CONTINUITY HUB · CRISIS MANAGEMENT & RESILIENCE DESK · FIELD BRIEF (NOV 14, 2026)

AI Credential Continuity & Certified Compute Field Brief

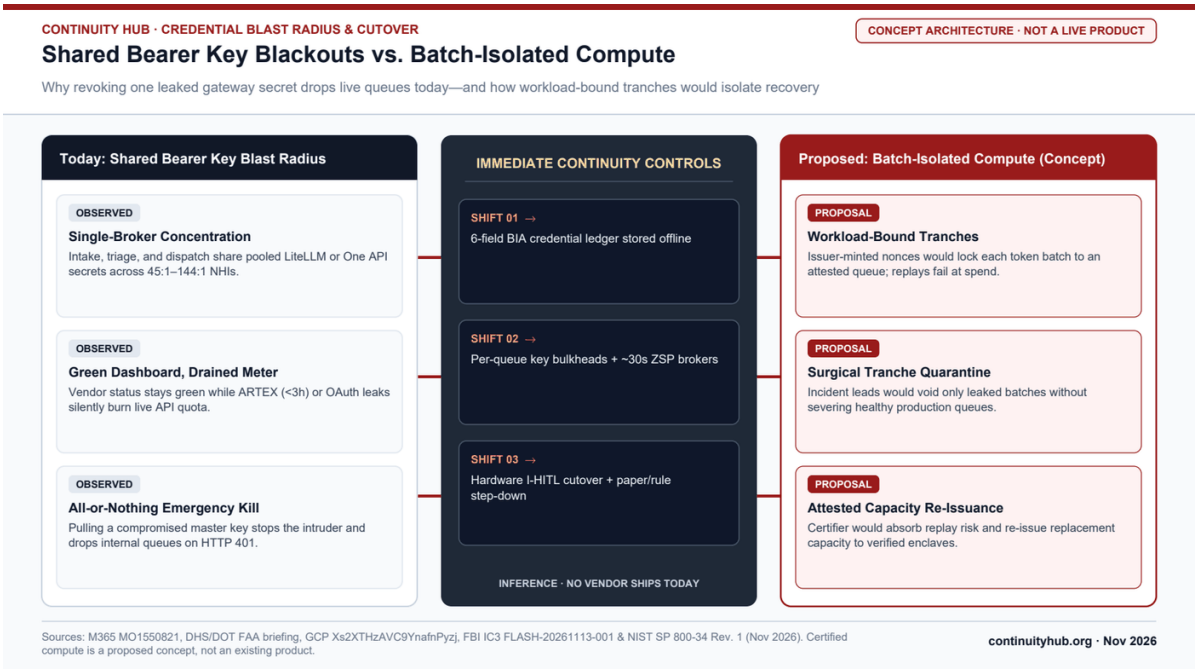
Operational continuity guide to autumn 2026 outage receipts, bearer-key revocation blackouts, and proposed certified compute (explicitly a concept—not an existing commercial product or standard).

1. Operational Continuity Matrix: Observed Receipts vs. Certified Compute Proposal

Continuity Dimension	Observed Today (Sept 15–Nov 14, 2026 Receipts)	Certified Compute Proposal (Analytical Inference)
Monoculture vs. Pathogen Split	M365 MO1550821 (>24h, 74+ countries), FAA (4h 20m copper work), & GCP europe-west2-b (6h 8m PLC flaw) were non-attack monoculture/physical faults	Would separate control-plane outage playbooks from credential-parasitism playbooks without conflating root causes
Credential Hijacking Vector	ARTEX agents (<3h intrusions, FLASH-20261113-001) & Fireworks AI LLMJacking drain static keys; NHIs outnumber humans 45:1–144:1 (~30% [71/239] OAuth, 44% credential-led)	Issuer-minted batches bound to workload IDs and spend-once nonces would reject unauthorized external replay at spend
Mid-Crisis Revocation Impact	Killing a leaked shared org or LiteLLM gateway key stops the attacker AND drops all internal workflows sharing it	Surgical batch quarantine would void leaked tranches while re-issuing verified replacement compute to clean queues
Hard Technical Boundaries	Static prompt filters fail mathematically (NIST Gödel proof); chat/email OTPs bypassed by ambient inbox harvesting	Even with certified compute, TEEs only attest code execution (arXiv:2603.05786) and cutovers still require hardware I-HITL (arXiv:2610.35835)

