World Lottery Association

Enterprise Risk Management in the lottery and gaming sector

Report issued by the WLA Security and
Risk Management Committee (SRMC)
in October 2020

Contents

Executive Summary

In July-August 2020 the WLA conducted the survey "Risk management in the lottery sector" among its lottery and sports betting members. The aim behind the Survey, created by the WLA Security and Risk Management Committee, was to have an industry-wide picture of risk perception and priorities.

According to the results, risk is a regular agenda item at Executive or Board of Directors level of WLA members and the effectiveness of the control environment is tested annually, at a minimum. Almost all of the WLA members who participated in the Survey (95%) can count on a Business Continuity Plan (BCP) which only proved effective for one-third of the responders in facing the pandemic of Covid-19.

Cybersecurity is perceived as the highest risk in terms of both potential impact and likelihood. Other information and communication technology (ICT) security risks that were perceived as high in the likelihood ranking are those related to logical access and the information security management system. Operational compliance and fraud are also key topics on the risk map.

In terms of residual risks and taking into account the controls that are put in place to mitigate the impact of risks, the perception of risk impact is mostly clustered around low and irrelevant levels. This result shows that there is an optimistic view of the controls identified, therefore making it imperative to delve deeper into the compliance activity to confirm the effectiveness of these controls.

Regarding changes in risk perception when compared to a pre-Covid-19 era; cybersecurity is still confirmed as one of the top priorities of lottery and gaming companies, however, unsurprisingly, health and safety are now included amongst the most relevant risks for the business.

The most important lesson to be learned from the pandemic concerns the organization of human resources and the use of digital tools to facilitate the business operations. The entire industry realized that the physical presence of employees in the company's premises could be limited to a few people (e.g. data center, control room, prize office) without any material impact on the company's ability to run its business properly and efficiently. It is timely, therefore, to ponder on how to adapt to the future homeworking environment by reshaping organizations, review processes, innovate products and modify cost and capital investment priorities. This, together with customer engagement in the new normal, are the immediate operational challenges facing the lottery industry.

The report illustrated in this document has a twofold objective:

1. Raising awareness of Enterprise Risk Management (ERM) among the WLA members; and
2. Sharing best practices with WLA members, thus providing a service aimed at supporting those members facing critical situations in the future such as the current one derived from the Covid-19 outbreak.

Background

What has happened and continues to transpire in 2020, regarding the Covid-19 outbreak, has shown us the importance of a good understanding of risks and, consequently, being prepared to manage a crisis and to try to reduce the impact on employees, customers, and our businesses.

Being prepared to manage risks is not only about *black swans*, which are defined as extremely rare and unpredictable events with severe consequences, like the COVID-19 outbreak. Risk management is about thinking ahead, drawing-up different scenarios, evaluating potential impacts and, most importantly, being aware of the risks. Raising the awareness on Enterprise Risk Management (ERM) and providing information to initiate or update plans to recognize and anticipate risks, thereby minimizing their impact, is among the goals of the WLA Security and Risk Management Committee (SRMC).

In July-August 2020 a survey was conducted amongst WLA members aimed at gathering insight into an industry-wide picture of risk perception and priorities. This paper presents the results of the Survey, showing an in-depth picture of how the lottery industry is assessed by our members with regards to risk management.

The WLA Security and Risk Management Committee (SRMC) is comprised of security specialists from the lottery and gaming sector, as well as other lottery professionals from around the world. SRMC members are duly appointed by the WLA Executive Committee. For more than two decades, the WLA SRMC has developed and maintained an internationally recognized security standard for the lottery and gaming sector known as the WLA Security Control Standard (WLA-SCS). The WLA SRMC reviews all security control standards on a regular basis and acts as a focal point for the sector on security and risk management issues.

The Panel

The Survey was sent to 80 participants and we received a response rate of 50%. We thank all those members who took the time to respond. The geographical split of responders is also consistent with that of WLA members and is as follows:

- 41% in Europe and near East
- 22% in North and South America
- 20% in Asia Pacific
- 17% in Africa

From a business standpoint, 98% of the companies interviewed run a lottery business. In most of the cases, other gaming operations are run beside the lottery business and 7% of the panel has a presence across all gaming segments (see Appendix 3).

