



MANAGED IT + SYSTEMS MODERNIZATION

Two-Part Proposal

Part 1: Managed IT and Security

Part 2: Crawl / Walk / Run Systems Roadmap

PREPARED FOR

Contour

PREPARED BY

Centervert

DATE

September 1, 2026

VALID THROUGH

September 30, 2026

OUR APPROACH

Build a secure, accountable IT foundation, then improve one measurable operating workflow at a time - without forcing a disruptive system replacement.

PROPOSAL OVERVIEW

Executive summary

THE CENTRAL ISSUE

Contour's primary constraint is not a lack of software. It is fragmentation: important information and responsibilities are distributed across Sage, email, the 3PL and EDI environment, HubSpot, spreadsheets, project tools, file systems, and multiple technology vendors.

Centervert proposes two coordinated but independently approvable tracks. **Part 1** establishes a responsive, documented, and secure managed IT foundation. **Part 2** improves systems and operating workflows through measured Crawl, Walk, and Run stages. Planning the tracks together prevents access, security, infrastructure, or vendor ownership from becoming blockers to process improvement.

This approach preserves Contour's existing investments and treats Sage 100 as the current operational and financial source of truth. It does not assume an ERP replacement, AWS migration, autonomous AI, phone-system change, or universal custom platform. Each major decision is released only after its technical, operational, security, and commercial prerequisites are verified.

Proposed engagement

Part 1 - Managed IT	Part 2 - Systems roadmap
Responsive service desk for Windows and Mac users	Crawl blueprint for systems, workflows, interfaces, governance, and measurements
Endpoint, network, identity, procurement, and vendor coordination	Walk pilot for one human-supervised operating workflow
Documented onboarding, ownership, escalation, and lifecycle management	Run production expansion only after a successful, accepted pilot
Cloud-readiness checkpoint without an assumed migration	Separate managed-solution care after production deployment

What success looks like

- Employees have one accountable support path and unresolved issues are actively owned through resolution or vendor handoff.
- Contour has a verified record of users, devices, servers, accounts, network components, vendors, backups, and responsibilities.
- One high-value workflow is measured, prototyped, and proven before Contour approves production automation.
- Customer messages, product claims, Sage writes, credits, warranty actions, and ambiguous orders remain under defined human control.
- Technology decisions are sequenced by business value, readiness, risk, and staff capacity rather than by a big-bang replacement plan.

COMMERCIAL SUMMARY

Investment and decision structure

The firm authorization is intentionally limited to work that can be responsibly scoped from the current evidence. Walk and Run are planning ranges, not implementation commitments, until the Crawl blueprint establishes interfaces, baselines, ownership, and acceptance criteria.

Recommended authorization now

Offering	Investment	Commercial treatment	Outcome
Managed IT and security	\$125 / managed user endpoint / month	14 preliminary endpoints = \$1,750/month	Support, Centervert management and security stack, phishing protection, lifecycle administration, reporting, and planning
Crawl systems blueprint	\$14,500 one time	Fixed	Two-workflow discovery, interface validation, governance, architecture, roadmap, and fixed Walk SOW

\$35,500

Known first-year base if endpoint MSP and Part 2 Crawl are both approved

Includes 14 managed user endpoints for twelve months (\$21,000) and the \$14,500 Crawl blueprint. Server and backup services, taxes, hardware, client-owned subscriptions, travel, network modernization, cloud migration, Walk, and Run are additional.

Optional and future authorizations

Item	Budget	Status
Unified UniFi network enhancement	\$9,500 not-to-exceed	Optional one-time project pending onsite port, cabling, rack, VPN, PoE, and RF validation
Five servers and backup services	Separate quote	Requires server roles, storage, retention, recovery objectives, and existing-backup validation
Walk - one controlled pilot	\$35,000-\$55,000	Budgetary range; final SOW issued after Crawl
Run - production hardening and expansion	\$65,000-\$125,000	Budgetary range; separate approval after Walk
Managed solution care	\$3,500-\$6,000 / month	Optional only after a production solution exists

EVIDENCE BOUNDARY

Confirmed needs and preliminary inventory are the proposal basis. Centervert recommendations are proposed scope. Unverified system details, savings, interfaces, cloud architecture, automation percentages, and implementation dates are not treated as approved facts.

PART 1

Managed IT, Security and Cloud Readiness

A responsive and documented support foundation that operates independently of any custom software or AI initiative.

