Resilience Architectures

ardantic SA

Jeff Primus & Henri Haenni

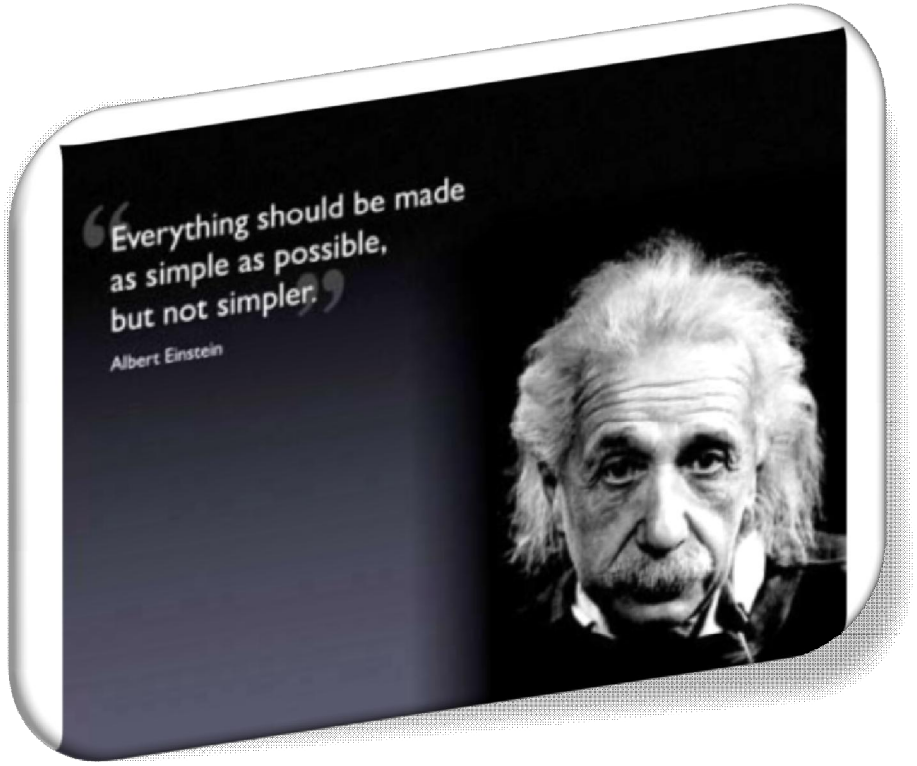
Senior Consultants

bienvenue@ardantic.ch

Agenda

Shapers of resilience strategies

Architectural solution space



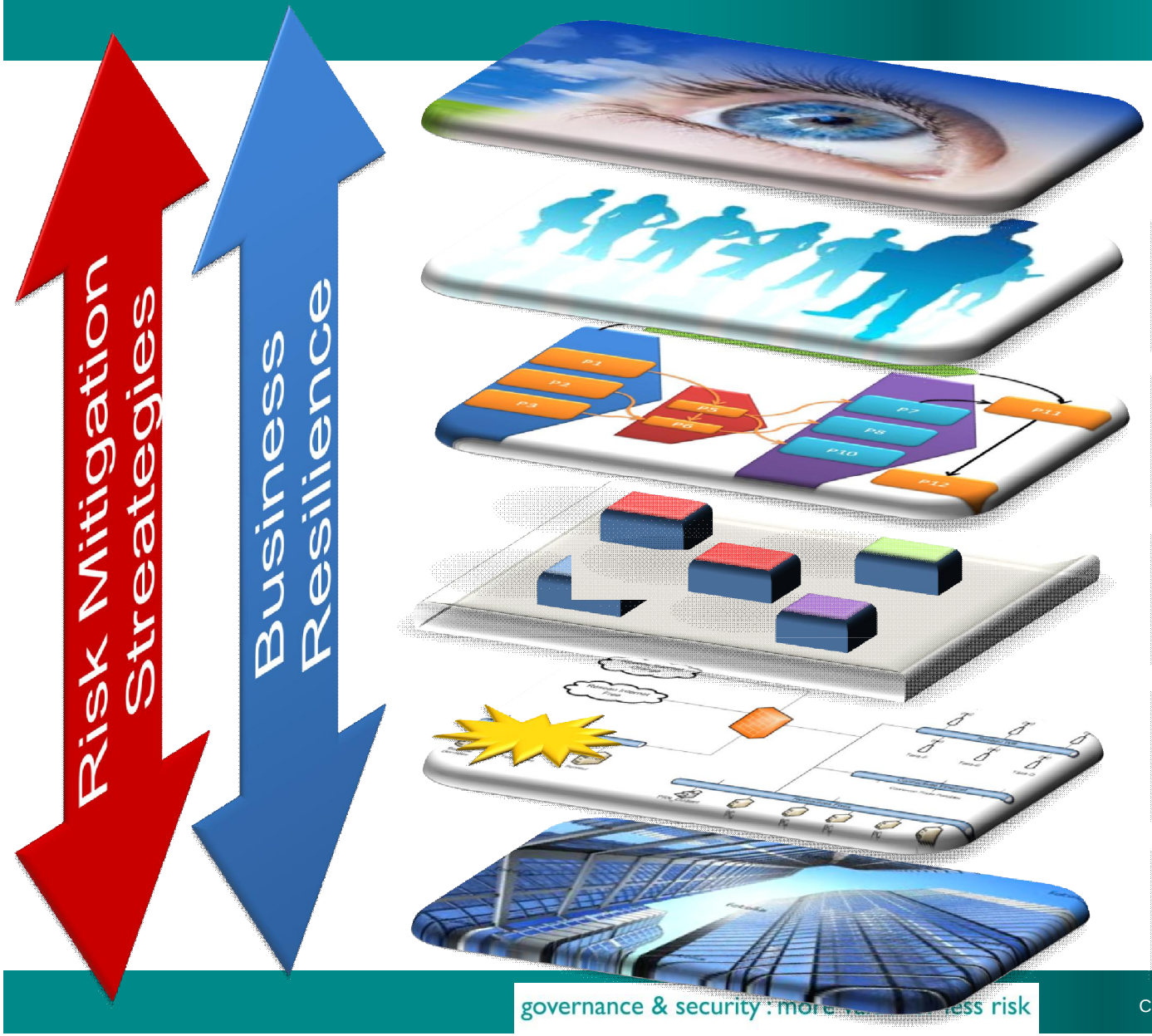
This is a little bit of art, not an exact science

