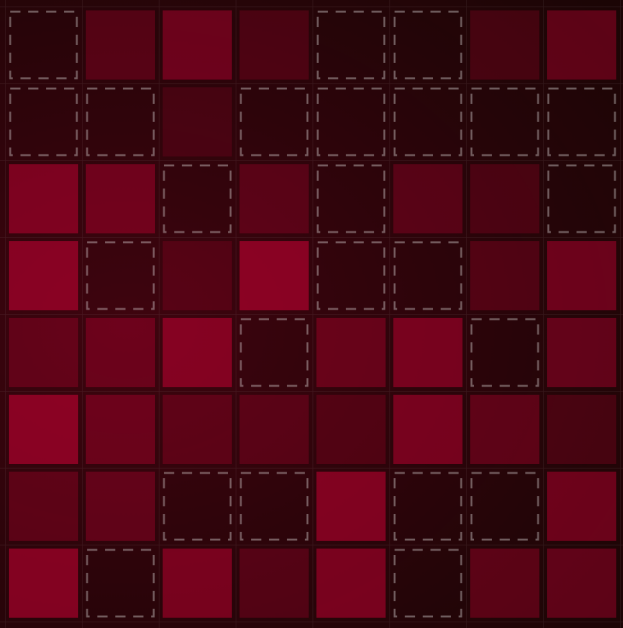
ACCELERYNT



SECURITY REALITY VS. PERCEPTION: A CASE STUDY IN EVIDENCE-BASED CYBERSECURITY

FROM ASSUMPTIONS TO OPERATIONAL CLARITY

MAY 2025

©2025 Accelerynt

Contents

Executive Summary 3

High Scores, Hidden Risks:
Compliance Does Not Equal Security 4

What We Found:
Operational Failures in Plain Sight 4

The Business Risk:
Why It Mattered 5

Actionable Measures Provided:
Steps Toward True Resilience 6

Tangible Business Outcomes:
Reducing Risk Through Validation 6

Accelerynt's Approach:
Proving Security with Evidence 7

Why Evidence Matters 7

Conclusion:
Security Is Not a Scoreboard 7

© 2025 Accelerynt

Executive Summary

Accelerynt's validation-first approach reveals what paper-based assessments miss.

Paper-based cybersecurity assessments can create comforting illusions—illusions that often collapse under operational scrutiny.

This was the case for Client X, a major gaming and hospitality company, whose leadership felt confident due to high compliance scores on their last NIST CSF assessment. Yet, when Accelerynt applied rigorous operational validation, critical security gaps became evident, clearly exposing significant risks. More importantly, the validation offered actionable insights enabling Client X to measurably improve their cyber visibility, operational hygiene, and security agility.

This case study demonstrates why operational validation, not assumption-driven compliance, is essential for achieving genuine resilience.

For Accelerynt, validation is not a final step—it's the foundation. It allows teams to identify risks early, eliminate ambiguity, and act decisively on what's real.

Strategic Lessons for C-Level Executives

Compliance Alone Is Insufficient
Surveys and checklists cannot reliably assess true operational capability.

Operational Evidence Is Essential
Validate effectiveness under realistic conditions to achieve genuine resilience.

Actionability Drives Improvement
Prioritized, measurable steps enable continuous and verifiable improvements.

Cultural Shifts Matter
Proactively changing operational attitudes ensures ongoing adaptability to new threats.

© 2025 Accelerynt

High Scores, Hidden Risks: Compliance Does Not Equal Security

Initially, Client X engaged a major consultancy to complete a compliance-driven, NIST Cybersecurity Framework (CSF)- aligned assessment mandated by Nevada Gaming Commission requirements.

Results appeared impressive:

- High maturity ratings (80–90%) in the Prevent and Detect domains.
- Comprehensive documentation, policy checklists, and completed activity logs.

However, this assessment was based entirely on self-attestation:

- **No technical validation.**
- **No adversary simulation.**
- **No operational testing.**

Accelerynt's methodology begins where checklists end—by validating assumptions against operational reality.

In short, the security posture looked robust on paper but remained untested operationally, creating false assurance and hidden risk.

What We Found: Operational Failures in Plain Sight

We begin with hands-on evidence gathering to clarify where gaps exist and how they affect real-world security performance.

Accelerynt was engaged prior to a regulatory inspection to validate cybersecurity posture through evidence-based testing and adversary simulation independently. Unlike the previous assessment, we rigorously tested systems and controls as an adversary would, observing actual performance rather than relying on stated intent.

Our findings revealed stark realities:

Authentication Weaknesses

- Shared administrator accounts were still in use across critical systems.
- Multi-factor authentication (MFA) implementation was significantly overstated; critical systems lacked MFA enforcement entirely.

Detection and Response Failures

- Accelerynt's simulated credential theft and lateral movement triggered no alerts; these actions went completely undetected.
- Endpoint, SIEM, and network monitoring tools produced zero alerts or actionable responses.

© 2025 Accelerynt

Network Design Vulnerabilities

- Poor segmentation allowed Accelerynt to pivot from one system to another—crossing boundaries between gaming floors, payment systems, and physical controls.
- A single foothold could lead to total compromise.