Objectives

- Create clear ownership of devices, servers, accounts, vendors, security controls, backups, and support responsibilities.
- Improve day-to-day support for office and remote Windows and macOS users.
- Standardize onboarding, role changes, offboarding, approvals, and vendor coordination.
- Preserve strong security and recovery practices while enabling governed modernization.
- Assess cloud suitability for Sage and other workloads before recommending a migration.
- Provide the access, identity, endpoint, network, and documentation foundation required by Part 2.

Covered-environment baseline

Pricing is based on the preliminary environment described during the August 28 discovery meeting. Counts, ownership, compatibility, and licensing will be reconciled during onboarding. A material variance will be documented and approved before pricing changes.

Area	Preliminary baseline
Managed user endpoints	14 primary company-owned Windows or macOS workstations or laptops at \$125 each per month; approved mobile email and MFA access do not create another endpoint charge
Servers	Five servers were reported; administration, server security, backup appliances, storage, retention, and recovery services require a separate assessment and quote
Location	One Charlotte office plus the identified remote-user footprint
Identity	Microsoft 365 and Duo, subject to tenant, license, and administrative-access review
Network	SonicWall firewall, NetExtender VPN, Cisco Catalyst switching, and UniFi wireless with a first-generation Cloud Key
Business systems	Sage 100 supported at the application level by ASI; Zoom Phone and other applications remain under current vendors unless separately changed

\$125 MANAGED USER ENDPOINT MODEL

A billable managed user endpoint is the employee's primary company-owned desktop or laptop enrolled in Centervert's management and security platform. Shared computers and additional workstations are billed when enrolled; reasonable support for that user's approved mobile email and MFA access is included.

PART 1 SCOPE

Managed service scope

Service desk and end-user support

- Unlimited reasonable remote support for covered incidents and routine requests during standard support hours.
- Support for supported versions of Windows and macOS, Microsoft 365, Duo, approved browsers, VPN access, printers, connectivity, and common office applications.
- Remote-user assistance for company-managed devices and reasonable support for approved mobile email and MFA enrollment.
- Ticket ownership through resolution or documented handoff to the responsible vendor, with status updates and escalation.
- Coordination with ASI, Microsoft, the ISP, Zoom, hardware vendors, and other approved providers when they must act.

Device and network management; server assessment

- Remote monitoring and management of covered user endpoints; server monitoring begins under the separately approved server and backup scope.
- Operating-system and supported third-party application patching on covered endpoints and any separately authorized servers.
- Endpoint, operating-system, warranty, lifecycle, assignment, and support-status tracking.
- Server, storage, backup, retention, and recovery requirements assessed and quoted separately after technical validation.
- Administration of covered firewall, switching, Wi-Fi, and VPN services where valid access and vendor support are available.
- Configuration backup for supported network devices where technically available.
- Current network overview, critical dependency map, vendor directory, and ownership record.

Identity, access and employee lifecycle

- Microsoft 365 and Duo administration through approved named administrative accounts.
- Role-based onboarding, role-change, and offboarding checklists.
- Provisioning and deprovisioning for systems within Centervert's administrative control, with vendor coordination where direct access is unavailable.
- Mailbox, shared-mailbox, distribution-list, group, and privileged-access administration.
- Secure administrative credential custody, with Contour retaining ownership and authorized access.
- A role-based hardware standard covering the approved computer, monitor, dock, accessories, warranty, and required applications.
- A new-hire ticket workflow capturing the employee, role, manager, start date, required applications, approvals, and shipping destination.
- After purchase approval, procurement, staging, security enrollment, standard application setup, and shipment of the device ready for first sign-in.

Standard procurement coordination and device preparation are included for covered employees when the approved standard and lead time are followed. Hardware, warranties, taxes, shipping, expedited fulfillment, nonstandard applications, data migration, and onsite placement are additional.

Backup assessment and recovery readiness

- Inventory existing backup jobs, destinations, retention, dependencies, protected capacity, and responsible vendors during service activation.
- Document recovery procedures, gaps, current restore-test evidence, and named owners.
- Define recovery-point, recovery-time, retention, and restore-testing requirements for the separate server and backup quote.
- Begin ongoing backup monitoring, remediation, storage, and representative restore validation only after Contour approves that separate scope.

New backup appliances, cloud storage, immutable retention, and full disaster-recovery testing are not included until protected capacity and recovery requirements are sized.