Within their respective organizations, 68% of the responders lead or belong to a control function like Risk Management, ICT Security, Audit, while 12% were at and executive level holding titles such as chairman, CEO, General Manager or CFO.

A copy of the Survey's question s is reproduced in the Appendix 1 below.

WLA Members’ risk management framework

Based on the Survey results, we are pleased to report that the risk management culture appears to be widespread among lottery companies around the world.

- For **95%** of the panel, risk is a regular agenda item at Executive or Board of Directors level.
- **49%** answered that this topic hits the top management agenda at least quarterly or monthly.
- The remaining companies are rather evenly split between yearly and twice-a-year review frequency.

The effectiveness of the control environment is also tested (on an annual basis) in **95%** of cases.

- **78%** of responders confirmed that their respective companies have an agreed Risk Appetite (i.e. how much risk you are prepared to accept) and Risk Tolerance (i.e. the maximum acceptable amount of risk, or how volatile your expected results can be).
- **80%** of the panel believes that the risk environment within their respective companies is mature or maturing.

This implies that the ERM framework is well advanced among WLA members and that they seem to have a quantitative approach to risk, signaling a rather high ERM maturity level.

From an organizational standpoint:

- **72%** of the companies manage their ERM with a risk manager and/or a dedicated team.
- **75%** of the responders answered that risk management function reports to top management, be it the CEO, the General Manager, the CFO, or the Management Committee.

On average, the risk management team is made up of five resources:

- The risk management team ranges from one (**10%** of occurrences) to seven or more (**21%** of occurrences). The size of an ERM team depends on the size of the company, its complexity and diversification.
- For **59%** of the teams, the number of dedicated staff ranges between four to six people.
- **72%** of the responders are also responsible for business continuity.

The Results

The WLA Survey was built around a list of 20 risks, cherry-picked from a Risk Library of approximately 60 different items. Attention was drawn to those risks that were most likely to be impacted by the recent pandemic and its devastating effects on people and economies around the world. The risk library containing the selected 20 risks can be found in Appendix 2.

The first set of questions was aimed at determining the perceived potential impact and probability of undesirable events, or Inherent Risk[1].

Responders were asked to assess the severity of impact for each risk on a 5-step scale from Extremely Low to Extremely High. Severity was determined by a blend of financial, reputational, and compliance consequences.

The same 5-step scale was used to determine the probability of occurrence for each of the 20 risks over the next three years.

Gross Risk

The average of impact and probability scores were blended to assess the magnitude of each Inherent Risk, the result of which is an overview of WLA members' Inherent Risk average perception. For several risks, the standard deviation shows a particular dispersion of answers, consistent with three features of the group of responders: (a) geographical footprint; (b) business diversity; and (c) ownership (State or privately owned, or a blend of the two).

