Insight

Back to Basics

Baseline considerations for ransomware recoverability

Protect against ransomware. Ensure recoverability. Start with the essentials.

When ransomware strikes, will your organization recover quickly? Or will it come to a screeching halt? Ongoing data protection and reliable business continuity require an airtight backup strategy and comprehensive disaster recovery plans — and it starts with strong foundational knowledge.

How familiar are you with the basics? Explore this infographic to find out.

Backups & disaster recovery: What's the difference?

Backups 101

Backups are copied data needed to ensure compliance and prevent data loss in case of:

- Data theft/ransomware
- Employee accidents
- Technical failures
- Natural disasters

Disaster Recovery 101

Disaster recovery is the plan or process for restoring operations post-incident, factoring in:

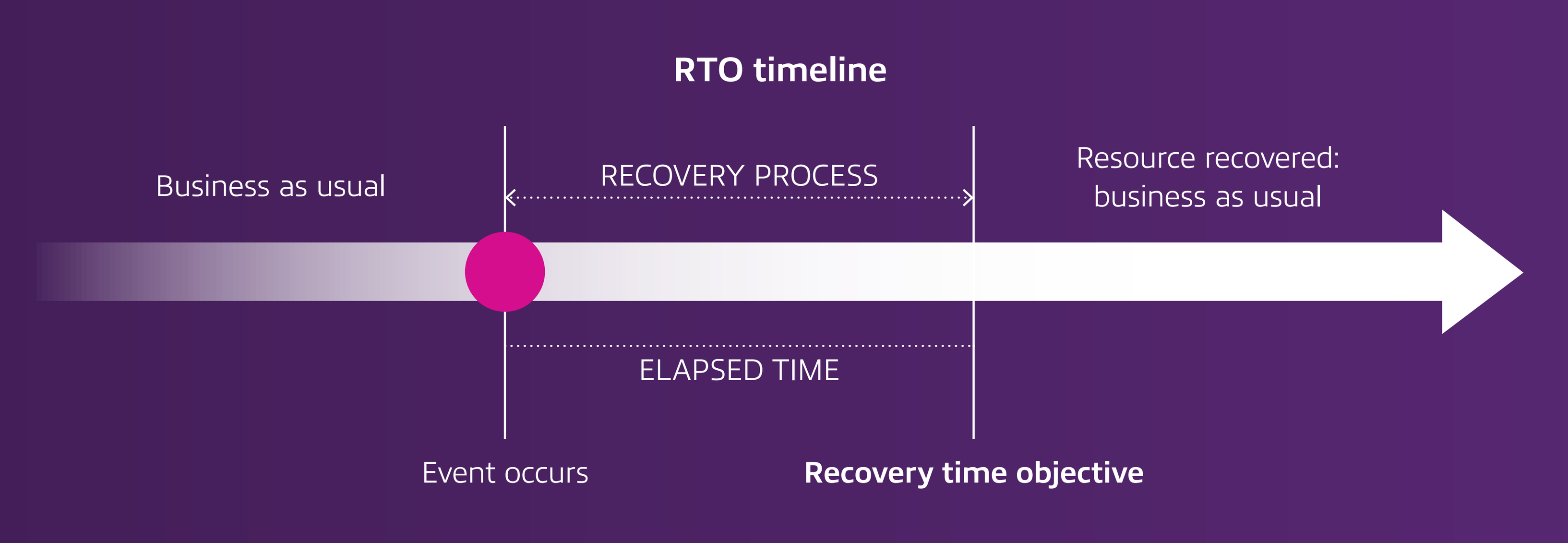
- Risk analysis
- Business impact analysis
- Recovery time objective
- Recovery point objective

Pop quiz: Test your disaster recovery vocabulary.

These are the need-to-know terms behind every good recovery strategy.

