REDACTED IC SAMPLE • $42M HEALTHCARE, LAB OT & MSO BUYOUT

48-Hour M&A Cyber, Carve-Out & CapEx Holdback Memorandum

Agentless AWS/Azure Control-Plane Audit, Parent TSA Separation, Flat Lab OT Segmentation & Pre-Wire RWI Clearance

100-DAY CAPEX HOLDBACK	RWI EXCLUSION RISK	TSA & BOLT-ON RISK
$1,420,000	**<12 CTO Hrs**	**60-Day Slip**
Defensible Escrow Adjustment	Cleared via 4 Pre-Wire Fixes	Parent AD/Cloud Entanglement

REDACTED IC SAMPLE

48-Hour M&A Cyber, Carve-Out & CapEx Quantification Memorandum

Target Entity: "Project Meridian" (Multi-Site Specialty Diagnostics, MSO & Billing Platform)

Transaction: $42.0M EV / $4.8M Adj. EBITDA

Mandate: Buy-Side Exclusivity • Pre-Sign RWI, TSA Carve-Out & CapEx Validation

Footprint: 48 Hrs • Read-Only API • Zero CTO Friction

100-DAY CAPEX HOLDBACK	UNMODELED RUN-RATE OPEX	RWI UNDERWRITING	TSA EXIT & BOLT-ON
$1,420,000	**+$165,000/yr**	**Exclusion Risk**	**60-Day Slip**
Specific Escrow / Price Adj.	~$1.65M EV Impact @ 10.0x	Cleared via 4 Pre-Sign Fixes	Parent AD/Cloud Entanglement

1. EXECUTIVE INVESTMENT COMMITTEE VERDICT

BALANCE-SHEET, RWI & DAY-1 CARVE-OUT IMPACT

QuantSec Advisory executed an agentless, read-only cloud control-plane, workload, and architecture diagnostic across Project Meridian's production AWS/Azure tenants and diagnostic lab gateways. Rapid bolt-on growth and shared parent infrastructure have accumulated **$1,420,000 in unbudgeted 100-Day CapEx debt** and **$165,000/yr in unmodeled security OpEx**. Left unaddressed pre-signing, commingled parent/MSO identity stores, flat lab OT analyzer subnets, unvetted commercial AI flows, and PCI DSS 4.0 gaps will trigger a blanket **RWI cyber/HIPAA/PCI exclusion** and extend TSAs by 60+ days. We recommend a **$1.42M escrow holdback** paired with **four surgical Seller pre-close fixes (<12 CTO hrs)**.

2. EMPIRICAL RISK, TSA CARVE-OUT & CAPEX HOLDBACK MATRIX

WIZ CONTROL-PLANE & VDR TELEMETRY

RISK DOMAIN	EMPIRICAL CLOUD, AI & OT TELEMETRY FINDING	DEAL, RWI & ENGINEERING BASIS	100-DAY CAPEX
1. Parent AD / IAM Entanglement CRITICAL • DAY 1–45	14 cross-account `AdministratorAccess` roles and shared Entra ID/RDS stores commingle 2.1M ePHI records with parent MSO analytics; 9 contractor keys active >365d without MFA.	Blocks Day-1 TSA exit and violates HIPAA isolation; triggers RWI exclusion. *Basis:* Clean AWS Control Tower landing zone, IdP split & KMS separation (~1,840 hrs).	**$460,000**
2. Flat Lab OT & EOL KEVs HIGH • DAY 1–45	Diagnostic lab analyzers bridge onto flat clinic VLANs alongside EOL PostgreSQL 11 billing clusters carrying 7 unpatched CISA KEVs exposed via public ALB rules.	Acute post-close ransomware blast radius across lab operations. *Basis:* IEC 62443 OT firewall zones, DB upgrade, WAF & private routing (~1,540 hrs).	**$385,000**
3. Shadow AI & PCI DSS 4.0 CRITICAL • DAY 1–30	Cleartext LLM API keys in container env variables route unredacted intake transcripts to public endpoints without BAA; co-pay page lacks PCI 4.0 script integrity headers.	Uninsured HIPAA breach & merchant fine exposure. *Basis:* Private BAA Bedrock/Azure OpenAI, PHI tokenization proxy & PCI 4.0 isolation (~1,180 hrs).	**$295,000**
4. SIEM, Vaults & Copyleft IP HIGH • DAY 46–100	CloudTrail disabled in 2 of 4 regions; immutable Backup Vault Lock absent on primary ePHI DBs; 3 restrictive AGPLv3 copyleft libraries inside SaaS containers.	Fails RWI ransomware minimums and contaminates exit IP. *Basis:* Centralized MDR/SIEM, WORM vault locks & AGPLv3 refactoring.	**$280,000**
TOTAL EXPOSURE	**30 Toxic Attack Paths • 9 Dormant Keys • 7 CISA KEVs • Flat Lab OT • 2 Shadow AI Flows**		**$1,420,000**

