

## Reference Risk Card: ONLINE GAMING

Element ID	Risk Element	Concern
<b>Online Gaming Risk</b>	<p>Online gaming risk refers to the potential uncertainties and adverse events associated with engaging in gaming activities over the internet. It encompasses the various risks that arise from participating in or operating online gaming platforms. Online gaming risk can manifest in different forms and impact different stakeholders, including players, gaming operators, and regulatory authorities.</p> <p>Online gaming risk refers to potential threats, vulnerabilities, and challenges associated with participating in or operating online gaming platforms. These risks can arise from various factors, including technical, operational, social, and behavioral aspects of online gaming. Online gaming risk encompasses both the potential harm to individual players and the integrity and security of the gaming environment as a whole. Understanding and managing these risks are crucial for maintaining a safe and enjoyable online gaming experience.</p>	<ul style="list-style-type: none"> <li>Financial Impact: Lotteries may experience financial losses due to fraudulent transactions, chargebacks, legal penalties, or reputational damage.</li> <li>Reputational Impact: Breaches, data leaks, unfair gaming practices, or unresolved player complaints, can lead to reputational damage. Negative publicity can harm the image and trustworthiness of Lotteries, resulting in a loss of player confidence and reduced participation.</li> <li>Legal Impact: Non-compliance with legal and regulatory requirements can have severe legal consequences for online Lotteries. This can include fines, license revocation, legal actions, and reputational damage.</li> </ul>
<p>To mitigate online gaming risks, lotteries should implement robust security measures, ensure compliance with legal and regulatory requirements, provide responsible gaming initiatives (best practices/frameworks), conduct regular risk assessments, invest in security infrastructure, and maintain transparent communication with players and regulatory authorities. By effectively managing these risks, I can protect their financial stability, maintain compliance, safeguard player interests, and build a reputable, sustainability and successful online gaming business.</p>		
<b>Frameworks/Methodologies/Standards/Tools (More relevant ones)</b>		
<b>ISO and WLA-SCS requirements</b>		
<p>WLA-SCS:2020</p> <p>ISO 27001 can be used as a valuable framework for addressing online gaming risks by implementing effective information security management systems (ISMS) within the gaming organization. Here's how ISO 27001 can be applied to mitigate online gaming risks:</p> <p>Data protection and privacy: Online gaming platforms handle sensitive user data, including personal information, financial details, and gaming history. Compliance with data protection and privacy regulations, such as the General Data Protection Regulation (GDPR), is crucial. ISO 27001 helps organizations establish a systematic approach to managing and protecting personal data, ensuring compliance with relevant legal and regulatory requirements.</p> <p>National Institute of Standards and Technology (NIST) Cybersecurity Framework: The NIST Cybersecurity Framework provides a risk-based approach to managing cybersecurity risks.</p>		

General Data Protection Regulation (GDPR): Although primarily focused on data protection and privacy in the European Union (EU), the GDPR's principles and requirements can be relevant to online gaming platforms worldwide.

The CIS Controls provide a prioritized set of best practices for securing IT systems and data. These controls encompass a wide range of security measures, including network security, user awareness, incident response, and vulnerability management.

## Key Risk Control (Broad) Actions (KRC–Actions)

Area	Generic		Lottery/Gaming Specific Aspects
	Objective/Action	Outcomes	
<b>Responsible gaming</b>	<ul style="list-style-type: none"> <li>To promote responsible gambling</li> <li>To ensure that minors cannot access online gaming.</li> <li>Player protection</li> </ul>	<ul style="list-style-type: none"> <li>Responsible Gaming Certification</li> <li>Socially responsible advertising and marketing code.</li> <li>Including responsible gaming messages in the advertising and marketing.</li> <li>Responsible gambling officer assigned.</li> <li>Promote responsible gaming habits.</li> <li>Robust age verification mechanisms during account creation.</li> <li>Parental controls.</li> <li>It must clearly display an 'over 18's only' or other legislated age requirement sign.</li> <li>Advertising not targeted to under the legal gambling age.</li> <li>Clear gambling contract.</li> <li>Responsible Gambling policy.</li> <li>Advice on responsible gambling.</li> <li>Sources of help on problem gambling.</li> <li>Accepted self-assessment tool to determine risk potential.</li> <li>List of player protection measures that are available on the web site.</li> </ul>	<ul style="list-style-type: none"> <li>Promote responsible gaming practices and implement measures to prevent and address problem gambling. Provide resources for self-exclusion, set betting limits, offer responsible gaming tools, and provide educational materials on responsible gambling.</li> <li>Online gaming risks, particularly related to addiction and player protection, can have social and personal consequences for players. Excessive gambling can lead to financial difficulties, strained relationships, and negative impacts on mental health and well-being. Insufficient player protection measures can fail to address these issues effectively.</li> </ul>