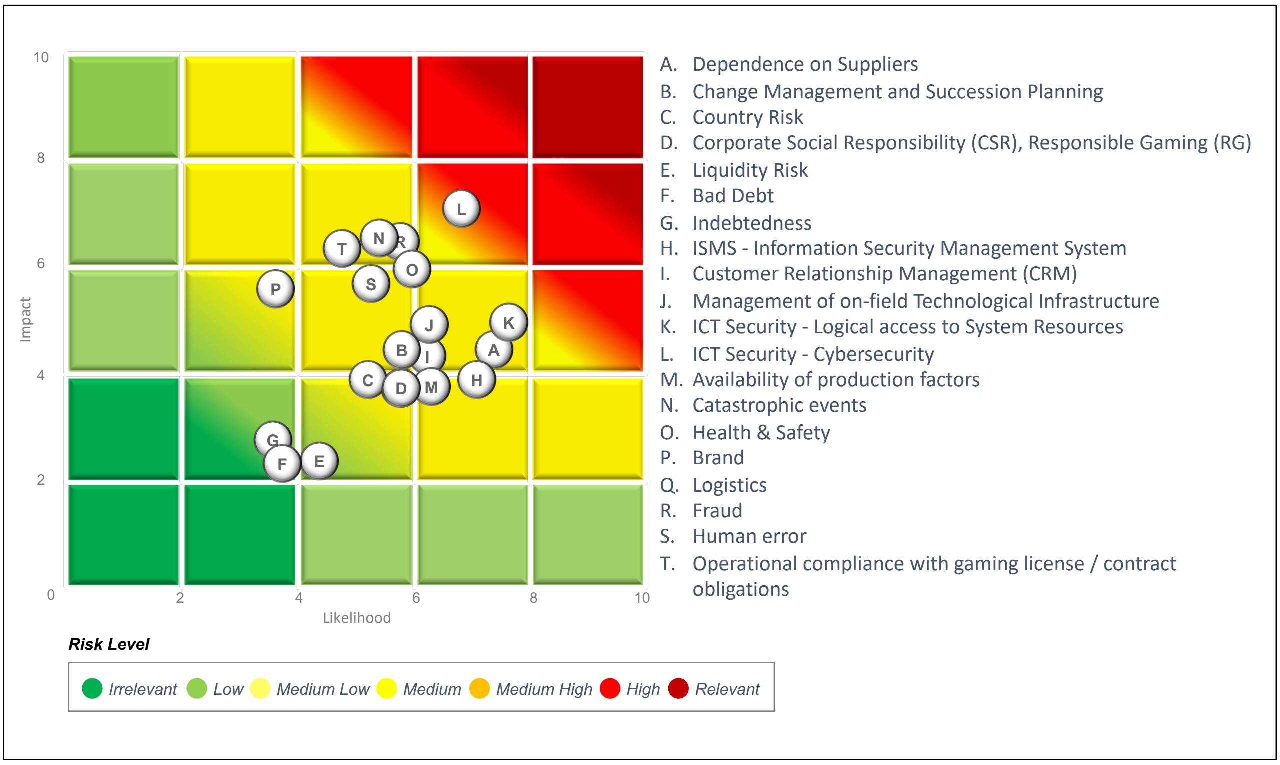

Figure 1. Overview of Inherent Risk

[1] A risk in its raw unmitigated form is an Inherent or Gross risk. Controls are put in place to mitigate a risk and once the risk is mitigated it can be assessed as a residual risk. The more effective the control, the less a company is exposed to that risk. The control's effectiveness is therefore the bridge between Inherent Risk and Residual Risk, or the level of risk that a business is facing. Risk cannot be completely eliminated, therefore very effective controls reduce a risk to a minimum level, but never to zero.

According to the panel, the most relevant risk in the lottery and gaming business is **Cybersecurity (L),** with relatively high levels of perceived likelihood and impact. This is not a surprise, since information and communication technology (ICT) is at the core of a transaction-based business, like lotteries or any other game of chance. Other **ICT Security risks (H, K)** – like those related to logical access and the information security management system – are also high in the likelihood ranking and just a notch below Cybersecurity in terms of estimated impact.

Two other typical risks in the gaming business rank high in terms of impact: **Operational Compliance (T)** and **Fraud (R).** Interestingly enough, the timing of the Survey – i.e. during the pandemic – might have influenced the likelihood of **Catastrophic Events (N), Health and Safety (O),** and **Dependence on Suppliers (A)**.

The perceived likelihood and impact of financial risks is surprisingly low. As far as indebtedness is concerned – i.e. an impairment between the company's ability to generate cash and its capacity to repay debt – a possible explanation could be that more than 50% of responders belong to state-owned companies. When looking at the possible inability of a business to meet its payment deadlines or the default risk of its customers, it is nonetheless difficult to explain the outcome of the Survey.

Control Effectiveness and Residual Risk

According to the Survey, in the lottery and gaming universe, controls are assessed as particularly effective (c. 80% or more) in mitigating the three financial risks (Liquidity Risk, Bad Debt and Indebtedness), the risks surrounding the Information Security Management System, and those risks to compliance with gaming licenses/contractual obligations. This picture seems consistent with the typical human and capital resources allocation priorities for a lottery company.

Country risk, Catastrophic Events and **Human Error** are the areas where the responders feel less "protected" by control effectiveness.

The chart below shows that based on the Survey results, overall, Residual Risk levels are mostly clustered around Low and Irrelevant levels; demonstrating that this may be an optimistic view of the controls identified. It would be interesting to delve deeper into the compliance activity to confirm the effectiveness of these controls.

