

Coordinate a critical enterprise customer escalation for a fictional B2B SaaS provider. A customer with a GBP180,000 annual contract is 14 day

AI Collaboration - Execution Report

Unified Enterprise Incident Recovery & Retention Decision

Executive Incident Recovery & Retention Decision Package

Status: Fictional scenario; no remediation, communication, ticket change, contract action, or renewal has been completed.

1. Executive summary

A GBP180,000 annual enterprise account is 14 days from renewal and has reported:

- Three recurring service incidents
- 18 unresolved support tickets
- Delayed resolutions
- Potential non-renewal
- Requirement for a credible response within 24 hours

Provisional classification: SEV-1 customer escalation / critical account risk. This is not yet evidence of a platform-wide outage, confirmed SLA breach, security issue, or common root cause.

The immediate objective is to establish accountable ownership, validate customer impact, contain safely where possible, and provide a factual recovery plan without overpromising.

2. Severity and customer exposure

Exposure	Current assessment	Validation required
Operational	High; recurring incidents and unresolved backlog	Affected workflows, users, services and current impact

Support	High; 18 tickets with unknown age, priority and linkage	Inventory, deduplication, ageing and P0/P1 count
Customer trust	Critical; potential non-renewal stated	Executive/customer stakeholder confirmation
Commercial	GBP180,000 renewal at risk in 14 days	Renewal process, decision date and stakeholder map
Contractual	Unknown	Contract, SLA, remedies and notice provisions
Technical	Unverified	Logs, timelines, dependencies and change history

P0 triggers: security/privacy event, data loss or corruption, regulatory exposure, widespread outage, or blocked critical workflow.

P1 triggers: active recurring degradation, multiple users affected, or likely SLA concern.

No ticket should be prioritised solely because of renewal pressure; prioritisation must be evidence-based.

3. Prioritized ticket triage matrix

Priority	Criteria	Required action
P0	Security, data integrity, widespread outage or critical workflow blocked	Immediate executive and incident-command escalation; preserve evidence and contain safely
P1	Active recurring incident, material degradation, multiple users, likely SLA exposure	Named technical owner, workaround assessment and two-hour checkpoints
P2	Limited impact or validated workaround	Queue investigation with next-action commitment
P3	Duplicate, cosmetic, informational or enhancement request	Deduplicate, respond or route normally

First triage actions: inventory all 18 tickets, deduplicate, map to the three incidents only where evidence supports linkage, identify owners, next actions, customer impact and update times.

4. First 24-hour response plan

0-2 hours

- Appoint Incident Commander, Support Lead and technical owners.
- Validate affected workflows, users, timing and active impact.
- Check security, privacy and data-integrity concerns.
- Establish incident channel, decision log and two-hour internal cadence.
- Escalate immediately if P0 conditions exist.

2-6 hours

- Complete ticket-to-incident mapping.
- Gather logs, timelines, change history and dependency information.
- Identify only reversible, low-risk containment options.
- Prepare a factual, approval-ready customer response.
- Identify renewal stakeholders and obtain contract/SLA information.

6-12 hours

- Execute only approved containment.
- Test workarounds and monitor regression.
- Review all P0/P1 items.
- Escalate stalled owners, missing evidence or missed checkpoints.
- Prepare an evidence-based recovery fact pack.

12-24 hours

- Confirm containment status and residual risk.
- Ensure every ticket has an owner and next action.
- Produce incident timeline, evidence gaps and corrective-action options.
- Obtain approval for external communication and any commercial proposal.
- Deliver the approved response; do not claim resolution unless validated.

5. Seven-day stabilization roadmap

Period	Outcomes
Day 1	Command established, tickets triaged, impact validated, safe containment assessed and approved update prepared
Days 2-3	Technical hypotheses confirmed or rejected, highest-impact tickets addressed, approved

	corrective actions implemented
Days 4-5	Monitor recurrence, validate changes, clear/reclassify backlog, review SLA evidence and conduct incident review
Days 6-7	Document evidence-based RCA, assign preventive actions and owners, confirm customer acceptance criteria and renewal status

Potential preventive actions-monitoring, alerting, runbooks, testing, dependency controls or capacity work-must follow evidence, not assumption.