Planning and governance

- Monthly service reporting and quarterly technology reviews.
- A maintained 90-day action plan and longer-term technology roadmap.
- Lifecycle, renewal, security, recovery, and modernization budget planning.
- Coordination with Part 2 without combining the commercial scope of MSP and custom systems work.

OPERATIONS MODEL

Security, service levels and onsite support

Proposed management and security stack

The \$125 endpoint rate includes Centervert's standard management and security technology licenses and the services required to operate them. Centervert may replace a named product with an equivalent supported tool during the agreement term. Deployment remains subject to compatibility testing and a controlled transition from incumbent tools.

Control area	Included approach	Boundary
Monitoring and patching	Centervert-standard RMM and patch-management platform; Datto RMM or equivalent	Included for covered user endpoints
Endpoint security	Managed endpoint detection and response; SentinelOne or equivalent	Included; no promise that every incident can be prevented
Email, web and phishing protection	Applicable TitanHQ services or equivalent, including the Centervert-standard phishing controls	Included stack licenses; tenant compatibility and configuration must be verified
Identity	Microsoft 365 and Duo administration; MFA and privileged-access review	Existing subscription fees remain Contour's responsibility
Network security	SonicWall and VPN administration subject to model, licensing, warranty, and supportability	Hardware replacement and redesign are projects
Backup	Inventory and document the verified existing platform during service activation	Ongoing monitoring, remediation, appliances, storage, retention, and recovery tests require the separate server/backup quote

Support hours and response targets

Standard support hours are 8:00 a.m.-6:00 p.m. Eastern Time, Monday through Friday, excluding published holidays. Monitoring operates continuously. Priority 1 emergency intake and remote triage are available outside standard hours.

Priority	Example	Initial response target
P1 - Critical	Active security incident, complete office outage, or core system unavailable to substantially all users	30 minutes; 24/7 remote triage
P2 - High	Multiple users materially impaired or a critical function significantly degraded	2 business hours
P3 - Normal	Single-user incident with a workaround or ordinary application/device issue	4 business hours
P4 - Request	New account, planned change, information request, or non-urgent enhancement	1 business day

Targets measure acknowledgement and active triage, not guaranteed resolution. The SLA clock pauses while Centervert awaits required access, information, approval, client availability, vendor action, or equipment.

Onsite-service policy

REMOTE-FIRST WITH CHARLOTTE DISPATCH AVAILABLE

When Centervert determines that a covered issue cannot reasonably be resolved remotely, a Greenville-based technician may be scheduled to assist at Contour's Charlotte office. Covered MSP support labor remains included; the associated travel cost is additional and will be approved before dispatch.

- There is no bundled monthly onsite block; visits are scheduled when remote resolution is not practical or Contour requests approved onsite assistance.
- Travel may include mileage, travel time, parking, tolls, lodging, or third-party dispatch when applicable; the charge is disclosed before scheduling.
- Network installation, cabling, equipment placement, office moves, mass deployment, server migration, after-hours changes, and major remediation are separately scoped project work.

TRANSITION

Onboarding, cutover and stabilization

Standard managed-service activation is included in the recurring endpoint rate; there is no separate onboarding fee. The target is a controlled 30-day technical transition followed by a 60-day stabilization period. The schedule depends on access, incumbent-provider cooperation, license ownership, and compatibility between management and security tools. Material inherited remediation and replacement work will be presented separately for approval.

1. **Access and verification.** Confirm authorized decision-makers; reconcile inventory; document users, devices, servers, network equipment, vendors, licenses, administrative accounts, Sage dependencies, backups, remote access, and open issues.
2. **Parallel deployment and baseline.** Check for tool conflicts; deploy approved monitoring and security controls; baseline patching, endpoint coverage, backup status, network access, supportability, lifecycle risk, and single points of failure.
3. **Controlled cutover.** Test monitoring, ticketing, endpoint protection, backup alerts, and escalation; remove incumbent tools only after continuity is confirmed and Contour approves cutover; transfer vendor relationships and administrative access.

4. **Stabilization.** Resolve or separately scope priority inherited issues; finalize lifecycle and employee-access standards; validate reporting; and deliver a 30/60/90-day infrastructure, recovery, and cloud-readiness roadmap.

