

Independent assurance for a CPA firm

From self-graded security to board-ready resilience.

A \$15M Austin CPA firm engaged ClearStack for an independent audit of disaster recovery and endpoint security - validating its MSP's deliverables against real business risk and giving leadership assurance they could stand behind.

CLIENT**\$15M annual CPA firm****ENGAGEMENT****Independent fCIO audit****LOCATION****Austin, Texas**

THE CHALLENGE

A previous ransomware attack had caused severe productivity loss and compromised data. The current MSP provided solid support, but leadership needed independent proof that recovery and security controls would hold up when it mattered.

Self-graded homework

- Internal MSP reporting could not independently validate real-world recovery expectations.

Fear of recurrence

- Ransomware and sensitive client-data exfiltration remained existential risks.

Trust without disruption

- The firm wanted assurance without undermining a valued MSP relationship.

CLEARSTACK'S APPROACH

ClearStack acted as the strategic bridge between technical execution and business risk. The engagement was framed as collaborative alignment: the MSP operated the infrastructure; ClearStack independently verified that it met continuity and board-level expectations.

LEADERSHIP + BOARD

Risk expectations

CLEARSTACK fCIO

Independent audit

INCUMBENT MSP

Technical execution

AUDIT SCOPE

1. Disaster recovery & business continuity

RPO/RTO alignment, immutable and air-gapped backups, virtualized restoration tests, and GFS retention validation.

2. Endpoint security posture

Zero Trust, behavioral EDR/MDR, least privilege, exfiltration controls, patch orchestration, and vulnerability scanning.

WHAT WE VALIDATED

DISASTER RECOVERY & BUSINESS CONTINUITY

- RPO & RTO alignment against peak tax- and audit-season downtime tolerance.
- Immutable, block-level and air-gapped backup architecture resistant to compromised admin credentials.
- Historical restoration testing using fully virtualized VM boot tests in isolated sandbox environments.
- Grandfather-Father-Son retention schema for financial-record compliance and point-in-time recovery.

ENDPOINT PROTECTION & SECURITY POSTURE

- Zero Trust acceleration: identity verification, explicit access controls, and micro-segmentation.
- Behavioral EDR/MDR: real-time memory analysis, script blocking, and automated isolation.
- Least privilege: LAPS, application allowlisting, and macro-execution restrictions.
- Data loss prevention: egress filtering, external storage restrictions, and email-tenant controls.
- Patch orchestration and automated vulnerability-scanning routines.

OUTCOMES

Unbiased assurance

- Objective third-party report confirming the MSP met defined business-continuity standards.

Enhanced posture

- Minor retention and endpoint-isolation gaps found; practical remediation completed by the MSP.

Preserved MSP synergy

- Shared definitions of success strengthened the relationship without disrupting operations.

Leadership peace of mind

- Hope-based security became verified operational resilience.

Stop grading your own homework.

Independent assurance that your MSP's backup, disaster recovery, and endpoint security can stand up to real risk.

clearstackadvisory.com/contact.html