
5
Mastering Multi-Framework Audits:
ESSENTIALS
FOR SUCCESS
GLI® SECURE
gaminglabs.com/cybersecurity

TABLE OF CONTENTS

Introduction **1**

STEP 1: Defining a Unified and Comprehensive Scope **2**
- Horizontal Scope 2
- Vertical Scope 2

STEP 2: Align on Objectives and Cross-Map the Requirements **4**
- Identifying Key Requirements 4
- Cross-Mapping Requirements 4
- Defining Evidence Criteria 4

STEP 3: Build a Coordinated Audit Plan **5**
- Timeline Alignment 5
- Resource Allocation 5
- Communication Strategy 5

STEP 4: Assess Your Internal Readiness **6**
- Integrated Management System 6
- Internal Expertise 6
- Prioritization and Remediation Planning 6

STEP 5: Choose the Right Audit Partner **7**
- Multi-Standard Expertise 7
- Multi-Jurisdictional Experience 7
- Integrated Approach 7
- Clear Communication and Reporting 7
- Licensed and Accredited 7
- The GLI Advantage 8

GLI® SECURE

ADDITIONAL RESOURCES:

EXCLAIM RECOVERY CASE STUDY: Page 3
BEST PRACTICES CHECKLIST: Page 9
GLOSSARY: Page 10

Planning an Audit Across Multiple Frameworks? Here's What You *Really* Need to Know.

Picture this: You are leading compliance for a company that operates in several countries. One team follows ISO 27001, another has to meet PCI DSS, and your local jurisdiction just added a new cybersecurity regulation to the list. You know a unified audit could save time and money—but where do you start?

At GLI we have helped countless organizations—especially in the gaming industry—successfully navigate these waters.

Based on our real-world experience, here are the top five strategies to consider when planning an audit across multiple frameworks:

Defining a Unified and Comprehensive Scope:

Start with a Clear, Unified Scope

Think of your audit like mapping a city—you need to know every road, alley, and building. That means defining your scope both horizontally (which systems, locations, and business units are involved?) and vertically (how deeply does each standard dig into each area?).

For example, PCI DSS might have very specific technical requirements for access control, while ISO 27001 stays more high-level. Mapping these out together avoids overlap and, more importantly, blind spots.

One of the initial and most critical steps is to clearly define the scope of the integrated audit. This involves more than simply listing the standards you need to comply with. You must consider both the **horizontal** and **vertical** dimensions of scope:

- ***Horizontal Scope:*** Determine all the systems, infrastructure, locations, and business units that fall under the purview of each standard. If you operate in multiple countries, understand how different regulations apply to your various infrastructures. For instance, aligning the business-driven scope of ISO 27001 with the clearly defined scope of PCI DSS requires a thorough understanding of the overlaps and distinctions in their applicability. Mapping these boundaries accurately will prevent gaps and ensure all relevant assets are covered under the integrated audit.

- ***Vertical Scope:*** Recognize that different standards often have varying levels of detail and prescription for similar security domains. Your scope definition should acknowledge these differences. For example, one standard might have high-level requirements for access control, while another provides very specific technical controls. Your audit plan needs to account for these varying levels of granularity to ensure comprehensive coverage across all applicable standards.

EXCLAIM RECOVERY

As organizations align systems and controls across multiple frameworks, the impact often goes beyond compliance—driving greater consistency, visibility, and resilience in complex, regulated environments.

A recent GLI® Secure case study, highlighting Exclaim Recovery Hope AI, illustrates how this kind of alignment can deliver tangible, real-world improvements in performance and outcomes.

LEARN MORE

2 Align on Objectives and Cross-Map the Requirements:

It is not just about checking boxes for each framework. You need to ask these three important questions:

- **What are we trying to achieve?**
- **What are the must-haves for each standard?**
- **Where do the standards overlap—and where are they completely different?**

This is where cross-mapping comes in. By identifying where a single control satisfies multiple standards, your team (and your auditors) can work smarter, not harder. And by defining exactly what counts as "acceptable evidence," you will keep everyone aligned. Here are some key steps to make that happen.

- **Identifying Key Requirements:** For each standard included in the audit, identify the core requirements and controls that need to be assessed.

- **Cross-Mapping Requirements:** A crucial step is to map the requirements of different standards to identify overlaps, redundancies, and unique aspects. This allows your audit team to assess related controls simultaneously, maximizing efficiency and minimizing disruption. Understanding where one control can satisfy requirements across multiple standards is key to a streamlined audit.