We will give guidelines and generate better understanding

Not possible to give selection rules that will fit all situations

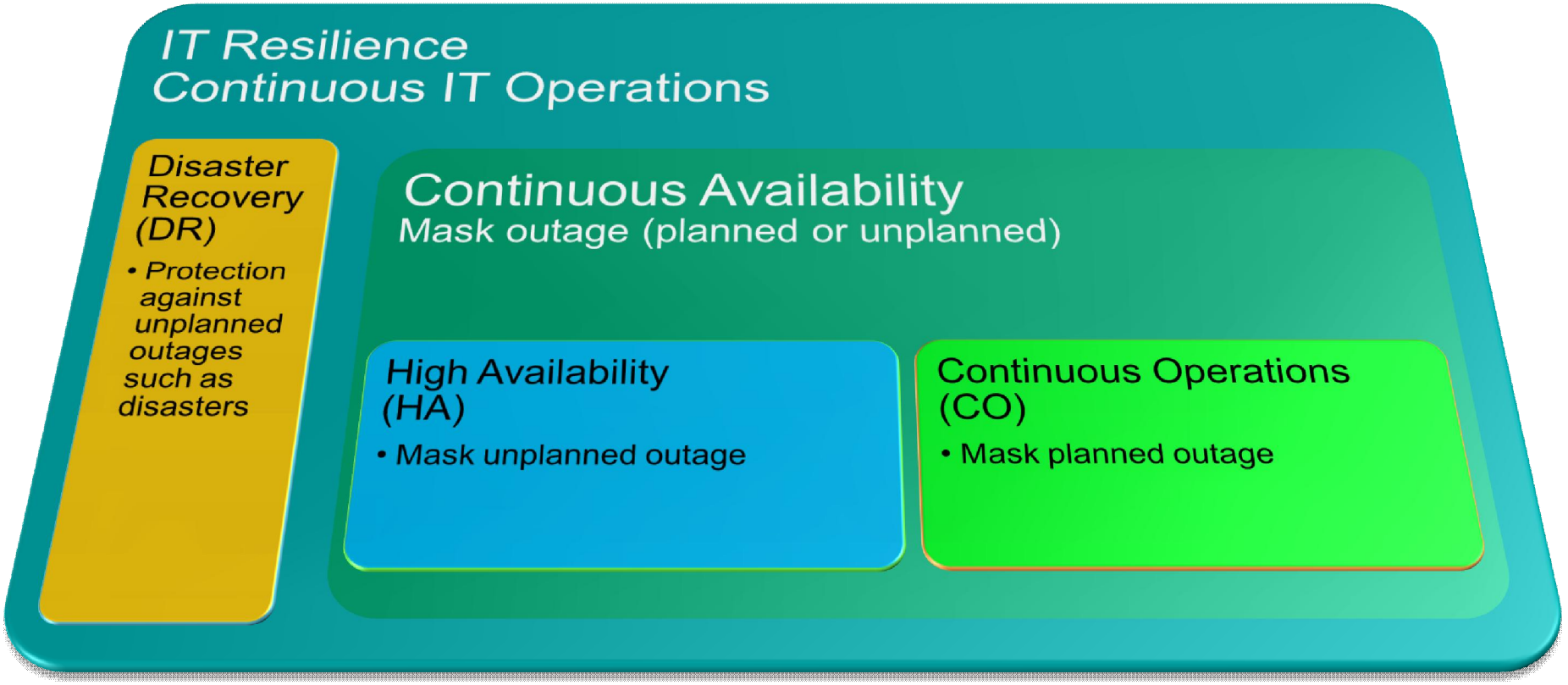
Business Resilience: across six layers

ardantic
governance & security



Resilience is the consistent, progressive development of traditional topics

Industry standard definitions



IT Resilience
Different strategies for different needs

High Availability

- Fault Tolerant
- Masks individual component failures
- Often provided by clustered servers
- Typically at one location

Continuous Operations

- Provide non-disruptive backups and maintenance
- The ability to keep uninterrupted access (24X7) to applications when everything is working properly

Disaster Recovery

- Ability to recover from unplanned outages
- Interruption with less or more downtime
- Performed on a site wide basis
- Usually on different hardware and /or site

Criteria for todayôs IT Resilience

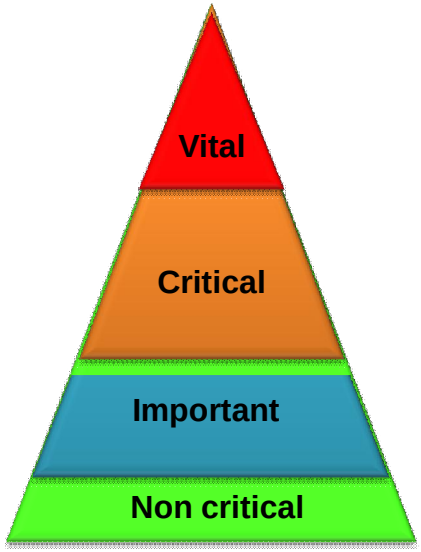
- **Recovery** times must be **repeatable** and reliable
  - ✓ Allows business continuity processes to be built
  - ✓ Upon a reliable, consistent recovery time

