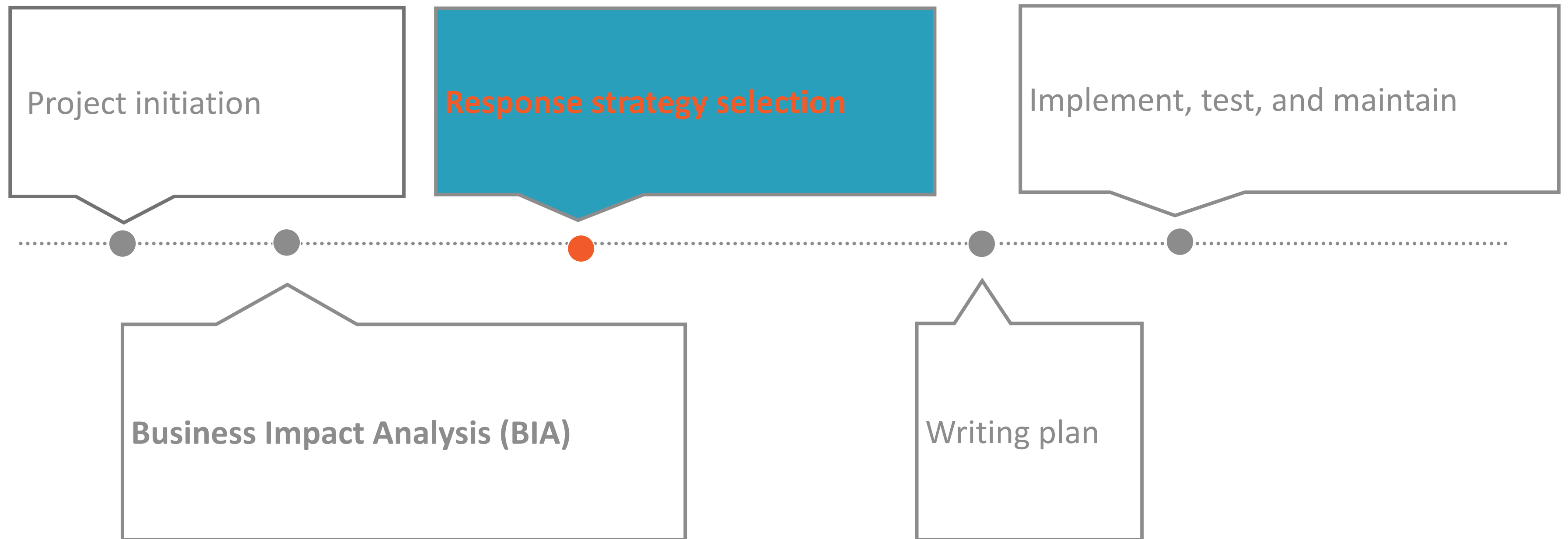
Business Continuity Plan Phases



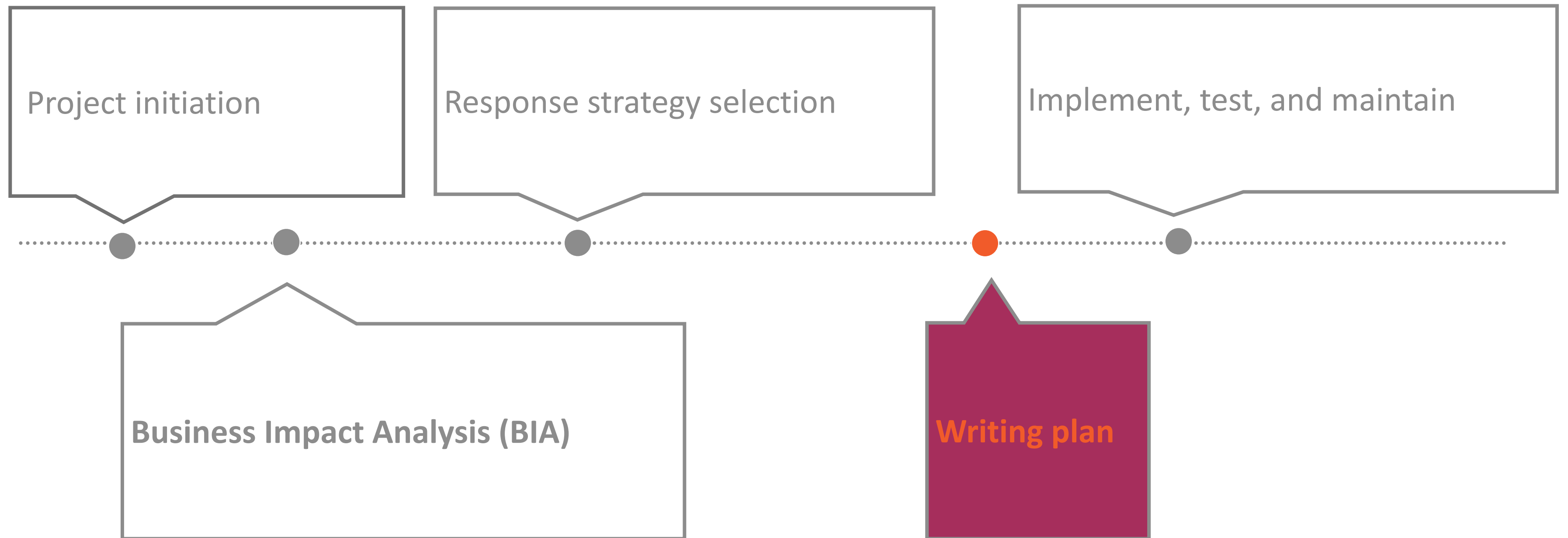
Business Continuity Plan Phases



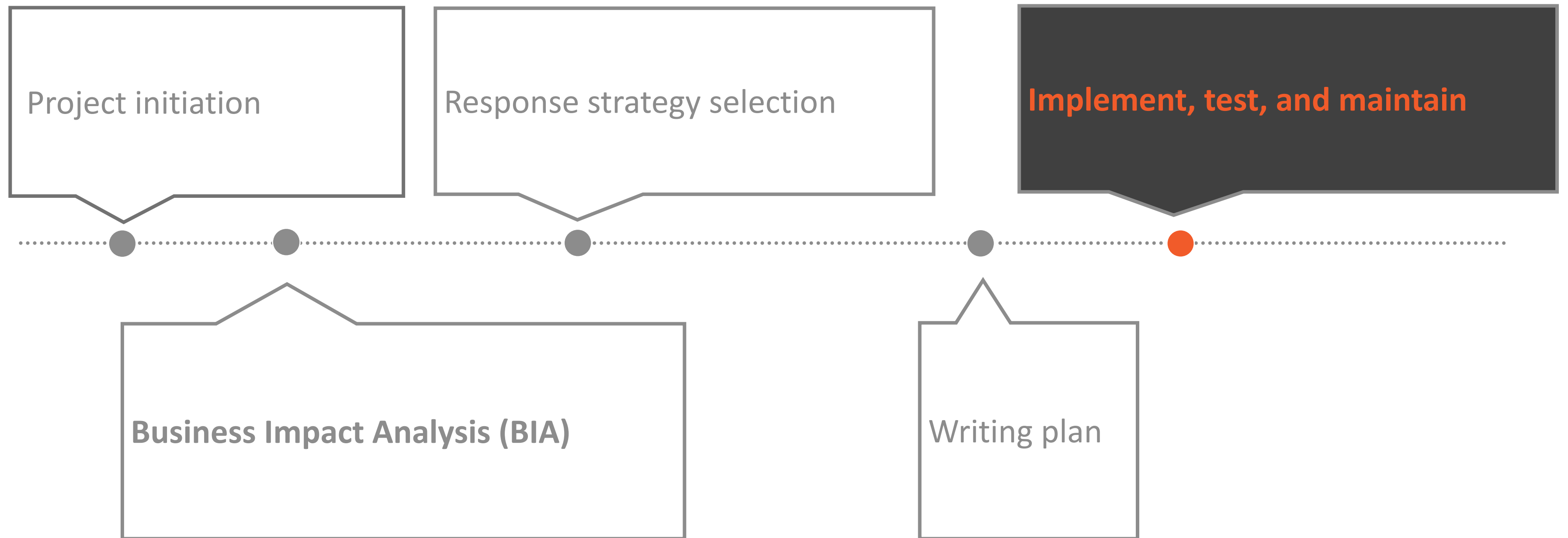
Business Continuity Plan Phases



Business Continuity Plan Phases



Business Continuity Plan Phases



BCP- Project Initiation and BIA



Project Initiation

Planning Includes

- Project scope
- Resources
- Timelines
- Deliverables
- Authority



BIA analyzes what critical elements of the business that given an outage would create a critical impact