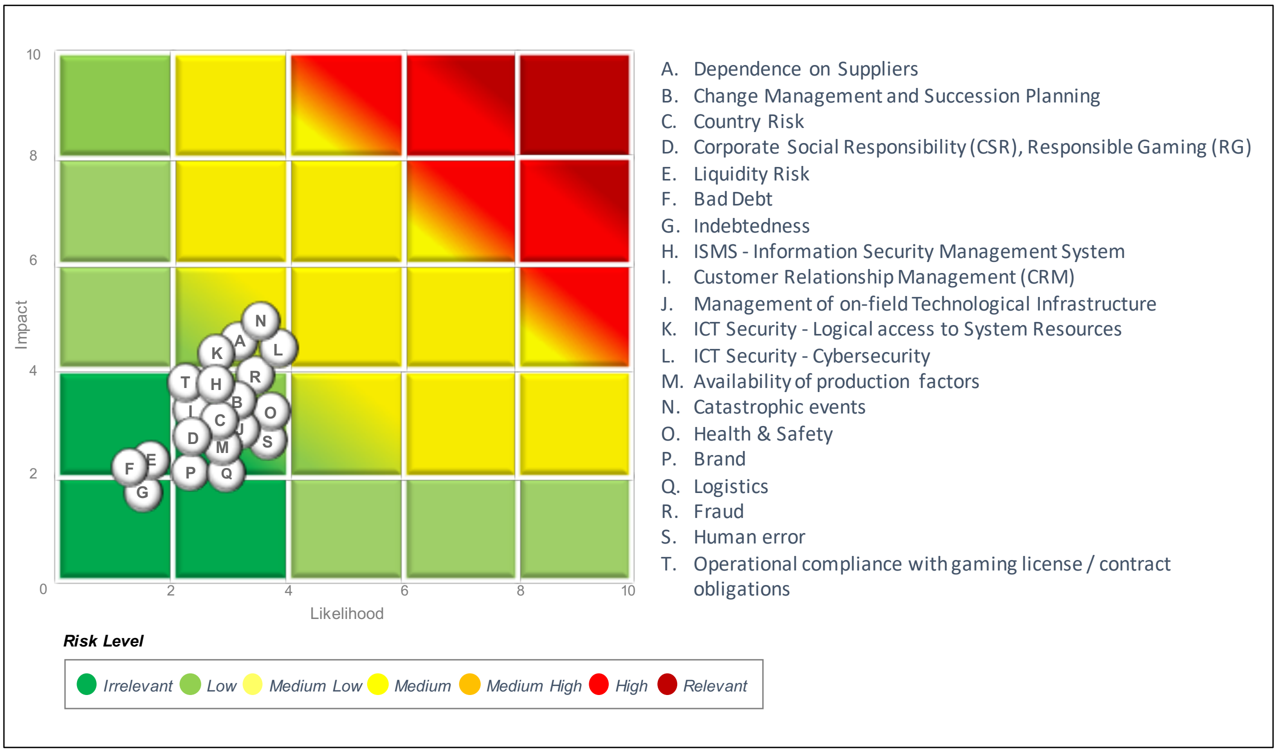

Figure 2. Overview of Residual Risk

Changes in Risk perception vs 2019

On average, responders believe that **Cybersecurity (L)** and **Health and Safety (O)** risks are more relevant for their respective businesses today, compared to 2019. **Dependence on Suppliers (A)**, **Catastrophic Events (N)** and **Change Management (B)** are also mentioned for their increased importance. Again, financial risks – **(E, F, and G)** – are at the bottom of the list as they are perceived as less important when compared to 2019.

Risk	Chg.	Risk	Chg.
ICT Security - Cybersecurity	+++	ISMS - Information Security Management System	+
Health & Safety	+++	Fraud	=
Dependence on Suppliers	++	Customer Relationship Management (CRM)	=
ICT Security - Logical access to System Resources	++	Management of on-field Technological Infrastructure	=
Catastrophic Events	++	Human Error	=
Change Management and Succession Planning	++	Brand	=
Corporate Social Resp. (CSR), Responsible Gaming (RG)	+	Logistics	-
Operational Compliance with License / Contract	+	Liquidity Risk	-
Availability of Production Factors	+	Bad Debt	--
Country Risk	+	Indebtedness	---

Key: +++ more important, = equally as important, --- less important.