3. PRE-SIGN RWI EXCLUSION CLEARANCE PROTOCOL (<12 SELLER CTO HOURS)

ZERO DEAL DELAY

PRE-WIRE CONDITION	SURGICAL TECHNICAL ACTION REQUIRED PRIOR TO CLOSING	UNDERWRITING EVIDENCE	EFFORT
CC-1: Stale Key Revocation	Deactivate all 9 dormant contractor IAM keys (>365d) and enforce FIDO2 MFA across AWS & Azure root accounts.	Updated CIEM Graph	**2.0 Hrs**
CC-2: Public Ingress Lock	Restrict public ALB & security-group ingress on PostgreSQL 11 clusters and lab gateways to VPN/bastion CIDRs.	VPC Exposure Diff	**3.0 Hrs**
CC-3: Shadow AI Halt	Rotate cleartext LLM keys into Secrets Manager and disable zero-BAA external prompt telemetry on intake forms.	Clean Secret Scan	**4.0 Hrs**
CC-4: Immutable Backups	Enable multi-region CloudTrail and activate S3 Object Lock / Backup Vault Lock (Compliance Mode) on ePHI snapshots.	AWS Vault Attestation	**2.5 Hrs**

4. POST-CLOSE 100-DAY CARVE-OUT & VALUE CREATION PLAN

Phase I — Day-1 TSA Split, OT Containment & AI/PCI Fix (Days 1–45 | $665k): Provision standalone AWS Control Tower & Entra ID tenant to exit parent TSA on schedule; enforce IEC 62443 firewall zones around lab analyzers; complete DB upgrade/KEV patching; deploy BAA AI & PCI 4.0 isolation.

Phase II — Portfolio Governance & Bolt-On Scale (Days 46–100 | $755k): Implement per-subsidiary KMS CMKs, deploy 24/7 MDR/SIEM aligned to SOC 2 Type II, and refactor 3 AGPLv3 packages—enabling M&A add-on onboarding in <14 days.

QOE PRO-FORMA OPEX

RECURRING EBITDA ADJUSTMENT	
24/7 Managed MDR / SIEM	**+$65,000/yr**
Immutable Cross-Region Vaults	**+$45,000/yr**
HIPAA-BAA AI & Enterprise SSO	**+$55,000/yr**
Total Unmodeled OpEx	**+$165,000/yr**

5. NON-INTRUSIVE 48-HOUR SPRINT EXECUTION CADENCE

ZERO AGENTS INSTALLED

SPRINT WINDOW	QUANTSEC PRINCIPAL EXECUTION ACTIVITY	TARGET CTO BURDEN
Hours 0 – 2	Target provisions standard AWS/Azure/GCP Read-Only IAM role via audited CloudFormation/Terraform template.	**15 Mins** (0 Agents)
Hours 2 – 24	Out-of-band Wiz graph & clean-room VDR inspection across CSPM, CIEM, DSPM, AI-SPM, OT ACLs, KEVs & SBOM licenses.	**0 Mins** (0 Prod Load)
Hours 24 – 48	Principal Architect modeling translating findings into IC-ready CapEx holdbacks, TSA timelines, QoE OpEx & RWI steps.	**Optional 30-Min Call**

Practice Lead: Ruben Benegas, MS, CISSP — Principal Security Architect, QuantSec Advisory (E-Comm Systems Inc., est. 1999) • Former Lead Product Cybersecurity Architect (Contract), Medtronic; Principal Security Engineer, U.S. Bank; VP & Lead Security Engineer, Wells Fargo • CISSP, CCSP, CCSK & 9 GIACs • **QuantSecAdvisory.com**