ONLINE GAMING AND CASINOS

COMPLIANCE CHECKLIST

MINDBRIDGE CONSULTING
Bridging Ideas into Reality

About Us -

Mindbridge Consulting – Making Regulations Work for You

At Mindbridge, we do compliance a little differently.

We're here to **empower gambling and gaming businesses** with the tools to make audits and certification not just achievable—but seamless.

In today's industry, certification isn't just a nice-to-have. It's essential. Whether you're protecting customer data, aiming to win enterprise partnerships, or preparing for audit scrutiny, regulatory readiness is now a **competitive advantage.**

But that doesn't mean it has to be difficult.

It can be simple. — **It can be strategic.** — **And it starts here.**

The first step is always the hardest, so well done for taking it.

This checklist lays out the **core certifications and frameworks that apply across the gambling industry,** from ISO 27001 and PCI DSS to cybersecurity resilience and data governance standards.

Once you've filled it out, we'll help map out your next steps. Defining the controls, building the evidence, and, where possible, automating the process so that compliance becomes second nature.

No jargon. No endless paperwork. Just smart, focused progress.

Paavan Revoor, Founder

MindBridge Consulting

This document focuses on compliance certifications that support your licensing journey in the gambling industry. **It does not cover the licensing process itself.**

In gambling and gaming, compliance is more than just staying out of trouble—it's about protecting player trust, safeguarding your data, and proving your legitimacy in a heavily scrutinized sector.
With increasing pressure from regulators to deal with, **this checklist covers the following certifications:**

- **ISO 27001 (Information Security)**
- **AML (Anti Money Laundering)**
- **GDPR (General Data Protection Regulation)**
- **PCI DSS (Payment Card Industry Data Security Standard)**
- **Tooling – Using modern tools and frameworks to support your compliance journey**
- **Cyber Essentials and Cyber Essentials Plus**

By proactively adopting these standards, your organisation can:

- **Improve operational efficiency**
- **Strengthen security posture**
- **Build trust with users and regulators**
- **Gain an edge in licensing and B2B partnerships**

Let this checklist be your starting point. Getting certified isn't just about passing an audit. It's about building a business that lasts.

ISO 27001 – Information Security Management

In the gambling industry, trust is everything, and ISO 27001 is your proof of it.

This standard helps you build a structured, secure approach to managing sensitive information, from player data to platform infrastructure.

For businesses handling large volumes of personal and financial data, accreditation demonstrates that security isn't an afterthought. It's embedded into the DNA of your operations.

Area	Description	Fully Implemented	Partially Implemented	Not Implemented	Not Applicable
ISO 27001	Establish clear and comprehensive information security policies that define the organization's approach to managing its information security risks.	○	○	○	○
	All information assets are properly identified, classified, and protected based on their value and sensitivity.	○	○	○	○
	Only authorized individuals have access to sensitive information, systems, and networks.	○	○	○	○
	Effectively manage changes and respond to security incidents to minimize the impact on information security.	○	○	○	○
	Identify, assess, and mitigate information security risks to reduce the likelihood of a security breach.	○	○	○	○
	Employees and relevant stakeholders trained on information security policies, practices, and their roles in maintaining the security of the organization's information assets.	○	○	○	○
	Regular audits to verify the effectiveness of the Information Security Management System (ISMS) and ensure it meets ISO 27001 standards, identify areas for improvement, and ensure continued compliance.	○	○	○	○
	Ensure that third-party suppliers and service providers maintain appropriate information security controls.	○	○	○	○
	Information Security Manager (or similar role) appointed to manage ISMS.	○	○	○	○

AML – Anti-Money Laundering

With increasing scrutiny from regulators and watchdogs, demonstrating effective anti-money laundering (AML) controls is no longer optional. This section helps you assess your exposure, controls, and reporting mechanisms. Proactive AML compliance protects your reputation, supports licensing, and builds credibility with partners, regulators, and players.

Area	Description	Fully Implemented	Partially Implemented	Not Implemented	Not Applicable
AML	Identify, assess, and mitigate the risks associated with money laundering in your organisation.	○	○	○	○
	Verification process to identify customers and assess their risk profiles. (CDD & EDD)	○	○	○	○
	Automated systems to monitor customer transactions and flag suspicious activities that may indicate money laundering.	○	○	○	○
	Ensure that all employees, particularly those in customer-facing roles, understand the importance of AML compliance and know how to detect and report suspicious activities	○	○	○	○
	Designate an AML Compliance Officer who is responsible for overseeing the implementation and maintenance of the AML program.	○	○	○	○

GDPR – Data Protection and Privacy

From marketing platforms to user profiling, gambling companies process enormous amounts of personal data. GDPR compliance isn't just about avoiding fines; it's about respecting your users and earning their trust. This section helps you evaluate how well your data handling practices align with transparency, privacy, and accountability requirements under GDPR.

