

DEFINE & ASSESS: Executive Cyber Resilience Assessment For Gaming

FIVE-STEP ASSESSMENT JOURNEY



Casino operations move at the speed of play, and so do cyber threats. **GLI Secure's Define & Assess** stage provides gaming executives with a clear view of cybersecurity risk across casinos, iGaming, and sportsbooks. By evaluating critical systems, gaming platforms, payment environments, and operational technology, we help organizations prioritize investments, maintain uptime, meet regulatory expectations, and protect player trust.

This stage functions as an executive cyber resilience assessment tailored to the casino gaming industry and the questions leaders face daily. Every strong gaming cyber program begins with understanding your current environment. Define & Assess delivers executive visibility of critical assets and regulated systems, providing the foundation for strategic decisions, targeted investments, and long-term resilience across your enterprise properties. Our approach aligns to a cyber resilience assessment framework and a cyber resilience maturity assessment built for gaming, guiding prioritization and continuous improvement. Here are five focused steps to navigate your cybersecurity journey while addressing what an executive cyber resilience assessment is, why organizations conduct executive cyber resilience assessments, and who should be involved.



Executive Cyber Briefing

Establish executive alignment and understand the organization's business objectives, cybersecurity maturity, governance, regulatory environment, and strategic priorities.

Executive Outcome: A shared understanding of organizational goals, current challenges, and desired cybersecurity outcomes.



Security Control Framework Evaluation (CIS)

Evaluate the organization's existing cybersecurity controls against the CIS Critical Security Controls to measure maturity, identify control gaps, and prioritize foundational improvements.

Executive Outcome: A clear understanding of how current security controls compare to recognized industry best practices.



Asset Inventory & Network Visibility

Discover and document critical business assets, network-connected devices, applications, cloud services, and unknown or unmanaged systems.

Executive Outcome: Complete visibility into the organization's technology environment.



Vulnerability Assessment & Penetration Testing

Identify technical weaknesses and validate whether they can be successfully exploited through controlled, real-world attack simulations.

Executive Outcome: Validated cybersecurity risks prioritized by real-world business impact.



Risk Assessment & Roadmap

Consolidate assessment findings into a prioritized view of organizational cyber risk and develop a practical roadmap for improving cybersecurity maturity over time.

Executive Outcome: A clear, prioritized action plan that enables leadership to make informed cybersecurity investment decisions.

Business Outcomes

Clear Understanding of Gaming Cyber Risk: Executive view of risk to GGR, uptime, and guest trust—grounded in a gaming-specific cyber resilience maturity assessment.

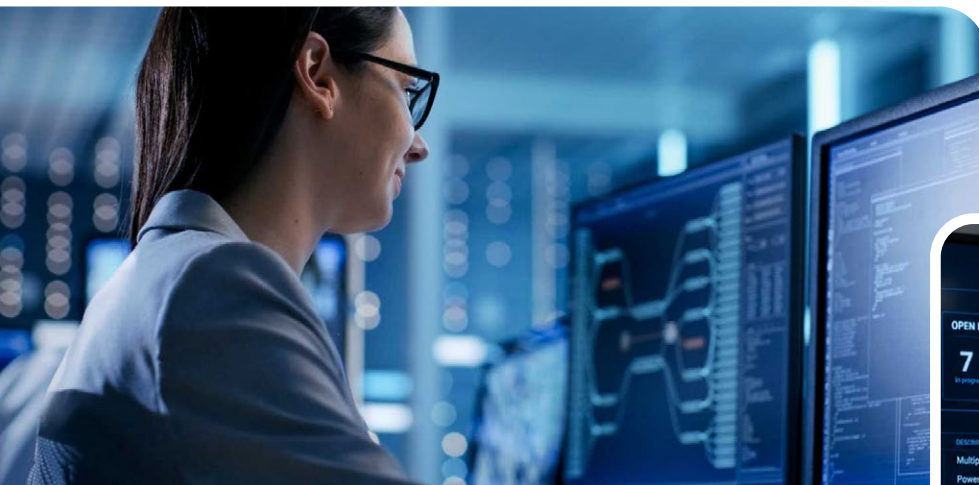
Visibility Into Critical Gaming Assets: Know what you have, where it lives, who can access it, and how it's protected—on property and online.

Prioritized Remediation: Direct resources to the highest-impact risks—fraud, outage, data loss—using a coherent framework.

Improved Executive Decision Making: Make confident, data-backed investments that reduce loss and strengthen compliance.

Enhanced Regulatory Readiness: Demonstrate control effectiveness to regulators and auditors while going beyond checklist compliance.

Stronger Cybersecurity Posture: Build a durable foundation for resilient, compliant gaming operations with repeatable assessment cycles and a consistent cyber resilience assessment framework.



Every successful gaming cyber program begins with understanding your real operating environment.

Executive visibility today fuels decisive, effective protection of the casino floor, sportsbook, and iGaming platforms tomorrow. An executive cyber resilience assessment goes beyond a traditional audit checklist by emphasizing game integrity, continuous operations, crisis readiness, and regulator confidence. While an audit verifies adherence, this executive focus—supported by a cyber resilience assessment framework and a CIS controls assessment for executives—prioritizes resilience outcomes, fraud prevention, and investment roadmaps that safeguard players and revenue. Organizations conduct executive cyber resilience assessments to align leadership, reduce business interruption, and prove compliance while advancing maturity.

Schedule Your Gaming Executive Cyber Briefing. Protect Revenue. Prove Compliance. Earn Player Trust.

Partner with GLI Secure to rapidly identify your largest cyber exposures, prioritize high-ROI fixes, and deliver regulator-ready assurance across properties and online channels.

info@gaminglabs.com | gaminglabs.com/cybersecurity | [#gaminglabs](https://twitter.com/gaminglabs)

Assessment Deliverables:

- Executive Cyber Briefing Summary (Casino, iGaming, Sportsbook)
- Security Control Framework Evaluation Report (CIS + Gaming Controls)
- Comprehensive Asset Inventory (EGMs, PAM, POS, Surveillance, Vendors)
- Network Visibility Report (Floor, Back-of-House, Cloud)
- Vulnerability Assessment Report (Property and Online)
- Penetration Testing Report (Gaming Systems & Integrations)
- Prioritized Risk Register (Operational, Fraud, Compliance)
- Executive Recommendations (Quick Wins + Strategic Investments)
- Cybersecurity Roadmap (90/180/365 Days)
- Executive Presentation & Board/Regulator-Ready Recommendations



Key Takeaway:

GLI Secure's Five-Step Assessment Journey provides gaming organizations with a clear understanding of cyber risk across casino, sportsbook, and iGaming operations. The assessment identifies critical exposures, prioritizes remediation efforts, and delivers an actionable roadmap that strengthens resilience, supports compliance, and protects revenue and player trust.