BC Plans from a pandemic perspective

It is not the aim of this report to understand why the perception of certain risks changed with the pandemic although this would be an interesting case-study for behavioral science experts, particularly when looking at likelihood assessments.

What is relevant are the lessons learned from the Survey, which can help businesses in fine-tuning and revising their mitigation plans.

Were lottery and gaming companies prepared to face such a *black swan*? According to the responders, **95%** of the panel have a Business Continuity Plan (BCP):

- Less than **33%** affirms that the BCP proved to be "very effective" during the pandemic.
- **54%** believes that their BCP was "somewhat effective" or "somewhat ineffective"
- **10%** answered "very ineffective".

Clearly facing such a disruptive and prolonged crisis obliged many companies to tweak and adjust their BCP, particularly in the health & safety area. Participants were asked whether during or in the aftermath of the pandemic their respective companies took any unplanned action or enhanced the BCP in any of the listed areas and this is the result:

	YES	NO
Health & safety risk mitigation	98%	2%
Supply chain / logistics risk mitigations	68%	32%
IT / cyber risk mitigations	73%	27%
Financial risk mitigations	61%	39%
Internal & external communication	85%	15%

Lessons learned

Responders pointed to several actions adopted during the pandemic to mitigate risks for business. Below is a list freely adapted from the answers received. As you may expect, during the lock-down company buildings were in fact locked and, in many countries, land-based games were temporarily closed, due to governmental decisions. Like in many other industries, large-scale homeworking was the prevailing turn-around solution adopted by gaming companies to keep operations up and running.

All of a sudden, the entire industry realized that the physical presence of staff on the company's premises could be limited to a few people (data center, control room, prize office, etc.) without any material impact on the company's ability to run its business properly and efficiently. This is the most important lesson learned from the pandemic and, at the same time, the next challenge: pondering on how to adapt to the future homeworking environment by reshaping organizations, reviewing processes, innovating products and modifying cost and capital investment priorities.

Main actions taken by gaming operators following the pandemic (obviously on top of all the measures adopted to ensure social distancing):

- Homeworking for almost all employees
- Expansion and strengthening of secure VPN connections
- Adapt BCPs in a dynamic way
- Financial risk monitoring
- Contingent initiatives to manage logistics
- Digitalization of previously manual processes
- Emergency laptop-provisioning plan
- Enhance and facilitate communication towards and among employees, including online training
- Pro-bono initiatives to support the Government's supply of protective equipment
- Explore feasibility of and, if possible, implement electronic draws to replace physical draws
- Divide critical teams into two sub-groups to avoid contagion and create a back-up
- Introduce a back-up site for draws
- Pre-approve budget to pay for expired winning tickets
- Digital-driven product innovation
- Re-assessment of risks across all business units following the pandemic
- Adjustments in salary and incentive plans

Finally, responders were asked to draw a list of what didn't work properly and could be improved. Here below are the most interesting comments received:

- "All of a sudden, we realized to be short of hardware stock (laptops, etc.) to face the emergency".
- "IT infrastructure capacity challenged by the emergency; it took some time to react".
- "Emergency was longer than any event foreseen in BCP".
- "Troubles in managing call center and customer care services".
- "BCP foresaw back-up sites for employees but physical alternatives were not viable in the pandemic".
- "Crisis management group was too big".
- "We were not allowed to sell our products online".
- "We thought it easier to get hand sanitizers and face masks, we'll keep them in stock".

Hopefully, lessons learned will feed into improving the BCPs of all businesses.