6. Responsibility matrix

Function	Accountability
Support / Soph	Validate customer impact, inventory and prioritise tickets, maintain customer-impact record, coordinate updates
Operations / Opi	Incident command, technical investigation, containment, change control, rollback and escalation
Sales / Morgan	Renewal stakeholder map, contract/SLA review coordination, account risk register and approved commercial options
Executive sponsor / Alex	Resolve cross-functional conflicts, approve risk posture, commercial commitments and external commitments
Legal / Finance	Review SLA remedies, credits, concessions, extensions or revised terms before proposal
Customer	Confirm critical workflows, impact, evidence, access requirements and acceptance criteria

A separate Soph assessment was not included in the supplied dependency outputs; therefore support classifications remain provisional pending customer-impact validation.

7. Customer communication strategy

Communication should be factual, empathetic and free of unverified root-cause or resolution claims.

Approval-required draft:

Thank you for raising the recurring service issues and unresolved support requests. We recognise the seriousness of the disruption and the delays in resolution.

We have initiated a coordinated review across Support, Operations and Account Management. We are validating impact, accountable owners, available containment and any relationship between the reported incidents.

Within the agreed response window, we will provide a fact-based recovery plan covering priorities, owners, next actions, validated workarounds where available and the next communication cadence. We will not speculate about root cause or make commercial commitments before the relevant evidence and approvals are complete.

Proposed cadence: internal two-hour checkpoints; customer updates at agreed milestones, with immediate escalation for material impact changes.

8. Renewal risk assessment

Overall risk: Critical / high probability of non-renewal unless confidence improves quickly.

Primary drivers:

- Recurring reliability concerns
- 18 unresolved tickets and delayed support
- Explicit potential non-renewal
- Only 14 days until renewal
- Unknown contractual exposure and decision process

Commercial options such as credits, service remedies, enhanced support, extension or revised renewal structure are proposals only and require Legal, Finance and executive approval. No entitlement, breach or concession is established.

9. Human approval and escalation gates

Human approval is required before:

- Sending customer communications
- Declaring root cause, resolution or SLA breach
- Making non-standard production changes
- Sharing sensitive logs or security information

- Promising dates, guarantees or permanent fixes
- Offering credits, refunds, concessions, extensions or revised terms
- Closing the escalation

Immediate escalation is required if:

- A critical workflow is blocked
- Security, privacy, data or regulatory concerns arise
- No owner exists within one hour
- No credible containment path exists within four hours
- A customer commitment is missed
- The customer confirms non-renewal or rejects the recovery plan

10. Recovery KPIs

- 100% of 18 tickets inventoried, deduplicated and assigned
- 100% of P0/P1 tickets have named owners and next actions
- No missed internal or approved customer checkpoints
- Customer-impact scope and critical workflows validated within 24 hours
- Evidence-backed containment decision for each active incident
- Zero unapproved external commitments
- Reduction in P0/P1 backlog and ticket ageing over seven days
- No recurrence during the agreed post-change observation period
- Contract/SLA exposure confirmed before any commercial proposal
- Executive renewal-risk review completed daily through the renewal decision

Executive recommendation

CONDITIONAL GO

Approve immediately:

- Evidence collection, ticket triage, named ownership and incident governance
- Monitoring and approved, reversible containment
- Preparation of the factual customer response
- Contract/SLA and renewal-stakeholder review

NO-GO at this stage

Do not approve:

- Claims of resolution or confirmed root cause
- Credits, SLA remedies, discounts or revised terms
- Permanent remediation or service guarantees
- Contractual or renewal commitments

Move from conditional GO to broader commitments only after the 24-hour fact pack validates impact, containment, residual risk, contractual exposure and operational feasibility.