Primary and secondary

Integral for success

Service value chains

Each function identified

Criticality level assigned

Key Concepts of Criticality



Two Types of Risk Analysis



Qualitative

Subjective likelihood consideration of risk and the non-numeric impact

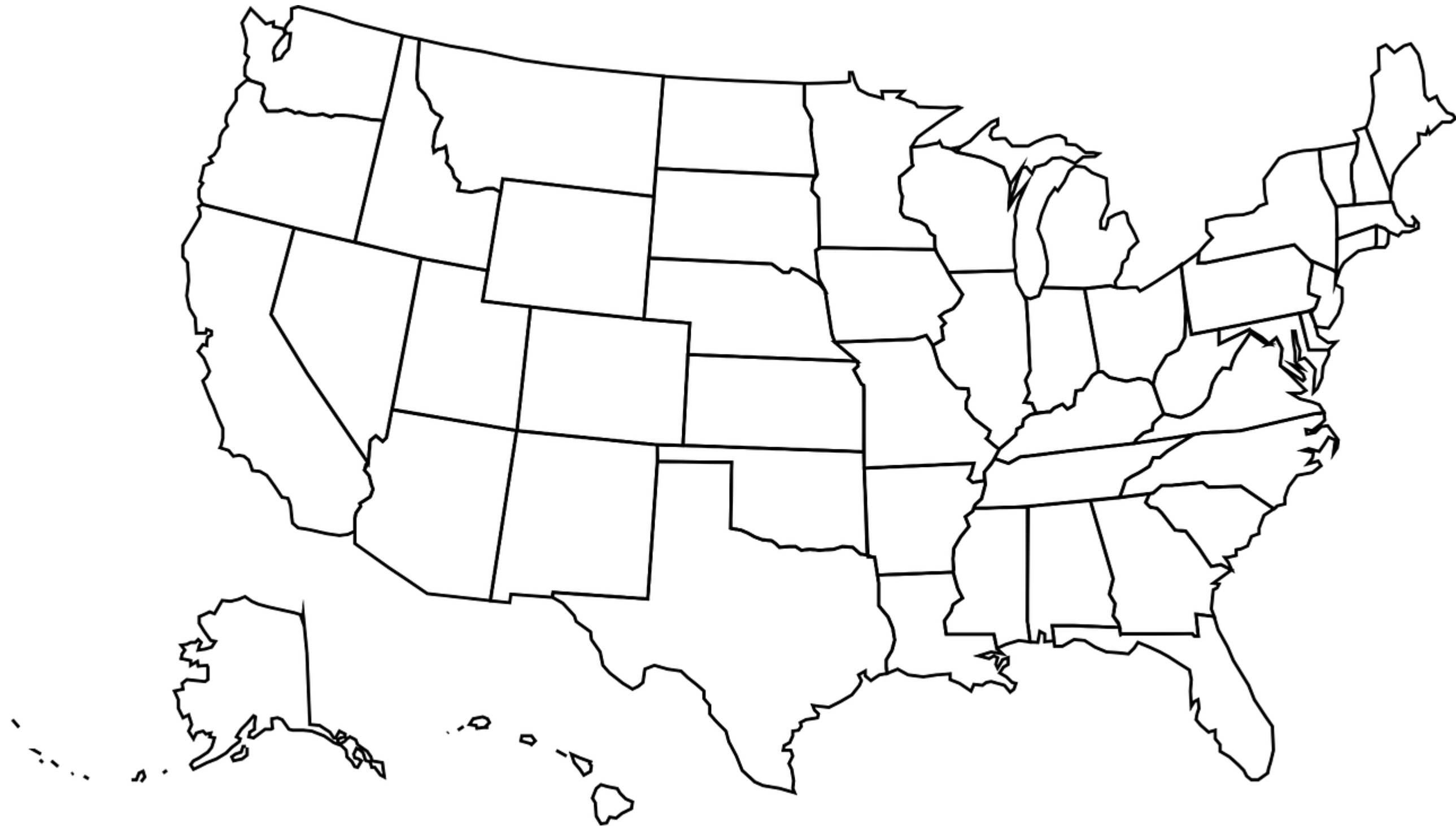


Quantitative

Objective empirical consideration of risk and corresponding cost if realized

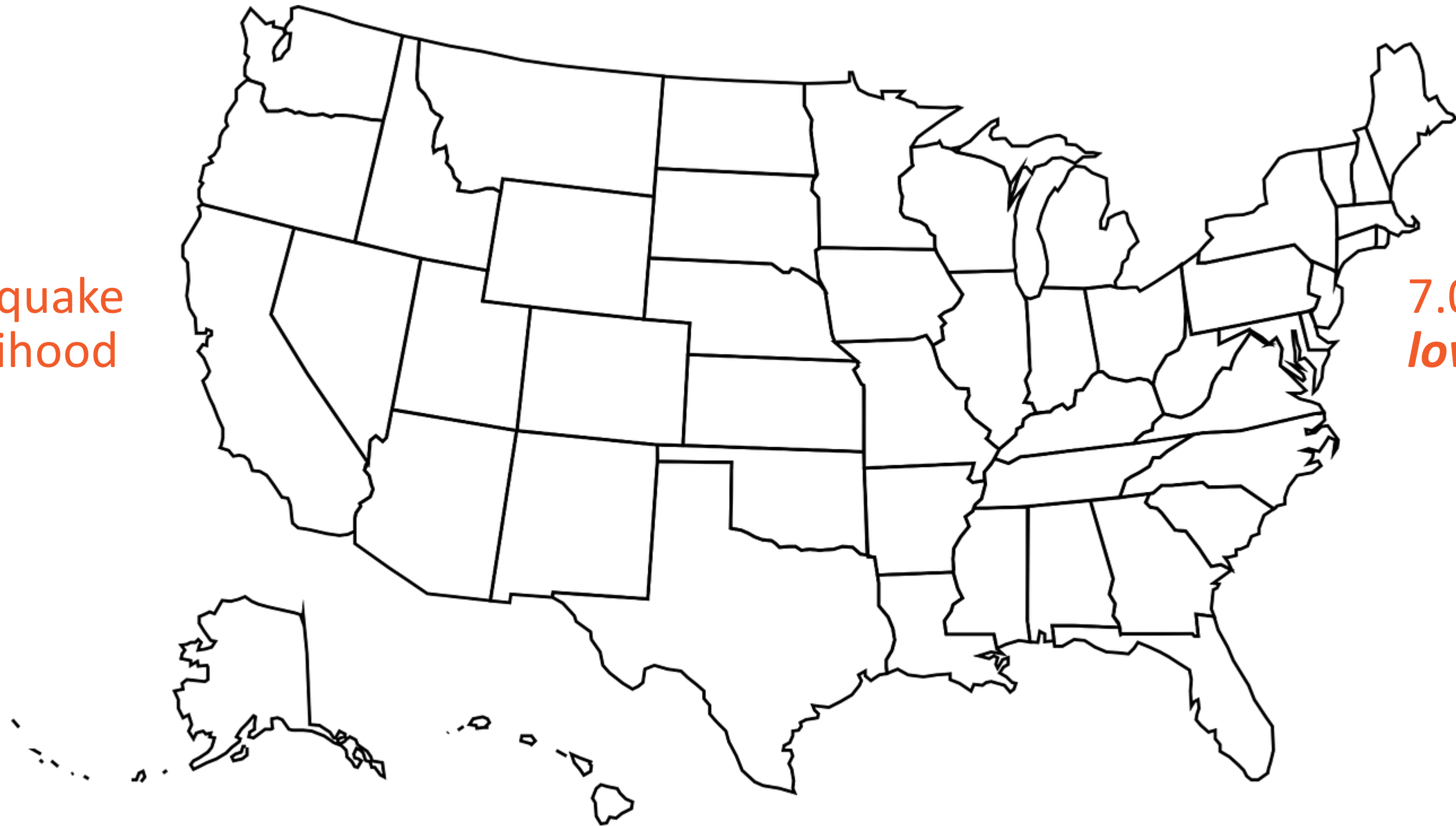
Likelihood and Impact

7.0 earthquake



Likelihood and Impact

7.0 earthquake
high likelihood



7.0 earthquake
low likelihood



Likelihood and Impact

7.0 earthquake
high likelihood

Next focus on impact



Three Elements of Business Survival

MTD

Pre-determined period of allowable outage

RTO

Time taken to recover ICT systems

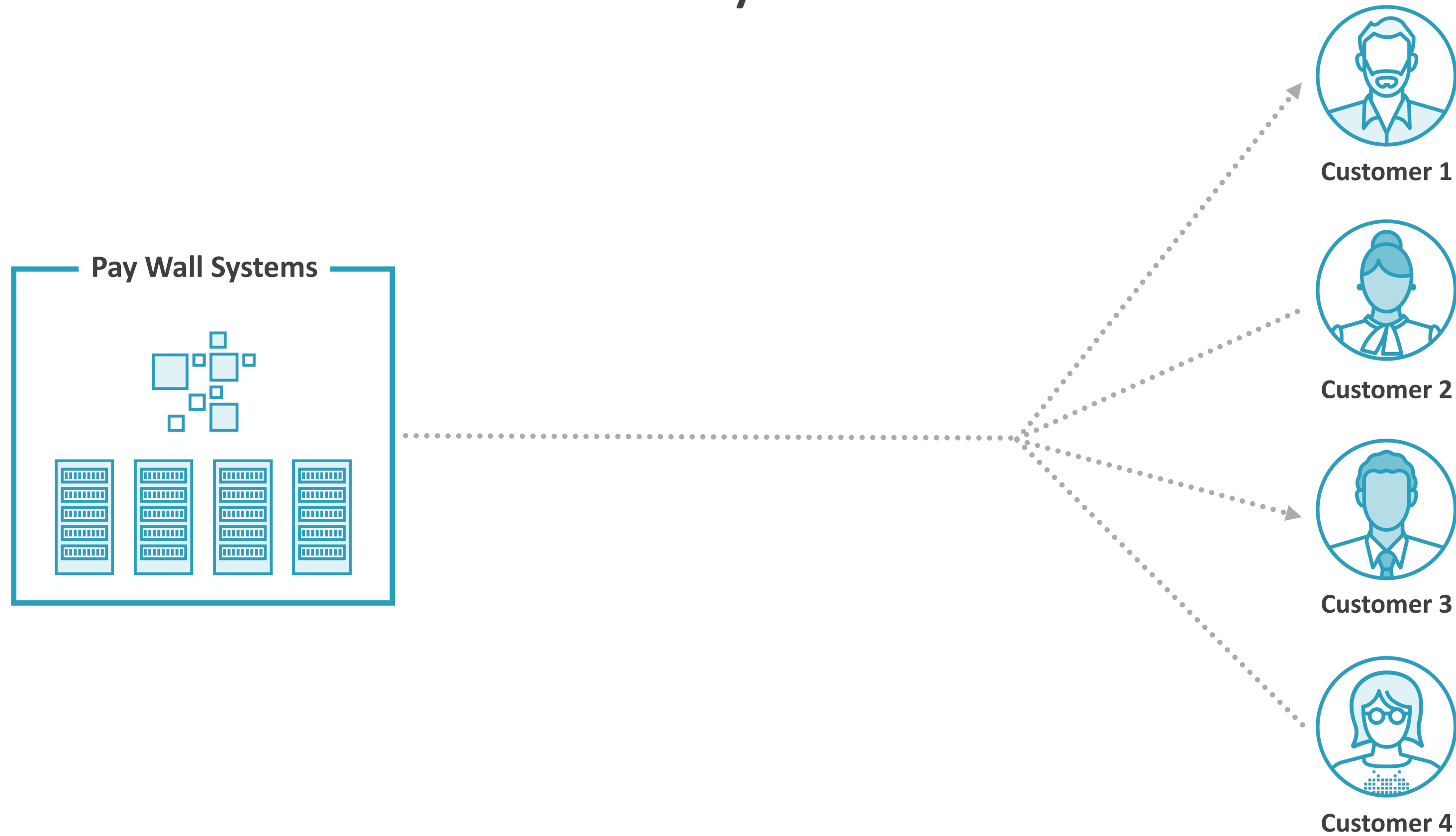
RPO

The amount of allowable data loss

RTO less than MTD – all elements business driven

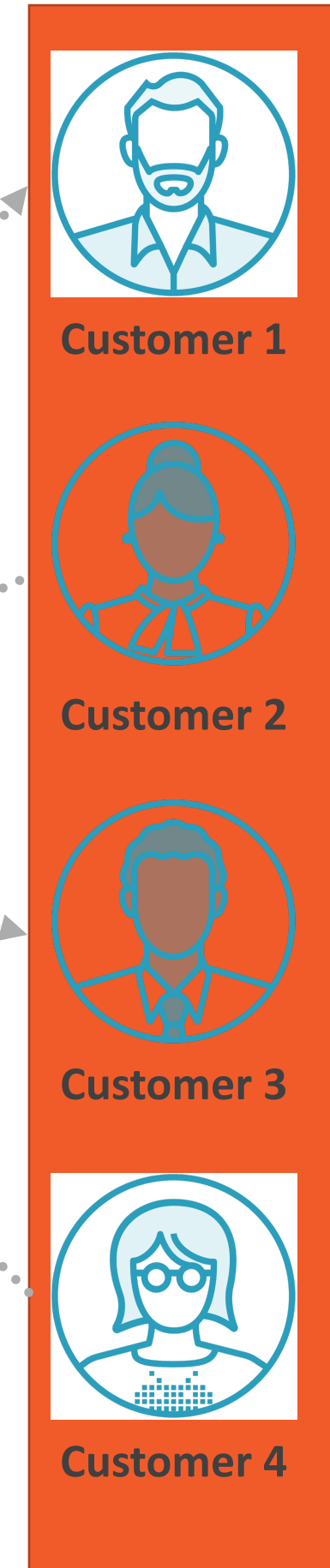
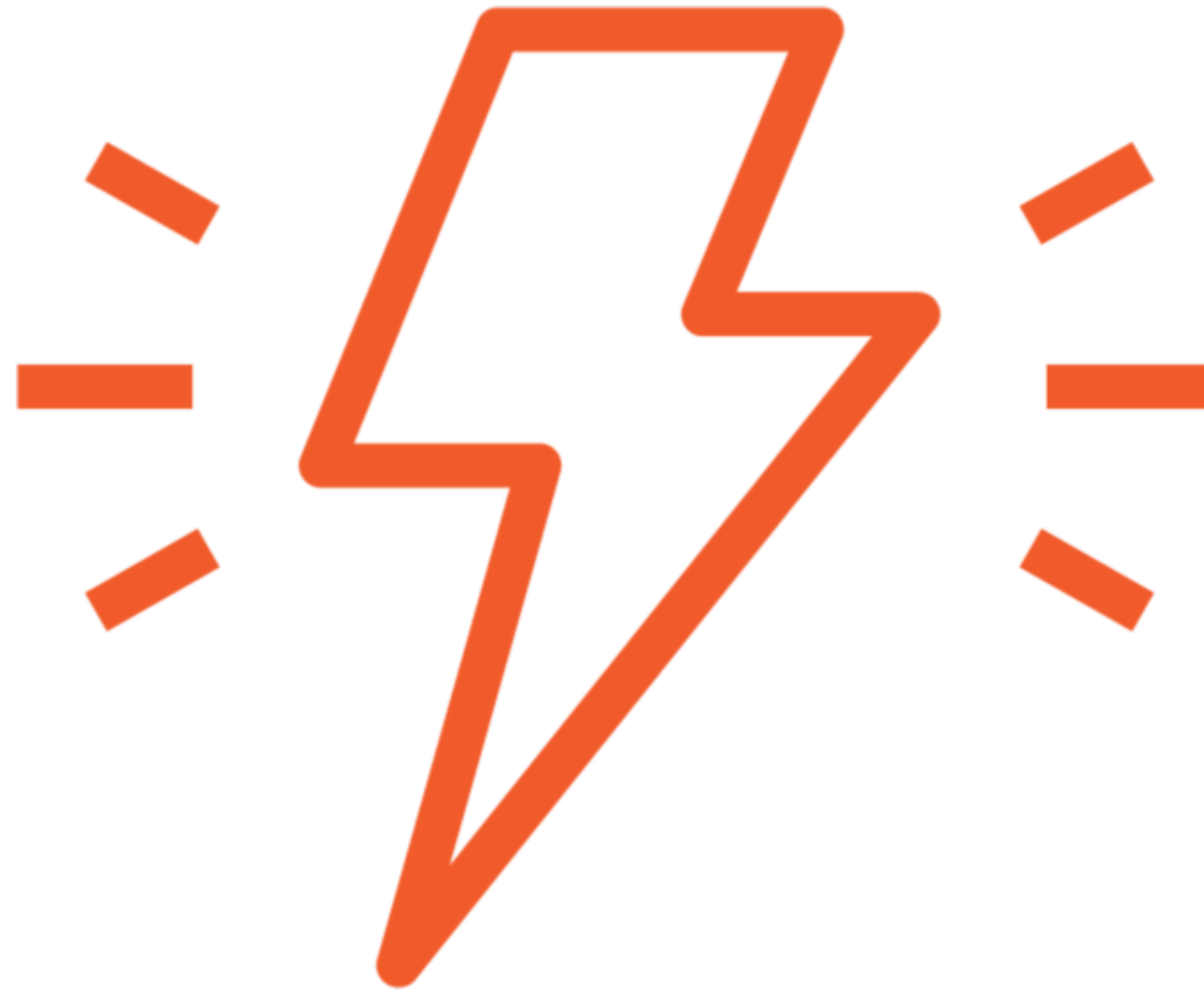
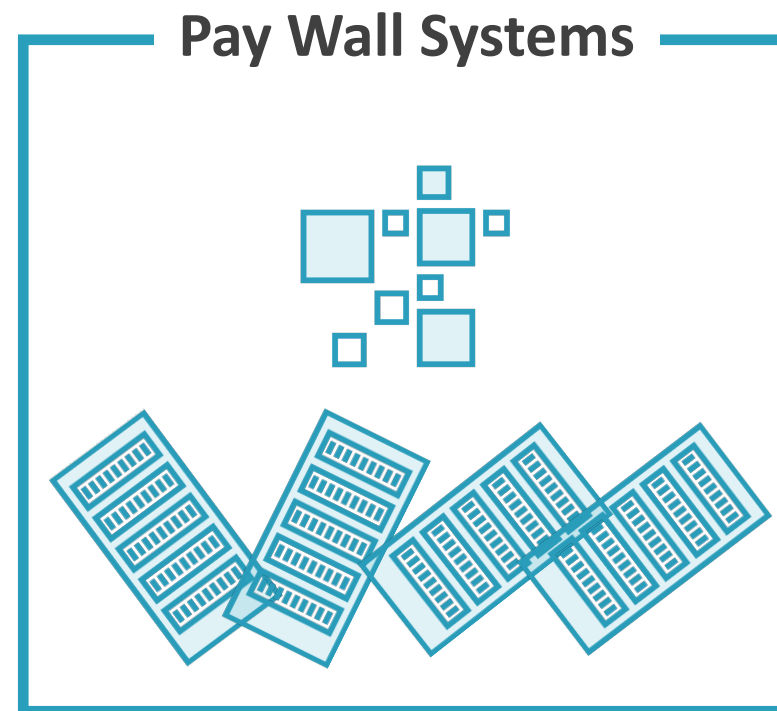