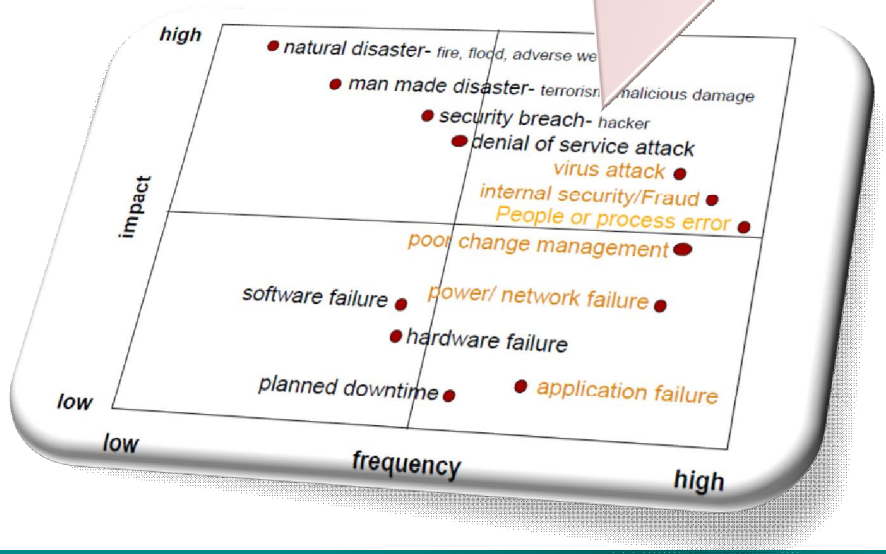
- **Large scalability**
  - ✓ Recovery times must be known even as the system scales
  - ✓ In todayôs time to market world, it is unacceptable to not have assured scalability

- **Affordable testing**
  - ✓ Repeatable, reliable, scalable business continuity can only be assured through testing that can be affordably be performed often