Appendix 1: WLA Survey – Risk management in the lottery sector

1. Please indicate the region where your company is located.
   - Africa
   - Asia Pacific
   - Europe & Near East
   - Latin America
   - North America & the Caribbean

2. Please describe your company's business by ticking where appropriate.
   - Lottery
   - Instant Tickets
   - Digital Gaming
   - Sports Betting
   - Horse racing
   - Machine Gaming (VLTs, etc.)
   - All of the above

3. Please describe your role in the organization.

4. Is risk a regular agenda item at your Executive/Board level?
   - No
   - Yes, at least once a year
   - Yes, at least twice a year
   - Yes, at least every quarter
   - Yes, at least every month

5. Is the effectiveness of the control environment reviewed annually? Yes or no

6. Does your company have an agreed Risk Appetite and Tolerance? Yes or no

7. Would you assess your company's risk environment as Mature or Maturing? Yes or no

8. Does your company have a risk manager and dedicated risk team? Yes or no

9. How many people are in your company's risk team?

10. Does the risk team also deal with Business Continuity Management (BCP) Yes or no

11. Whom does the risk team report to?

Questions 12, 13, 14, and 15 are based on the risk library in Appendix 2.

12. When thinking of the major risks your business is facing, please rank each of the 20 risks below based on your perceived magnitude. Indicate, assuming the risk occurs, the severity of the impact as a blend of financial, reputational and compliance impact for your company. Please provide your answers on a scale of 1 (Extremely low) to 5 (Extremely high)

13. Make your assessment on the probability that each risk occurs within the next three years. Please keep in mind that the probability should not be underestimated if the risk already occurred in the past. Please provide your answers on a scale of 1 (Extremely low) to 5 (Extremely high)

14. How effective are the controls deployed by your organization to mitigate each risk? "Very effective" controls mean the risk exposure is maximum, while "Very Effective" controls minimize the risk but never eliminate it. Please provide your answers on a scale of 1 (Very ineffective) to 5 (Very effective)

15. How relevant is the risk today for your business compared to 2019? Please provide your answers on a scale of 1 (much less relevant) to 5 (much more relevant)

16. Does your company have a Business Continuity Plan (BCP)? Yes or no

17. How effective was the implementation of the BCP to mitigate the impact of the recent COVID-19 outbreak? Please provide your answers on a scale of 1 (Very ineffective) to 5 (Very effective)

18. During (or in the aftermath of) the pandemic, did your company take any previously unplanned actions or enhanced the BCP in the following areas?
    - Health & safety risk mitigation
    - Supply chain / logistics risk mitigations
    - IT / cyber risk mitigations
    - Financial risk mitigations
    - Internal & external communication

19. Are there some other actions / best practices / hints your company identified or implemented to mitigate risks for the business during the pandemic? If yes, please provide some information.

20. Please elaborate on what actions have not worked during the pandemic, and on possibilities for improvement.

Appendix 2: Risk Library

Area	Type	Risk	Description
Strategic	Strategy & Initiatives	Dependence on Suppliers	Failure to deliver by a supplier, delays on scheduled supplies or pricing power may compromise the achievement of company's objectives and/or impact revenues and profitability
Strategic	Strategy & Initiatives	Change Management and Succession Planning	New processes, systems or organization don't work properly because of resistance to change, poor leadership, disruption, etc., impacting earnings or the value of assets. Also, inadequate succession planning may weaken the ability to achieve company goals.
Strategic	Market Environment	Country Risk	Political, social or economic changes may increase costs or reduce sales
Strategic	Communication	Corporate Social Responsibility (CSR), Responsible Gaming (RG)	Unsuitable CSR or RG practices (i.e. skewed or shallow, window dressing for marketing purposes, excess of bureaucracy, etc.) may negatively impact on the company's reputation, governance, earnings, ability to achieve objectives.
Financial	Liquidity & Credit	Liquidity Risk	Company's inability to meet its cash obligations, as a consequence of poor planning, lack of financial resources, limited access to capital markets, etc.

Area	Type	Risk	Description
Financial	Liquidity & Credit	Bad Debt	Customers may fail to make payments due, negatively affecting the company's earnings and cash flow.
Financial	Capital	Indebtedness	Inability to maintain an adequate financial structure (i.e. over/under indebtedness as measured by debt/equity and/or leverage ratio) may impact earnings growth or the ability to stay in business. A credit rating downgrade may increase interest expense or trigger events of default
Operations	Games & Services Ops	ISMS - Information Security Management System	A threat to ISMS assets' confidentiality, integrity and/or availability may prevent the company from achieving its goals or have an impact on its reputation
Operations	Games & Services Ops	Customer Relationship Management (CRM)	A CRM weakness impairs the company's ability to understand the needs/satisfaction of its customers, impacting revenues and reputation
Operations	Games & Services Ops	Management of on-field Technological Infrastructure	Poor management (inventory, installation, maintenance, divestment, etc.) of on-field technological infrastructure (i.e. terminals, gaming machines, POS, last-mile network, screens) may impact the value of assets, increase costs or reduce revenues