Recovery Scenario

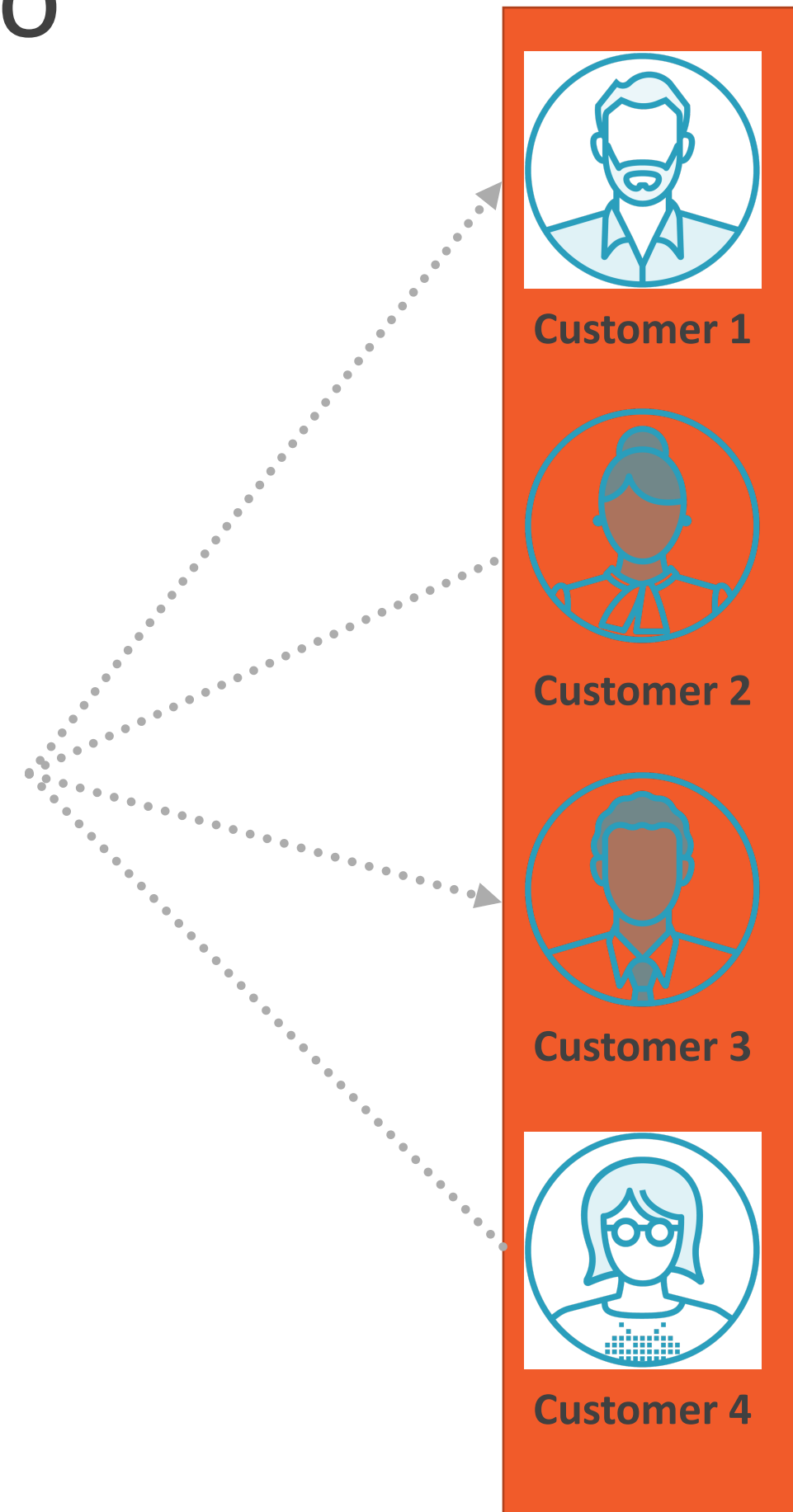
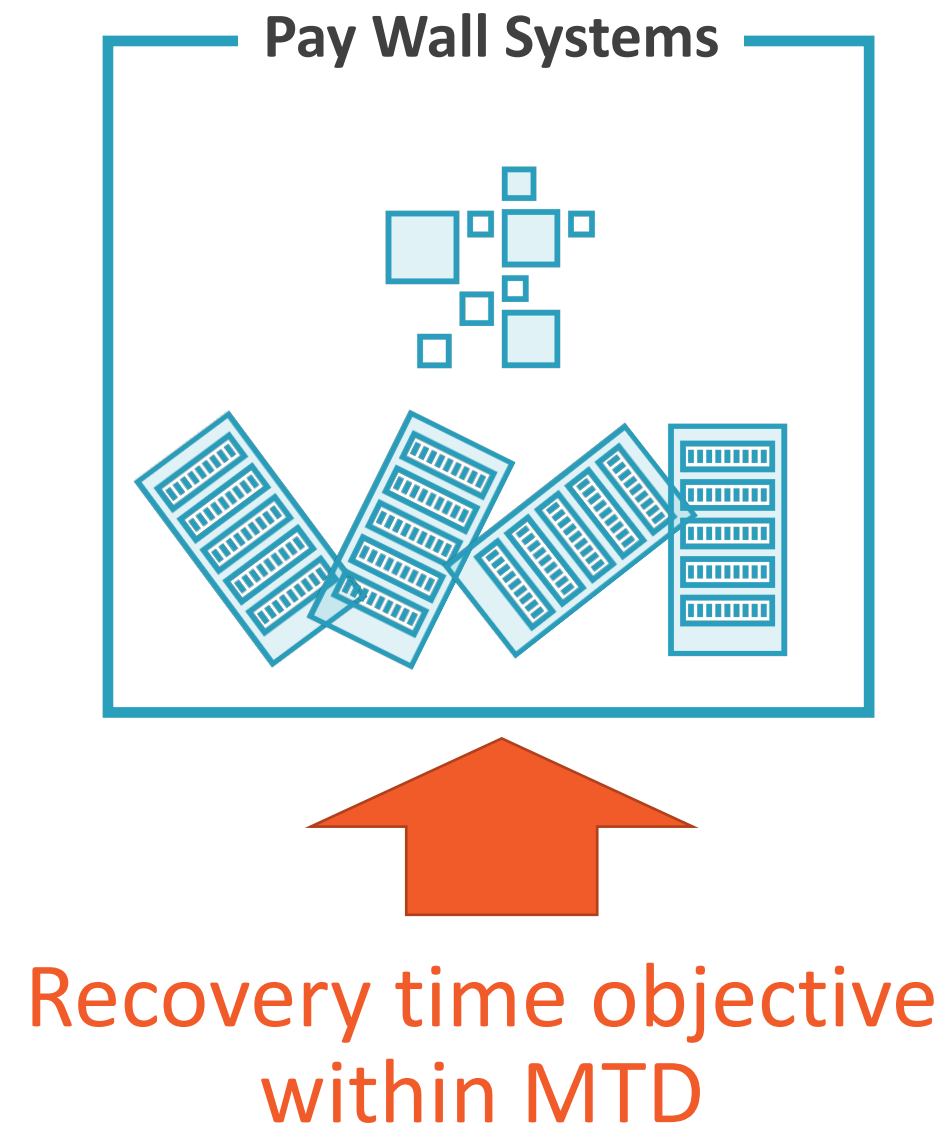


Recovery Scenario

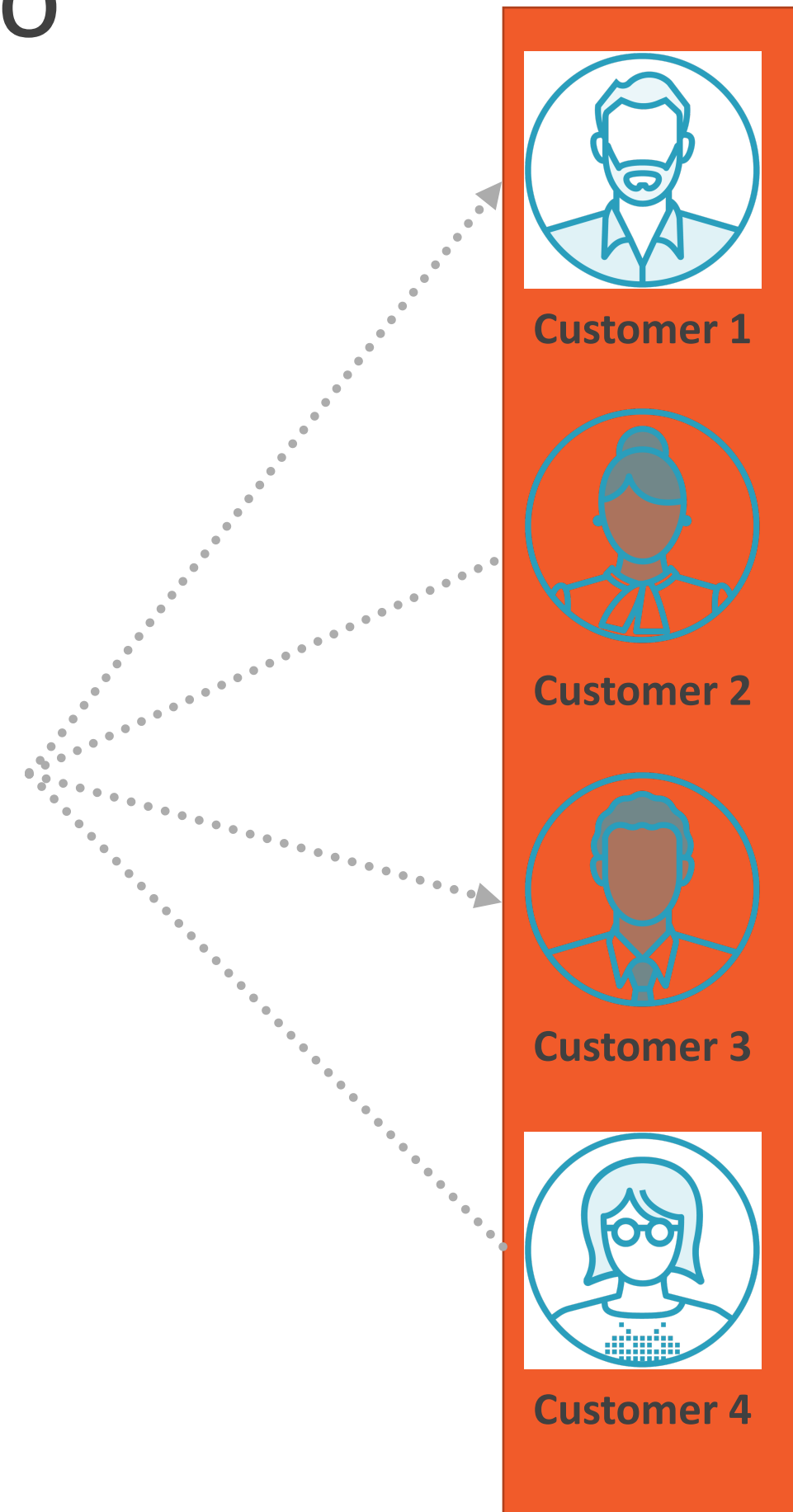
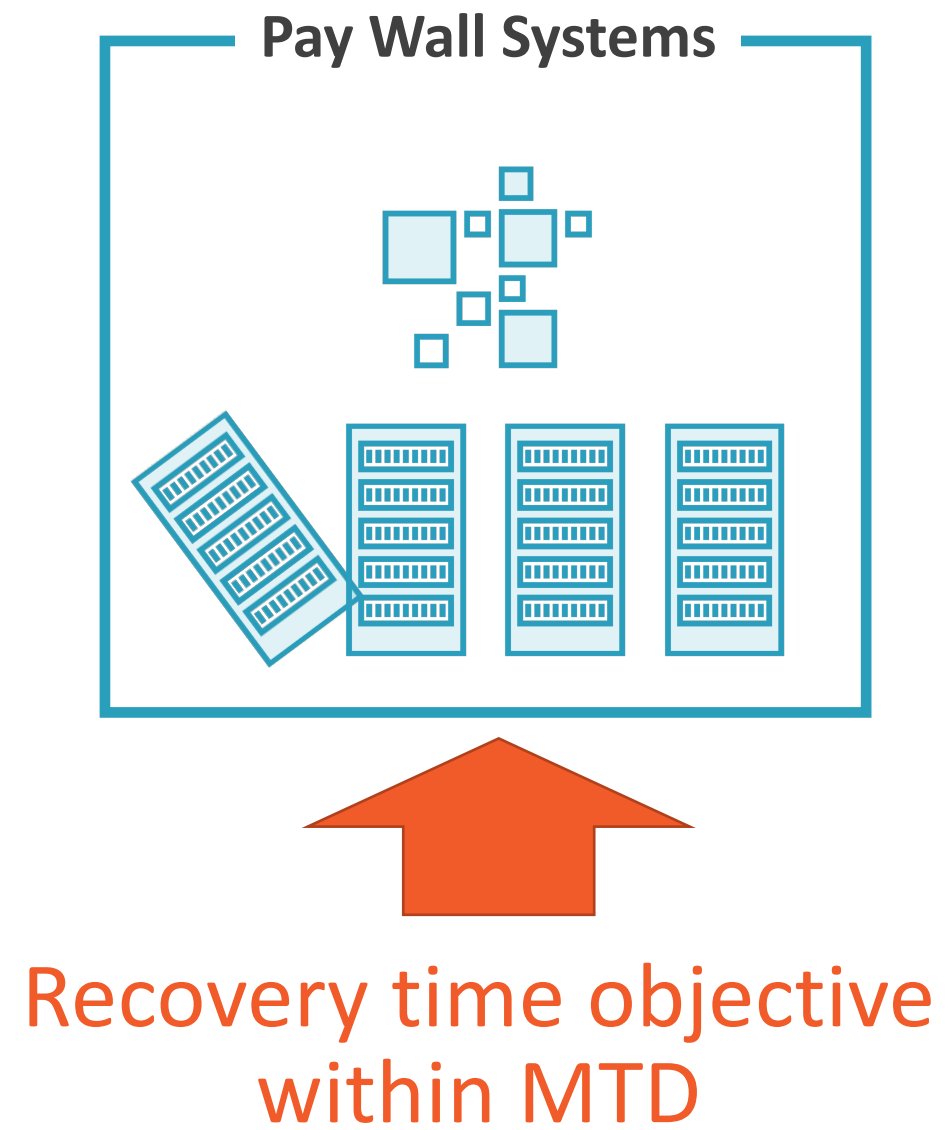
Maximum tolerable
downtime (MTD) clock
begins