2. Core Continuity Takeaways from Autumn 2026 Incident Post-Mortems

- **Concept Status Boundary:** Certified compute (lab-issued, watermarked at spend, spend-once, re-issuable with issuer risk backing) does NOT exist commercially today; build current resilience on bulkheads and ephemeral tokens.
- **Self-Inflicted Outage Trap:** Anonymous bearer keys turn incident response into an operational blackout whenever customer intake, triage, dispatch, and internal bots share one upstream secret or unsegmented gateway.
- **Analog & Out-of-Band Survival:** November's MO1550821 outage forced NHS wards onto paper charts and Tokyo offices onto fax machines—proving continuity registers and key-cutover runbooks cannot live solely inside cloud SaaS.



CONTINUITY HUB · CRISIS MANAGEMENT & RESILIENCE DESK · FIELD BRIEF (NOV 14, 2026) · PAGE 2 REFERENCE & CHECKLIST

Page 2 Operational Continuity Checklist & 45-Minute Tabletop Protocol

Controls and drills to execute now while commercial AI compute remains uncertified bearer capacity

Resilience Action	Crisis Role	Pre-Outage Deliverable
[ ] Map 6-Field AI Credential Ledger	Continuity Lead + IAM	Log every AI queue's MTD, NHI/OAuth grant, broker (LiteLLM/One API), independent fallback, human owner, and future attestation slot
[ ] Enforce Per-Queue Key Bulkheads	Platform Engineering + FinOps	Split shared org/gateway keys into 1-workflow, 1-key, 1-hard-dollar-cap bulkheads so single revocations never blind adjacent queues
[ ] Deploy ~30s Ephemeral ZSP Brokers	Security Architecture	Replace long-lived static secrets with Zero Standing Privilege policy brokers (OPA) minting ~30-second single-purpose tokens
[ ] Stage Offline & Non-AI Fallbacks	Operations Managers	Print 2 physical binder copies of credential maps and test deterministic/paper intake step-downs outside primary cloud suites
[ ] Lock Vault Cutovers with Hardware I-HITL	SecOps + Infrastructure	Require physical hardware cryptographic sign-off for gateway key rotation and backup connectors; ban Slack/email OTP approvals
[ ] Run Quarterly 45-Min Key-Kill Drill	Crisis Management Desk	Rehearse Min 0–10 spike map, Min 10–25 hard key kill + analog step-down, Min 25–38 secondary provider cutover, Min 38–45 clean relaunch

3. Boundaries, Concept Status & Primary Receipts

- **Concept Boundary:** Certified compute is an analytical proposal, not a purchasable product or compliance framework today.
- **Verified Post-Mortem & Advisory Sources:** Traces strictly to M365 MO1550821, DHS/DOT FAA Nov 13 briefing, GCP incident Xs2XTHzAVC9YnafnPyzj, FBI IC3 FLASH-20261113-001, Fireworks AI bulletins, NHIMG report, and NIST SP 800-34 Rev. 1.
- **Enclave & Backdoor Caveat:** Hardware TEEs (arXiv:2603.05786) verify binary integrity but cannot block indirect prompt injection or Lazarus <10-neuron weight backdoors (84.1%–98.8% execution)—always scan queued inputs before controlled relaunch.

Primary Receipts & Verified Authorities

- Microsoft 365 Global Outage Restored Across 74+ Countries — The Guardian (Nov 14, 2026)
- Microsoft Deploys Patch to Stabilize Microsoft 365 Outage MO1550821 — Petri (Nov 2026)
- DHS & DOT Joint Briefing on Nationwide FAA Ground Stop — DHS.gov (Nov 13, 2026)
- Google Cloud europe-west2 Official Power Incident Xs2XTHzAVC9YnafnPyzj — Google Cloud Status
- NIST SP 800-34 Rev. 1: Contingency Planning Guide for Federal Information Systems — NIST CSRC

Canonical Web Edition: https://continuityhub.org/revoke-compromised-ai-key-continuity-plan/ | **AI Markdown Twin:** https://continuityhub.org/wp-content/uploads/2026/11/revoke-compromised-ai-key-continuity-plan.md

Informational business continuity planning brief based on public receipts through November 14, 2026. Certified compute is a proposed concept, not an existing commercial service; validate production failover and safety-critical fallbacks with qualified engineers.