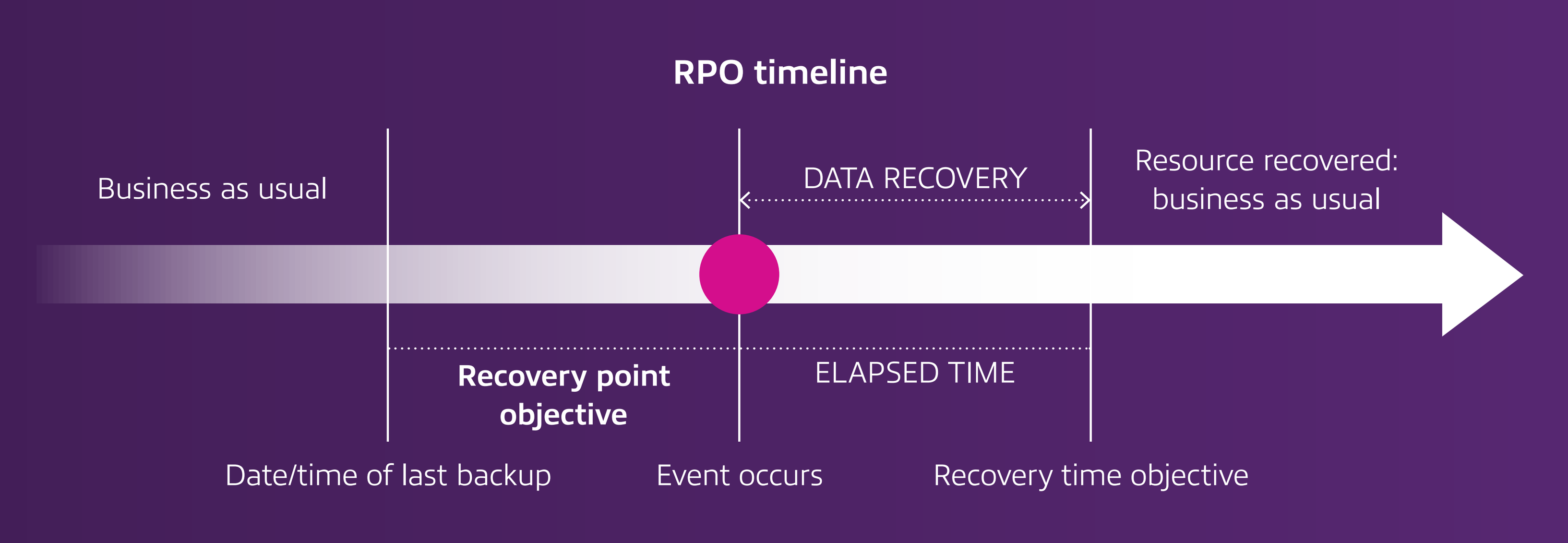
Recovery Time Objective (RTO)

The acceptable amount of time to recover normal operations post-incident



Recovery Point Objective (RPO)

The acceptable amount of data loss to occur during an incident, measured in time-based increments and corresponding to frequency of data backups



Failover

The process of automatically switching operations to backup systems during an incident