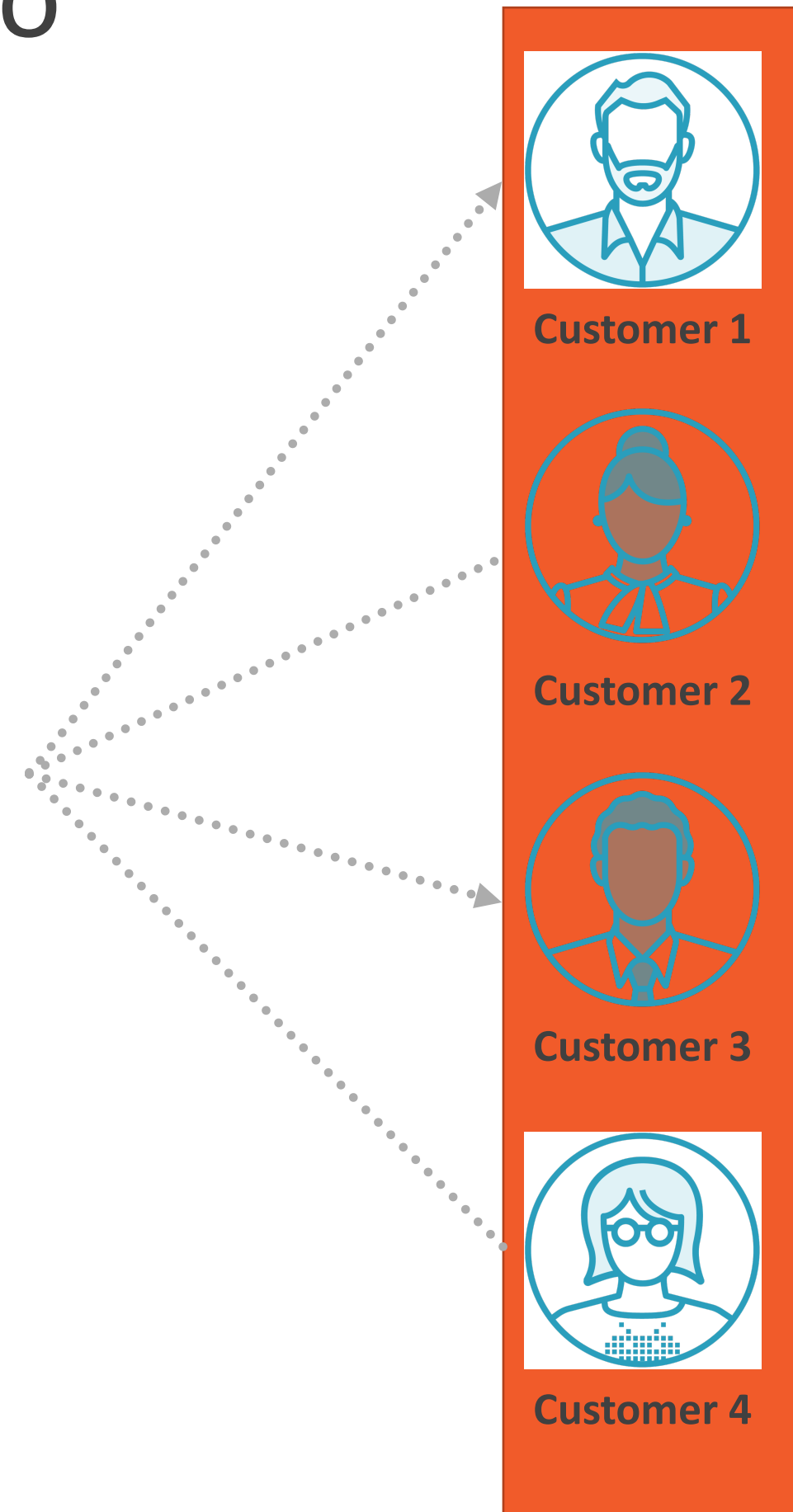
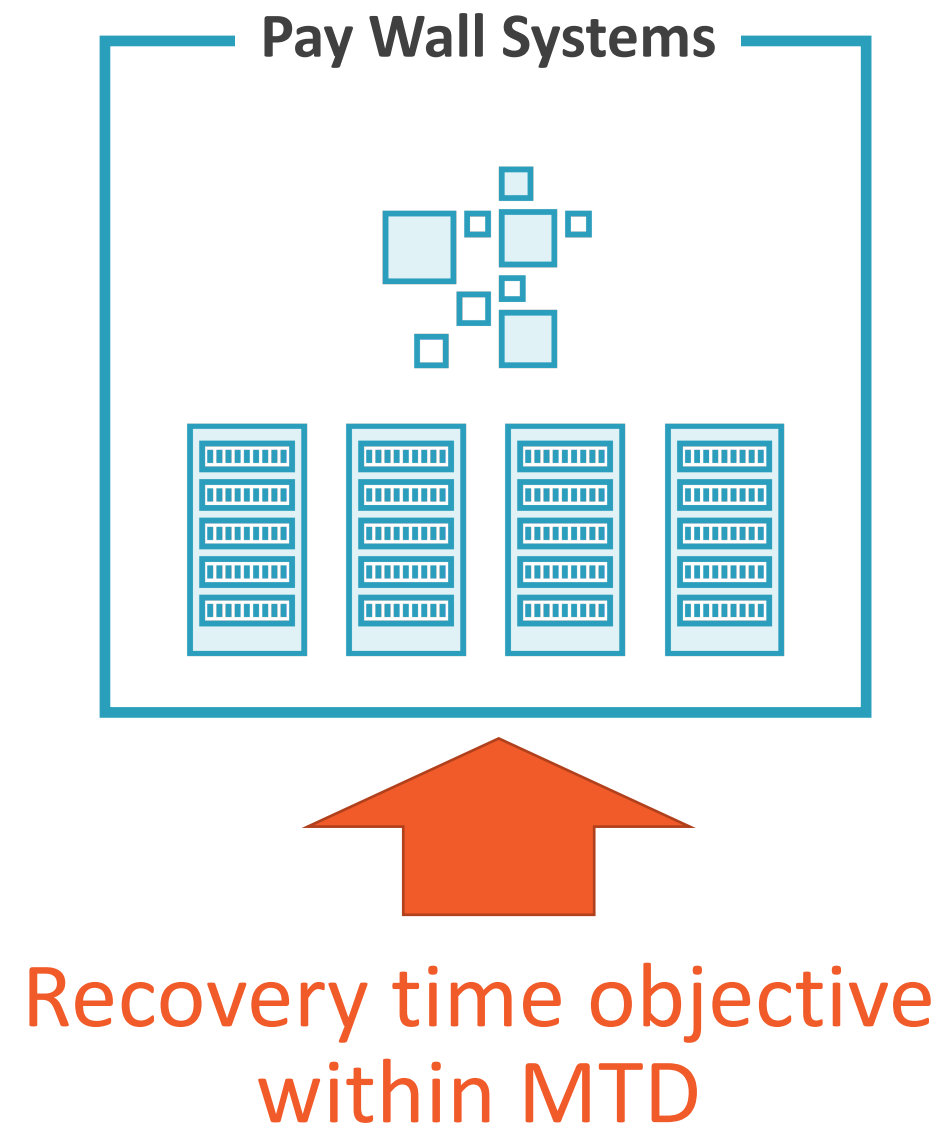
Recovery Scenario



Recovery Scenario



Recovery Scenario

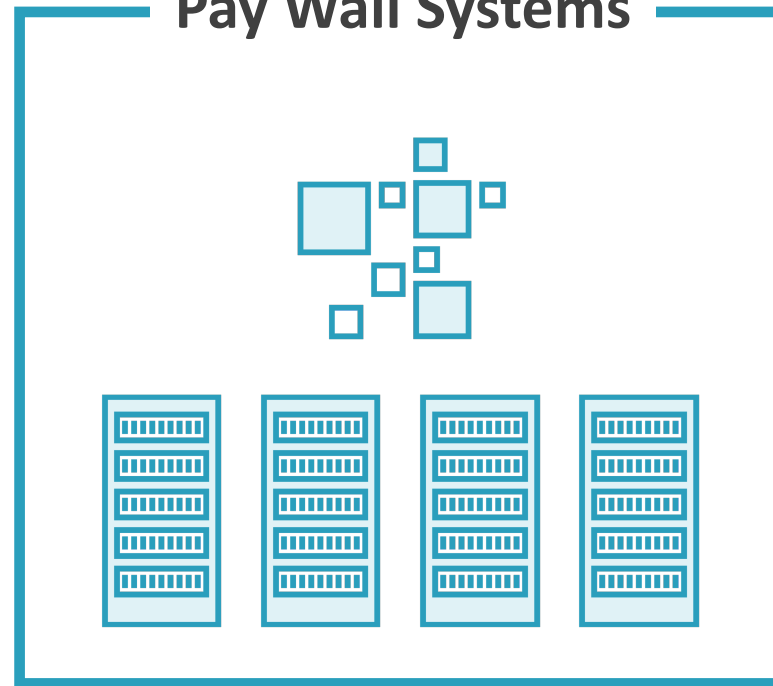


Recovery Scenario

Recovery point objective
allowable data loss



Pay Wall Systems



Recovery time objective
within MTD



Customer 1



Customer 2



Customer 3



Customer 4



BCP - Technology for Data Redundancy



Data backup
RAID
Offsite storage
Clustering
Electronic vaulting
Remote journaling

Data Redundancy Technology



Backup Schema

Full

All data regardless of
archive bit

Differential

All data changed since last
full and doesn't reset
archive bit

Incremental

Backs up all data changed
since last full and resets
archive bit

Full is longest backup quickest restore

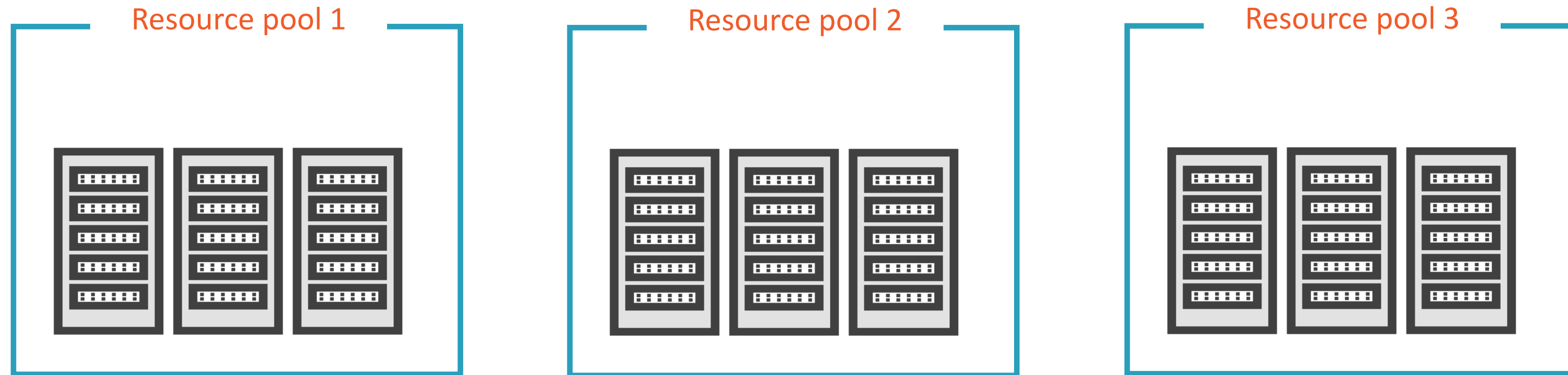


Clustering, Load Balancing, and High Availability

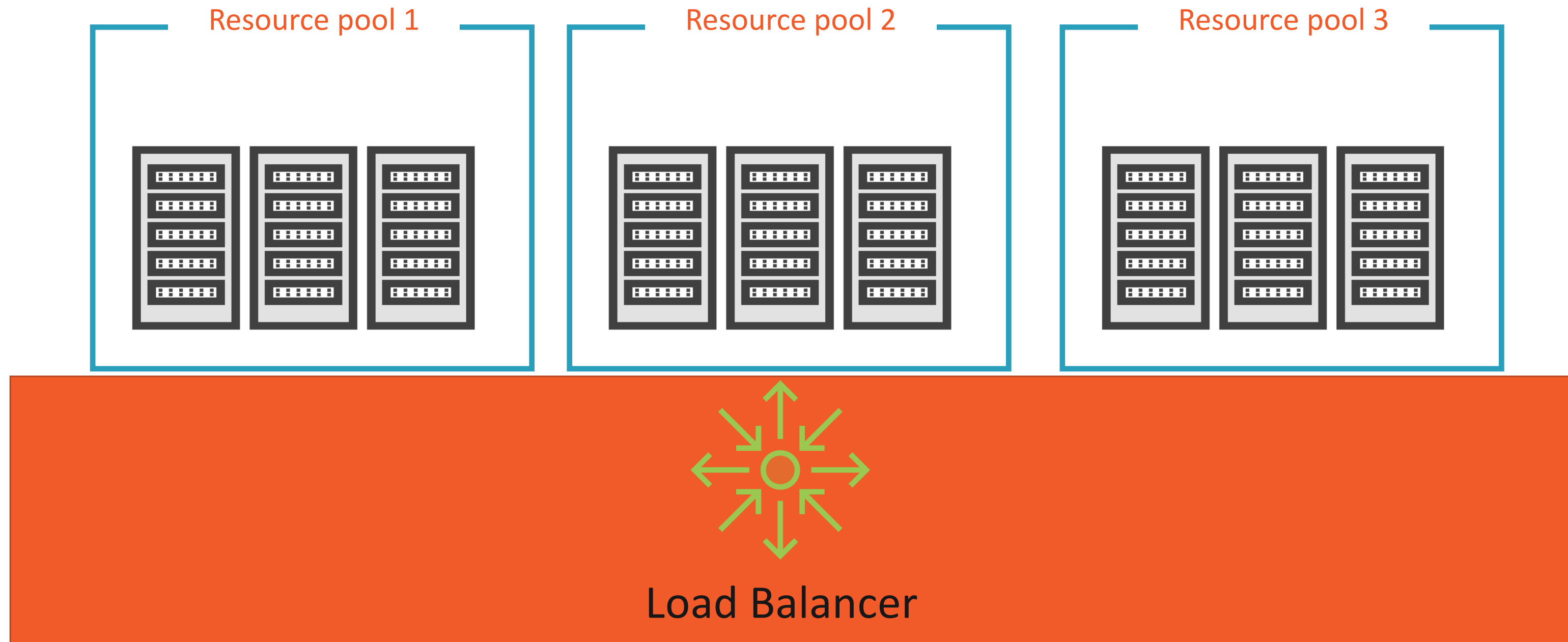


Clustered Servers

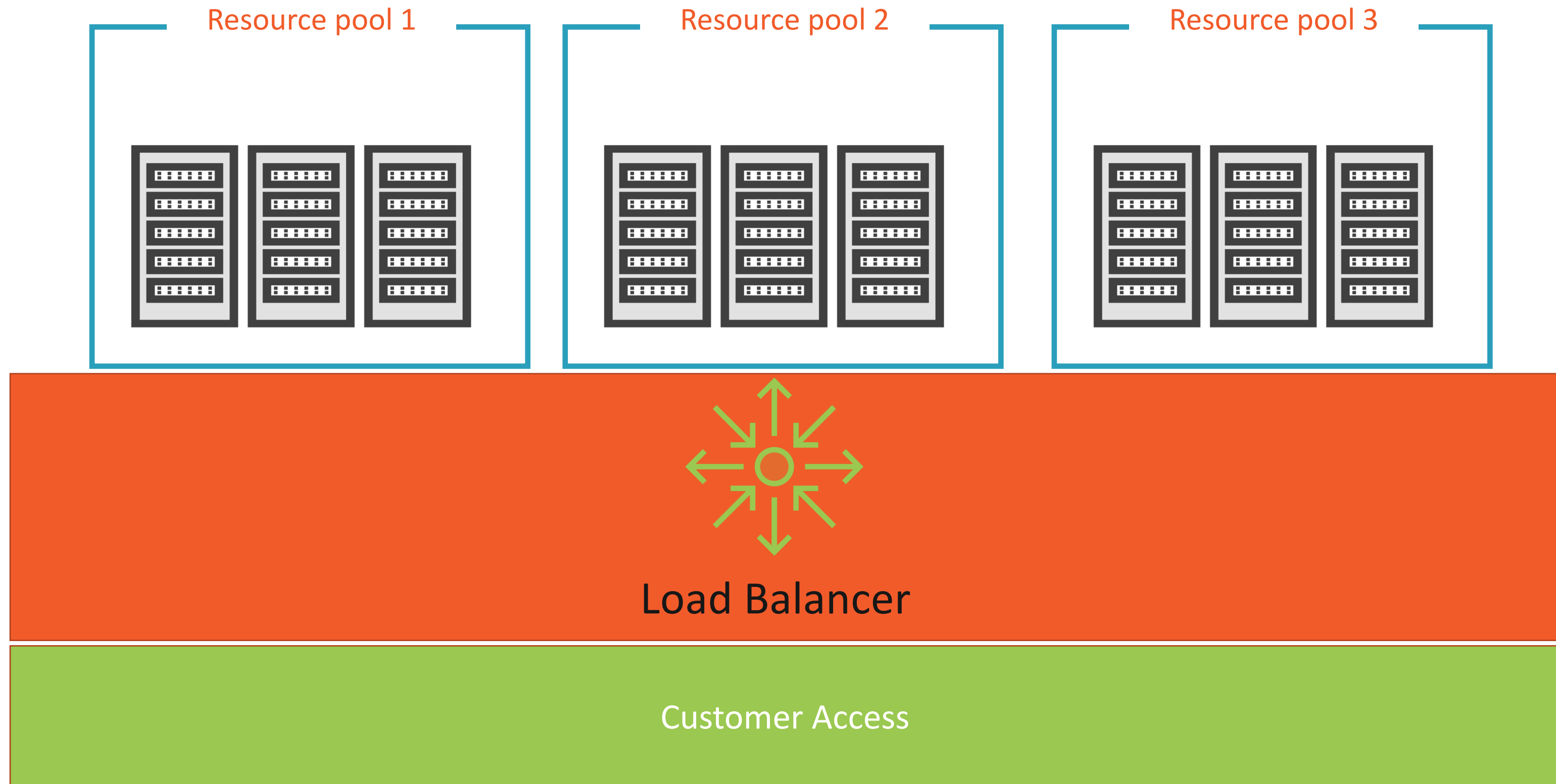
Clustering, Load Balancing, and High Availability