Onboarding deliverables

- Verified asset, user, server, network, account, license, and vendor records, with unresolved discrepancies identified.
- Administrative ownership and credential-custody matrix.
- Network and critical-dependency overview.
- Patch, endpoint-security, backup, supportability, and lifecycle baseline.
- Support portal, escalation path, severity process, and primary contacts.
- Role-based onboarding and offboarding checklist.
- Open-issues register and prioritized 30/60/90-day remediation plan.
- Preliminary cloud-readiness record for each server and critical workload.

Acceptance criteria

1. At least 95% of supported, reachable managed devices have approved monitoring and endpoint-security controls active; every exception is documented.
2. Known in-scope users, devices, servers, network equipment, and vendors are recorded.
3. Named administrative accounts and secure credential custody exist for each managed system.
4. Patch, endpoint-security, backup, and critical infrastructure risks are baselined.
5. The support portal and Priority 1 escalation process are tested with designated Contour contacts.
6. Contour receives the environment record, responsibility matrix, employee-lifecycle checklist, open-issues register, and 30/60/90-day plan.
7. The incumbent provider's overlapping tools are removed or excepted only after Contour approves cutover.

CHANGE PROTECTION

Centervert will not migrate Sage, relocate servers, remove working security controls, or make a material production change without an approved change plan, maintenance window, and rollback procedure.

PART 1 COMMERCIAL TERMS

Managed IT investment and infrastructure options

Service	Fee	Notes
Managed IT and security	\$125 / managed user endpoint / month	Preliminary 14-endpoint quantity = \$1,750/month; billed monthly in advance
Standard service activation	Included	Inventory validation, supported stack deployment, support activation, and transition documentation
Additional managed endpoint	\$125 / month	Added when an additional workstation or shared computer is enrolled

Service	Fee	Notes
Five servers and backup environment	Separate quote	Depends on server roles, protected capacity, retention, recovery objectives, and existing design
Charlotte onsite travel	Quoted before dispatch	Covered MSP support labor remains included; travel cost is additional

Billing begins when Centervert starts deploying the management and security stack to the authorized endpoints. The verified active-endpoint count is reconciled during service activation and adjusted as endpoints are added or retired. Centervert's standard management, endpoint-security, and phishing stack licenses are included while the MSP agreement remains active. Hardware, taxes, shipping, client-owned subscriptions, server/backup services, travel, and separately authorized projects are additional.

Optional unified UniFi network enhancement

\$9,500

NTE

One-time optional replacement of the mixed-vendor network with a centrally managed UniFi environment

Includes the assumed hardware and core-equipment allowance, onsite validation, final design, procurement, staging, installation, migration, testing, documentation, Greenville-Charlotte project travel, and one coordinated cutover. Acceptance of this project is not required to approve the MSP service.

Planning component	Allowance
Cloud gateway / security appliance	One UniFi Dream Machine Pro Max or appropriately sized current equivalent
Switching	Up to 48 centrally managed ports using one 24-port PoE switch and one 24-port expansion switch
Wireless	Up to four Wi-Fi 7 access points; final models, quantity, and placement set by onsite RF validation
Resilience and accessories	Rack UPS or equivalent, power distribution, 10 Gb interconnects, patching, labeling, mounts, and core-equipment coverage allowance
Professional services	Assessment, design, staging, firewall/VPN and VLAN migration, installation, cutover, testing, rollback plan, network diagram, and administrative handoff

The NTE assumes no more than 48 active switch ports and four access points, reusable structured cabling except for minor corrective work, adequate rack power and space, and standard firewall/VPN requirements. Extensive cabling, conduit, firestopping, electrical work, lift rental, ISP changes, camera/access-control/phone replacement, specialized compliance controls, additional ports or APs, server migration, and additional cutover visits require a written change order. If onsite validation materially changes the assumptions, Centervert will issue a revised quote before equipment is ordered.

PART 2

Crawl / Walk / Run Systems Roadmap

Reduce operating friction by connecting approved information and introducing automation through measurable, human-controlled stages.

The roadmap begins with Contour's confirmed operating problems: inconsistent order intake, manual Sage-to-3PL reconciliation, email-dependent customer service, weak reporting, scattered product-development information, and limited internal capacity for a large transformation.

Delivery principles

- Start with read-only access and human-assisted work before allowing system writes.
- Integrate existing systems where practical before considering replacement.
- Measure current performance before claiming time savings or automation percentages.
- Use least-privilege access, role-based permissions, auditable actions, and tested rollback.
- Treat inbound email and attachments as untrusted content.
- Require human approval for customer messages, product claims, pricing, credits, warranty decisions, and Sage transactions during early stages.
- Release each stage only after Contour accepts the prior stage's evidence and results.

