WORKSHEET 1: SPECTRUM COMPARISON SCORING MATRIX

Score candidate recovery architectures against organizational tolerance (Score 1 = Unacceptable / Fails Need, 3 = Moderate Fit, 5 = Optimal Alignment). Selection must balance recovery speed against ongoing cost, geographic diversification, and operational complexity.

Architectural Metric	Hot Site	Warm Site	Cold Site	Cloud / DRaaS
Recovery Time (RTO) Speed to restore service	Seconds to minutes *Score (1–5): [ ]*	Hours (4–24 hrs) *Score (1–5): [ ]*	Days to weeks *Score (1–5): [ ]*	<1 min to hours (tunable) *Score (1–5): [ ]*
Recovery Point (RPO) Data loss tolerance	Near zero (real-time sync) *Score (1–5): [ ]*	Seconds to minutes (sync 4–24h) *Score (1–5): [ ]*	Backup interval (24h+) *Score (1–5): [ ]*	Seconds to minutes *Score (1–5): [ ]*
Pre-Provisioned Hardware Standing idle capacity	Full duplicate running live *Score (1–5): [ ]*	Scaled-down functional stack *Score (1–5): [ ]*	Space, power & cooling only *Score (1–5): [ ]*	On-demand compute; storage idle *Score (1–5): [ ]*
Capital & Licensing Cost Relative financial expense	Highest (5–10x cold; $200k–$500k) *Score (1–5): [ ]*	Moderate (30–60% less than hot) *Score (1–5): [ ]*	Lowest (80–90% less than hot) *Score (1–5): [ ]*	Pay-as-you-go ($50–$200/VM/mo) *Score (1–5): [ ]*
Operational Complexity Staff & sync maintenance	High: continuous sync, 24/7 staff *Score (1–5): [ ]*	Medium: periodic sync, test restore *Score (1–5): [ ]*	Low: facility contract, manual build *Score (1–5): [ ]*	Medium: cloud automation scripts *Score (1–5): [ ]*
Failover Validation ISO 22301 drillability	Automated DNS/load-balancer *Score (1–5): [ ]*	Power-up, scale-up, validate data *Score (1–5): [ ]*	Full hardware install & OS load *Score (1–5): [ ]*	Automated spin-up runbooks *Score (1–5): [ ]*
TOTAL SCORE (Sum 1–30):	**[ ] / 30**	**[ ] / 30**	**[ ] / 30**	**[ ] / 30**

CANDIDATE ARCHITECTURE EVALUATION NOTES

Recommended Architecture Class:

Lead Evaluator / Title:

Key Justification Drivers:

Assessment Date:

ISO 22301 BIA Alignment Reference:

Approved Review Date:

WORKSHEET 2: PER-FUNCTION RECOVERY TARGET DERIVATION

Work backward from the RTO and RPO each workload can tolerate, as established in your Business Impact Analysis (BIA). Match recovery investment to business impact — never buy one expensive tier for everything.

System / Function Name	Business Impact Category	Target RTO	Target RPO	Replication / Backup Cadence	Assigned Site Class	Tier Class
e.g. Payment Processing / Trading	Revenue-critical / Catastrophic	< 5 minutes	Near-zero	Continuous synchronous	Hot Site / Multi-Site Active	**Tier 1**
e.g. Clinical EHR / Emergency	Life-safety / Regulatory	< 15 minutes	Near-zero	Continuous synchronous	Hot Site / Warm Standby	**Tier 1**
e.g. Corporate Email & Collab	Operational / Bounded	4–24 hours	4–12 hours	Scheduled sync (4–12h)	Warm Site / Pilot Light	**Tier 2**
e.g. ERP (Non-Real-Time Ops)	Internal productivity	12–24 hours	12–24 hours	Scheduled sync (12–24h)	Warm Site / Pilot Light	**Tier 2**
e.g. Reporting / Analytics DB	Delayed impact	24–48 hours	24 hours	Daily backup snapshot	Cloud Cold / Backup-Restore	**Tier 3**
.....	.....	.....	.....	.....	.....	[ ]
.....	.....	.....	.....	.....	.....	[ ]
.....	.....	.....	.....	.....	.....	[ ]
.....	.....	.....	.....	.....	.....	[ ]
.....	.....	.....	.....	.....	.....	[ ]

TIER SUMMARY & DECISION RULES (FROM ARTICLE)

• **RTO in seconds to minutes, RPO near zero:** Use Hot site or Cloud Warm Standby / Multi-Site Active-Active. Reserve for revenue-critical, customer-facing, and regulated systems where downtime causes direct loss.