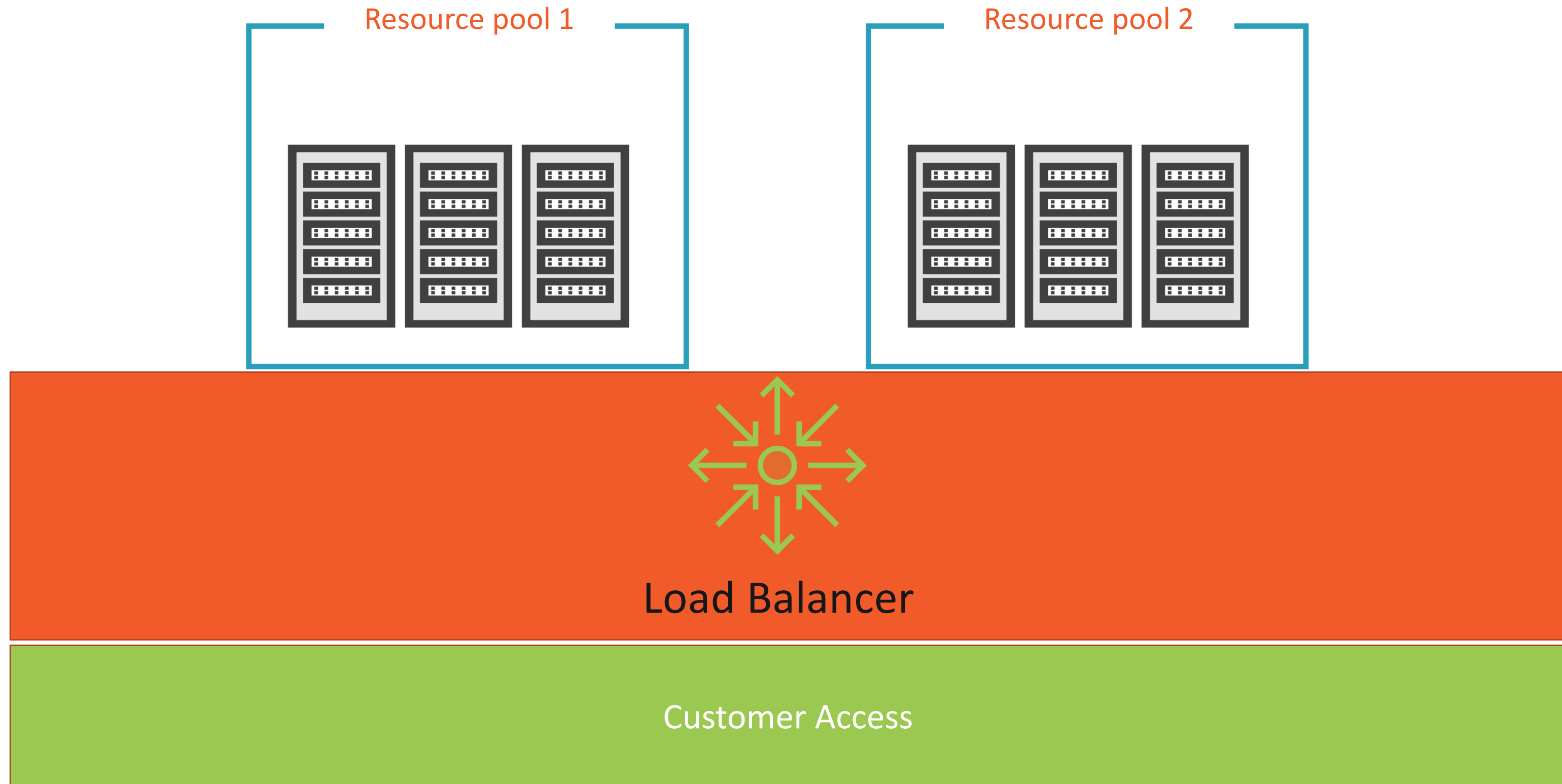
Clustering, Load Balancing, and High Availability