Three-stage roadmap

CRAWL	WALK	RUN
Discover and design	Prove one workflow	Operationalize and scale
4-6 weeks	8-12 weeks	3-6 months
\$14,500 fixed	\$35,000-\$55,000 planning range	\$65,000-\$125,000 planning range
Two workflows, interfaces, governance, baselines, architecture, roadmap	One human-supervised pilot in shadow or draft mode	Production hardening, approved integrations, monitoring, and selected additional capabilities
Gate: approve a fixed Walk SOW	Gate: approve production authority	Gate: accept sustained performance and ongoing care

SYSTEM-OF-RECORD POSITION

Sage 100 remains the current operational and financial source of truth. This proposal does not assume an ERP replacement, custom ERP, AWS migration, autonomous AI deployment, or a universal connector layer.

PART 2 - STAGE 1

Crawl: Systems and workflow blueprint

\$14,500

Fixed discovery and design engagement

Proposed duration: 4-6 weeks. Delivers a build-ready roadmap and fixed Walk statement of work; no production software or migration is included.

Bounded scope

- No more than eight stakeholder working sessions, designed to minimize disruption to Contour's lean team.
- Deep review of two workflows: incoming order processing and Sage-to-3PL exception reconciliation.
- One normal and one exception example for each workflow, with additional anonymized samples used where Contour can provide them.
- Verification of Sage version, modules, customizations, licensing, database, supported import/export or API methods, and ASI's required role.
- Identification of the exact Fosdick warehouse platform, SPS/EDI document path, interface ownership, vendor permissions, testing process, and likely change fees.
- Current volumes, touches, handling time, delays, errors, rework, escalation, and response baselines.
- Authoritative ownership of customer, product, SKU, pricing, order, shipment, policy, document, and reporting information.
- Data classification, human-review rules, security controls, and AI-vendor requirements.
- Build-versus-buy analysis and sequencing by value, feasibility, risk, data readiness, and staff effort.

Deliverables

Deliverable	Purpose
Verified systems and ownership map	Identifies what exists, who owns it, what is authoritative, and where access or responsibility is unclear
Current-state workflow diagrams	Shows normal and exception paths, handoffs, duplicate entry, delays, and control points
Interface and vendor-dependency matrix	Separates supported interfaces from assumptions and assigns required vendor action
Data and AI governance framework	Defines allowed data, accounts, retention, logging, human gates, and incident shutdown
Baseline and success-measure plan	Creates measurable criteria for any later value or automation claim
Prioritized 12-month roadmap	Sequences improvements by value, feasibility, risk, and Contour capacity
Architecture recommendation	Documents the proposed data flow, integration pattern, access model, hosting options, and operational controls
Fixed Walk SOW	Defines one selected pilot, test data, acceptance criteria, schedule, price, ownership, and exclusions

Crawl acceptance gate

1. Contour's designated owners approve the system and workflow maps.
2. Required interfaces, vendors, permissions, and data-access paths are documented.

3. Baseline measures and pilot success criteria are agreed.
4. Human-review, product-claim, customer-communication, and data-use rules are approved.
5. Contour selects one first pilot and authorizes a separate fixed Walk SOW.

PART 2 - STAGE 2

Walk: One controlled pilot

\$35k-\$55k

Budgetary range for one pilot

Proposed duration: 8-12 weeks after Crawl. Final scope, fixed price, test set, security controls, timeline, and acceptance criteria come from the approved Crawl deliverables.

Contour will select one pilot. The pilot begins in shadow or draft mode: it may read approved data, interpret information, flag uncertainty, and prepare staff work, but it will not autonomously send customer communications or post production transactions.

Pilot option A: assisted order intake

- Monitor one approved order mailbox and one defined order category.
- Read common order emails and purchase-order attachments.
- Extract customer, PO, SKU, customer item number, quantity, unit or case designation, requested date, addresses, and special instructions.
- Match information against approved customer and product sources.
- Identify missing, conflicting, duplicate, or low-confidence information rather than guessing.
- Draft a clarification request and present it for staff approval.
- Prepare a structured review package or import-ready draft without posting directly to Sage.