Area	Type	Risk	Description
Operations	Information Technology	ICT Security - Logical access to System Resources	Inappropriate management of access to systems may result in impact on confidentiality, integrity and/or availability of information, with potential economic and reputational consequences for the business
Operations	Information Technology	ICT Security - Cybersecurity	Offensive actions that target the Company's IT assets (i.e. information systems, infrastructures, networks, devices, etc.) may impact confidentiality, integrity and/or availability of information, with potential economic and reputational consequences for the business
Operations	Business Interruption	Availability of production factors	Occurrence of one or more events that interfere with the company's ability to function in the short or longer term (electrical or telecommunications fault, fire, or any other unavailability of any key production factor, due to internal or external causes). Includes BI events attributable to suppliers
Operations	Business Interruption	Catastrophic events	Occurrence of a "black swan" (extremely low probability, extremely high impact event) with disruptive effects on a local or larger scale, like massive terrorist attacks or natural disasters (i.e. flood, earthquake, drought, pandemia, forest fire, etc.), and the resulting Government actions (i.e. lockdown, etc.)
Operations	People	Health & Safety	A hazard is a potential source of harm or adverse health effect on a person or persons. Inappropriate hazards management can lead to the harm, injury, death, or illness of a worker in a company's workplace

Area	Type	Risk	Description
Operations	Sales & Marketing	Brand	Loss of value of a brand or failure of a new brand as a consequence of issues in customer experience and/or perception, recognition, awareness, positioning, loyalty, etc.
Operations	Supply Chain	Logistics	A negative occurrence in Logistics (i.e. procurement, purchasing, inventory, warehousing, distribution, transportation, etc.) may increase costs, reduce revenues or damage reputation
Operations	Fraud, Corruption, Human error	Fraud	Fraud: unlawful behavior through which a person with artifices or deception, by inducing someone in error, causes himself or others an unfair profit at the expense of someone else. Frauds may generate losses and/or reputational damage.
Operations	Fraud, Corruption, Human error	Human error	Unexpected failure of a human action intended to achieve a desired outcome (i.e. failure to execute a manual control, bad execution of procedure, etc.) may impact earnings or reputation
Operations	Games & Services Ops	Operational compliance with gaming license / contract obligations	The company can incur in penalties or litigations in case it does not comply with its contractual obligations or service levels (SLAs)

Appendix 3: Type of business' distribution

The table below shows the type of business' distribution of the lottery and gaming companies interviewed.

% of Panel	Lottery	Instant Tickets	Digital Gaming	Sports Betting	Machine Gaming	Horse Racing	All Games
17%	X						
17%	X	X					
17%	X	X	X	X			
10%	X	X	X				
7%							X
7%	X	X	X	X	X		
7%	X	X			X		
2%		X				X	
2%	X	X	X		X		
2%	X	X	X	X		X	
2%	X	X				X	
2%	X	X		X			
2%	X	X		X		X	
2%	X			X		X	

World Lottery Association
The World Lottery Association (WLA) is an international trade organization that represents state-sanctioned lotteries and sports betting operators, as well as suppliers to the global gaming industry. According to WLA By-Laws, member lotteries and sports betting operators must be licensed or authorized to conduct lotteries or sports betting by the jurisdiction within which their gaming products are sold.

WLA SRMC
The WLA Security and Risk Management Committee (SRMC) comprises security specialists from the lottery and sports betting sector, as well as other lottery professionals from around the world. SRMC members are duly appointed by the WLA Executive Committee. The WLA SRMC is authorized, to oversee the selection process of certification auditors, and to advise the WLA and its members on security and risk management issues.

Authors of the survey and the report: Giuliano Boggiali, Lottomatica; Thibault Bulabois, Française des Jeux; and Kate Michael, Camelot UK