Clustering, Load Balancing, and High Availability

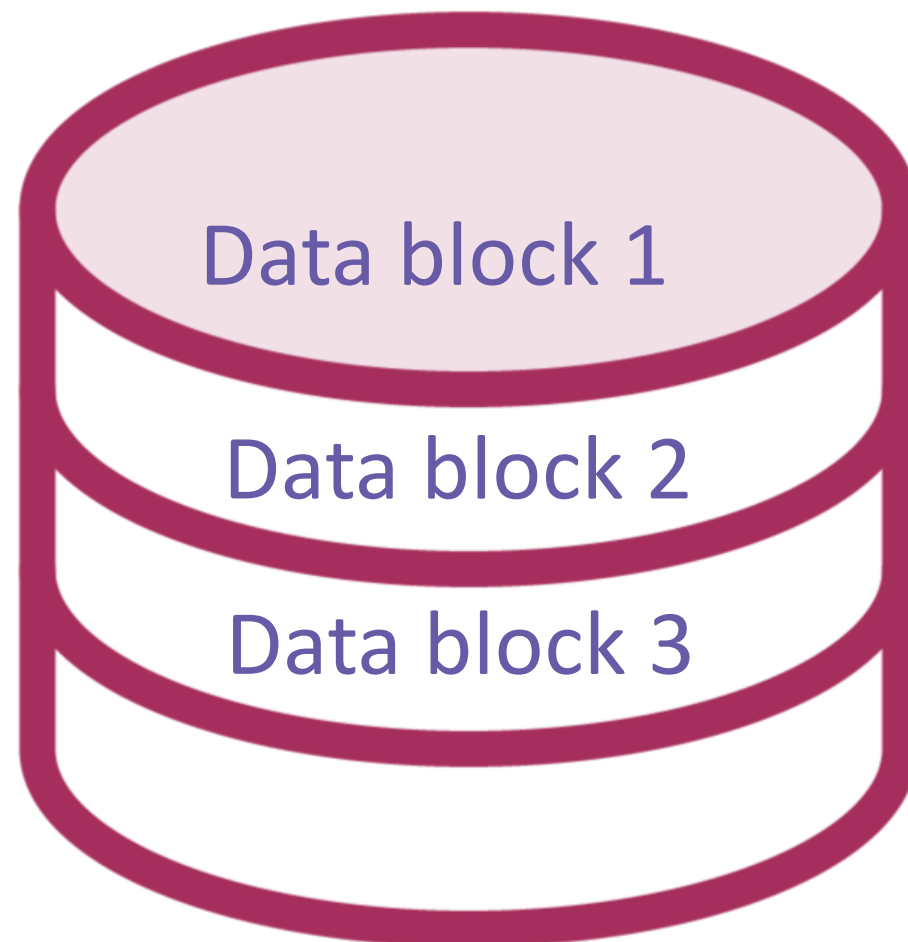


Clustering, Load Balancing, and High Availability

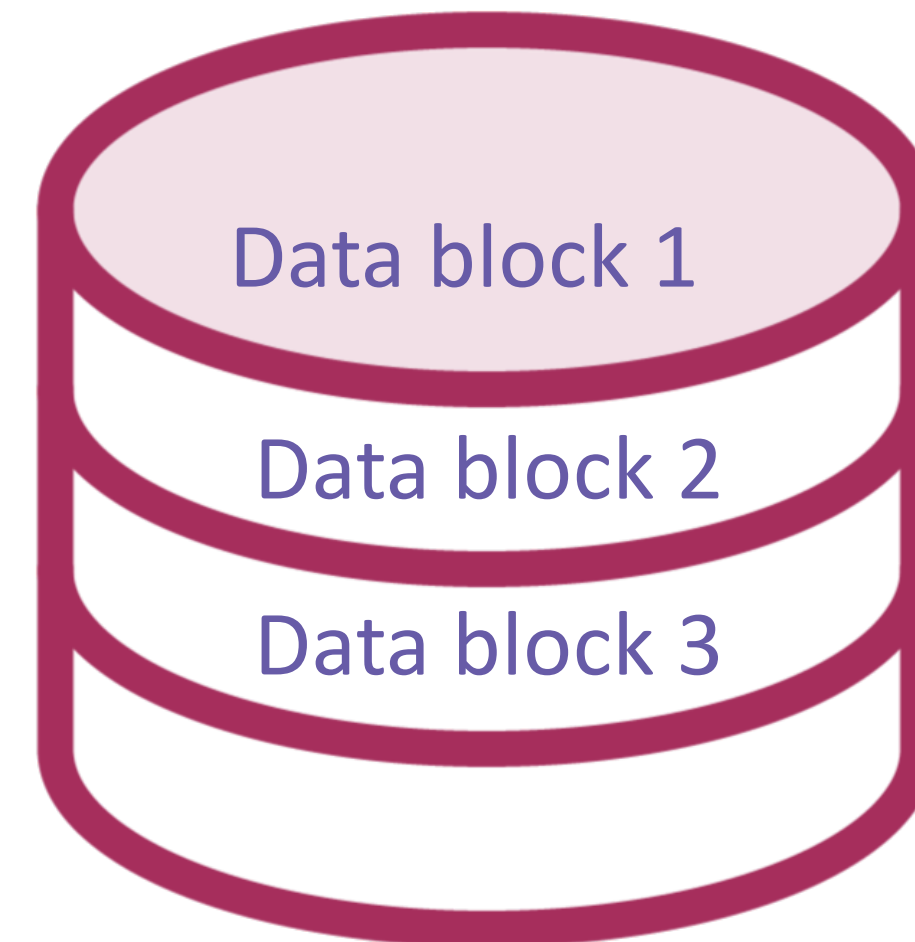


Disk Mirroring

Disk 1



Disk 2

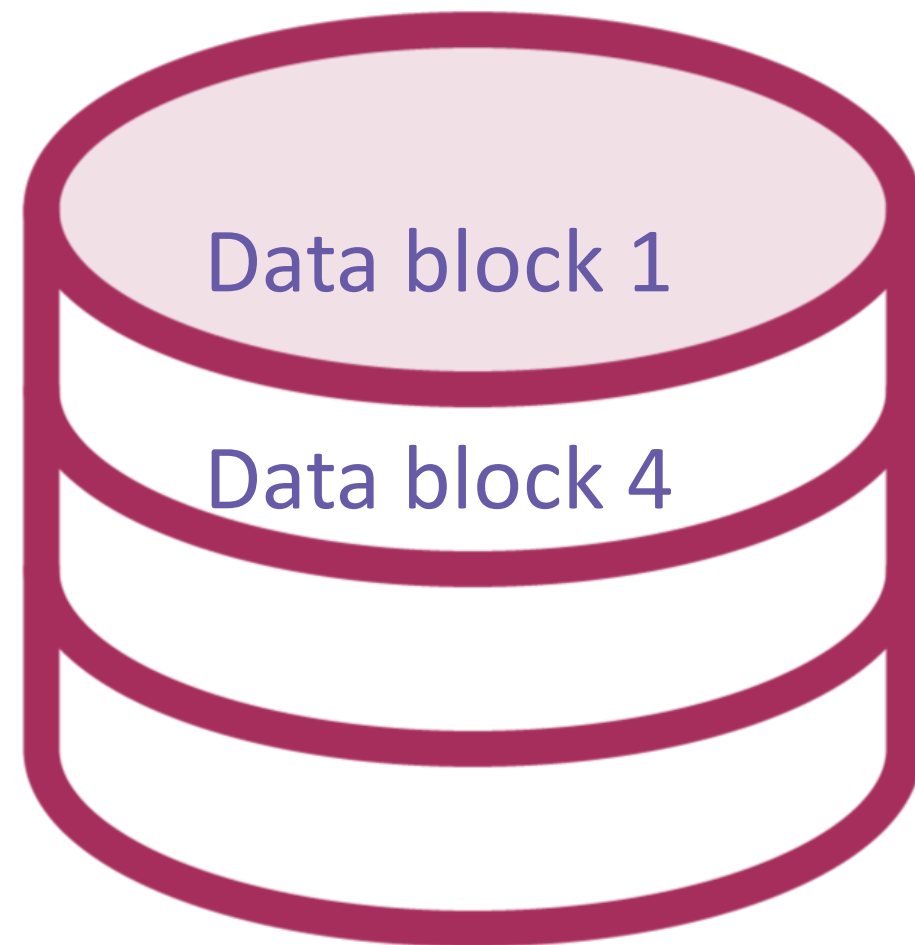


Identical Data

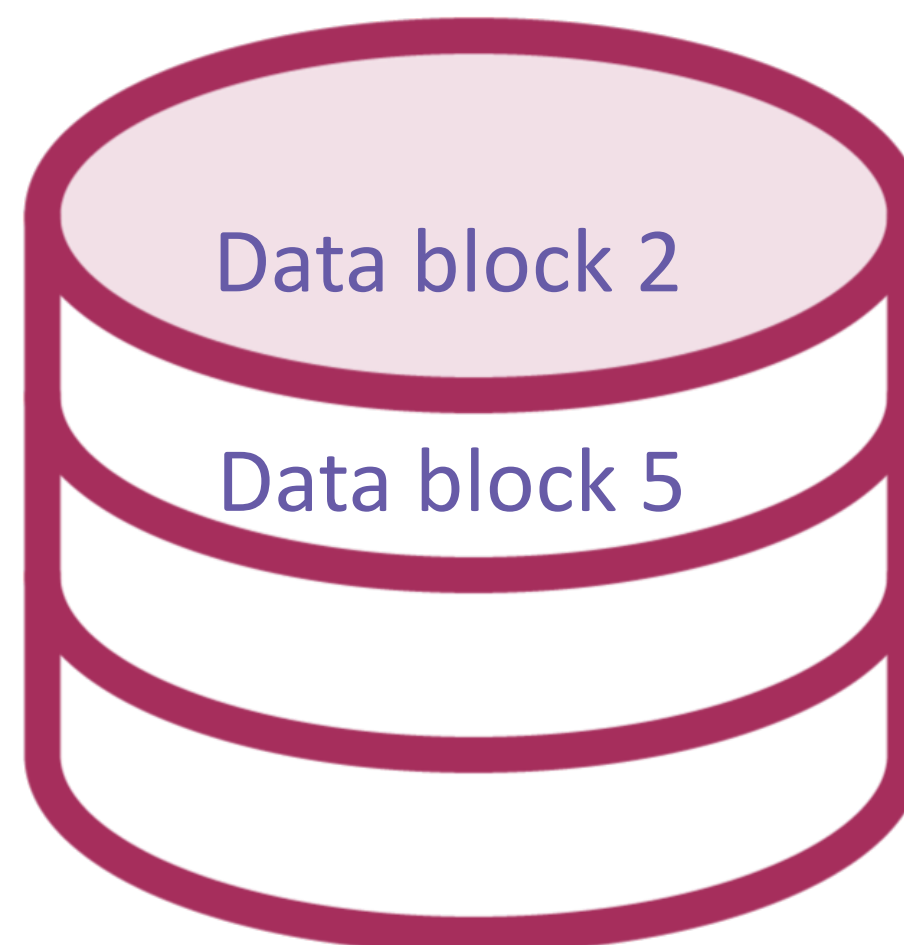


Disk Striping

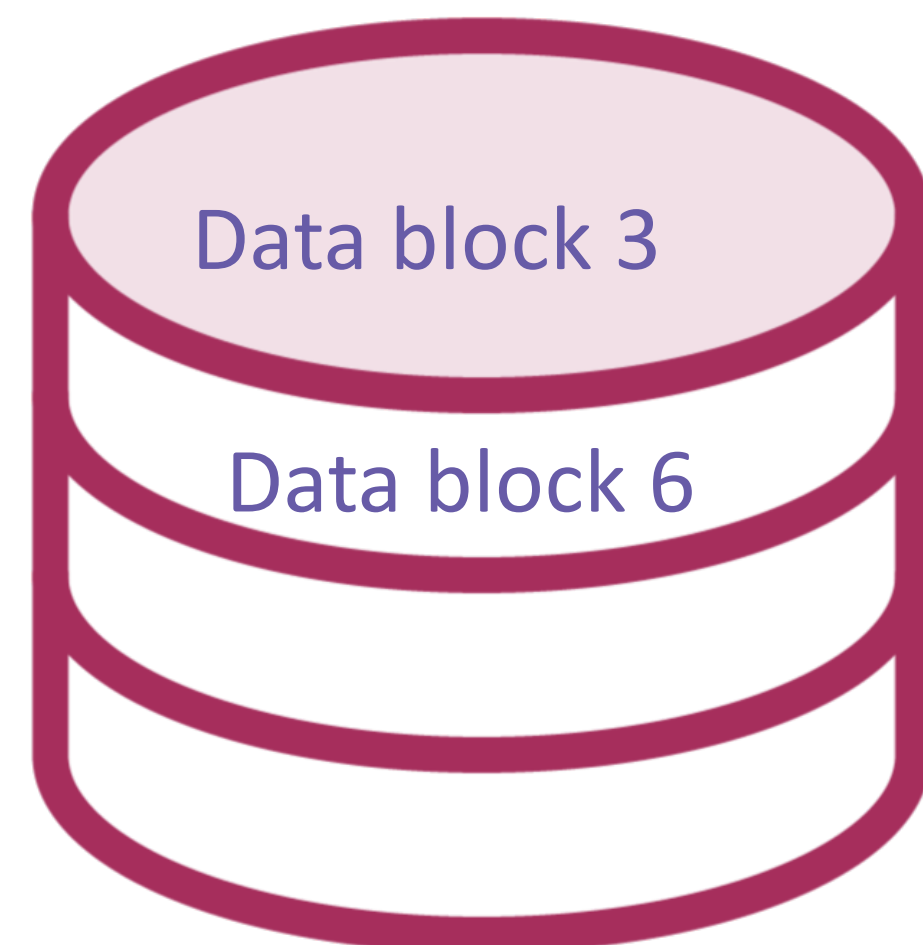
Disk 1



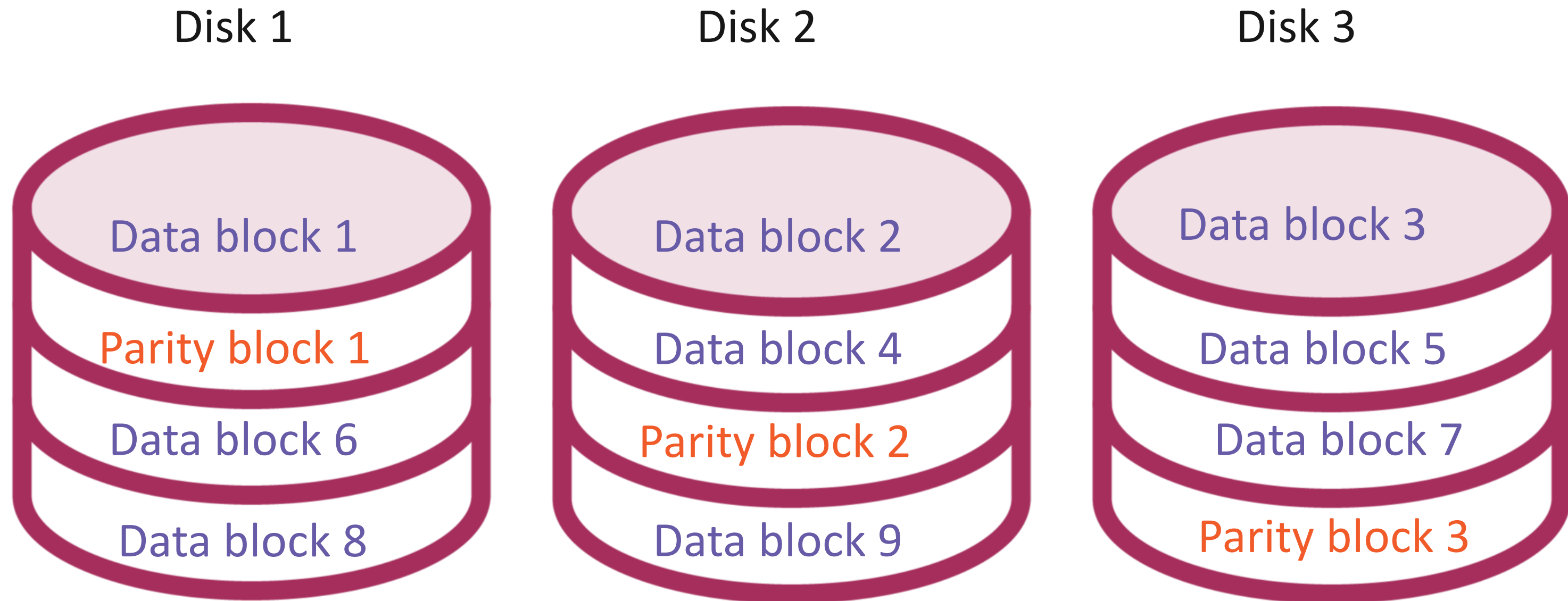
Disk 2



Disk 3



Disk Striping With Parity



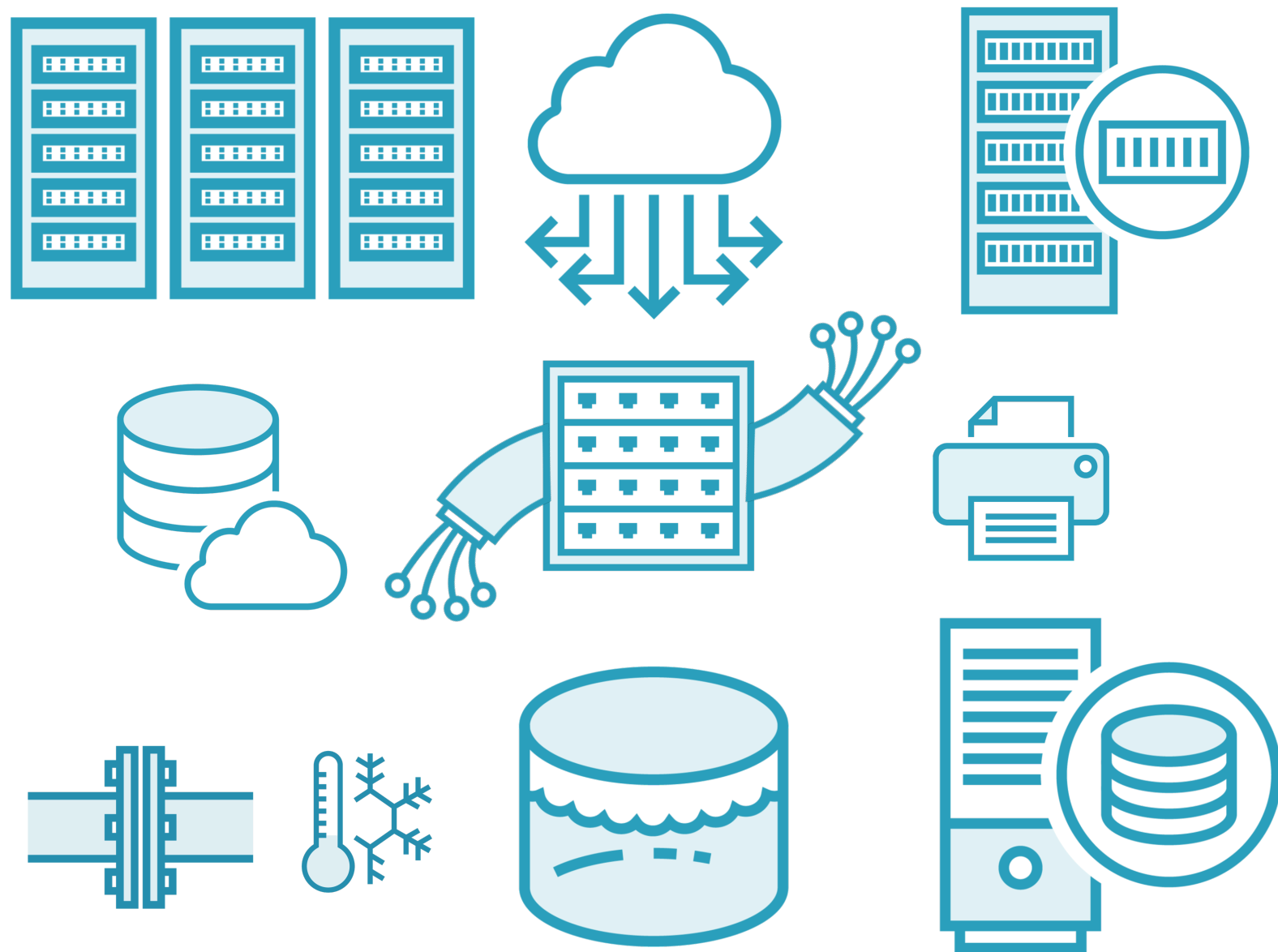
BCP- Response Strategy Selection



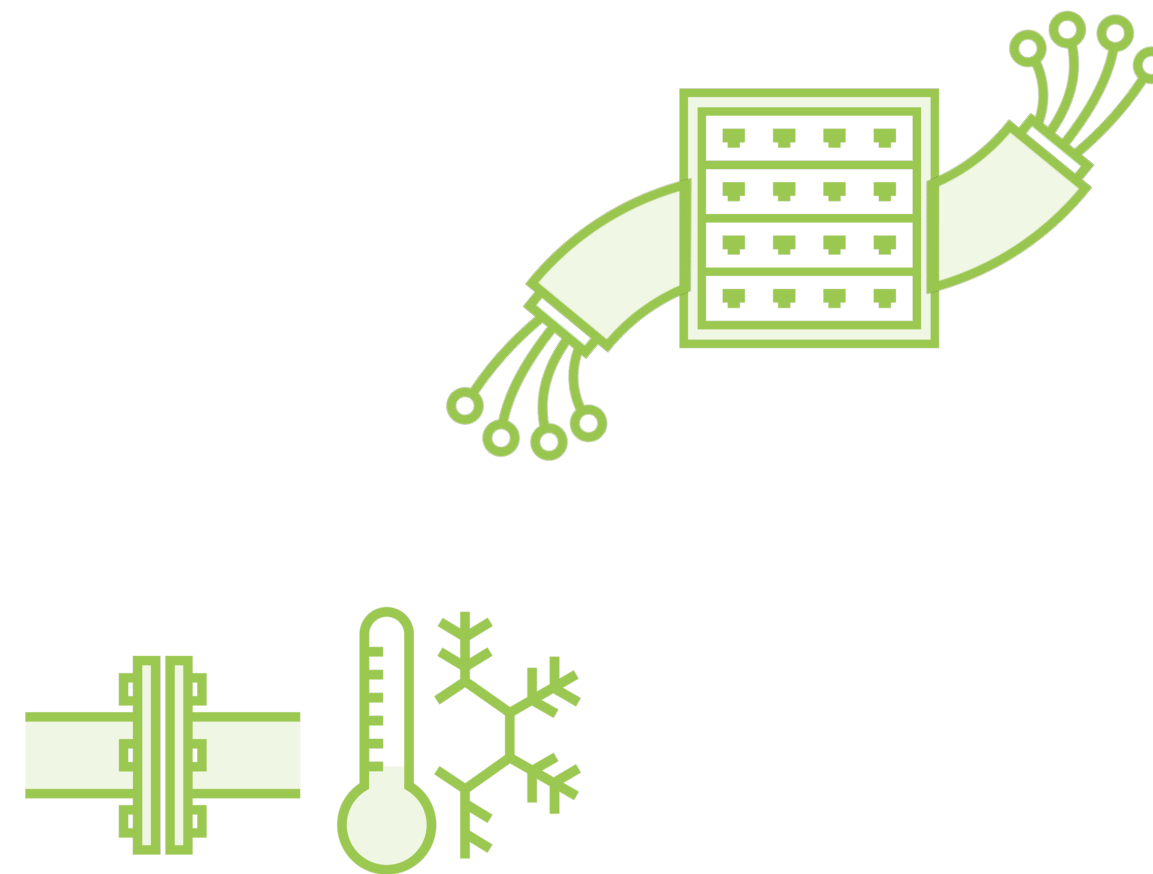
Cold Site

Recovery measured in weeks

Primary
Datacenter