Pilot option B: Sage-to-3PL exception reconciliation

- Ingest approved read-only Sage and 3PL order or shipment data through supported exports or interfaces.
- Normalize identifiers and order or shipment status.
- Detect missing, rejected, late, mismatched, partially shipped, or unshipped orders.
- Present only true exceptions to the responsible employee.
- Preserve the source data, comparison result, assignment, disposition, and audit history.

Walk deliverables and gate

- Secure development and test environment with role-based access.
- Working pilot and staff review interface.
- Audit, error, and operational logs.
- Test evidence using an approved historical dataset.
- User-acceptance session, training, and operating documentation.
- Performance report comparing pilot results with the Crawl baseline.
- Productionization recommendation, operating cost, support plan, and fixed Run SOW.

RELEASE CONDITION

The pilot must surface uncertainty, meet agreed test thresholds, complete user acceptance, and record zero unapproved customer messages or production writes before Contour considers Run.

PART 2 - STAGE 3

Run: Production hardening and expansion

**\$65k-
\$125k**

Budgetary production range

Proposed duration: 3-6 months after an accepted Walk. Final scope depends on selected modules, vendor interfaces, production authority, data quality, and operating requirements.

Run is not a commitment to replace Contour's systems. It is the stage where proven workflows may receive production-grade integrations, monitoring, recovery, controlled write authority, and selected additional capabilities.

Potential Run capabilities

- Production integrations, authentication, role-based access, monitoring, alerting, audit trails, duplicate prevention, and tested rollback.
- Controlled Sage staging or supported imports and daily 3PL exception operations.
- Straight-through processing for narrowly defined, low-risk order categories, with people handling exceptions.
- Governed customer-service drafting from approved product, policy, warranty, shipping, and order information, with source references and immediate escalation.
- Approved external messages or system writes only under explicit rules and release authority.
- Operational reporting for incoming orders, pending items, exceptions, response times, and resolution history.
- Shared metric and data definitions and controlled reporting refreshes.
- Role-based search across approved product-development, customer, sales, and document information without forcing every asset into Sage.
- Data-quality preparation for demand forecasting and inventory-planning recommendations.
- Formal evaluation of longer-term platform consolidation or ERP replacement only if evidence supports it.

Human-control boundary

Product claims, unusual pricing, credits, refunds, warranty decisions, high-value transactions, and ambiguous orders retain human approval unless Contour explicitly approves a narrower, tested rule set. The system must stop safely when source data, confidence, permissions, or dependencies are insufficient.

Optional managed solution care

Service	Included operating support
Monitoring and recovery	Workflow and integration monitoring, failure investigation, replay, alerting, and incident coordination
Security and dependencies	Access review, dependency maintenance, vendor-interface change management, and protective-control updates
Knowledge and policy	Approved knowledge-source updates, policy changes, evaluation sets, and controlled release management
Performance and roadmap	Usage and performance reporting, minor monthly improvements, and quarterly roadmap review

\$3.5k-
\$6k/mo

Managed solution care planning range

Separate from endpoint, network, and help-desk MSP coverage. Cloud, AI-model, vendor, and software usage fees are additional.

PROGRAM CONTROLS

Governance, engineering and measurement

Data and responsible-AI controls

- Approved business accounts, AI vendors, data-retention and model-training terms, deletion procedures, and access owners.
- Classification rules for customer, employee, financial, payment, confidential, potentially health-related, and product-claims information.
- Least-privilege access, role-based permissions, named administrators, and audit-log retention.
- Human-approval thresholds for messages, transactions, pricing, product claims, credits, warranties, and exceptions.
- Controls against malicious attachments, prompt injection, data exfiltration, duplicate actions, and unauthorized system writes.
- Incident shutdown, manual fallback, replay, recovery, and rollback procedures.
- Named business and technical owners for every production workflow.

Engineering and handoff standards

- Documented architecture and data flow.
- Development, test, and production separation.
- Version-controlled source, configuration, and deployment records.
- Vendor-supported APIs, EDI, SFTP, imports, or exports wherever practical.
- Automated tests, approved evaluation sets, and user-acceptance evidence.
- Monitoring, error handling, audit trails, deployment instructions, and rollback steps.
- Administrator and end-user documentation, training, and operational handoff.
- Explicit ownership, licensing, hosting, portability, and termination provisions in each implementation SOW.