		<ul style="list-style-type: none"> <li>Information to assist players in making informed decisions about their gambling available on the web site. (Dangers of gaming, chances of winning on the activity, pay-out ratios of the game, price structures of the game.</li> <li>Self-exclusion option.</li> <li>Betting limits option.</li> <li>to set limits on time option</li> <li>Set limit to money and losses option.</li> <li>Identifying problem gambling behaviour.</li> <li>Self-prohibited verification mechanisms.</li> <li>Clear information about games.</li> </ul>	
<b><u>Legal and Regulatory</u></b>	<ul style="list-style-type: none"> <li>Lack or inefficiency of a money laundering detection and control system.</li> <li>Lack or inefficiency of a fraud detection and control system.</li> <li>Personal data privacy protection.</li> <li>Third party intellectual property infringement.</li> <li>Regulatory changes.</li> </ul>	<ul style="list-style-type: none"> <li>Program for the detection of money laundering behavior: Program for the detection of fraudulent behavior &amp; Internal control systems that monitor unusual transaction volumes or fraudulent activities.</li> <li>Strong privacy policies and practices to safeguard players' personal information.</li> <li>Review of third-party logos, advertising, images, etc.</li> <li>Action plan.</li> </ul>	<ul style="list-style-type: none"> <li>Online gaming platforms are susceptible to fraud and cheating attempts by players or external actors. This includes activities such as collusion, identity theft, use of fraudulent payment methods, and the manipulation of gaming outcomes. Fraud and cheating risks undermine the fairness, credibility, and trustworthiness of the gaming platform.</li> </ul>
<b><u>Operational</u></b>	<ul style="list-style-type: none"> <li>Lack of availability of the central service Lack of internet service</li> </ul>	<ul style="list-style-type: none"> <li>Availability of backup systems.</li> <li>Availability of a backup provider</li> </ul>	<ul style="list-style-type: none"> <li>Internet gaming relies heavily on technology infrastructure, including gaming software, servers, network connectivity, and data storage systems.</li> </ul>

	<ul style="list-style-type: none"> <li>Software error</li> <li>Power outage</li> <li>Operating error</li> </ul>	<ul style="list-style-type: none"> <li>Acceptance tests before the implementation of a software in production</li> <li>Communication of the service interruption to website.</li> <li>Restoration plan to the previous point.</li> <li>Team available to resolve possible incidents.</li> <li>Availability of alternative energy source</li> <li>Operating procedures.</li> <li>Continuous training to operators.</li> <li>Communication of the incident</li> </ul>	<p>Technological risks include system failures, software bugs, compatibility issues, hardware malfunctions, and disruptions in internet connectivity. These risks can result in game interruptions, delayed payments, dissatisfied players, and reputational damage.</p>
<b><u>Security</u></b> <b><u>Cybersecurity</u></b>	<ul style="list-style-type: none"> <li>Identity theft</li> <li>Phishing emails</li> <li>DDoS attacks.</li> </ul>	<ul style="list-style-type: none"> <li>Encrypted personal data.</li> <li>Restricted access to data</li> <li>Access audit log.</li> <li>Restricted access to production equipment.</li> <li>In the game control it must be made clear that data will never be requested through mails.</li> <li>Give the message on the sales website.</li> <li>Plan for DDoS attacks.</li> <li>Increase bandwidth.</li> <li>Implement server-level DDoS protection.</li> <li>CDN / Multi CDN Solution.</li> <li>Firewall or router to drop incoming ICMP packets.</li> </ul>	<ul style="list-style-type: none"> <li>Online gaming platforms are vulnerable to cybersecurity risks, including hacking, data breaches, malware attacks, and unauthorized access to sensitive player information. These risks can lead to financial losses, reputational damage, legal liabilities, and the loss of player trust. Robust cybersecurity measures are necessary to mitigate these risks and protect the integrity and security of online gaming operations.</li> </ul>

	<ul style="list-style-type: none"><li>Data breaches</li></ul>	<ul style="list-style-type: none"><li>Block DNS responses from outside your network (by blocking UDP port 53).</li><li>Employee Training and Awareness.</li><li>Data Backup and Encryption.</li><li>Malware detection software running on both your servers (hosted or not) and workstations and ensure that your firewalls are up and secure</li><li>Strong Password Security Policies.</li><li>Timely Patch Installation and System Updates.</li><li>Restrict Access to Sensitive Data.</li></ul>						
<u>Communication</u>	<ul style="list-style-type: none"><li>False messages on social networks.</li></ul>	<ul style="list-style-type: none"><li>Communication plan in case of false messages on the networks.</li></ul>	<ul style="list-style-type: none"><li>Reputation and Brand Risk: Adverse events or negative publicity related to online gaming operations can have a significant impact on the reputation and brand image of the gaming operator. Negative media coverage, player complaints, data breaches, or unethical practices can lead to loss of trust, reduced player participation, and reputational damage.</li></ul>					
<u>Business</u>	<ul style="list-style-type: none"><li>Unattractive sales website.</li><li>Competitive online gaming environment – Market loss.</li></ul>	<ul style="list-style-type: none"><li>User testing/customer experience.</li></ul>						
Key Performance Indicators (KPI) (radar diagram)		Means of assessments of controls and management effectiveness						
		<table><tr><td>Self-assessment</td></tr><tr><td>Peer assessment</td></tr><tr><td>Second party assessment</td></tr><tr><td>Accredited third party assessment</td></tr><tr><td>EL Certification (eventually)</td></tr></table>		Self-assessment	Peer assessment	Second party assessment	Accredited third party assessment	EL Certification (eventually)
Self-assessment								
Peer assessment								
Second party assessment								
Accredited third party assessment								
EL Certification (eventually)								