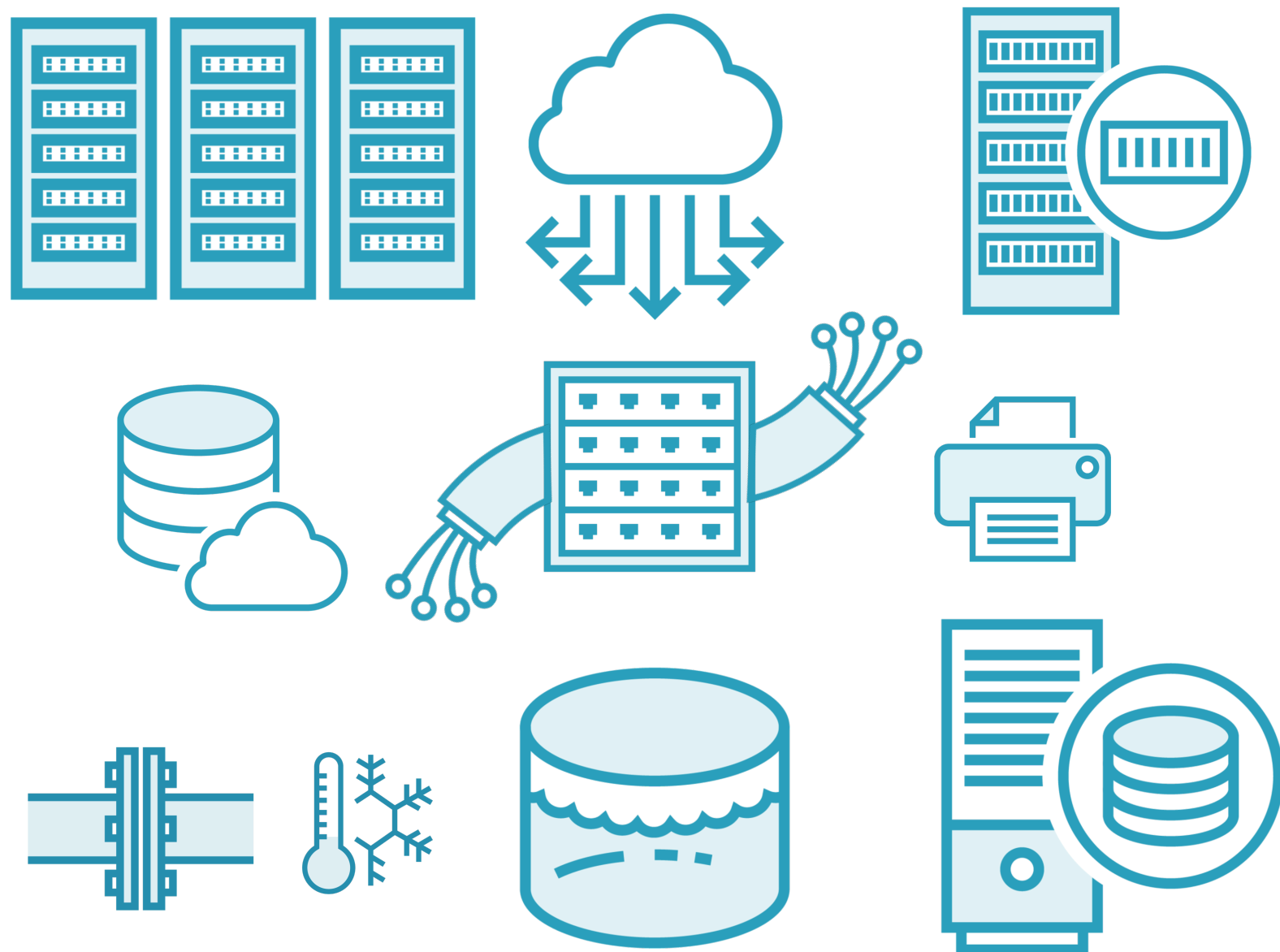
Alternate Site



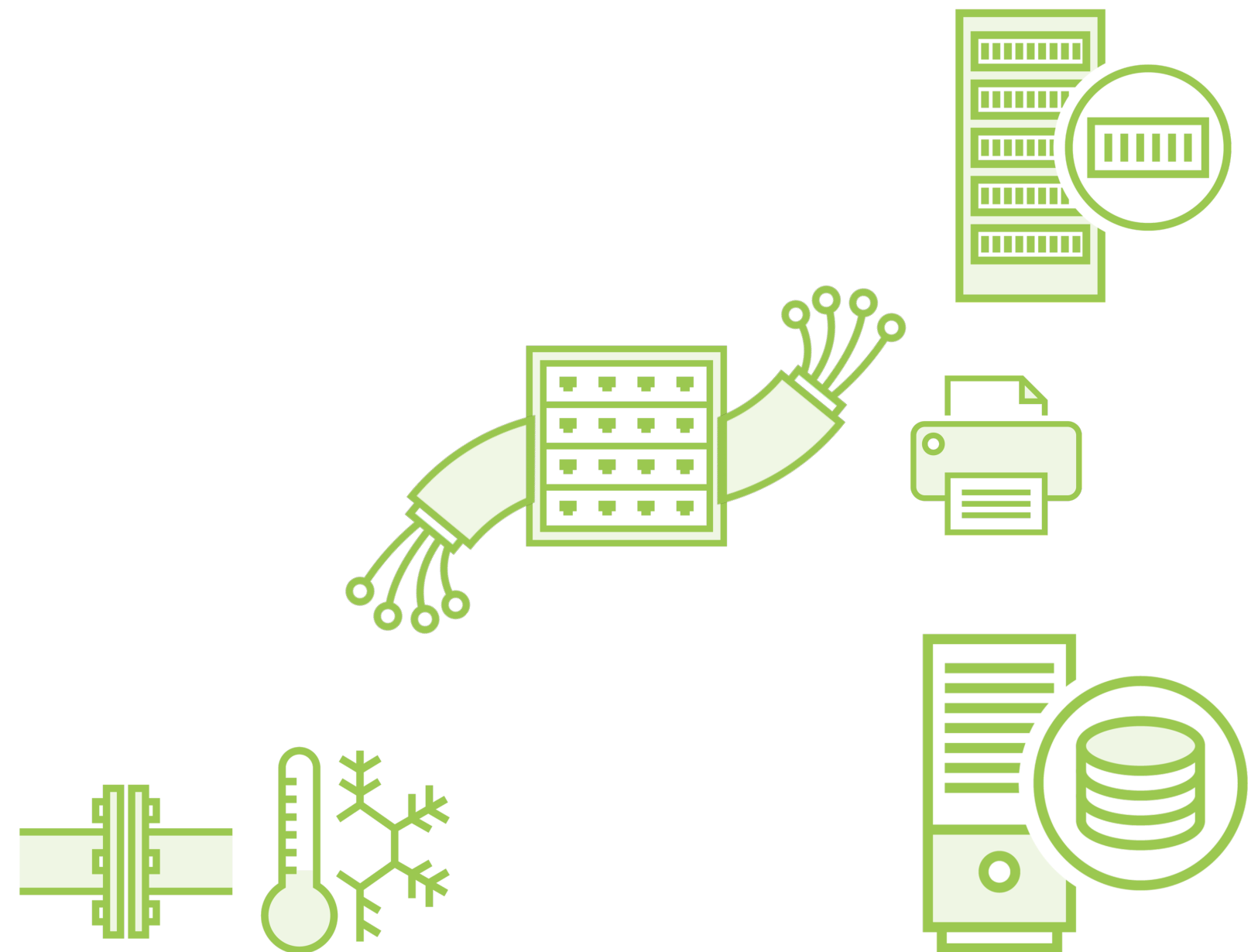
Warm Site

Recovery measured in days

Primary
Datacenter



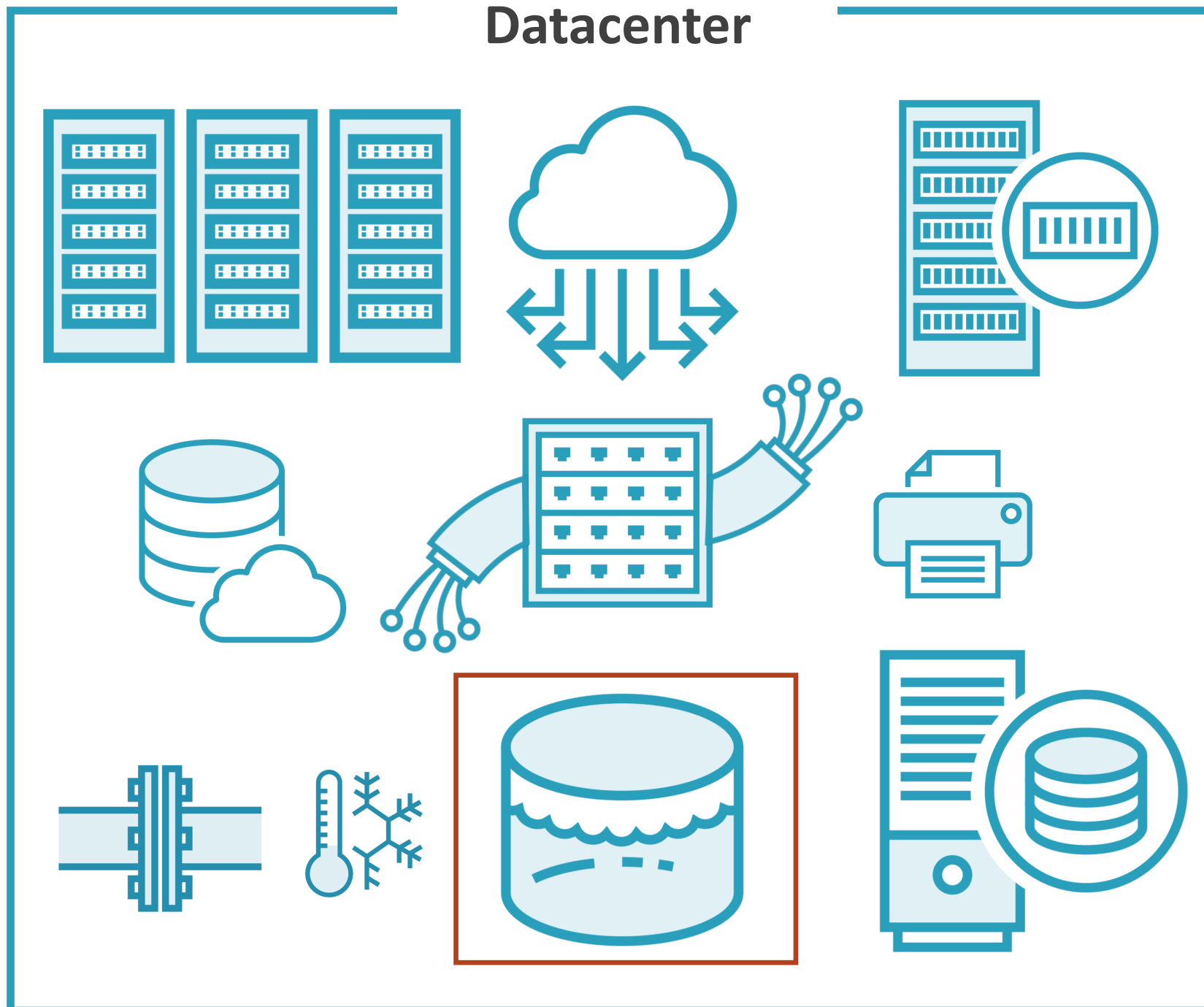
Alternate Site



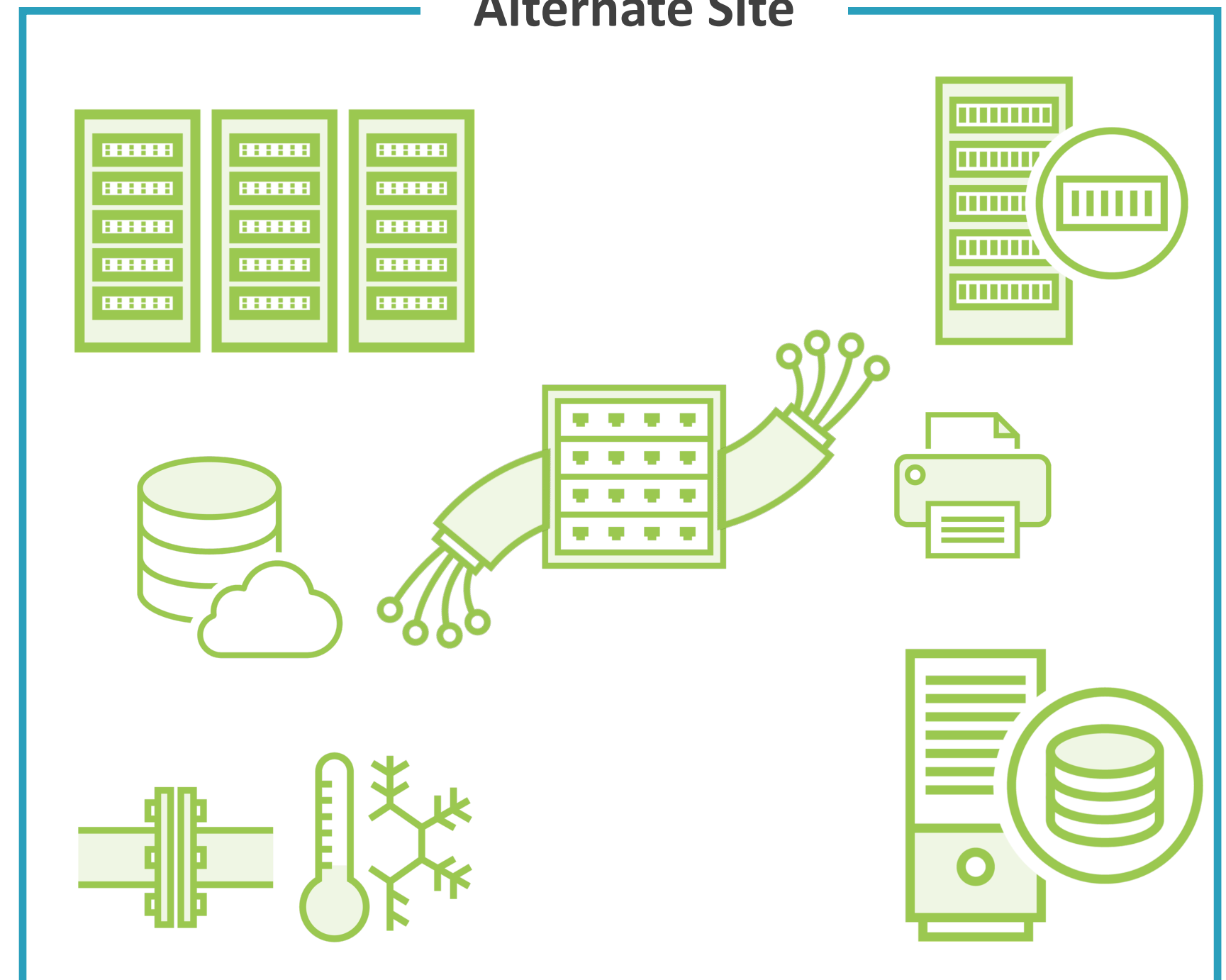
Hot Site

Recovery measured in hours

Primary
Datacenter



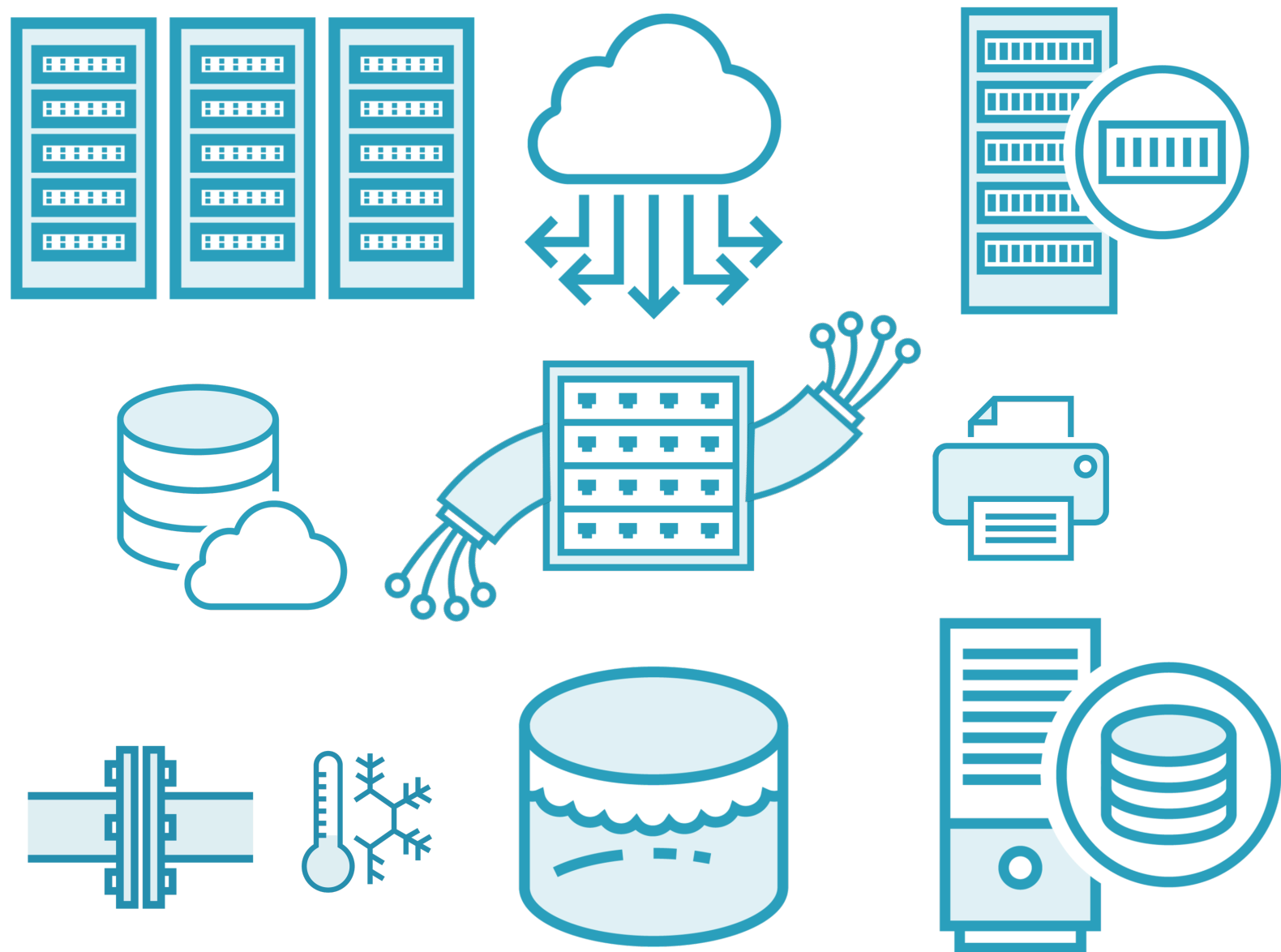
Alternate Site



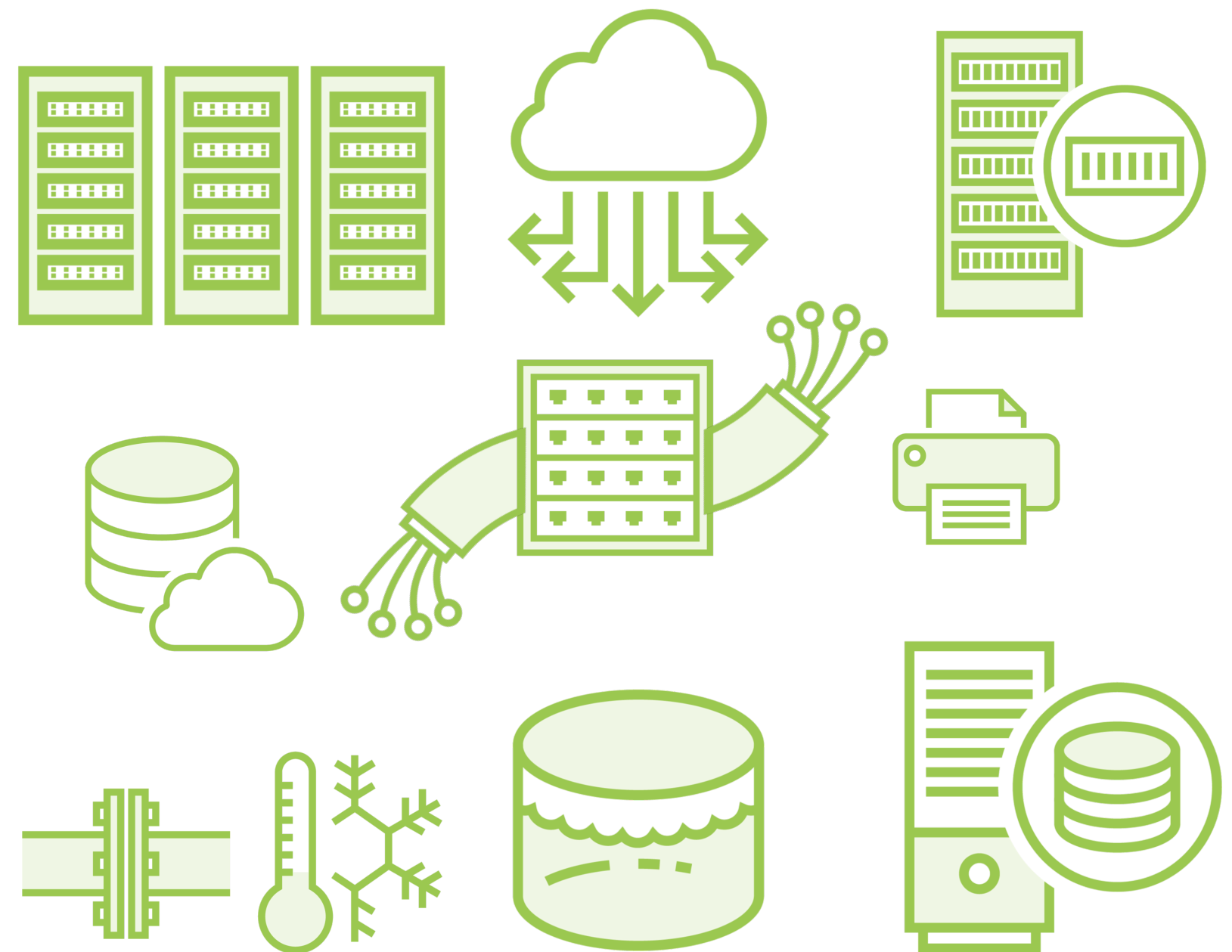
Mirrored Site

Recovery measured in minutes

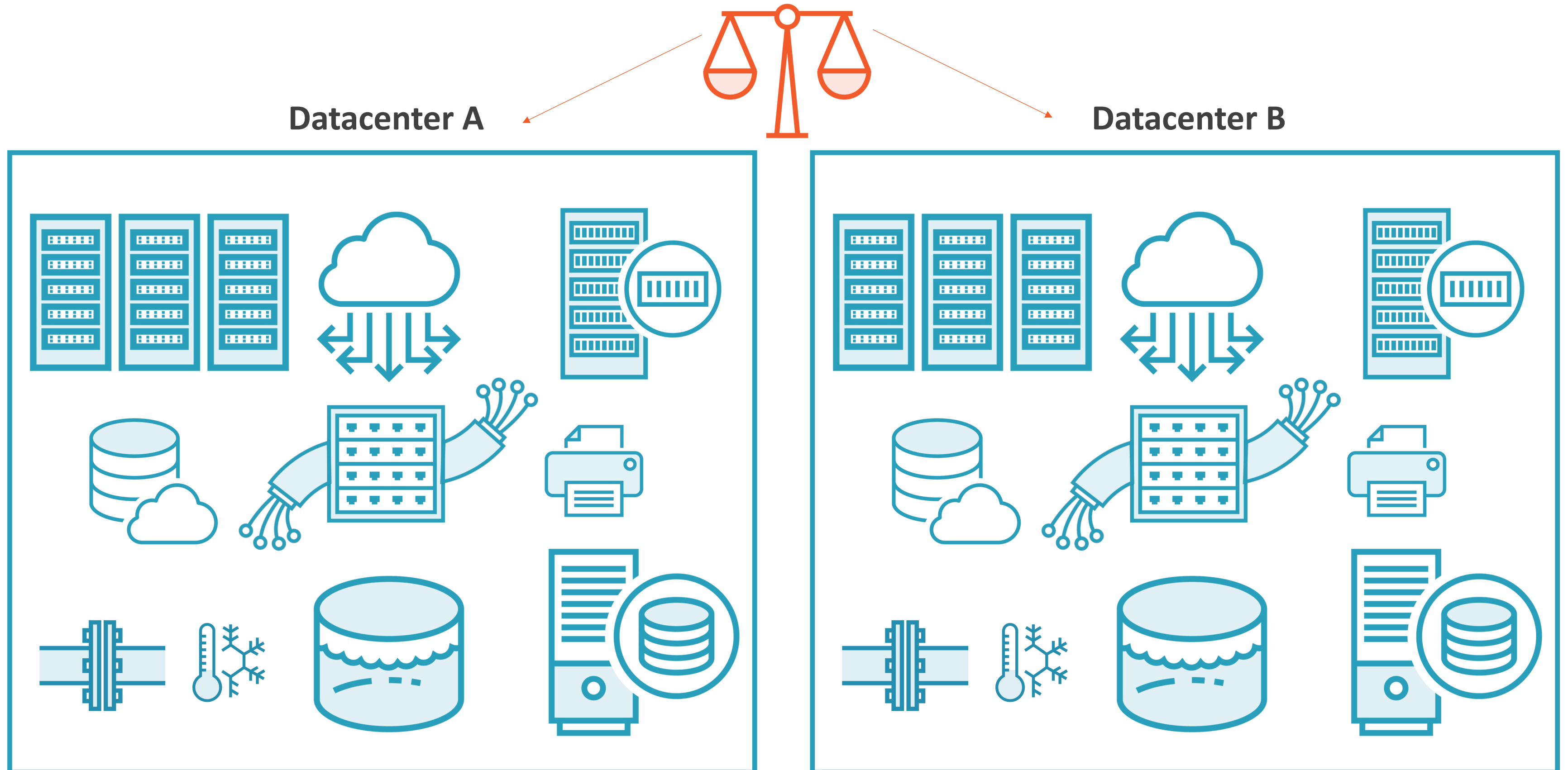
Primary
Datacenter



Alternate Site



Multiple Processing Centers



BCP – Writing, Implementing, and Testing



The one's writing the plan should
be closely aligned with those
implementing the plan.