• **RTO of a few hours, RPO of minutes to an hour:** Warm site or Cloud Pilot-Light / Warm-Standby is the value sweet spot for important internal systems.

• **RTO of a day or more, RPO of a day:** Cold site or Cloud Backup-and-Restore is sufficient for non-critical/archival data, freeing budget for critical tiers.

WORKSHEET 3: SITE-BY-SITE GEOGRAPHIC AUDIT CHECKLIST

Recovery sites must be geographically separated to survive regional disasters — but close enough to maintain acceptable data replication latency. Use this site-by-site checklist for evaluating candidate primary and secondary locations.

Primary Site Location: .....

Candidate Recovery Site Location: .....

Geographic Dimension	Article Standard & Verification Rule	Observed Value	Pass / Fail / Action
Minimum Physical Separation	Standard minimum distance is **100–200 miles** for protection against regional natural disasters.	Distance: ..... miles	☐ PASS ☐ FAIL
Hurricane / Coastal Storm Corridor	Organizations in hurricane zones require **500+ miles** of separation across different weather tracks.	Storm corridor check:	☐ PASS ☐ FAIL ☐ N/A
Seismic / Fault Line Diversity	Must be separated across **different fault systems** / tectonic boundaries so both sites do not shake simultaneously.	Fault zone check:	☐ PASS ☐ FAIL ☐ N/A
Hydrological / Flood Plain Risk	Recovery facility must not reside in the same **flood plain** or watershed as the primary data center.	Flood zone / plain:	☐ PASS ☐ FAIL
Electrical Power Grid Separation	Must connect to a **separate regional power grid** / interconnect to survive wide-area blackouts.	Power grid / utility:	☐ PASS ☐ FAIL
Replication Network Latency	Must maintain acceptable round-trip latency. Synchronous replication requires low latency (<5–10ms); asynchronous required if distance >100mi.	Measured RTT latency: ..... ms	☐ Sync Capable ☐ Async Required
Data Sovereignty Jurisdiction	Must remain in compliant legal jurisdiction under **GDPR, HIPAA, or national data residency laws**.	Jurisdiction / Country:	☐ Fully Compliant ☐ Non-Compliant
Cloud Region / AZ Selection	Select cloud recovery regions in **different geographic zones within the same compliant country**.	Primary Region: ..... DR Region:	☐ PASS ☐ FAIL

CLOUD PROVIDER CONCENTRATION RISK AUDIT

- ☐ **Multi-Cloud Check:** Is recovery infrastructure deployed to a separate cloud provider (mitigating global provider outages like 2024 CrowdStrike)?
- ☐ **Air-Gapped Offline Backups:** Are immutable backups stored completely independent of cloud provider infrastructure?
- ☐ **Out-of-Band Runbook Access:** Are DR playbooks, network diagrams, and recovery credentials accessible without active cloud connectivity?

WORKSHEET 4: TIERED HYBRID ARCHITECTURE PLANNER

Design the tiered architecture combining physical and cloud recovery tiers. Match recovery investment to business impact by grouping applications into the article's four standard operational tiers.