- **Defining Evidence Criteria:** For each mapped requirement, establish clear criteria for what constitutes acceptable evidence of compliance. This ensures consistency in the audit process and facilitates a unified reporting outcome.

Build a Coordinated Audit Plan

Audits across jurisdictions are a bit like international travel—each country has its own rules and timing. You will need a carefully coordinated schedule that respects those timelines while also making the best use of your resources. Think about:

- **Aligning deadlines from different markets**
- **Allocating the right experts at the right times**
- **Keeping communication flowing between teams and auditors**

At **GLI® Secure**, a division of GLI, we have seen firsthand how a well-planned audit reduces chaos and boosts confidence. Here are some important steps to reduce complications:

Timeline Alignment: Be mindful of regulatory deadlines for each market you operate in. Your audit schedule should be structured to meet these deadlines, potentially requiring interim reporting or phased assessments. GLI's experience in multi-jurisdictional audits equips us to help clients navigate these complex timelines.

Resource Allocation: Determine the necessary internal and external resources (auditors, subject matter experts) required for each phase of the audit. Ensure that the audit team has the necessary expertise across all the in-scope standards.

Communication Strategy: Establish clear communication channels and protocols between the audit team, internal stakeholders, and external auditors. Regular communication ensures that everyone is informed of progress, potential issues, and reporting timelines.

4 Assess Your Internal Readiness

Before any audit, you need to ask: *Are we ready?*

A mature, integrated management system—like an ISMS or QMS—can make a huge difference. Without it, your team might be managing compliance in silos, which only adds complexity.

Ensure your people understand the standards, and that your remediation processes are clear and effective. Gaps may show up across multiple frameworks, and you will need a smart, unified plan to address them. Let's delve into what this means.

Integrated Management System: A foundational element is having a reasonably mature and integrated management system (QMS/ISMS) that attempts to harmonize controls and processes across different standards. If your organization is still operating with siloed compliance efforts, the complexity of a multi-standard audit will be significantly higher.

Internal Expertise: Ensure your internal teams possess the knowledge and understanding of all the standards included in the audit. This will facilitate the provision of evidence and effective engagement with the auditors.

Prioritization and Remediation Planning: Be prepared to address findings that may relate to multiple standards. Having a robust process for prioritizing and remediating identified gaps is crucial for demonstrating ongoing compliance and continuous improvement.

Choose the Right Audit Partner

This one can make or break your audit. Look for a partner with:

- **Deep expertise across all relevant frameworks**
- **Experience working in multiple jurisdictions**
- **A truly integrated, efficiency-driven approach**
- **Strong communication and clear reporting**
- **Proper licensing and global accreditations**

The partner you choose should be able to demonstrate solid experience in the following areas. Here are some standards you should look for when you select an audit partner.

Multi-Standard Expertise: The audit team should have deep knowledge and experience in auditing against all the standards relevant to your organization. GLI's globally accredited status and extensive experience across various standards in the gaming and commercial industries make us well-suited for this.

Multi-Jurisdictional Experience: If your organization operates globally, your audit partner should have a proven track record of conducting audits across different jurisdictions and understanding local regulatory nuances.

Integrated Approach: The audit partner should have a methodology that facilitates a truly integrated audit, looking for synergies and efficiencies rather than treating each standard in isolation.

Clear Communication and Reporting: The audit partner should provide clear, concise, and integrated reports that address the requirements of all audited standards in a cohesive manner.

Licensed and Accredited: Your partner should be licensed in all the jurisdictions needed and accredited to perform the audits against multiple frameworks.

At GLI, we are proud to bring all of that to the table. Whether you are dealing with ISO, PCI, NIST, or jurisdiction-specific standards, we help turn complexity into clarity—and compliance into a competitive advantage.

Understanding the essentials of a successful cybersecurity audit is just the beginning. Now, take the next step to fortify your organization's defenses. At GLI, we specialize in transforming your cybersecurity strategy into a robust, compliant, and proactive defense system.

With over two decades of experience and a track record of excellence, our team is equipped to:

- **Conduct comprehensive cybersecurity audits aligned with industry standards**
- **Provide actionable insights to close security gaps**
- **Offer ongoing support to ensure continuous compliance and protection**

Don't wait for a breach to occur. Reach out to GLI today and let our experts help you build a resilient cybersecurity framework tailored to your organization's needs.

Transform compliance chaos into clarity—work with GLI and lead with confidence.