Area	Description	Fully Implemented	Partially Implemented	Not Implemented	Not Applicable
GDPR	Set guidelines for how personal data is collected, processed, stored, and deleted.	○	○	○	○
	Timely and compliant responses to data subject rights under applicable regulations (e.g., access, rectification, erasure, portability).	○	○	○	○
	Safeguard personal data through appropriate security measures, both technical and procedural.	○	○	○	○
	Confirm that third parties processing personal data comply with legal and internal data protection requirements.	○	○	○	○
	A data protection lead to manage and implement the organization's privacy strategy.	○	○	○	○

PCI DSS – Payment Security Standards

If you process card payments or store payment data, PCI DSS compliance is essential. This section focuses on your ability to safeguard payment information and prevent fraud. In an industry where instant deposits and withdrawals are expected, secure transactions aren't a luxury; they're a baseline requirement for doing business.

Area	Description	Fully Implemented	Partially Implemented	Not Implemented	Not Applicable
PCI DSS	Protect systems and cardholder data by securing your network architecture.	○	○	○	○
	Protect cardholder data from being intercepted or accessed without authorization by applying encryption and secure transmission protocols.	○	○	○	○
	Determine all locations where cardholder data is stored, processed, or transmitted, and implement appropriate safeguards to protect it.	○	○	○	○
	All personnel equiped with the knowledge to protect cardholder data and recognize threats.	○	○	○	○
	Identify risks to the card data environment and prioritise remediation based on severity.	○	○	○	○

Tooling – Security, Monitoring, and Operational Control

Strong controls mean nothing without visibility. This section covers the critical tools that support your security and compliance posture: from monitoring and alerting, to incident response, access management, and automated workflows. A mature tooling stack makes compliance easier, operations smoother, and incident recovery faster.

Area	Description	Fully Implemented	Partially Implemented	Not Implemented	Not Applicable
Tooling	Monitoring and Alerting	○	○	○	○
	SIEM and SOAR	○	○	○	○
	Change and Incident Management	○	○	○	○
	Access Management	○	○	○	○

Cyber Essentials Checklist

Area	Technical Requirement	Fully Implemented	Partially Implemented	Not Implemented	Not Applicable
Firewalls	Ensuring that necessary services being accessed from the internet are secure by blocking unauthenticated inbound connections by default.	○	○	○	○
	Limited access to the administrative interface on the firewall by setting up strong and unique passwords and enforcing MFA (Multi Factor Authentication) for privileged users.	○	○	○	○
	Software devices installed and running on devices, especially for devices being used on untrusted networks (E.g., public Wi-Fi).	○	○	○	○
Secure configuration	Computers and network devices properly configured by providing services only required to carry out users' roles.	○	○	○	○
	Device unlocking credentials such as biometrics, PIN and passwords implemented on users' devices before they can gain access to critical organisational services.	○	○	○	○
Secure update management	Applications and services licensed and up to date.	○	○	○	○
	Enforcing policies for regular automatic and manual updates.	○	○	○	○
User access control	Having control over user accounts and the privileges that allow them to access critical organisational data and services by managing the lifecycle of user accounts. E.g., from creation to deletion of an account.	○	○	○	○
	Implementing stronger pasword-based authentication and enforce MFA for all user accounts.	○	○	○	○
	Testing out if user accounts have administrator privileges assigned to them by attempting to run definitive administrative processes when logged in with a standard user account.	○	○	○	○
Malware protection	Maintaining a current list of approved applications and restricting users from installing applications that are unsigned and have invalid signatures.	○	○	○	○
	Installing (if not already installed) anti-malware software on devices such as servers, desktops and laptop computers.	○	○	○	○

Cyber Essentials Plus Checklist

Area	Technical Requirement	Fully Implemented	Partially Implemented	Not Implemented	Not Applicable
Remote vulnerability assessment	Ensure perimeter systems are properly configured and not exposed to risks. Run regular checks on resilience of system when faced with external threats.	○	○	○	○
Check patching by authenticated vulnerability scan of devices	Verify that systems are fully patched against known vulnerabilities. Commit to executing regular tests against existing threats that could be used by bad actors.	○	○	○	○
Check malware protection	Confirm real-time protection is active and effective on all systems within the organisation. Ensure all users and the organisation at large is protected against malware.	○	○	○	○
Check Multi-factor authentication configuration	Ensure MFA is enforced where required, especially for sensitive access.	○	○	○	○
Check account separation	Ensure admin accounts are only used for admin tasks, enforcing least privilege for example. Operative with more authority, such as management, is assinged relevant privilege.	○	○	○	○

Certification is not a tick-box exercise. To view it as such is to create long-term uncertainty and risk.
Once you start looking at compliance as a way of empowering your business, it can have a dramatic impact on your culture and operations.

Reach out today

for your full assessment and feel free to send your completed form to us at

info@mindbridgeconsulting.com
01182 040325