System Tier	Architecture Strategy	Replication Mechanism	Failover Mechanism	Planned Testing Cadence
Tier 1 Near-zero RTO	Hot Site replication OR Cloud Active/Active	Continuous synchronous replication across high-bandwidth link	Automated DNS / Global Load Balancer failover (< 5 mins)	Bi-annual live simulated failover (ISO 22301)
Tier 2 4–24h RTO	Cloud Warm Recovery / Warm Standby	Scheduled replication (every 4–24 hours) to cloud storage	Automated cloud compute spin-up & application health checks	Annual functional recovery test
Tier 3 24–72h RTO	Cloud Cold Recovery / Daily Backups	Daily asynchronous snapshots & object storage transfer	Manual on-demand compute provisioning & database restore	Annual tabletop & sample database restore
Tier 4 72+ hours RTO	Backup restoration to on-demand cloud	Weekly/monthly archival backup snapshots	Rebuild on cloud infrastructure as resources allow	Periodic restore verification

CLOUD NATIVE DR PROVIDER SERVICE MAPPING

Cloud Provider	Target DR Service	Architecture Model Selected	Target Cloud Region
AWS	AWS Elastic Disaster Recovery (EDR) / CloudEndure	☐ Backup/Restore ☐ Pilot Light ☐ Warm Standby ☐ Active/Active	Primary: ..... DR: .....
Microsoft Azure	Azure Site Recovery (ASR)	☐ On-prem-to-Azure ☐ Azure-to-Azure ☐ Pilot Light ☐ Warm Standby	Primary: ..... DR: .....
Google Cloud (GCP)	Asynchronous PD replication / Regional Failover	☐ Persistent Disk Async ☐ Regional Failover ☐ Pilot Light ☐ Multi-Region	Primary: ..... DR: .....

FAILOVER SEQUENCING & DEPENDENCY CHAIN

Step 1 (Core Identity & Network): Active Directory / DNS / Firewall / VPN failover — Target: 0–15 mins.
Step 2 (Tier 1 Applications): Automated cutover of revenue/clinical databases and web portals — Target: 15–30 mins.
Step 3 (Tier 2 Internal Ops): Spin up warm compute instances, sync delta logs, remap internal endpoints — Target: 4–8 hours.
Step 4 (Tier 3 & 4 Back-Office): Initiate storage restores for analytics, reporting, and archives — Target: 24–48 hours.

WORKSHEET 5: DISASTER RECOVERY TOTAL COST OF OWNERSHIP (TCO)

Cost is driven by RTO and RPO, not by labels. The major cost drivers are: duplicate compute & storage, continuous-replication bandwidth, duplicate software licensing, facility or cloud egress charges, DR testing, and operational staff.

Cost Driver (from Article)	Cold Site Model	Warm Site Model	Hot Site Model	Cloud / DRaaS Model
Standby Compute & Storage	Minimal (floor space, power, offsite tape/disk)	Scaled-down infrastructure (~40–70% of prod)	Full duplicate production stack running live	Storage rates (cents/GB); compute billed only at drill/failover
Replication Bandwidth	None (batch transport or offsite backup)	Scheduled delta bandwidth (every 4–24 hours)	Continuous high-bandwidth synchronous link	Continuous asynchronous egress / transfer bandwidth
Software Licensing	Cold standby rules (often single license)	Warm standby licensing terms	Duplicate production software licensing	Mobility / pay-per-use licenses where supported
Facility / Egress Charges	Monthly facility lease & utility maintenance	Shared facility or colo rack fee	Dedicated facility lease, cooling, generator contracts	Inter-region egress charges + storage fees
DR Testing & Exercises	High labor cost to transport & load hardware	Semi-annual recovery testing labor	Quarterly/annual automated failover drills	Hourly compute fees during test drills
Dedicated Operations Staff	On-call sysadmins for manual rebuild	Secondary operations support team	24/7 engineering staff to manage dual environments	Cloud infrastructure / DevOps engineers
Benchmark Range (Article)	**Lowest (80–90% < Hot)**	**~$125,000 / year (directional)**	**$200,000–$500,000 / year**	**$50–$200/VM/mo ($500–$2k/mo SMB)**
Estimated Annual Spend:	**$ ..... / yr**	**$ ..... / yr**	**$ ..... / yr**	**$ ..... / yr**

INVESTMENT JUSTIFICATION & BIA SIGN-OFF

Selected Strategy: .....

Net Annual DR Investment: $ .....

Protected Annual Revenue / Assets: $ .....

Expected Recovery RTO / RPO: .....

IT Lead / Architect: .....

Chief Information Officer (CIO): .....

Chief Risk Officer (CRO): .....

Formal Sign-Off Date: .....