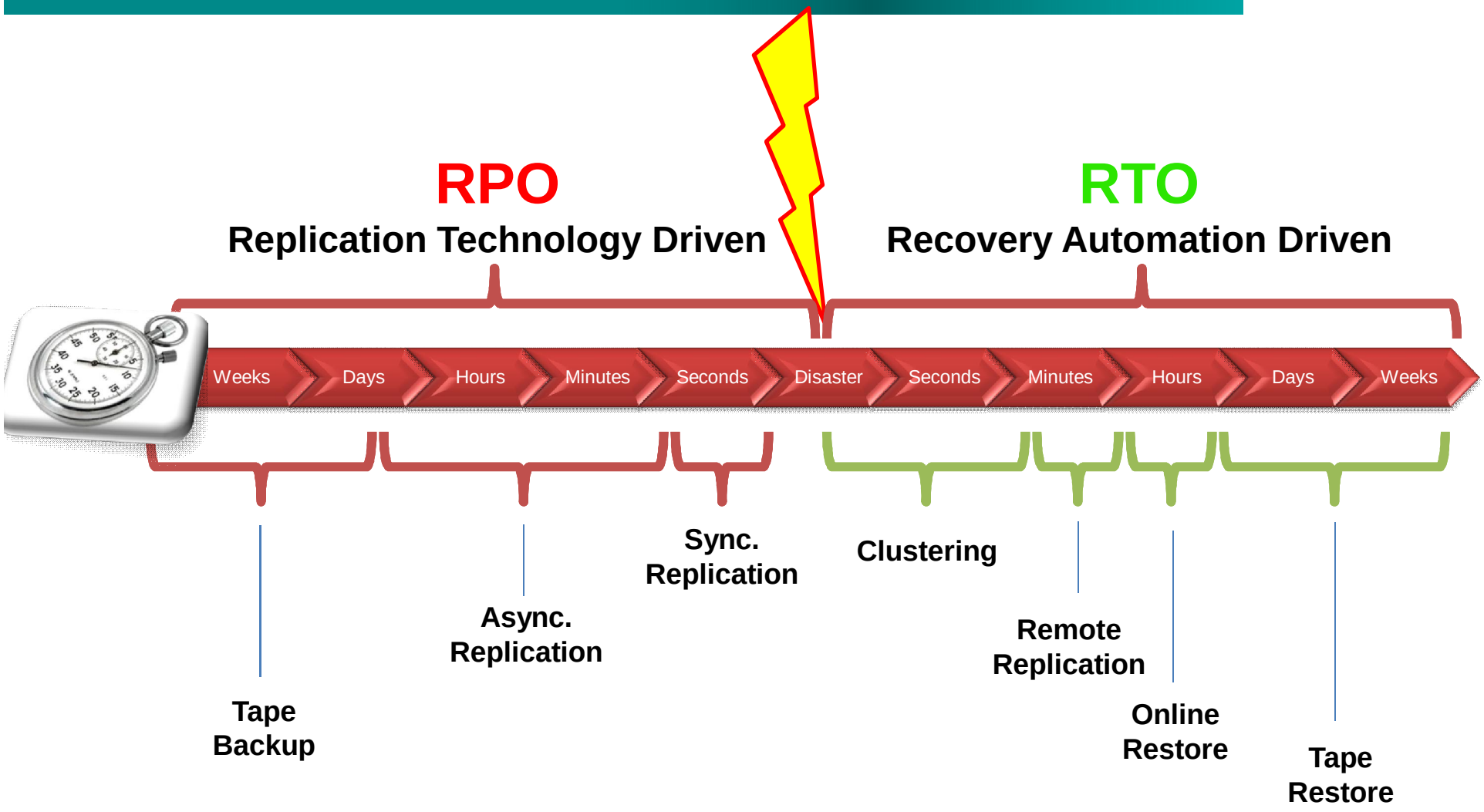
- **Adequate level of automation**

Planning for the resilience

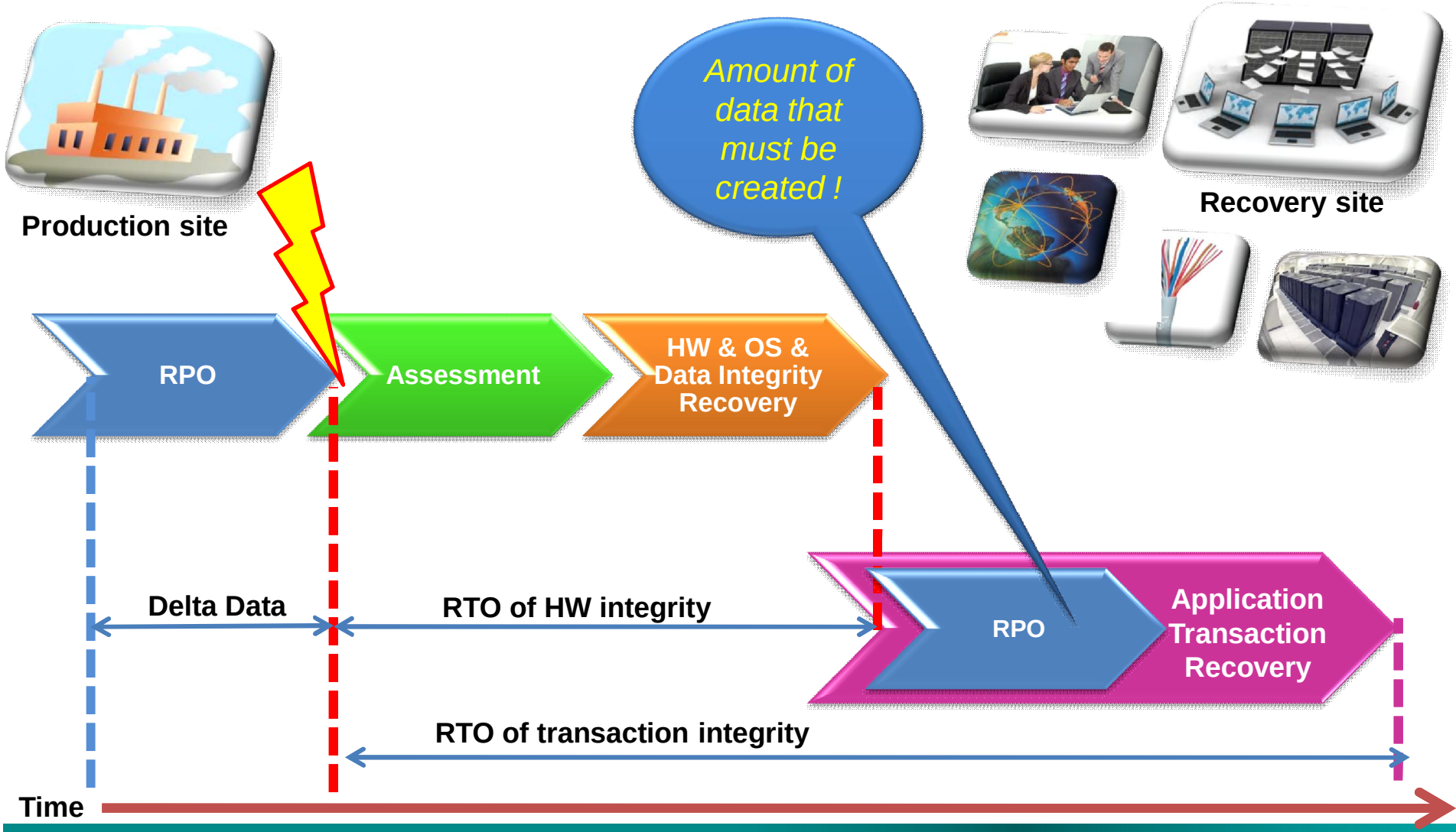




Resilience Objectives



Recovery chronology & How RTO is affected by RPO



Recovery chronology & Value of automation

Production site

Recovery site

RPO

Assessment

HW

Delta Data

RTO of HW integrity

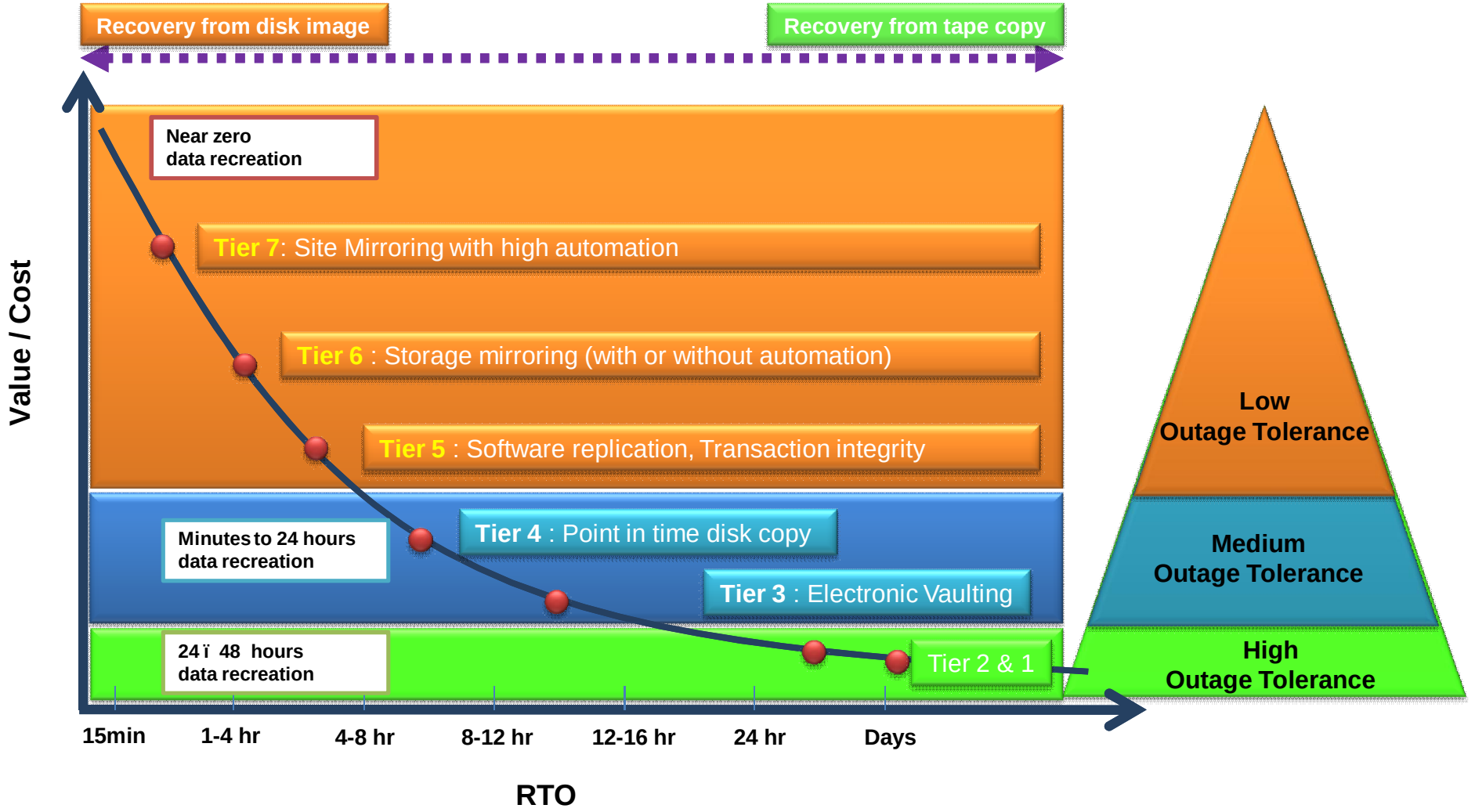
RPO

Application Transaction Recovery

RTO of transaction integrity

Time

Resilience Tiers & Application Outage Tolerance Levels



7 Tiers of Resilience solution

Tier 1 ***Back up data at an off-site facility (without Hot Site)***	▪ Several days to weeks of data loss ▪ Lacks the systems on which to restore data ▪ Pickup Truck Access Method (PTAM)
Tier 2 ***Regular back up data at an off-site (Hot site)***	▪ Like Tier 1 and combined with hot site infrastructure in which to restore systems from those tapes in the event of a disaster. ▪ Solutions make regular backups on tape ▪ This tier solution will still result in the need to recreate several hours to days worth of data, but it is less unpredictable in recovery time
Tier 3 ***Electronic Vaulting***	▪ Utilize components of Tier 2. ▪ Additionally, some mission-critical data is electronically vaulted. ▪ This electronically vaulted data is typically more current than that which is shipped via PTAM.
Tier 4 ***PIT (Point in Time Copy)***	▪ Incorporate more disk-based solutions ▪ Several hours of data loss is still possible but it is easier to make such point-in-time (PIT) copies with greater frequency