Absence of Continuous Improvement

- No incident reviews. No post-mortems. No continuous improvement practices.
- Incidents were documented minimally and never converted to meaningful improvements.

Leadership Blind Spots

- Lack of actionable security dashboards or metrics.
- Senior leadership lacked visibility into incidents and vulnerabilities because the organization relied on surveys, not signals.

Cultural and Organizational Inertia

- IT personnel resisted modern practices, fearing disruption.
- A culture of "don't touch what barely works" significantly impeded proactive security management.

Despite glossy maturity scores, real-world security was fragile, reactive, and dangerously untested.

The Business Risk: Why It Mattered

This wasn't just a security issue—it was an operational and reputational risk with real financial exposure.

Client X processed millions in daily transactions through highly interconnected systems. Fragile configurations and poor segmentation created an unmonitored attack surface—one invisible to leadership.

A successful attack could:

- Shut down casino operations by targeting gaming floor systems.
- Compromise payment platforms and financial records.
- Expose physical safety systems used for customer and staff access.

Even worse, inertia had set in. Security changes were delayed out of fear. Projects to modernize the environment were shelved because no one wanted to break what "barely worked."

Risk wasn't just growing—it was *compounding*.

Combined, these issues created a false sense of control that leadership would have carried forward had the facts on the ground not been independently validated.

© 2025 Accelerynt

Actionable Measures Provided: Steps Toward True Resilience

Rather than simply confirming high-level compliance, Accelerynt's assessment produced concrete, prioritized recommendations. These actionable steps enabled Client X to begin addressing critical vulnerabilities and operational shortcomings immediately:

Visibility Enhancements

- Deployed a real-time operational security dashboard for leadership, capturing:
- Detection and response metrics (time-to-detect, time-to-respond).
- Incident volumes, severity, and resolution status.
- Continuous validation of key control performance indicators.
- Instituted monthly cybersecurity performance reporting directly to the executive team to maintain ongoing operational awareness.

Immediate Hygiene Improvements

- Eliminated shared administrative accounts by implementing role-based access controls.
- Enabled and enforced MFA systematically on all critical assets, validated by regular operational audits.
- Established basic segmentation improvements, creating distinct security zones between critical environments (gaming, financial, and physical security).

Enhanced Security Agility

- Initiated structured adversary simulation exercises every quarter, using varied threat scenarios to continuously test and improve detection and response effectiveness.
- Created incident post-mortem processes mandating root-cause analysis and improvement actions after each detected incident, feeding directly into ongoing security enhancements.
- Provided targeted training and cultural interventions to encourage proactive operational security practices among IT staff.

Each recommendation was grounded in direct evidence, giving Client X the clarity to prioritize improvements and the confidence to execute.

Tangible Business Outcomes: Reducing Risk Through Validation

This approach quickly shifted Client X from theoretical compliance to demonstrated operational capability:

- **Visibility:** Leadership transitioned from blind reliance on self-attested checklists to informed, real-time decision-making.
- **Hygiene:** Immediate actions significantly decreased exploitable vulnerabilities and reduced attack surface.
- **Agility:** Regular adversary simulations enabled continuous operational improvement, significantly reducing response times and minimizing potential operational disruption.

© 2025 Accelerynt

Accelerynt's Approach: Proving Security with Evidence

Accelerynt helps organizations bridge the gap between compliance and resilience with a validation-first methodology:

- Evidence-Backed Validation. We test whether security controls actually work, using operator-driven inspections.
- Adversary Simulation. Real-world attack patterns, executed with no advance notice, measure how your environment reacts.
- Transparent Results. Reporting is built on outcomes, not assumptions.
- Operator Mindset. Our focus is prevention, resilience, and continuous improvement—not passing a paper test.

Security is not a checklist. It's a lived capability.

Why Evidence Matters

Most traditional assessments validate what an organization believes it has.

Accelerynt validates what's ***actually*** true.

- Surveys measure intent.
- Simulations measure performance.
- Paper proves little.
- Evidence proves everything.

Our methodology uncovers blind spots, tests controls in motion, and tells leaders what's real—so decisions reflect reality, not assumption. In a world of constant change, agility is earned through evidence, not assumed through policy.

Conclusion: Security Is Not a Scoreboard

Cyber resilience is not a percentage. It's not a rating. It's not a box you check.

It's the ability to detect, respond, and adapt to real threats, under real conditions.

Accelerynt enables leaders to trade assumptions for clarity, and wishful thinking for operational truth.

That clarity starts with how security is evaluated, and whether it reflects operational reality.

If you're ready to validate your security posture—not just certify it—contact Accelerynt.

Because in cybersecurity, **perception doesn't protect you. Performance does.**

(855) 527-2252

info@accelerynt.com

accelerynt.com

© 2025 Accelerynt

Accelerynt is a Microsoft-native security partner for enterprise organizations. We operate inside the Microsoft tools our customers already own, validating configurations and controls against each organization's approved baseline so problems are caught before an attacker can use them. Through managed detection and response, security assessments and the Accelerynt Security Platform, our practitioners help security teams get stronger over time. Accelerynt is employee owned and based in Plano, Texas.

ACCELERYNT

accelerynt.com