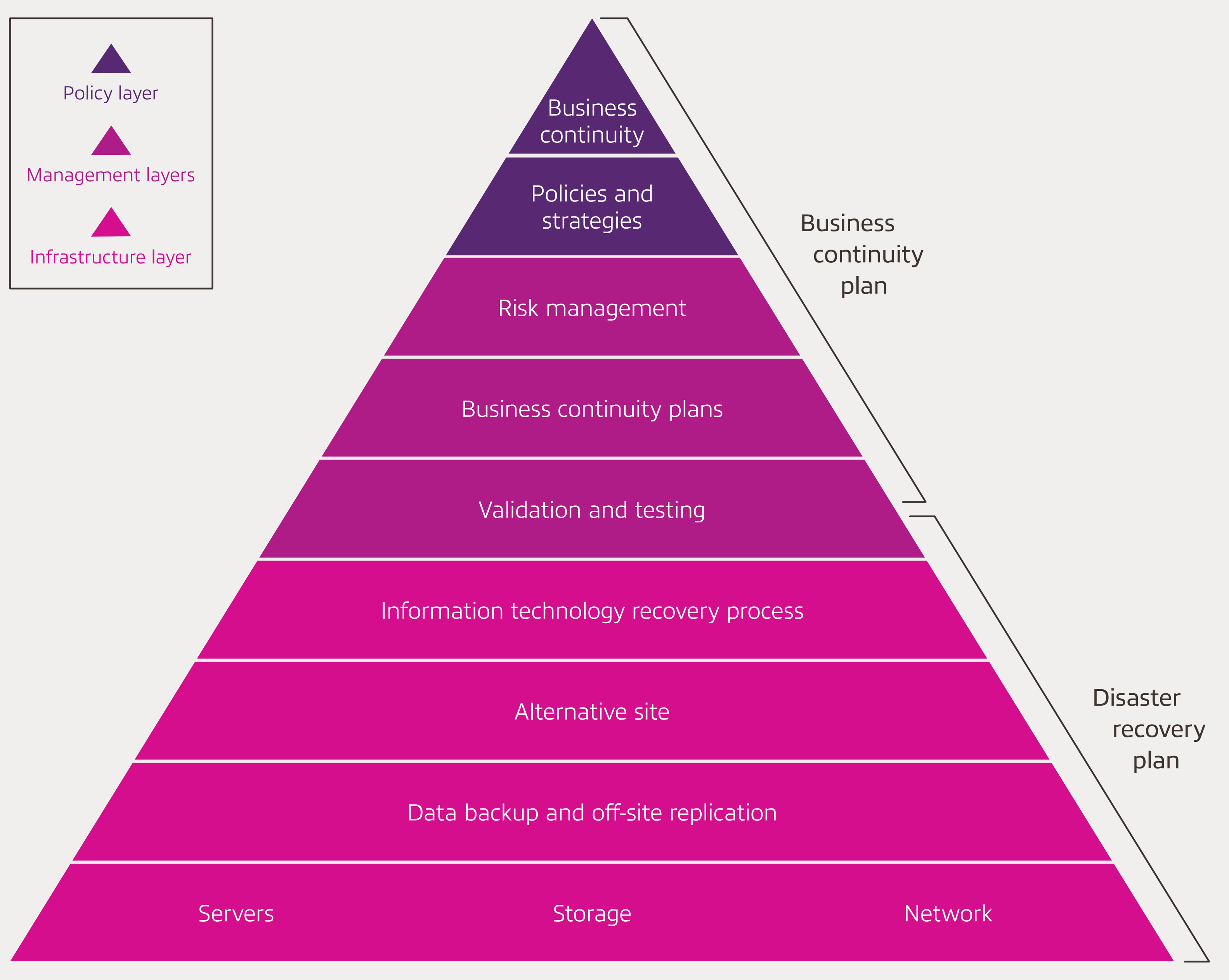
Failback

The process of switching back to the original systems post-incident

Restore

The process of moving backups from storage onto the primary system

Blueprints for building a business continuity and disaster recovery plan



Three questions to consider:

How much productive time **can you afford to lose?**

What is your **minimum backup schedule frequency?**

How will you **prioritize workload recovery?**

Determining workload priority

Risk tolerance and recovery objectives differ by workload and industry.

Critical — 0–1 hour
Example: banking transactions

Semi critical — 1–4 hours
Example: chat logs

Less critical — 4–12 hours
Example: marketing information

Infrequent — 12–24 hours
Example: product specifications

Recoverability standards and infrastructure choices

The best infrastructure for your ransomware recoverability strategy will depend on your organization's unique workloads and objectives.

Factors for consideration:

What to recover:
- Data
- Infrastructure
- Services

Where it resides:
- On-premises
- Cloud
- Multiplatform

When you need it:
- Seconds
- Minutes
- Hours

Don't forget data locality.

How close is your data to your restore location? Smart backup solutions prioritize local, immutable copies for immediate restoration post-incident.

Make sure data is **easy to move.**

Make sure data is accessible **from wherever it's needed.**

Make sure data storage **is flexible and scalable.**

Questions?

Find the answers you need for building a stronger approach to business continuity with Insight.

Sources:
Brush, K. (May 2022). Disaster Recovery Plan (DRP). TechTarget.
Mehrotra, A. (2022, Jan. 18). Disaster Recovery — A practical guide (Part 1). Medium.
Rangan, K. (2022, July 14). Why Your Business Needs Recovery Time Objective to Survive. G2.