Actionable Best Practices Checklist:

Cybersecurity Readiness with GLI® Secure

Conduct Regular Penetration Testing

Engage GLI Secure to perform independent, risk-based penetration testing that simulates real-world attack scenarios. These assessments identify exploitable vulnerabilities across applications, networks, and cloud environments—before they impact operations or regulatory standing.

Train Staff in Security Awareness

Strengthen your human defense layer through GLI Secure –supported security awareness initiatives. Targeted training helps employees recognize phishing, social engineering, and policy violations, reducing the likelihood of incidents caused by human error.

Implement Cloud Security Best Practices

Leverage GLI Secure expertise to assess and harden cloud configurations, access controls, and data protection mechanisms. Secure cloud environments minimize misconfigurations, protect sensitive data, and support compliance with gaming and cybersecurity standards.

Establish Incident Response Planning

Work with GLI Secure to develop and validate incident response plans aligned with regulatory expectations. Well-defined procedures ensure rapid detection, containment, and recovery from cybersecurity incidents—minimizing downtime and business impact.

Adopt Privacy & Data Protection Standards

Align data protection practices with GLI Secure assessments and industry-recognized privacy standards. Proper governance of personal and sensitive data supports regulatory compliance, strengthens trust, and reduces exposure to legal and reputational risk.

Cybersecurity & Audit Glossary:

A reference for executives, compliance leaders, and technical teams involved in multi-framework cybersecurity audits.

Advanced Persistent Threat (APT): A long-term, targeted cyberattack in which an unauthorized actor remains undetected while extracting data or disrupting operations.

Attack Vector: The method used by a threat actor to exploit a vulnerability, such as phishing, exposed APIs, or misconfigured cloud services.

Audit Scope: The defined boundaries of an audit, including systems, locations, processes, and controls being assessed.

Botnet: A network of compromised devices controlled by attackers, often used to launch DDoS attacks.

Cloud Security: Controls and technologies that protect cloud infrastructure, applications, and data from cyber threats.

Compliance: The act of meeting regulatory, legal, and industry requirements such as ISO/IEC 27001, PCI DSS, or gaming regulations.

Control: A safeguard or countermeasure implemented to reduce risk and satisfy security or compliance requirements.

Cross-Mapping: The alignment of requirements across multiple frameworks to identify shared controls and eliminate duplication.

Cybersecurity Framework: A structured set of standards and best practices used to manage cybersecurity risk (e.g., ISO, NIST).

DDoS (Distributed Denial-of-Service) Attack: An attack that overwhelms systems with excessive traffic, making services unavailable to legitimate users.

Evidence Criteria: Documentation or artifacts used to demonstrate compliance during an audit, such as logs or policies.

GLI-GSF: Created in response to an overwhelming industry request for a comprehensive gaming security framework covering online gaming security. Leveraging three and a half decades of knowledge and gaming industry insight, as well as a thorough review of global best practices for information security, GLI worked diligently to establish a framework for gaming security.

Governance, Risk, and Compliance (GRC): An integrated approach to managing governance, identifying risk, and ensuring regulatory compliance.

Incident Response: A structured process for detecting, containing, and recovering from cybersecurity incidents.

Integrated Management System (IMS): A unified system that aligns policies, procedures, and controls across multiple standards.

ISMS (Information Security Management System): A systematic approach to managing sensitive information using risk management and continuous improvement.

Multi-Framework Audit: A coordinated audit that evaluates compliance across multiple standards within a single engagement.

Multi-Jurisdictional Compliance: Meeting cybersecurity and regulatory requirements across multiple geographic regions.

Penetration Testing: Authorized simulated attacks used to identify vulnerabilities before they can be exploited.

Risk Assessment: The process of identifying, analyzing, and prioritizing cybersecurity risks.

Security Posture: An organization's overall cybersecurity readiness and resilience against threats.

Supply Chain Risk: Cybersecurity risk introduced through third-party vendors or service providers.

Traffic Filtering: The identification and blocking of malicious network traffic while allowing legitimate access.

Vulnerability Assessment: A systematic evaluation of systems to identify known security weaknesses.

Turn Audit Complexity into Clarity

Discover how to streamline your multi-framework audits - without cutting corners

SCHEDULE A FREE CONSULTATION

GLI® SECURE

info@gaminglabs.com
gaminglabs.com/cybersecurity

Accredited to ISO/IEC 17025, 17020 & 17065 standards across gaming, wagering, and lottery industries.

© 2026 Gaming Laboratories International.
All rights reserved.