Measurement framework

Outcome area	Recommended measures
Order intake	Median handling time, touches, clarification rate, correction/rework rate, duplicate rate, and unresolved-order age
Fulfillment reconciliation	Comparison time, true exception count, exception age, false-positive rate, and resolution time
Customer service	First-response time, draft acceptance, human escalation, unresolved cases, and incorrect or unauthorized messages
Reporting and knowledge	Report preparation time, data freshness, definition consistency, search success, and staff adoption
Safety	Unauthorized customer messages or system writes; target is zero

NO PREMATURE GUARANTEE

Centervert will not guarantee an automation percentage, savings amount, forecast accuracy, staffing reduction, or throughput improvement before Contour approves the baseline and a controlled pilot demonstrates the result.

ENGAGEMENT BOUNDARIES

Responsibilities, assumptions and exclusions

Contour responsibilities

- Name an executive sponsor, authorized commercial contact, emergency contact, and one operational owner per selected workflow.
- Provide accurate inventory, contracts, administrative access, licensing, vendor contacts, and the incumbent MSP's transition information.
- Secure cooperation from the incumbent MSP, ASI, SPS Commerce, Fosdick, and other required vendors, including their fees and schedules.
- Supply representative anonymized orders, exceptions, customer-service examples, policies, product data, SKU mappings, pricing, warranty rules, and approved claims.
- Identify regulated, financial, customer, employee, payment, confidential, and product-claims data and applicable obligations.
- Participate in testing and provide consolidated decisions or feedback within five business days.
- Approve every production communication and system-write permission before release.
- Maintain supported hardware, connectivity, subscriptions, application licenses, and cyber insurance.
- Notify Centervert before material system, workflow, staffing, vendor, or facility changes.

Key assumptions

- The preliminary baseline of 14 billable managed user workstations and five separately scoped servers is materially accurate.
- Valid administrative access and vendor cooperation can be obtained within the transition schedule.
- Sage remains the current source of truth unless a later decision changes it.

- Contour will provide lawful authority to access and use the approved data supplied for support, discovery, testing, and implementation.
- Work occurs remotely or during standard business hours unless otherwise approved.
- Client or vendor delays extend the schedule without placing Centervert in default.
- A supported interface or approved export path must exist before any production integration is committed.

Exclusions unless specifically authorized

- Microsoft 365, Duo, Sage, ISP, backup appliance/storage, cloud, AI, vendor, and other client-owned subscriptions or usage fees not expressly listed; Centervert's standard endpoint management, security, and phishing stack is included while the MSP agreement is active.
- Hardware, shipping, taxes, warranties, cabling, electrical work, ceiling repair, lift rental, construction, and permits except for allowances expressly included in the optional network-enhancement quote.
- Sage accounting support, customization, upgrades, ERP programming, EDI-map development, and vendor professional services.
- Cloud migration, server relocation, application replacement, tenant consolidation, office moves, and new-site deployment.
- Data migration, extensive cleanup, historical reconciliation, file migration, custom ERP, phone replacement, and a universal integration layer.
- Printer hardware repair, consumables, manufacturer depot work, and unsupported or end-of-life systems.
- Large-scale incident recovery, digital forensics, legal response, breach notification, cyber-insurance claims, compliance certification, and legal advice.
- Guaranteed Wi-Fi coverage before onsite RF and cable validation.
- Autonomous customer responses, product claims, refunds, credits, warranty decisions, or Sage writes without an approved release gate.

COMMERCIAL FRAMEWORK

Terms, change control and ownership

Commercial terms

Term	Proposed treatment
Proposal validity	Through September 30, 2026
MSP term	12 months beginning at managed-service go-live; month-to-month thereafter; 60-day non-renewal notice
MSP billing	\$125 per active managed user endpoint, monthly in advance; preliminary quantity 14; standard service activation included
Crawl billing	50% at authorization, 30% after workshops and access review, 20% at final delivery
Walk / Run billing	Milestone schedule in separate fixed SOWs
Hardware and third parties	Written approval required; costs may be due before procurement; taxes, shipping, usage, vendor fees, and price changes passed through unless included in a fixed project allowance
Deliverable review	Five business days for consolidated acceptance feedback; written defects are corrected, enhancements are changes
Annual MSP adjustment	After the initial term, the greater of 3% or documented increase in included third-party licensing, with advance notice

Change control

- Additional work begins only after a written change order identifies the added scope, price, schedule, assumptions, and acceptance impact.
- A material variance in endpoints, servers, locations, workloads, data, interfaces, compliance duties, or support demand may require a scope and price adjustment.
- Client or vendor delays, unavailable access, unsupported interfaces, inaccurate records, and changed requirements extend the schedule and may create additional cost.
- Project defects against written acceptance criteria are corrected during the defined stabilization period. New features, changed criteria, and new source data are change requests.