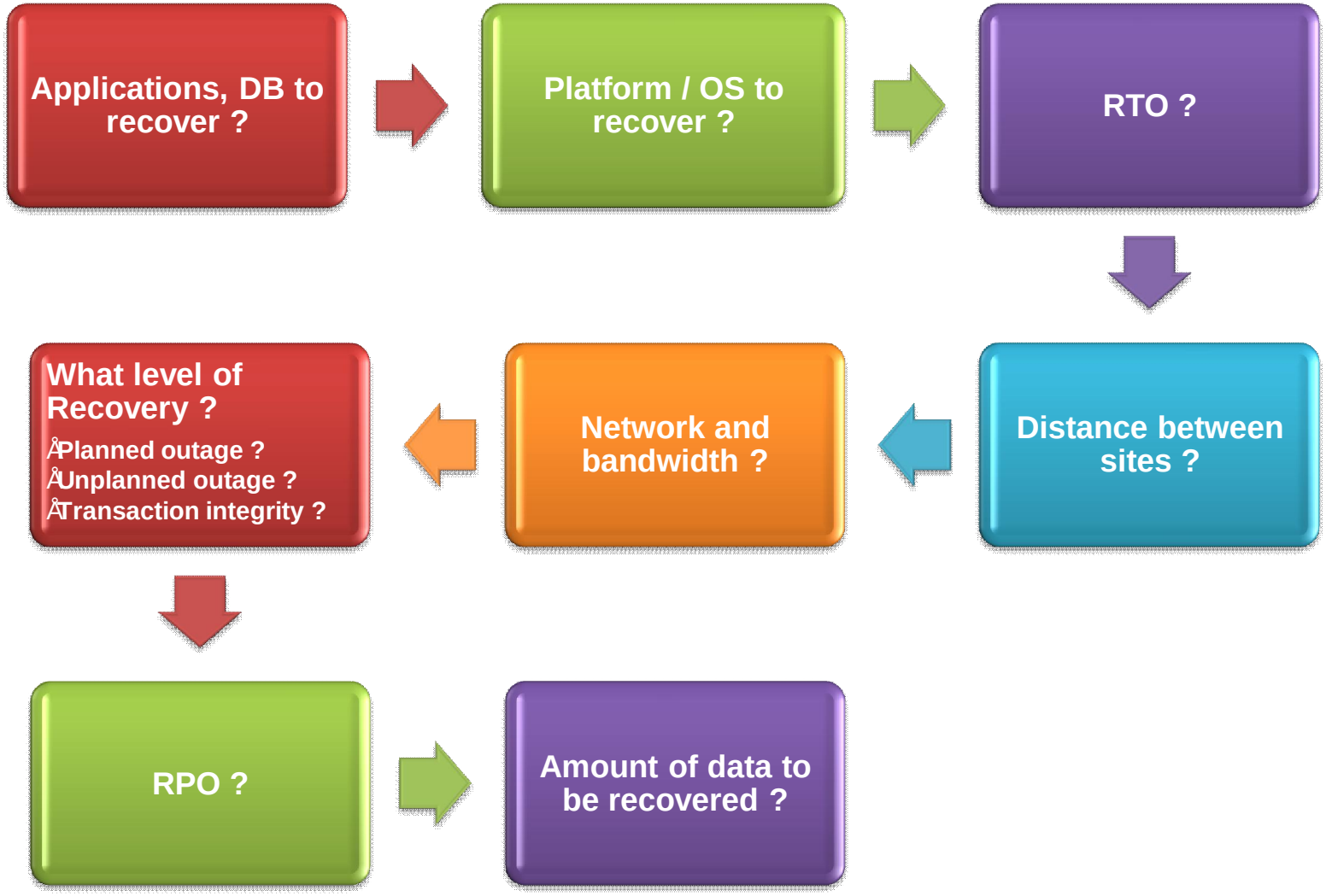
7 Tiers of Resilience solution

Tier 5 ***Software replication Transaction integrity***	▪ For businesses with a requirement for consistency of data between production and recovery data centers (mirroring) ▪ There is little to no data loss in such solutions ▪ The presence of this functionality is entirely dependent on the application in use
Tier 6 ***Zero or little data loss***	▪ Maintain the highest levels of data currency ▪ No dependence on the applications to provide data consistency ▪ OS Mirroring
Tier 7 ***Highly automated, business-integrated solution***	▪ Include all the major components being used for a Tier 6 solution with additional integration of automation ▪ Ensure consistency of data granted by Tier 6 solutions ▪ Additionally, recovery of the applications is automated

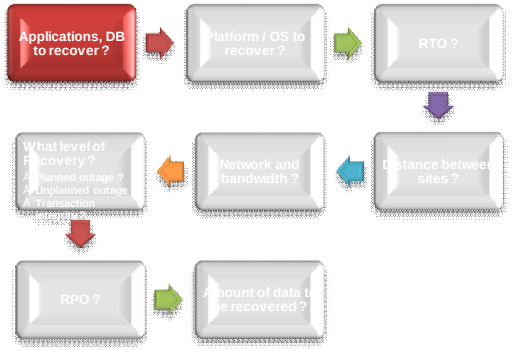
Strategy Design: Architecture review

- Review the business function the application provides
- Review function(s) of key transactions
- Walkthrough the key transactions across the infrastructure
  - ✓ Understand each infrastructure component supporting the transaction
  - ✓ Understand how the workload enters the system
  - ✓ Understand the transaction is created and modified across the application path
- Identify potential limitations affecting availability
- Determine the distance between sites
  - ✓ Sites must not be affected by the same disaster
  - ✓ Easy access to both (staff, telco, syn techniques)
  - ✓ Cost
  - ✓ Available locations

Key IT Business Continuity Requirements Analysis



Key IT Business Continuity Requirements Analysis



- What applications or databases to recover ?
  - ✓ Application software level recovery indicated ?
  - ✓ Application level integration tools required ?

Application / DB (Tier 5)

- ✓ Requires least bandwidth
- ✓ More complex implementation

Server replication (Tier 6)

- ✓ Storage and application independent
- ✓ Span of recovery limited to the server platform

Storage Replication (Tier 6)

- ✓ Common recovery across multiple application stacks and server platforms
- ✓ Requires more bandwidth

More bandwidth

More complexity

more value for less risk !

ardantic
governance & security

Merci pour votre attention !

Nous restons à votre disposition pour toute questions ou informations

Pour nous contacter :
info@ardantic.ch