Realistic plans come with



BCDR Teams

Executive

Declare disaster and
manage overall crises

Recovery

Works at alternate
location in critical to least
critical order

Restoration

Works at original site in
least critical to critical
order

Name two reasons for restoration directive



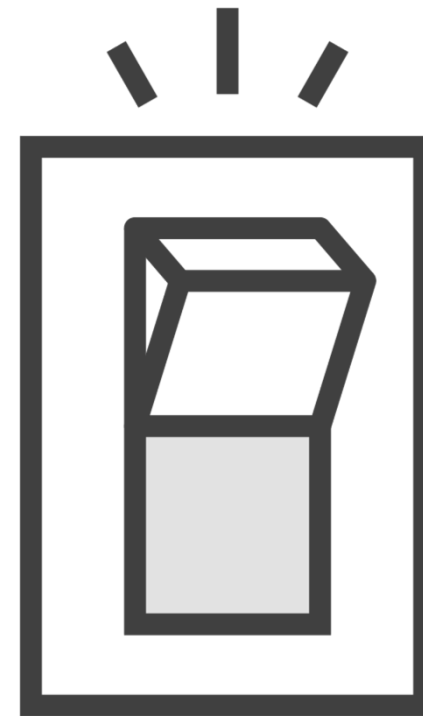
Types of BCDR Tests



Desk check



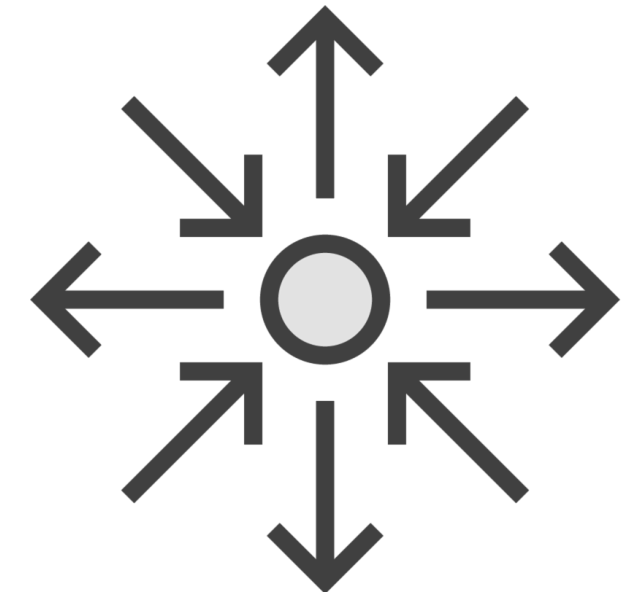
Tabletop



Simulation



Parallel



Full

Summary



Which areas of business continuity planning deserve the most attention

What are the recovery strategies that best suit your organization

What kind of tests have been completed to prove effectiveness