Data, credentials and intellectual property

- Contour retains ownership of its accounts, credentials, data, configurations, and client-specific paid deliverables.
- Centervert will use client-owned vendor accounts where commercially available and will not intentionally create avoidable lock-in.
- Centervert retains ownership of its pre-existing tools, reusable frameworks, methods, templates, libraries, and general know-how.
- Each implementation SOW will identify any third-party or open-source components, client-specific source delivery, hosting, licensing, portability, and exit obligations.
- At termination, Centervert will provide Contour-owned documentation, credentials, and reasonable transition cooperation. Extended transition labor may be separately billed.

The final MSA, data-processing terms, confidentiality language, warranties, liability limits, insurance, and legal remedies should receive legal review. This proposal summarizes commercial scope and does not replace those agreements.

APPROVAL

Recommended next steps

1. Confirm the 14 managed-user-endpoint baseline and complete the separate five-server and backup assessment.
2. Authorize Part 1 endpoint managed service and, if approved, start the Part 2 Crawl blueprint concurrently.
3. Schedule the inventory, administrative-access, vendor, and optional unified-network site-validation handoffs.
4. Name the executive sponsor and the operational owners for order intake and Sage-to-3PL reconciliation.

Authorization selections

Initial	Service	Investment
	Part 1 - Managed IT and security for 14 managed user endpoints	\$1,750/month (14 x \$125)
	Part 2 - Crawl systems and workflow blueprint	\$14,500 fixed
	Optional unified UniFi network enhancement	\$9,500 NTE

Accepted for Contour

Authorized representative	Title	Signature	Date
---------------------------	-------	-----------	------

APPENDIX

Proposal basis and open verification items

Preliminary current environment

Area	Current understanding	Status
Business	Lean Charlotte-based team with remote employees; contract manufacturing and third-party fulfillment	Confirmed in meeting
ERP	Sage 100 is the operational and financial source of truth; ASI is the reseller	Confirmed; version and interfaces unknown
Order / fulfillment	SPS Commerce and EDI connect to Fosdick; the warehouse-platform name may be Depasco	System name and technical path unverified
Sales / marketing	HubSpot, Shopify, Amazon, ClickUp, Dropbox, Google Docs, Excel, Power BI, and other tools hold related context	Use and ownership require inventory validation
IT	Approximately 14 workstations and five servers with Microsoft 365, Duo, SonicWall, NetExtender, Cisco switching, and UniFi wireless	Preliminary call-time inventory
Wi-Fi	Conference-room coverage remains unresolved; floor plan shows a rear area labeled warehouse but no conference room	Onsite validation required

Items required before implementation pricing

- Actual user, device, server, mailbox, shared-device, remote-user, and application counts.
- Current MSP agreement, monthly cost, notice, SLA, ticket history, administrative ownership, tool stack, and transition obligations.
- Server roles, models, operating systems, warranties, utilization, storage, workload dependencies, backup platform, retention, immutability, restore tests, RPO, and RTO.
- Sage version, modules, customizations, licensing, database, supported interfaces, test environment, and ASI's scope and fees.
- Exact Fosdick warehouse platform, SPS/EDI maps and acknowledgements, interface methods, ownership, vendor cooperation, testing, and change fees.
- Representative normal and exception orders, customer-service examples, volumes, time, errors, approved product/SKU/policy sources, and escalation rules.
- AI data-use, retention, logging, training, deletion, approval, incident-response, and compliance requirements; named approvers, workflow owners, budget direction, timing, and decision process.

Human-readable sources

- Contour x Centervert discovery meeting, August 28, 2026, approximately 80 minutes; preserved transcript and verified debrief.
- Contour IT Discovery & Roadmap agenda email supplied before the meeting; systems not substantively re-confirmed remain email-reported until inventory validation.
- CLT Logistics, 3400 IAD, Suite 900 architectural plans dated July 2024; used only as a preliminary Wi-Fi geometry reference.
- Ubiquiti official Dream Machine Pro Max, Pro Max and Standard switching, U7 wireless, and vintage/legacy-product documentation accessed September 1, 2026; product availability and pricing remain subject to vendor change.